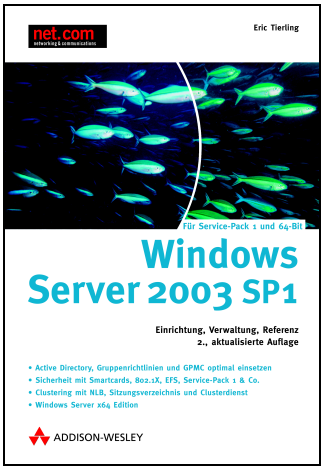
ISA Server 2004

net.com
networking & communications

Netzwerke, Betriebssysteme, Sicherheit ... hierzu bietet Ihnen die Reihe net.com umfassende, praxisnahe Information. Neben Fragen der Systemverwaltung greift sie auch Themen wie Protokolle, Technologien und Tools auf. Profitieren Sie bei Ihrer täglichen Arbeit vom Praxiswissen unserer erfahrenen Autoren.



Windows Server 2003

Eric Tierling
1344 Seiten, € 59,95 [D]
ISBN 3-8273-2243-X

Der Bestseller jetzt auch für Service Pack 1 und 64-Bit! Ausführlich widmet sich dieses Buch allen wesentlichen Aspekten von Windows Server 2003. Die detaillierte Beschreibung von Active Directory, Gruppenrichtlinien, Windows NT-Domänenupgrade, TCP/IP-Diensten und Sicherheitsmerkmalen ermöglicht Unternehmen einen optimalen Einsatz. Clustering mit Netzwerklastenausgleich und Clusterdienst, E-Mail-Server, GPMC, Terminaldienste, Remotedesktop und Webverwaltung, Volumen-Schattenkopie sowie die Smartcard-Integration und sichere Wireless-LAN-Unterstützung stellen weitere Highlights dieses Buches dar.

Exchange Server 2003

William Boswell
900 Seiten, € 69,95[D]
ISBN 3-8273-2227-8

William Boswell beantwortet die drei Schlüsselfragen eines jeden Administrators: Wie funktionieren die Features tatsächlich? Wie hole ich das meiste aus meinem System heraus? Was mache ich bei Problemen? Dabei legt er ein besonderes Augenmerk auf Systemabhängigkeiten und beschreibt z.B., wie Exchange problemlos mit Outlook und anderen E-Mail-Clients zusammenarbeitet. Außerdem berücksichtigt er zahlreiche nützliche third-party-tools, die dem Administrator die Arbeit erleichtern und zeigt, dass Exchange 2003 nicht nur ein Mail-Server, sondern ein fester Bestandteil der Kommunikations-Infrastruktur des Unternehmens ist.

PEARSON Education

ADDISON-WESLEY

Stephanie Knecht-Thurmann

ISA Server 2004

Das Handbuch für Installation und Administration

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

Bibliografische Information Der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

10 9 8 7 6 5 4 3 2 1

08 07 06

ISBN 3-8273-2330-4

Einbandgestaltung: Marco Lindenbeck, webwo GmbH, mlindenbeck@webwo.de
Lektorat: Sylvia Hasselbach, shasselbach@pearson.de
Korrektorat: Michelle Kottemann, Bonn
Herstellung: Claudia Bäurle, cbaeurle@pearson.de
Satz: MediaService, Siegen, www.media-service.tv
Druck und Verarbeitung: Bercker, Kevelaer
Printed in Germany

Inhaltsverzeichnis

Vorwort

In den letzten Jahren hat das Thema Sicherheit in Windows-Netzwerken immer größere Bedeutung erlangt. Auch die zum Teil immensen Kosten bei Ausfällen, die auf Sicherheitslücken zurückzuführen sind, haben bei vielen kleinen und mittleren Firmen ein Umdenken bewirkt. Von einem Randthema vor einigen Jahren hat sich die Internet-Sicherheit zu einem durchaus unternehmenskritischen IT-Bereich entwickelt. Allein der Imageverlust, der entstehen könnte, wenn ein Unternehmen Viren oder Würmer in Mails an Kunden oder Lieferanten verschickt, ist heute ein ernst zu nehmendes Thema. Selbstverständlich werden in diesem Bereich Produkte und Konzepte besonders aufmerksam beobachtet.

Der Microsoft ISA Server 2004 stellt unter diesem Aspekt eine integrierte und skalierbare Komplettlösung dar. In der Standardversion auch als ein Bestandteil des Small-Business Server 2003, ist er an die Bedürfnisse kleiner und mittlerer Unternehmen angepasst. In der Enterprise-Version erfüllt er die Anforderungen an verteilte Standorte mittlerer bis großer Unternehmen. Der ISA Server 2004 ist gut in bestehende Microsoft-Architekturen zu integrieren. Er bietet z.B. optimierte Zusammenarbeit mit Active Directory, Exchange, SQL-Server, IIS usw.

Durch die integrierten Komponenten lässt er sich optimal auf die Bedürfnisse aller Arten von Netzwerken und Sicherheitskonzepten anpassen und problemlos integrieren. Daneben stellt der ISA Server 2004 eine Schlüsselkomponente in der Trustworthy Computing-Initiative dar, die die Sicherheit in Netzwerken entscheidend verbessern soll.

Warum nun ein Buch zu diesem Thema? Höchstwahrscheinlich aus demselben Grund, warum Sie als Leser zu einem Buch greifen. Nahezu alle relevanten Informationen finden sich zu diesem Thema auch in der Microsoft Knowlegde Base, den Microsoft Newsgroups und in den weiteren veröffentlichten Informationen von Microsoft. Dieses Material ist jedoch sehr detailliert und darum umfangreich. Manchmal wird man von der Fülle regelrecht erschlagen.

Für den Einstieg, das Nachschlagen einer bestimmten Problemstellung ist ein Buch, das diese Information strukturiert und gegliedert darstellt, eine echte Hilfe.

Dieses Buch richtet sich in erster Linie an Administratoren, technische Projektleiter, Consultants und Berater, die im Unternehmensumfeld kleine, mittlere und große Netzwerke designen und den Einsatz von ISA Server 2004 planen. Neben den planerischen Aspekten und Vorüberlegungen sowie der Installation wird auch auf Update-Szenarien und natürlich den eigentlichen Tagesbetrieb eingegangen. Die Inhalte habe ich meiner täglichen Arbeit entnommen. Sie sind daher stark an der Praxis orientiert. Es war nicht beabsichtigt ein Sicherheitskompendium zu verfassen, sondern anwendbare Informationen zu vermitteln.

Mein Dank gilt an dieser Stelle meiner Lektorin Frau Sylvia Hasselbach, die dieses Projekt konstruktiv und kompetent begleitet hat, meinem Mann für seine Geduld und auch seine fachliche Kritik, die manches Gute noch verbessert hat, und nicht zuletzt auch Ihnen, dem Leser. Ich hoffe, dass dieses Buch Ihnen bei der Planung, der Implementierung und dem Einsatz des ISA Server 2004 eine echte Hilfe ist.

Barsinghausen im September 2005

Stephanie Knecht-Thurmann

Die Autorin

Stephanie Knecht-Thurmann berät seit 2002 mit Ihrer Firma Knecht-Consult in Barsinghausen Unternehmen zum Einsatz von Microsoft-Produkten in unternehmenskritischen Bereichen. Weitere Schwerpunkte ihrer Tätigkeit sind neben dem Projektgeschäft (z.B. die Beratung eines namhaften Zeitungsverlages in Vancouver/Kanada und Internet-basierte Projekte für verschiedene Firmen in Taschkent/Usbekistan) auch unterschiedliche Migrationsprojekte und die Anbindung verschiedener Directory Services an das Active Directory mittels Metadirectory-Konzeptionen sowie Veröffentlichungen zu diesen Themenbereichen mit starkem Praxis-Bezug. Im Jahre 2003 erschien sehr erfolgreich ihr Buch „Active Directory“ bei Addison-Wesley sowie 2004 das Buch „Small Business Server 2003“ ebenfalls in diesem Verlag. Weitere Veröffentlichungen sind in Arbeit.

Die Icons in diesem Buch

Sie finden an verschiedenen Stellen im Text Icons, die Sie auf Besonderheiten, Gefahren und zusätzliches Material auf der Buch-CD hinweisen sollen. Im Einzelnen handelt es sich hierbei um folgende Icons:

Hier finden Sie Hintergrundinformationen zum gerade behandelten Thema und Hinweise, wie Sie Ihr Wissen noch vertiefen können.

Hier erhalten Sie Tipps und Tricks, die Ihnen bei Ihrer Arbeit helfen.

Hier erfahren Sie, welche Fehler und Probleme auftreten können und wie Sie diese am besten beseitigen und was Sie unbedingt vermeiden sollten.

Hier erhalten Sie Hinweise auf das Material, das sich auf der Buch-CD befindet.

1 Der ISA Server 2004 stellt sich vor

Zwei Funktionen in einer Lösung

Der ISA Server 2004, der mit vollständigem Namen Internet Security and Acceleration Server heißt, besteht aus zwei verschiedenen Funktionen, die in einem Produkt vereint worden sind. Auf Seiten der „Internet Security" steht eine komplette Firewall- und VPN-Lösung, auf Seiten der „Acceleration" ein Server für das Webcaching. Beide Funktionalitäten werden in den Kapiteln 1.1 und 1.2 ausführlich vorgestellt. Über den ISA Server werden Firmennetzwerke beliebiger Größe an das Internet angebunden. Der ISA Server 2004 bietet eine umfassende Microsoft-Lösung für die *Trustworthy Computing Initiative*.

Die Trustworthy Computing Initiative

Die Trustworthy Computing Initiative ist eine von Microsoft ausgehende Initiative, um das Engagement im Bereich der Sicherheit zu unterstreichen. Zur Umsetzung dieser Initiative sind von Microsoft einerseits spezielle Applikationen entwickelt worden, aber auch in den Betriebssystemen integrierte Sicherheitsfeatures zählen dazu. Neben dem ISA Server 2004 gehören beispielsweise auch der *Microsoft Baseline Security Analyzer (MBSA)*, die *Windows Software Update Services (WSUS)* oder der *Microsoft Identity and Integration Server (MIIS)* dazu.

Das dreistufige Sicherheits-Framework

Die Trustworthy Computing Initiative basiert auf dem *SD Security Framework*. Dieses Framework besteht aus den drei *Komponenten Secure by Design*, *Secure by Default* und *Secure in Deployment*.

Secure by Design: Die Programmierer werden im Bereich Sicherheit geschult, der Quellcode wird auf Sicherheitslücken hin überprüft. In den Quellcode werden Sicherheitsmechanismen integriert.

Secure by Default: Um für eine Software höhere Sicherheit zu bieten, werden potenziell gefährliche Features standardmäßig zunächst deaktiviert und müssen manuell aktiviert werden. Ein Beispiel dafür sind die *Internet Information Services (IIS)* des Windows Server 2003.

Secure in Deployment: Microsoft stellt verschiedene kostenlose Tools bereit, mit denen Administratoren Sicherheitsaspekte auf den Servern, Clients und im Netzwerk prüfen können. Auch das automatische Windows-Update durch Patches und Fixes leistet seinen Beitrag zu diesem Bereich des SD Security Framework.

1.1 Der Internet Security Server

Der Teilbereich Internet Security Server des ISA Server ist für die Absicherung des Firmennetzwerks gegen Angriffe aus dem Internet zuständig. Je mehr Angriffe und weitere Sicherheitsrisiken wie z.B. Viren, Trojanische Pferde oder auch Spam-E-Mails für ein Unternehmensnetzwerk im Laufe der Zeit auftraten, desto größer wurde der Bedarf an einer Lösung zum Schutz und zur Absicherung des Netzwerks.

Im Gegensatz zu einer Hardware-Firewall ist der ISA Server 2004 bereits für Microsoft-Netzwerke und -Server sowie Windows-Technologien optimiert und vereinfacht die Integration in das Netzwerk.

Die folgenden Features werden über den Internet Security Server realisiert:

1.1.1 Mehrere Netzwerke

DMZ-Unterstützung

Gehören zum Unternehmen mehrere Netzwerke, so können diese über den ISA Server sowohl physisch als auch logisch getrennt werden. So ist auch der Einsatz einer DMZ möglich, so dass die Server, auf die vom Internet aus zugegriffen wird, vom übrigen Netzwerk separiert sind, um dieses zu schützen. Auch das interne Netzwerk kann vom ISA Server in verschiedene Segmente geteilt werden. Der gesamte Netzwerkverkehr zwischen allen Netzwerken wird vom ISA Server bis hinunter auf die Anwendungsebene überwacht.

1.1.2 Virtuelle private Netzwerke

Der ISA Server 2004 verfügt über eine komplette Lösung für virtuelle private Netzwerke (VPN). Diese basiert auf dem Dienst ROUTING UND RAS des Windows Server. Es können sowohl Standort-zu-Standort-VPNs als auch Remote VPN-Clients unterstützt werden. Dabei können die drei Protokolle PPTP, L2TP over IPSec sowie IPSec eingesetzt werden.

ISA Server als VPN-Server

Sofern der ISA Server selbst als VPN-Server konfiguriert ist, ist es möglich, direkt am ISA Server den kompletten VPN-Verkehr zu entschlüsseln, zu analysieren und zu protokollieren. Zur Maximierung der Sicherheit können Zugriffsregeln erstellt werden, die sicherstellen, dass die VPN-Benutzer nur Zugriff auf die Ressourcen erhalten, die sie unbedingt benötigen.

1.1.3 Intrusion Detection

Über das Intrusion Detection System (IDS) des ISA Server 2004 werden Angriffsversuche erkannt, blockiert und protokolliert. Sobald ein Angriff vom ISA Server erkannt wird, ist es möglich, den Administrator umgehend per E-Mail zu informieren, um schnell und zielgerichtet auf den Angriff reagieren zu können.

1.1.4 Paketfilterung

Der ISA Server 2004 unterstützt die statusunabhängige Paketfilterung. Bei dieser Form der Filterung werden automatisch dynamisch die benötigten Ports geöffnet. Es werden die IP-Header aller Verbindungen geprüft. Dabei werden nur die Pakete weitergeleitet, die auf eine Anfrage hin als Antwort gesendet werden.

Neben der Anwendungsfilterung notwendig

Ohne Paketfilterung würde z.B. jedes http-Paket die Firewall ungeprüft passieren können, sofern eine Regel den http-Verkehr gestattet. Der Inhalt des Pakets würde erst auf dem Zielserver gelesen werden. Befindet sich in dem Paket bösartiger Code, hätte dies möglicherweise den Absturz des Servers zur Folge. Nur durch die Paketfilterung ist sichergestellt, dass der Inhalt bereits an der Firewall geprüft wird.

1.1.5 Anwendungsfilterung

Der ISA Server verwendet Anwendungsfilter, über die das Transportprotokoll analysiert und die Pakete daraufhin untersucht werden, ob sie ungültig sind oder einen veränderten Inhalt aufweisen. Durch diese Form der Filterung werden beispielsweise Buffer-Overflow-Angriffe frühzeitig erkannt.

Dynamische Ports

Durch die Anwendungsfilterung ist auch die Unterstützung von Protokollen wie FTP oder RPC möglich, die dynamische Ports bei ihrer Verbindung verwenden. Der ISA Server kann die für die Verbindung erforderlichen Ports dynamisch öffnen und der jeweils anderen Seite den aktuell verwendeten Port mitteilen.

1.1.6 Circuit-Filterung

Anwendungstransparente Filterung

Die Circuit-Filterung wird auch als Filterung auf Sitzungsebene bezeichnet. Diese Art der Filterung arbeitet unabhängig von einer bestimmten Anwendung. Der ISA Server fungiert hierbei vielmehr als Proxy-Server, der zwei Verbindungen zwischen zwei Geräten aufbaut und verwaltet. Eine Verbindung besteht zwischen dem ISA Server und dem externen Gerät, die zweite Verbindung zwischen dem externen Gerät und dem ISA Server.

1.1.7 Content-Filterung

Die vierte Form der Filterung ist die Content-Filterung, also die Filterung der Inhalte. Dadurch ist es möglich, dass der ISA Server bestimmte Dateitypen wie *.exe* oder *.vbs* blockiert und nicht an den Client im Netzwerk weiterleitet. Ferner ist auch das Blockieren bestimmter Internetseiten oder bestimmter Inhalte wie z.B. Video oder Audio möglich.

1.1.8 Veröffentlichen von Servern

Mit Hilfe des ISA Server können auch Server des Unternehmens in sicherer Weise veröffentlich werden, so dass externen Benutzern der Zugriff auf diese Ressourcen möglich ist. Dabei kann es sich beispielsweise um einen Webserver, FTP-Server oder Mail-Server handeln. Sobald ein Zugriff auf einen veröffentlichten Server erfolgt, wird die entsprechende Verbindung bis hinunter auf die Anwendungsebene analysiert.

Schutz vor verschlüsselten Paketen

Soll ein Webserver veröffentlicht werden, kann dieser auch als HTTPS-Server konfiguriert sein. Dazu wird die SSL-to-SSL-Bridging-Funktion verwendet. Dadurch wird der HTTPS-Tunnel am ISA Server beendet. Alle verschlüsselten Pakete der Verbindung werden am ISA Server entschlüsselt und überprüft. Nach der Prüfung werden die Pakete wieder verschlüsselt und an den HTTPS-Webserver weitergeleitet. Würden die verschlüsselten Pakete nicht entschlüsselt, könnte keine Analyse deren Inhalte erfolgen. In diesem Fall wäre das Risiko sehr hoch, dass schädliche Inhalte in das Unternehmensnetzwerk gelangen.

1.1.9 Authentifizierung

Ist beispielsweise ein Mail-Server veröffentlicht, auf dem *Outlook Web Access (OWA)* ausgeführt wird, so kann die Authentifizierung des Benutzers am ISA Server erfolgen und nicht am Mail-Server selbst. Dies bietet den Vorteil, dass eine Verbindung zum Server erst dann hergestellt werden kann, wenn die Authentifizierung erfolgreich durchgeführt wurde. Damit werden potenzielle Risiken für den internen Mail-Server minimiert.

Als Authentifizierungsverfahren können entweder Windows-Verfahren oder auch die Verfahren RADIUS oder SecurID sowie die formularbasierte OWA-Authentifizierung verwendet werden.

1.1.10 Überwachung

Echtzeitprotokollierung

Der ISA Server 2004 ist in der Lage, nahezu in Echtzeit die Inhalte seiner Prüfungen und weitere Aktivitäten zu protokollieren und anzuzeigen. Diese Inhalte können wahlweise als herkömmliche Protokolldatei, in graphischer Form oder über das Dashboard des ISA Server angezeigt werden. Im Dashboard finden sich zusammengefasst die wichtigsten Daten wie Alarme, Ereignisse und Informationen zur Serverauslastung.

Ist ein bestimmtes definiertes Ereignis eingetreten, kann beispielsweise der Administrator direkt per E-Mail über den entsprechenden Alarm informiert werden.

1.2 Der Acceleration Server

Die zweite integrierte Komponente des ISA Server bildet der *Acceleration Server*. In dieser Funktion ist der Server für die Optimierung von Daten der Internetverbindung zuständig. Diese Funktion wird immer wichtiger, je mehr und größere Datenmengen aus dem Internet heruntergeladen werden.

Cachefunktion für oft benötigte Web-Objekte

Der Acceleration Server stellt eine interne Cachefunktion bereit. In diesem Cache werden für sämtliche Benutzer des Netzwerks Internetobjekte anhand definierbarer Regeln vorgehalten und den Benutzern beim Aufruf zur Verfügung gestellt. Dadurch beschleunigt sich für den Benutzer der Zugriff auf das Internet, da nicht alle benötigten Objekte direkt von dort bezogen werden müssen. Für das Unternehmen ergibt sich der Vorteil, dass die Bandbreite der Internetverbindung nicht voll ausgelastet werden muss, da nicht alle Objekte aus dem Internet geholt werden müssen.

Auch für den Zugriff externer Benutzer auf veröffentlichte Server kann die Cache-Funktion verwendet werden.

Der Acceleration Server besitzt die folgenden Features.

1.2.1 Zwischenspeicherung

Jedem im Cache befindlichen Objekt wird eine bestimmte Gültigkeitsdauer zugeteilt. Ist diese Dauer abgelaufen, ist das entsprechende Objekt nicht länger gültig. Ein Objekt kann automatisch aktualisiert werden, sobald die Auslastung des Netzwerks nicht zu hoch ist.

1.2.2 Festplatten- und RAM-Cache

Sinnvolle Objektverteilung im Array

Beim Caching werden sowohl die Festplatte als auch der RAM zur Speicherung der Objekte verwendet. Nach einem bestimmten Algorithmus werden die Webobjekte auf den Festplatten aller Mitglieder eines Arrays verteilt. Ein Objekt ist dabei nur auf einem einzigen ISA Server vorhanden. In der Standardversion hingegen verwendet jeder Server seinen eigenen Cache, so dass dasselbe Objekt redundant auf mehreren Servern liegen kann. Dies gilt für das Cachen von Webobjekten aus Internetseiten für die Netzwerkbenutzer ebenso wie für das Cachen von Webobjekten veröffentlichter Server für externe Benutzer.

1.2.3 Planmäßige Aktualisierungen

Für Internetseiten, die von den Benutzern besonders häufig angefordert werden, kann ein Zeitplan erstellt werden, nach dem diese Seiten komplett in den Cache des ISA Server übertragen werden. Dadurch werden die Client-Anfragen an die Objekte dieser Seiten wesentlich beschleunigt.

1.3 Verbesserungen gegenüber ISA Server 2000

Der ISA Server 2004 ist gegenüber seinem Vorgänger in vielen Punkten überarbeitet und verbessert worden. Auch viele zusätzliche Leistungsmerkmale sind in den Server integriert worden. Insbesondere bei der Installation auf einem Windows Server 2003 wird das komplette Leistungsspektrum der neuen Version deutlich. Deshalb kann auch die Enterprise-Version des ISA Server 2004 nur unter Windows Server 2003, *nicht* jedoch unter Windows Server 2000 installiert werden.

1.3.1 Neue Features

Die als erstes auffallende Änderung ist die Modifikation der Benutzeroberfläche. Diese wurde neu designed und dabei zwar in der Handhabung vereinfacht, aber dennoch für den neuen Leistungsumfang verbessert.

Weitere Änderungen und Verbesserungen sind:

Diverse Netzwerke und DMZ

- Unterstützung für unterschiedliche Netzwerk-Designs und mehrere Netzwerke. Der ISA Server 2000 kannte nur das interne und externe Netzwerk, der ISA Server 2004 unterstützt nativ auch eine DMZ sowie beliebig viele Netzwerke. Je nach ihrer IP-Adresse können diese über Route- oder NAT-Übersetzungen verbunden werden.

- Verbesserte VPN-Unterstützung mit breiter Protokollunterstützung. Dazu zählt auch die VPN-Quarantänefunktion, die nur VPN-Clients, die bestimmten Anforderungen entsprechen, den Netzwerkzugang gestattet. Für VPN-Clients können bestimmte Zugriffsregeln festgelegt werden. Ein VPN-Tunnel kann auch am ISA Server beendet werden, damit die Inhalte dort analysiert werden können.

VPN-Quarantänefunktion

- Erstellen benutzerdefinierter Firewall-Gruppen
- Erweiterte Protokollunterstützung und individuelle Protokolldefinitionen. Es können nun ICMP-Protokolle für sämtliche Regeln verwendet werden. Auch IPSec-Verbindungen werden unterstützt.
- Verbesserte Anwendungsfilter. Neu ist der http-Filter, über den http-Verbindungen untersucht werden können. Dabei können URLs normalisiert und zu große bzw. zu lange http-Anfragen blockiert werden. Ferner ist es möglich, dass über http getunnelte Applikationen wie z.B. der MSN Messenger erkannt und blockiert werden.
- Veröffentlichungsassistent für *Outlook Web Access (OWA*)
- FTP-Upload- und -Downloadrichtlinien werden besser unterstützt
- Verbesserte Webveröffentlichung
- Portumleitung für Serververöffentlichungsregeln
- Optimierte Cacheregeln für die zentrale Objektspeicherung
- Pfadzuweisung für Webveröffentlichungsregeln
- RADIUS-Unterstützung für Webproxyclient-Authentifizierung
- Verbesserte Authentifizierungsmöglichkeiten. Der ISA Server 2004 unterstützt neben den Windows-Authentifizierungsmechanismen auch RADIUS, SecurID, RSA und formularbasierte OWA-Authentifizierung.
- Delegierung der Standardauthentifizierung
- Formularbasierte Authentifizierung (durch die Firewall generierte Formulare)
- Verbesserte SMTP-Nachrichtenüberwachung und http-Filterung
- Linkübersetzung
- Überwachung und Berichtfunktion wurden verbessert. Wichtigste Neuerung ist das Dashboard, auf dem schnell und übersichtlich die wichtigsten ISA-Daten wie Alarme, Ereignisse oder Auslastung dargestellt werden. Die Protokollierung kann nun auch in einer MSDE-Datenbank erfolgen, so dass die Datenbankabfragen nach bestimmten Ereignissen auf dem ISA Server direkt generiert werden können. Zusätzlich werden in bestimmten Abständen interne und externe Server auf ihre Antwortzeit hin überprüft.

Protokollierung über MSDE/SQL Server

Ergeben sich hier Abweichungen von den Standardwerten, kann auch wie bei Alarmen des ISA Server der Administrator oder eine andere Person direkt informiert werden, um schnell auf das Problem reagieren zu können.

- Verbesserte Import- und Exportfunktion. Unter ISA Server 2000 konnte nur die gesamte Konfiguration exportiert und im Fall eines Problems wieder importiert werden. Neben dieser Funktion erlaubt der ISA Server 2004 auch den Import und Export einzelner Bestandteile der Konfiguration, z.B. von Filtereinstellungen oder Zugriffsregeln.

1.3.2 Gestrichene Features

Kaum genutzte Features wurden gestrichen

Spätestens bei der Installation wird Ihnen auffallen, dass einige Features des ISA Server 2000 nicht mehr vorhanden sind. Einige dieser Features sind gestrichen worden, weil diese anhand von Kundenaussagen nahezu kaum genutzt wurden, andere Features sind nun in anderer Weise verfügbar.

Komplett gestrichen wurden das *H.323-Gateway* sowie das *Live Stream Media Splitting*. Bei beiden Features hat Microsoft herausgefunden, dass diese von den Kunden so gut wie gar nicht eingesetzt wurden. Deshalb wurden diese Komponenten nicht mehr unter ISA Server 2004 integriert.

Auch die *Bandbreitenkontrolle* und das *Aktive Caching* sind in der alten Form nicht mehr vorhanden. Bei der Bandbreitenkontrolle kam es sehr häufig zu Problemen bei der Konfiguration, die nicht selten zu einer Neuinstallation des Windows und ISA Server führte. Aus diesem Grund wird die Bandbreitenkontrolle unter ISA 2004 nicht mehr angeboten. Das Aktive Caching wurde einerseits von den Anwendern auch nicht allzu häufig verwendet, andererseits wurde dieses Feature durch die verbesserten Funktionen des Acceleration Server auch nahezu überflüssig.

1.4 Versionen des ISA Server 2004

Der ISA Server 2004 ist in einer Standardversion und in einer Enterprise-Version erhältlich. In der folgenden Tabelle finden Sie eine Übersicht über die Funktionsunterschiede der beiden Versionen, die zur Entscheidungsfindung für den Einsatz der richtigen Version dienen soll.

Funktions-merkmal	Standardversion	Enterprise Version
Einsatz mehrerer ISA Server	Jeder eingesetzte ISA Server muss separat eingerichtet und verwaltet werden. Die Server werden einzeln mit DNS Round Robin oder NLB (Network Load Balancing) betrieben.	Mehrere ISA Server können zu einem Server-Array zusammengefasst werden. Die Konfiguration erfolgt für das Array und nicht für jeden darin enthaltenen Server einzeln. Die Array-Konfiguration wird an alle Array-Mitglieder weitergegeben.
Caching	Jeder ISA Server besitzt und verwaltet seinen eigenen Cache. Ein hierarchisches Caching ist nicht möglich. Dadurch können Webobjekte auf mehreren Servern doppelt vorhanden sein.	Für sämtliche Mitglieder eines Arrays wird ein gemeinsamer Cache verwendet. Ein Webobjekt wird nur auf einem einzelnen Server gespeichert und nicht auf mehreren vorgehalten. Sämtliche Webobjekte werden nach einem bestimmten Algorhitmus auf den Festplatten aller Array-Mitglieder gleichmäßig verteilt.
Server-Ausfall	Sobald ein ISA Server ausfällt, müssen die Clients gegebenenfalls zur Benutzung eines anderen ISA Servers konfiguriert werden.	Sobald ein ISA Server als Mitglied eines Arrays ausfällt, können die Clients mit den übrigen ISA Servern des Arrays kommunizieren. Eine Umkonfiguration der Clients ist dazu nicht notwendig. Erst wenn kein Server im Array mehr erreichbar ist, müssen die Clients für einen anderen ISA Server konfiguriert werden.
Active Directory	Nicht notwendig	Zur Speicherung der Array-Informationen muss ein Active Directory vorhanden sein.
Unterstützte Prozessoren	Maximal vier	Beliebig, nur abhängig vom eingesetzten Betriebssystem

Tabelle 1.1: Die Unterschiede der ISA Standard- und Enterprise-Version

1.5 Updatemöglichkeiten

Verwenden Sie bereits einen ISA Server 2000 in der Standard- oder Enterprise-Version, so bestehen die folgenden Updatemöglichkeiten. Der ISA Server 2004 in der Standardversion kann nur auf die Enterprise-Version aktualisiert werden. Das Update eines Microsoft Proxy-Servers auf ISA Server 2004 gleich welcher Version ist nicht möglich.

Tabelle 1.2: Die Updatemöglichkeiten bei den Versionen des ISA Server 2004

Update von/auf	ISA Server 2004 Standard	ISA Server 2004 Enterprise
ISA Server 2000 Standard	möglich	möglich
ISA Server 2000 Enterprise	Nicht möglich	möglich
ISA Server 2004 Standard	Nicht möglich	möglich
ISA Server 2004 Enterprise	Nicht möglich	Nicht möglich

1.6 Systemanforderungen

Für die Installation der Standard- und Enterprise-Version des ISA Server 2004 gelten dieselben Anforderungen an die Hardware, jedoch Unterschiede in der Software.

1.6.1 Hardwareanforderungen

Die von Microsoft empfohlenen Voraussetzungen finden Sie in der folgenden Tabelle. Bedenken Sie jedoch immer, dass es sich dabei um die Minimalvoraussetzung handelt.

Tabelle 1.3: Minimale Hardwareanforderungen für die Installation des ISA Server 2004

Komponente	Minimale Anforderung
Prozessor	Pentium III 500 MHz
Arbeitsspeicher	256 MB
Festplattenspeicher	150 MB auf dem Dateisystem NTFS. Weiterer Speicherplatz wird für den Inhalt des Web-Cache erforderlich.
Weitere Hardware	▶ Ein Netzwerkadapter zur Kommunikation mit dem internen Netzwerk. Je ein weiterer Netzwerkadapter, ein Modem oder ISDN-Adapter zur Kommunikation mit weiteren Netzwerken. Ein zusätzlicher Netzwerkadapter, wenn Network Load Balancing (NLB) in der Enterprise-Version eingesetzt wird ▶ CD-ROM oder DVD-ROM-Laufwerk ▶ VGA-Monitor oder Monitor mit höherer Auflösung ▶ Microsoft-kompatible Maus und Tastatur

1.6.2 Softwareanforderungen

Für die Installation eines ISA Server 2004 in der Standardversion können die folgenden Betriebssysteme verwendet werden:

Windows 2000 oder 2003 Server

- Windows Server 2003 Standard oder Enterprise
- Windows Server 2000, Advanced Server 2000 oder Datacenter Server 2000

Unter Windows 2000 muss mindestens das Service Pack 4 installiert sein sowie der *Internet Explorer* in der Version 6.0.

Unter Windows 2000 muss zwingend auch das im Microsoft-KB-Artikel 821887 beschriebene Hotfix installiert sein. Sie finden den Artikel und das Hotfix auf der Begleit-CD.

Windows Server 2003 erforderlich

Für die Installation des ISA Server 2004 Enterprise ist ein Windows Server 2003 Standard oder Enterprise erforderlich. Eine Installation unter Windows Server 2000 ist *nicht* möglich.

Für beide Versionen gilt gleichermaßen, das vor Beginn der Installation sämtliche Hotfixes und Patches auf dem Betriebssystem eingespielt sein sollten.

1.7 Lizenzierung des ISA Server 2004

Lizenzierung pro Prozessor

Für den ISA Server 2004 muss wie für jedes andere Produkt selbstverständlich auch eine Lizenz vorliegen. Der ISA Server 2004 ist im Gegensatz zu anderen Serverprodukten lediglich als Prozessor-Lizenzvariante erhältlich. Dies bedeutet, dass für jeden physikalischen Prozessor des Servers eine Lizenz vorliegen muss. Diese Lizenzierungsvariante greift gleichermaßen für die Standard- und Enterprise-Version. Eine Ausnahme stellt lediglich die Hyperthreading-Funktion dar. Diese emuliert lediglich einen zusätzlichen Prozessor. Eine separate Lizenz für einen emulierten Prozessor ist jedoch nicht erforderlich.

Die Prozessor-basierte Lizenzierung erlaubt den Zugriff beliebig vieler Benutzer bzw. Geräte auf den ISA Server. Es besteht auch keinerlei Beschränkung bezüglich der Anzahl der IP-Adressen oder der nutzbaren Bandbreite.

Werden auf dem Windows Server 2000 oder 2003, auf dem der ISA Server 2004 installiert wird, keine Funktionen der Datei- und Druckdienste bereitgestellt, so werden für das Serverbetriebssystem keine Clientzugriffslizenzen (Client Access Licence, CAL) erforderlich. Hierbei handelt es sich um eine Sonderregelung für den ISA Server.

Die Komponenten ISA Server-mmc, Installationsfreigabe für den Firewallclient sowie die Nachrichtenüberwachung dürfen auf einem separaten Computer installiert werden. Die Nutzung ist jedoch nur in Kombination mit der ISA Server-Software gestattet. Standardmäßig dürften diese Lizenzen aber dennoch vorhanden sein.

Mit einer Lizenz des ISA Server 2004 besitzen Sie automatisch die Berechtigung, auf den ISA Server 2000 oder den Proxy Server downzugraden. Sobald jedoch der ISA Server 2004 installiert wurde, dürfen die früheren Versionen nicht mehr benutzt werden.

Separate Lizenz unter SBS 2003

In der Premium-Version des *Small Business Server 2003 (SBS)* wird noch der ISA Server 2000 ausgeliefert. Um auf ISA Server 2004 upzudaten, ist eine separate Lizenz erforderlich. In dem Service Pack 1 für den SBS 2003 soll jedoch der ISA Server 2004 enthalten sein.

1.8 Zunächst eine Testversion

Bevor Sie sich entschließen, den ISA Server 2004 produktiv im Unternehmen einzusetzen, besteht die Möglichkeit, zuvor über eine Testversion des ISA Server 2004 mit der Applikation vertraut zu werden und zu entscheiden, ob die Kosten für diese Software investiert werden sollen oder nicht.

120 Tage-Version

Eine Testversion ist sowohl für die Standard- als auch für die Enterprise-Version verfügbar. Beide Versionen sind 120 Tage lang lauffähig und kostenlos bei Microsoft erhältlich. Sie können entweder die gewünschte Version downloaden oder sich diese auf einer CD zuschicken lassen. Im Funktionsumfang sind diese Versionen nicht eingeschränkt. Eine Testversion ist in den Sprachen Deutsch, Englisch, Französisch, Spanisch und Japanisch erhältlich. In der produktiven Umgebung sollte eine Testversion jedoch *niemals* eingesetzt werden, da für diese keinerlei Supportanspruch besteht.

Sie finden auch auf der Begleit-CD jeweils eine Testversion des ISA Server 2004 in der Standard- und Enterprise-Version. Diese Versionen sind als selbstentpackendes Archiv verfügbar. Zum Extrahieren der Dateien müssen auf dem Laufwerk C mindestens 150 MB freier Speicherplatz vorhanden sein. Von dort aus erfolgt dann die Installation.

1.9 Quantitative und qualitative Risikoanalyse

Für die Durchführung einer Risikoanalyse gibt es gute Gründe, die jeweils aus der Sicht verschiedener Zuständigkeiten unterschiedlich aussehen. Für Administratoren und IT-Consultants ist die Risikoanalyse die Grundlage für die Berechnung von Kosten, die einerseits durch Angriffe entstehen können und andererseits mit der Absicherung einhergehen sollten. Für das Management stellt die Risikoanalyse eine Grundlage dar, nach der die Kosten sowie der Personalaufwand für den Bereich Sicherheit geplant werden können.

Risikoanalyse in verschiedenen Sichtweisen

Beide Gruppen sollten die Ergebnisse ihrer Risikoanalyse zusammentragen und ein gemeinsames Sicherheitskonzept entwickeln. In dieser gemeinsamen Sichtweise werden Punkte, die von einer Gruppe möglicherweise nur unzureichend oder gar nicht bedacht wurden, für beide Seiten transparent. Zudem können so vorhandene Ressourcen gebündelt gegen bestehende Schwachstellen und Angriffspunkte eingesetzt werden.

1.9.1 Quantitative Risikoanalyse

Um die quantitative Risikoanalyse, also die Ermittlung der Kosten, die durch Schäden aufgrund mangelnder Sicherheit im Netzwerk entstehen, festzustellen, gibt es eine auf Industriestandards basierende Formel:

$$ALE = SLE * ARO$$

Die Abkürzungen haben folgende Bedeutung:

Abkürzung	Bedeutung	Beschreibung
ALE	Annualized Loss Expectancy	Gesamtsumme, die für ein Jahr aufgrund von Schäden durch Viren etc. erwartet wird
SLE	Single Loss Exposure	Summe, die bei einem einzelnen Schadensfall erwartet wird
ARO	Annualized Rate of Occurence	Prozentuale Wahrscheinlichkeit für einen Schadensfall

Tabelle 1.4: Die Konstanten der Formal zur quantitativen Risikoanalyse

Beispielrechnung

Für eine Beispielrechnung sollen die folgenden Eckdaten gelten: Das Unternehmen verfügt über 1.000 Clients. Es besteht eine Gefahr von 80 %, dass mindestens einmal pro Jahr durch einen Virus Schaden an 75 % der Clients entsteht. Für jeden Client sind Kosten von durchschnittlich 50 Euro notwendig, um den Virus wieder zu entfernen.

Darin enthalten sind Kosten für entsprechende Tools und Personal. Der Wert für die SLE setzt sich demnach folgendermaßen zusammen:

1.000 Clients × 50 Euro × 75% betroffene Computer = 37.500 Euro

Daraus ergibt sich folgender ALE-Wert:

37.500 Euro × 80% Schadenswahrscheinlichkeit = 30.000 Euro

In dieser Beispielrechnung sind noch nicht die Kosten eingerechnet, die durch den Verlust von Daten entstehen. Auch mögliche Kosten zur Datenwiederherstellung sowie weitere daraus resultierende Folgekosten sind in dieser Rechnung nicht enthalten. Werden diese mit einbezogen, liegt die Schadenssumme möglicherweise noch um ein Vielfaches höher. Und ein Imageschaden, der dem Unternehmen zusätzlich entsteht, kann bei weitem höhere mittelbare Kosten verursachen.

1.9.2 Qualitative Risikoanalyse

Neben der quantitativen Risikoanalyse kann auch eine qualitative Risikoanalyse durchgeführt werden. In dieser geht es weniger um die Wahrscheinlichkeit, dass ein bestimmtes Ereignis eintrifft, als vielmehr um die Analyse des Netzwerks bezüglich seiner Charakteristiken und daraus resultierenden Schwachpunkten bei einem möglichen Angriff.

Basierend auf dieser Analyse werden Konzepte erarbeitet, um die Schwachstellen zu beseitigen oder zumindest zu minimieren sowie daraus resultierende Schäden möglichst gering zu halten.

1.10 Erkennen von Risiken und Bedrohungen

Vor der Reaktion auf Risiken und Sicherheits-Schwachstellen müssen diese selbstverständlich zunächst erkannt werden. Generell werden die Bedrohungen in interne und externe Bedrohungen unterteilt.

Gefahren aus externen Quellen

Unter externen Bedrohungen werden alle Gefahren zusammengefasst, die von außerhalb des Unternehmensnetzwerks, in der Regel über das Internet, auftreten. Zu diesen Gefahren zählen zum einen Hacker, die es auf beliebige Unternehmensnetzwerke abgesehen haben, und zum anderen Angriffe, die gezielt auf das Unternehmen gerichtet sind. Im letzteren Fall kann es sich möglicherweise auch um Spionageangriffe handeln. Aber auch Personen, die einen persönlichen Racheakt gegen das Unternehmen führen, spielen oftmals eine wesentliche Rolle. Hierbei kann es sich beispielsweise um entlassene Mitarbeiter oder auch Psychopathen handeln.

Gefahren durch interne Mitarbeiter

Ebenso darf aber die Gefahr, die von den eigenen Mitarbeitern oder Vertragspartnern innerhalb des Netzwerks ausgeht, nicht unterschätzt werden. Diese Gefahren mögen zwar in der Regel nicht absichtlich von den Mitarbeitern ausgehen; dennoch aber sind diese Gefahren vorhanden, und es muss ebenfalls auf sie reagiert werden. Zu diesem Gefahrenkreis zählen Personen, die beispielsweise versehentlich Daten löschen oder Konfigurationen ändern. Besonders schlimm wird dies, wenn ein Administrator mit entsprechenden Berechtigungen bei Experimenten am produktiven System derartige Gefahren heraufbeschwört.

1.10.1 Mögliche Gefahren

Nachdem die Quellen der möglichen Gefahren bekannt sind, muss auch darüber nachgedacht werden, welche Schäden durch diese Gefahrenquellen angerichtet werden können. Auch in diesem Bereich gibt es wieder viele verschiedenen Möglichkeiten, die auch oft in Kombination miteinander auftreten:

- Unerlaubter Zugriff auf Unternehmensdaten
- Löschen von Unternehmensdaten
- Verändern oder Beschädigen von Unternehmensdaten
- Veröffentlichen von vertraulichen Informationen
- DoS-Attacken (Denial of Service) oder andere Angriffe, die zur Überlastung des Netzwerks führen
- Einschleusen von Viren, Trojanischen Pferden, Würmern usw.

Im Zuge der Auflistung von Gefahren müssen natürlich auch Schäden durch höhere Gewalt eingeschlossen werden, z.B. Schäden durch Feuer, Wasser oder Stromausfall. Diese Punkte spielen zwar im Zusammenhang mit der Absicherung gegen innere und äußere Gefahren durch den ISA Server keine Rolle, müssen aber dennoch in das Gesamt-Sicherheitskonzept des Unternehmens einbezogen werden.

1.10.2 Ermitteln der Gefahrenwahrscheinlichkeit und Kosten

Nachdem die potenziellen Gefahren bekannt sind, ist es als nächstes nötig zu ermitteln, wie hoch die Wahrscheinlichkeit ist, dass eine bestimmte Gefahr eintritt. Sämtliche Gefahrenquellen sollten dazu in drei Gruppen kategorisiert werden, z.B. niedrige, mittlere und hohe Wahrscheinlichkeit des Eintritts. Je niedriger die Wahrscheinlichkeit ist, dass eine bestimmte Bedrohung eintritt, desto weniger Beachtung muss diesem Bereich geschenkt werden. Dennoch darf ein Bereich nie ganz vernachlässigt werden, denn das Risiko einer bestimmten Bedrohung kann sich *niemals* ganz ausgeschlossen werden.

Kosten der Schadensbeseitigung

Für jede potenzielle Bedrohung muss zusätzlich der Aufwand für das Unternehmen geschätzt werden, der für die Beseitigung des Schadens zu erwarten ist. Steht z.B. für einen Tag das Unternehmensnetzwerk nicht zur Verfügung, so muss geschätzt werden, wie hoch die Verluste des Unternehmens dadurch sind. Dazu zählen Ausfälle durch möglicherweise entgangene Aufträge ebenso wie Kosten für das Personal, das während des Netzwerkausfalls nicht produktiv arbeiten konnte.

Immaterielle Schäden

Sind beispielsweise interne Informationen in der Öffentlichkeit bekannt gemacht worden, muss eingeschätzt werden, wie hoch der Vertrauensverlust für das Unternehmen ist und ob möglicherweise ein gerichtliches Verfahren auf das Unternehmen zukommt, für das ebenfalls die Kosten zu tragen wären.

Sobald für jede Gefahrenquelle die Wahrscheinlichkeit und der zur Schadensbehebung notwendige Aufwand definiert sind, können die Ergebnisse in Form einer Matrix aufgelistet werden. Die Inhalte dieser Matrix sollten die Grundlage für die Definition von allgemeinen Sicherheitsrichtlinien für das Unternehmen bilden.

1.11 Erkennen von Schwachstellen

Um Bedrohungen vorbeugen zu können, müssen die Schwachstellen innerhalb der Netzwerkstruktur und der Unternehmensorganisation analysiert werden.

1.11.1 Netzwerk

Insbesondere die Schwachstellen in der Netzwerkstruktur beruhen in vielen Fällen auf einer falschen Konfiguration von Betriebssystemen, Diensten oder Applikationen. Sicherheitslücken, die an diesen Komponenten auftreten, sollten in jedem Fall immer so schnell wie möglich durch die entsprechenden Patches, Updates oder Fixes geschlossen werden.

Häufige Angriffspunkte sind beispielsweise auch offene TCP- oder UDP-Ports, die eigentlich nicht benötigt werden, aber dennoch nicht geschlossen wurden. Je mehr Ports einem Hacker zur Verfügung stehen, desto mehr Möglichkeiten zum Eindringen in das Netzwerk eröffnen sich ihm.

Auch die Java-Konfiguration im Webbrowser kann für potenzielle Bedrohungen sorgen, wenn diese die Ausführung beliebigen Codes zulässt.

Sie sehen bereits anhand dieser beiden kleinen Beispiele, dass ein Weniger an erlaubten Einstellungen oftmals ein deutliches Mehr an Sicherheit bedeuten kann.

Wählverbindung vs. dauerhafte Verbindung

Eine weitere Bedrohung stellen die Internetverbindungen des Unternehmens dar. Bei einer permanenten Verbindung wie bei einer Standleitung oder dem Einsatz einer DSL-Flatrate erhöht sich das Risiko im Gegensatz zu einer Wählverbindung, die nur kurzzeitig hergestellt und nach Abschluss wieder getrennt wird. In der Regel wird beim Einsatz einer Wählverbindung auch eine dynamische IP-Adresse benutzt. Diese sowie der relativ kurze Zeitraum der bestehenden Verbindung erschweren einem potenziellen Angreifer das Eindringen in das Netzwerk. Allerdings stellt eine Wählverbindung ein höheres Risiko z.B. für Dialer dar.

Mehrere Internetverbindungen

Befinden sich auf einem Computer mehrere Internetverbindungen, z.B. eine LAN-Verbindung für den DSL-Zugang und eine Modemverbindung, die entweder aus Redundanzgründen beim Ausfall der DSL-Verbindung oder auch einfach nur als Relikt der Prä-DSL-Zeit übrig geblieben ist, so erhöht sich wieder das Risiko. Sofern der Computer mit dem internen Netzwerk verbunden ist (was bei nahezu jedem Client der Fall sein dürfte), kann dieser als Router fungieren, so dass ein Angreifer nicht nur auf den Client selbst, sondern auch auf die anderen Computer des Netzwerks zugreifen kann.

In jedem Fall sollten möglichst wenig Verbindungen von dem Unternehmensnetzwerk nach außen gehen. Dies erleichtert die Kontrolle der einzelnen Zugriffspunkte auf das Netzwerk.

Wird ein Modem eingesetzt, damit der Benutzer eine Verbindung zu einem anderen privaten Netzwerk herstellen kann, so sollte über den Einsatz eines VPN (Virtual Private Network) nachgedacht werden, das eine VPN-Verbindung zu einem anderen Netzwerk über die LAN-Internetverbindung herstellt.

Um Schwachstellen im Netzwerk zu erkennen, gibt es verschiedene Tools, die anhand einer Datenbank mit den bekanntesten Schwachstellen das vorhandene Netzwerk auf Risiken hin prüfen. Ein derartiges Programm sollte in jedem Fall eingesetzt werden, um sich zunächst einen Überblick über die Netzwerkkonfiguration zu verschaffen.

1.11.2 Zugriff auf Daten

Schutz von Daten mit unternehmenskritischen Inhalten

Auch auf die Organisation des Zugriffs auf unternehmensinterne, vertrauliche Daten muss ein besonderes Augenmerk gerichtet werden. Welchem Unternehmen wäre es schließlich schon recht, wenn die Konkurrenz über Verkaufszahlen oder Marketingstrategien informiert würde?

Besonders schützenswert sind Dokumente der folgenden unternehmenskritischen Inhalte:

- Daten über die finanzielle Situation, z.B. Verkaufszahlen oder Kostenpläne
- Personalinformationen wie z.B. Arbeitsverträge
- Informationen über Kunden und Geschäftspartner
- Weitere Unternehmensgeheimnisse, z.B. Dokumente über Patente, Erfindungen usw.
- Marketingstrategien und Businesspläne
- Vertrauliche private Korrespondenz

Balance zwischen Sicherheit und Zugriff

Generell gilt: je wichtiger eine Information für das Unternehmen ist, desto besser sollte diese auch geschützt werden. Je größer das Unternehmensnetzwerk ist, desto mehr Personen besitzen automatisch auch Zugriff auf dieses Netzwerk. Und dadurch erhöht sich auch das Risiko des unerlaubten Zugriffs, sei es nun von innen oder von außen. Die Ziele Sicherheit und Zugriff bilden immer ein Paar. Je mehr der Schwerpunkt auf einer der beiden Seiten liegt, desto geringer ist automatisch die andere Seite.

In einigen Unternehmen, besonders in Behörden und Verwaltungen, wird eher ein sehr restriktiver Zugriff gestattet, wobei die Sicherheit eindeutig im Vordergrund steht. Möglicherweise muss der Zugriff auf bestimmte Dateien zunächst schriftlich durch den Mitarbeiter begründet werden. Demgegenüber steht als andere Variante ein natürlich auch gesichertes Netzwerk, in dem jedoch die Zugriffsrichtlinien wesentlich weniger restriktiv gehandelt werden. In Unternehmen, die diese Philosophie verfolgen, steht oftmals die Zufriedenheit des Mitarbeiters an vorderer Stelle.

Auch Gesetze und Verträge können für die Definition bestimmter Richtlinien eine Rolle spielen, an die ein Unternehmen gebunden ist. Dies gilt z.B. bei Behörden und Ämtern oder auch, wenn in Unternehmensverträgen das Veröffentlichen bestimmter Informationen im Netzwerk untersagt ist.

1.12 Implementieren einer Sicherheitslösung

Sobald die Schwachstellen analysiert sind, muss mit dem Management abgeklärt werden, wie hoch das Budget ist, das für die Implementierung einer Sicherheitslösung zur Verfügung steht. Abhängig von den Anforderungen und dem zur Verfügung stehenden Budget können eine oder mehrere der folgenden Lösungen implementiert werden.

1.12.1 Hardware-Lösungen

Nicht nur eine Firewall

Beim Einsatz einer Hardware-Lösung werden ein oder mehrere Geräte wie z.B. Firewalls als Netzwerkgeräte hinzugefügt. Auch andere Geräte, wie z.B. ein Kartenlesegerät für Smart Cards zur Authentifizierung der Benutzer an den lokalen Computern, gehören in diese Kategorie.

Um zu verhindern, dass die Benutzer unerlaubt Software installieren, ist das Entfernen von CD-Laufwerken und Disketten-Laufwerken ein probates Mittel.

Um insbesondere den Zutritt zu Hochsicherheitsbereichen zu kontrollieren, bieten sich biometrische Authentifizierungssysteme an.

Dies sind nur einige Beispiele für die Implementierung von Hardware zur Absicherung des Netzwerks und des Zugriffs. Hardwarelösungen sind nahezu immer kostenintensiver als der Einsatz einer Software-Lösung. Dafür ist jedoch auch der Sicherheitsfaktor in vielen Fällen höher. Auch eine Kombination beider Lösungen kann ein zufrieden stellendes Gesamtergebnis liefern.

1.12.2 Software-Lösungen

Für die Implementierung von Software-Lösungen stehen zahlreiche Applikationen für verschiedene Einsatzbereiche zur Verfügung. Nur eine davon ist der ISA Server 2004, der als Firewall verwendet wird. Daneben finden sich Lösungen in den Bereichen Intrusion Detection, Paket-Filterung, Applikations-Filterung oder Antiviren-Programme und Programme zum Schutz gegen Spyware.

Auch Netzwerksniffer zur Überwachung des Netzwerkverkehrs stellen ein probates Mittel dar, um unberechtigte Zugriffe zu erkennen.

Eine Selbstverständlichkeit sollte das Einspielen aller verfügbaren Patches, Fixes und Updates für die eingesetzten Betriebssysteme sowie Applikationen sein, um dadurch vorhandene Sicherheitslücken rasch zu schließen. Das Einspielen dieser Patches sollte nach Möglichkeit automatisch erfolgen, um so den Verwaltungsaufwand zu minimieren. Microsoft bietet dazu die *Windows Server Update Services (WSUS)* an. Diese Komponente kann kostenlos bei Microsoft downgeloadet werden. Der WSUS versorgt automatisch die Client- und Server-Betriebssysteme sowie bestimmte Applikationen wie z.B. *Office 2003* mit allen notwendigen Patches.

1.12.3 Richtlinien-basierte Lösungen

Auf Einhaltung der Richtlinien ist zu achten

Bei diesem Lösungsansatz wird theoretisch weder eine Hardware- noch eine Software-Lösung implementiert. Die Mitarbeiter erhalten lediglich ein umfassendes Regelwerk zum Umgang mit sicherheitsrelevanten Aspekten. Allerdings sollten Sie bedenken, dass allein diese Implementierung keinen optimalen Schutz darstellt, sie sollte mit einer der anderen beiden Lösungen kombiniert werden. Hardware- und Software-Lösungen können ebenfalls, wenn auch auf einer anderen Ebene, die Durchsetzung von Richtlinien erzwingen.

Richtlinien dieser Kategorie können die folgenden Inhalte haben:

- Den Mitarbeitern wird untersagt, Benutzerkennwörter weiterzugeben, z.B. auch nicht an einen anderen Kollegen.
- Die Mitarbeiter dürfen ohne vorherige Erlaubnis keine Software auf den Computern installieren.
- Es darf kein anderer Mitarbeiter den Computer benutzen, nachdem sich der Mitarbeiter angemeldet hat. Verlässt er seinen Arbeitsplatz zwischendurch, muss der Computer gesperrt werden.

Lokale Sicherheitsrichtlinie

Selbstverständlich sollten auch lokale Sicherheitsrichtlinien konfiguriert werden, die den Benutzer zur Verwendung eines komplexen Kennworts zwingen, das zudem in bestimmten Intervallen geändert werden muss.

Anhand dieses Kapitels sollte Ihnen klar geworden sein, dass die Gewährleistung der Sicherheit keineswegs mit der Installation und Konfiguration des ISA Server abgeschlossen ist. Dazu ist das Gebiet Sicherheit zu vielschichtig.

2 Einsatzszenarien für den ISA Server 2004

Primär für mittlere und große Unternehmen ausgelegt

Dieses Kapitel beschreibt die vielfältigen Einsatzmöglichkeiten des ISA Server 2004. Die Unternehmensgröße ist für den Einsatz des ISA Server eher zweitrangig. Schon für kleine und mittlere Unternehmen kann der ISA Server eingesetzt werden, wenngleich er prinzipiell für mittlere und große Unternehmen ausgelegt ist, was sich teilweise in der Komplexität der Konfigurationseinstellungen widerspiegelt. Somit befindet sich der ISA Server auch bereits im Lieferumfang des *Small Business Server 2003 Premium Version*.

Nichtsdestotrotz erfüllt der ISA Server auch in kleinen Unternehmen und im SOHO-Bereich zuverlässig seine Aufgaben. Dort dürfte lediglich der Kostenfaktor gegen den Einsatz dieses Systems sprechen.

Ein besonderes Augenmerk ist noch darauf zu richten, ob der ISA Server als Mitglied einer Domäne oder Arbeitsgruppe eingerichtet wird. Er kann als Domänencontroller, Mitgliedserver und allein stehender Server betrieben werden.

2.1 ISA Server 2004 – Einsatzmöglichkeiten

Der ISA Server 2004 kann in vielen unterschiedlichen Szenarien und Modellen eingesetzt werden, die in den folgenden Kapiteln näher erläutert werden.

Dieser weite Einsatzbereich spricht bereits für die Flexibilität des Produkts. Zudem verfügt der ISA Server gegenüber den meisten anderen Firewall-Lösungen auch über eine Cache-Funktion zur Optimierung des Internetzugriffs. Der ISA Server bietet damit eine Zwei-in-Eins-Funktion.

Die Absicherung der Verbindungen geschieht durch Filterungen auf Sitzungsebene sowie statusunabhängige Paketfilterung (Stateful Inspection). Letztere bestimmt, welche Pakete ins interne Netzwerk und die Anwendungsebene der Proxy-Dienste gelangen dürfen. Dadurch ist es möglich, dass die benötigten Ports nur im Bedarfsfall geöffnet und direkt nach Abschluss der Kommunikation wieder geschlossen werden.

Die Filterung auf Sitzungsebene verwendet anwendungsunabhängige Gateways für zahlreiche Internetprotokolle und Dienste wie z.B. *Telnet*, *Windows Media* oder *RealAudio*.

Neben den eben genannten Filterungen wird auch eine Filterung auf Anwendungsebene durchgeführt. Dazu werden Anwendungs-, Daten- und Befehlsfilter verwendet. Beispielsweise kann dadurch http-, ftp-, VPN-, SMTP-, POP3-, DNS- oder RPC-Datenverkehr angenommen oder blockiert, weitergeleitet oder geändert werden.

Eigenes SDK für ISA Server 2004

Für weitere Funktionen werden von zahlreichen Drittanbietern weitere Filter für den ISA Server angeboten. Zur eigenen Entwicklung stellt Microsoft das *ISA Server–SDK (Software Development Kit)* zur Verfügung. Das ISA Server-SDK finden Sie auf der Begleit-CD dieses Buches.

Ein weiterer Pluspunkt des ISA Server ist seine Benutzerfreundlichkeit. Dazu zählen verschiedene Assistenten, Vorlagen, Richtlinien-Editoren sowie Werkzeuge zur Problembehandlung. Des Weiteren können Konfigurationsdaten in einfacher Weise per *.xml*-Datei exportiert werden, und auch eine Echtzeit-Überwachungsfunktion ist gegeben.

In den ISA Server wurde eine vollständige VPN-Funktion integriert, die auf dem Routing- und RAS-Dienst des Windows Server beruht. Über den IPSec-Tunnelmodus kann der ISA Server Standort-zu-Standort-VPNs zu anderen Zweigstellen oder Geschäftspartnern etablieren. Ein weiteres Feature ist dabei die VPN-Quarantäne, die den Zugriff von Clients auf das Netzwerk unterbindet, die nicht definierten Standards, z.B. in puncto Sicherheit, entsprechen.

2.2 ISA Server mit einer Netzwerkkarte

Ein ISA Server, der nur über eine Netzwerkkarte verfügt, stellt das einfachste und am wenigsten komplexe Einsatzmodell dar. Dabei ist der ISA Server lediglich mit dem Netzwerk verbunden, während die Internetverbindung über eine andere Firewall, z.B. eine Hardware-Firewall, hergestellt wird (siehe Abbildung 2.1). Diese Konfiguration ist sinnvoll, wenn der ISA Server lediglich als Cache- und Proxy-Server eingesetzt werden soll.

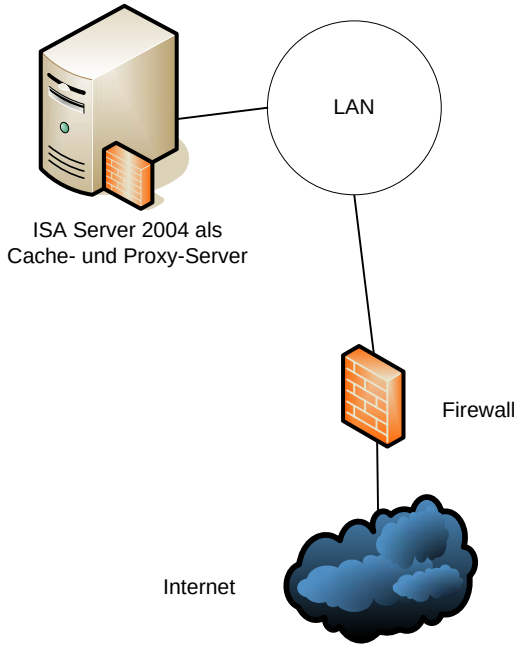


Abbildung 2.1: Verfügt der ISA Server nur über eine Netzwerkkarte, die ihn mit dem LAN verbindet, so muss die Internetverbindung über eine andere Firewall hergestellt werden

Über Zugriffsregeln kann festgelegt werden, welche Benutzer und Computer auf welche Internetinhalte bzw. -seiten zugreifen dürfen. Zudem können die Anfragen der internen Netzwerkclients beschleunigt werden, indem der ISA Server in diesem Modell als zentraler Cache-Server für die ausgehenden Anfragen eingesetzt wird. Der ISA Server dient zusätzlich auch als Proxy-Server für die ausgehenden Anfragen. Für sämtliche Internetverbindungen, die über den ISA Server abgewickelt werden, können vom Administrator Protokolldaten abgerufen werden.

Der ISA Server kann in diesem Modell auch zum Reverse-Caching eingesetzt werden, um einen Lastenausgleich für einen veröffentlichten Webserver zu realisieren. Dabei werden die von außen eingehenden Anfragen von der Firewall an den ISA Server weitergeleitet. Nachdem der ISA Server diese Anfragen erhalten hat, prüft er, ob sich das angeforderte Objekt in seinem lokalen Cache befindet. Nur wenn sich Objekte nicht im lokalen Cache befinden, leitet der ISA Server die Anfrage an den Webserver weiter, anderenfalls beantwortet er die Anfrage selbst. Dies entlastet den veröffentlichten Webserver.

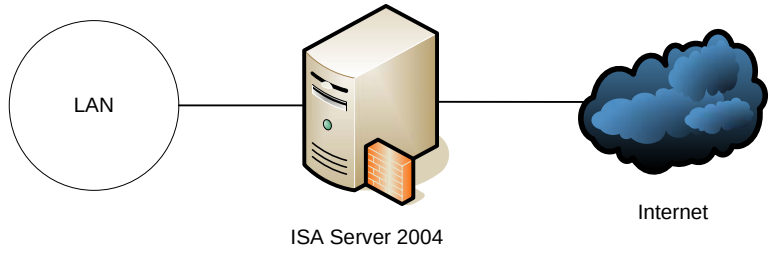
Reine Cache-, aber keine Firewall-Funktion

In diesem Modell stehen eindeutig die Cache-Funktionen des ISA Server im Vordergrund, seine Firewall-Funktionalität kann er so nicht unter Beweis stellen, da als Firewall ein anderes Gerät fungieren muss.

2.3 Edge-Firewall

Das Modell der Edge-Firewall dürfte eines der häufigeren Einsatzszenarien sein. Hierbei besitzt der ISA Server zwei Netzwerkkarten, wobei über eine Karte die Verbindung zum internen Unternehmensnetzwerk und über die andere die Verbindung zum Internet direkt oder über einen Router hergestellt wird (siehe Abbildung 2.2).

Abbildung 2.2: Die Edge-Firewall ist das Standardmodell, das bei der Installation des ISA Server vorgeschlagen wird



Die Firewall des ISA Server kann hierbei den kompletten eingehenden und ausgehenden Datenverkehr bis hinunter zur Anwendungsschicht statusunabhängig überprüfen und blockieren.

Der ISA Server kontrolliert auch die Kommunikation zwischen veröffentlichten Servern und externen Clients.

In diesem Modell kann der ISA Server gleichermaßen seine Cache- und seine Firewall-Funktion ausspielen.

Gefahr für das gesamte interne Netzwerk bei einem Angriff

Sobald es jedoch einem Angreifer gelingt, die Sicherheitsmechanismen auszuhebeln oder er in irgendeiner anderen Weise unrechtmäßigen Zugang zum Netzwerk erlangt, so ist in diesem Modell das komplette lokale Netzwerk vom Angriff betroffen, da sich darin sämtliche Server und Clients befinden.

2.4 DMZ-Modell

In diesem Modell muss der ISA Server über drei Netzwerkkarten verfügen, wobei eine Verbindung zum internen Netzwerk, eine Verbindung zum Internet und eine Verbindung zur DMZ hergestellt wird (siehe Abbildung 2.3). DMZ steht für demilitarisierte Zone. Die drei Abschnitte des Netzwerks werden logisch und physikalisch voneinander getrennt und garantieren so einen besseren Schutz des Unternehmensnetzwerks.

In einer DMZ befinden sich die Geräte und Server, mit denen von externen Clients direkt über das Internet kommuniziert wird, z.B. ein Webserver oder ein DNS-Server für die Namensauflösung externer Domänen. Die Server in der DMZ werden veröffentlicht, die erforderlichen Dienste werden geprüft und über Paketfilter und Anwen-

dungsfilter wird der komplette eingehende und ausgehende Datenverkehr zur DMZ analysiert.

Private und öffentliche IP-Adressen möglich

Die Geräte in der DMZ können sowohl private, als auch öffentliche IP-Adressen besitzen. Über Netzwerkregeln wird die Beziehung (NAT oder Route) zwischen der DMZ sowie den externen Geräten festgelegt. In der DMZ des ISA Server 2000 mussten noch zwangsläufig öffentliche IP-Adressen verwendet werden.

In einer DMZ sollten niemals Server eingerichtet werden, die den Zugriff auf das Active Directory benötigen, z.B. ein Exchange Server. Für die Kommunikation eines Exchange Servers in der DMZ mit einem Domänencontroller im lokalen Netzwerk müssen auf dem ISA Server bestimmte Ports geöffnet werden. Auf diese Ports kann ein Angreifer zurückgreifen, um Informationen über das interne Netzwerk zu erhalten, so dass dieses danach angegriffen werden kann.

Angriffe auf die DMZ kompromittieren nicht das interne Netzwerk

Sobald ein Angreifer Zugang zur DMZ erlangt, erfolgt in diesem Modell nicht automatisch auch ein Angriff auf das lokale Netzwerk. Sofern für bestimmte Dienste jedoch eine Kommunikation mit Geräten des lokalen Netzwerks erforderlich ist, kann der ISA Server für diese Kommunikation bestimmte Regeln verwenden. Allerdings minimiert eine solche, wenn auch geregelt, Kommunikation zwischen der DMZ und dem internen Netzwerk dessen Sicherheit.

Im lokalen Netzwerk befinden sich sämtliche Geräte, die nicht direkt vom Internet aus angesprochen werden können, also Clients, Domänencontroller, Datei- und Druckserver usw.

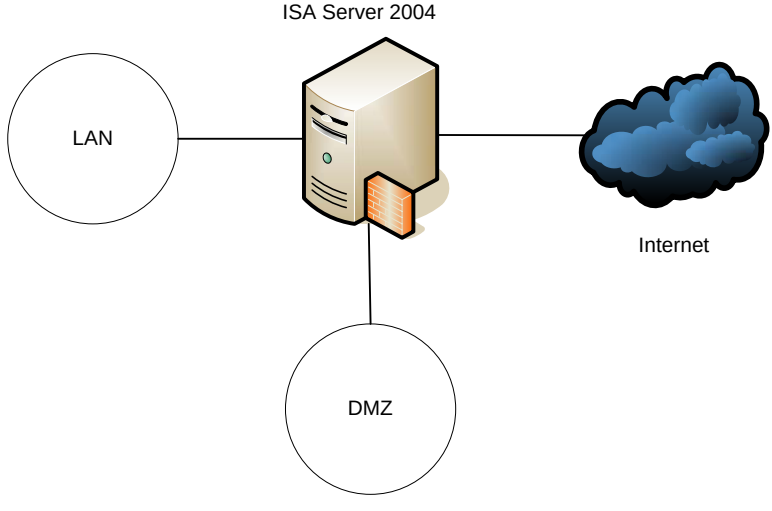
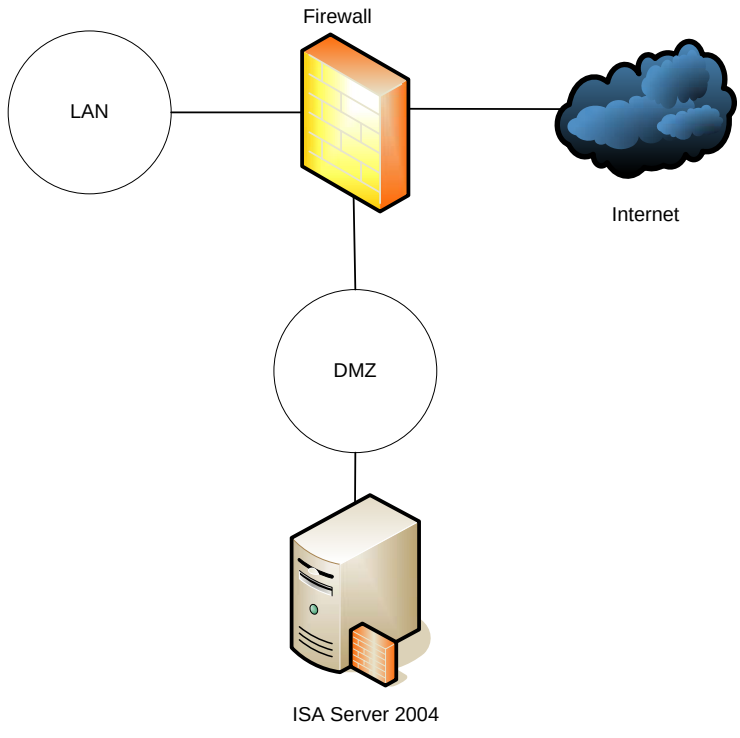


Abbildung 2.3: Der ISA Server grenzt die drei Bereiche logisch und physikalisch voneinander ab, was die Sicherheit der Ressourcen im LAN erhöht

2.5 ISA Server in einer DMZ

Dieses Modell kann eine gute Zwischenlösung darstellen, bis ein Unternehmen seine bisherige Firewall, die das Netzwerk in die drei Bereiche intern, extern und DMZ teilt, durch den ISA Server ablöst. Es kann aber ebenso gut auch eine dauerhafte Lösung darstellen. In diesem Szenario wird der ISA Server zunächst in eine bereits vorhandene DMZ gesetzt (siehe Abbildung 2.4).

Abbildung 2.4: Dieses Modell kann als Zwischenlösung oder sogar als dauerhafte Lösung eingesetzt werden



Verbergen der veröffentlichten Server

Innerhalb der DMZ kann der ISA Server andere dort befindliche Server veröffentlichen. Zwar ist diese Funktion theoretisch überflüssig, da sie bereits von der anderen Firewall übernommen wird, allerdings kann die Firewall Verbindungen für bestimmte Protokolle an den ISA Server in der DMZ weiterleiten. Über den ISA Server wird über eine Veröffentlichungsregel der betreffende Server veröffentlicht. Der veröffentlichte Server ist auf diese Weise verborgen und zusätzlich können Mechanismen wie Anwendungsfilterung oder Authentifizierung angewendet werden, auch wenn die andere Firewall diese Funktionen nicht bietet.

Sie können den ISA Server in der DMZ als Proxy-Server und Cache-Server einsetzen, so dass die ausgehenden Verbindungen in der Geschwindigkeit optimiert werden und eine Zwischenspeicherung von Objekten möglich wird. Zudem kann der ISA Server das Reverse-Caching anwenden, um einen veröffentlichten Webserver zu entlasten.

2.6 Anbinden von Geschäftspartnern

Volle VPN-Funktionalität

Über die VPN-Funktion des ISA Server 2004 können externe Zugriffe auf bestimmte Inhalte des Unternehmensnetzwerks ermöglicht werden. Auf diese Weise kann beispielsweise Geschäftspartnern der Zugriff auf eingeschränkte Informationen ermöglicht werden (siehe Abbildung 2.5). Dabei können Sie genau steuern, auf welche Anwendungen oder Server der Zugriff beschränkt werden soll. Es wird der gesamte Datenverkehr zwischen den beiden VPN-Endpunkten verschlüsselt, und er kann somit nicht geändert werden. Die Authentifizierung zwischen den Endpunkten wird erzwungen. Danach werden auch die Zugriffs- und Routingrichtlinien zur Zugriffskontrolle auf das Netzwerk durchgesetzt.

Auch ein Schutz vor Angriffen auf Anwendungsebene ist über Anwendungsfilter-Regeln möglich.

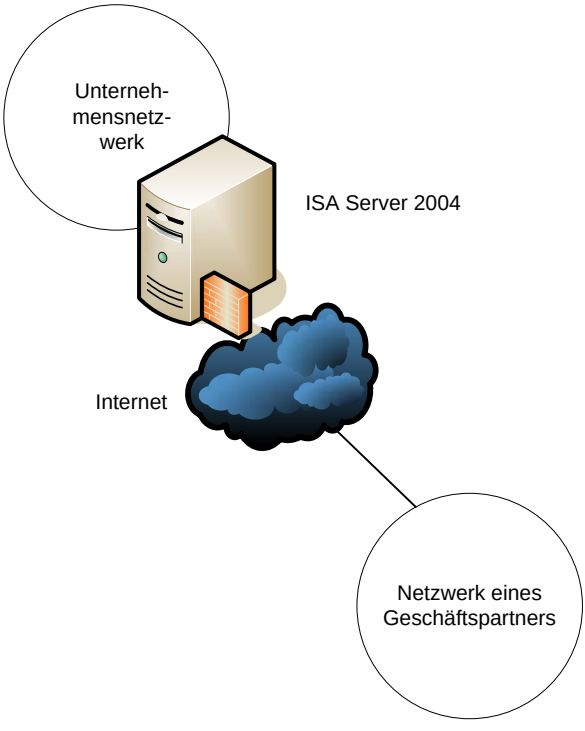
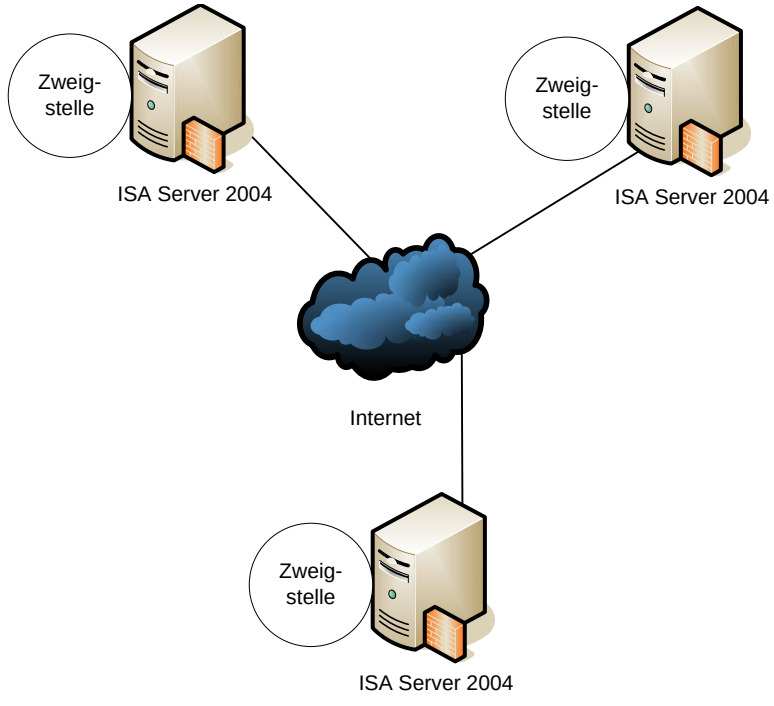


Abbildung 2.5: Der Zugriff auf das Unternehmensnetzwerk durch Geschäftspartner kann ebenfalls durch den ISA Server geregelt und eingeschränkt werden

2.7 Verbinden und Anbinden von Zweigstellen

Ähnlich wie beim Anbinden eines Geschäftspartners können auch mehrere Zweigstellen des Unternehmens über das Internet miteinander verbunden werden (siehe Abbildung 2.6). Jede einzelne dieser Zweigstellen verwendet den ISA Server als Edge-Firewall (siehe Kapitel 2.3). Auch in diesem Modell wird auf die VPN-Funktionlität des ISA Server zurückgegriffen.

Abbildung 2.6: Auch mehrere Zweigstellen können durch ISA Server über das Internet miteinander verbunden werden



Verbinden von Zweigstellen untereinander

In seiner Funktion als Edge-Firewall wird jeweils das lokale Netzwerk einer Zweigstelle abgesichert. Zusätzlich werden die Zweigstellen untereinander verbunden. Diese Verbindung ist sicher und verschlüsselt. Jede der VPN-Verbindungen wird am ISA Server beendet, da der ISA Server in diesem Modell als VPN-Gateway fungiert. Die verschlüsselten Daten werden vom ISA Server entschlüsselt und bis zur Anwendungsebene hin überprüft.

Wie auch bei der Anbindung von Geschäftspartnern kann festgelegt werden, welcher Benutzer auf welche Ressourcen zugreifen darf und welche nicht verfügbar sind.

Verbindung von Zweigstellen und Zentrale

Neben der Verbindung mehrerer Zweigstellen untereinander können auch Zweigstellen direkt mit der Unternehmenszentrale verbunden werden. Die Kommunikation erfolgt dabei ebenfalls in verschlüssel-

ter Form über das Internet. Erst am VPN-Gateway werden wiederum die Daten entschlüsselt und überprüft.

Zusätzlich zur Verbindung zur Zentrale können die einzelnen Filialen auch optional untereinander über die VPN-Funktion des ISA Server verbunden sein.

2.8 Multi Network-Firewall

Über den ISA Server kann eine unbegrenzte Anzahl von Netzwerken verwaltet werden. Einzige Voraussetzung ist, dass der ISA Server für jedes Netzwerk eine eigene Netzwerkkarte besitzt, um die Verbindung zu diesem herzustellen.

Für dieses Modell (siehe Abbildung 2.7) kann es verschiedene Gründe geben. Innerhalb des Firmennetzwerks können verschiedene Ressourcen zu jeweils einem eigenen Netzwerk zusammengefasst werden, so dass der Netzwerkverkehr zwischen diesen Netzwerken besser überwacht werden kann. So können Sie z.B. ein Netzwerk für die Clients, ein weiteres für die Server und ein drittes für die Testumgebung erstellen.

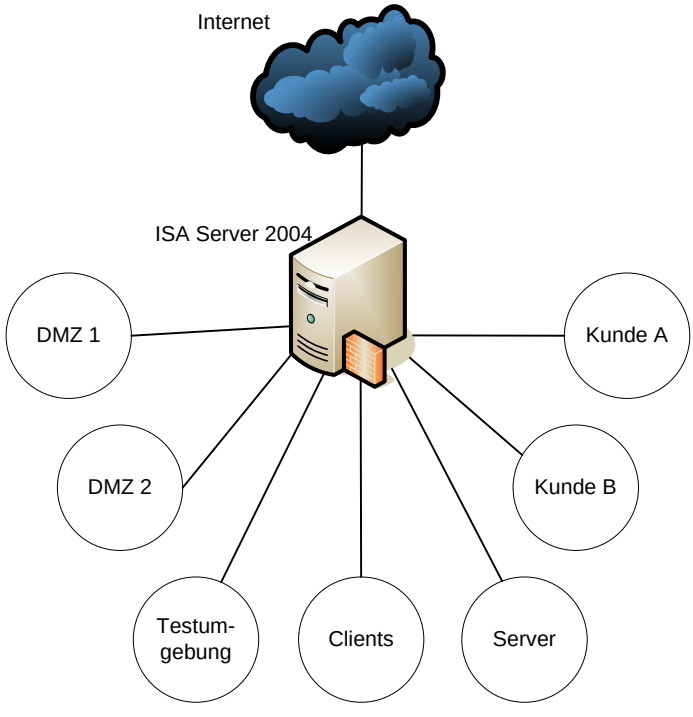


Abbildung 2.7: Der ISA Server 2004 kann beliebig viele Netzwerke verwalten und Beziehungen zwischen den einzelnen Netzwerken herstellen

Unterschiedliche Sicherheitsanforderungen

Aber auch, wenn Sie für verschiedene Kunden mit unterschiedlichen Sicherheitsansprüchen Hosting betreiben, ist dieses Modell sehr sinnvoll. So können für jeden Kunden eigene Regeln bezüglich der Sicherheit für Server oder DMZ aufgestellt werden.

Zwischen den einzelnen Netzwerken können NAT- oder Route-Beziehungen festgelegt werden.

2.9 Back-to-Back-Firewall

Im Modell der Back-to-Back-Firewall befinden sich zwei ISA Server, die eine DMZ nach innen und nach außen hin absichern (siehe Abbildung 2.8).

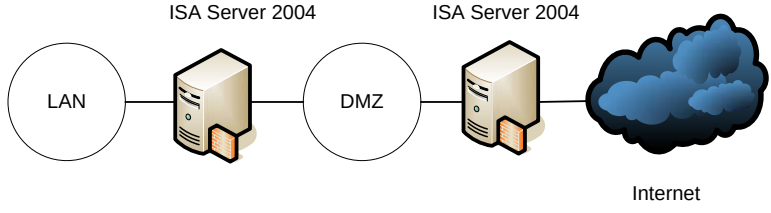


Abbildung 2.8: In einer Back-to-Back-Firewall sichern zwei ISA Server eine DMZ nach innen und außen hin ab

Alle Server, die in der DMZ veröffentlicht sind, werden in diesem Modell ebenso geschützt wie im DMZ-Modell (siehe Kapitel 2.4). Durch den Einsatz der zweiten Firewall wird das interne Netzwerk zusätzlich geschützt, so dass bei einem Angriff auf die äußere Firewall nicht zwangsläufig ein Angriff auf das lokale Netzwerk gegeben ist.

Einsatz unterschiedlicher Firewalls

Als innere Firewall muss nicht zwangsläufig auch ein ISA Server eingesetzt werden. Es kann sogar sinnvoll sein, ein anderes Firewall-Produkt einzusetzen. Hat ein Angreifer in einer Firewall eine Sicherheitslücke entdeckt, so steht immer noch die zweite zur Verfügung, die mit hoher Wahrscheinlichkeit nicht dieselbe Lücke aufweist. Gegen den Einsatz zweier verschiedener Firewalls spricht jedoch der Konfigurationsaufwand. Bevor ein neues Firewall-Produkt produktiv eingesetzt werden kann, muss dieses entsprechend getestet und konfiguriert worden sein. Bei zwei Produkten erfordert dies den doppelten Aufwand an Zeit, Personal und Wissen.

Handelt es sich auch bei der internen Firewall um einen ISA Server, so kann dieser als Mitglied der Domäne eingerichtet werden, so dass er direkt auf die Kontoinformationen des Active Directory zugreifen kann. Diese Informationen können für die Authentifizierung und die auf Benutzer- und Gruppenkonten basierenden Zugriffsregeln genutzt werden. Der interne ISA Server kann auch als VPN-Gateway für den Zugriff externer Clients auf das Firmennetzwerk eingerichtet werden.

Der externe Server sollte nicht als Domänenmitglied, sondern als allein stehender Server eingerichtet werden. Über diesen ISA Server werden die Server und Dienste in der DMZ veröffentlicht. Da für die Authentifizierung an diesen Servern keine Informationen des Active Directory notwendig sind, ist eine Konfiguration des ISA Server als Domänenmitglied nicht sinnvoll, da bei einem Angriff auf diese

Informationen unberechtigter Zugriff erfolgen könnte. Handelt es sich jedoch um einen allein stehenden Server, so befindet sich der Angreifer nach der Aushebelung dieses Servers lediglich vor der zweiten Firewall. Bevor der Angreifer auch noch diesen Server aushebeln kann, sollte der Angriff auf den äußeren ISA Server bemerkt und unterbunden worden sein.

Weitere Hinweise zum Einrichten von ISA Servern als Domänenmitglied oder allein stehender Server finden Sie in Kapitel 2.16.

2.10 Absichern der Remote-Verbindung

Der ISA Server ermöglicht Remote-Benutzern den sicheren Zugriff auf das Unternehmensnetzwerk und schützt dabei das Netzwerk vor Angriffen und Gefahren wie Viren oder Würmern. Es werden dazu komplexe Prüf- und Filterkriterien angewendet.

Es können Netzwerkrichtlinien erstellt werden, um bestimmten VPN-Benutzern oder –Gruppen nur den Zugriff auf bestimmte Anwendungen oder Server zu ermöglichen.

VPN-Quarantäne

Neu ist die Funktion der VPN-Quarantäne. Hierüber können sämtliche VPN-Clients isoliert werden, die nicht den Sicherheitsrichtlinien des Unternehmens entsprechen, z.B. kein Antivirenprogramm oder keine Updates installiert haben. Diesen potenziell unsicheren Computern wird solange der Zugriff auf das Netzwerk verwehrt, bis diese die Anforderungen des Unternehmens erfüllt haben. Erst danach ist diesen Clients der Zugriff gestattet.

2.11 Veröffentlichen von Web-Servern

Intranetinformationen und –anwendungen können mit Hilfe von Server- und Webveröffentlichungsregeln in sicherer Weise im Internet veröffentlicht werden. Für diese Aufgabe steht ein komfortabler Assistent bereit, um Misskonfigurationen und Einrichtungsfehler zu unterbinden. Die Funktion der Linkübersetzung bietet eine Umwandlung von Internetlinks zu öffentlich zugänglichen Websites.

Die Benutzung gültiger URLs kann erzwungen und der Datenverkehr auf Gültigkeit hin überprüft werden. Auch eine Vorab-Authentifizierung der Benutzer über vorhandene Authentifizierungssysteme ist möglich. Dadurch werden anonyme Anfragen an den veröffentlichten Server unterbunden.

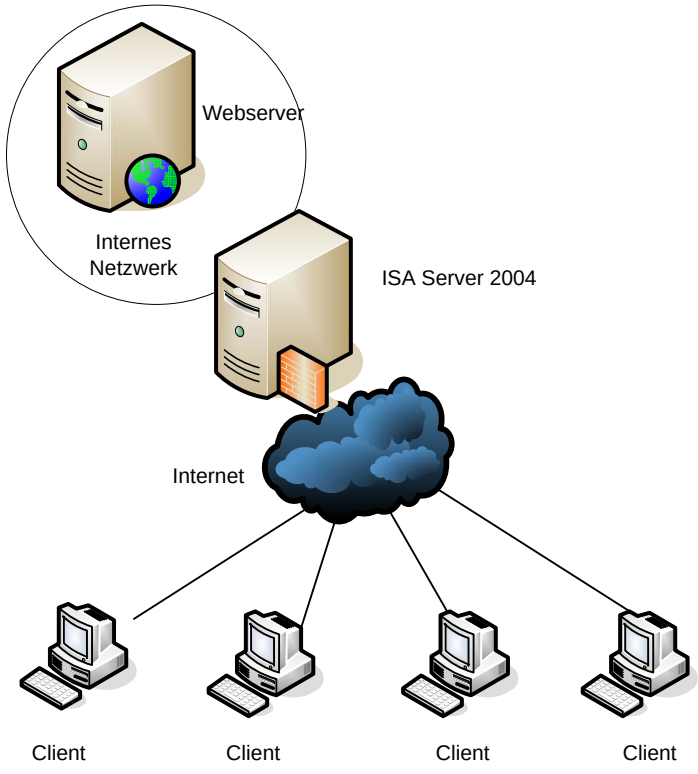


Abbildung 2.9: Absicherung des Webservers durch den ISA Server 2004 vor unbefugtem Clientzugriff

2.12 E-Mail-Zugriff von außerhalb

Sichere Authentifizierung

Durch die Unterstützung von *Outlook Web Access* durch den ISA Server 2004 ist auch für Mitarbeiter außerhalb des Firmennetzwerks ein sicherer und risikoloser Zugriff auf die von *Exchange* bereitgestellten E-Mails, Kalender und Kontakte möglich. Hierzu wird eine Webveröffentlichungsregel erstellt, die eine formularbasierte, und somit sichere Authentifizierung erzwingt. Anonyme Benutzeranmeldungen sind nicht mehr möglich, was einen besseren Schutz der internen Server bedeutet.

Es kann auch überprüft werden, ob bei Remote-E-Mails RADIUS (Remote Authentication Dial-In User Service) oder RSA SecurID verwendet wird. So können keine anonymen Anfragen an den internen Exchange-Server gelangen.

Des Weiteren ist auch ein Schutz der E-Mails vor Angriffen möglich. Durch den Einsatz von SSL-Verschlüsselung (Secure Sockets Layer) kann der gesamte SSL-Verkehr auf gefährlichen Code hin analysiert werden. Des Weiteren können über den http-Filter Anwendungsinhalte geprüft werden.

Fast selbstverständlich ist schon das Blockieren bestimmter E-Mail-Anhänge sowie das Setzen von Sitzungstimeouts. Auf diese Weise wird verhindert, dass eine Sitzung auf unbestimmte Zeit geöffnet bleibt und für andere Benutzer zugänglich wird.

Der ISA Server 2004 ermöglicht den sicheren Exchange-Zugriff bei einem breiten Spektrum von Zugriffsmöglichkeiten durch Mitarbeiter außerhalb des internen Firmennetzwerks.

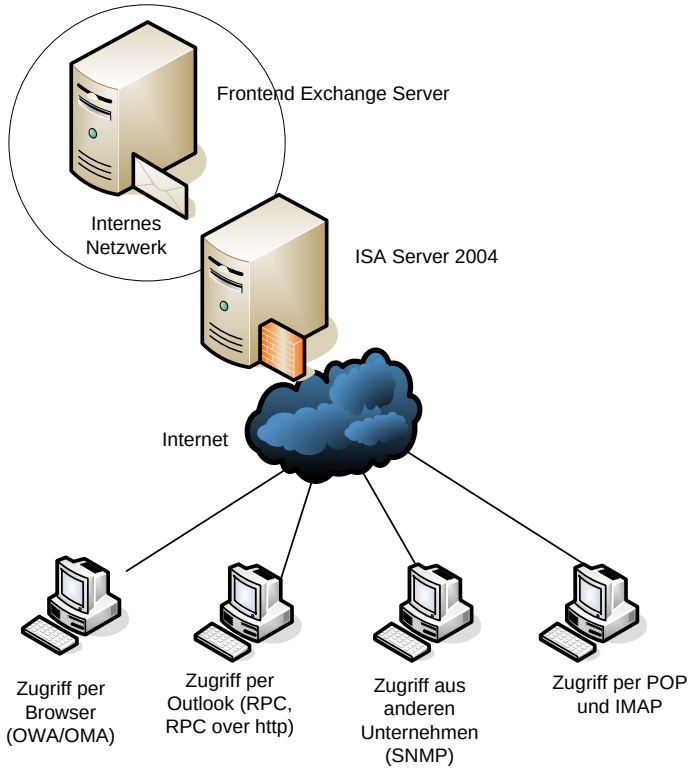


Abbildung 2.10: Der ISA Server 2004 sichert den Zugriff auf Exchange bei vielfältigen Zugriffsmöglichkeiten ab

2.13 Die Benutzung des Internets absichern

Für den ISA Server können Zugriffsrichtlinien für das Internet erstellt werden, so dass Benutzern bestimmte Internetseiten oder Inhalte nicht zur Verfügung stehen. Auf diese Weise können Sie einerseits Seiten blockieren, auf denen sich potenziell gefährliche Inhalte wie Viren oder Würmer befinden, andererseits auch Seiten, die die Benutzer von der produktiven Arbeit ablenken. Hier sind hauptsächlich Seiten aus dem Porno-Bereich, aber auch inhaltlich unbedenkliche Seiten wie z.B. ebay möglich, die der Benutzer während seiner Arbeitszeit für den privaten Gebrauch nutzt.

Instant-Messaging und Peer-to-Peer-Verbindungen unterbinden

Mit Hilfe der http-Filterung ist es auch möglich, Instant-Messaging-Applikationen wie den MSN-Messenger oder Peer-to-Peer-Anwendungen wie z.B. Tauschbörsen zu unterbinden. Durch Anwendungsfilter werden auch Angriffe auf dieser Netzwerkebene im Vorfeld erkannt. Des Weiteren wird geprüft, ob ein eingehendes Datenpaket auf einer Clientanforderung beruht. Ist dies nicht der Fall, wird dieses Paket blockiert und nicht an den Client weitergeleitet.

Das Erstellen der Regeln wird vereinfacht, da der ISA Server 2004 auf die Benutzerdatenbank des Active Directory zurückgreifen kann.

2.14 Performancegewinn bei Webinhalten

Downstream-Cache

Die Cache-Funktion des ISA Server bringt einen Performancegewinn bei Zugriff auf häufig genutzte Webinhalte. Der ISA Server verwendet bestimmte Funktionen, um Muster im Internet-Datenverkehr zu ermitteln und oft besuchte Websites automatisch downzuloaden, um so den Zugriff darauf zu beschleunigen und zu optimieren. Dazu wird der Downstream-Cache verwendet (siehe Abbildung 2.11).

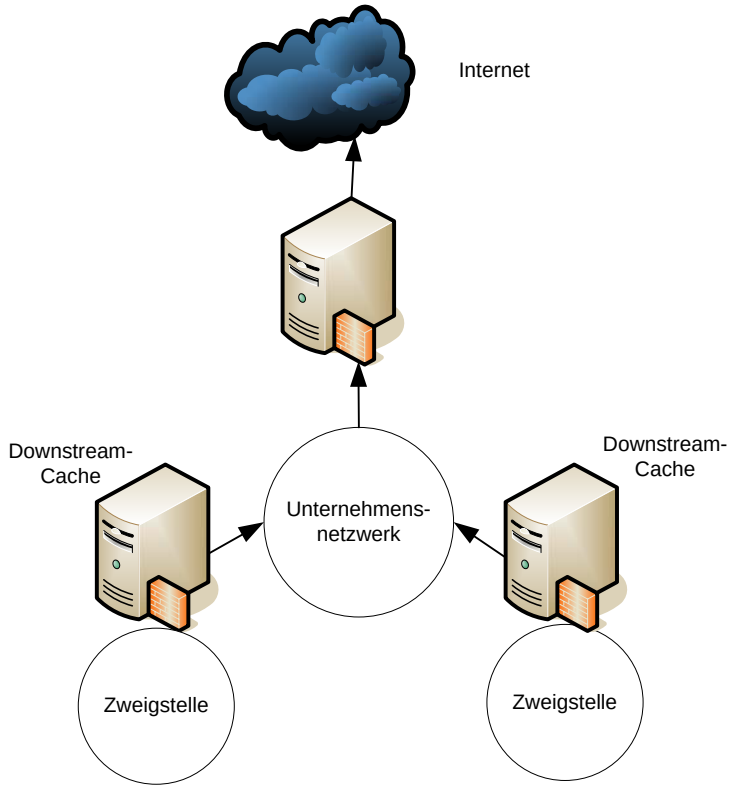


Abbildung 2.11: Der Downstream-Cache optimiert den Zugriff auf häufig benutzte Internetseiten und -objekte

Sobald der Downstream-Cache gefüllt ist, können vom ISA Server Anfragen an den Upstream-Cache-Server weitergeleitet werden (siehe Abbildung 2.12).

Upstream-Cache

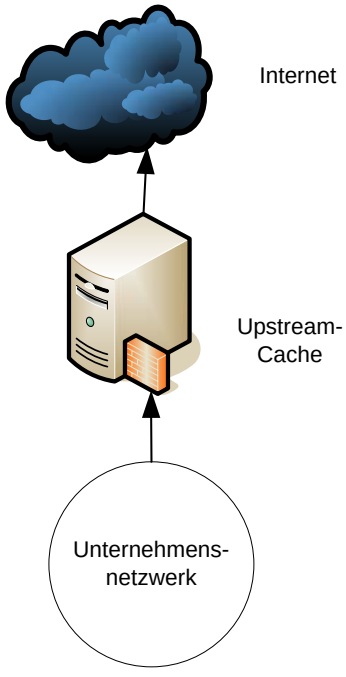


Abbildung 2.12: Sobald der Downstream-Cache gefüllt ist, steht der Upstream-Cache zur Verfügung

2.15 Theoretische Grundlagen

Nach der Beschreibung der praktischen Einsatzmodelle des ISA Server werden nachfolgend auch die theoretischen Grundlagen vorgestellt. Dazu gehören das OSI-Modell sowie das TCP/IP-Modell. Diese Modelle basieren auf unterschiedlichen Schichten, die wiederum für den ISA Server wichtig sind, da er ebenfalls schichtbasiert den Netzwerkverkehr analysiert und blockiert.

2.15.1 Das OSI-Referenzmodell

Theoretisch, aber nicht überflüssig!

Die Abkürzung OSI-Modell steht für Open Systems Interconnection Model. Dabei handelt es sich um ein siebenstufiges Modell, das gemäß ISO die komplette Netzwerkkommunikation beschreibt. Diese sieben Schichten werden bei jeder Netzwerkanfrage, die von einem Computer ausgeht, durchlaufen.

Die Bedeutung der sieben Schichten des OSI-Modells wird in Tabelle 2.1 beschrieben.

Tabelle 2.1: Die sieben Schichten des OSI-Modells und deren Bedeutung

Schicht	Beschreibung
Anwendungsschicht	Diese Schicht kommuniziert direkt mit der Anwendung, die die Kommunikation einleitet. Sie stellt der Applikation, z.B. einem Browser, die Netzwerkfunktion zur Verfügung.
Darstellungsschicht	Über die Darstellungsschicht wird das Datenformat bestimmt, in dem die Daten ausgetauscht werden und von der jeweiligen Applikation dargestellt werden können.
Sitzungsschicht	In dieser Schicht kann die Anwendung eine Verbindung zu einer Anwendung eines anderen Geräts herstellen. Die Sitzungsschicht ist für die Herstellung, die Unterhaltung sowie das Beenden einer Verbindung zuständig. Dabei wird auch bestimmt, ob es sich um eine bidirektionale oder unidirektionale Verbindung handelt.
Transportschicht	Die Transportschicht ist für den Transport der Pakete zuständig. Dabei wird auch der korrekte Transport und Empfang gewährleistet, indem für empfangene Pakete Bestätigungen versendet und doppelt gesendete Pakete verworfen werden. Der Paketempfänger setzt die einzelnen Pakete wieder zusammen. Danach erfolgt eine Übergabe an die weiteren Schichten.
Vermittlungsschicht	In dieser Schicht werden die Pakete weitergeleitet und geroutet. Beim Einsatz des TCP/IP-Protokolls werden die Pakete an die korrekten IP-Adressen weitergeleitet.
Sicherungsschicht	In der Sicherungsschicht wird aus den Daten ein Rahmen erstellt. An diesen Rahmen werden CRC-Informationen (Cyclic Redundancy Check) angehängt, die zur Erkennung und Korrektur von Fehlern in der Übertragung verwendet werden.
Bitübertragungsschicht	In dieser letzten Schicht werden die Daten zum Versenden auf das jeweilige Medium, z.B. ein Kupferkabel oder einen Lichtwellenleiter, übertragen und versendet.

2.15.2 Das TCP/IP-Modell

Basiert auf OSI-Modell

Im Gegensatz zum OSI-Referenzmodell besteht das TCP/IP-Modell lediglich aus vier Schichten, ist ansonsten dem OSI-Modell jedoch recht ähnlich. In Abbildung 2.13 sehen Sie, wie das TCP/IP-Modell die sieben Stufen des OSI-Modells in sich vereint.

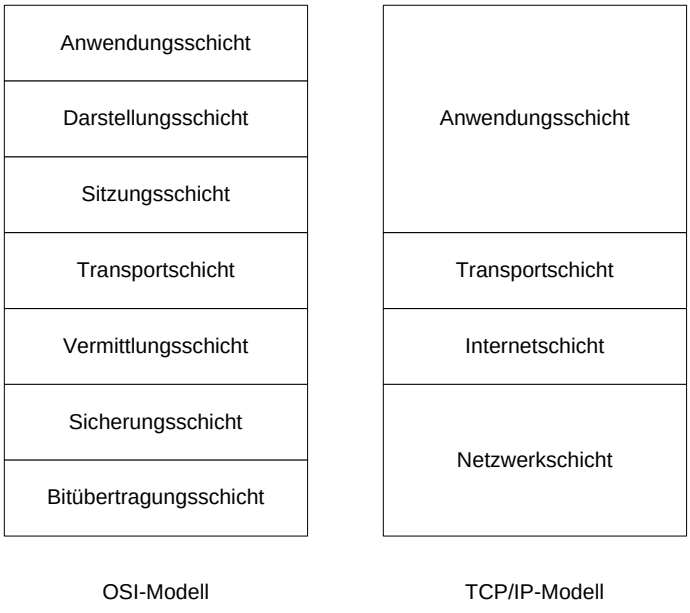


Abbildung 2.13: Das OSI-Modell und das TCP/IP-Modell im Vergleich

Die einzelnen Stufen des TCP/IP-Modells haben die in Tabelle 2.2 beschriebenen Bedeutungen.

Schicht	Beschreibung
Anwendungsschicht	In dieser Schicht werden Anwendungen TCP/IP-basierte Protokolle zur Verfügung gestellt. Dabei kann es sich beispielsweise um http, ftp, smtp, pop3, imap4 oder dns handeln.
Transportschicht	In der Transportschicht werden die Protokolle TCP und UDP verwendet. TCP ist ein verbindungsorientiertes Protokoll, während UDP verbindungslos arbeitet. Bei Verwendung von TCP werden die Daten nach dem TCP-Handshake so übermittelt, dass verlorene Pakete erneut versendet werden, bis alle Pakete den Empfänger erreicht haben. TCP wird beispielsweise von http und ftp verwendet. Bei Verwendung von UDP wird nicht geprüft, ob alle Pakete vollständig übermittelt worden sind. Dieses Manko bringt jedoch gegenüber TCP Vorteile in der Übertragungsgeschwindigkeit. UDP wird beispielsweise aus Performance-Gründen für DNS-Abfragen verwendet.
Internetschicht	In der Internetschicht erfolgen wie in der Vermittlungsschicht des OSI-Modells die Weiterleitung und Adressierung der IP-Pakete sowie das Routing.
Netzwerkschicht	Wie in der Bitübertragungsschicht des OSI-Modells werden in dieser untersten Schicht die Daten zum Versenden auf das jeweilige Medium, z.B. ein Kupferkabel oder einen Lichtwellenleiter, übertragen.

Tabelle 2.2: Die vier Schichten des TCP/IP-Modells und deren Bedeutung

2.15.3 Filtermethoden

Die Filterungen des ISA Server werden auf verschiedenen Ebenen durchgeführt. Dies gilt für die dynamische Paketfilterung, die Circuit-Filterung sowie die Anwendungsfilterung.

Dynamische Paketfilterung

Vermittlungsschicht

Die dynamische Paketfilterung wird zum größten Teil in der Vermittlungsschicht des OSI-Modells bzw. der Internetschicht des TCP/IP-Modells durchgeführt. Dabei werden die Paketinformationen analysiert, die von dieser Schicht dem Paket hinzugefügt wurden, nämlich der IP-Header, die Quell-IP-Adresse und die Ziel-IP-Adresse.

Außerdem wird auch der TCP/UDP-Header geprüft, der von den Protokollen der darüberliegenden Transportschicht erstellt worden ist.

Die dynamische Paketfilterung spielt für den Einsatz von Filterregeln eine wichtige Rolle, da z.B. der Verkehr von bestimmten Quellen aus oder an bestimmte Ziele unterbunden werden kann. Sofern keine definierte Regel eine Verbindung gestattet, wird die Verbindung getrennt und das zugehörige Paket verworfen.

Stateful Inspection

Auch bei der Stateful Inspection werden auf der Internetschicht die eingehenden Pakete analysiert, zusätzlich werden jedoch auch Informationen geprüft, die von anderen Schichten geliefert werden. Um sicherzustellen, dass ein bestimmtes Paket zu einer bestehenden Verbindung gehört, werden bei der Stateful Inspection die Quell-IP-Adresse und Ziel-IP-Adresse sowie die Protokolltypen, Ports und der Status der Verbindung analysiert. Ein Paket kann nur dann den ISA Server passieren, wenn es zu einer bestehenden Verbindung gehört und durch den Paketfilter zugelassen ist.

Dabei wird auch das dynamische Öffnen und Schließen der benötigten Ports unterstützt, so dass nicht für eine Antwort diverse Ports offen gehalten werden müssen.

Circuit-Filterung

Die Circuit-Filterung bzw. Sitzungsfilterung funktioniert wie ein Proxy-Server zwischen zwei Geräten, so dass diesen eine direkte Verbindung untereinander impliziert wird. Dabei wird die komplette Sitzung überwacht, so dass Pakete erkannt werden, die nicht als Antwort auf eine ausgehende Anfrage eingehen.

Anwendungsfilterung

Voraussetzung für eine sichere Firewall

Moderne Angriffe werden häufig auf der Anwendungsebene ausgeführt, um z.B. einen bestimmten Dienst durch ein Häufung von Anfragen zum Absturz zu bringen. Durch die Paketfilterung und Cir-

cuit-Filterung können lediglich die Paket-Header überprüft werden. Deshalb sollte die Firewall-Lösung auch unbedingt die Anwendungsfilterung unterstützen, um auch andere Formen von Bedrohung erkennen zu können.

Sobald ein Paketfilter ein bestimmtes Paket die Firewall passieren lässt und an einen Server weiterleitet, ist damit noch nicht sichergestellt, dass sich in dem Paket nicht bösartiger Code befindet, der den Server z.B. zum Absturz bringen kann, da das Protokoll bei den Filterungen auf unteren Schichten nicht geprüft werden kann. Erst die Anwendungsfilterungen arbeiten auf der Anwendungsschicht und erkennen Protokolle wie http oder ftp und können diese analysieren. Damit ist es möglich, dass auch die Inhalte der Anfragen geprüft und schädliche Inhalte erkannt und abgewehrt werden können.

Über Anwendungsfilter können bestimmte Protokolle auch nur für bestimmte Benutzer zugelassen und für andere blockiert werden.

2.16 Die Serverrolle des ISA Server

Vor der Installation des ISA Server muss geklärt werden, in welcher Rolle dieser zu einer Domäne oder Arbeitsgruppe hinzugefügt werden soll. Der ISA Server kann in einer Domäne als Domänencontroller (DC), als Mitgliedserver oder als allein stehender Server konfiguriert werden.

2.16.1 Allein stehender Server

Arbeitsgruppe

Der ISA Server kann auch als ein allein stehender Server in einer Arbeitsgruppe implementiert werden. Diese Konfiguration bietet den Vorteil, dass bei einem Angriff auf den ISA Server nur dieser allein betroffen ist. Für die Benutzerauthentifizierung der lokalen Benutzer- und Gruppenkonten wird RADIUS verwendet.

2.16.2 Domänencontroller und Mitgliedserver

Domäne

Besteht eine Domäne, so kann der ISA Server als Domänencontroller oder als Mitgliedserver zu dieser hinzugefügt werden. Aufgrund von Sicherheitsüberlegungen ist es nicht sinnvoll, dass auf dem ISA Server Informationen wie z.B. die Benutzerdatenbank des Active Directory vorhanden ist, da auf den ISA Server direkt aus dem Internet zugegriffen werden kann. Bei einem Einsatz als Domänencontroller wäre jedoch die komplette Benutzerdatenbank bzw. beim Einsatz mehrerer Domänencontroller ein Replikat dieser auf dem ISA Server vorhanden.

Wir der ISA Server als Mitgliedserver eingerichtet, befindet sich auf diesem zwar nicht die Benutzerdatenbank, dennoch ist im Gegensatz

zur Konfiguration als allein stehender Server bei einem Angriff auf den ISA Server schnell auch das dahinter stehende Netzwerk betroffen.

Allerdings gibt es auch einige Modelle, in denen der ISA Server zwangsläufig als Domänencontroller oder Mitgliedserver konfiguriert werden muss.

ISA Server 2004 Enterprise-Version

Active Directory erforderlich

Der ISA Server 2004 in der Enterprise-Version erfordert ein Active Directory, in dem die Konfigurationseinstellungen des ISA Server bzw. des Arrays gespeichert werden. Dazu muss der ISA Server als Mitgliedserver eingerichtet sein. Die Konfiguration als Domänencontroller ist jedoch nicht erforderlich. Ein ISA Server 2004 Enterprise kann nicht in einer Arbeitsgruppe installiert werden.

Back-to-Back-Firewall

Beim Einsatz einer Back-to-Back-Firewall (siehe Kapitel 2.9) ist der interne ISA Server nicht direkt aus dem Internet ansprechbar. Die Verbindung zum Internet erfolgt über eine andere Firewall. Bei dieser kann es sich auch um einen ISA Server handeln. Sofern der interne ISA Server als Mitgliedserver eingerichtet wird, kann dieser einerseits über die Gruppenrichtlinien des Active Directory verwaltet werden, andererseits ergibt sich auch ein geringerer Verwaltungsaufwand bei der Konfiguration der Zugriffsregeln, da direkt die Benutzer- und Gruppenkonten des Active Directory verwendet werden können.

2.16.3 Small Business Server 2003

Auch beim Einsatz des Small Business Server (SBS) in der Enterprise-Version wird der ISA Server zwangsläufig als Domänencontroller konfiguriert, da sich in diesem Fall sämtliche Komponenten des SBS auf einem Computer befinden müssen. Eine Installation der ISA-Komponente des SBS auf einem anderen Server ist nicht möglich.

2.16.4 Vertrauensstellungen

Hauptdomäne oder vertrauende Domäne

Wenn ein ISA Server zu einer Domäne hinzugefügt werden soll, ist zu überlegen, ob dieser direkt zur Hauptdomäne oder auch zu einer dieser vertrauenden Domänen hinzuzufügen ist. Es muss zwischen der Hauptdomäne und der anderen Domäne eine einseitige Vertrauensstellung bestehen, so dass der ISA Server in der vertrauenden Domäne die Informationen der Benutzerkonten auslesen kann, um dadurch das Erstellen der Zugriffsrichtlinien zu erleichtern.

Erfolgt ein Angriff auf den ISA und damit auch auf die vertrauende Domäne, so kann der Angreifer auch mit der Berechtigung des Domänen-Administrators keine weiteren Informationen aus der Hauptdomäne auslesen.

3 Installation

Dieses Kapitel beschreibt die Installation des ISA Server 2004 sowie die Voraussetzungen, die für die Installation erfüllt sein müssen. Es werden sowohl die manuelle als auch die unbeaufsichtigte Installation beschrieben. Nach der Installation sollte das Service Pack 1 für den ISA Server eingespielt werden, jedoch nur für die Standardversion und nicht für die Enterprise-Version. Auch dieses Verfahren wird beschrieben, ebenso wie Hinweise zur Protokollierung während dieser Installation. Ferner wird auch auf die Deinstallation des ISA Server eingegangen sowie auf die ersten Konfigurationsschritte nach Ende der Installation wie das Prüfen der Installationsprotokolle, das Testen der Ports oder der Konfiguration des statischen oder dynamischen Routing.

3.1 Installationsvoraussetzungen

Bevor die Installation auf dem Zielserver ausgeführt werden kann, müssen auf diesem verschiedene Voraussetzungen erfüllt sein.

3.1.1 Softwareseitige Voraussetzungen

Der ISA Server 2004 kann je nach Version auf unterschiedlichen Server-Betriebssystemen installiert werden. Für einen ISA Server 2004 Standard muss eines der folgenden Betriebssysteme installiert sein:

- Windows Server 2000 mit Service Pack 4
- Windows Advanced Server 2000 mit Service Pack 4
- Windows Server 2003 Standard
- Windows Server 2003 Enterprise

Enterprise-Version nur unter Windows Server 2003 lauffähig

Für einen ISA Server 2004 Enterprise muss eines der folgenden Betriebssysteme installiert sein:

- Windows Server 2003 Enterprise
- Windows Server 2003 Standard

Des Weiteren sollten sämtliche Patches und Hotfixes für das jeweilige Betriebssystem eingespielt sein.

Als Betriebssystem-Grundlage wird in diesem Buch ein Windows Server 2003 Enterprise verwendet.

3.1.2 Hardwareseitige Voraussetzungen

Absolute Minimalwerte

Der ISA Server stellt auch einige, wenn auch recht niedrige Anforderungen an die Hardware. Bedenken Sie jedoch, dass es sich bei den in der folgenden Tabelle angegebenen Werten um die absoluten Minimalwerte handelt, die Microsoft empfiehlt. Demgegenüber sind in der zweiten Spalte realistische Anforderungswerte aufgeführt, die einen performanten Einsatz des ISA Server mit mehreren veröffentlichten Servern sowie für ca. 250 Benutzer garantieren.

Tabelle 3.1: Hardwarevoraussetzungen des ISA Server

Komponente	Minimalanforderung	Empfohlen
Prozessor	PIII 550 MHz	P4 2.0 GHz
RAM	256 MB	1.024 MB
Festplatte	150 MB freier Speicherplatz, als Cacheserver zusätzlicher Platz auf einer NTFS-Partition	Partition für das System RAID1, Partition für den Cache RAID0 oder RAID1+0
Netzwerkkarte	Mindestens eine, beim Einsatz als Firewall mindestens zwei	Drei Netzwerkkarten, je eine für LAN, WAN und DMZ

Weiterführende Planungen einbeziehen

In die Planungen zur Hardware-Ausstattung des Servers müssen in jedem Fall Überlegungen zur späteren Konfiguration einfließen. Dazu gehören folgende Punkte:

- Anzahl der Benutzer und Applikationen, die auf das Internet zugreifen werden
- Anzahl der veröffentlichten Server
- Anzahl der VPN-Verbindungen für mobile Benutzer und Standort-zu-Standort-Verbindungen
- Konfiguration der Firewall (Anzahl der Regeln usw.)
- Auftretender Datendurchsatz des Internetverkehrs. Dieser Wert sollte auch für die Zukunft bedacht und möglicherweise hochgerechnet werden.

Ausfallsicherheit maximieren

Eine redundante Auslegung des ISA Server verringert zudem das Ausfallrisiko des Servers. Dazu zählt neben der Implementierung eines RAID auch die Verwendung einer USV. Bedenken Sie, dass beim Ausfall des ISA Server nicht nur die internen Benutzer und Applikationen keinen Zugriff mehr auf das Internet haben, sondern auch veröffentlichte Server wie z.B. *Exchange* für die externen Clients nicht mehr erreichbar sind.

Wird der Server, auf dem der ISA Server ausgeführt wird, auch noch für weitere Dienste verwendet, so müssen die genannten Hardwareanforderungen möglicherweise nach oben hin korrigiert werden.

3.1.3 Netzwerkseitige Voraussetzungen

Auch im Bereich des Netzwerks müssen einige Voraussetzungen erfüllt sein.

Konfiguration der Subnetze

Mindestens zwei Netzwerkkarten erforderlich

Die Netzwerkkonfiguration muss vor der Installation des ISA Server abgeschlossen sein. Der Server muss über mindestens zwei Netzwerkkarten verfügen, von denen eine die interne, die andere die externe Verbindung herstellt. Diese beiden Schnittstellen müssen sich in unterschiedlichen IP-Subnetzen befinden.

Die folgende Tabelle zeigt eine Übersicht über eine mögliche Zuteilung der IP-Adressen für die verschiedenen Netzwerke und Netzwerkkarten.

Komponente	IP-Adresse
DSL-Router externe Schnittstelle	Dynamisch vom Provider zugewiesen
DSL-Router interne Schnittstelle	192.168.2.1
ISA Server externe Schnittstelle	192.169.2.15
ISA Server interne Schnittstelle	192.168.2.15
LAN	192.168.2.xx

Tabelle 3.2: Übersicht über die den verschiedenen Schnittstellen zugewiesenen IP-Adressen

Zusätzlich sollten Sie den verschiedenen Netzwerkverbindungen eindeutige Namen zuweisen. Anstelle der Namen LAN-VERBINDUNG 1, LAN-VERBINDUNG 2 usw. sollten Sie die Verbindungen lieber in INTERNE VERBINDUNG und EXTERNE VERBINDUNG oder LAN und WAN umbenennen. Das Umbenennen geschieht über das entsprechende Kontextmenü der jeweiligen Verbindung unter NETZWERKVERBINDUNGEN.

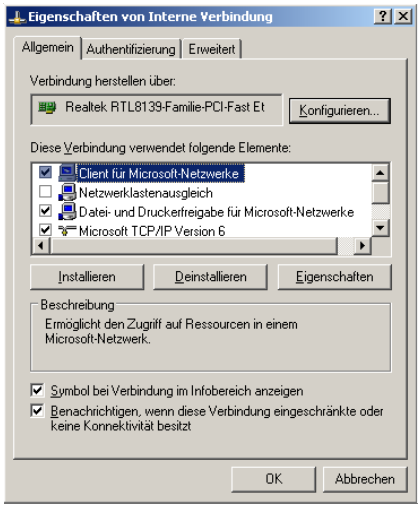
Bindung der Netzwerkprotokolle

Die Netzwerkverbindung, die die interne Verbindung herstellt, muss die folgenden Elemente besitzen (siehe Abbildung 3.1):

- CLIENT FÜR MICROSOFT-NETZWERKE
- DATEI- UND DRUCKERFREIGABE FÜR MICROSOFT-NETZWERKE
- INTERNETPROTOKOLL (TCP/IP)

Für die interne Verbindung darf *kein* Standardgateway konfiguriert werden.

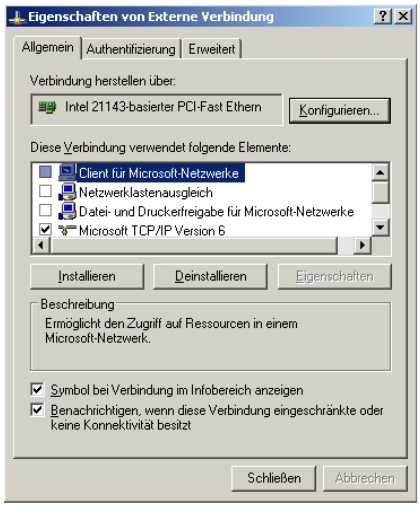
Abbildung 3.1: Die Eigenschaften der internen Netzwerkverbindung



Die Netzwerkverbindung für die externe Verbindung sowie eine optionale DMZ muss lediglich über das INTERNETPROTOKOLL (TCP/IP) verfügen (siehe Abbildung 3.2). Deaktivieren Sie für diese Verbindung die folgenden Funktionen:

- Client für Microsoft-Netzwerke
- Datei- und Druckfreigabe für Microsoft-Netzwerke
- Dynamische DNS-Registrierung (Deaktivieren der Checkbox ADRESSEN DIESER VERBINDUNG IN DNS REGISTRIEREN auf der Registerkarte DNS der erweiterten TCP/IP-Einstellungen)
- LMHosts-Abfragen (Deaktivieren der Checkbox LMHOSTS-ABFRAGE AKTIVIEREN auf der Registerkarte WINS)
- NetBIOS über TCP/IP (Auswahl NETBIOS ÜBER TCP/IP DEAKTIVIEREN auf der Registerkarte WINS)

Abbildung 3.2: Die Eigenschaften der externen Netzwerkverbindung



Für die externe Verbindung darf *kein* DNS-Server konfiguriert werden.

Reihenfolge der Netzwerkkarten-Bindungen

Zuerst intern, am Schluss extern

Auch die Reihenfolge der Bindungen ist wichtig. Die Bindung der internen Verbindung muss zuerst erfolgen, die der externen Verbindung zuletzt. Ist zusätzlich eine Netzwerkkarte für die DMZ konfiguriert, wird diese zwischen die beiden anderen gebunden. Um diese Reihenfolge herzustellen, klicken Sie im Fenster NETZWERKVERBINDUNGEN auf das Menü ERWEITERT/ERWEITERTE EINSTELLUNGEN. Dort stellen Sie die entsprechende Reihenfolge über die Pfeiltasten her (siehe Abbildung 3.3).

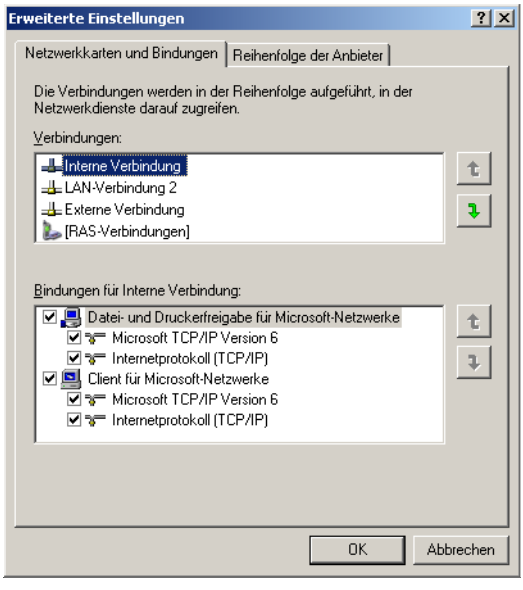


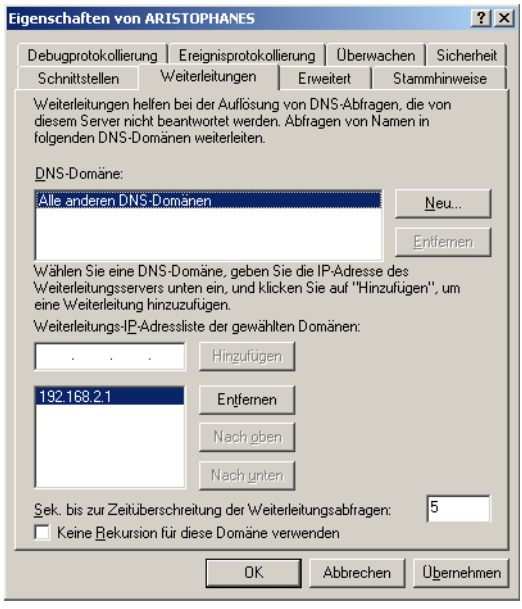
Abbildung 3.3: Die Bindungsreihenfolge der Netzwerkverbindungen

DNS-Konfiguration

Der ISA Server muss kein DNS-Server sein

Auf dem ISA Server muss nicht zwangsläufig ein DNS-Server installiert sein. Die Verteilung der Serverrollen ist abhängig von der Größe des Netzwerks und somit der Anzahl der vorhandenen Server. Ist ein DNS-Server installiert, so muss er keine eigene DNS-Zone besitzen, sondern kann über eine Active Directory-integrierte Zonenkopie zurückgreifen. In diesem Fall werden sämtliche DNS-Anfragen für alle DNS-Domänen an eine andere IP-Adresse weitergeleitet (siehe Abbildung 3.4).

Abbildung 3.4: Die DNS-Konfiguration



3.2 Durchführen der Installation

Nachdem alle eben genannten Voraussetzungen erfüllt sind, kann mit der Installation begonnen werden. Bei der Installation sind einige Schritte unterschiedlich, je nachdem, ob es sich um eine Standard- oder Enterprise-Version handelt. Die Installation einer Testversion weicht nicht vom hier beschriebenen Prozess ab.

3.2.1 Die Installation der Standard-Version

Um die Standardversion des ISA Server 2004 zu installieren, führen Sie die folgenden Schritte aus:

1. Sobald die CD eingelegt wurde, erhalten Sie das in Abbildung 3.5 dargestellte Fenster. Klicken Sie hier auf ISA Server 2004 installieren.

Um weitere Informationen über den ISA Server zu erhalten, können Sie unter ANMERKUNGEN ZUR VERSION ANZEIGEN oder BENUTZERHANDBUCH ERSTE SCHRITTE ANZEIGEN zusätzliche Hinweise anzeigen lassen.

In einem zusätzlichen Fenster werden Sie über den jeweiligen Installationsstatus informiert. Der Installationsprozess gliedert sich in die drei Vorgänge KERNKOMPONENTEN, ZUSÄTZLICHE KOMPONENTEN sowie SYSTEMINITIALISIERUNG.

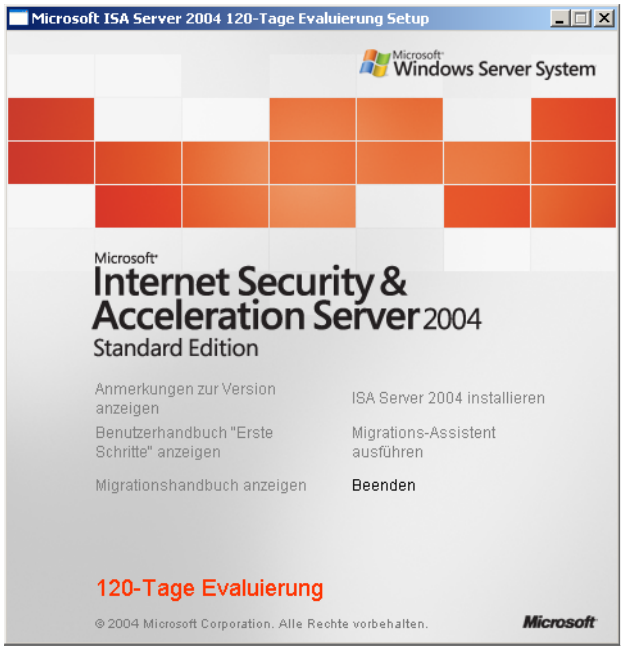


Abbildung 3.5: Die Installation des ISA Server 2004 Standardversion

2. Im Willkommensfenster der Installation klicken Sie auf Weiter. Als Nächstes müssen Sie in den beiden folgenden Fenstern die Lizenzbedingungen akzeptieren sowie die 25-stellige Produkt-ID eingeben (siehe Abbildung 3.6). Klicken Sie jeweils auf Weiter.

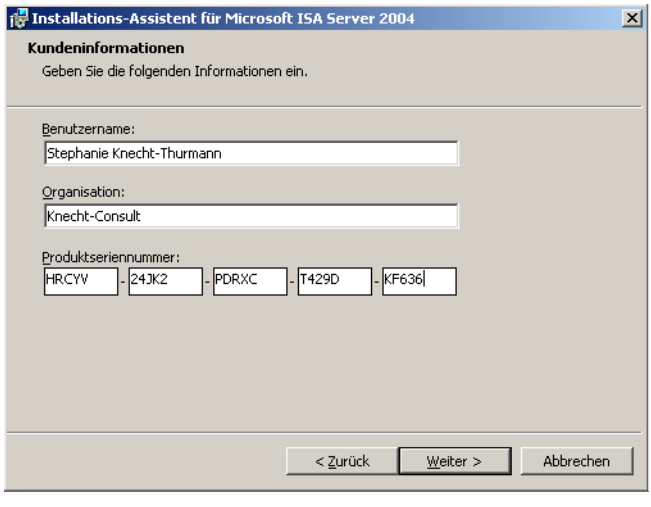


Abbildung 3.6: Eingabe der Benutzerinformationen und der Lizenznummer

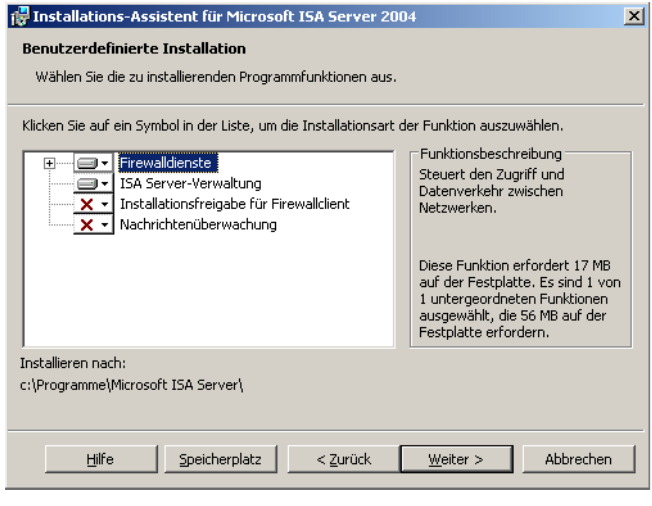
3. Als Nächstes wird der Setup-Typ gewählt (siehe Abbildung 3.7). Bei der Installationsart TYPISCH werden sämtliche Komponenten bis auf die NACHRICHTENÜBERWACHUNG installiert, bei VOLLSTÄNDIG alle Komponenten. Über ÄNDERN kann ein anderes Installations-

verzeichnis gewählt werden. Das Standardverzeichnis lautet `C:\Programme\Microsoft ISA Server`. Klicken Sie dann auf WEITER.

Abbildung 3.7: Die Auswahl der Installationsart

4. Als Nächstes werden im Fenster KOMPONENTENAUSWAHL (siehe Abbildung 3.8) die zu installierenden Komponenten des ISA Server ausgewählt. Die einzelnen Komponenten können entweder lokal installiert werden, eine lokale Installation aller Komponenten ist möglich, oder eine Komponente ist nicht verfügbar. Im rechten Teilbereich FUNKTIONSBESCHREIBUNG erhalten Sie nähere Hinweise zu der jeweiligen Komponente. Klicken Sie dann auf WEITER.

Abbildung 3.8: Die Auswahl der zu installierenden Komponenten des ISA Server



Für die weiteren Installationsschritte werden hier sämtliche Komponenten ausgewählt. Sind nicht alle Komponenten gewählt, können die folgenden Fenster geringfügig abweichen.

Installationsfreigabe des Firewallclients

Sie sehen, dass Sie die Möglichkeit haben, die Komponente INSTALLATIONSFREIGABE FÜR FIREWALLCLIENT nicht auszuwählen. Unter dem ISA Server 2000 musste sich diese Komponente zwangsläufig auf dem ISA Server befinden, unter ISA 2004 kann die Komponente auch auf einem beliebigen Dateiserver liegen. Die Freigabe \MSPCLNT ist für die Installation des Clients nicht mehr nötig. Dies liegt darin begründet, dass der ISA Server 2004 in der Lage ist, nur bestimmte Protokolle über seine Netzwerkschnittstelle zum LAN zuzulassen und den Rest zu blockieren, so dass bei einer Sperrung des Dateizugriffs keine Installation des Firewallclients vom ISA Server aus möglich wäre.

Die Komponente NACHRICHTENÜBERWACHUNG kann nur installiert werden, wenn auf dem Computer ein virtueller SMTP-Server installiert ist. Ist dies nicht der Fall, erhalten Sie einen entsprechenden Hinweis. Die Installation des SMTP-Servers geschieht über die SERVERVERWALTUNG.

5. Nun werden im Fenster INTERNES NETZWERK (siehe Abbildung 3.9) die Adressbereiche bestimmt, die der ISA Server als internes Netzwerk einbeziehen soll. Klicken Sie auf HINZUFÜGEN, um ein Netzwerk zu wählen.

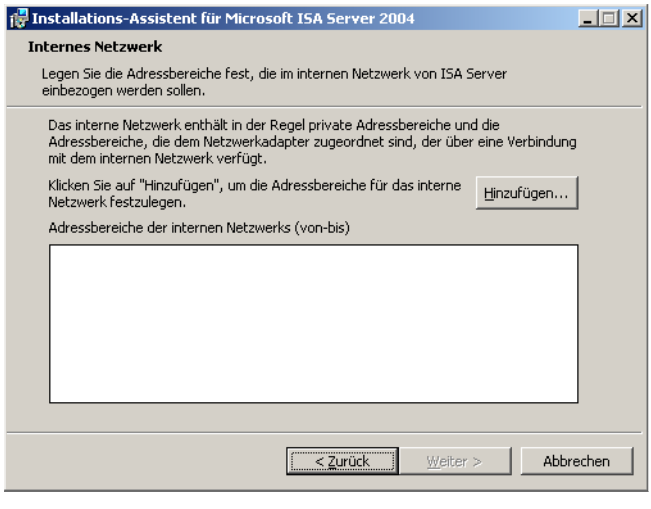
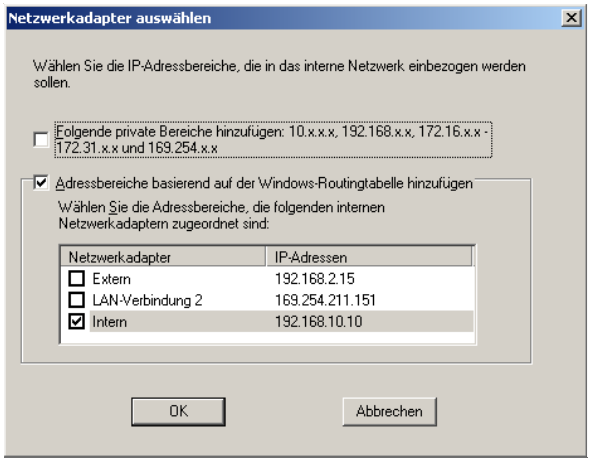


Abbildung 3.9: Hinzufügen des Adressbereichs für das interne Netzwerk

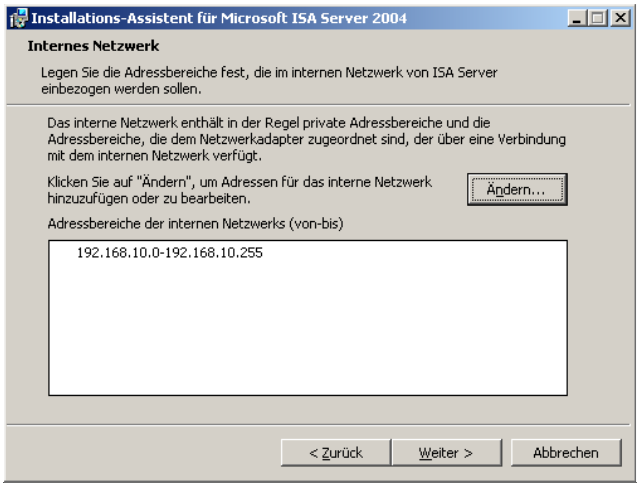
Es können entweder manuell die Adressbereiche festgelegt werden, oder Sie klicken auf NETZWERKADAPTER AUSWÄHLEN, um den Bereich zu bestimmen. Bei dieser Option können Sie entweder die vordefinierten privaten Adressbereiche oder die Adressbereiche basierend auf der Windows-Routingtabelle auswählen (siehe Abbildung 3.10). Markieren Sie im zweiten Fall die gewünschte Netzwerkkarte mit dem ihr zugewiesenen Adressbereich. Klicken Sie dann auf OK.

Abbildung 3.10: Die Auswahl der IP-Adressbereiche für das interne Netzwerk



Sobald Sie die Adressbereiche ausgewählt haben, werden diese in der Liste angezeigt (siehe Abbildung 3.11) und können über ÄNDERN modifiziert werden. Klicken Sie dann auf WEITER.

Abbildung 3.11: Weitere Netzwerke können hinzugefügt oder geändert werden



Abwärtskompatibilität vs. höhere Sicherheit

6. Im Fenster VERBINDUNGSEINSTELLUNGEN FÜR DEN FIREWALLCLIENT (siehe Abbildung 3.12) wird bestimmt, ob Firewallclients älterer Versionen noch eine Verbindung zum ISA Server 2004 herstellen sollen oder nicht.

   Da der ISA Server 2004 eine verschlüsselte Verbindung zwischen Firewallclient und Server herstellt und die älteren Clients diese Funktionalität noch nicht beherrschen, wird die Verschlüsselungsfunktion beim Aktivieren der Checkbox deaktiviert, so dass auch ältere Clients die Verbindung herstellen sollen. Hierdurch gehen Sie jedoch ein gewisses Risiko ein. Um die sichere, verschlüsselte Verbindung nutzen zu können, sollten Sie allen Clients den neuen Firewallclient bereitstellen. Klicken Sie dann auf WEITER.

Abbildung 3.12: Bestimmen Sie, ob frühere Versionen des Firewallclients auf den ISA Server 2004 zugreifen dürfen

7. Das nächste Fenster DIENSTEWARNUNG (siehe Abbildung 3.13) informiert Sie darüber, dass während der Installation des ISA Server einige Dienste neu gestartet und andere deaktiviert werden. Um welche Dienste es sich dabei handelt, ist abhängig von der Konfiguration des Servers, auf dem der ISA Server installiert werden soll. Klicken Sie dann auf WEITER. Im folgenden Fenster wird die Installation über die Schaltfläche INSTALLIEREN gestartet.

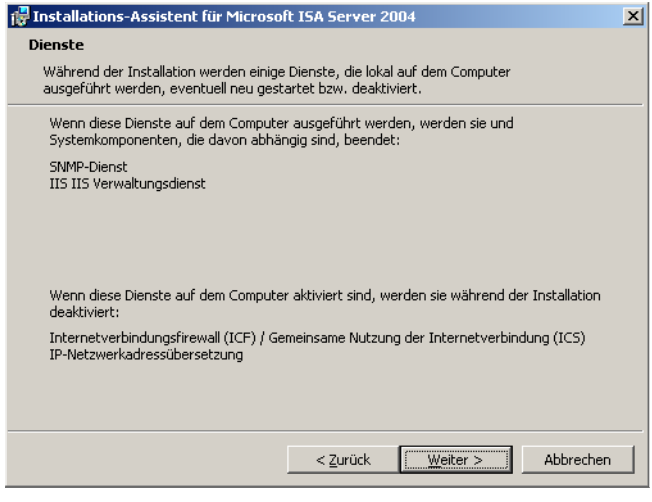


Abbildung 3.13: Informationen über die Dienste, die neu gestartet und deaktiviert werden

8. Sobald die Installation beendet wurde, erhalten Sie das Fenster FERTIGSTELLEN DER INSTALLATION. Klicken Sie hier auf FERTIG STELLEN, um die Installation zu beenden.
9. Nach Abschluss der Installation muss der Computer neu gestartet werden.

3.2.2 Die Installation der Enterprise-Version

Die Installation der Enterprise-Version gleicht prinzipiell der der Standardversion, ist aber aufgrund der größeren Auswahlmöglichkeit der Features wie z.B. des Konfigurationsspeicherservers komplexer. Der vollständige Installationsprozess wird in diesem Kapitel beschrieben.

1. Sobald die CD eingelegt wurde, erhalten Sie das in Abbildung 3.14 dargestellte Fenster. Klicken Sie hier auf ISA SERVER 2004 INSTALLIEREN.

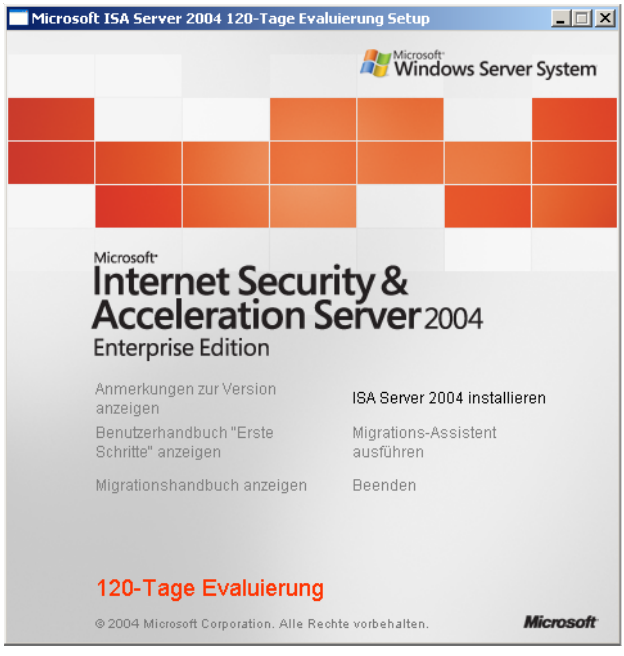


Abbildung 3.14: Die Installation des ISA Server 2004 Enterprise-Version

Um weitere Informationen über den ISA Server zu erhalten, können Sie unter ANMERKUNGEN ZUR VERSION ANZEIGEN oder BENUTZERHANDBUCH ERSTE SCHRITTE ANZEIGEN zusätzliche Hinweise anzeigen lassen.

In einem zusätzlichen Fenster werden Sie über den jeweiligen Installationsstatus informiert. Der Installationsprozess gliedert sich in die drei Vorgänge KERNKOMPONENTEN, ZUSÄTZLICHE KOMPONENTEN sowie SYSTEMINITIALISIERUNG.

2. Im Willkommensfenster der Installation klicken Sie auf WEITER. Als Nächstes müssen Sie in den beiden folgenden Fenstern die Lizenzbedingungen akzeptieren sowie die 25-stellige Produkt-ID eingeben (siehe Abbildung 3.15). Klicken Sie jeweils auf WEITER.

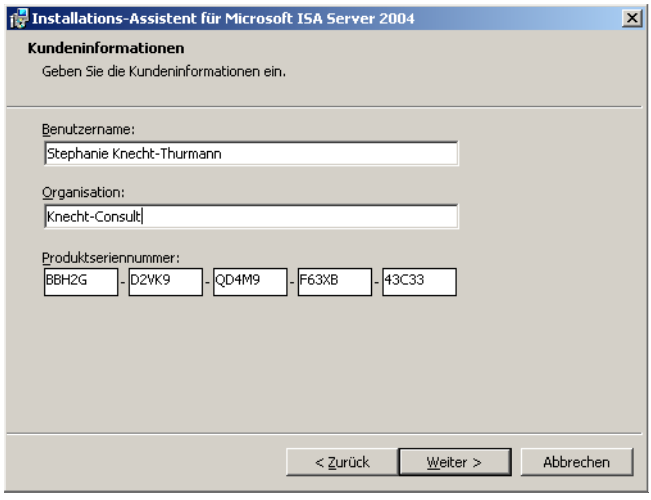


Abbildung 3.15: Eingabe der Benutzerinformationen und der Lizenznummer

3. Im Fenster SETUP-SZENARIEN wählen Sie einen der folgenden vier Punkte (siehe Abbildung 3.16) und klicken dann auf WEITER.

Abbildung 3.16: Auswahl des durchzuführenden Setups

STANDARDAUSWAHL

- ISA SERVER-DIENSTE INSTALLIEREN: Die Installation des ISA Server wird als Arraymitglied durchgeführt.
- KONFIGURATIONSSPEICHERSERVER INSTALLIEREN: Auf dem Computer wird die Konfiguration gespeichert, die die ISA Server-Arrays verwenden. Die ISA Server stellen zum Abrufen dieser Konfiguration eine Verbindung zu diesem Computer her.
- ISA SERVER-DIENSTE UND KONFIGURATIONSSPEICHERSERVER INSTALLIEREN: Der Computer wird sowohl als ISA Server eingerichtet als auch zur Speicherung der Konfiguration genutzt. Diese Option wird hier als Grundlage gewählt.

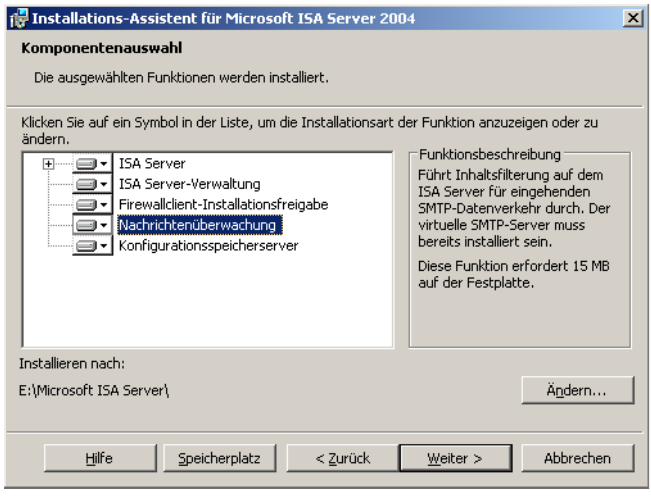
Was ist ein Konfigurationsspeicherserver?

Der Konfigurationsspeicherserver ist nur in der Enterprise-Version des ISA Server 2004 verfügbar. Dieser Speicher wird auf nur einem einzelnen Computer angelegt. In diesem wird die Konfiguration für sämtliche ISA Server-Arrays gespeichert. Jeder ISA Server stellt zum Konfigurationsspeicherserver eine Verbindung her, um von dort die Konfiguration abzurufen.

- ISA SERVER-VERWALTUNG INSTALLIEREN: Über diesen Computer kann die Remote-Verwaltung eines ISA Server durchgeführt werden.

4. Als Nächstes werden im Fenster KOMPONENTENAUSWAHL (siehe Abbildung 3.17) die zu installierenden Komponenten des ISA Server ausgewählt. Die einzelnen Komponenten können entweder lokal installiert werden, eine lokale Installation aller Komponenten ist möglich, oder eine Komponente ist nicht verfügbar. Im rechten Teilbereich FUNKTIONSBESCHREIBUNG erhalten Sie nähere Hinweise zu der jeweiligen Komponente. Über ÄNDERN kann auch das Installationsverzeichnis des ISA Server geändert werden. Das Standardverzeichnis lautet `C:\Programme\Microsoft ISA Server`. Klicken Sie dann auf WEITER.

Abbildung 3.17: Die Auswahl der zu installierenden Komponenten des ISA Server



Für die weiteren Installationsschritte werden hier sämtliche Komponenten ausgewählt. Sind nicht alle Komponenten gewählt, können die folgenden Fenster geringfügig abweichen.

Installationsfreigabe des Firewallclients

Sie sehen, dass Sie die Möglichkeit haben, die Komponente *Installationsfreigabe für Firewallclient* nicht auszuwählen. Unter dem ISA Server 2000 musste sich diese Komponente zwangsläufig auf dem ISA

Server befinden, unter ISA 2004 kann die Komponente auch auf einem beliebigen Dateiserver liegen. Die Freigabe \MSPCLNT ist für die Installation des Clients nicht mehr nötig. Dies liegt darin begründet, dass der ISA Server 2004 in der Lage ist, nur bestimmte Protokolle über seine Netzwerkschnittstelle zum LAN zuzulassen und den Rest zu blockieren, so dass bei einer Sperrung des Dateizugriffs keine Installation des Firewallclients vom ISA Server aus möglich wäre.

Die Komponente *Nachrichtenüberwachung* kann nur installiert werden, wenn auf dem Computer ein virtueller SMTP-Server installiert ist. Ist dies nicht der Fall, erhalten Sie einen entsprechenden Hinweis. Die Installation des SMTP-Servers geschieht über die SERVERVERWALTUNG.

5. Im folgenden Fenster UNTERNEHMENSINSTALLATIONSOPTIONEN (siehe Abbildung 3.18) legen Sie fest, ob ein neues ISA Server-Unternehmen erstellt werden soll oder ein Replikat der Unternehmenskonfiguration.

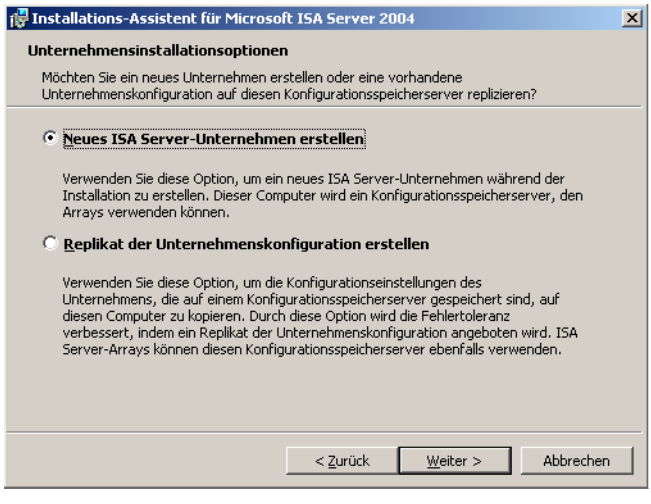


Abbildung 3.18: Erstellen eines neuen ISA-Server-Unternehmens oder Kopieren eines vorhandenen Konfigurationsspeichers als Replikat

Im ersten Fall wird ein neuer, erster ISA Server für das Unternehmen eingerichtet, der auch gleichzeitig als Konfigurationsspeicher dient. Diese Option wird in diesem Beispiel gewählt.

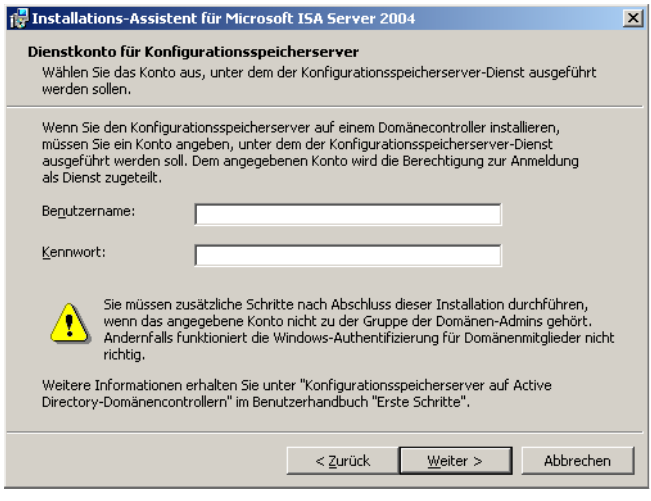
Über die zweite Option wird der Konfigurationsspeicher von einem bereits vorhandenen Computer auf diesen kopiert. Durch diese Replizierung der Konfiguration erhöht sich die Fehlertoleranz. Alle ISA Server-Arrays können automatisch auch auf dieses Replikat zugreifen. Klicken Sie dann auf WEITER.

6. Sie erhalten nach dieser Auswahl das Hinweisfenster NEUES UNTERNEHMEN (siehe Abbildung 3.19), in dem Sie über die Einrichtung des Unternehmens näher informiert werden. Klicken Sie dann auf WEITER.

Abbildung 3.19: Hinweisfenster mit Informationen zur Einrichtung eines neuen Unternehmens

7. Als Nächstes werden das Benutzerkonto und das zugehörige Kennwort für das Dienstkonto des Konfigurationsspeichers festgelegt (siehe Abbildung 3.20). Dieses Konto muss über die Berechtigung zur Anmeldung als Dienst verfügen. Klicken Sie dann auf WEITER.

Abbildung 3.20: Auswahl des Benutzerkontos für das Dienstkonto des Konfigurationsspeicherservers



8. Nun werden im Fenster INTERNES NETZWERK die Adressbereiche bestimmt, die der ISA Server als internes Netzwerk einbeziehen soll. Klicken Sie auf HINZUFÜGEN, um ein Netzwerk zu wählen.

Sie können entweder manuell einen bestimmten BEREICH HINZUFÜGEN, einen ADAPTER HINZUFÜGEN oder einen PRIVATEN ADAPTER mit vordefinierten Adressbereichen auswählen (siehe Abbildung 3.21). Über BEARBEITEN und ENTFERNEN können bestehende Einträge modifiziert werden. Klicken Sie auf OK und im dann erscheinenden Fenster auf WEITER.

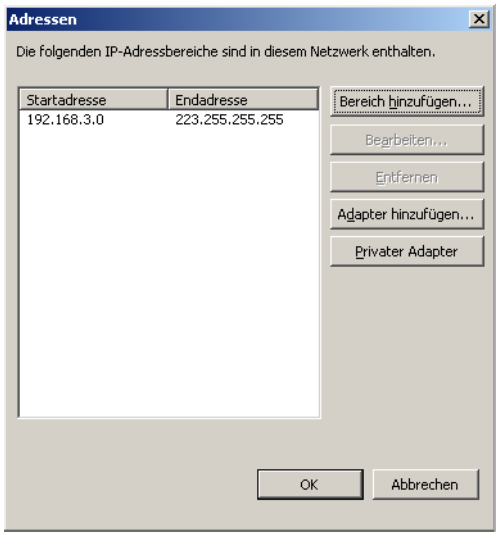


Abbildung 3.21: Die Auswahl der IP-Adressbereiche für das interne Netzwerk

Haben Sie die Option ADAPTER HINZUFÜGEN gewählt, werden alle vorhandenen Netzwerkkarten mit ihrem zugehörigen Adressbereich angezeigt (siehe Abbildung 3.22). Markieren Sie den gewünschten Adapter und klicken auf OK.

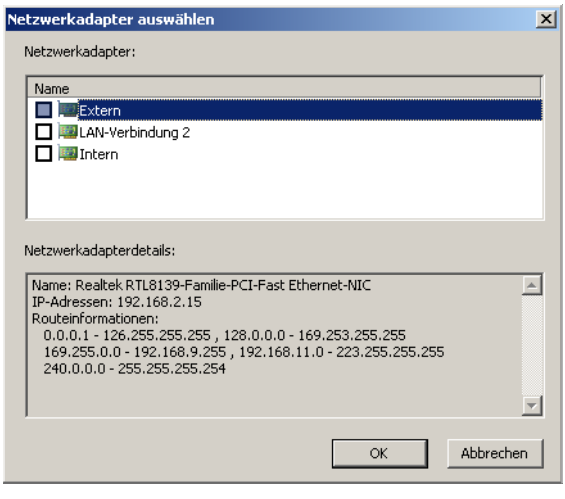
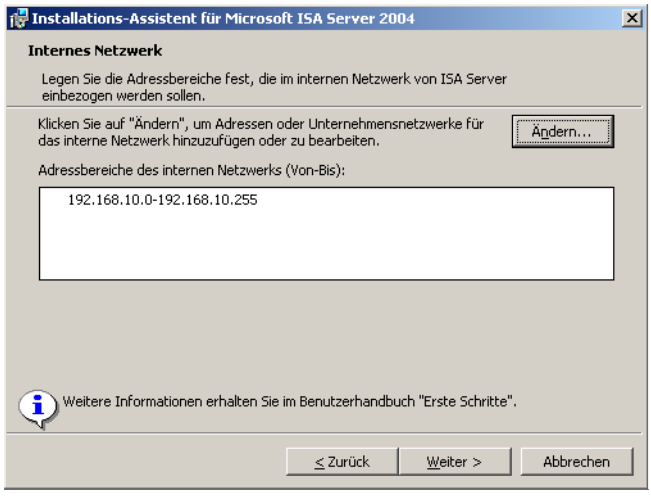


Abbildung 3.22: Die Auswahl eines Netzwerkadapters mit zugehörigem Adressbereich

Haben Sie Ihre Auswahl abgeschlossen, wird das gewählte interne Netzwerk angezeigt (siehe Abbildung 3.23). Über ÄNDERN können noch weitere Netzwerke hinzugefügt werden. Klicken Sie dann auf WEITER.

Abbildung 3.23: Die gewählten internen Netzwerke werden aufgelistet



Abwärtskompatibilität vs. höhere Sicherheit

9. Im Fenster VERBINDUNGSEINSTELLUNGEN FÜR DEN FIREWALLCLIENT (siehe Abbildung 3.24) wird bestimmt, ob Firewallclients älterer Versionen noch eine Verbindung zum ISA Server 2004 herstellen sollen oder nicht. Da der neue Firewallclient des ISA Server 2004 eine verschlüsselte Verbindung benutzt, kann diese nicht verwendet werden, wenn ältere Clients, die noch keine Verschlüsselung kennen, auf den ISA Server 2004 zugreifen. Um die sichere, verschlüsselte Verbindung nutzen zu können, sollten Sie allen Clients den neuen Firewallclient bereitstellen. Klicken Sie dann auf WEITER.

Abbildung 3.24: Bestimmen Sie, ob frühere Versionen des Firewallclients auf den ISA Server 2004 zugreifen dürfen

10. Das nächste Fenster DIENSTEWARNUNG (Abbildung 3.25) informiert Sie darüber, dass während der Installation des ISA Server einige Dienste neu gestartet und andere deaktiviert werden. Um welche Dienste es sich dabei handelt, ist abhängig von der Konfiguration des Servers, auf dem der ISA Server installiert werden soll. Klicken Sie dann auf WEITER. Im folgenden Fenster wird die Installation über die Schaltfläche INSTALLIEREN gestartet.

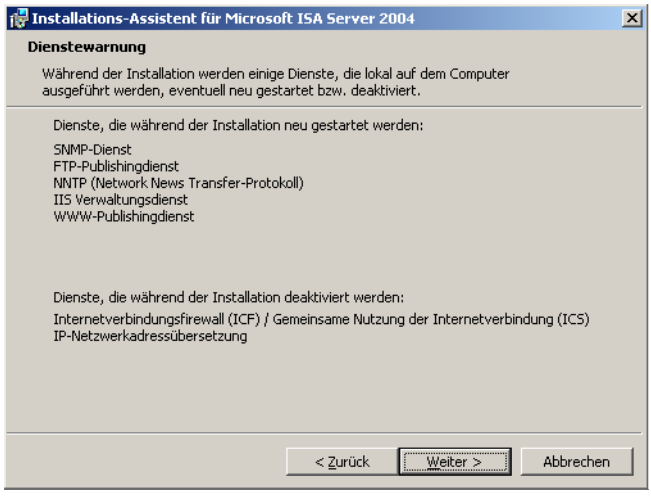


Abbildung 3.25: Informationen über die Dienste, die neu gestartet und deaktiviert werden

11. Sobald die Installation beendet wurde, erhalten Sie das Fenster FERTIGSTELLEN DER INSTALLATION. Klicken Sie hier auf FERTIG STELLEN, um die Installation zu beenden.
12. Nach Abschluss der Installation muss der Computer neu gestartet werden.

3.3 Die unbeaufsichtigte Installation

Wie bei einem Betriebssystem kann auch die Installation des ISA Server unbeaufsichtigt durchgeführt werden. Auch hierbei wird eine Antwortdatei verwendet, in die die Werte zu schreiben sind, die während einer herkömmlichen Installation von Hand in die verschiedenen Eingabefelder geschrieben werden.

Diese Form bietet sich an, wenn mehrere ISA Server möglichst ohne viel Aufwand installiert werden sollen. Auch für die rasche Wiederherstellung, die beispielsweise in einer Testumgebung des Öfteren notwendig werden kann, ist dieses Verfahren gut geeignet. Die unbeaufsichtigte Installation führt hierbei die Basisinstallation durch. Konfigurationseinstellungen wie Regeln und Filter können danach

von einem bereits konfigurierten ISA Server importiert werden. Auch dieser Import kann automatisiert ablaufen.

Für die unbeaufsichtigte Installation besitzt der ISA Server bereits eine Vorlage einer Antwortdatei. Sie finden diese auf der Installations-CD im Verzeichnis `\FPC`. Die Antwortdatei trägt den Namen *msisaund.ini*. Dort sind sämtliche Parameter und deren Bedeutung beschrieben, die in die Datei eingefügt werden können. Für die folgenden Parameter können die gewünschten Werte angegeben werden:

Tabelle 3.3: Die Parameter, die in einer Antwortdatei angegeben werden können

Parameter	Beschreibung
PIDKEY= 12345123451234512345123 45	Installationsschlüssel (25-stellig) des ISA Server
INTERNALNETRANGES= 1 192.168.2.0-192.168.2.255	Bestimmt die IP-Adressen des internen Netzwerks. Es können auch mehrere Bereiche angegeben werden.
SUPPORT_EARLIER_CLIENTS=0/1	Bestimmt, ob auch ältere Firewallclients vom ISA Server unterstützt werden sollen. Mit dem Wert 0 (Standard) gibt es keine Unterstützung, über den Wert 1 wird die Unterstützung aktiviert.
INSTALLDIR=C:\Programme\ Microsoft ISA Server	Gibt das Installationsverzeichnis für den ISA Server an
COMPANYNAME= Firmenname	Gibt den Firmennamen an
DONOTDELLOGS=0/1	Wenn eine unbeaufsichtigte Deinstallation durchgeführt werden soll, gibt der Wert 0 an, dass die ISA-Protokolldateien dabei gelöscht werden, mit dem Wert 1 bleiben sie erhalten.
DONOTDELCACHE=0/1	Gilt ebenfalls nur für die unbeaufsichtigte Deinstallation. Über den Wert 0 wird der ISA-Cache gelöscht, über den Wert 1 bleibt dieser erhalten.

Parameter	Beschreibung
ADDLCAL=All	Beschreibt die zu installierenden Komponenten des ISA Server. Folgende Werte sind möglich: ▶ All = Alle Komponenten ▶ MSFirewall_Services = Dienste des ISA Server ▶ MSDE = Microsoft Desktop Engine für die Protokollierung ▶ Publish_Share_Directory = Freigabe für den Firewallclient ▶ Message_Screener = E-Mail-Nachrichtenfilter
REMOVE=All	Für eine unbeaufsichtigte Deinstallation werden die zu entfernenden Komponenten angegeben.
IMPORT_CONFIG_FILE=Pfad\Konfigurationsdatei.xml	Nach der unbeaufsichtigten Installation wird eine *.xml*-Datei mit der weiteren Konfiguration (z.B. Richtlinien usw.) des ISA Server importiert.

Um mit der Datei arbeiten zu können, muss diese zuvor auf einen beschreibbaren Datenträger kopiert werden. In Abbildung 3.26 sehen Sie ein Beispiel für eine Antwortdatei.

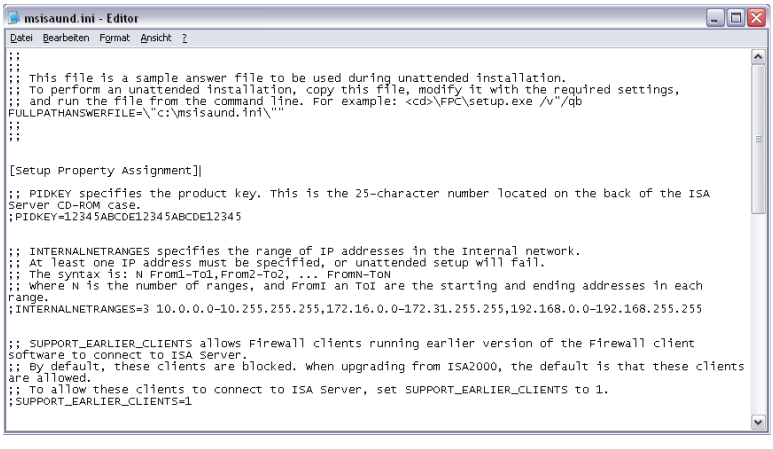


Abbildung 3.26: Beispiel einer Antwortdatei für die unbeaufsichtigte Installation

Sobald diese Datei fertig gestellt ist, wird die unbeaufsichtigte Installation über den folgenden Befehl an der Eingabeaufforderung gestartet:

```
CD-Laufwerk\FPC\Setup.exe [/[X|R]] /V“ /Q[b|n]
FULLPATHANSWERFILE=\“Pfad zur Antwortdatei\““ ↵
```

Die Parameter der Befehlszeile haben folgende Bedeutung:

Tabelle 3.4: Parameter für die Befehlszeile der unbeaufsichtigten Installation

Parameter	Beschreibung
`[/[X|R]]`	Optionaler Parameter. Ohne dessen Angabe erfolgt eine herkömmliche unbeaufsichtigte Installation, über X eine Deinstallation und über R eine Neuinstallation.
`/V`	Die Installationsschritte werden ausführlich protokolliert (Verbose Logging).
`/Q[b|n]`	/Q steht für quiet, also eine Installation im Hintergrund, bei der die einzelnen Fenster nicht angezeigt werden. Die zusätzliche Option b bestimmt, dass das Dialogfenster, das den Abschluss der Installation verkündet, angezeigt wird, mit n wird dieses Fenster nicht angezeigt. Ist die Option nicht gesetzt, werden zwar die in der Antwortdatei angegebenen Werte übernommen, allerdings muss jeder einzelne Installationsschritt bestätigt werden.

Der erforderliche Neustart nach Abschluss der Installation wird automatisch durchgeführt.

3.4 Installation des Service Pack 1 für die Standardversion

Begleit-CD

Ab Februar 2005 ist das Service Pack 1 für den ISA Server 2004 Standard verfügbar. Dieses sollten Sie auf jeden Fall direkt nach der Installation des Servers ebenfalls installieren. Für die Installation des Service Pack sollte auf dem ISA Server 2004 der Windows Installer in der Version 3.0 vorhanden sein. Sie finden diesen auf der Begleit-CD. Führen Sie vor Beginn der Installation eine Sicherung des Systems durch.

Das Service Pack 1 für den ISA Server 2004 Standard darf lediglich auf der Standard-Version, *keinesfalls* jedoch auf der Enterprise-Version installiert werden.

Um das Service Pack installieren zu können, muss auf dem ISA Server der Windows Installer in mindestens der Version 3.0 installiert sein. Sie finden diese Version ebenfalls auf der Begleit-CD. Bevor Sie mit der Installation des Service Pack beginnen, müssen alle Anwendungen beendet sein, die auf die Daten zugreifen. Anderenfalls erhalten Sie während der Installation einen entsprechenden Hinweis, um dann die Applikation zu beenden (siehe Abbildung 3.27).

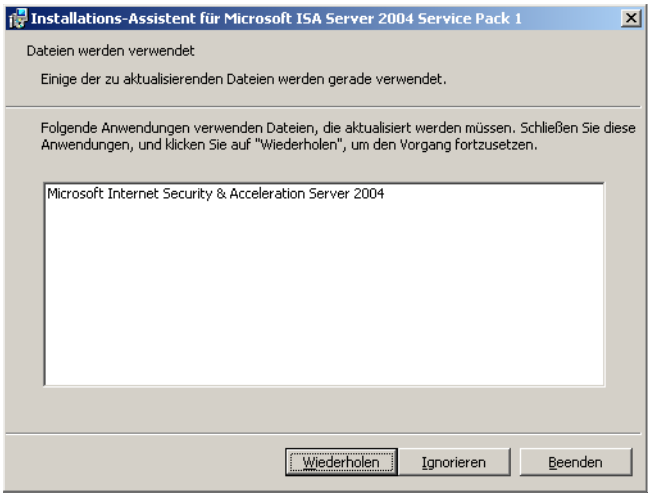


Abbildung 3.27: Zur Installation des Service Pack müssen alle Anwendungen beendet sein, die auf die ISA-Daten zugreifen

Nach der Installation des Service Pack muss das System neu gestartet werden.

Nachdem das Service Pack installiert worden ist, müssen die Firewallclients aktualisiert werden. Hierzu starten Sie das Skript *Update.bat*. Dieses Skript befindet sich in der Freigabe für den Firewallclient (standardmäßig in \CLIENTS\WEBINST auf dem ISA Server).

Windows Server 2000

Wird das Service Pack 1 für den ISA Server 2004 auf einem Windows Server 2000 in einer unbeaufsichtigten Installation installiert, findet sich in dem Ereignisprotokoll möglicherweise die Ereignis-ID 3009. Diese bezieht sich lediglich auf die Leistungsindikatoren und kann ignoriert werden. Es handelt sich dabei um keine Fehlermeldung.

3.4.1 Enthaltene Hotfixes und Patches

Im Service Pack 1 sind verschiedene Hotfixes enthalten, die bestimmte Probleme unter dem ISA Server 2004 beheben. Tabelle 3.5 gibt eine Übersicht über die enthaltenen Hotfixes und deren Funktion.

Tabelle 3.5: Die im Service Pack 1 enthaltenen Hotfixes und deren Funktionen

Hotfix	Beschreibung
884569	Auf einem Multiprozessor-Computer können die Dienste *ISACTRL* sowie *WSPSRV* nicht gestartet werden.
884560	Wird für eine Webveröffentlichungsregel die formbasierte Authentifizierung von OWA (Outlook Web Access) verwendet, kann RADIUS nicht verwendet werden.
884580	Es ist kein Zugriff durch FTP-Clients auf einen FTP-Server möglich, wenn vor diesen ein ISA Server 2004 geschaltet ist.

Hotfix	Beschreibung
888422	Bei Anmeldeinformationen, die einen Umlaut beinhalten, schlägt der *CookieAuthFilter* fehl.
891510	Eine Überprüfung der Zertifikatssperrliste durch die Webveröffentlichungsregel schlägt fehl, wenn das Root-Zertifikat nicht über eine Erweiterung für Sperrlisten-Verteilungspunkte verfügt.
885683	Die Fehlermeldung *401 Nicht autorisiert* wird angezeigt, wenn mit dem ISA 2004-Firewallclient auf eine Website zugegriffen wird.
893171	Probleme unter Windows 98 mit dem ISA 2004-Firewallclient

Weitere Hinweise zu den einzelnen Hotfixes finden Sie unter der entsprechenden Nummer in der Microsoft Knowledgebase im Internet.

3.4.2 Protokollierung der Service Pack-Installation

Manueller Aufruf der Protokollierung

Bei der Installation eines Service Pack wird, wie auch bei der Installation anderer Hotfixes, kein Installationsprotokoll angelegt. Lediglich in der Ereignisanzeige finden sich Hinweise, wenn es bei der Installation zu Problemen gekommen ist. Da eine detailliertere Aufzeichnung der Probleme in einem Protokoll für die Fehlersuche und –behebung aber sehr hilfreich sein kann, kann die Protokollierung der Installation über einen entsprechenden Befehl an der Kommandozeile aktiviert werden. Verwenden Sie dazu den folgenden Befehl:

```
Msiexec /p Name.msp REINSTALL=ALL REINSTALLMODE=omus /
l*vx! Protokolldatei.log ↵
```

Die einzelnen Parameter in dieser Befehlskette haben die folgenden Bedeutungen:

Tabelle 3.6: Bedeutung der Parameter für die Befehlszeile zum Aktivieren der Protokollierung

Parameter	Beschreibung
`Msiexec /p`	Ruft den Windows Installer auf und zeigt an, dass eine Updateinstallation ausgeführt werden soll
`Name.msp`	Gibt den Namen und den Pfad der Service-Pack-Datei an.
`REINSTALL=ALL`	Alle bereits installierten Funktionen sollen erneut installiert werden.
`REINSTALLMODE`	Die Parameter von REINSTALLMODE beschreiben den Modus der erneuten Installation.
`O`	Fehlende Dateien sowie Dateien mit einer älteren Version werden erneut installiert.

Parameter	Beschreibung
M	Einträge in den Registry-Schlüsseln HKEY_LOCAL_MACHINE sowie HKEY_CLASSES_ROOT werden erneut geschrieben.
U	Einträge in den Registry-Schlüsseln HKEY_CURRENT_USER sowie HKEY_USERS werden erneut geschrieben.
S	Alle Verknüpfungen und Symbole werden erneut installiert.
/l	Schaltet den Protokollierungsmodus ein.
*vx	Dieser Parameter bestimmt die Ausführlichkeit der Protokollierung.
Protokoll-datei.log	Gibt den Namen der Protokolldatei an. Standardmäßig befindet sich diese in demselben Ordner wie das Programm *msiexec.exe*.

3.4.3 Hinweise zur Service Pack-Deinstallation

Das Service Pack 1 kann zu einem späteren Zeitpunkt wieder deinstalliert werden, auch wenn sich über den Sinn dieser Aktion streiten lässt. Für die Deinstallation sind die folgenden Punkte zu bedenken:

- Es muss Zugriff auf Quelldateien des Service Pack bestehen, also auf die CD oder eine Netzwerkfreigabe, von der aus die Installation durchgeführt wurde.
- Vor der Deinstallation sollte der ISA Server physikalisch vom Netzwerk getrennt werden, da der Paketfiltertreiber (*fweng*) zur Anwendung der Firewall-Richtlinien während des Deinstallationsvorgangs angehalten werden kann.

Trennung vom Netzwerk!

- Der Dienst ROUTING UND RAS ist zu deaktivieren.

3.5 Prüfen der ISA Server-Installation

Nachdem die Installation des ISA Server 2004 und gegebenenfalls für die Standardversion auch des Service Pack 1 abgeschlossen ist, sollten Sie prüfen, ob dabei auch alles korrekt abgelaufen ist. Um mögliche Fehler zu erkennen, sollten Sie die Ereignisanzeige und die Protokollierung beachten.

Finden sich in der Ereignisanzeige Hinweise auf Probleme, so müssen diese in jedem Fall behoben werden, bevor der ISA Server weiter eingesetzt wird. Ansonsten werden diese Fehler mit an Sicherheit grenzender Wahrscheinlichkeit im laufenden Betrieb Probleme verursachen.

3.5.1 Installationsprotokolle

Während der Installation werden drei verschiedene Installationsprotokolle erstellt. Sie befinden sich im Verzeichnis `\Windows\Temp`. Die Protokolle enthalten Informationen zu erfolgreichen und fehlerhaften Installationsvorgängen.

- *ISAFWSV_xxx.log*: Details zur Installation des ISA Server
- *ISAMSDE_xxx.log*: Details zur Installation der MSDE
- *ISAWRAP_xxx.log*: Installationszusammenfassung

3.5.2 Installierte Ordnerstruktur

Ebenfalls sollten Sie einen Blick auf den Installationsordner des ISA Server und dessen Struktur werfen. Abbildung 3.28 zeigt die Datei- und Ordnerstruktur eines ISA Server in der Standardversion.

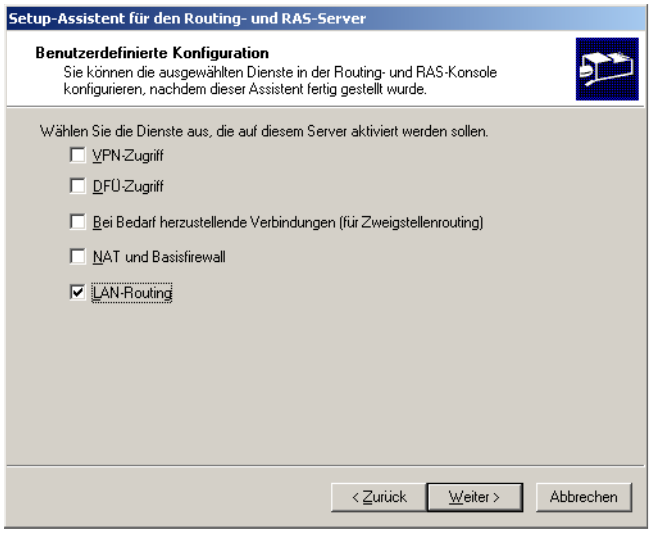


Abbildung 3.28: Die Ordnerstruktur des ISA Server nach der Installation

3.5.3 Dienste des ISA Server

Durch die Installation des ISA Server werden auch verschiedene Dienste zum System hinzugefügt. Bei einem ISA Server der Standardversion müssen die folgenden Dienste vorhanden sein:

- Microsoft ISA Server-Auftragsplanung
- Microsoft ISA Server-Speicher
- Microsoft ISA Server-Steuerung
- Microsoft Firewall

Sämtliche Dienste besitzen den Starttyp AUTOMATISCH. Die beiden Dienste MICROSOFT FIREWALL und MICROSOFT ISA SERVER-SPEICHER werden unter dem Konto NETZWERKDIENST gestartet, die beiden anderen unter dem Konto LOKALES SYSTEM.

Wurde auch die Komponente ERWEITERTE PROTOKOLLIERUNG gewählt, müssen zusätzlich die drei folgenden Dienste vorhanden sein:

- MSSQL$MSFW
- MSSQLServerADHelper
- SQLAgent$MSFW

Bei der Installation des ISA Server in der Enterprise-Version ist zusätzlich der Dienst ISASTGCTRL vorhanden. Die Abkürzung steht für ISA Storage Control. Dieser Dienst ist für die Steuerung des Konfigurationsspeicherservers zuständig.

3.5.4 Startmenüeinträge

In das Startmenü werden zwei Einträge geschrieben. Dabei handelt es sich um die Verknüpfungen zu den Verwaltungsinstrumenten ISA SERVER-LEISTUNGSMONITOR und ISA SERVER-VERWALTUNG. Der Leistungsmonitor des ISA Server ist ein um ISA-spezifische Leistungsindikatoren erweiterter Leistungsmonitor des Windows Server. Die ISA SERVER-VERWALTUNG ist das zentrale Werkzeug für alle Einstellungen rund um den ISA Server.

3.5.5 Ports überprüfen

Portscanner einsetzen

Als Letztes sollte noch geprüft werden, ob die Filterfunktion des ISA Server in der Grundeinstellung korrekt funktioniert. Standardmäßig werden in dieser Einstellung sämtliche eingehenden Pakete für alle Schnittstellen blockiert. Um dies zu testen, sollten Sie mit einem beliebigen Portscanner von einem anderen Computer aus die Kommunikationsfähigkeit des ISA Server überprüfen. Diese Prüfung sollte ergeben, dass der ISA Server auf der externen Schnittstelle keine Anfragen sendet und annimmt.

3.6 Weitere Schritte

Nach Abschluss der Installation und deren Prüfung steht der Konfiguration und dem Einsatz des ISA Server theoretisch nichts mehr im Wege. Dennoch sollten die folgenden Schritte durchgeführt werden.

3.6.1 Routenkonfiguration

Nur bei weiteren Netzwerken erforderlich

Die folgend beschriebenen Schritte müssen nur durchgeführt werden, wenn sich im internen Netzwerk weitere Netzwerke befinden, die über keine direkte Verbindung zum ISA Server verfügen. Anderenfalls sind diese Schritte nicht notwendig.

Um die ISA Server-Informationen sämtlichen Segmenten des Netzwerks bereitzustellen, muss die Routing-Tabelle des ISA Server bearbeitet werden. Mit Hilfe derer Informationen stellt der ISA Server fest, welches Paket an welches Netzwerksegment geschickt werden soll. Routen können statisch und dynamisch festgelegt werden.

Statisches Routing über route.exe

Um Routen festzulegen, wird das Kommandozeilenprogramm *route.exe* verwendet. Dabei ist folgende Syntax anzuwenden:

```
Route.exe add Segment mask Subnetzmaske Gateway -p ↵
```

Die Parameter haben folgende Bedeutungen. Weitere Informationen erhalten Sie über den Aufruf von `route.exe /?` ↵ .

Tabelle 3.7: Parameter für das Kommandozeilenprogramm route.exe

Parameter	Beschreibung
`Add`	Über diesen Parameter wird eine neue Route hinzugefügt.
`Segment`	Netzwerksegment, über das der ISA Server informiert werden soll.
`Mask`	Parameter zur Angabe der Subnetzmaske
`Subnetzmaske`	Subnetzmaske im angegebenen Netzwerksegment
`Gateway`	Adresse des Gateway, über das der ISA Server die Pakete in das Netzwerksegment senden soll.
`-p`	-p steht für persistent. Dies bedeutet, dass der hinzugefügte Eintrag in der Routing-Tabelle auch nach einem Neustart des ISA Server noch vorhanden ist.

Um die hinzugefügten Routen zu prüfen, lassen Sie sich diese über den Befehl `route.exe print` ↵ auf dem Bildschirm anzeigen.

Statisches Routing über die mmc Routing und RAS

Bevorzugen Sie zum Hinzufügen neuer Routen anstelle der Kommandozeile die graphische Oberfläche, so verwenden Sie dazu die mmc ROUTING UND RAS. Zuvor müssen Sie den Dienst ROUTING UND RAS aktivieren, sofern dieses nicht bereits geschehen ist.

Die mmc ROUTING UND RAS wird über die Verwaltung aufgerufen. Um den Dienst zu aktivieren, wählen Sie aus dem Kontextmenü des Servernamens den Eintrag ROUTING UND RAS KONFIGURIEREN UND AKTIVIEREN. Im Assistenten wählen Sie im Fenster KONFIGURATION die Option BENUTZERDEFINIERTE KONFIGURATION. Im folgenden Fenster wird nur der Punkt LAN-ROUTING markiert (siehe Abbildung 3.29). Danach wird der Dienst installiert und gestartet.

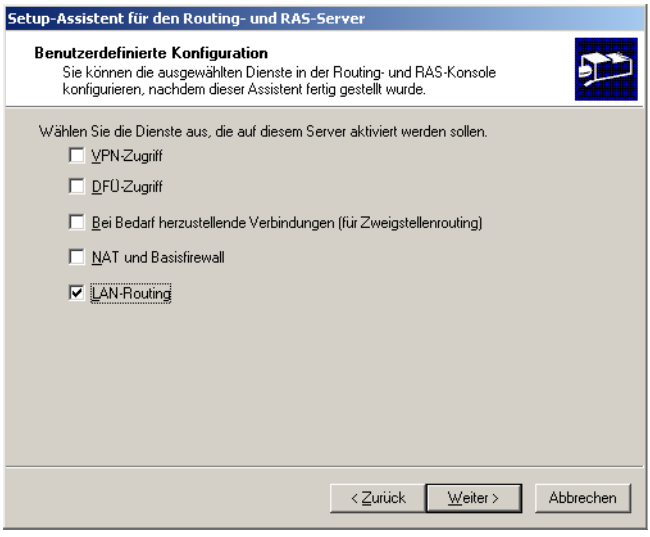


Abbildung 3.29: Auswahl des Dienstes LAN-Routing für Routing und RAS

Um eine neue statische Route hinzuzufügen, wählen Sie in der mmc aus dem Kontextmenü von STATISCHE ROUTEN den Eintrag NEUE STATISCHE ROUTE. Als SCHNITTSTELLE muss die Verbindung zum internen Netzwerk angegeben werden (siehe Abbildung 3.30). Unter METRIK muss nur dann der Wert geändert werden, wenn mehrere Routen zu dem Netzwerk laufen. Dies könnte aus Gründen der Fehlertoleranz der Fall sein. Sollen mehrere Routen zu einem Netzwerk erstellt werden, geben Sie der Route mit der höchsten Priorität den Wert 1 und den übrigen höhere Werte. Bestätigen Sie Ihre Eingaben mit OK.

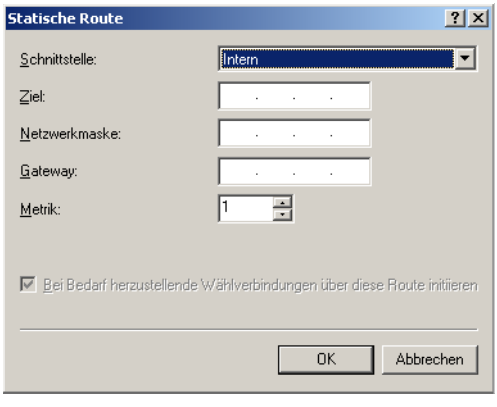


Abbildung 3.30: Die Definition der neuen statischen Route

Dynamisches Routing

Kein Konfigurations- und Pflegeaufwand

Welche der beiden eben beschriebenen Methoden Sie auch zum Erstellen der Routen verwenden, Sie sehen, dass die Konfiguration mit ein wenig Aufwand verbunden ist. Sofern sich die Topologie des Netzwerks ändert, müssen jedes Mal die Routen wieder entspre-

chend angepasst werden. Um diesen Pflegeaufwand zu unterbinden, kann auch dynamisches Routing verwendet werden.

Dabei werden spezielle Routing-Protokolle wie RIP oder OSFP verwendet. Beim dynamischen Routing stellen die einzelnen Router des internen Netzwerks die Informationen ihrer Routing-Tabellen auch den anderen Routern bereit. Dadurch sind den Routern die Routen zu allen Netzwerken bekannt.

3.6.2 Aktualisierung durch Updates

Um sowohl den ISA Server als auch den zugrunde liegenden Windows Server immer auf dem aktuellen Stand zu halten, müssen dort regelmäßig alle verfügbaren Service Pack, Updates, Patches und Hotfixes installiert werden.

Ob auf dem System alle aktuellen Patches vorhanden sind, können Sie über das Windows Update prüfen (*http://windowsupdate.microsoft.com*). Ein automatisches Update zu festen Zeiten oder auch der Einsatz von *Windows Server Update Services* (*WSUS*) zur Verteilung der Updates an Clients und Server im Netzwerk ist hier anzuraten.

Fehlende Updates für den ISA Server 2004 finden Sie unter dem Link *http://www.microsoft.com/germany/isaserver/default.mspx* unter DOWNLOADS.

4 Migration eines ISA Server 2000

Dieses Kapitel beschäftigt sich mit den zwei verschiedenen Möglichkeiten, die es für die Migration eines ISA Server 2000 auf die Version 2004 gibt. So kann entweder ein *direktes Update* von ISA 2000 auf 2004 durchgeführt werden. Bei dieser Aktualisierung wird kein weiterer Server benötigt. Allerdings kann diese Methode ein gewisses Risiko darstellen, da der wesentlich komplexere ISA Server 2004 möglicherweise nicht alle Einstellungen der Vorgängerversion übernehmen kann.

Wahl zwischen zwei Verfahren

Die in dieser Hinsicht sichere, aber auch aufwändigere Methode ist das *Exportieren* und folgende *Importieren* der ISA-Konfiguration. Für dieses Verfahren werden zwei physikalische Server benötigt: der ISA Server 2000, von dem die Einstellungen exportiert werden, und der ISA Server 2004, auf dem die Konfiguration wieder importiert wird. Diese beiden Verfahren werden in den folgenden Kapiteln näher vorgestellt.

Besondere Hinweise werden für die Migration eines ISA Server 2000 auf ISA Server 2004 Enterprise gegeben.

4.1 Importieren und Exportieren der Konfiguration

Wie bereits erwähnt, ist der Export und Import der ISA-Konfiguration die aufwändigere Methode als das direkte Update. Allerdings treten bei diesem Verfahren auch weniger Probleme auf. Im Zuge dieser Migration wird die ISA-Konfiguration in eine XML-Datei geschrieben. Diese XML-Datei wird vom ISA Server 2000 auf den ISA Server 2004 übertragen.

Beachten Sie, dass für das Erstellen der XML-Datei auf dem ISA Server 2000 das Service Pack 1 installiert sein muss.

4.1.1 Exportieren der ISA Server 2000-Konfiguration

Migrationsassistent

Um mit der Migration zu beginnen, klicken Sie entweder nach dem Autostart der ISA Server 2004-CD auf den Link MIGRATIONS-ASSISTENT AUSFÜHREN oder starten direkt von der CD aus dem Verzeichnis \TOOLS das Programm *ISA2KEXPORT.EXE*.

1. Im Willkommenfenster (siehe Abbildung 4.1) werden Sie über die anstehenden Aufgaben informiert. Sie erhalten auch einen Hinweis, dass nicht alle Einstellungen des ISA Server 2000 exportiert werden können. Klicken Sie hier auf WEITER.

Abbildung 4.1: Der Migrationsassistent wird gestartet

2. Im Fenster DATEIPFAD (siehe Abbildung 4.2) geben Sie den Pfad der Exportdatei an. Als Dateiname wird der Name *ISA2KExport.xml* automatisch gesetzt, dieser kann jedoch geändert werden. Um diese Datei auf dem ISA Server 2004 importieren zu können, muss der ISA Server 2004 auf den Speicherort zugreifen können. Klicken Sie dann auf WEITER.

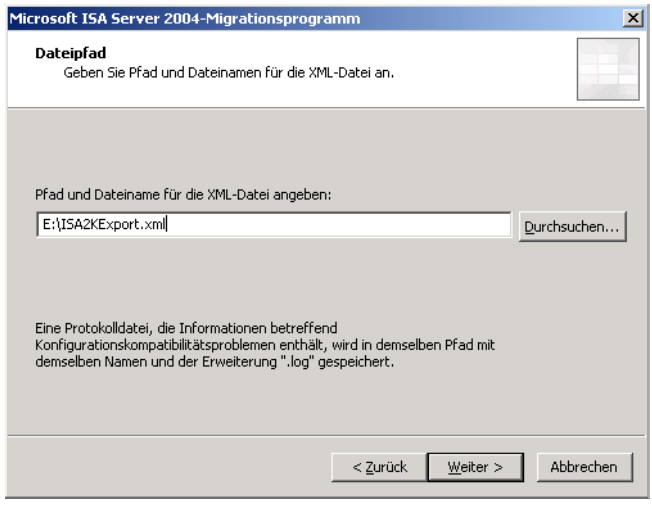


Abbildung 4.2: Auswahl des Speicherorts für die Exportdatei

3. Der Export-Assistent fragt im Fenster AUSWÄHLEN DER STANDARDFIREWALLRICHTLINIE, ob die Clients des internen Netzwerks auf den ISA Server 2004 zugreifen dürfen oder nicht (siehe Abbildung 4.3). Bei der Wahl der ersten Option ist der Zugriff nur möglich, wenn entsprechende Firewallregeln auf dem ISA Server 2004 erstellt werden. Anderenfalls können Remote-Anwendungen gesperrt werden. Die zweite Option gewährt den Zugriff auf den ISA Server 2004. Sie spiegelt das Standardverhalten unter ISA Server 2000 wieder. Klicken Sie dann auf WEITER.

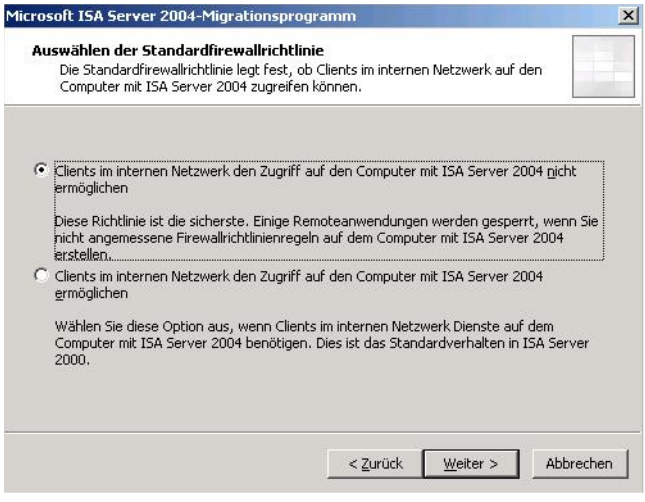


Abbildung 4.3: Festlegen, ob interne Clients auf den ISA Server zugreifen dürfen oder nicht

4. Im folgenden Fenster MIGRATIONSDATEI ERSTELLEN (siehe Abbildung 4.4) klicken Sie auf ERSTELLEN, um die Datei anzulegen. Im unteren Bereich des Fensters werden Sie über den Status der Erstellung informiert. Klicken Sie dann auf WEITER.

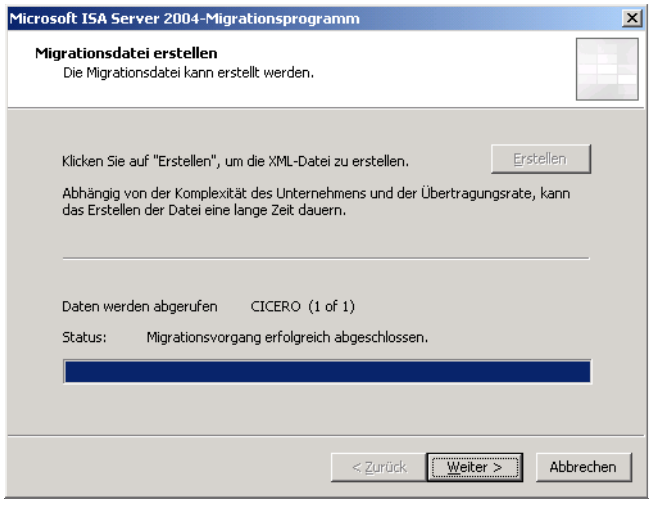
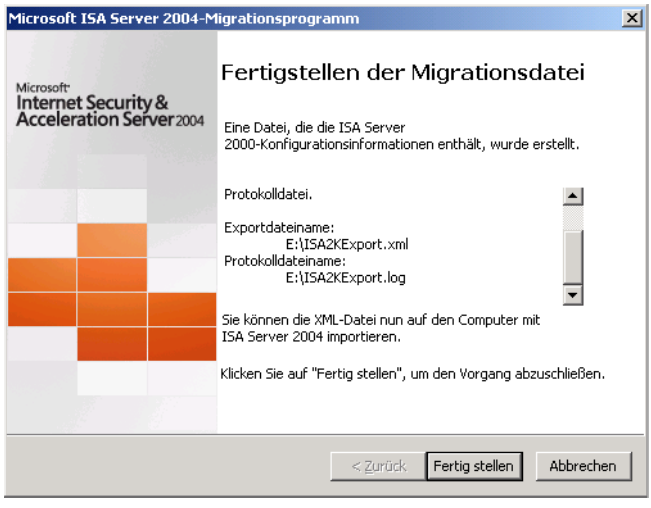


Abbildung 4.4: Die Migrationsdatei wird erstellt und der aktuelle Status angezeigt

5. Im Verzeichnis der Exportdatei befindet sich auch die Protokolldatei des Exports (*ISA2KExport.log*, siehe Abbildung 4.5). Prüfen Sie diese auf Fehlermeldungen hin, bevor Sie mit dem Import der Datei auf einem ISA Server 2004 beginnen. Klicken Sie dann auf FERTIG STELLEN.

Abbildung 4.5: Die Migrationsdatei ist fertig gestellt



4.1.2 Importieren der XML-Datei auf dem ISA Server 2004

Die eben erstellte Exportdatei wird verwendet, wenn der ISA Server 2000 auf die Version 2004 aktualisiert wird. Die Datei ist beim direkten Update anzugeben. Dabei werden die Informationen des ISA Server 2000 auf ISA Server 2004 übertragen. Weitere Hinweise finden Sie in Kapitel 4.2.

4.1.3 Einstellungen, die unter ISA Server 2004 nicht beibehalten werden

Wenig genutzte Funktionen wurden entfernt

Mit Hilfe der Export-/Importfunktion werden nahezu sämtliche Einstellungen auf das neue System übertragen. Lediglich einige Einstellungen, die z.B. unter ISA 2004 nicht mehr verfügbar sind, werden nicht übernommen. Dazu zählen:

- *H.323-Gatekeeper*. Dieser wird unter ISA Server 2004 nicht mehr unterstützt und wurde deshalb entfernt. Der H.323-Gatekeeper war für die Steuerung und das Routing von Voice over IP-Anrufen (VoIP) zuständig. Allerdings kam es immer wieder zu Problemen mit diesem Dienst, wenn inkorrekte Pakete an diesen gerichtet wurden. Diese Probleme waren zwar mit Service Pack für ISA Server 2000 behoben, aber dennoch konnte sich der Gatekeeper auch

nur schwer durchsetzen, da seine Konfiguration in vielen Fällen erhebliche Schwierigkeiten bereitete. Mit der weiteren Verbreitung von VoIP wurde vermehrt das SIP-Protokoll (Session Initiation Protocol) anstelle von H.323 verwendet. Da sich dieses immer mehr zum Standard entwickelt, wird der H.323-Gatekeeper vom ISA Server 2004 nicht mehr unterstützt.

- *Bandbreitenkontrolle*. Auch die Regeln zur Bandbreitenkontrolle werden nicht mehr unterstützt und sind deshalb entfernt worden. Es war unter ISA Server 2000 möglich, über eine Bandbreitenregel in Kilobyte einen festen Wert für die Bandbreite zu bestimmen. Darüber konnte beispielsweise die Priorität für Verbindungen eingestellt werden. Genutzt wurde diese Funktion vom QoS-Dienst (Quality of Service). Allerdings wurde von diesem Feature vielfach erwartet, dass darüber einzustellen sei, wieviel an Bandbreite maximal für eine bestimmte Verbindung zulässig sei. In vielen Fällen führte dies zu einer Misskonfiguration des Systems, die nicht selten die Neuinstallation des ISA Server 2000 notwendig machte.
- *Active Caching*. Im Gegensatz zum ISA Server 2004 unterstützte der ISA Server 2000 auch das Active Caching (zusätzlich zu den immer noch verfügbaren Methoden Forward/Reverse-Caching sowie hierarchisches und verteiltes Caching. Beim Active Caching wurden die im Zwischenspeicher befindlichen Objekte automatisch vom Quellserver aktualisiert, bevor ein Objekt des Cache nicht mehr gültig war. Über eine Richtlinie konnte festgelegt werden, wie häufig die Updates der zwischengespeicherten Objekte erfolgen sollten. Da hierbei auch nicht unwesentlich Bandbreite erforderlich war, gab es häufiger Probleme. Unter ISA Server 2004 kann das Active Caching optional aktiviert und in seiner Häufigkeit konfiguriert werden.
- *Protokoll- sowie Reporteinstellungen.* Diese können nicht aktualisiert werden.
- *Einstellungen an Berechtigungen*. SACLs z.B. können nicht aktualisiert werden.

4.1.4 Übersicht über direkt migrierte und veränderte Komponenten

Teilweise Konfigurationsumstellungen

Neben den eben beschriebenen Komponenten, die unter ISA Server 2004 nicht mehr unterstützt werden, sind einige Komponenten des ISA Server 2000 nun unter einem anderen Namen vorhanden, während andere Konfigurationsobjekte unverändert migriert werden. Die nachfolgende Tabelle gibt nähere Anhaltspunkte dazu.

Tabelle 4.1: Übersicht über ISA Server 2000-Komponenten, die unter anderem Namen oder unverändert bereitstehen

Komponente des ISA Server 2000	Komponente des ISA Server 2004
Webveröffentlichungregeln	Werden unverändert migriert
Serververöffentlichungsregeln	Werden unverändert migriert
Inhaltsgruppen	Werden unverändert migriert
Zielsätze	Migration in Computersätze, URL-Sätze oder Domänennamensätze
Clientadresssätze	Werden als Computersätze migriert
Weblistener	Werden unverändert migriert
Site- und Inhaltsregeln	Diese Regeln werden als Zugriffsregeln migriert. Einige dieser Regeln werden auch zusammen mit Protokollregeln als Zugriffsregeln migriert.
Protokollregeln	Auch diese Regeln werden als Zugriffsregeln migriert. Einige der Protokollregeln werden auch zusammen mit Site- und Inhaltsregeln zu einer einzigen Zugriffsregel zusammengefasst.
Routing-Regeln	Die Routingregeln werden als Cache- und Routing-Regeln migriert.
Anwendungsfilter und -regeln	Die Komponenten werden nur teilweise migriert, da ein Teil dieser Filter und Regeln unter ISA Server 2004 in anderer Form vorkommt.
Paketfilter	Die unter ISA Server 2000 vordefinierten Paketfilter werden in die Systemrichtlinie migriert, die übrigen als Zugriffsregeln.
Alarmkonfiguration	Alle Alarmkonfigurationen werden übernommen. Mit dem Webproxy-Dienst verknüpfte Alarme werden mit dem Firewall-Dienst verknüpft, da der Webproxy-Dienst nicht mehr vorhanden ist.
Cachekonfiguration	Nahezu alle Einstellungen werden migriert.
Zeitpläne	Werden unverändert migriert
ACLs der ISA-Objekte	ACLs können nicht migriert werden. Die ISA-Objekte erhalten die Standardberechtigungen des ISA Server 2004.
Firewallverkettung	Wird unverändert migriert

Komponente des ISA Server 2000	Komponente des ISA Server 2004
DFÜ-Verbindungen	Die DFÜ-Verbindung wird in der Form migriert, dass die Inhalte dem externen Netzwerk hinzugefügt werden.
Lokale Adresstabelle (LAT)	Wird in der Form migriert, dass die Inhalte dem internen Netzwerk hinzugefügt werden
Lokale Domänentabelle (LDT)	Wird in der Form migriert, dass die Inhalte dem internen Netzwerk hinzugefügt werden

4.1.5 Hinweise für den Import und Export nach der Installation von Service Pack 1

Einschränkungen im Import und Export

Nach der Installation des Service Pack 1 sind die beiden folgenden Punkte für den Import und Export zu bedenken:

- Vertrauliche Informationen können nicht mehr von einem ISA Server 2004 Standard mit Service Pack 1 auf einen ISA Server 2004 Standard ohne Service Pack 1 exportiert und oder von dort importiert werden.
- Vertrauliche Informationen können nicht mehr aus einem ISA Server 2004 Standard mit Service Pack 1 an einen ISA Server 2004 Enterprise importiert werden. Sie erhalten in diesem Fall den Hinweis, dass das Kennwort falsch ist, obwohl dieses korrekt eingegeben worden ist.

4.2 Das direkte Update

Update auf demselben Computer

Im Gegensatz zu der bereits bestehenden Methode des Imports und Exports wird beim direkten Update die Aktualisierung des ISA Server auf demselben Computer durchgeführt. Im Zuge des Update wird ebenfalls die Konfiguration des ISA Server 2000 exportiert, der Import erfolgt jedoch auf denselben Computer.

Vor dem Update müssen die folgenden Punkte erfüllt sein:

- Für den ISA Server 2000 muss mindestens das Service Pack 1 installiert sein.
- Die Standardversion des ISA Server 2000 kann nur auf die Standardversion des ISA Server 2004 aktualisiert werden. Ebenfalls kann die Aktualisierung auf die ISA Server 2004 Enterprise-Version nur von der ISA Server 2000 Enterprise-Version aus vorgenommen werden.

Anwendungsfilter-Kompatibilität klären

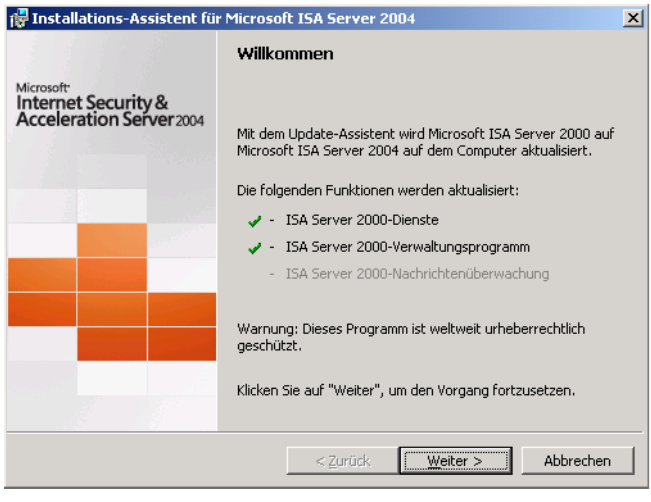
- Sofern Sie Webfilter oder Anwendungsfilter von Drittanbietern verwenden, müssen diese vor Beginn des Updates deinstalliert werden. Diese Filter sind nicht mit ISA Server 2004 kompatibel und müssen nach der Aktualisierung durch eine neuere Version ersetzt werden, sofern die Hersteller eine Version für ISA Server 2004 anbieten.

Um das direkte Update durchzuführen, sind folgende Schritte erforderlich:

Eine vollständige Sicherung des Systems sowie der ISA-Komponenten vor Beginn des Updates sollte eigentlich eine Selbstverständlichkeit sein.

1. Legen Sie die ISA Server 2004-CD ein und klicken Sie auf den Link ISA SERVER 2004 INSTALLIEREN. Von der Installationsroutine wird dabei automatisch erkannt, dass bereits ein ISA Server 2000 vorhanden ist und es sich nicht um eine Neuinstallation handelt (siehe Abbildung 4.6). Klicken Sie auf WEITER.

Abbildung 4.6: Bei der Installation werden vorhandene ISA Server 2000-Komponenten automatisch erkannt



2. Sie müssen dann dem Lizenzvertrag zustimmen und die Lizenznummer des ISA Server 2004 angeben. Zusätzlich ist das Installationsverzeichnis für ISA 2004 anzugeben. Klicken Sie jeweils auf WEITER.
3. Im nächsten Fenster MICROSOFT ISA 2000 SERVER-KONFIGURATION EXPORTIEREN klicken Sie auf EXPORTIEREN, um die Einstellungen des ISA Server 2000 zu sichern (siehe Abbildung 4.7).

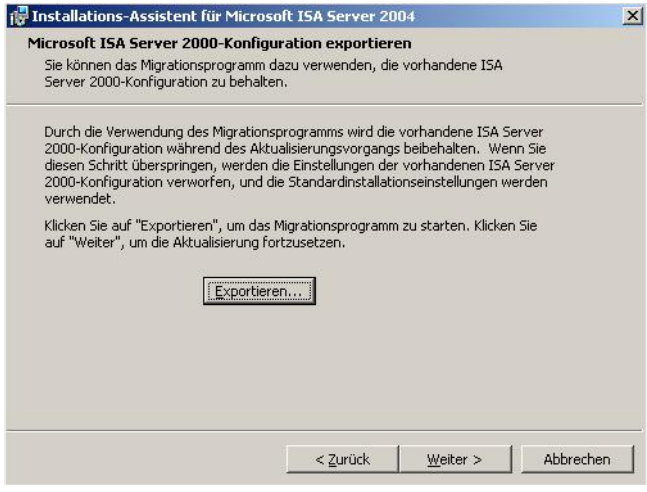


Abbildung 4.7: Exportieren der ISA Server 2000-Konfiguration

4. Der Export-Assistent fragt im Fenster AUSWÄHLEN DER STANDARDFIREWALLRICHTLINIE (siehe Abbildung 4.8), ob die Clients des internen Netzwerks auf den ISA Server 2004 zugreifen dürfen oder nicht. Bei der Wahl der ersten Option CLIENTS IM INTERNEN NETZWERK DEN ZUGRIFF AUF DEN COMPUTER MIT ISA SERVER 2004 NICHT ERMÖGLICHEN ist der Zugriff nur möglich, wenn entsprechende Firewallregeln auf dem ISA Server 2004 erstellt werden. Anderenfalls können Remote-Anwendungen gesperrt werden. Diese Methode ist sicherer als die zweite. Die zweite Option CLIENTS IM INTERNEN NETZWERK DEN ZUGRIFF AUF DEN COMPUTER MIT ISA SERVER 2004 ERMÖGLICHEN gewährt den Zugriff auf den ISA Server 2004. Sie spiegelt das Standardverhalten unter ISA Server 2000 wider. Klicken Sie dann auf WEITER.

Abbildung 4.8: Festlegen, ob interne Clients auf den ISA Server zugreifen dürfen

5. Um die Exportdatei zu erstellen, klicken Sie im Fenster MIGRATIONSDATEI ERSTELLEN auf die gleichnamige Schaltfläche. Sie werden über den Status des Exports informiert. Klicken Sie dann auf WEITER.
6. Im Fenster VON ISA SERVER 2000 GENERIERTE DATEIEN (siehe Abbildung 4.9) werden Sie darüber informiert, dass während des Updates sämtliche Protokolldaten sowie gecachten Dateien des ISA Server 2000 gelöscht werden. Klicken Sie dann auf WEITER.

Abbildung 4.9: Informationen zu den vom ISA Server 2000 generierten Dateien

Sollen diese Daten auch nach der Aktualisierung wieder genutzt werden, müssen diese vor Beginn der Aktualisierung in einen anderen Ordner kopiert werden.

Eigentliche Installation des ISA Server 2004

7. Im letzten Fenster PROGRAMM KANN JETZT INSTALLIERT WERDEN klicken Sie auf INSTALLIEREN (siehe Abbildung 4.10). Bei der Aktualisierung wird zunächst der ISA Server 2004 installiert. Diese Installation unterscheidet sich nicht von einer Neuinstallation des ISA Server 2004. Danach erfolgt die Aktualiserung selbst. Dazu wird auf die Exportdatei aus Schritt 5 zurückgegriffen, über die die Konfigurationseinstellungen des ISA Server 2000 auf das neue System übernommen werden. Nach Abschluß des Updates muss das System neu gestartet werden. Der ISA Server 2004 ist nun funktionstüchtig.

Da während der Aktualisierung zunächst der ISA Server 2000 deinstalliert wird, ist für diesen Zeitraum kein Schutz des Netzwerks gewährleistet. Aus Sicherheitsgründen sollte deshalb die externe Verbindung des ISA Server unterbrochen werden. Nach Abschluss des Updates kann die Verbindung wiederhergestellt werden.

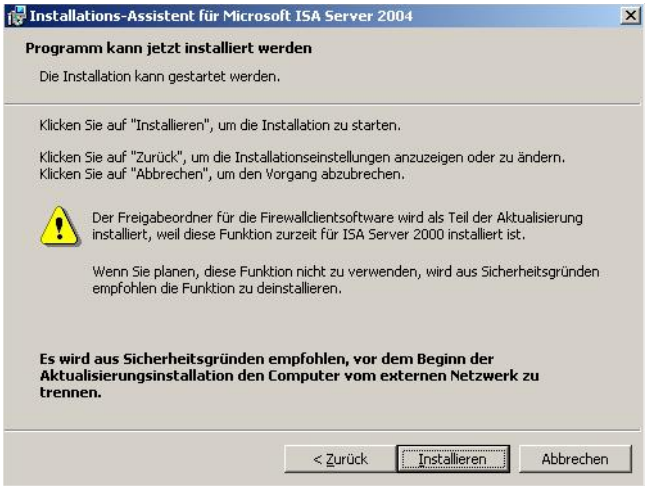


Abbildung 4.10: Die eigentliche Installation des ISA Server 2004 kann gestartet werden

4.3 Migration auf ISA Server 2004 Enterprise

Unterschiede je nach zu installierenden Komponenten

Für die Migration des ISA Server 2000 auf ISA Server 2004 Enterprise sind einige Besonderheiten zu bedenken. Die einzelnen Schritte unterscheiden sich danach, welche Komponenten des ISA Server 2004 Enterprise installiert werden sollen. Der ISA Server 2000 kann in folgender Weise aktualisiert werden:

- Upgrade auf einen reinen ISA Server
- Upgrade auf einen Konfigurationsspeicherserver
- Upgrade von ISA Server-Routing und Remotezugriff
- Upgrade von Add-Ons

4.3.1 Voraussetzungen

Damit ein Upgrade auf ISA Server 2004 durchgeführt werden kann, müssen die folgenden Punkte erfüllt sein:

- Das Upgrade kann nur vom ISA Server 2000 Enterprise, nicht aber von der Standardversion aus vorgenommen werden.
- Der ISA Server 2000 und 2004 müssen dieselbe Sprachversion besitzen.
- Auf dem ISA Server 2000 muss Service Pack 1 oder 2 installiert sein.

- Wenn das Upgrade auf einem anderen Computer vorgenommen wird, sollten vor dem Import der XML-Konfigurationsdatei alle notwendigen Zertifikate installiert sein.
- Ist der ISA Server 2000 unter Windows Server 2000 installiert, muss unbedingt Service Pack 1 oder 2 für den ISA Server installiert sein. Beim Einsatz des Service Pack 1 muss zusätzlich auch das Hotfix des Artikel KB331062 installiert sein. Erst danach kann das Betriebssystem auf Windows Server 2003 aktualisiert werden.

Der entsprechende Knowledgebase-Artikel sowie das Hotfix finden Sie auf der Begleit-CD im Ordner PATCHES UND FIXES.

4.3.2 Upgrade eines ISA Server 2000-Arrays

Bei einem Upgrade eines ISA Server 2000-Arrays sind die folgenden Schritte erforderlich:

1. Erstellen Sie einen ISA Server 2004 Konfigurationsspeicherserver. Der Computer, auf dem dieser Server erstellt wird, sollte nicht zu dem ursprünglichen ISA Server 2000-Array gehören.
2. Danach werden die Mitglieder des ISA Server 2000-Arrays auf ISA Server 2004 aktualisiert.

Zusätzlicher Server im Array

Soll dauerhaft kein zusätzlicher Computer zum ISA Server 2004-Array hinzugefügt werden, auf dem sich der Konfigurationsspeicherserver befindet, führen Sie die folgenden Schritte aus:

1. Installieren Sie auf einem ISA Server 2004 die Komponente *Konfigurationsspeicherserver*. Stellen Sie sicher, dass dabei die Option EIN REPLIKAT ERSTELLEN gewählt ist.
2. Verbinden Sie jedes Mitglied des ISA Server 2004-Arrays mit dem Server des Konfigurationsspeicherservers.
3. Deinstallieren Sie die Komponente des Konfigurationsspeicherservers wieder von dem Computer, der ursprünglich nicht zum ISA Server 2000-Array gehört hat.

4.3.3 Upgrade eines allein stehenden ISA Server 2000

Zusätzlicher Computer erforderlich

Der Upgrade-Prozess eines allein stehenden ISA Server 2000 ähnelt dem Upgrade-Vorgang des ISA Server 2000-Arrays. Sie benötigen auch in diesem Fall einen zusätzlichen Server, auf dem die Komponente *Konfigurationsspeicherserver* installiert werden kann.

4.3.4 Upgrade eines ISA Server 2004 Standard

Um einen ISA Server 2004 Standard auf ISA Server 2004 Enterprise upzugraden, müssen Sie die folgenden Schritte durchführen:

1. Exportieren Sie die Konfiguration des ISA Server 2004 in der Standardversion.
2. Installieren Sie die Komponente *Konfigurationsspeicherserver* des ISA Server 2004 Enterprise.
3. Installieren Sie ein Array-Mitglied. Dies kann entweder auf dem Konfigurationsspeicherserver oder einem separaten Computer geschehen.
4. Importieren Sie die in Schritt 1 erstellte Konfigurationsdatei in das in Schritt 3 erstellte Array.
5. Installieren Sie zusätzliche Mitglieder des ISA Server 2004-Arrays. Zum Zeitpunkt des Imports der Konfigurationsdatei darf sich erst ein Mitglied im Array befinden.

4.3.5 Upgrade auf einen Computer, der die ISA Server-Dienste ausführt

Da die einzelnen Komponenten des ISA Server 2004 Enterprise auf unterschiedlichen Computern installiert werden können, unterscheidet sich der Upgrade-Vorgang danach, welche Komponente installiert werden soll.

Prüfen der Regeln

Werden die Dienste des ISA Server installiert, wird ein einfaches Update des ISA Server 2000 vorgenommen. Der Update-Prozess wird automatisch ausgeführt. Allerdings müssen danach die verschiedenen Regeln nochmals analysiert werden, da diese möglicherweise nicht korrekt oder optimal aktualisiert werden.

4.3.6 Upgrade auf einen Konfigurationsspeicherserver

Um von ISA Server 2000 auf den Konfigurationsspeicherserver des ISA Server 2004 Enterprise zu aktualisieren, müssen Sie die folgenden Schritte ausführen:

1. Führen Sie auf dem ISA Server 2000 den Migrationsassistenten aus, um eine XML-Datei mit den Konfigurationsinformationen erstellen zu lassen.
2. Bei der Installation des ISA Server 2004 Enterprise wählen Sie die Installation der Komponente *Konfigurationsspeicherserver*.
3. Führen Sie ein Backup des ISA Server 2004 und seiner aktuellen Einstellungen durch und importieren Sie die XML-Datei dort.

4.3.7 Upgrade des ISA Server 2000-Routing und Remote-Zugriff

Beim Upgrade des Routing und Remote-Zugriffs des ISA Server 2000 gibt es die folgenden Einschränkungen:

- Die maximale Anzahl der Remote-VPN-Clients, die sich mit dem ISA Server 2004 verbinden können, wird auf den Wert gesetzt, der größer ist: entweder die Anzahl der PPTP-Ports oder die Anzahl der L2TP-Ports.
- Ist die Anzahl der statisch zugewiesenen IP-Adressen geringer als die Anzahl der VPN-Clients, wird die Anzahl der VPN-Clients auf die Anzahl der statisch zugewiesenen IP-Adressen begrenzt. Der Benutzer erhält während des Upgrade-Prozesses eine entsprechende Warnmeldung.
- Der statische Adresspool wird nicht migriert.
- Preshared Schlüssel für Routing und Remote-Zugriff werden nicht exportiert. Es wird ebenfalls eine Warnmeldung angezeigt.
- Ist für den primären DNS-Server eine ungültige IP-Adresse gesetzt, wird diese nicht exportiert. Stattdessen werden die DHCP-Einstellungen verwendet. Sie erhalten ebenfalls eine Warnmeldung. Ist die IP-Adresse des sekundären DNS-Servers ungültig, so wird diese ebenfalls nicht exportiert und Sie erhalten eine Warnmeldung. Dasselbe gilt auch, wenn eine ungültige IP-Adresse für den primären oder sekundären WINS Server gesetzt ist.
- Ist eine Standort-zu-Standort-Verbindung unter Routing und Remotezugriff zuerst als PPTP eingerichtet (danach als L2TP), erfolgt die Aktualisierung auf dem ISA Server 2004 nur für die Benutzung von PPTP. Es wird eine entsprechende Warnmeldung ausgegeben.
- Ist eine Standort-zu-Standort-Verbindung unter Routing und Remotezugriff zuerst als L2TP eingerichtet (danach als PPTP), erfolgt die Aktualisierung auf dem ISA Server 2004 nur für die Benutzung von L2TP. Es wird eine entsprechende Warnmeldung ausgegeben.
- Preshared Schlüssel für Standort-zu-Standort-Verbindungen unter Routing und Remote-Zugriff werden nicht exportiert, Sie erhalten einen entsprechenden Hinweis.
- Für Standort-zu-Standort-Verbindungen hinterlegte Anmeldeinformationen werden nicht exportiert. Auf dem ISA Server 2004 bleiben die ausgehenden VPN-Verbindungen solange deaktiviert, bis die Anmeldeinformationen erneut konfiguriert wurden. Es wird ebenfalls eine Warnmeldung ausgegeben.
- Die Konfigurationseinstellungen der XML-Datei können nur in ein leeres Array des ISA Server 2004 Enterprise importiert werden.

4.3.8 Upgrade der Add-Ons

Drittanbieter-Filter unter ISA 2004 nicht kompatibel

Wurden unter ISA Server 2000 Applikationsfilter und Web-Filter von Drittanbietern verwendet, sind diese nicht mit ISA Server 2004 kompatibel. Finden Sie zunächst heraus, ob der Hersteller aktualisierte Filter anbietet. Ist dies der Fall, sind die folgenden Schritte erforderlich; werden keine aktualisierten Filter angeboten, kann die entsprechende Funktion des alten Filters nicht mehr genutzt werden.

1. Deinstallieren Sie die Drittanbieter-Filter vom ISA Server 2000.
2. Führen Sie das Upgrade auf ISA Server 2004 durch.
3. Installieren Sie die neuen Versionen der Drittanbieter-Filter.

4.3.9 Upgrade des Message Screener

Das Upgrade des Message Screener (Nachrichtenüberwachung) wird durchgeführt, indem Sie ein direktes Upgrade des ISA Server 2000 durchführen.

5 Die Clients des ISA Server

In diesem Kapitel werden die vom ISA Server 2004 unterstützten Client-Typen beschrieben. Dabei handelt es sich um den Firewallclient, den SecureNAT-Client sowie den Webproxy-Client. Jeder Client kann mehrere Typen von ISA-Clients besitzen. So ist es möglich, dass gleichzeitig ein Firewall-Client und ein SecureNAT-Client verwendet werden. Neben der Konfiguration der verschiedenen Clients wird auch auf verschiedene Möglichkeiten zur Installation des Firewallclients eingegangen.

5.1 Der Firewallclient

Installation des Clients auf den lokalen Computern

Ein Firewallclient ist jeder Clientcomputer, auf dem eine vom ISA Server verwendete Winsock-Anwendung ausgeführt wird. Diese Winsock-Anwendung wird bei der Installation des Firewallclients konfiguriert. Diese kann auch von anderen Anwendungen genutzt werden. Der Firewallclient entscheidet dann, ob der Aufruf einer Anwendung an den ISA Server weitergeleitet werden muss oder nicht. Nur wenn der Aufruf an einen Computer desselben Netzwerks wie der Client erfolgt, erfolgt eine direkte Kommunikation, ohne dass der ISA Server daran beteiligt wird. Beim Aufruf einer externen Quelle wird die entsprechende Anfrage an den Firewall-Dienst des ISA Server weitergeleitet. Aufgrund von Zugriffsregeln und Filtern wird von diesem entschieden, ob die Verbindung zum externen Computer zugelassen wird oder nicht.

5.1.1 Clientunterstützung

Port 1745

Die Unterstützung des Firewallclients kann für jedes ISA-Netzwerk aktiviert oder deaktiviert werden. Ist die Unterstützung aktiviert, werden eingehende Anforderungen über den Port 1745 verarbeitet.

Sobald von einem Firewallclient über Winsock von einem Computer ein Objekt angefordert wird, wird vom Client geprüft, ob es sich um einen lokalen Computer handelt oder nicht. Als lokaler Computer werden alle Computer mit IP-Adressen eingestuft, die sich im Adressbereich des Netzwerks befinden. Handelt es sich um keine lokale Adresse des aufzurufenden Computers, wird die Anforderung weiter an den Firewallclient gesendet. Je nach konfigurierter Firewallrichtlinie erfolgt nach der Verarbeitung eine Weiterleitung an das gewünschte Ziel.

Winsock steht als Abkürzung für Windows Socket. Winsock ist eine Windows-API, über die Windows-basierten Programmen die Kommunikation mit anderen Computern über das TCP/IP-Protokoll möglich gemacht wird. Ein Firewallclient fängt die Winsock-Aufrufe ab, so dass z.B. ICMP-Protokolle oder genauer gesagt alle Protokolle der unteren Netzwerkschichten nicht berücksichtigt werden können. Ist ein Computer nur als Firewallclient eingerichtet, ist es nicht mehr möglich, dass dieser z.B. Ping-Aufrufe an externe Geräte senden kann.

Über den Firewallclient können an den ISA Server Benutzerinformationen zur Authentifizierung gesendet werden. Dies gilt für die Protokolle http, https sowie ftp.

Breite Betriebssystemunterstützung

Der Firewallclient, dessen Software sich auf der Installations-CD des ISA Server 2004 befindet, kann auf Computern der folgenden 32-Bit-Betriebssysteme installiert werden:

- Windows Server 2003
- Windows XP
- Windows 2000 Server und Professional
- Windows NT 4.0 Workstation und Server
- Windows ME
- Windows 98SE (Installation des Internet Explorer in mindestens der Version 5 oder höher erforderlich)

Die Installation des Firewallclients darf jedoch *nicht* auf dem ISA Server selbst durchgeführt werden. Eine Installation ist jedoch auf Computern möglich, auf denen lediglich die Verwaltungstools des ISA Server installiert sind.

Anstelle des Firewallclients des ISA Server 2004 können Sie auch die Client-Software des ISA Server 2000 verwenden. Eine Kommunikation ist jedoch nur möglich, wenn Sie während der Installation die Kommunikation zwischen ISA Server 2004 und älteren Firewallclients zugelassen haben.

Abwärtskompatibilität vs. Sicherheit

Die Verwendung der alten Version sollten Sie überdenken, da diese noch keine verschlüsselte Verbindung zwischen Clients und ISA Server unterstützt. Entscheiden Sie selbst, ob Ihnen eine erhöhte Sicherheit oder der Aufwand für die Firewallclient-Konfiguration der neuen Version wichtiger ist.

Sobald der Firewallclient installiert ist, erfolgt dessen Aktivierung automatisch. Die Konfiguration des Clients geschieht ausschließlich auf dem ISA Server und nicht auf Seiten des Clients. Der Client überprüft in regelmäßigen Intervallen, ob für ihn auf dem ISA Server Konfigurationsänderungen vorgenommen worden sind.

Beliebige Installationsfreigabe

Im Gegensatz zu früheren Versionen muss sich die Installationssource für den Firewallclient nicht mehr in der Freigabe /MSPCLNT des ISA Server befinden. Die Installationssource kann auch auf einem anderen Server bereitgestellt werden.

Bei der Einrichtung der Installationsfreigabe des Firewallclients wird standardmäßig die Systemrichtlinie FIREWALLCLIENT/FIREWALL-CLIENTINSTALLATION aktiviert (siehe Abbildung 5.1). Erst dadurch können die Clients zur Installation auf die Freigabe zugreifen.

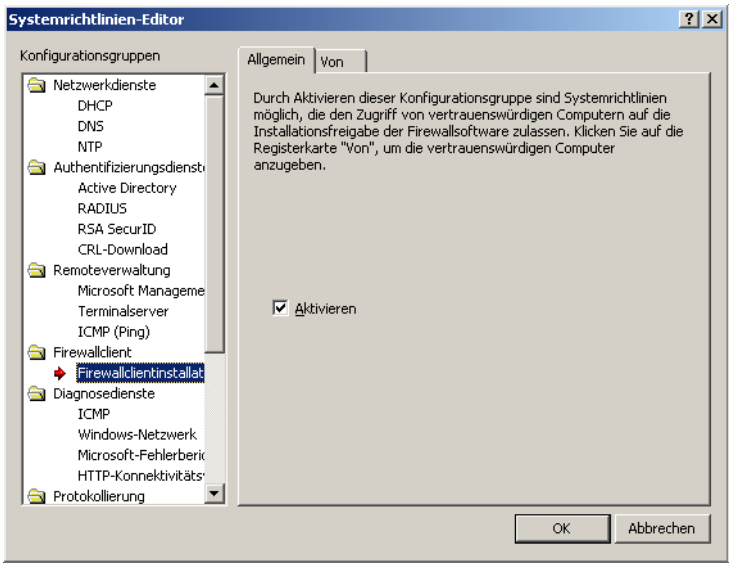


Abbildung 5.1: Die Systemrichtlinie für den Zugriff auf die Installationsfreigabe wird standardmäßig aktiviert

5.1.2 Serverunterstützung

Serverseitig erfolgt die Konfiguration des Clients über KONFIGURATION/NETZWERKE in der ISA-mmc. Wählen Sie dann den Kontextmenüeintrag EIGENSCHAFTEN des Objekts INTERN unter NETZWERKE und wechseln Sie auf die Registerkarte FIREWALLCLIENT (siehe Abbildung 5.2). Zusätzlich können Sie die Checkbox AUTOMATISCHES KONFIGURATIONSSKRIPT VERWENDEN markieren, um dann eine *.ins*-Datei zur Einstellungskonfiguration anzugeben, die mit dem *IEAK (Internet Explorer Administration Kit)* erstellt wurde.

Das *IEAK* finden Sie auf der Begleit-CD. Weitere Informationen zum Erstellen und Verwenden von *.ins*-Dateien sind in der Online-Hilfe des *IEAK* nachzulesen. Weitere Informationen zum IEAK finden Sie auch im Internet unter dem Link *http://www.microsoft.com/technet/prodtechnol/ie/ieak/default.mspx*.

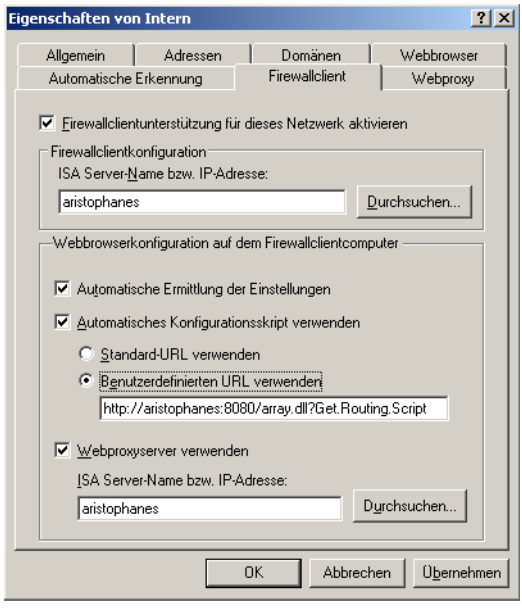


Abbildung 5.2: Die serverseitige Konfiguration für den Firewallclient

Automatische Erkennung

Damit der ISA Server die Informationen veröffentlicht, wechseln Sie auf die Registerkarte AUTOMATISCHE ERKENNUNG, markieren dort die Checkbox INFORMATIONEN FÜR DIE AUTOMATISCHE ERKENNUNG VERÖFFENTLICHEN und tragen den Port ein, der für die Veröffentlichung dieser Informationen genutzt werden soll (siehe Abbildung 5.3).

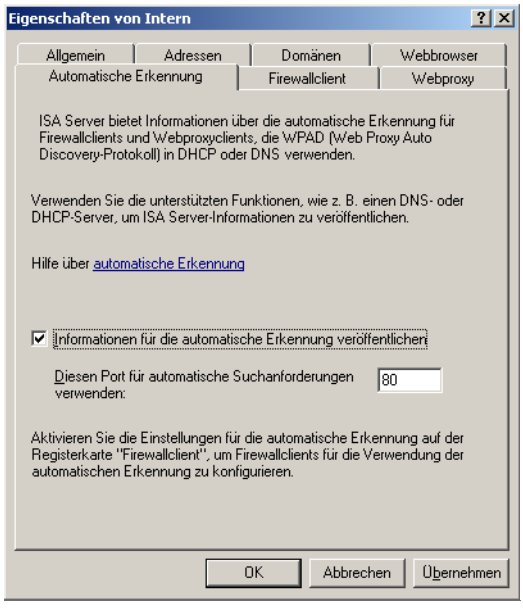


Abbildung 5.3: Der ISA Server kann die Informationen für die automatische Erkennung veröffentlichen

5.2 Installation des Firewallclients

Zur Installation des Firewallclients gibt es drei verschiedene Methoden:

- Manuelle Installation
- Installation über die Softwareverteilung in den Gruppenrichtlinien des Active Directory
- Skriptbasierte, unbeaufsichtigte Installation

Diese drei Verfahren werden im Folgenden näher vorgestellt.

5.2.1 Manuelle Installation

Auswahl der Installationsfreigabe

Vor der manuellen Installation sollten Sie zunächst im Netzwerk einen Computer für eine Freigabe wählen, von der aus die Installation durchgeführt werden kann. Diese Freigabe muss (und sollte) sich nicht auf dem ISA Server befinden. Nachdem der freigegebene Ordner erstellt wurde, führen Sie die folgenden Schritte aus:

1. Um die Installationsfreigabe zu erstellen, legen Sie die ISA Server-CD ein und klicken auf ISA SERVER 2004 INSTALLIEREN.
2. Stimmen Sie dem Lizenzvertrag zu und geben Sie den Benutzer- und Firmennamen sowie die Lizenznummer ein.
3. Wählen Sie dann die BENUTZERDEFINIERTE INSTALLATION und selektieren nur die Komponente INSTALLATIONSFREIGABE FÜR FIREWALLCLIENT. Schließen Sie dann den Installationsassistenten ab.
4. Im Installationsverzeichnis des ISA Server befindet sich der Ordner \CLIENTS. Dieser Ordner ist automatisch als Freigabe eingerichtet worden.

Installation

Bei der manuellen Installation auf dem Client wird die Datei *setup.exe* aus der Installationsfreigabe des Firewallclients oder der Installations-CD des ISA Server aus dem Verzeichnis \CLIENTS aufgerufen.

1. Um den Firewallclient zu installieren, stellen Sie zunächst vom Client aus eine Verbindung zur Installationsfreigabe her. Starten Sie die Installation über die Datei *MS_FWC.msi*.
2. Ein Assistent führt Sie durch die Installation. Nach dem Willkommensbild müssen Sie entscheiden, ob der ISA Server von den Clients automatisch ermittelt oder manuell angegeben werden soll (siehe Abbildung 5.4). Tragen Sie im zweiten Fall die IP-Adresse oder den Hostnamen des Servers ein und klicken Sie auf WEITER.
3. Haben Sie die Option ENTSPRECHENDEN ISA SERVER-COMPUTER AUTOMATISCH ERMITTELN gewählt, sind für die Ermittlung weitere Schritte erforderlich. Lesen Sie dazu das folgende Kapitel. Ansonsten ist die Konfiguration der manuellen Installation abgeschlossen.

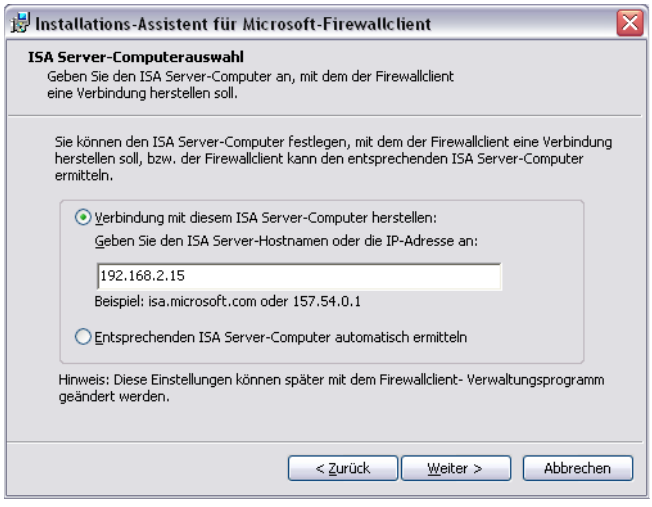


Abbildung 5.4: Angabe des ISA Server oder dessen automatische Ermittlung

5.2.2 Automatische Suche der Client-Einstellungen über WPAD/WSPAD

Haben Sie die Option ENTSPRECHENDEN ISA SERVER-COMPUTER AUTOMATISCH ERMITTELN gewählt, können die Clients über die Suchfunktion des ISA Server automatisch den ISA Server suchen und finden. Diese Art der Konfiguration ist besonders für mobile Clients sinnvoll, die auf diese Weise den nächstgelegenen ISA Server ermitteln können.

Unterschiedliche Einstellungen für verschiedene Standorte

Besitzt ein Unternehmen mehrere Standorte und ist an jedem der Standorte ein ISA Server vorhanden, kann ein mobiler Benutzer zwischen den verschiedenen Standorten wechseln, ohne dass aufgrund der verschiedenen Netzwerke eine Änderung an den Konfigurationseinstellungen des Internetbrowsers oder des Firewallclients erforderlich wird.

Durch die automatische Suche der Clients nach dem ISA Server wird auch der administrative Aufwand eingeschränkt, da bei Änderungen am Netzwerk die Clients nicht mehr einzeln manuell angepasst werden müssen.

Mindestens Internet Explorer 5.0 nötig

Die Grundlage für die automatische Suche bilden das Webproxy Autodiscovery-Protokoll (WPAD) sowie das Winsock Proxy Autodiscovery-Protokoll (WSPAD). Beide Protokolle erfordern eine funktionsfähige DNS- und/oder DHCP-Umgebung. Voraussetzung für WPAD ist ein Internet Explorer in mindestens der Version 5.0.

WPAD/WSPAD über DHCP kann von den folgenden Betriebssystemen genutzt werden:

- Windows 98
- Windows ME
- Windows 2000
- Windows XP
- Windows Server 2003

WPAD/WSPAD über DNS kann von den folgenden Betriebssystemen genutzt werden:

- Windows 98
- Windows ME
- Windows NT 4.0
- Windows 2000
- Windows XP
- Windows Server 2003

Ist für einen Firewallclient die automatische Suche konfiguriert, stellt er eine Verbindung zu einem DNS- oder DHCP-Server her und stellt eine Anfrage nach einem WPAD-Eintrag, der auf einen ISA Server referenziert. Wird ein solcher WPAD-Eintrag gefunden, benutzt der Client den dahinterstehenden ISA Server.

Zur Nutzung der automatischen Suche werden Einstellungen am DNS- bzw. DHCP-Server sowie am ISA Server selbst vorgenommen.

Einstellungen am ISA Server

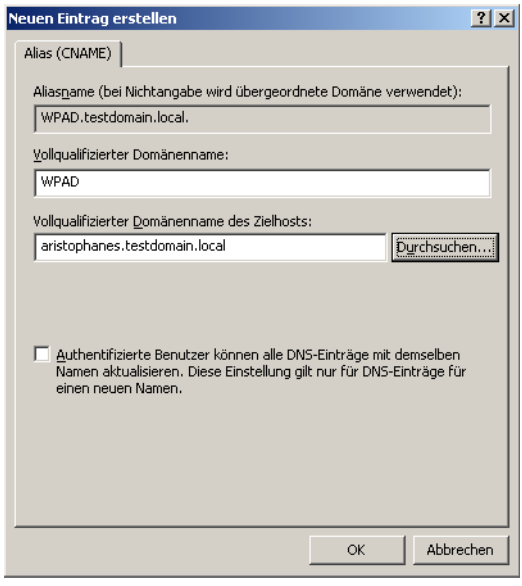
Die WPAD-Informationen sind für jedes interne Netzwerk separat konfigurierbar. Um die Informationen anzugeben, navigieren Sie in der ISA-Verwaltungskonsole zu SEVERNAME/KONFIGURATION/NETZWERKE/NETZWERKNAME. Über die EIGENSCHAFTEN des Eintrags wechseln Sie auf die Registerkarte AUTOMATISCHE ERKENNUNG. Dort markieren Sie die Checkbox INFORMATIONEN FÜR DIE AUTOMATISCHE ERKENNUNG VERÖFFENTLICHEN und geben einen Port an (siehe bereits Abbildung 5.3). Port 80 kann zusammen mit den Anfragen für ausgehende Internetverbindungen genutzt werden. Ein anderer Port ist nur anzugeben, wenn Port 80 z.B. vom IIS genutzt wird.

DNS-Einstellungen

Aliaseintrag zur DNS-Zone hinzufügen

In der internen DNS-Zone muss ein Alias (CName) für den ISA Server erstellt werden. Wählen Sie dazu in der DNS-mmc aus dem Kontextmenü der gewünschten Forward-Lookup-Zone den Eintrag NEUER ALIAS. Im Fenster NEUEN EINTRAG ERSTELLEN (siehe Abbildung 5.5) tragen Sie unter ALIASNAME den Wert WPAD ein und im zweiten Feld den vollqualifizierten Domänennamen des ISA Server.

Abbildung 5.5: Hinzufügen eines neuen DNS-Eintrags

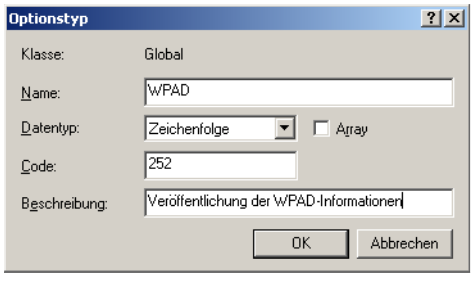


DHCP-Einstellungen

Neuer DHCP-Eintrag

In der DHCP-mmc muss ein neuer Eintrag vorgenommen werden, wenn WPAD über DHCP genutzt werden soll. Wählen Sie in der mmc aus dem Kontextmenü des Servernamens den Eintrag VORDEFINIERTE OPTIONEN EINSTELLEN. In dem dann erscheinenden Fenster VORDEFINIERTE WERTE UND OPTIONEN klicken Sie auf HINZUFÜGEN. Sie erhalten dann das Fenster OPTIONSTYP (siehe Abbildung 5.6), in dem Sie unter NAME den Wert WPAD, unter DATENTYP Zeichenkette und unter CODE 252 angeben. Optional kann auch eine Beschreibung angegeben werden.

Abbildung 5.6: Bestimmen des neuen Optionstyps WPAD



Klicken Sie dann auf OK. Sie erhalten wieder das Fenster VORDEFINIERTE OPTIONEN UND WERTE. Tragen Sie dort unter ZEICHENFOLGE den Pfad zum ISA Server ein (siehe Abbildung 5.7).

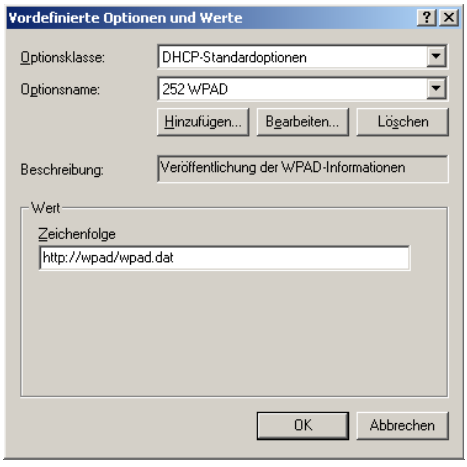


Abbildung 5.7: Der Option WPAD wird ein Wert hinzugefügt

Der Pfadname ist immer in dem Format *http://Name:Portnummer für Auto-Discovery/wpad.dat* anzugeben. Wurde der DNS-Eintrag WPAD erstellt und der Port bei dem Wert 80 belassen, ist die Angabe *http://wpad/wpad.dat* ausreichend. Ansonsten ist als Name der vollqualifizierte Domänenname des ISA Server anzugeben und die entsprechende Portnummer, unter der die Informationen für die automatische Suche vom ISA Server bereitgestellt werden. Dieser Port kann mit dem Port für ausgehende Webanfragen übereinstimmen.

Übernahme durch den DHCP-Server

Danach müssen Sie dafür sorgen, dass die eben erstellte Option auch vom DHCP-Server verwendet wird. Öffnen Sie dazu in der DHCP-mmc das Kontextmenü OPTIONEN KONFIGURIEREN unter BEREICHSOPTIONEN.

Im Fenster BEREICHOPTIONEN (siehe Abbildung 5.8) muss die Option 252 WPAD markiert werden.

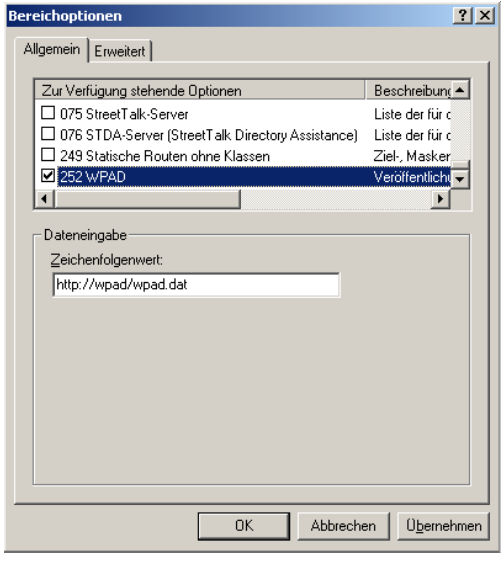
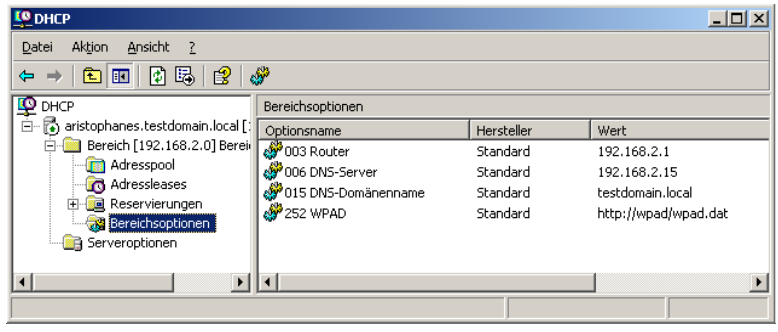


Abbildung 5.8: Aktivieren der Option WPAD in dem Bereich

Danach sollte der DHCP-Bereich folgendermaßen aussehen (siehe Abbildung 5.9).

Abbildung 5.9: Die DHCP-Bereichsoptionen nach Hinzufügen der Option WPAD



Die Client-Einstellungen konfigurieren

Automatische Suche für die Clients konfigurieren

Am ISA Server muss nun noch eingestellt werden, dass die Firewallclients bei der Installation die Informationen für die automatische Suche erhalten. Öffnen Sie dazu wieder die ISA-mmc und öffnen Sie die EIGENSCHAFTEN des internen Netzwerks unter KONFIGURATION/NETZWERKE. Wechseln Sie auf die Registerkarte FIREWALLCLIENT (siehe Abbildung 5.10). Markieren Sie dort die Checkboxen FIREWALLCLIENT-UNTERSTÜTZUNG FÜR DIESES NETZWERK AKTIVIEREN, AUTOMATISCHE ERMITTLUNG DER EINSTELLUNGEN und WEBPROXYSERVER VERWENDEN. Geben Sie jeweils die IP-Adresse oder den Namen des ISA Server an. Damit werden die Clients automatisch zur Verwendung von WPAD und als Webproxyclient konfiguriert.

Die einzelnen Optionen dieser Registerkarte haben die folgenden Bedeutungen:

Tabelle 5.1: Die Optionen der Registerkarte Firewallclient

Option	Beschreibung
Firewallclientunterstützung für dieses Netzwerk aktivieren	Für das gewählte Netzwerk wird der Firewallclient verfügbar. Man spricht auch vom Firewall-Listener.
ISA Server-Name bzw. IP-Adresse	Es ist die IP-Adresse oder der vollqualifizierte Domänenname des ISA Server anzugeben, nicht jedoch der NetBIOS-Name.
Automatische Ermittlung der Einstellungen	Die Computer, auf denen der Firewallclient vorhanden ist, werden auch als Webproxy-Clients konfiguriert. Die Einstellungen dafür werden über WPAD oder WSPAd bezogen.
Automatisches Konfigurationsskript verwenden	Die Konfigurationseinstellungen erhält der Client nicht über WPAD bzw. WSPAD, sondern über ein Konfigurationsskript, für das die URL angegeben werden kann.
Webproxy-Server verwenden	Die Firewallclients werden automatisch auch als Webproxy-Clients eingerichtet.

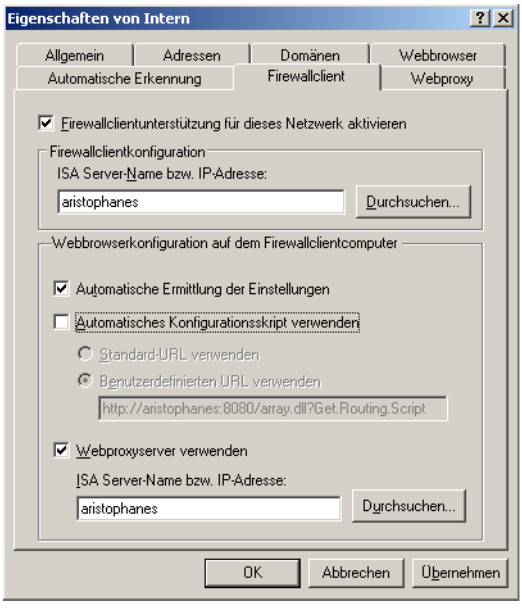


Abbildung 5.10: Dem internen Netzwerk werden die ISA-Informationen für die Installation des Firewallclients mitgeteilt

Ausnahmen für die Webproxyserver-Verwendung

Um weitere Eigenschaften für das interne Netzwerk zu bestimmen, wechseln Sie auf die Registerkarte WEBBROWSER. Dort können Sie bestimmen, dass der Proxyserver nicht für Webserver benutzt werden soll, die sich im internen Netzwerk befinden (siehe Abbildung 5.11). Des Weiteren können auch noch weitere Server und Domänen hinzugefügt werden, auf die ohne den Einsatz des Proxyservers zugegriffen werden soll.

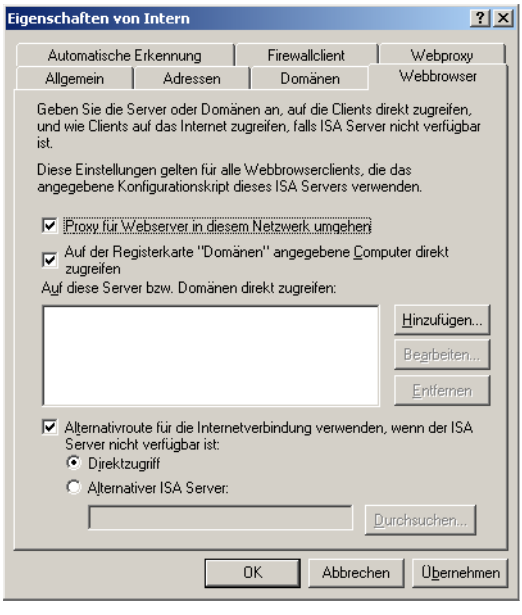


Abbildung 5.11: Proxy-Einstellungen für den Internetbrowser

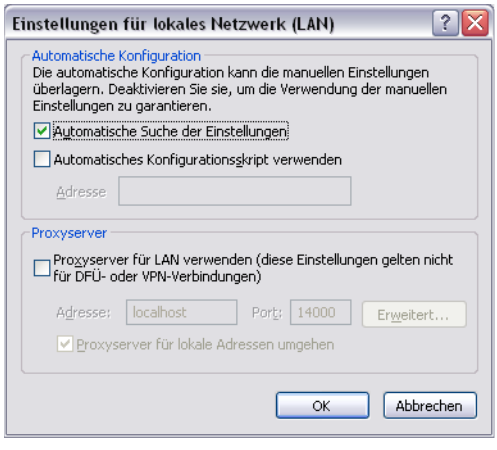
Einrichten des Internetbrowsers

Internet Explorer und Automatische Suche

Sofern der Firewallclient nicht installiert ist, müssen Sie den *Internet Explorer* anpassen, damit dieser die automatische Suche verwenden kann. Öffnen Sie dazu im *Internet Explorer* das Menü EXTRAS/INTERNETOPTIONEN und wechseln Sie auf die Registerkarte VERBINDUNGEN. Unter LAN-EINSTELLUNGEN klicken Sie auf EINSTELLUNGEN. Aktivieren Sie dann die Checkbox AUTOMATISCHE SUCHE DER EINSTELLUNGEN (siehe Abbildung 5.12). Bei einer standardmäßigen Installation des *Internet Explorer* ist diese Checkbox bereits aktiviert.

Da der Client selbst die Einstellungen suchen muss, kann es bei dem ersten Aufruf des *Internet Explorer* einen Moment dauern, ehe die gewünschte Seite angezeigt wird. Dieses Verhalten ist jedoch völlig normal und stellt keinen Fehler dar.

Abbildung 5.12: Einstellungen im Internet Explorer für die automatische Konfiguration



Den Firewallclient konfigurieren

Firewallclient und automatische Suche

Die automatische Suche kann auch beim Einsatz des Firewallclients aktiviert werden. Nach der Installation des Clients befindet sich das Icon des Firewallclients im Systemtray. Über das Kontextmenü KONFIGURIEREN dieses Icons muss auf der Registerkarte ALLGEMEIN (siehe Abbildung 5.13) die Option ISA SERVER AUTOMATISCH SUCHEN gewählt werden.

Abbildung 5.13: Die Konfiguration des Firewallclients

5.2.3 Installation über Gruppenrichtlinien

Softwareverteilung im Active Directory

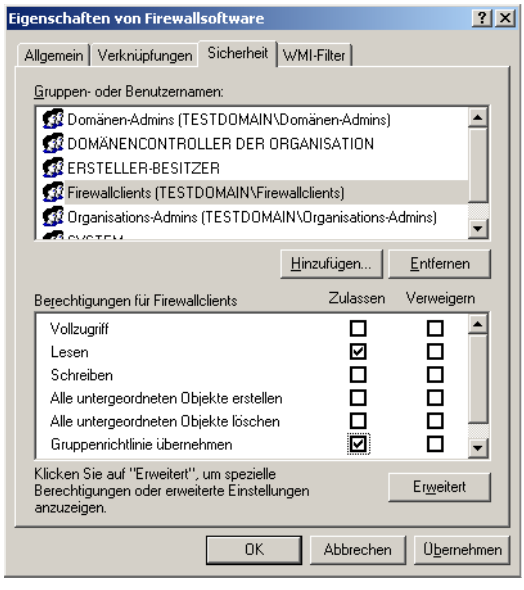
Der Firewallclient kann auch über die Gruppenrichtlinien-basierte Softwareverteilung im Windows 2003/2000 Active Directory erfolgen. Bedenken Sie jedoch, dass nur an Clients mit den Betriebssystemen Windows 2000, XP und Windows Server 2003 Software automatisch verteilt werden kann. Bei älteren Clients ist dieses nicht möglich. Für die Verteilung über eine Gruppenrichtlinie müssen Sie die folgenden Schritte ausführen:

1. Erstellen Sie dazu zunächst auf dem Dateiserver, von dem aus die Software installiert werden soll, eine Freigabe. Für die Freigabe muss die Benutzergruppe *Jeder* die Berechtigung *Lesen* besitzen. Verwenden Sie zur Verteilung die Datei *MS_FWC.msi* aus dem Ordner \CLIENTS der Installations-CD. Kopieren Sie diese in das erstellte Freigabeverzeichnis.
2. Öffnen Sie die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER und erstellen Sie eine globale Gruppe mit z.B. dem Namen *Firewallclients*.
3. Fügen Sie zu dieser Gruppe alle Computerkonten als Mitglieder hinzu, auf denen der Firewallclient installiert werden soll.
4. Wählen Sie dann das Kontextmenü EIGENSCHAFTEN der Domäne und wechseln Sie auf die Registerkarte GRUPPENRICHTLINIE. Klicken Sie dann auf NEU.

Haben Sie die *GPMC* (*Group Management Policy Console*) zur Verwaltung der Gruppenrichtlinien installiert, so verwenden Sie diese für die folgenden Schritte. Achten Sie darauf, dass die neue Gruppenrichtlinie mit der Domäne verknüpft wird.

5. Geben Sie der neuen Gruppenrichtlinie einen Namen, z.B. *Firewallsoftware*.
6. Klicken Sie dann auf EIGENSCHAFTEN und wechseln Sie auf die Registerkarte SICHERHEIT. Löschen Sie dort die Gruppe *Authentifizierte Benutzer* und fügen die neu erstellte Gruppe *Firewallclients* hinzu. Dieser Gruppe geben Sie die Berechtigungen *Lesen* sowie *Gruppenrichtlinie übernehmen* (siehe Abbildung 5.14).

Abbildung 5.14: Zuweisen von Berechtigungen für die neue Gruppe Firewallclients



7. Klicken Sie dann auf der Eigenschaftsseite der Domäne auf BEARBEITEN.
8. Im Fenster GRUPPENRICHTLINIENOBJEKT-EDITOR navigieren Sie zu COMPUTERKONFIGURATION/SOFTWAREEINSTELLUNGEN/SOFTWAREINSTALLATIONEN und wählen aus dem Kontextmenü NEU/PAKET.
9. Im Fenster ÖFFNEN navigieren Sie zu dem Netzwerkpfad der in Schritt 1 erstellten Freigabe und wählen die Datei *MS_FWC.msi* aus. Klicken Sie dann auf ÖFFNEN.

Handelt es sich bei dem Pfad um keinen Netzwerkpfad, sondern einen lokalen Ordner, erhalten Sie einen entsprechenden Hinweis. Der Vorgang kann aber dennoch fortgesetzt werden.

Zuweisen der Software

10. Im Fenster SOFTWARE BEREITSTELLEN (siehe Abbildung 5.15) wählen Sie die Option ZUGEWIESEN. Damit ist sichergestellt, dass die Software des Firewallclients nach dem nächsten Neustart der Computer automatisch installiert wird. Diese Applikation wird danach unter SYSTEMSTEUERUNG/SOFTWARE angezeigt. Klicken Sie dann auf OK.

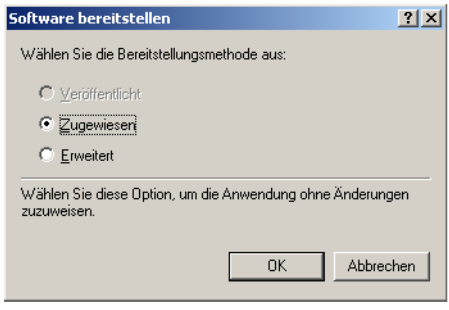


Abbildung 5.15: Auswahl der Option Zugewiesen für die Softwarebereitstellung

11. Öffnen Sie dann die EIGENSCHAFTEN des neu hinzugefügten Software-Pakets. Wechseln Sie auf die Registerkarte BEREITSTELLUNG VON SOFTWARE und klicken auf ERWEITERT.
12. Markieren Sie dort die beiden Checkboxen (siehe Abbildung 5.16) und klicken Sie auf OK.

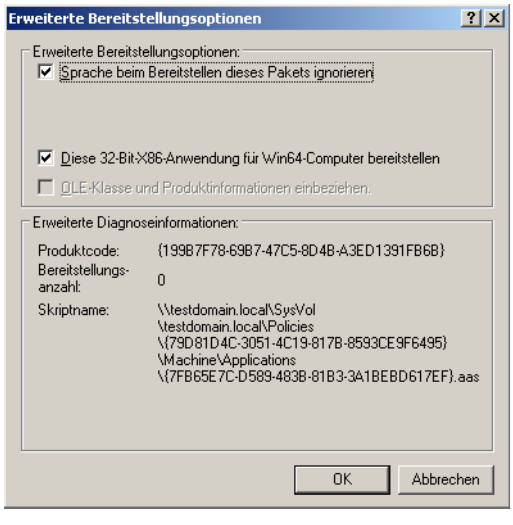


Abbildung 5.16: Weitere Konfigurationen für die Software-Bereitstellung

13. Schließen Sie nun das Eigenschaftsfenster des Software-Pakets. Die Software für den Firewallclient wird bei dem nächsten Neustart der Computer der Gruppe *Firewallclients* automatisch installiert.

5.2.4 Skriptbasierte, unbeaufsichtigte Installation

Zur Installation auf einer großen Anzahl von Clients

Die dritte Möglichkeit zur Installation des Firewallclients besteht in der skriptgesteuerten, unbeaufsichtigten Installation. Um eine unbeaufsichtigte Installation durchzuführen, verwenden Sie an der Eingabeaufforderung des Firewallclients den folgenden Befehl oder binden diesen in ein Skript ein. Auf diese Weise kann der Firewallclient automatisch auf mehreren Computern installiert werden.

```
Installationsfreigabe des Clients\Setup /v"[SERVER_NAME_
OR_IP=Servername] [ENABLE_AUTO_DETECT={1|0}] [REFRESH_
WEB_PROXY={1|0}] /qn" ↵
```

Die einzelnen Parameter haben folgende Bedeutung:

Tabelle 5.2: Die Parameter zum Aufruf der unbeaufsichtigten Installation des Firewallclients

Parameter	Bedeutung
`Installationsfreigabe`	Gibt die Installationsfreigabe des Firewallclients an. Standardmäßig befindet sich dieser in der Freigabe \MSPCLNT auf dem ISA Server. Unter ISA Server 2004 kann sich dieser auch auf einem anderen Computer befinden.
`Servername`	Gibt den ISA Server an, zu dem der Firewallclient seine Verbindung aufbauen soll
`ENABLE_AUTO_DETECT=1`	Der Firewallclient erkennt automatisch den ISA Server, über den die Verbindungen hergestellt werden sollen.
`REFRESH_WEB_PROXY=1`	Die Konfiguration des Firewallclients wird mit der auf dem ISA Server definierten Webproxy-Konfiguration automatisch aktualisiert.

Um die Deinstallation durchzuführen, ist folgender Befehl erforderlich (dazu ist eine administrative Berechtigung erforderlich):

```
Msiexec.exe /x {199B7F78-69B7-47C5-8D4B-A3ED1391FB6B} /
qn ↵
```

5.3 Weitere Einstellungen am Firewallclient

Sobald der Firewallclient installiert ist, gelten für ihn die auf dem ISA Server festgelegten Konfigurationseinstellungen. Bei jedem Neustart des Clients sowie im Dauerbetrieb alle sechs Stunden prüft der Firewallclient, ob auf dem ISA Server Änderungen an seiner Konfiguration vorgenommen worden sind. Auch über die IP-Adressen, die für

den Client als lokale IP-Adressen gelten sollen, wird er regelmäßig vom ISA Server informiert. Die eben beschriebenen Aktualisierungen werden standardmäßig so vorgenommen.

Lokale Einstellungen am Firewallclient

Es kann jedoch zusätzlich notwendig werden, lokale Konfigurationseinstellungen am Firewallclient vorzunehmen. Diese Änderungen sind jedoch nur für bestimmte Winsock-Applikationen wie z.B. *Outlook* erforderlich. Diese lokalen Konfigurationseinstellungen werden an verschiedenen *.ini*-Dateien des Firewallclients vorgenommen. Für die allermeisten Winsock-Anwendungen sind die Standardeinstellungen des Firewallclients jedoch völlig ausreichend.

Wurde die lokale Konfiguration geändert, werden diese Einstellungen erst bei der Aktualisierung der Clientkonfiguration umgesetzt.

5.3.1 Bearbeiten der .ini-Dateien

Für die Bearbeitung der Konfigurationsdaten werden drei verschiedene *.ini*-Dateien verwendet. Dabei handelt es sich um die folgenden Dateien:

- *common.ini*
- *management.ini*
- *application.ini*

Die beiden ersten Dateien werden standardmäßig in die Verzeichnisse `C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\Microsoft\Firewall Client 2004` sowie `C:\Dokumente und Einstellungen\Benutzername\Lokale Einstellungen\Anwendungsdaten\Microsoft\Firewall Client 2004` installiert, die *Application.ini* muss manuell erstellt werden. Je nach Betriebssystem können die Speicherorte entsprechend variieren. Alle drei *.ini*-Dateien gelten für den angemeldeten Benutzer und können für jeden Benutzer des Computers erstellt werden. Eine nur für einen Benutzer gesetzte Konfiguration hat immer Vorrang vor den allgemeinen Konfigurationseinstellungen.

Common.ini

In der Datei *Common.ini* sind Einstellungen gesetzt, die für sämtliche Anwendungskonfigurationen gelten. Die Datei kann folgendes Aussehen haben:

Listing 5.1: Inhalt der Datei common.ini

```
[Common]

ServerName=192.168.2.15

Disable=0

Autodetection=0
```

Automatische Erkennung

Unter `Disable` wird angegeben, ob der Firewallclient deaktiviert ist oder nicht, unter `Autodetection`, ob die automatische Erkennung des ISA Server aktiviert ist.

Management.ini

Firewall- und/ oder Webproxy-Client

In der Datei *management.ini* ist angegeben, ob der Firewallclient gleichzeitig auch als Webproxy-Client konfiguriert ist. Die Datei hat folgendes Aussehen:

Listing 5.2: Inhalt der Datei management.ini

```
[WebBrowser]
EnableWebProxyAutoConfig=1
```

Application.ini

Blockade bestimmter Applikationen

Diese Datei wird nicht installiert, sondern muss manuell erstellt werden. In dieser Datei befinden sich für den Client Informationen zu Applikationen, die nicht zentral über den ISA Server konfiguriert sind. Auf diese Weise können z.B. auf einem bestimmten Computer bestimmte Applikationen blockiert werden.

Um eine einzelne Applikation zu blockieren, suchen Sie deren Anwendungsnamen im Task-Manager unter PROZESSE. Diesen Namen setzen Sie in eckige Klammern und fügen in der nächsten Zeile `disable=1` hinzu. Die *Application.ini* kann somit folgendermaßen aussehen:

Listing 5.3: Möglicher Inhalt der Datei application.ini

```
[Prozessname]
Disable=1
```

5.3.2 Zentrale Einstellung am ISA Server

Sollen für die *application.ini* zentrale, am ISA Server eingestellte Optionen gelten, navigieren Sie in der ISA-mmc zu KONFIGURATION/ ALLGEMEIN und klicken auf den Link FIREWALLCLIENTEINSTELLUNGEN DEFINIEREN. Wechseln Sie dann auf die Registerkarte ANWENDUNGSEINSTELLUNGEN (siehe Abbildung 5.17).

Alle Einstellungen, die Sie hier vornehmen, gelten für sämtliche Firewallclients. Sie können jedoch durch Einstellungen an den *.ini*-Dateien außer Kraft gesetzt werden.

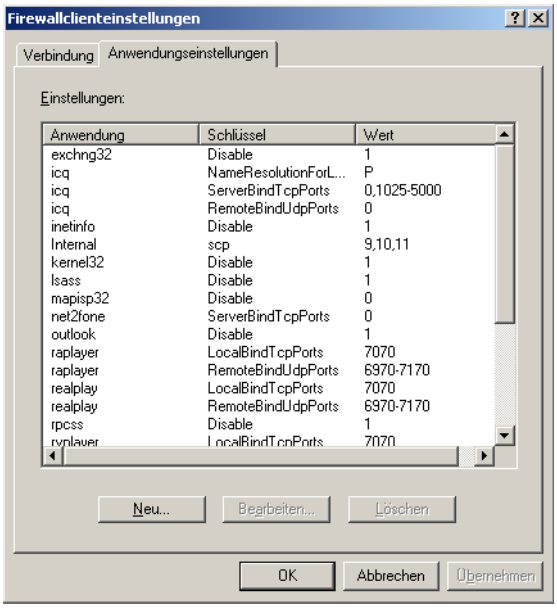


Abbildung 5.17: Einstellungen des Firewallclients für verschiedene Applikationen

Probleme mit Outlook und dem Firewallclient

Häufig bereitet die Applikation *Microsoft Out*look Probleme, wenn der Firewallclient aktiviert ist. Dies liegt darin begründet, dass die Standardeinstellung des Firewallclients *Outlook* bei Verwendung der Firewall deaktiviert.

Deshalb müssen Sie im Fenster ANWENDUNGSEINTRAGSEINSTELLUNGEN (siehe Abbildung 5.18) für *Outlook* den Schlüssel `Disable` auf den Wert `0` statt auf `1` setzen.

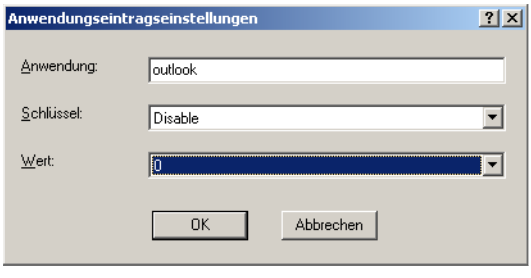


Abbildung 5.18: Ändern des Werts für Microsoft Outlook

Definition zahlreicher Schlüssel möglich

Außer dem Schlüssel `Disable` können noch viele weitere Schlüssel definiert werden. In Tabelle 5.3 finden Sie eine Übersicht und Beschreibung dazu.

Tabelle 5.3: Weitere mögliche Schlüssel für die Anwendungseinstellungen

Schlüssel	Beschreibung
`ServerName`	Name des ISA Server, zu dem der Firewallclient eine Verbindung herstellt
`Disable`	Als Werte sind 0 oder 1 möglich. Wert 1 deaktiviert die Firewallclientanwendung für die jeweilige Applikation.
`DisableEx`	Als Werte sind 0 oder 1 möglich. Wert 1 deaktiviert die Firewallclientanwendung für die jeweilige Applikation. Dies bezieht sich nur auf den Firewallclient des ISA Server 2004. Ist diese Option aktiviert, wird die Einstellung DISABLE aufgehoben.
`Name Resolution`	Als Werte sind L oder R möglich. Ist der Wert auf L (Local) gesetzt, geschieht die Namensauflösung auf dem lokalen Computer, bei dem Wert R (Redirection) wird die Auflösung an den ISA Server weitergeleitet. In der Standardeinstellung werden Domänennamen (in dezimaler oder durch Punkte getrennter Schreibweise sowie Internetdomänennamen) zur Namensauflösung an den ISA Server-Computer weitergeleitet. Alle weiteren Namen werden lokal auf dem Computer aufgelöst.
`LocalBind Tcp Ports`	Bestimmt einen TCP-Port, eine TCP-Liste oder einen TCP-Bereich mit lokaler Bindung
`LocalBind UdpPorts`	Bestimmt einen UDP-Port, eine UDP-Liste oder einen UDP-Bereich mit lokaler Bindung
`RemoteBind TcpPorts`	Bestimmt einen TCP-Port, eine TCP-Liste oder einen TCP-Bereich mit Remote-Bindung
`RemoteBind UdpPorts`	Bestimmt einen UDP-Port, eine UDP--Liste oder einen UDP-Bereich mit Remote-Bindung
`ServerBind TcpPorts`	Bestimmt einen TCP-Port, eine TCP-Liste oder einen TCP-Bereich für alle Ports, die mehr als nur eine Verbindung annehmen sollen
`Persistent`	Als Werte sind 0 oder 1 möglich. Durch den Wert 1 kann, wenn der ISA Server beim Starten oder Beenden eines Dienstes nicht antwortet, ein bestimmter Serverstatus auf dem ISA Server-Computer aufrecht erhalten werden. Während einer aktiven Sitzung werden vom Firewallclient in regelmäßigen Abständen Keep-Alive-Meldungen an den ISA Server geschickt. Wenn der Server nicht darauf antwortet, wird vom Client nach dem Neustart des Servers der Status der gebundenen und abhörenden Sockets wieder herzustellen versucht.

Schlüssel	Beschreibung
`Force Credentials`	Diese Einstellung kann nur am Firewallclientcomputer vorgenommen werden. Sie wird verwendet, wenn ein Windows-Dienst oder eine Windows-Serveranwendung als Firewallclientanwendung genutzt wird. Über den Wert 1 wird die Verwendung anderer Anmeldeinformationen für die Benutzerauthentifizierung erzwungen. Diese Authentifizierungsinformationen sind auf dem lokalen, den Dienst ausführenden Computer gespeichert. Diese Informationen werden auf dem Client mit Hilfe des Programms *Credtool.exe* gespeichert. Dieses Programm befindet sich im Lieferumfang der Firewallclientsoftware. Diese Anmeldeinformationen müssen auf ein vom ISA Server authentifizierbares Benutzerkonto verweisen. Es kann sich entweder direkt auf dem ISA Server oder in einer ihm vertrauenswürdigen Domäne befinden. Das Benutzerkonto sollte so eingerichtet sein, dass es nie abläuft, da ansonsten vor jedem Ablauf des Kontos die Benutzerinformationen aktualisiert werden müssten.
`Name Resolution ForLocal-Host`	Es sind die Werte "L" (Standardeinstellung), "P" oder "E" möglich. Der Wert gibt an, wie der lokale Computername des Clients beim Aufruf der API *gethostbyname* aufgelöst werden soll. Durch Aufruf der Winsock-API-Funktion *gethostbyname()* (unter Verwendung der Zeichenfolge *LocalHost*, einer leeren Zeichenfolge oder eines NULL-Zeichenfolgenzeigers) wird der Computername *LocalHost* aufgelöst. Alle Winsock-Anwendungen rufen zur Suche der lokalen IP-Adresse sowie deren Sendung an den Internetserver die API *gethostbyname(LocalHost)* auf. Über den Wert L gibt der API-Aufruf *gethostbyname()* die IP-Adressen des lokalen Computers zurück. Über den Wert "P" werden über den API-Aufruf die IP-Adressen des ISA Server und über den Wert E nur die externen IP-Adressen des ISA Server ausgegeben.
`Control Channel`	Es sind die beiden Werte "Wsp.udp" und "Wsp.tcp" (Standardeinstellung) möglich. Sie geben den Wert des verwendeten Steuerkanals an.
`EnableRoute Mode`	Es sind die Werte 0 und 1 (Standardeinstellung) möglich. Ist für *EnableRouteMode* der Wert 1 gesetzt und eine Route zwischen dem Firewallclient und dem angeforderten Ziel vorhanden, wird die IP-Adresse des Firewallclients als Quelladresse verwendet. Ist der Wert auf 0 gesetzt, wird die IP-Adresse des ISA Server benutzt. Diese Einstellung wird von älteren Versionen des Firewallclients nicht unterstützt.

5.3.3 Abarbeitungsreihenfolge

Vorrang der .ini-Dateien

Sind sowohl an den *.ini*-Dateien als auch auf dem ISA Server Konfigurationseinstellungen vorgenommen worden, werden zunächst vorrangig die Einstellungen der *.ini*-Dateien im jeweiligen Benutzerordner abgearbeitet. Danach werden die *.ini*-Dateien des Ordners \ALL USERS ausgewertet. Sind zusätzlich noch zentrale Einstellungen konfiguriert, werden diese auch übernommen. Sofern diese jedoch einer *.ini*-Einstellung widersprechen, werden die zentralen Einstellungen ignoriert und nicht verwendet.

5.3.4 IP-Adressen des Firewallclients

Vom Firewallclient werden alle IP-Adressen als lokale IP-Adressen angesehen, die sich in demselben Netzwerk befinden wie der Client selbst und die in der lokalen Routing-Tabelle des Clients als lokal gekennzeichnet sind.

Lokale IP-Adressen

Stellt der Firewallclient eine Verbindung zum internen Netzwerkadapter des ISA Server her, werden alle dem internen Netzwerk zugewiesenen IP-Adressen als lokale Adressen angesehen. Sobald eine Winsock-Anwendung des Clients eine Verbindung zu einer IP-Adresse herstellen möchte, prüft dieser anhand der Datei *locallat.txt*, ob sich diese IP-Adresse im internen Netzwerk befindet. Ist dies der Fall, wird die Verbindung direkt hergestellt, anderenfalls über den ISA Server. Diese Datei kann im Verzeichnis `C:\Dokumente und Einstellungen\All Users\Lokale Einstellungen\Anwendungsdaten\Microsoft\Firewall Client 2004` erstellt werden. Die Datei wird auch als *LAT (Local Address Table)* bezeichnet.

Die Datei *locallat.txt* kann mit einem beliebigen Texteditor erstellt werden. Dort können alle IP-Adressbereiche oder einzelne IP-Adressen eingetragen werden, die für den Client als zum internen Netzwerk gehörig gelten sollen. Die Adressen werden in die Datei in Form von Paaren eingetragen, z.B.

Listing 5.4: Beispiel für Einträge in der locallat.txt

```
192.168.2.1 192.168.2.200,
192.168.2.20 192.168.2.20.
```

In der ersten Zeile des Beispiels ist ein Adressbereich angegeben, in der zweiten Zeile lediglich eine einzelne IP-Adresse.

Sowohl anhand dieser Datei, aber auch seiner Routing-Tabelle und der ISA Server-Einstellungen kann der Client die Adressen des internen Netzwerks ermitteln.

5.3.5 Clientseitige Einstellungen

Symbol im Systemtray

Nachdem der Firewallclient installiert wurde, befindet sich im Systemtray ein entsprechendes Icon, das Sie über den Status des Clients informiert. Ist der Firewallclient deaktiviert, findet sich dort das in Abbildung 5.19 dargestellte Symbol. Ist der Client aktiv, wird stattdessen ein grüner Pfeil im Icon angezeigt.

Abbildung 5.19: Symbol des deaktivierten Firewallclients

Um die Konfiguration aufzurufen, klicken Sie das Icon doppelt oder rufen über das Startmenü die MICROSOFT FIREWALLCLIENTVERWALTUNG auf. Sie erhalten dadurch die schon in der Abbildung 5.13 gezeigte sowie in der folgenden Abbildung dargestellten Registerkarten.

Aktivierung des Firewallclients

Auf der Registerkarte ALLGEMEIN bestimmen Sie, ob der Firewallclient auf dem Computer aktiviert werden soll oder ob der ISA Server automatisch gesucht oder manuell ausgewählt werden soll. Zusätzlich können Sie festelegen, ob bei bestehender Verbindung zum ISA Server das Symbol in der Taskleiste angezeigt werden soll oder nicht.

Über die Registerkarte WEBBROWSER (siehe Abbildung 5.20) wird bestimmt, ob der Webbrowser des Clientcomputers automatisch so konfiguriert werden soll, dass der angegebene ISA Server auch als Proxyserver fungiert.

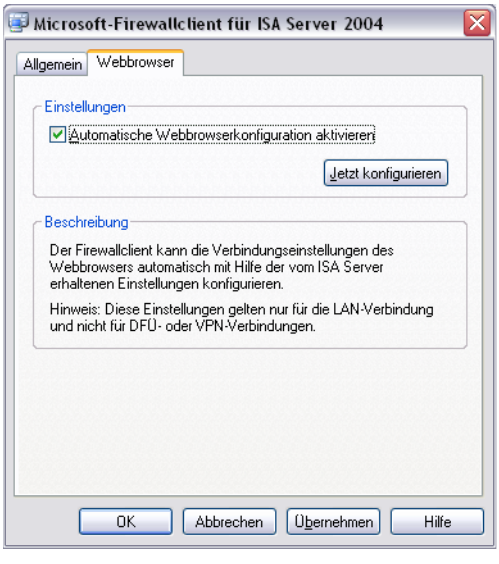


Abbildung 5.20: Die Registerkarte Webbrowser in der Konfiguration des Firewallclients

Alle Hinweise zu diesen Konfigurationseinstellungen finden Sie auch in der Datei *ISAClient.htm* im Verzeichnis `C:\Programme\Microsoft Firewall Client 2004`.

Benutzerberechtigungen

Um zu verhindern, dass der Benutzer den Firewallclient deaktiviert, sollte für den Benutzer nur die Berechtigung *Lesen* für die Datei *common.ini* vergeben werden.

5.3.6 Verschlüsselte Kommunikation

Im Gegensatz zu früheren Versionen bietet der Firewallclient des ISA Server 2004 die Möglichkeit, die Kommunikation zwischen dem Firewallclient und dem ISA Server zu verschlüsseln. Verwenden Sie noch ältere Firewallclients, so müssen Sie die Verschlüsselung ausschalten. Dies geschieht in der ISA-Verwaltung unter ALLGEMEIN in den FIREWALLCLIENTEINSTELLUNGEN auf der Registerkarte VERBINDUNG. Aktivieren Sie dort die Checkbox UNVERSCHLÜSSELTE FIREWALLVERBINDUNGEN ZULASSEN. Danach erfolgt ausschließlich eine unverschlüsselte Kommunikation (siehe Abbildung 5.21).

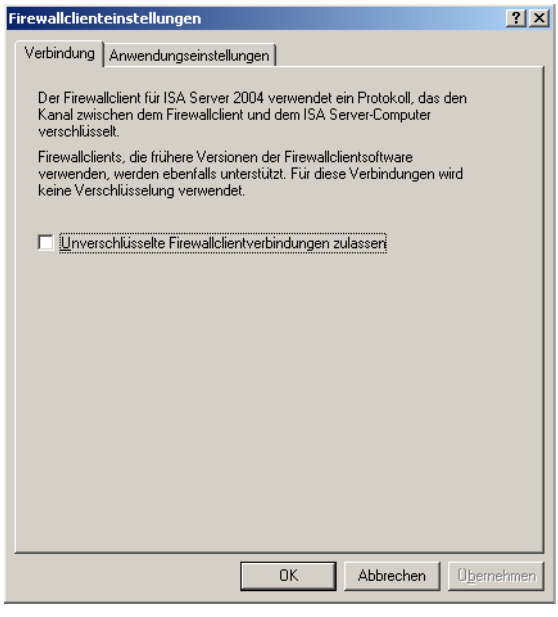


Abbildung 5.21: Legen Sie fest, ob die Verbindung zwischen dem ISA Server und den Firewallclients verschlüsselt oder aus Gründen der Abwärtskompatibilität unverschlüsselt erfolgen soll

5.4 Der SecureNAT-Client

Auf einem SecureNAT-Client ist keine Firewallclient-Software installiert. Dennoch können diese Clients viele Funktionen des ISA Server nutzen. Lediglich eine Authentifizierung auf Benutzerebene sowie die Unterstützung komplexer Protokolle ist nicht möglich.

Keine Benutzerauthentifizierung

Sofern bei einer ausgehenden Verbindung Zugriffsregeln auf dem ISA Server hinterlegt sind, verlangt der ISA Server Informationen zur Authentifizierung des Benutzers. Der SecureNAT-Client kann diese

Informationen jedoch nicht an den ISA Server senden. Ist also eine Zugriffsregel an die Authentifizierung eines Benutzers gebunden, kann der SecureNAT-Client diese Verbindung nicht herstellen. Die Verbindungen zwischen SecureNAT-Client und ISA Server sind immer anonym.

Dynamisch zugewiesene Ports

Von einem komplexen Protokoll spricht man, wenn während der Verbindung die Kommunikation von einem Port auf den anderen verlegt wird. Der SecureNAT-Client kann mit Portänderungen nur dann zurechtkommen, wenn auf dem ISA Server für das Protokoll ein Anwendungsfilter eingerichtet ist, der die Ports zwischen den beiden Endgeräten aushandelt und den Client über den aktuellen Port informiert. Sofern kein Anwendungsfilter eingerichtet ist, können vom ISA Server die dynamischen Ports nicht ermittelt und bereitgestellt werden, so dass die Kommunikation fehlschlägt.

Standardgateway

Für einen SecureNAT-Client muss jedoch ein Standardgateway konfiguriert sein, über das der Client den an das Internet gerichteten Verkehr an den ISA Server schickt. Diese Konfiguration kann manuell oder per DHCP-Server erfolgen.

DNS-Server

Des Weiteren muss der SecureNAT-Client zur Verwendung eines DNS-Servers eingerichtet sein, da der Client bei ausgehenden Zugriffen selbst für die Namensauflösung zuständig ist. Ist der Client Mitglied einer Domäne, so muss der interne DNS-Server zur Namensauflösung genutzt werden. Über die DNS-Weiterleitung werden die Anfragen an externe Webserver an DNS-Server im Internet weitergeleitet. Ist kein interner DNS-Server vorhanden, z.B. bei der Verwendung einer Arbeitsgruppe, die auf Basis der LMHOSTS-Einträge intern kommuniziert, muss für den SecureNAT-Client ein DNS-Server im Internet konfiguriert werden, z.B. der des Internetproviders.

Spezieller NAT-Treiber

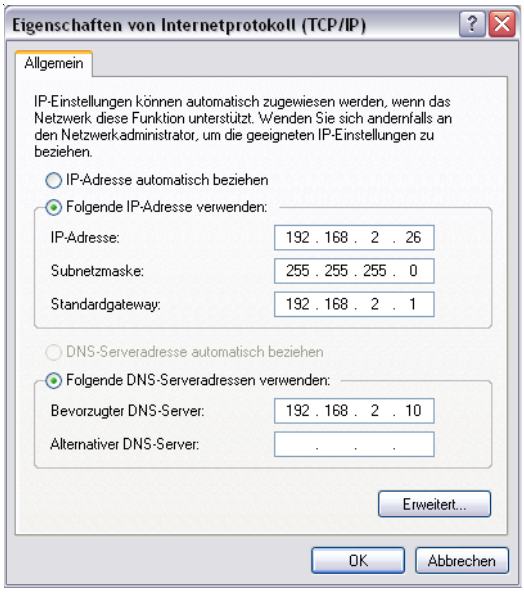
Zur Kommunikation verwendet der ISA Server einen speziellen NAT-Treiber. Dieser ist für die Übersetzung der privaten IP-Adresse des Clients in die externe IP-Adresse des ISA Server (also die öffentliche Adresse) zuständig. Sobald die private in die öffentliche IP-Adresse übersetzt wurde, wird die Anfrage an den Firewall-Dienst des ISA Server gesendet, der dann prüft, ob aufgrund von Zugriffsregeln oder Filterkonfigurationen die Anfrage gestellt werden darf. Zusätzlich wird bei einer ausgehenden Anfrage ermittelt, ob sich die angeforderten Inhalte bereist im Cache des ISA Server befinden. Sofern dies nicht der Fall ist, wird die Anfrage an den gewünschten Webserver weitergeleitet.

5.4.1 Den SecureNAT-Client manuell konfigurieren

Um den SecureNAT-Client manuell zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Öffnen Sie über die Eigenschaften der LAN-Verbindung die Eigenschaften von INTERNETPROTOKOLL (TCP/IP).
2. Tragen Sie als STANDARDGATEWAY die Adresse des ISA Server ein und unter BEVORZUGTER DNS-SERVER die des internen Domänencontrollers, der den DNS-Dienst ausführt (siehe Abbildung 5.22).

Abbildung 5.22: Die manuelle Konfiguration des SecureNAT-Clients



Paketweiterleitung

Befindet sich der Client nicht in demselben Netzwerk wie der ISA Server, muss als Standardgateway die IP-Adresse des Routers eingetragen werden, der für die Weiterleitung der Pakete an ein anderes Netzwerksegment zuständig ist.

5.4.2 Den SecureNAT-Client per DHCP konfigurieren

Die eben beschriebene Konfiguration kann auch über einen DHCP-Server verteilt werden. Die entsprechenden Einträge werden über die DHCP-mmc in den DHCP-Bereichs- oder Serveroptionen festgelegt. Der Eintrag für das Standardgateway wird über den Eintrag 003 ROUTER festgelegt (siehe Abbildung 5.23). Im Beispiel erfolgt die Konfiguration in den BEREICHSOPTIONEN.

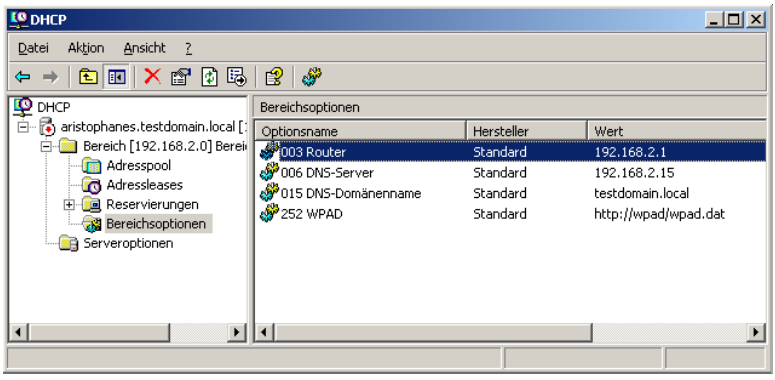


Abbildung 5.23: Festlegen des Standardgateways in den Bereichs- oder Serveroptionen des DHCP-Servers

Die Einstellung kann auch über die EIGENSCHAFTEN von INTERNETPROTOKOLL (TCP/IP) über die EIGENSCHAFTEN der NETZWERKVERBINDUNG erfolgen. Für Clients ab Windows XP ist die zusätzliche Registerkarte ALTERNATIVE KONFIGURATION verfügbar, wenn die automatische Konfiguration gewählt wurde. Sofern kein DHCP-Server verfügbar ist, kann für den Client eine fixe IP-Adresse festgelegt werden. Diese wird als alternative Konfiguration bezeichnet.

Anfrage-Verarbeitung durch Firewall-Dienst

Die Anfrage eines SecureNAT-Clients wird vom Firewalldienst verarbeitet. Zur Authentifizierung können lediglich Regeln anhand der IP-Adressen benutzt werden, eine Authentifizierung auf Benutzerbasis ist nicht möglich.

Die Clients benötigen grundsätzlich für den ausgehenden Verkehr eine Firewallrichtlinie. Auch wenn eine Protokollregel zur Freigabe des gesamten Datenverkehrs definiert ist, bezieht sich diese nur auf die Protokolle und Ports. Für die Auflösung der DNS-Namen ist der SecureNAT-Client selbst verantwortlich, während beim Einsatz des Firewallclients und Webproxyclients der ISA Server diese Aufgabe übernimmt.

Wird der ISA Server im reinen Cachemodus ausgeführt, werden SecureNAT-Clients nicht unterstützt.

5.5 Der Webproxy-Client

Keine Software erforderlich

Als Webproxyclient wird jeder Computer bezeichnet, auf dem ein Webbrowser eingerichtet ist, der für ausgehende Webanfragen den Webproxyfilter des ISA Server verwendet. Weitere Software muss für einen Webproxyclient nicht installiert sein, lediglich die Konfiguration des Webbrowsers ist entscheidend. Der Browser muss lediglich http 1.1-kompatibel sein. Der *Internet Explorer* als Webbrowser ist nur dann erforderlich, wenn die Authentifizierung auf Benutzerebene ausgeführt werden soll, da z.B. der *Netscape Navigator* lediglich die Standardauthentifizierung unterstützt. Vom Webproxyfilter werden die Protokolle http, https sowie ftp unterstützt.

Die Einstellungen im Webbrowser für den Proxy werden entweder per Gruppenrichtlinie zugewiesen oder manuell auf den Clients vorgenommen.

Um die Einstellung manuell vorzunehmen, öffnen Sie im *Internet Explorer* das Menü EXTRAS/OPTIONEN und wechseln auf die Registerkarte VERBINDUNGEN. Klicken Sie auf EINSTELLUNGEN. Im Fenster EINSTELLUNGEN FÜR LOKALES NETZWERK (LAN) (siehe Abbildung 5.24) tragen Sie die IP-Adresse und den Port des Proxyservers ein. Auch die Option PROXYSERVER FÜR LOKALE ADRESSEN UMGEHEN sollte aktiviert werden.

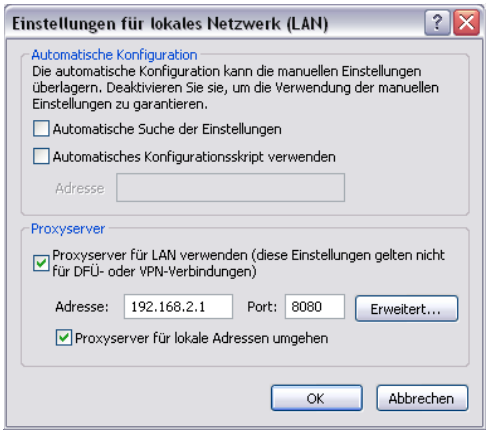


Abbildung 5.24: Die Einstellungen für den Proxyserver im Internet Explorer

Verwendung anderer Browser

Verwenden Sie einen anderen Webbrowser, tragen Sie dort auch die IP-Adresse des Proxyservers ein. Möglicherweise müssen Sie bei einigen Webbrowsern die IP-Adresse für den http-Proxy, ftp-Proxy sowie SSL-Proxy getrennt eingeben.

Geben Sie immer die IP-Adresse (die des Netzwerkadapters, der die Verbindung mit dem internen Netzwerk herstellt) und *nicht* den DNS-Namen oder Computernamen des ISA Server an. Anderenfalls würde bei der Namensauflösung die externe IP-Adresse benutzt werden, so dass die Anfragen des Webbrowsers nicht beantwortet werden können, da sich diese Adresse nicht in der lokalen Adresstabelle befindet.

Diese Einstellungen können auch automatisch bei der Installation des Firewallclients gesetzt werden. Dazu müssen Sie die entsprechende Einstellung auf dem ISA Server vornehmen. Öffnen Sie dazu in der ISA-mmc den Eintrag NETZWERKE/INTERN. Wechseln Sie auf die Registerkarte FIREWALLCLIENT und nehmen Sie die in Abbildung 5.25 dargestellten Einstellungen vor.

Konfigurationsskript

Über AUTOMATISCHES KONFIGURATIONSSKRIPT VERWENDEN wird die Standard-URL zur Konfiguration benutzt. Diese lautet *http://Name_ISA-Server:Port/array.dll?Get.Routing.Script*. Dieses Konfigurationsskript wird automatisch vom ISA Server erstellt.

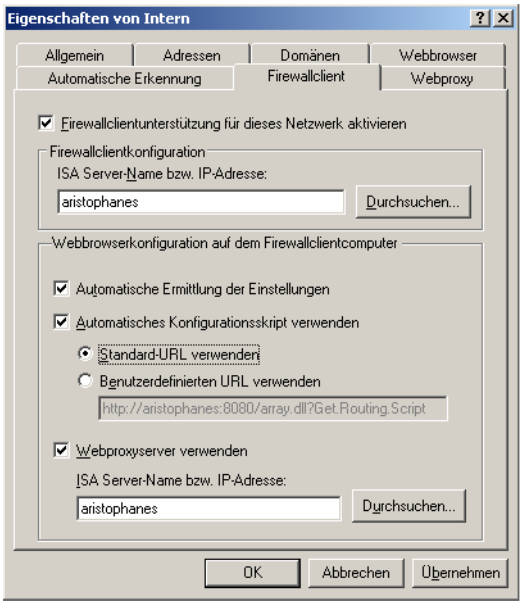


Abbildung 5.25: Einstellungen des Firewallclients für das Netzwerk Intern

Es ist auch möglich, dass der ISA Server bei jedem Aufruf des Webbrowsers ein Clientkonfigurationsskript automatisch downloadet. Dieses Skript beinhaltet eine Liste von ISA Servern, die vom Webbrowser beim Aufruf der URL verwendet werden. Dazu wird WPAD benutzt. Wechseln Sie dazu auf die Registerkarte WEBBROWSER (siehe Abbildung 5.26). Dort können Sie festlegen, für welche Zugriffe auf welche Server der Proxyserver umgangen werden soll.

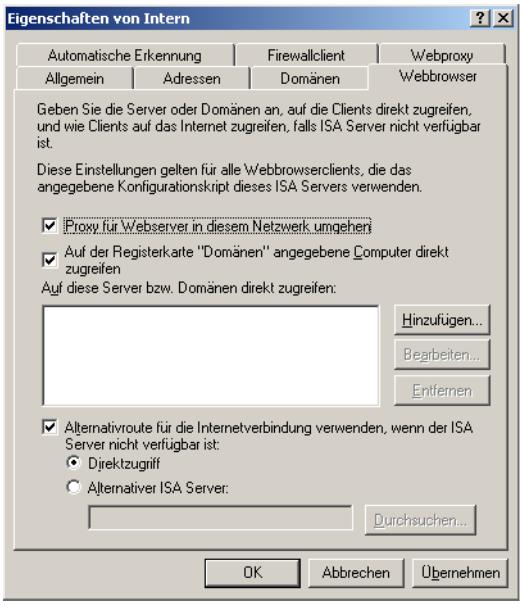


Abbildung 5.26: Proxy-Konfiguration des Webbrowsers für das Netzwerk Intern

Alternativrouten Sofern im Netzwerk mehrere ISA Server vorhanden sind, können Sie die Checkbox ALTERNATIVROUTE FÜR DIE INTERNETVERBINDUNG VERWENDEN, WENN DER ISA SERVER NICHT VERFÜGBAR IST. Tragen Sie dann unter ALTERNATIVER ISA SERVER die gewünschte Maschine ein.

6 Verwaltung des ISA Server

Dieses Kapitel beschreibt die verschiedenen Verwaltungsmöglichkeiten des ISA Server. Zunächst werden die Verwaltungswerkzeuge des ISA Server näher vorgestellt. Eine entscheidende Neuerung dabei ist die ISA-Toolbox, die ebenfalls ausführlich vorgestellt wird. Die Verwaltung kann nicht nur lokal am ISA Server, sondern auch von einem beliebigen Remote-Computer aus durchgeführt werden. Auch die Verwaltungsmöglichkeit über einen Terminalserver wird dabei vorgestellt. Zur Entlastung des Administrators kann auch eine Delegierung der ISA Server-Verwaltung durchgeführt werden. Ferner werden in diesem Kapitel die wichtigsten Verwaltungsaufgaben wie die Sicherung und Wiederherstellung sowie der Import und Export von Konfigurationseinstellungen beschrieben.

6.1 Die Verwaltungswerkzeuge

Nach der Installation des ISA Server finden Sie im Startmenü zwei Einträge unter MICROSOFT ISA SERVER. Dabei handelt es sich um den ISA SERVER-LEISTUNGSMONITOR sowie die ISA SERVER-VERWALTUNG.

Der Leistungsmonitor des ISA Server ist eine Weiterentwicklung des bekannten Windows-Systemmonitors, dem spezielle Leistungsindikatoren für den ISA Server hinzugefügt wurden. Der Leistungsmonitor wird ausführlich in Kapitel 12 vorgestellt.

6.1.1 Die ISA Server-Verwaltung

Eigene Verwaltungs-mmc

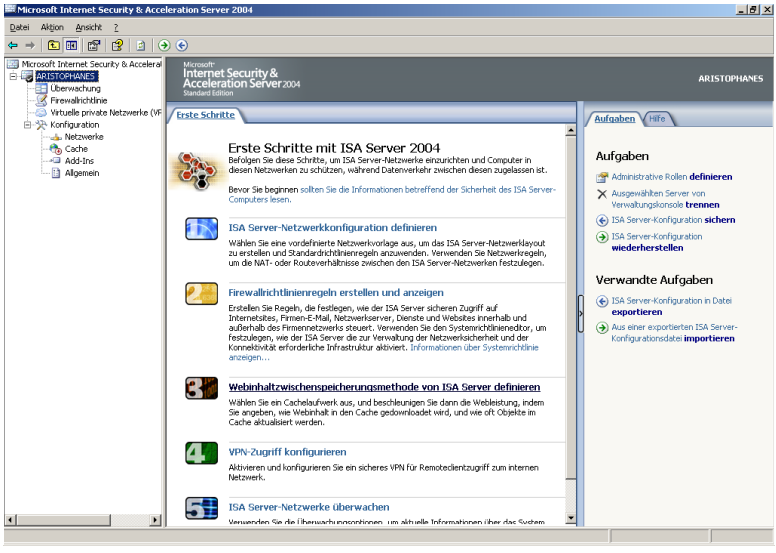
Über den zweiten Eintrag, die ISA SERVER-VERWALTUNG, nehmen Sie nahezu sämtliche Konfigurationseinstellungen sowie einige Überwachungsfunktionen und die Fehlersuche am ISA Server vor.

Das Verwaltungsfenster ist immer in drei Abschnitte gegliedert (siehe Abbildung 6.1). Im linken Bereich befindet sich wie in jeder Windows-mmc die *Baumstruktur* der verschiedenen Snap-Ins für die Konsole, in denen Sie wie gewohnt navigieren können. In der Mitte befindet sich das *Detailfenster*. In diesem werden die Konfigurationen des jeweiligen Snap-Ins angezeigt und können geändert werden. Der rechte Abschnitt wird als *Aufgabenfenster* bezeichnet. In diesem können Sie zu bestimmten Objekten die häufigsten Aufgaben mit nur einem Klick aufrufen. Besondere Bedeutung kommt in der Aufgaben-

liste der *Toolbox* zu, die Sie aufrufen können, wenn das Snap-In *Firewallrichtlinie* markiert ist. Über die *Toolbox* können sämtliche Elemente wie Protokolle, Benutzer, Inhaltstypen usw. konfiguriert werden, die für das Erstellen von Zugriffsregeln notwendig sind.

Ausführlich wird die Toolbox im Zusammenhang mit den Richtlinien in Kapitel 7 vorgestellt.

Abbildung 6.1: Überblick über die drei Bereiche der ISA Server-Verwaltungskonsole



Die verschiedenen Einträge in der Baumstruktur der mmc haben die folgenden Bedeutungen:

Tabelle 6.1: Übersicht über die Objekte in der Baumstruktur

Objekt	Beschreibung
Überwachung	Überwachungsfunktion des ISA Server. Es handelt sich um diverse Ansichten von der Echtzeitüberwachung bis hin zur Darstellung von Daten in Berichten und Grafiken. Die Überwachungsfunktion wird in Kapitel 12 ausführlich beschrieben.
Firewall-Richtlinie	Über die Firewall-Richtlinie werden sämtliche Regeln für die Filterung des eingehenden und ausgehenden Netzwerkverkehrs definiert, die den Zugriff für bestimmte Benutzer oder Computer auf bestimmte Ressourcen wie Server oder Dienste gestatten oder unterbinden. Die Konfiguration von Richtlinien wird in Kapitel 7 behandelt.

Objekt	Beschreibung
Virtuelle private Netzwerke (VPN)	In diesem Abschnitt können VPNs erstellt und verwaltet werden. Dies gilt für Standort-zu-Standort-VPNs und Remote-VPNs. Das Thema VPN wird in Kapitel 10 näher behandelt.
Konfiguration/ Netzwerke	Die verschiedenen Netzwerke (z.B. intern, extern, DMZ) können in diesem Abschnitt erstellt, bearbeitet und untereinander verknüpft werden
Konfiguration/ Cache	In diesem Abschnitt wird die Cache-Funktionalität verwaltet, die einen beschleunigten Zugriff auf das Internet sowie auch auf veröffentlichte Server bietet. Die Cache-Funktion des ISA Server wird detailliert in Kapitel 11 beschrieben.
Konfiguration/ Add-Ins	Über ADD-INS können Webfilter und Applikationsfilter erstellt werden, die ebenfalls zur Steuerung der Kommunikation verwendet werden. Die Konfiguration dieser Filter wird in Kapitel 9 weiter ausgeführt.
Konfiguration/ Allgemein	In diesem letzten Abschnitt befinden sich weitere Objekte, die thematisch zu keinem der anderen Punkte passen und deshalb hier zusammengefasst sind.

Übersichtlichkeit schaffen

Das Detailfenster kann über das Pfeilsymbol neben dem Detailbereich oder über die entsprechende Schaltfläche (siehe Abbildung 6.2) jederzeit ein- und ausgeblendet werden. Um mehr Übersicht im Detailfenster zu erhalten, sollten Sie das Aufgabenfenster schließen.

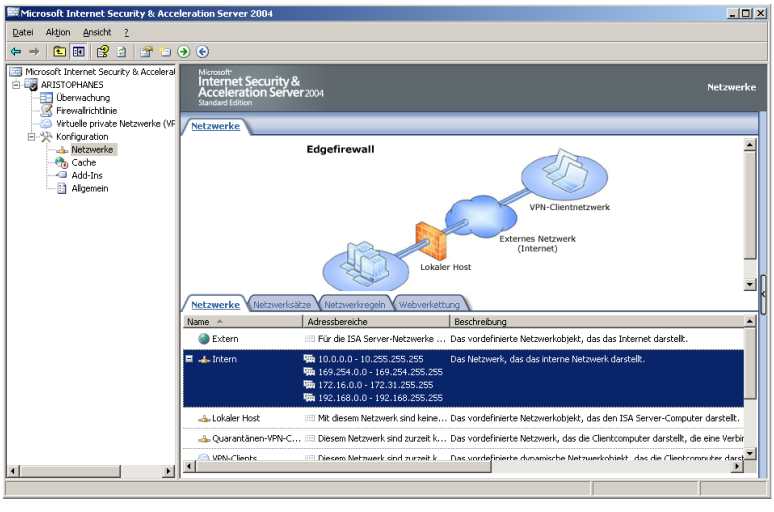


Abbildung 6.2: Die Aufgabenliste lässt sich zuklappen, so dass der Detailbereich übersichtlicher wird

6.1.2 Übernehmen von Änderungen

Vergessen Sie nicht diesen Schritt

Sobald Sie eine neue Einstellung am ISA Server vorgenommen oder eine bestehende geändert haben, müssen Sie diese Änderung übernehmen, bevor diese wirksam werden kann. Dazu erscheint im oberen Bereich des Detailfensters ein entsprechender Hinweis (siehe Abbildung 6.3). Über die Schaltfläche ÜBERNEHMEN werden die Änderungen akzeptiert und sind von nun an für den ISA Server gültig, über VERWERFEN können Sie eine Änderung ablehnen.

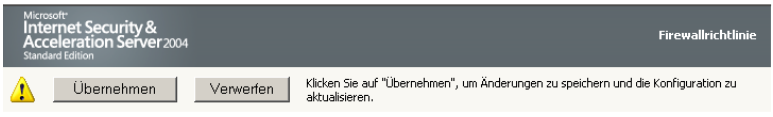


Abbildung 6.3: Änderungen an der Konfiguration müssen aus Sicherheitsgründen übernommen werden

Dieser Mechanismus ist nicht gedacht, um den Administrator zu ärgern oder ihn mit zusätzlichen Mausklicks zu belästigen, sondern dient der Sicherheit, damit nicht durch einen unbedachten oder ungewollten Mausklick eine Änderung permanent erhalten bleibt, die nicht geplant war.

Auf diese Weise können auch mehrere Einstellungen nacheinander geändert werden. Mit einem einzigen Klick auf ÜBERNEHMEN werden alle seit der letzten Übernahme vorgenommenen Änderungen gespeichert.

6.1.3 Erstellen einer benutzerdefinierten mmc

Mehrere Funktionen in einer mmc zusammenfassen

Wenn der Administrator nicht nur für die Verwaltung des ISA Server, sondern auch für andere Verwaltungsaufgaben am Active Directory und Windows Server zuständig ist, macht es sinn, wenn verschiedene Verwaltungskonsolen aus Gründen der Übersichtlichkeit und Effektivität in einer zusammengefasst werden, so dass nicht mehrere Fenster gleichzeitig geöffnet sein müssen.

Um mehrere Konsolen in einer einzigen zusammenzufassen, führen Sie die folgenden Schritte aus:

1. Geben Sie unter AUSFÜHREN den Befehl `mmc.exe` ein. Sie erhalten dadurch eine leere mmc.
2. Wählen Sie das Menü DATEI/SNAP-IN HINZUFÜGEN/ENTFERNEN.
3. Klicken Sie auf HINZUFÜGEN und wählen Sie die gewünschten Snap-Ins aus. Jedes Snap-In wird einzeln mit HINZUFÜGEN eingefügt. Klicken Sie dann auf SCHLIEßEN und auf OK.
4. Wählen Sie dann das Menü DATEI/SPEICHERN UNTER, um die neue mmc zu sichern. In der Abbildung 6.4 sehen Sie eine benutzerdefinierte mmc mit verschiedenen Snap-Ins.

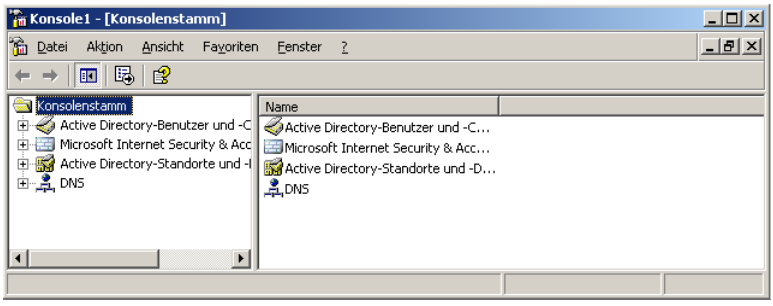


Abbildung 6.4: Hinzufügen mehrerer Snap-Ins zu einer benutzerdefinierten mmc

6.2 Die Remoteverwaltung des ISA Server

Drei Möglichkeiten zur Remoteverwaltung

Für den ISA Server 2004 ist auch die Remoteverwaltung von einem beliebigen anderen Computer aus möglich. Über diesen können sämtliche Verwaltungsaufgaben des ISA Server ausgeführt werden. Voraussetzung ist, dass der Verwaltungscomputer die Remoteverbindung entweder über einen Terminaldienstclient wie z.B. die Remotedesktopverbindung herstellt oder auf diesem die ISA-Verwaltungskonsole installiert ist. In einer großen Umgebung mit mehreren ISA Servern kann die Verwaltung sämtlicher Server über einen einzigen Verwaltungscomputer durchgeführt werden.

Ist auf einem Remotecomputer das Service Pack 1 für den ISA Server 2004 in der Standardversion installiert, auf dessen Protokolle und Sitzungen zugegriffen werden soll, so muss auf dem ISA Server, der die Verwaltungskonsole beherbergt, ebenfalls das Service Pack 1 installiert sein. Ansonsten kann es zu Problemen kommen.

Als Drittes besteht auch die Möglichkeit, den ISA Server von einem anderen ISA Server aus zu verwalten. Hierzu öffnen Sie die ISA-mmc und wählen aus dem Kontextmenü von MICROSOFT INTERNET SECURITY AND ACCELERATION SERVER 2004 den Eintrag VERBINDUNG HERSTELLEN. Geben Sie dann den Namen oder die IP-Adresse des zu verwaltenen ISA Server an.

6.2.1 Remote-Verwaltung über Terminalserver oder Verwaltungskonsole?

Bevor Sie die Remoteverwaltung des ISA Server durchführen, müssen Sie entscheiden, ob die Verbindung über die Verwaltungskonsole, also eine mmc, oder eine Terminalserververbindung wie z.B. die Remotedesktopverbindung hergestellt werden soll.

Terminalserver

Verwaltung eines einzelnen ISA Server

Über die Terminalserververbindung wie die Remotedesktopverbindung wird der Desktop des ISA Server direkt angezeigt. Sie können wie auf dem Server selbst arbeiten. Sämtliche Änderungen werden sofort am Server vorgenommen. An den Client werden lediglich die Tastatureingaben und Mausbewegungen übertragen. Allerdings kann auf diese Weise nur ein einzelner ISA Server angezeigt werden. Jedoch können so Verbindungen zu Servern hergestellt werden, die sich in unterschiedlichen Netzwerken befinden.

Verwaltungskonsole

Verwaltung mehrerer ISA Server

Bei der Verwaltung über die mmc erfolgt die Aktualisierung langsamer, da die Konfigurationseinträge an den ISA Server übertragen werden müssen. Allerdings ist es über die mmc möglich, mehrere ISA Server gleichzeitig zu verwalten, da mehrere parallele Verbindungen hergestellt werden können. Dies ist besonders interessant, wenn sich die ISA Server an mehreren entfernten Standorten befinden oder ein externer Consultant die Verwaltung der ISA Server verschiedener Unternehmen übernommen hat. Die ISA-mmc ist eine Komponente des ISA Server und kann separat auf einem Verwaltungscomputer installiert werden. Der Verwaltungscomputer muss sich in diesem Szenario in demselben Netzwerk befinden wie der ISA Server. Die Verwaltungs-mmc kann auf Clients der Betriebssysteme Windows 2000 Professional und Server, Windows XP sowie Windows Server 2003 installiert und ausgeführt werden.

Verwaltung per VPN-Client

Erfolgt die Verwaltung über einen VPN-Client, sollte nach Möglichkeit die Terminalverbindung genutzt werden. Sofern bei einigen Konfigurationsänderungen ein Neustart von Diensten notwendig wird, wird dabei auch der Routing- und RAS-Dienst (RRAS) beendet, wobei auch die Remote-Verbindung der Verwaltungs-mmc gekappt wird. Die Verbindung muss wieder neu hergestellt werden, nachdem der RRAS-Dienst auf dem ISA Server wieder gestartet ist. Bei einer Verbindung über die Terminalserver-Remoteverwaltung besteht dieses Problem nicht.

Sollen mehrere ISA Server über einen einzigen ISA Server verwaltet werden, so muss eine Zugriffsregel für die Verbindungsgenehmigung vom Verwaltungs-ISA Server zu den übrigen ISA Servern erstellt werden.

Die Art der Authentifizierung sowie der zu sendenden Informationen des Remoteclients am ISA Server unterscheidet sich je nachdem, ob der ISA Server Mitglied in einer Domäne oder Arbeitsgruppe ist. Auf beide Methoden wird in den folgenden Kapiteln eingegangen.

6.2.2 Serverkonfiguration zur Remoteverwaltung

Bevor die Remoteverwaltung des ISA Server durchgeführt werden kann, müssen auf dem Server einige Konfigurationsschritte durchgeführt werden. Dazu zählen der Export der Systemrichtlinien, die Konfiguration der Remoteverwaltung auf Server und Verwaltungscomputer sowie das Erstellen einer Zugriffsregel.

6.2.3 Export der Systemrichtlinie

Änderungen rückgängig machen

Zum Einsatz der Remote-Verwaltung muss die Systemrichtlinie des ISA Server bearbeitet werden. Um Änderungen an der Systemrichtlinie später wieder schnell rückgängig machen zu können, sollten Sie diese zuvor exportieren.

1. Klicken Sie dazu auf FIREWALLRICHTLINIE und im Aufgabenbereich auf der Registerkarte AUFGABEN auf SYSTEMRICHTLINIE EXPORTIEREN.
2. Geben Sie einen aussagekräftigen Namen für die zu exportierende Konfiguration an und klicken auf EXPORTIEREN und danach auf OK.

6.2.4 Aktivieren der Remotedesktopverwaltung

Haben Sie sich für die Verwaltung über die Terminaldienste entschieden, muss auf dem ISA Server auch die Remotedesktopverwaltung aktiviert und konfiguriert werden. Je nachdem, ob der ISA Server unter Windows Server 2000 oder 2003 ausgeführt wird, unterscheiden sich die jeweiligen Verfahren.

Windows Server 2000

Um die Remotedesktopverwaltung unter Windows Server 2000 zu aktivieren, öffnen Sie SYSTEMSTEUERUNG/SOFTWARE. Wählen Sie dort WINDOWS KOMPONENTEN HINZUFÜGEN/ENTFERNEN. Markieren Sie dann die Option TERMINALDIENSTE. Beim Setup der Terminaldienste wählen Sie die Option REMOTEVERWALTUNGSMODUS.

Windows Server 2003

Unter Windows Server 2003 ist das Aktivieren der Remotedesktopverbindung wesentlich einfacher.

Öffnen Sie die Eigenschaften des Arbeitsplatzes und wechseln Sie auf die Registerkarte REMOTE. Dort markieren Sie die Checkbox BENUTZERN ERLAUBEN, EINE REMOTEDESKTOPVERBINDUNG HERZUSTELLEN.

Verwechseln Sie diese Option nicht mit der dort ebenfalls möglichen Option zur Aktivierung der Remoteunterstützung.

6.2.5 Konfiguration des ISA Server

Computersatz Remoteverwaltungscomputer

Die Remoteverwaltung ist nach der Installation des ISA Server zwar aktiviert, jedoch ist sie nur für den bestimmten Computersatz *Remoteverwaltungscomputer* aktiviert. Dieser Computersatz verfügt nach der Installation jedoch noch über keinerlei Mitglieder. Führen Sie die folgenden Schritte aus, um zu prüfen, ob die Remoteverwaltung aktiviert ist und Netzwerke auszuwählen, von denen aus die Remoteverwaltung gestattet ist.

1. Markieren Sie die FIREWALLRICHTLINIE und klicken Sie im Aufgabenbereich auf der Registerkarte AUFGABEN auf SYSTEMRICHTLINIE BEARBEITEN.
2. Wechseln Sie dort unter KONFIGURATIONSGRUPPEN zu REMOTEVERWALTUNG/MICROSOFT MANAGEMENT CONSOLE. Stellen Sie sicher, dass auf der Registerkarte ALLGEMEIN die Checkbox AKTIVIEREN markiert ist.

Ist zu diesem Zeitpunkt bereits eine Remoteverbindung von einem Verwaltungscomputer aus hergestellt und ändern Sie hier die Einstellung, so bleibt diese Sitzung dennoch aktiv und bestehen, bis der Client die Verbindung trennt.

3. Wechseln Sie dann auf die Registerkarte VON. Dort ist in der Liste lediglich der Computersatz REMOTEVERWALTUNGSCOMPUTER eingetragen (siehe Abbildung 6.5). Alle Computer, die in dieser Liste stehen, können über die Verwaltungskonsole die Remoteverwaltung des ISA Server durchführen. Über die entsprechenden Schaltflächen können Sie entweder die *Regelelemente Netzwerke, Netzwerksätze, Computer, Adressbereiche, Subnetze* oder *Computersätze* (siehe Tabelle 6.2) hinzufügen bzw. löschen sowie Einstellungen vorhandener Objekte bearbeiten. Unter AUSNAHMEN können Auswahlen aus denselben Objekten hinzugefügt werden.

Was sind Regelelemente?

Regelelemente werden nicht nur im Zusammenhang mit der Definition von Objekten für die Remoteverwaltung verwendet. Allgemein werden Regelelemente benutzt, um Richtlinien genauer zu definieren. So kann besipielsweise eine Richtlinie erstellt werden, die für einen kompletten Netzwerksatz gültig ist oder bei der Ausnahmen für ein bestimmtes Subnetz gelten sollen.

Es gibt die folgenden Netzwerk-Regelelemente, die zum Festlegen von Systemrichtlinien für die Remoteverwaltung geeignet sind. Weitere Regelelemente lernen Sie in Kapitel 7 kennen.

Regelelement	Beschreibung
Netzwerk	Ein Netzwerk besteht aus allen Computern, die direkt oder über einen Router eine Verbindung zu einer Netzwerkkarte des ISA Server herstellen.
Netzwerksatz	Ein Netzwerksatz ist eine Gruppe von einem oder mehreren einzelnen Netzwerken.
Computer	Es handelt sich um einen einzelnen über die IP-Adresse identifizierten Computer.
Computersatz	Ein Computersatz umfasst einen Satz von Computern, Adressbereichen und Subnetzen.
Adressbereich	Dieses Element gibt einen bestimmten Satz von Computern an, die über einen fortlaufenden Bereich von IP-Adressen verfügen.
Subnetz	Es handelt sich um ein Subnetz des Netzwerks. Das Subnetz wird über die Netzwerkadresse und die Netzwerkmaske gekennzeichnet.

Tabelle 6.2: Übersicht über die verschiedenen Regelelemente

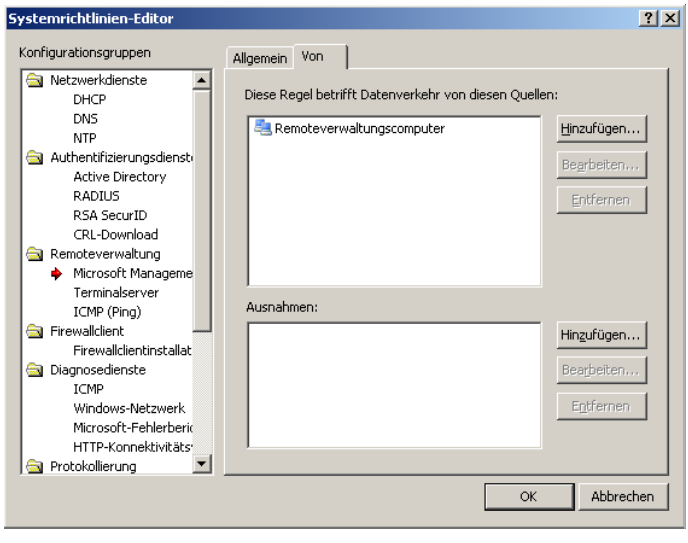


Abbildung 6.5: Hinzufügen von Computern und weiteren Regelelementen, denen die Remoteverwaltung über die Verwaltungskonsole gestattet ist

Hinzufügen von Objekten

Wollen Sie den Standardcontainer REMOTEVERWALTUNGSCOMPUTER benutzen, so müssen Sie diesem standardmäßig leeren Container zunächst Objekte hinzufügen.

Soll z.B. einem bestimmten Netzwerk die Remoteverwaltung erlaubt sein, so fügen Sie dies der oberen Liste hinzu. Soll jedoch einem bestimmten Computer dieses Netzwerks die Verwaltung nicht gestattet sein, so fügen Sie diesen unter AUSNAHMEN hinzu. Klicken Sie danach auf OK.

4. Wechseln Sie dann unter KONFIGURATIONSGRUPPEN zum Eintrag REMOTEVERWALTUNG/TERMINALSERVER. Prüfen Sie dort auf der Registerkarte ALLGEMEIN, dass diese Option aktiviert ist. Standardmäßig sollte die Remoteverwaltung über Terminalserver nach der Installation aktiviert sein.
5. Auf der Registerkarte VON fügen Sie dann wie in Schritt 3 beschrieben die gewünschten Regelelemente hinzu und definieren gegebenenfalls auch Ausnahmen.

6.2.6 Konfiguration des Verwaltungscomputers

Dieses Kapitel beschreibt die Konfiguration des Remotecomputers für den Zugriff auf den ISA Server. Es wird sowohl das Verfahren für die Verwaltungskonsole als auch für die Terminaldienste beschrieben.

Konfiguration der Verwaltungskonsole

Installation der ISA-mmc

Soll die Verwaltung über die ISA-Verwaltungskonsole erfolgen, so muss auf dem Verwaltungscomputer die entsprechende mmc installiert werden. Führen Sie dazu die folgenden Schritte aus:

1. Legen Sie die ISA-CD ein und klicken Sie nach dem Autostart der CD auf den Link ISA SERVER 2004 INSTALLIEREN.
2. Stimmen Sie in den folgenden Fenstern dem Lizenzvertrag zu und geben Sie die Kundeninformationen sowie Lizenznummer des ISA Server an.

Zur Installation der Verwaltungskonsole auf einem Verwaltungscomputer ist keine separate Lizenz erforderlich.

3. Verwenden Sie ein anderes Betriebssystem als Windows Server 2000 oder 2003, erhalten Sie im Fenster ZUSAMMENFASSUNG DER INSTALLATIONSANFORDERUNGEN einen Hinweis, dass lediglich die Verwaltungskonsole, nicht aber die Komponenten der Firewall installiert werden können. Klicken Sie hier auf WEITER.
4. Wird die Verwaltungskonsole unter Windows Server 2000 oder 2003 installiert, wählen Sie die Installationsart BENUTZERDEFINIERT. Bei anderen Betriebssystemen kann ohnehin nur die ISA Serververwaltung installiert werden. Wählen Sie diesen Eintrag im Fenster BENUTZERDEFINIERTE INSTALLATION aus und klicken Sie auf WEITER.
5. Im letzten Fenster schließen Sie die Installation durch einen Klick auf INSTALLIEREN ab.

Konfiguration der Terminaldienste

Terminaldienstclient

Damit die Remoteverbindung zur Verwaltung des ISA Server hergestellt werden kann, muss auf dem Verwaltungscomputer ein Terminaldienstclient vorhanden sein. Verwenden Sie auf dem Verwaltungs-

computer Windows XP oder Windows Server 2003, kann hierzu die Remotedesktopverbindung genutzt werden.

Verwenden Sie die Betriebssysteme Windows 9x, ME, NT 4.0 oder 2000, so führen Sie die folgenden Schritte für die Bereitstellung des Terminaldienstclients durch:

1. Auf einem Computer des Betriebssystems Windows Server 2003 muss der Clientinstallationsordner freigegeben werden. Der zukünftige Verwaltungscomputer des ISA Server muss über eine Netzwerkverbindung zu diesem Computer verfügen.
2. Geben Sie auf dem Verwaltungscomputer unter AUSFÜHREN den folgenden Befehl ein:

   ```
   \\Name_Windows_2003_Server\Tsclient\Win32\Setup.exe ↵
   ```

3. Zur weiteren Installation folgen Sie den Anweisungen des Installationsassistenten.

6.2.7 Erstellen einer Zugriffsregel

Die in diesem Kapitel beschriebene Konfiguration einer Zugriffsregel muss nur ausgeführt werden, wenn die Verwaltung von einem anderen ISA Server aus erfolgt. Beim Benutzen der Verwaltungskonsole oder der Terminalverbindung ist dieser Schritt nicht notwendig.

Damit die Verwaltung von einem anderen ISA Server aus erfolgen kann, müssen Sie sicherstellen, dass sich beide Server in demselben lokalen Netzwerk befinden.

Regel für Verwaltungszugriff

Damit die Daten für die Verwaltung zwischen den beiden ISA Servern ausgetauscht werden können, muss eine Zugriffsregel erstellt werden. Dazu müssen Sie auf dem ISA Server, von dem aus die Verwaltung erfolgen soll, die folgenden Schritte ausführen:

1. Navigieren Sie in der ISA-mmc zum Eintrag FIREWALLRICHTLINIE und wechseln Sie im Aufgabenbereich auf die Registerkarte AUFGABEN. Wählen Sie dort NEUE ZUGRIFFSREGEL ERSTELLEN. Es wird ein Assistent zum Erstellen dieser Regel gestartet.
2. Geben Sie der Zugriffsregel einen aussagekräftigen Namen, z.B. ISA-VERWALTUNG ZULASSEN, und klicken Sie auf WEITER.
3. Im Fenster REGELAKTION wählen Sie ZULASSEN und klicken auf WEITER.
4. Im folgenden Fenster PROTOKOLLE wählen Sie die Option AUSGEWÄHLTE PROTOKOLLE und klicken dann auf HINZUFÜGEN. Im Fenster PROTOKOLLE HINZUFÜGEN erweitern Sie den Eintrag ALLE PROTOKOLLE und wählen MS-FIREWALLSTEUERUNG (siehe Abbildung 6.6). Klicken Sie danach auf HINZUFÜGEN und SCHLIEßEN sowie dann auf WEITER.

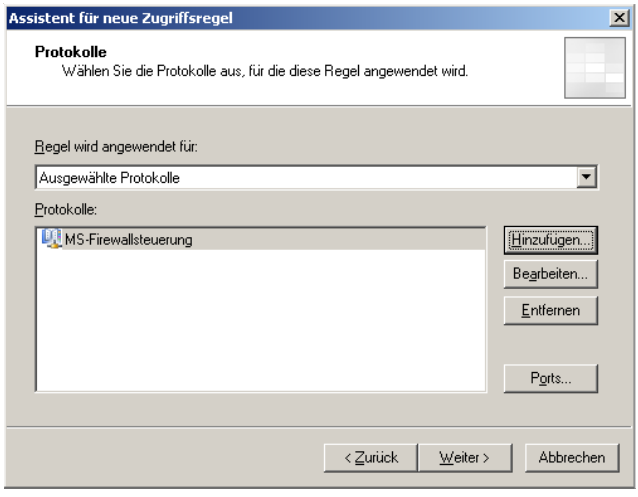


Abbildung 6.6: Das Protokoll MS-Firewallsteuerung zur Zugriffsregel hinzufügen

5. Es erscheint das Fenster ZUGRIFFSREGELQUELLEN. Klicken Sie dort auf HINZUFÜGEN und erweitern Sie im Fenster NETZWERKIDENTITÄTEN HINZUFÜGEN den Eintrag NETZWERKE. Dort wählen Sie LOKALER HOST und klicken danach nacheinander auf HINZUFÜGEN, SCHLIEßEN und WEITER.
6. Im nächsten Fenster ZUGRIFFSREGELZIELE klicken Sie auf HINZUFÜGEN. Im dann erscheinenden Fenster NETZWERKIDENTITÄTEN HINZUFÜGEN erweitern Sie den Eintrag NETZWERKE und wählen dort das NETZWERK aus, in dem sich der zu verwaltende ISA Server befindet. Klicken Sie dann wieder nacheinander auf HINZUFÜGEN, SCHLIEßEN und WEITER.
7. Als Nächstes wird festgelegt, für welche Benutzer diese Zugriffsregel gelten soll. Im Fenster BENUTZERSÄTZE wählen Sie ALLE BENUTZER, wenn diese Regel für sämtliche Benutzer des Verwaltungs-ISA Server gelten soll. Anderenfalls markieren Sie den Eintrag ALLE BENUTZER und klicken Sie auf ENTFERNEN und dann auf HINZUFÜGEN. In dem dann erscheinenden Fenster BENUTZER HINZUFÜGEN wählen Sie entweder den gewünschten Benutzersatz aus oder erstellen über NEU einen neuen Benutzersatz. Klicken Sie danach auf WEITER.
8. In der Zusammenfassung werden Ihre Einstellungen angezeigt. Sind diese korrekt, klicken Sie auf FERTIG STELLEN.
9. Damit die neue Zugriffsrichtlinie gültig wird, klicken Sie im Detailbereich der Verwaltungskonsole auf ÜBERNEHMEN. Prüfen Sie danach, ob sich die neue Regel an der korrekten Position befindet, wenn bereits andere Regeln definiert sind. Gegebenenfalls ändern Sie die Position der neuen Zugriffsrichtlinie über die Pfeiltasten.

Auf jedem ISA Server notwendig

Die eben beschriebenen Schritte müssen auf jedem ISA Server durchgeführt werden, von dem aus ein anderer ISA Server remote administriert werden soll.

6.2.8 Verwalten des ISA Server über den Remotecomputer

Dieses Kapitel beschreibt, wie Sie über die Verwaltungskonsole und den Terminalclient den ISA Server remote verwalten.

Verwaltung über die Verwaltungskonsole

Erfolgt die Remoteverwaltung des ISA Server über die Verwaltungskonsole, müssen Sie zu deren Durchführung folgende Schritte ausführen:

1. Wählen Sie aus dem Startmenü den Eintrag MICROSOFT ISA SERVER/ISA SERVER-VERWALTUNG.
2. In der Verwaltungskonsole markieren Sie den Eintrag MICROSOFT INTERNET SECURITY AND ACCELERATION SERVER 2004. Im Aufgabenbereich wechseln Sie auf die Registerkarte AUFGABEN und klicken auf VERBINDUNG HERSTELLEN MIT LOKALEM ODER REMOTE-ISA SERVER.
3. Sie erhalten das Fenster VERBINDUNG HERSTELLEN. Wählen Sie dort die Option ANDEREN COMPUTER (REMOTEVERWALTUNG) und geben entweder den Namen des ISA Server an oder klicken auf DURCHSUCHEN, um diesen zu finden (siehe Abbildung 6.7).

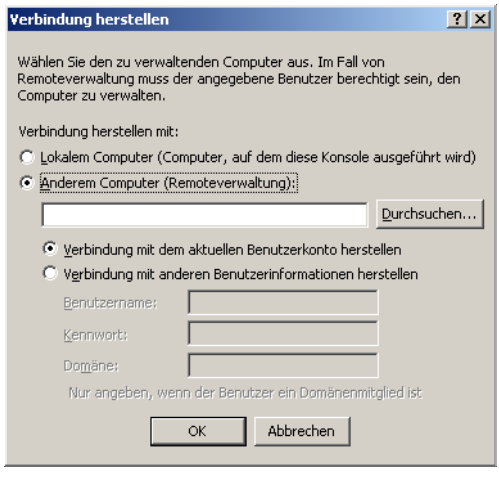


Abbildung 6.7: Herstellen einer Verbindung zur Verwaltung des ISA Server über einen Remotecomputer

4. Als Nächstes werden die Anmeldeinformationen angegeben. Deren Angabe unterscheidet sich danach, ob sich der Verwaltungscomputer und der ISA Server in derselben Domäne befinden oder in unterschiedlichen Domänen bzw. einer anderen Arbeitsgruppe.

   Mitgliedschaft in Arbeitsgruppe oder Domäne

   Sind beide Computer Mitglied derselben Domäne und verfügen Sie auf dem ISA Server über administrative Berechtigungen, wählen Sie die Option VERBINDUNG MIT DEM AKTUELLEN BENUTZERKONTO HERSTELLEN.

Ist der ISA Server Mitglied einer anderen Domäne oder einer Arbeitsgruppe, gibt es keinen Domänencontroller, der die Anmeldeinformationen kennt (Ausnahme: Es besteht eine Vertrauensstellung zwischen den Domänen). Wählen Sie in diesem Fall die Option VERBINDUNG MIT ANDEREN BENUTZERINFORMATIONEN HERSTELLEN und geben den Benutzernamen, das Kennwort sowie die Domäne oder Arbeitsgruppe für das Benutzerkonto an, das über die Berechtigung zur Verwaltung des ISA Server verfügt.

5. Nach erfolgreicher Authentifizierung können Sie an der Verwaltungskonsole wie an einem lokalen System den Remote-ISA Server verwalten.

Die eben beschriebenen Schritte müssen Sie separat an jedem Computer durchführen, von dem aus die Verwaltung des ISA Server über die Verwaltungskonsole erfolgen soll.

Verwaltung über die Terminaldienste

Erfolgt die Verwaltung über den Dienst des Terminalclients, müssen Sie zur Verwaltung die folgenden Schritte vornehmen:

1. Öffnen Sie im Startmenü die Einträge PROGRAMME/ZUBEHÖR/KOMMUNIKATION und wählen dort REMOTEDESKTOPVERBINDUNG.
2. Im Fenster REMOTEDESKTOPVERBINDUNG tragen Sie unter COMPUTER den Namen des ISA Server ein (siehe Abbildung 6.8).

Abbildung 6.8: Verbinden mit dem ISA Server über die Remotedesktopverbindung

3. Sobald die Verbindung hergestellt ist, müssen Sie den Benutzernamen und das Kennwort eingeben. Selbstverständlich muss dieses Benutzerkonto über die Berechtigungen zur Verwaltung des ISA Server verfügen.

Anzeige des ISA Server-Desktops

4. Wurde die Authentifizierung erfolgreich durchgeführt, wird der komplette Desktop des ISA Server angezeigt. Wählen Sie hier aus dem Startmenü die ISA SERVER-VERWALTUNG auf. Sie können nun mit der ISA-mmc wie an einem lokalen System arbeiten. Sie werden allenfalls je nach Verbindungsgeschwindigkeit leichte Verzögerungen bemerken.

6.2.9 Verbindungstrennung zum ISA Server

Sicherheitsaspekte

Bei der Remoteverwaltung sollten Sie aus Sicherheitsgründen immer daran denken, die Remote-Verbindung zum ISA Server wieder zu trennen, sobald Sie Ihre Aufgaben dort erledigt haben.

Verbindungstrennung beim Einsatz der Verwaltungskonsole

Soll die Verbindung vom ISA Server beim Einsatz der Verwaltungskonsole getrennt werden, führen Sie die folgenden Schritte durch.

1. Markieren Sie in der Verwaltungskonsole den Namen des ISA Server, zu dem die Verbindung getrennt werden soll.
2. Wechseln Sie im Aufgabenbereich auf die Registerkarte AUFGABEN und klicken dort auf AUSGEWÄHLTEN SERVER VON VERWALTUNGSKONSOLE TRENNEN. Bestätigen Sie im folgenden Dialogfeld die Nachfrage mit JA.

Verbindungstrennung beim Einsatz der Terminaldienste

Bei der Verwendung der Terminaldienste wird die Verbindung in folgender Weise getrennt:

1. Auf dem Remotecomputer klicken Sie im Fenster REMOTEDESKTOPVERBINDUNG auf START und dann auf ABMELDEN.
2. Sie erhalten das Fenster VON WINDOWS ABMELDEN. Dort klicken Sie auf ABMELDEN. Damit ist die Verbindung zum ISA Server getrennt.

6.2.10 Skriptausführung auf dem Remotecomputer

Vom Remotecomputer aus können auch Skripte für die effektivere Verwaltung des ISA Server, insbesondere bei immer wiederkehrenden Aufgaben, ausgeführt werden. Die Skripte verwenden zur Zugriffs-, Konfigurations- und Richtliniensteuerung oder zur Steuerung eines ISA Server-Arrays ISA Server-Verwaltungsobjekte.

Eine ausführliche Hilfe zum Erstellen dieser Verwaltungsskripte finden Sie in der Hilfe des *ISA Server SDK*, das auf der Begleit-CD mitgeliefert wird.

Je nachdem, ob ein Skript oder Programm auf dem Remotecomputer oder dem ISA Server ausgeführt wird, bestehen folgende Unterschiede:

- Die Skripte und Programme auf dem Remotecomputer müssen eine Verbindung zum ISA Server herstellen.
- Wird ein Skript auf dem Remotecomputer ausgeführt, muss das Stammobjekt *FPCDS* sein, anderenfalls *FPC*.

Folgend erhalten Sie eine kurze Anleitung zum Erstellen eines Stammobjekts für die Remoteverwaltung.

Unter JScript verwenden Sie folgenden Code:

```
objFPCROOT = new ActiveXObject ("FPCDS.Root");
```

Unter VBScript ist folgender Code erforderlich:

```
Set objFPC = CreateObject ("FPCDS.Root")
```

Unter Visual Basic gibt es zwei verschiedene Möglichkeiten:

```
Dim objFPC As New FPCLib.FPCDS
```

oder

```
Dim objFPC As New FPCLib.FPC
Set objFPC = CreateObject("FPCDS.Root")
```

Methode FPCArrays. Connect

Um die Verbindung mit dem ISA Server herzustellen, benutzen Sie die Methode *FPCArrays.Connect*. Diese Methode verwendet die folgenden Parameter:

- *Server* [in] BSTR, um den ISA Server anzugeben, zu dem die Verbindung hergestellt werden soll
- *UserName* [in, jedoch optional] BSTR, um einen Benutzernamen anzugeben. Der Standardwert ist eine leere Zeichenfolge (BSTR).
- *Domain* [in, jedoch optional] BSTR, um die Benutzerdomäne anzugeben. Der Standardwert ist eine leere Zeichenfolge (BSTR).
- *Password* [in, jedoch optional] BSTR, um das Kennwort anzugeben. Der Standardwert ist eine leere Zeichenfolge (BSTR).

Sobald ein Skript oder Programm abgearbeitet ist, wird die Verbindung zwischen dem Remotecomputer und dem ISA Server automatisch wieder getrennt.

6.3 Delegieren der Verwaltung

Wie im Active Directory

Zur Aufteilung von Verwaltungs- und Überwachungsaufgaben an mehrere Administratoren ist auch auf dem ISA Server 2004 eine Delegierung der Verwaltung an andere Benutzer oder Benutzergruppen möglich. Grundsätzlich entspricht die Delegierung hier der Delegierung von Verwaltungsaufgaben im Active Directory.

6.3.1 Rollen

Um die Delegierung zu vereinfachen, gibt es auf dem ISA Server drei verschiedene vordefinierte Rollen:

- ISA Server-Hauptadministrator
- ISA Server-Standardüberwachung
- Erweiterte ISA Server-Überwachung

Diese drei Rollen haben die folgende Bedeutung:

Rolle	Beschreibung
ISA Server-Hauptadministrator	Mitgliedern dieser Rolle ist es möglich, die komplette Konfiguration des ISA Server zu lesen und zu modifizieren. Da diese Rolle die meisten Berechtigungen beinhaltet, sollte diese Rolle lediglich einer geringen Anzahl von ISA-Administratoren mit ausreichend Erfahrung zugewiesen werden.
ISA Server-Standardüberwachung	Mitglieder dieser Rolle können den ISA Server überwachen. Dabei können zwar Einträge des Bereichs ÜBERWACHUNG angezeigt, jedoch nicht geändert werden.
Erweiterte ISA Server-Überwachung	Die Mitglieder dieser Rolle können sowohl die Einträge im Bereich ÜBERWACHUNG anzeigen, als auch ändern.

Tabelle 6.3: Übersicht über die Rollen zur Delegierung der Verwaltung

Um einen genaueren Überblick über die einzelnen Rechte zu erhalten, die die verschiedenen Rollen besitzen, finden Sie diese Informationen in der folgenden Tabelle aufgelistet.

Berechtigung	ISA Server-Hauptadministrator	ISA Server-Standardüberwachung	ISA Server-Überwachung
Anzeigen der Übersicht, Alarme, Sitzungen, Dienste und Konektivität	X	X	X
Erstellen von Berichten	X	-	X
Anzeigen von Protokollen	X	-	X
Alarme zurücksetzen und bestätigen	X	X	X
Alarme konfigurieren	X	-	X
Sitzungen und Dienste beenden und starten	X	-	X
Firewall-Richtlinie anzeigen	X	-	X
VPN-Konfiguration anzeigen	X	-	X
Exportieren der ISA Server-Konfiguration	X	-	X

Tabelle 6.4: In den einzelnen Rollen enthaltene Berechtigungen

Berechtigung	ISA Server-Hauptadministrator	ISA Server-Standardüberwachung	ISA Server-Überwachung
Exportieren, Importieren, Sichern und Wiederherstellen der ISA Server-Konfiguration	X	-	-
Firewall- und VPN-Richtlinie konfigurieren	X	-	-
Cache konfigurieren	X	-	-

6.3.2 Die Delegierung anwenden

Nur von ISA-Administratoren durchführbar

Die Delegierung der ISA Server-Verwaltung kann nur von Benutzern vorgenommen werden, die über die vollständige Berechtigung zur Verwaltung des ISA Server verfügen. Zur Verwaltungsdelegierung sind die folgenden Schritte erforderlich:

1. Markieren Sie in der ISA-mmc das Serverobjekt und wählen Sie in der Aufgabenliste ADMINISTRATIVE ROLLEN DEFINIEREN.
2. Es wird eine Liste der Rollen und deren Mitglieder angezeigt. Über HINZUFÜGEN können Sie neue Benutzer oder Gruppen auswählen, an die die Verwaltung delegiert werden soll (siehe Abbildung 6.9).

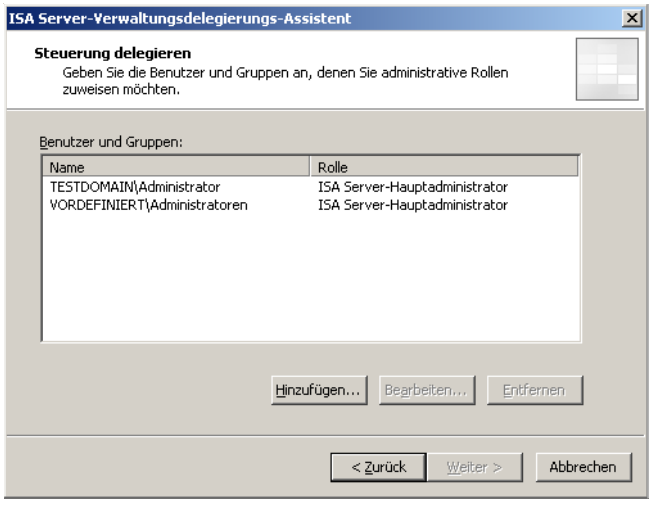


Abbildung 6.9: Übersicht über Benutzergruppen und deren Rollen zur Verwaltungsdelegierung

3. Haben Sie alle Benutzer zu den gewünschten Rollen hinzugefügt, beenden Sie den Assistenten und klicken im Detailbereich der mmc auf ÜBERNEHMEN, damit die neuen Einstellungen wirksam werden.

Um zu testen, ob die neuen Berechtigungen auch tatsächlich funktionieren, sollten Sie diese testen. Rufen Sie dazu die ISA-mmc im Startmenü auf, halten die Taste ⇧ gedrückt und wählen Sie den Kontext-

menüeintrag AUSFÜHREN ALS. Im gleichnamigen Fenster können Sie den Benutzernamen und das Kennwort angeben. Sie müssen sich in diesem Fall nicht erst vom System abmelden und unter einem anderen Benutzerkonto neu anmelden.

Wenn die Option AUSFÜHREN ALS direkt am Domänencontroller verwendet wird, muss das betreffende Benutzerkonto dort über die Berechtigung der lokalen Anmeldung verfügen.

6.4 Sicherung und Wiederherstellung

Die – am besten regelmäßige - Sicherung der ISA Server-Konfiguration sollte ebenso wie die regelmäßige Sicherung des zugrunde liegenden Betriebssystems zu den Standardaufgaben des Administrators gehören.

6.4.1 Sicherung

Nicht nur beim Serverausfall hilfreich

Eine Sicherung der Konfiguration ist nicht nur sinnvoll (oder besser gesagt notwendig), wenn der ISA Server ausgefallen ist. Selbst wenn es nicht möglich ist, den ursprünglichen Computer wiederherzustellen, kann die gesicherte Konfiguration auf einem anderen ISA Server wieder eingespielt werden – vorausgesetzt, die Sicherungsdatei wird auch regelmäßig auf einem anderen Computer gespeichert. Auch wenn nur bestimmte Teile der Konfiguration versehentlich falsch konfiguriert wurden, kann das Einspielen der Sicherung die schnellste Hilfsmaßnahme sein, wenn nicht mehr erkennbar ist, an welcher Stelle die falsche Konfiguration aufgetreten ist. Auch für eine externe Analyse von Problemen durch einen Dienstleister kann die gesicherte Konfigurationsdatei sehr gut verwendet werden.

Die Sicherung der Konfiguration erfolgt in einer *.xml*-Datei. Um die Sicherung durchzuführen, sind die folgenden Schritte erforderlich:

1. Markieren Sie in der ISA-mmc das ISA Server-Objekt und wählen Sie im Aufgabenbereich ISA SERVER-KONFIGURATION SICHERN.
2. Geben Sie dann für die Sicherung den Speicherort und einen Namen an. Idealerweise enthält dieser das Datum und die Uhrzeit, um später schneller die gewünschte Sicherungsdatei finden zu können. Zusätzlich müssen Sie ein Kennwort festlegen, das beim späteren Import der Datei abgefragt wird. Dieses Kennwort muss aus mindestens acht Zeichen bestehen.

   In der *.xml*-Datei werden einige Informationen verschlüsselt dargestellt. Dazu zählen RADIUS-Kennwörter, bereits installierte Schlüssel für L2TP/IPSec-Verbindungen oder Benutzernamen und Kennwörter für eine SQL-Protokollierung.

6.4.2 Wiederherstellung

Aktuelle Einstellungen werden überschrieben

Die Wiederherstellung der gesicherten Daten kann zu jedem beliebigen Zeitpunkt durchgeführt werden. Bedenken Sie, dass durch das Zurückspielen der Daten sämtliche aktuellen Einstellungen und Daten durch die Inhalte der Sicherung überschrieben werden.

Um die gesicherten Daten zu einem späteren Zeitpunkt wiederherstellen zu können, sind die folgenden Schritte durchzuführen:

1. In der ISA-mmc markieren Sie das ISA Server-Objekt und wählen im Aufgabenbereich ISA SERVER-KONFIGURATION WIEDERHERSTELLEN.
2. Wählen Sie dann die gewünschte *.xml*-Sicherungsdatei aus und geben Sie das zugehörige Passwort ein, damit die verschlüsselten Bereiche der Sicherungsdatei während der Wiederherstellung entschlüsselt werden können.
3. Klicken Sie dann auf ÜBERNEHMEN. Sie erhalten danach den Hinweis, dass der Firewalldienst neu gestartet werden muss. Führen Sie dies nach der Aufforderung durch.

6.5 Import und Export

Sicherung definierter Konfigurationselemente

Neben der Sicherung und Wiederherstellung des ISA Server ist der Import und Export der Konfigurationseinstellungen die zweite wichtige Verwaltungsaufgabe. Diese Aufgabe ähnelt prinzipiell der eben beschriebenen Sicherung und Wiederherstellung, allerdings besteht beim Import und Export die Möglichkeit, dass nur bestimmte Konfigurationen und Daten im- bzw. exportiert werden können, während bei der Sicherung und Wiederherstellung sämtliche Einstellungen verwendet werden. Beim Import und Export können die folgenden Konfigurationsdaten benutzt werden:

Tabelle 6.5: Im- und exportierbare Konfigurationseinstellungen des ISA Server

Snap-In der ISA-mmc	Im- oder exportierbare Konfiguration
Server	Komplette Konfiguration
Überwachung	Sitzungen/Filterdefinitionen, Konnektivität/Konnektivitätsverifizierungen und Protokollierung/Filterdefinitionen
Firewallrichtlinie	Alle Einstellungen, einzelne Regeln, Systemrichtlinie
VPN	Alle Einstellungen
Konfiguration	Sämtliche oder einzelne Netzwerke, Netzwerksätze, Netzwerkregeln, Webverkettungen und sämtliche oder einige Cache-Einstellungen

Vielfältige Einsatzzwecke

Deshalb macht es Sinn, die Import- und Exportfunktion zu benutzen, wenn nur ein bestimmter Konfigurationsbereich des ISA Server wiederhergestellt werden soll, andere Bereiche jedoch die aktuellen Einstellungen behalten sollen.

Auch für die schnelle Konfiguration eines neuen ISA Server können Sie den Import verwenden. Im Klonverfahren erhält so der neue Server sämtliche Konfigurationen des vorhandenen Servers.

Ein drittes sinnvolles Einsatzgebiet ist der Export der ISA-Konfiguration aus der Testumgebung in die produktive Umgebung. Nachdem die Konfiguration in der Testumgebung erfolgreich validiert wurde, sparen Sie sich viel Zeit und umgehen auch potenzielle Fehlerquellen, wenn die Konfiguration auf dem produktiven System nicht manuell, sondern durch den Import der Konfiguration durchgeführt wird.

6.5.1 Exportieren

Der Export der Daten erfolgt wie die Sicherung in einer *.xml*-Datei. Um den Export aller oder nur bestimmter Konfigurationseinstellungen durchzuführen, sind die folgenden Schritte erforderlich:

1. Öffnen Sie in der ISA-mmc ein Snap-In gemäß Tabelle 6.5.
2. Im Aufgabenfenster wechseln Sie auf die Registerkarte AUFGABEN und klicken auf den gewünschten Link zum Export.
3. Geben Sie dann einen Namen für die Exportdatei an. Um diese später besser identifizieren zu können, sollte der Dateiname den Inhalt sowie Datum und Uhrzeit enthalten.

   Im Gegensatz zur Sicherung haben Sie zusätzlich beim Export die Möglichkeit, zwei weitere Optionen zu wählen (siehe Abbildung 6.10). Dies ist jedoch abhängig von der gewählten zu exportierenden Konfiguration.

   - BENUTZERBERECHTIGUNGSEINSTELLUNGEN EXPORTIEREN: Haben Sie diese Checkbox markiert, werden zusätzlich auch delegierte Verwaltungsberechtigungen der Konfigurationsobjekte exportiert. Diese Option ist nur möglich, wenn unter dem Snap-In SERVER die komplette Konfiguration exportiert werden soll.
   - VERTRAULICHE INFORMATIONEN EXPORTIEREN (VERSCHLÜSSELUNG VERWENDEN): Ist diese Checkbox markiert, werden auch vertrauliche Informationen in den Export miteinbezogen. Allerdings ist aus Sicherheitsgründen die Angabe eines Kennworts erforderlich, das später zur Entschlüsselung der Daten beim Import anzugeben ist.

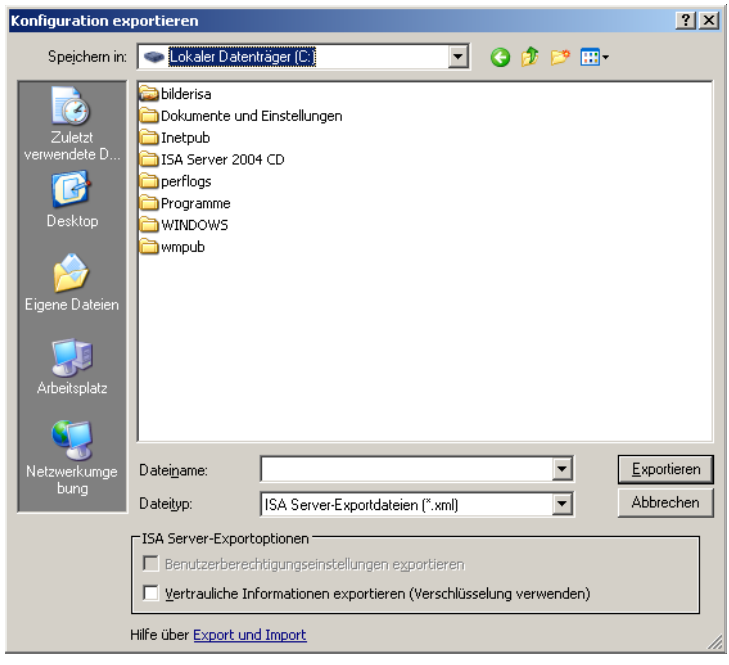


Abbildung 6.10: Zusätzliche Optionen beim Export einiger ISA-Konfigurationselemente

4. Abschließend klicken Sie auf EXPORTIEREN, um den Vorgang zu starten.

6.5.2 Importieren

Überschreiben aktueller Einstellungen

Bei einem Import werden die aktuellen Konfigurationseinstellungen wie bei einer Wiederherstellung ebenfalls überschrieben. Allerdings erfolgt im Gegensatz zur Wiederherstellung nur das Überschreiben der gewählten Einstellungen. Alle anderen Konfigurationen bleiben in ihrem ursprünglichen Zustand erhalten. So ist es auch möglich, zusätzliche Konfigurationen hinzuzufügen. Haben Sie beispielsweise auf einem ISA Server eine Zugriffsregel B exportiert und auf einem anderen ISA Server befindet sich nur die Zugriffsregel A, so wird die Regel B zur Konfiguration hinzugefügt. Zugriffsregel A bleibt weiterhin unverändert bestehen.

Nur beim Import der gesamten Konfiguration wird wie bei der Wiederherstellung die gesamte Konfiguration überschrieben.

Zum Import sind folgende Schritte notwendig:

1. Markieren Sie in der ISA-mmc das Snap-In, dessen Konfiguration importiert werden soll.
2. Wechseln Sie im Aufgabenfenster auf die Registerkarte AUFGABEN und klicken Sie den gewünschten Link für den Import an.

3. Suchen Sie die gewünschte Importdatei aus. Sofern möglich, wählen Sie die Optionen BENUTZERBERECHTIGUNGSEINSTELLUNGEN IMPORTIEREN und VERTRAULICHE INFORMATIONEN IMPORTIEREN (VERSCHLÜSSELUNG VERWENDEN).
4. Klicken Sie dann auf ÜBERNEHMEN. Möglicherweise erhalten Sie einen Hinweis, dass der Firewalldienst neu gestartet werden muss, dies hängt jedoch von den importierten Konfigurationsdaten ab. Sofern ein Neustart des Dienstes erforderlich ist, führen Sie diesen jetzt durch.

7 Richtlinien und Regeln

Dieses Kapitel beschäftigt sich mit den Firewallrichtlinien. Diese Richtlinien bilden eine wichtige Grundlage für die Konfiguration des ISA Server. Bevor jedoch mit der Konfiguration dieser Regeln begonnen werden kann, muss gewährleistet sein, dass alle internen und externen Netzwerke sowie möglicherweise vorhandenen DMZs korrekt im ISA Server konfiguriert sind, da die Richtlinien ansonsten nicht korrekt angewendet werden können. Des Weiteren wird zuvor noch die ISA-Toolbox beschrieben, die die Konfiguration von Protokollen, Richtlinien usw. stark vereinfacht.

7.1 Die ISA-Toolbox

Hier werden vorab sämtliche Konfigurationsobjekte angelegt

Eine wichtige und sehr hilfreiche Neuerung gegenüber der Verwaltungskonsole des ISA Server 2000 ist die TOOLBOX, die Sie im Aufgabenbereich der ISA-mmc finden. Dort sind übersichtlich in einer Liste sämtliche Elemente (PROTOKOLLE, BENUTZER, INHALTSTYPEN, ZEITPLÄNE und NETZWERKOBJEKTE) zusammengefasst, die zum Erstellen der Zugriffsregeln notwendig sind (siehe Abbildung 7.1). In der Toolbox können diese Elemente einmalig zentral schnell und effektiv vorkonfiguriert werden, so dass diese später nur in die entsprechenden Regeln oder Richtlinien eingefügt werden müssen. Um dieses Fenster aufzurufen, müssen Sie das Snap-In FIREWALLRICHTLINIE markieren.

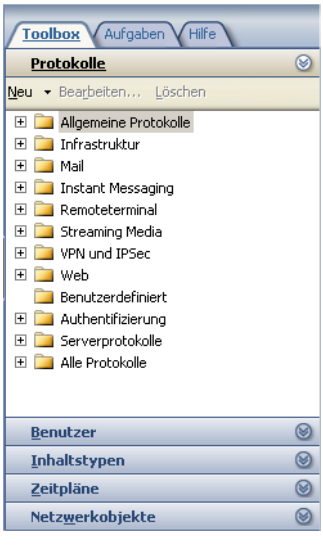


Abbildung 7.1: Die Toolbox als Teil der Verwaltungskonsole

Die folgenden Kapitel zeigen, wie diese Elemente in der Toolbox vorkonfiguriert werden können.

7.1.1 Protokolle

Über 100 Protokolldefinitionen

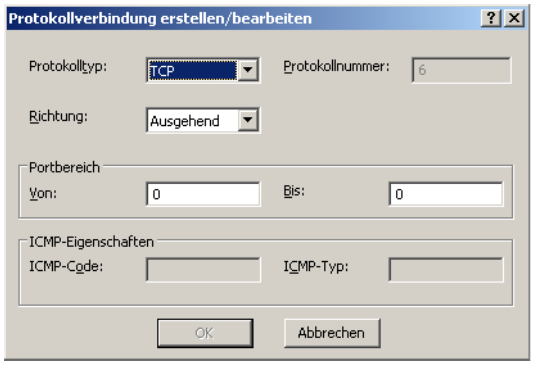
Wie Sie in Abbildung 7.1 sehen, sind dort die Netzwerkprotokolle bereits nach Typen gruppiert. Insgesamt verfügt der ISA Server 2004 über 100 verschiedene Protokolldefinitionen. Benötigen Sie zu diesen bereits vorhandenen Protokolldefinitionen noch weitere, so können diese zusätzlich erstellt werden. Für die Protokolldefinition werden zwei verschiedene Protokollarten verwendet, nämlich RPC-Protokolle und Nicht-RPC-Protokolle.

Nicht-RPC-Protokolle

Wie es der Name schon sagt, werden in dieser Kategorie alle Protokolle zusammengefasst, die nicht RPC verwenden. Um ein solches Protokoll hinzuzufügen, müssen Sie die folgenden Schritte durchführen:

1. Klicken Sie in der Toolbox auf PROTOKOLLE und dann auf das Menü NEU/PROTOKOLL.
2. Geben Sie einen Namen für das zusätzliche Protokoll an.
3. Danach wird das Protokoll näher definiert. Klicken Sie unter PRIMÄRE VERBINDUNGSINFORMATIONEN auf NEU. Im Fenster PROTOKOLLVERBINDUNG ERSTELLEN/BEARBEITEN (siehe Abbildung 7.2) wird der Port bzw. ein Bereich von mehreren Ports bestimmt, die das Protokoll verwenden. Zusätzlich ist die Richtung des Protokolls sowie die Basis (TCP = verbindungsorientiert oder UDP = verbindungslos) zu definieren. Bestätigen Sie die Werte mit OK und klicken dann auf WEITER.

Abbildung 7.2: In diesem Fenster werden weitere Angaben zum neuen Protokoll gemacht



4. Im folgenden Fenster SEKUNDÄRE VERBINDUNGEN (siehe Abbildung 7.3) wählen Sie, ob das Protokoll sekundäre Verbindungen verwendet. Ist dies der Fall, markieren Sie die Option JA, klicken auf NEU und tragen den Port oder Portbereich der sekundären Verbindung ein.

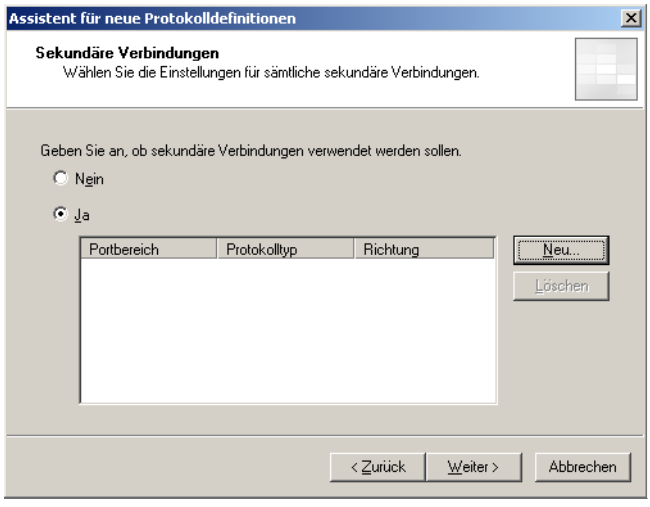


Abbildung 7.3: Einstellungen für eine optionale sekundäre Verbindung

Man spricht von einer sekundären Verbindung, wenn ein Netzwerkprotokoll für die Kommunikation einen anderen Port verwendet als den Port, der für den Aufbau der Verbindung verwendet wird.

5. Klicken Sie dann auf WEITER und beenden Sie den Assistenten. Das hinzugefügte Protokoll wird in der Toolbox unter PROTOKOLLE/BENUTZERDEFINIERT angezeigt.

RPC-Protokolle

Port 135 und dynamische Ports

Im Gegensatz zu den eben beschriebenen normalen Protokollen werden sämtliche RPC-Protokolle vom Client aus über Port 135 angestoßen. Der ISA Server nimmt die Client-Anfrage an und weist dem Client dynamisch einen bestimmten Port für die Verbindung zu. Stellt der Client weitere Anfragen, verwendet er dazu den dynamisch vom Server zugewiesenen Port.

Vom ISA Server werden drei verschiedene Protokolldefinitionen für RPC-Protokolle bereitgestellt:

- *RPC (Alle Schnittstellen)*: Interne Clients können auf den gesamten ausgehenden Verkehr auf RPC-basierte Dienste eines anderen Netzwerks zugreifen, beispielsweise im Internet.
- *RPC-Server (Alle Schnittstellen)*: RPC-basierte Dienste können im internen Netzwerk oder in einem Perimeternetzwerk veröffentlicht werden.
- *Exchange-RPC-Server*: *Exchange Server* können sicher veröffentlicht werden, so dass die Clients des internen Netzwerks nicht über OWA auf den *Exchange Server*, sondern direkt, z.B. über *Outlook 2003*, auf die Dienste des *Exchange Server* Zugriff haben.

Wie schon bei den Nicht-RPC-Protokollen können auch hier zusätzliche Protokolle hinzugefügt werden. Dies geschieht auf folgende Weise:

1. Klicken Sie in der Toolbox auf PROTOKOLLE und dann auf das Menü NEU/RPC-PROTOKOLL.
2. Geben Sie einen Namen für das zusätzliche Protokoll an.
3. Im Fenster SERVER AUSWÄHLEN (siehe Abbildung 7.4) wählen Sie die Option SCHNITTSTELLEN AUSWÄHLEN und geben dann den Namen des Servers an, der veröffentlicht werden soll. Alternativ kann die RPC-UUID des Servers auch manuell bestimmt werden. Klicken Sie dann auf WEITER.

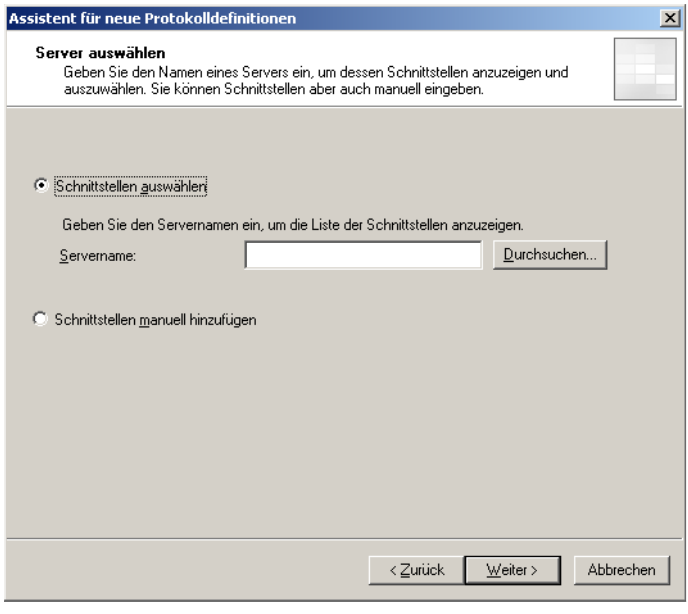


Abbildung 7.4: Auswahl des Servers und der Schnittstellen für das RPC-Protokoll

4. Tragen Sie dann bei der Wahl von SCHNITTSTELLEN MANUELL HINZUFÜGEN im Fenster SCHNITTSTELLEN HINZUFÜGEN/ENTFERNEN (siehe Abbildung 7.5) die UUID der Schnittstelle sowie deren Namen ein. Des Weiteren ist festzulegen, ob die Schnittstelle auf einem dynamisch zugewiesenen Port oder einem bestimmten Port veröffentlicht werden soll. Klicken Sie dann auf OK.
5. Klicken Sie dann auf WEITER und beenden Sie den Assistenten. Das hinzugefügte Protokoll wird in der Toolbox unter PROTOKOLLE/BENUTZERDEFINIERT angezeigt.

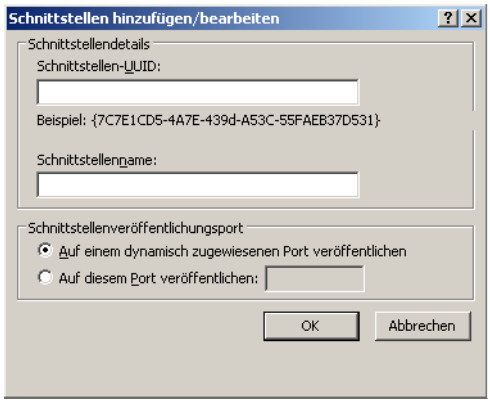


Abbildung 7.5: Manuelles Bestimmen der Schnittstelle

Sollen die im Assistenten definierten Eigenschaften zu einem späteren Zeitpunkt geändert werden, wählen Sie die EIGENSCHAFTEN des Protokolls und bearbeiten diese. Des Weiteren können über die Registerkarte PARAMETER auch Anwendungsfilter zu einem Protokoll hinzugefügt werden. Weitere Hinweise zu Anwendungsfiltern finden Sie in Kapitel 9.

7.1.2 Benutzersätze

Auf Benutzersätze werden die Regeln angewendet

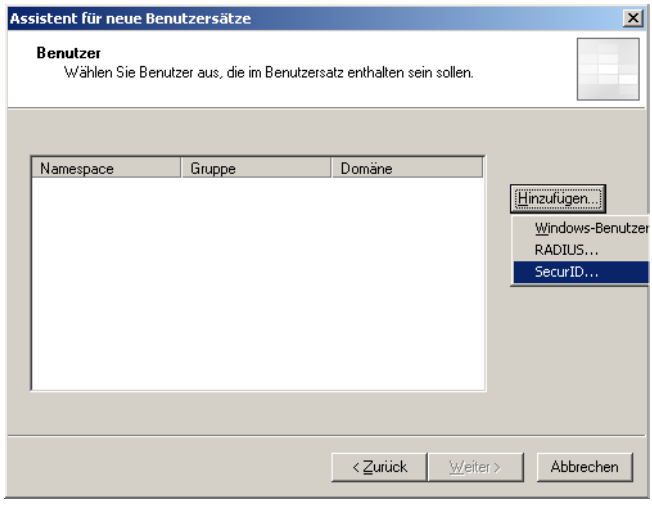
Ein weiteres wichtiges Element zur Steuerung und Umsetzung der definierten Firewall-Regeln sind die Benutzersätze. Ein Benutzersatz umfasst eine Reihe von Benutzern oder Benutzergruppen oder, wenn auch eher selten, nur einen einzelnen Benutzer. So ist es möglich, dass bestimmte Regeln nur für bestimmte Benutzer oder Gruppen gelten sollen. Dazu stellt der ISA Server 2004 bereits die folgenden drei vordefinierten Benutzersätze zur Verfügung:

- *Alle authentifizierten Benutzer*: Zu diesem Benutzersatz zählen alle Benutzer, die sich erfolgreich am ISA Server authentifiziert haben. Da SecureNAT-Clients keine Anmeldeinformationen an den ISA Server übertragen können, ist eine Authentifizierung dieser Clients nicht möglich. Dies gilt jedoch nicht, wenn der SecureNAT-Client gleichzeitig auch als Webproxy- oder Firewallclient konfiguriert ist oder die Authentifizierung des SecureNAT-Clients über VPN erfolgt.
- *Alle Benutzer*: In diesem Benutzersatz sind neben den authentifizierten Benutzern auch alle nicht authentifizierten Benutzer enthalten.
- *System- und Netzwerkdienst*: Dieser Benutzersatz wird nur für die Systemrichtlinien verwendet. In diesem sind die beiden Windows-Dienste *System* und *Netzwerk* enthalten.

Zusätzlich zu diesen drei vordefinierten Benutzersätzen können Sie weitere hinzufügen. Führen Sie dazu die folgenden Schritte aus:

1. Klicken Sie in der Toolbox auf BENUTZER und dann auf das Menü NEU.
2. Geben Sie einen Namen für den zusätzlichen Benutzersatz an.
3. Im Fenster BENUTZER (siehe Abbildung 7.6) klicken Sie auf HINZUFÜGEN. Sie können wahlweise WINDOWS-BENUTZER UND -GRUPPEN, RADIUS oder SECURID hinzufügen. Soll ein Windows-Benutzer oder eine Windows-Benutzergruppe hinzugefügt werden, müssen Sie den Namen des Kontos sowie der Domäne angeben, in der sich das betreffende Konto befindet. RADIUS- und SecureID-Benutzer werden unter Angabe des jeweiligen Benutzernamens hinzugefügt. Allerdings muss dazu bereits eine entsprechende Umgebung vorhanden sein.

Abbildung 7.6: Hinzufügen eines neuen Benutzersatzes



4. Klicken Sie dann auf WEITER und beenden Sie den Assistenten.

7.1.3 Inhaltstypen

Nur für http- und ftp-Verkehr

Unter Inhaltstypen versteht man eine Zusammenfassung von Inhalten bzw. Typen (z.B. MIME-Inhaltstypen oder Dateitypen). Allerdings kann nur bei http-Verkehr sowie getunneltem FTP-Verkehr eine Prüfung der Inhalte sowie ein daraus resultierendes Zulassen oder Verweigern des Inhaltsaufrufs angewendet werden.

Um zu den bereits definierten Inhaltstypen eigene hinzuzufügen, sind folgende Schritte erforderlich:

1. Klicken Sie in der Toolbox auf INHALTSTYPEN und dann auf das Menü NEU.

2. Im Fenster NEUER INHALTSTYPENSATZ (siehe Abbildung 7.7) geben Sie einen Namen sowie eine Beschreibung des neuen Satzes an. Aus der Liste VERFÜGBARE TYPEN wählen Sie die gewünschten Inhaltstypen aus und klicken auf HINZUFÜGEN. Sobald Sie mit OK bestätigt haben, wird der neue Inhaltstyp in der Liste der Toolbox verfügbar.

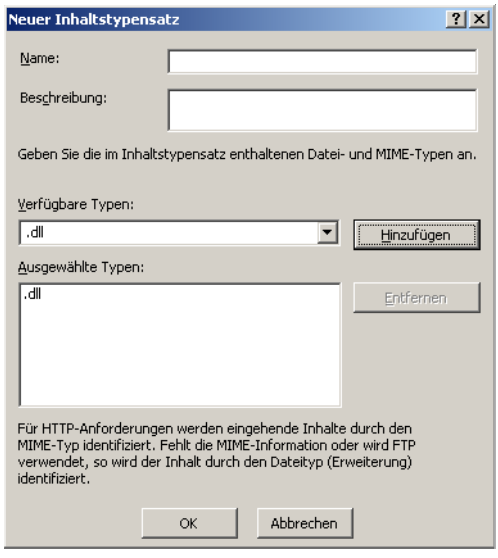


Abbildung 7.7: Erstellen eines neuen Inhaltstyps

7.1.4 Zeitpläne

Anpassungen der Zeitpläne möglich

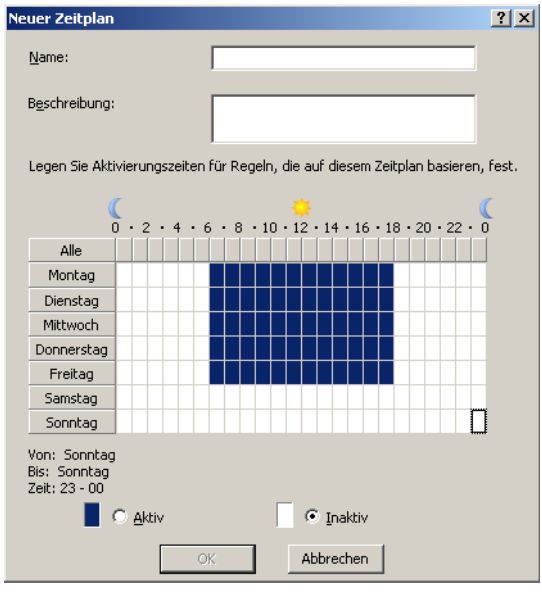
Die Nutzung eines Zeitplans ist sinnvoll, wenn Regeln nur zu bestimmten Zeiten gelten sollen. So kann beispielsweise festgelegt werden, dass zu den Kernarbeitszeiten kein Webzugriff für die Clients erfolgen darf oder nur der Zugriff auf bestimmte Seiten und Inhalte. Der ISA Server bietet dazu bereits die beiden folgenden vordefinierten Zeitpläne:

- *Normale Arbeitszeit*: Dieser Zeitplan umfasst an den Werktagen Montag bis Freitag die Zeiten von 9:00 h bis 17:00 h. Es ist jedoch möglich, diesen Zeitplan an die Gegebenheiten des Unternehmens über die Eigenschaften anzupassen.
- *Wochenende*: Dieser Zeitplan umfasst den kompletten Samstag und Sonntag.

Soll ein neuer Zeitplan definiert werden, führen Sie folgende Schritte aus:

1. Klicken Sie in der Toolbox auf ZEITPLÄNE und dann auf das Menü NEU.
2. Geben Sie im Fenster NEUER ZEITPLAN (siehe Abbildung 7.8) einen Namen und eine Beschreibung für den zusätzlichen Zeitplan an. Markieren Sie dann die gewünschten Zeiten und wählen, ob diese aktiv oder inaktiv sein sollen. Bestätigen Sie mit OK.

Abbildung 7.8: Erstellen eines neuen Zeitplans



7.1.5 Netzwerke

Logische Gruppierungen der Computer

Das letzte Element, das über die Toolbox vordefiniert werden kann, sind die Netzwerkobjekte. Dazu zählen beispielsweise Netzwerke, Netzwerksätze, Subnetze, Computer usw. Jedes dieser Objekte wird über einen eigenen Assistenten oder ein eigenes Fenster hinzugefügt oder bearbeitet. Diese Objekte werden in den folgenden Kapiteln näher vorgestellt, beginnend mit den Netzwerken.

Ein Netzwerk ist eine Zusammenfassung mehrerer Computer. Es kann bestimmt werden, zwischen welchen Netzwerken welche Art von Verkehr gestattet ist. Die folgenden vordefinierten Netzwerke sind bereits verfügbar:

- *Extern*: Diesem Netzwerk werden kurz gesagt sämtliche Netzwerke zugeordnet, die nicht zu einem der anderen Netzwerke oder zu einem Perimeternetzwerk gehören. Ein externes Netzwerk befindet sich immer außerhalb des ISA Server.
- *Intern*: In diesem Netzwerk befinden sich alle internen Clients und sonstigen Netzwerkgeräte. Dieses Netzwerk wird bereits während der Installation des ISA Server basierend auf den IP-Adressbereichen eingerichtet. Allein dieses Netzwerk gilt als vertrauenswürdig. Ein Perimeternetzwerk gehört nicht zum internen Netzwerk.
- *Lokaler Host*: Zum Netzwerk *Lokaler Host* gehört lediglich der ISA Server selbst. Über dieses Netzwerk wird geregelt, welcher Netzwerkverkehr zum ISA Server hin bzw. von diesem ausgehend gestattet ist.

- *Quarantäne-VPN-Clients*: Die Mitglieder dieses Netzwerks können sich im Gegensatz zu den bisher genannten dynamisch ändern. Sobald ein VPN-Client eine Verbindung mit dem Unternehmensnetzwerk herstellen möchte, wird anhand eines Skripts geprüft, ob der VPN-Client definierten Sicherheitsansprüchen des Netzwerks genügt oder nicht (z.B. müssen bestimmte Patches installiert oder ein Virenscanner vorhanden sein). Erst wenn der Client diese Voraussetzungen erfüllt hat, wird er automatisch in das Netzwerk *VPN-Clients* verschoben. Solange sich Clients in diesem Netzwerk befinden, sind sie sehr stark in ihren Berechtigungen eingeschränkt.
- *VPN-Clients*: In diesem Netzwerk befinden sich die VPN-Clients, die sich nicht mehr in Quarantäne befinden und über eine Verbindung zum Unternehmensnetzwerk verfügen. Da zu diesem Netzwerk alle Clients automatisch hinzugefügt werden, die die Quarantäne-Anforderungen erfüllen, sind auch hier die Mitgliedschaften dynamisch.

Netzwerke hinzufügen und bearbeiten

Zusätzliche Netzwerke wie Perimeternetzwerk

Zusätzlich können Sie noch weitere Netzwerke hinzufügen. Dies kann erforderlich werden, wenn Sie beispielsweise ein zweites internes Netzwerk oder ein Perimeternetzwerk verwenden. Um ein neues Netzwerk hinzuzufügen, sind die folgenden Schritte erforderlich:

1. Klicken Sie in der Toolbox auf NETZWERKOBJEKTE und dann auf das Menü NEU/NETZWERK.
2. Geben Sie einen Namen für das zusätzliche Netzwerk an.
3. Im Fenster NETZWERKTYP (siehe Abbildung 7.9) können Sie einen der vier folgenden Typen wählen: INTERNES NETZWERK, UMKREISNETZWERK, VPN-STANDORT-ZU-STANDORT-NETZWERK oder EXTERNES NETZWERK. Zu jedem dieser Typen wird eine kurze Beschreibung angegeben. Klicken Sie dann auf WEITER.

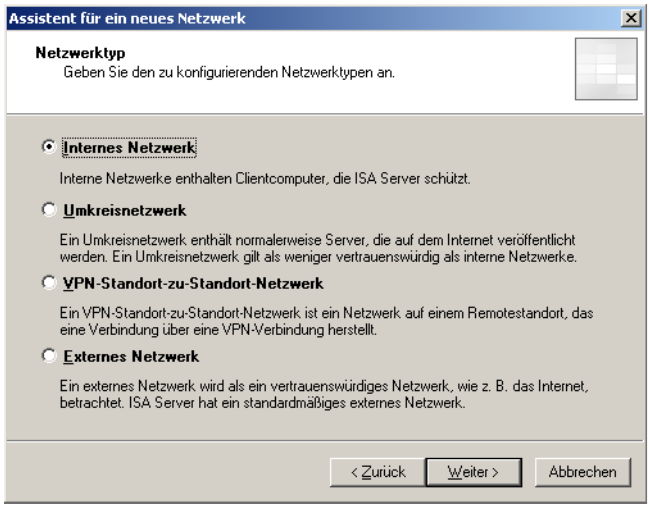


Abbildung 7.9: Bestimmen des Netzwerktyps für das neue Netzwerk

4. Als Nächstes wird der Adressbereich für das Netzwerk festgelegt (siehe Abbildung 7.10). Dies geschieht über die Schaltfläche HINZUFÜGEN. Vorhandene Einträge können über BEARBEITEN oder ENTFERNEN modifiziert werden. Wählen Sie hingegen ADAPTER HINZUFÜGEN, selektieren Sie eine Netzwerkkarte des ISA Server. Die Zuordnung erfolgt in diesem Fall basierend auf der Routingtabelle des ISA Server. Möchten Sie vordefinierte private Adressbereiche für das Netzwerk verwenden, können Sie diese Bereiche über PRIVATER ADAPTER auswählen. Bestätigen Sie Ihre Eingaben und beenden Sie den Assistenten. Das neu erstellte Netzwerk wird danach in der Liste der vorhandenen Netzwerke angezeigt.

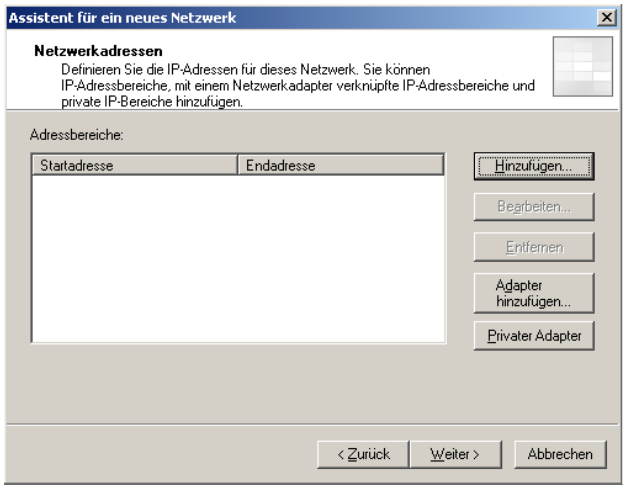


Abbildung 7.10: Festlegen der IP-Adressen, die zu dem neuen Netzwerk gehören

Sobald das Netzwerk hinzugefügt wurde, können dessen Einstellungen über die EIGENSCHAFTEN weiter bearbeitet werden. In den EIGENSCHAFTEN sind die folgenden Registerkarten verfügbar:

- ADRESSEN: In diesem Bereich werden die IP-Adressen der Netzwerke konfiguriert, so dass der ISA Server und die Clients wissen, welche Computer zu welchem Netzwerk gehören.
- DOMÄNEN: Hier werden Domänennamen angegeben, die lediglich in dem gewählten Netzwerk benutzt werden.
- WEBBROWSER: Auf dieser Registerkarte werden die Clienteinstellungen bezüglich des Webbrowsers konfiguriert.
- WEBPROXY: Nur wenn in dem Netzwerk Webproxy-Clients verwendet werden, muss auf dem ISA Server der entsprechende Listener aktiviert werden.
- FIREWALLCLIENT: Sofern in dem Netzwerk Firewall-Clients benutzt werden, muss auf dem ISA Server ebenfalls der entsprechende Listener aktiviert werden.
- AUTOMATISCHE ERKENNUNG: Ist die automatische Erkennung aktiviert, können die Firewall- und Webproxy-Clients automatisch konfiguriert werden.

Netzwerke konfigurieren

Verknüpfen von Netzwerken

Sie haben bereits gelesen, wie ein neues Netzwerk hinzugefügt und dessen Eigenschaften bearbeitet werden. Allerdings müssen Sie das neue Netzwerk mit anderen Netzwerken verknüpfen. Diese Verknüpfung erfolgt mit Hilfe von Netzwerkregeln. Erst wenn Netzwerke über diese Regeln miteinander verknüpft sind, können sie miteinander kommunizieren. Der ISA Server kann nur zu einem solchen Netzwerk Pakete von einem anderen Netzwerk für die Kommunikation weiterleiten.

Um diese Verknüpfung zu realisieren, ist Folgendes zu tun:

1. Markieren Sie in der ISA-mmc unter KONFIGURATION den Eintrag NETZWERKE. Dort wechseln Sie auf die Registerkarte NETZWERKREGELN. Dort werden die vorhandenen Verknüpfungen der Netzwerke angezeigt (siehe Abbildung 7.11).

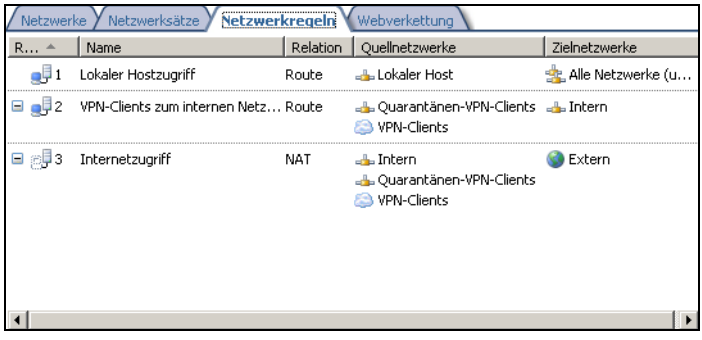


Abbildung 7.11: Übersicht über die vorhandenen Netzwerkregeln

2. Sie sehen, dass das neue Netzwerk in der obersten Regel LOKALER HOSTZUGRIFF bereits automatisch vorhanden ist, da als ZIELNETZWERKE der Wert ALLE NETZWERKE gesetzt ist. Dies liegt darin begründet, dass der ISA Server als alleiniges Mitglied des Netzwerks LOKALER HOST mit allen anderen Netzwerken kommunizieren muss.

   Um für das neue Netzwerk beispielsweise den Internetzugriff zu ermöglichen, muss eine neue Netzwerkregel erstellt werden. Öffnen Sie dazu den Kontextmenüeintrag EIGENSCHAFTEN der Regel INTERNETZUGRIFF.

3. Wechseln Sie dort auf die Registerkarte QUELLNETZWERKE und fügen Sie das neue Netzwerk zur Liste hinzu (siehe Abbildung 7.12). Klicken Sie dann auf OK.

4. Damit die Clients des internen Netzwerks auf das neue Netzwerk und umgekehrt zugreifen können, müssen diese beiden Netzwerke miteinander verknüpft werden. Wechseln Sie dazu wieder auf die Registerkarte NETZWERKREGELN und wählen Sie aus der Aufgabenliste NEUE NETZWERKREGEL ERSTELLEN.

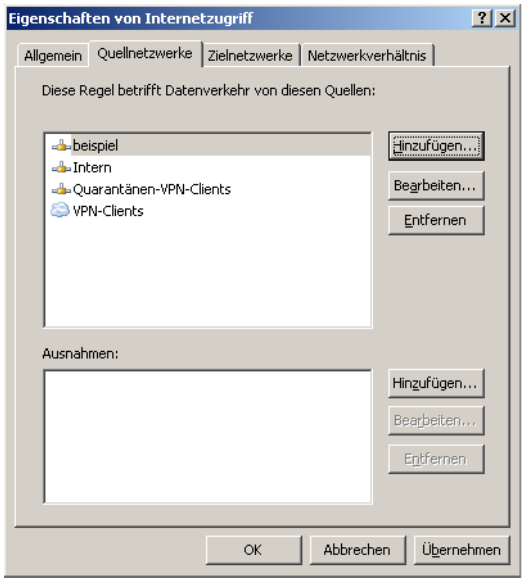


Abbildung 7.12: Hinzufügen der Quellnetzwerke für den Internetzugriff

5. Geben Sie der neuen Regel einen Namen.
6. Als Nächstes wird das Quellnetzwerk für die Kommunikation bestimmt. Dort ist das Netzwerk INTERN zu wählen.
7. Danach wird das Zielnetzwerk festgelegt. Dort geben Sie den Namen des neu erstellten Netzwerks an.
8. Im folgenden Fenster NETZWERKVERHÄLTNIS (siehe Abbildung 7.13) wird festegelegt, wie die Weiterleitung der Daten zwischen den beiden Netzwerken erfolgen soll. Dazu gibt es die beiden Möglichkeiten NAT (NETWORK ADDRESS TRANSLATION) und ROUTE.

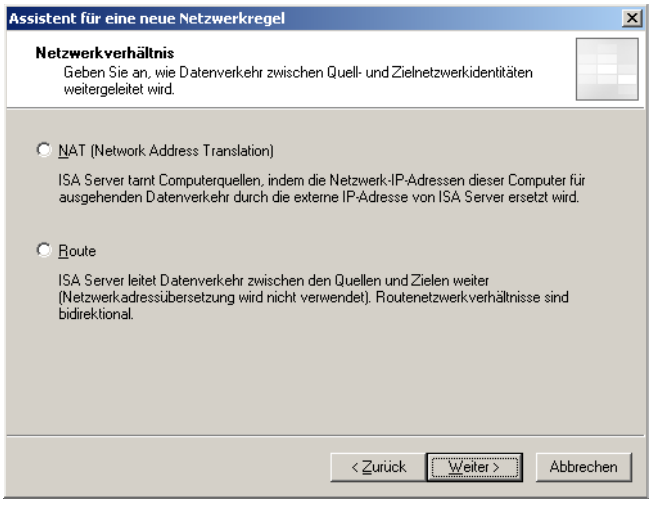


Abbildung 7.13: Wahl zwischen NAT und Route für die Weiterleitung des Datenverkehrs

Private oder öffentliche IP-Adressen

Wählen Sie NAT, wenn in dem einen Netzwerk private, in dem anderen Netzwerk öffentliche IP-Adressen verwendet werden, so dass der ISA Server die Adressen zur Weiterleitung der Pakete übersetzt. Eine NAT-Verbindung besteht zwischen dem internen und dem externen Netzwerk (Internet). Verfügen hingegen beide Netzwerke über private oder öffentliche Adressen, so muss keine Adressübersetzung zur Weiterleitung der Pakete erfolgen. Wählen Sie in diesem Fall die Option ROUTE. Eine Route-Verbindung besteht zwischen den Netzwerken Intern und VPN-Clients.

9. Beenden Sie den Assistenten und klicken Sie dann auf ÜBERNEHMEN. Ab diesem Zeitpunkt ist die Kommunikation möglich. Zur Steuerung des erlaubten und verweigerten Netzwerkverkehrs müssen noch Zugriffsregeln erstellt werden. Dieser werden näher in Kapitel 8 vorgestellt.

7.1.6 Netzwerksätze

Zusammenfassung mehrerer Netzwerke

In einem Netzwerksatz werden mehrere Netzwerke zu Gruppen zusammengefasst. Diese Zusammenfassung ist dann sinnvoll, wenn für mehrere einzelne Netzwerke dieselben Regeln zugewiesen werden sollen. Die Netzwerksätze vereinfachen somit die Konfiguration. Standardmäßig verfügt der ISA Server bereits über zwei verschiedene Netzwerksätze:

- *Alle geschützten Netzwerke*: In diesem Netzwerksatz befinden sich alle Netzwerke außer dem Netzwerk Extern. Dieser Netzwerksatz kann nicht modifiziert werden.
- *Alle Netzwerke (und lokaler Host)*: In diesem Netzwerksatz sind alle auf dem ISA Server erstellten Netzwerke vorhanden.

Um einen neuen Netzwerksatz hinzuzufügen, sind die folgenden Schritte erforderlich.

1. Öffnen Sie in der Toolbox die NETZWERKOBJEKTE und wählen Sie das Menü NEU/NETZWERKSATZ.
2. Geben Sie einen Namen für den neuen Netzwerksatz an.
3. Im Fenster NETZWERKAUSWAHL (siehe Abbildung 7.14) markieren Sie entweder alle Netzwerke, die zum neuen Netzwerksatz hinzugefügt werden sollen, und wählen die Option ENTHÄLT ALLE AUSGEWÄHLTEN NETZWERKE oder Sie markieren die Netzwerke, die nicht enthalten sein sollen, und wählen die Option ENTHÄLT ALLE NETZWERKE MIT AUSNAHME DER AUSGEWÄHLTEN NETZWERKE.

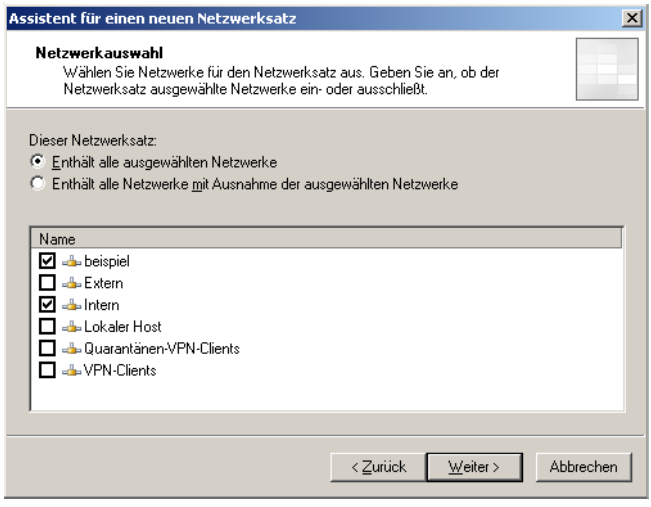


Abbildung 7.14: Hinzufügen von Netzwerken zu einem Netzwerksatz

4. Klicken Sie dann auf WEITER und beenden Sie den Assistenten. Vergessen Sie nicht, mit ÜBERNEHMEN die Konfiguration zu aktualisieren.

7.1.7 Computer

Beliebiger Netzwerkcomputer

Unter dem Regelelement *Computer* versteht man einen beliebigen einzelnen Computer eines Netzwerks. Die Anwendung dieses Elements ist sinnvoll, wenn für einen bestimmten Computer eines Netzwerks andere Regeln gelten sollen als für den Rest. Führen Sie die folgenden Schritte durch, um ein neues Regelelement *Computer* hinzuzufügen:

1. Öffnen Sie in der Toolbox die NETZWERKOBJEKTE und wählen Sie das Menü NEU/COMPUTER.
2. Geben Sie im Fenster NEUES COMPUTERREGELELEMENT (siehe Abbildung 7.15) den Namen und die IP-Adresse des Computers an. Optional kann noch eine Beschreibung hinzugefügt werden.

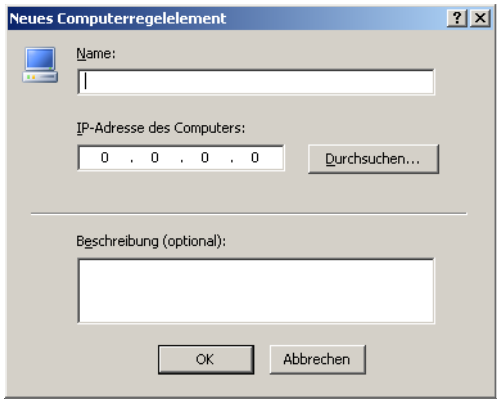


Abbildung 7.15: Erstellen des Regelelements Computer

7.1.8 Adressbereiche

Teile von Subnetzen

Im Regelelement *Adressbereiche* werden Bereiche von IP-Adressen zusammengefasst, auf die bestimmte Regeln angewendet werden sollen. Befinden sich mehrere einzelne Computer in einem bestimmten Adressbereich, so ist der Einsatz dieses Regelelements einfacher als das einzelne Hinzufügen aller dort enthaltenen Computer.

Fügen Sie den neuen Adressbereich in folgender Weise hinzu:

1. Öffnen Sie in der Toolbox die NETZWERKOBJEKTE und wählen das Menü NEU/ADRESSBEREICH.
2. Geben Sie dann im Konfigurationsfenster (siehe Abbildung 7.16) einen Namen sowie die Start- und Ziel-IP-Adresse des Adressbereichs an. Optional kann auch eine Beschreibung hinzugefügt werden.

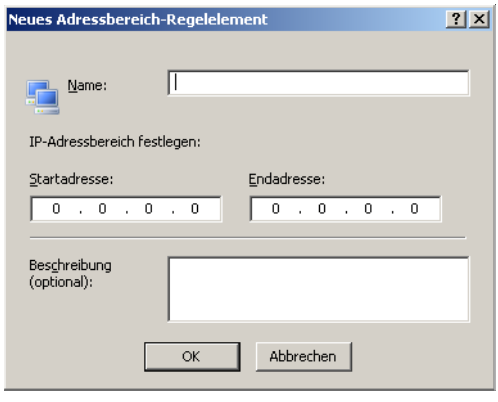


Abbildung 7.16: Erstellen des Regelelements Adressbereich

7.1.9 Subnetze

Vollständige Subnetze

Das Regelelement Subnetz repräsentiert ein vollständiges Subnetz, z.B. 192.168.2.0. Auf diese Weise können Regeln auf komplette Subnetze angewendet werden. Um ein neues Subnatz hinzuzufügen, sind die folgenden Schritte erforderlich:

1. Öffnen Sie in der Toolbox die NETZWERKOBJEKTE und wählen Sie das Menü NEU/SUBNETZ.
2. Geben Sie im Fenster NEUES SUBNETZREGELELEMENT (siehe Abbildung 7.17) einen Namen für das Subnetz an. Geben Sie des Weiteren die Netzwerkadresse sowie die zugehörige Subnetzmaske und optional noch eine Beschreibung an.

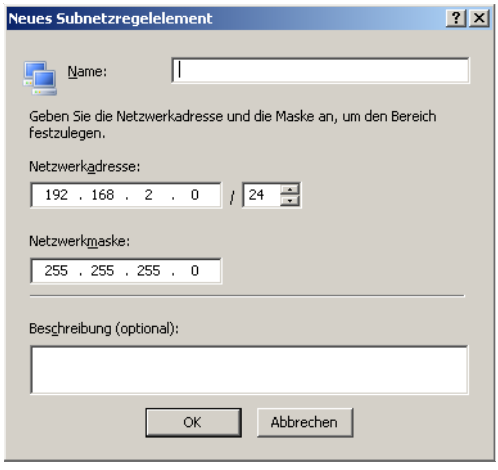


Abbildung 7.17: Erstellen des Regelelements Subnetz

7.1.10 Computersätze

Computer, Adressbereiche oder Subnetze

Unter dem etwas irreführenden Namen Computersatz versteht man Sammlungen von Computern, Adressbereichen oder Subnetzen. Dieses Regelelement wird beispielsweise verwendet, wenn identische Regeln für bestimmte Computer gelten sollen, die zu unterschiedlichen Subnetzen oder Adressbereichen gehören, so dass diese Regelelemente nicht angewendet werden können. Es gibt die drei folgenden vordefinierten Computersätze:

- BELIEBIG: Dieser Computersatz umfasst sämtliche vorhandenen Geräte, da er den IP-Adressbereich 0.0.0.0 bis 255.255.255.255 umfasst. Dieser Computersatz kann nicht geändert werden.
- IPSEC-REMOTEGATEWAYS: Wenn ein Standort-zu-Standort-VPN eingerichtet ist, werden zu diesem Computersatz automatisch die Computer des jeweils anderen Standorts hinzugefügt. Eine manuelle Bearbeitung dieses Computersatzes ist ebenfalls nicht möglich.
- REMOTEVERWALTUNGSCOMPUTER: Zu diesem standarmäßig leeren Computersatz fügen Sie sämtliche Computer hinzu, die für die Remoteverwaltung des ISA Server vorgesehen sind. Dieser Computersatz verfügt über die entsprechende Berechtigung. Weitere Computer sollten Sie aus Sicherheitsgründen nicht zu diesem Computersatz hinzufügen.

Um einen zusätzlichen Computersatz einzurichten, sind die folgenden Aktionen durchzuführen:

1. Öffnen Sie in der Toolbox die NETZWERKOBJEKTE und wählen Sie das Menü NEU/COMPUTERSATZ.
2. Geben Sie einen Namen für den neuen Computersatz an. Über HINZUFÜGEN kann entweder ein Computer, Adressbereich oder Subnetz hinzugefügt werden (siehe Abbildung 7.18).

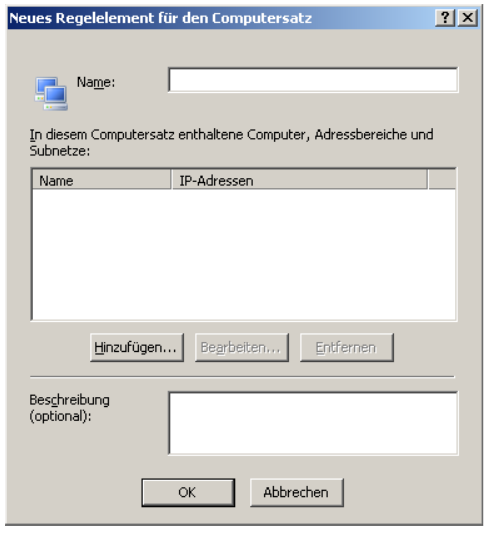


Abbildung 7.18: Erstellen des Regelelements Computersatz

7.1.11 URL-Sätze

Verweigern des Zugriffs auf URLs

Ein URL-Satz umfasst eine oder mehrere URLs. Dieses Regelelement sollte eingesetzt werden, um URLs zusammenzufassen, auf die entweder gar nicht oder ausschließlich zugegriffen werden darf und um den URL-Satz dann mit einer entsprechenden Regel zu verknüpfen. Fügen Sie einen neuen URL-Satz in folgender Weise hinzu:

1. Öffnen Sie in der Toolbox die NETZWERKOBJEKTE und wählen Sie das Menü NEU/URL-SATZ.
2. Im Konfigurationsfenster (siehe Abbildung 7.19) geben Sie einen Namen für den URL-Satz ein. Über NEU fügen Sie die entsprechenden URLs hinzu.

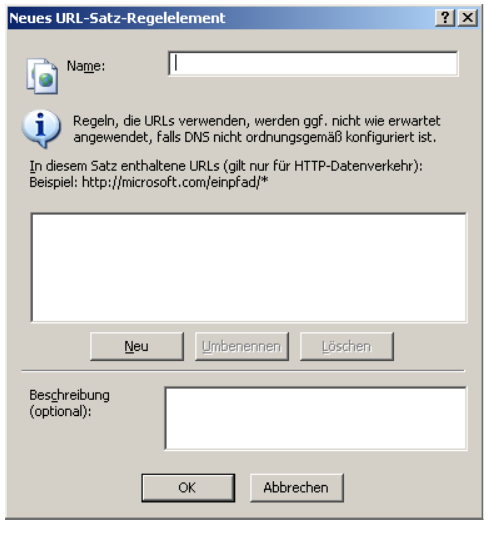


Abbildung 7.19: Erstellen des Regelelements URL-Satz

7.1.12 Domänennamensätze

DNS-Domänennamen

Im Regelelement Domänennamensätze werden DNS-Domänennamen zusammengefasst. So kann beispielsweise für Domänen von Geschäftspartnern o.Ä. eine Zugriffsrichtlinie erstellt werden, die den Zugriff auf das Firmennetzwerk gestattet. Es gibt bereits zwei vordefinierte Domänennamensätze:

- DURCH SYSTEMRICHTLINIE ZUGELASSENE SITES: Dieser Satz besteht aus den drei Domänen *microsoft.com*, *windows.com* und *windowsupdate.com* sowie deren untergeordneten Domänen. Selbst wenn keine explizite Zugriffsregel für ausgehenden Netzwerkverkehr erstellt ist, ist aufgrund der Systemrichtlinie der Zugriff auf diese Domänen immer gestattet.
- MICROSOFT-FEHLERBERICHTERSTATTUNGS-SITES: Zu diesem Domänennamensatz gehört die Domäne *watson.microsoft.com* mit untergeordneten Domänen. Hierbei handelt es sich um die Seiten, die zum Senden von Fehlermeldungen an Microsoft verwendet werden.

Um zusätzliche Domänennamensätze hinzuzufügen, sind die folgenden Schritte notwendig:

1. Öffnen Sie in der Toolbox die NETZWERKOBJEKTE und wählen das Menü NEU/DOMÄNENNAMENSATZ.
2. Im Konfigurationsfenster (siehe Abbildung 7.20) geben Sie einen Namen an. Danach werden über NEU die Domänennamen hinzugefügt.

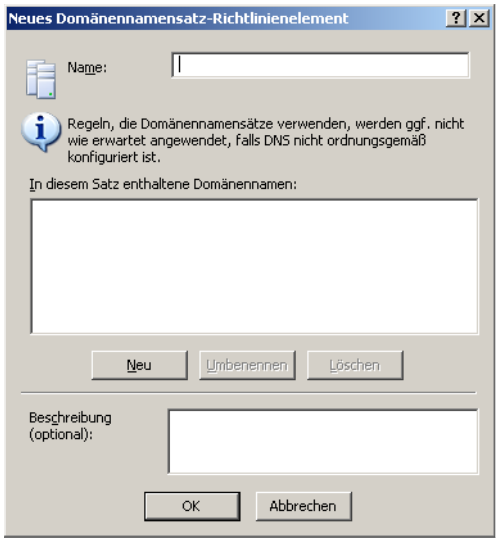


Abbildung 7.20: Erstellen des Regelelements Domänennamensatz

7.1.13 Weblistener

Abhören von Web-Anfragen

Ein Weblistener wird benutzt, damit der ISA Server eingehende und ausgehende Web-Anfragen abhören und anhand der definierten Regeln weiter verarbeiten kann. So kann eine Anfrage zugelassen oder blockiert werden. Fügen Sie Weblistener in folgender Weise hinzu:

1. Öffnen Sie in der Toolbox die NETZWERKOBJEKTE und wählen Sie das Menü NEU/WEBLISTENER.
2. Bestimmen Sie einen Namen für den Weblistener und klicken auf WEITER.
3. Im Fenster IP-ADRESSEN (siehe Abbildung 7.21) bestimmen Sie die Netzwerkkarte des ISA Server, über die die Web-Anfragen abgehört werden sollen. Besitzt der ISA Server mehrere IP-Adressen in einem Netzwerksegment, so kann das Abhören auf einer einzigen oder mehreren dieser Adressen erfolgen. Treffen Sie diese Einstellung über die Schaltfläche ADRESSE. Standardmäßig werden alle IP-Adressen verwendet.

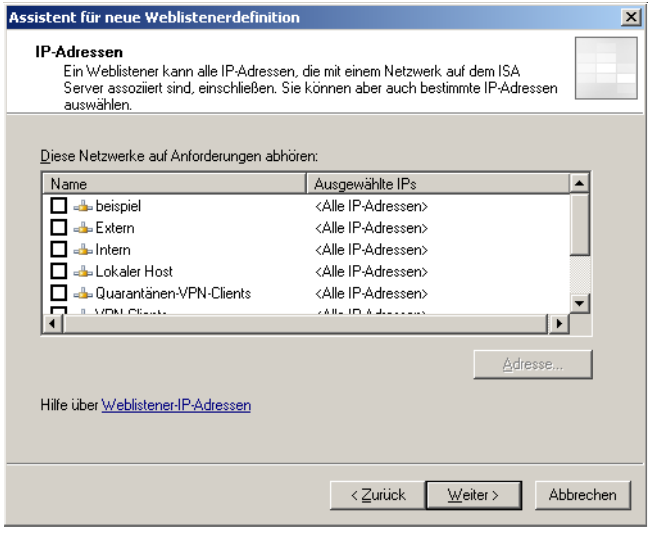


Abbildung 7.21: Auswahl der Netzwerke für den Weblistener

4. Soll nur eine bestimmte IP-Adresse benutzt werden, wählen Sie entweder die Standardadresse oder eine oder mehrere explizit anzugebende IP-Adressen aus und klicken Sie auf OK (siehe Abbildung 7.22).
5. Im folgenden Fenster PORTSPEZIFIZIERUNG (siehe Abbildung 7.23) können Sie den Port bestimmen, auf dem die Web-Anfragen abgehört werden sollen. Tragen Sie hier entweder die Standardports 80 für http bzw. 443 beim Einsatz einer SSL-Verschlüsselung ein und geben gegebenenfalls das Zertifikat an. Es können jedoch auch benutzerdefinierte Ports angegeben werden. Klicken Sie dann auf WEITER und beenden Sie den Assistenten.

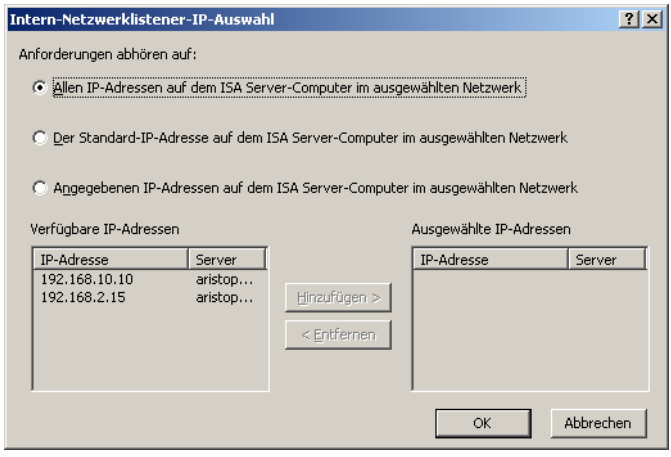


Abbildung 7.22: Konfiguration der IP-Adresse(n) für den Weblistener

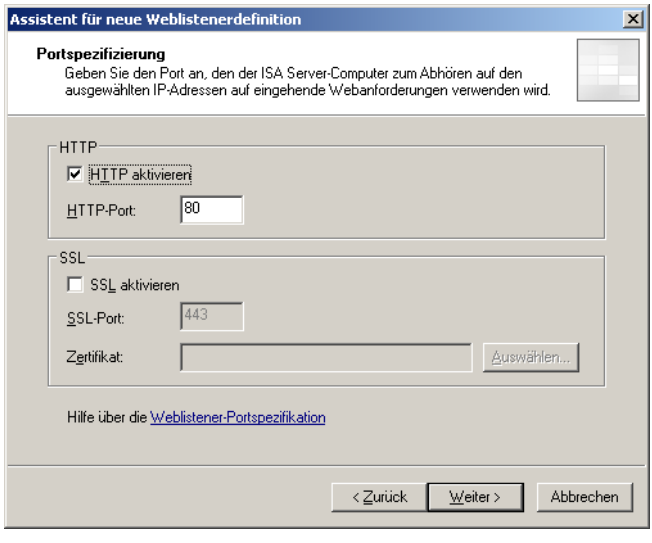


Abbildung 7.23: Konfiguration des Ports für den Weblistener

7.1.14 Arbeiten mit den Regelelementen

Import und Export

Wenn Sie in der Toolbox ein Regelelement markieren und dessen Kontextmenü aufrufen, können Sie darüber dessen Eigenschaften bearbeiten sowie einen Import oder Export durchführen. Je nach Regelelement kann auch eine Auswahl importiert und exportiert werden. Um schnell ähnliche Regelelemente erstellen zu können, können diese auch kopiert werden. Auch das Löschen der Elemente ist über das Kontextmenü möglich.

7.2 Firewall-Richtlinien

Kernstück der Zugriffskontrolle

Die Firewall-Richtlinien bilden ein Kernstück der ISA Server-Konfiguration. Über diese wird festgelegt, von welchem Ort zu welchem Ort welcher Benutzer zu welchem Zeitpunkt eine Netzwerkverbindung herstellen darf oder nicht. Bei der Konfiguration der Richtlinien ist immer zu bedenken, dass weniger oftmals mehr ist. So sollten keineswegs zuviele Objekte zu den einzelnen Richtlinien hinzugefügt werden. Z.B. macht es keinen Sinn, zu einer Richtlinie Netzwerkprotokolle hinzuzufügen, die nicht benötigt werden, oder womöglich den kompletten Netzwerkverkehr zuzulassen.

Werden derartige unsinnige Firewall-Richtlinien aufgestellt, ist es theoretisch überhaupt nicht erst notwendig, einen ISA Server einzusetzen. Ohne eine durchdachte Konfiguration kann der ISA Server das Unternehmensnetzwerk nicht absichern.

7.2.1 Aufbau einer Firewall-Richtlinie

Um den Aufbau einer Firewall-Richtlinie besser zu verstehen, sind die in ihr enthaltenen Elemente in Abbildung 7.24 dargestellt.

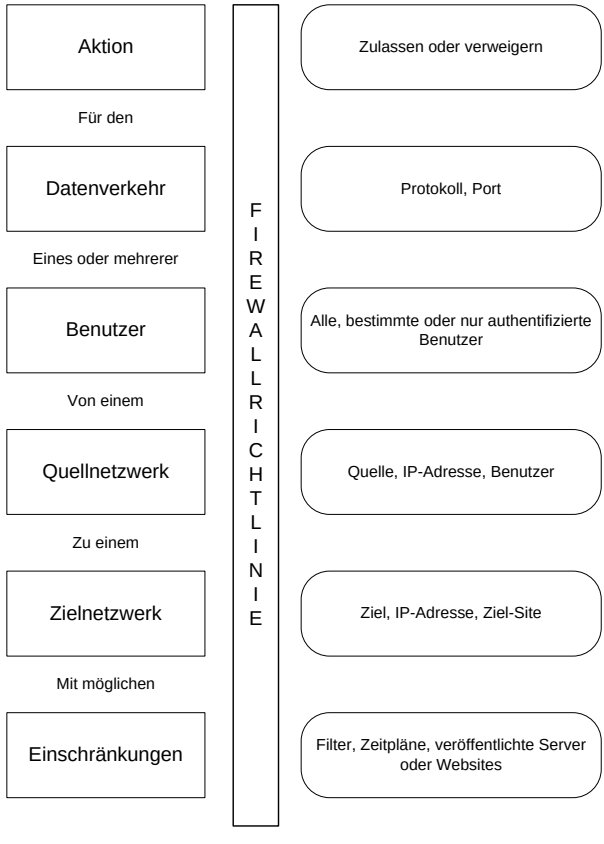


Abbildung 7.24: Schematische Übersicht über die Funktion einer Firewall-Richtlinie

Sie sehen dort die Elemente *Aktion, Datenverkehr, Benutzer, Quellnetzwerk, Zielnetzwerk* und *Einschränkungen*. Diese verschiedenen Elemente haben die folgenden Bedeutungen:

Tabelle 7.1: Die Elemente einer Firewall-Richtlinie

Element	Beschreibung
Aktion	Als Aktion kann *Zulassen* oder *Verweigern* gewählt werden. Sie müssen jedoch beim Erstellen mehrerer Richtlinien darauf achten, dass sich deren Inhalte nicht widersprechen. Bedenken Sie immer, dass mehrere Richtlinien in der gesetzten Reihenfolge von oben nach unten abgearbeitet werden. Haben Sie so z.B. in der zweiten Regel Benutzer A die Verwendung eines Protokolls gestattet und in der vierten Regel allen Benutzern die Verwendung dieses Protokolls untersagt, so kann Benutzer A dennoch dieses Protokoll verwenden, da die Richtlinie, die ihm dies erlaubt, zuerst abgearbeitet wird.
Datenverkehr	Die Richtlinie kann entweder für einen bestimmten TCP- oder UDP-Port gelten oder für ein bestimmtes IP-Protokoll.
Benutzer	Bestimmt, für welche (authentifizierten) Benutzer die Richtlinie gelten soll
Quellnetzwerk	In der Quelle wird angegeben, von welchem Netzwerk bzw. Netzwerksatz, Computersatz oder Adressbereich aus ein erlaubtes oder verweigertes Protokoll genutzt werden kann.
Zielnetzwerk	Das Ziel bestimmt, an welches Netzwerk bzw. an welchen Netzwerksatz, Computersatz oder Adressbereich der erlaubte oder verweigerte Netzwerkverkehr von der angegebenen Quelle aus geleitet wird.
Einschränkungen	Eine Richtlinie kann z.B. durch Zeitpläne oder Filter weiter eingeschränkt werden. So kann z.B. ein bestimmter Zugriff nur zu festen Zeiten erfolgen oder über einen http-Filter etwa der Messenger in einer http-Verbindung blockiert werden.

Innerhalb einer Richtlinie können für jede Kategorie (außer für Aktion) mehrere Elemente benutzt werden. So können beispielsweise mehrere Benutzer, Zeitpläne oder mehrere Quellnetzwerke für eine Firewall-Richtlinie festgelegt werden. Sie müssen lediglich bei der Konfiguration darauf achten, dass sich die Elemente einer Kategorie nicht gegenseitig widersprechen.

Vereinfachter Konfigurationszugriff

Im Gegensatz zum ISA Server 2000 wurde die Verwaltung der Firewall-Richtlinien vereinfacht. So müssen Sie nicht mehr an verschiedenen Stellen der ISA-mmc Einstellungen vornehmen, da die Firewall-

Richtlinien zentral an einer Stelle administriert werden, nämlich dem gleichnamigen Snap-In in der ISA-mmc.

Lediglich die Systemrichtlinien für den ISA Server selbst werden an einer anderen Stelle in der ISA-mmc eingestellt.

Die Standardregel blockiert jeden Verkehr

Nach der Erstinstallation des ISA Server ist bereits eine Firewall-Richtlinie namens *Standardregel* vorhanden. Aus Sicherheitsgründen unterbindet diese den gesamten Datenverkehr von allen Netzwerken zu allen Netzwerken für alle Benutzer (siehe Abbildung 7.25). Auf diese Weise wird der Administrator gezwungen, die Firewall stückchenweise zu öffnen, anstatt eine standardmäßig offene Firewall erst nach und nach schließen zu müssen.

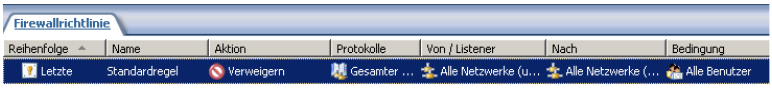


Abbildung 7.25: Standardmäßig blockiert die Firewall-Richtlinie sämtlichen Datenverkehr

Es ist auch nicht möglich, diese Richtlinie zu bearbeiten oder zu löschen. Um Datenverkehr zuzulassen, muss zunächst eine entsprechende Richtlinie erstellt werden. Die Standardregel besitzt immer die Reihenfolge LETZTE und wird auch als letzte abgearbeitet. So ist sichergestellt, dass sämtlicher Datenverkehr blockiert wird, der nicht ausdrücklich in einer anderen Firewall-Richtlinie erlaubt worden ist. Lediglich die Protokollierungseinstellungen können für die Standardregel angepasst werden.

Erst konfigurieren, dann produktiv einsetzen

Aufgrund dieser Tatsache ist es *nicht* möglich, mit dem ISA Server direkt nach der Installation ohne weitere Konfigurationseinstellungen produktiv zu arbeiten.

7.2.2 Ausgehende Zugriffe

Überwachung des ausgehenden Netzwerkverkehrs

Mit dem Wort Firewall assoziieren die meisten Leute sicherlich den Schutz des Netzwerks vor Angriffen von außen. Dabei wird oft übersehen, dass auch der aus dem Netzwerk nach außen gehende Verkehr überwacht werden muss, da auch dieser ein Sicherheitsrisiko darstellen kann. Man bezeichnet den nach außen gehenden Datenverkehr auch als ausgehende Zugriffe. Über eingehende Zugriffe wird im Rahmen der Serververöffentlichungen in Kapitel 8 gesprochen.

Sobald ein Client des internen Netzwerks eine Verbindung mit einem externen Webserver oder einem beliebigen anderen Computer in einem anderen Netzwerk herstellen möchte, prüft der ISA Server als Erstes, ob die beiden Netzwerke miteinander verknüpft sind. Ist keine Verknüpfung vorhanden, können die Pakete nicht gesendet werden und die Anfrage des Clients kann nicht bearbeitet werden.

Sind die beiden Netzwerke miteinander verknüpft, sucht der ISA Server nach einer passenden Zugriffsregel. Über eine solche Regel wird bestimmt, ob und welcher Netzwerkverkehr von welchem Computer

und Benutzer für welche Protokolle und zu welchen Zeiten gestattet ist. Sobald eine zutreffende Regel gefunden wird, wird geprüft, welche Anwendungs- und Webfilter mit dieser Regel verknüpft sind. Diese Filter werden ausführlich in Kapitel 9 abgehandelt.

Also nur, wenn keine Zugriffsregel und auch kein Filter die Anfrage verweigert, kann die Verbindung vom Client aus zum gewünschten Ziel hergestellt werden.

Ist die Verbindung zugelassen, muss der ISA Server ermitteln, ob die beiden Netzwerke über NAT oder Route miteinander verknüpft sind. Da das interne Netzwerk in aller Regel private IP-Adressen verwendet und das externe öffentliche IP-Adressen, besteht eine NAT-Verbindung. In diesem Fall muss der ISA Server die private IP-Adresse des internen Netzwerks in eine öffentliche IP-Adresse umwandeln.

Zusätzlich wird dabei geprüft, wie die Anfragen geroutet werden. Sollten zusätzlich noch Webverkettungs- oder Firewall-Verkettungsregeln konfiguriert sein, so werden auch die dort konfigurierten Regeln beachtet.

7.2.3 Erstellen von Firewall-Richtlinien

In diesem Kapitel lernen Sie, wie eine Firewall-Richtlinie konfiguriert wird. Als Beispiel dient ein Benutzer, der von seinem Computer aus während des kompletten Arbeitstages (Arbeitszeit und Mittagspause) nur E-Mails von einem POP3-Server abrufen darf.

Bevor Sie mit dem Erstellen der Richtlinien beginnen, sollten Sie in der Toolbox alle erforderlichen Regelelemente erstellt haben, da diese über den Assistenten der Regelerstellung abgefragt werden. Sind Sie beim Erstellen einer Regel und bemerken, dass ein Regelobjekt noch nicht erstellt worden ist, müssen Sie den Vorgang abbrechen und zunächst in der Toolbox das entsprechende Element erstellen.

Gemäß der oben beschriebenen Struktur einer Firewall-Richtlinie gelten die folgenden Konstanten:

- Aktion: Zulassen
- Datenverkehr: POP3
- Benutzer: User1
- Quelle: Computer1 (IP-Adresse 192.168.2.25)
- Ziel: POP3-Server des E-Mail-Providers (IP-Adresse 123.124.125.126)
- Einschränkungen: Zeitplan für die Arbeitszeit. Die Zeitpläne können jedoch nicht über den Assistenten gewählt werden. Diese können erst nach dem Erstellen der Regel über die Eigenschaften hinzugefügt werden. Dies wird im Kapitel 7.2.4 beschrieben.

Um die Richtlinie zu erstellen, sind die folgenden Schritte notwendig:

1. Zunächst werden über die Toolbox die notwendigen Elemente erstellt, sofern diese dort noch nicht vorhanden sind. Dabei handelt es sich um die Regelelemente *Computer* (Computer 1 sowie der POP3–Server im Internet) und die beiden Zeitpläne für Arbeitszeit und Mittagspause.
2. Unter NETZWERKOBJEKTE wird ein neuer Computer erstellt. Dieser trägt im Beispiel den Namen Computer1 und die IP-Adresse 192.168.2.25.
3. Als zweites Regelelement wird der Computer des POP3-Servers erstellt. Dieser hat im Beispiel den Namen POP3-Server und die IP-Adresse 123.124.125.126.
4. Danach werden die Zeitpläne für die Arbeitszeit und die Mittagspause eingerichtet. Die Arbeitszeit läuft von 8:00 h - 12:00 h sowie von 13:00 h - 17:00 h, die Mittagspause von 12:00 h - 13:00 h.
5. Nachdem diese Elemente über die Toolbox erstellt worden sind, wechseln Sie im Aufgabenbereich auf die Registerkarte AUFGABEN und klicken auf NEUE ZUGRIFFSREGEL ERSTELLEN.
6. Ein Assistent führt Sie durch die Einrichtung. Im Willkommensfenster (siehe Abbildung 7.26) geben Sie einen Namen für die Richtlinie an und klicken auf WEITER.

Abbildung 7.26: Der Assistent zum Erstellen einer neuen Firewall-Richtlinie

7. Im Fenster REGELAKTION wird entschieden, ob die Aktion zugelassen oder verweigert werden soll. Wählen Sie in diesem Beispiel ZULASSEN und klicken Sie auf WEITER.
8. Danach wählen Sie im Fenster PROTOKOLLE (siehe Abbildung 7.27) den Eintrag AUSGEWÄHLTE PROTOKOLLE. Klicken Sie dann auf HINZUFÜGEN und wählen Sie unter MAIL den Eintrag POP3. Klicken Sie dann auf WEITER.

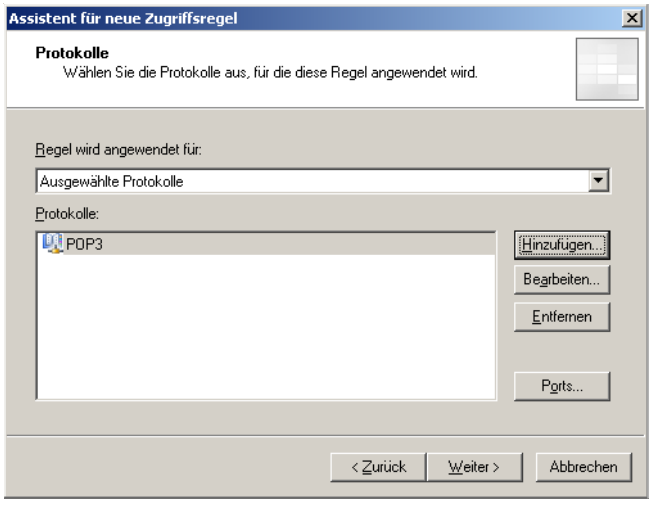


Abbildung 7.27: Auswahl des Protokolls, das zugelassen bzw. verweigert werden soll

9. Als Nächstes wird im Fenster ZUGRIFFSREGELQUELLEN der Computer *Computer1* über HINZUFÜGEN ausgewählt. Klicken Sie dann auf WEITER. Im folgenden Fenster ZUGRIFFSREGELZIELE wird analog der Computer *POP3-Server* gewählt.
10. Dann werden im Fenster BENUTZERSÄTZE die Benutzer ausgewählt, für die die Regel gelten soll. Standardmäßig ist dort das Objekt *Alle Benutzer* eingetragen. Ist auf dem Computer der Firewallclient installiert, so kann über diesen die Benutzerauthentifizierung erzwungen werden. Auf diese Weise ist sichergestellt, dass nur für *User1*, aber nicht für *User2* die erstellte Regel gilt, sofern dieser sich an *Computer1* anmeldet. Klicken Sie dann auf WEITER.

Haben Sie den Benutzersatz *Alle Benutzer* aus der Liste gelöscht und durch einen anderen Benutzersatz ersetzt, so fordert der ISA Server Anmeldeinformationen des Benutzers an. Bedenken Sie, dass nur Webproxy- und Firewallclients die Anmeldeinformationen senden können, nicht jedoch SecureNAT-Clients. Deren Verbindungsversuch wird in diesem Fall scheitern.

11. Sie erhalten eine ZUSAMMENFASSUNG (siehe Abbildung 7.28). Klicken Sie dort auf FERTIG STELLEN und übernehmen Sie anschließend die Änderung über die entsprechende Schaltfläche. Die neue Zugriffsregel wird danach an erster Stelle in der Liste FIREWALLRICHTLINIE angezeigt

Abbildung 7.28: Abschließende Anzeige der Angaben für die Firewall-Richtlinie

7.2.4 Weitere Konfiguration einer erstellten Zugriffsregel

Ist die Zugriffsregel erstellt, können Sie diese über ihre Eigenschaften noch weiter konfigurieren. Dabei sind noch weitere Optionen möglich, die über den eben beschriebenen Assistenten nicht gesetzt werden können.

So ist es auf den Registerkarten VON und NACH möglich, im Bereich AUSNAHMEN bestimmte Netzwerkobjekte hinzuzufügen, für die die gewählte Einstellung nicht gelten soll. Wählen Sie diese bei Bedarf über HINZUFÜGEN aus (siehe Abbildung 7.29). Auch für Benutzer können auf der gleichnamigen Registerkarte Ausnahmen gesetzt werden.

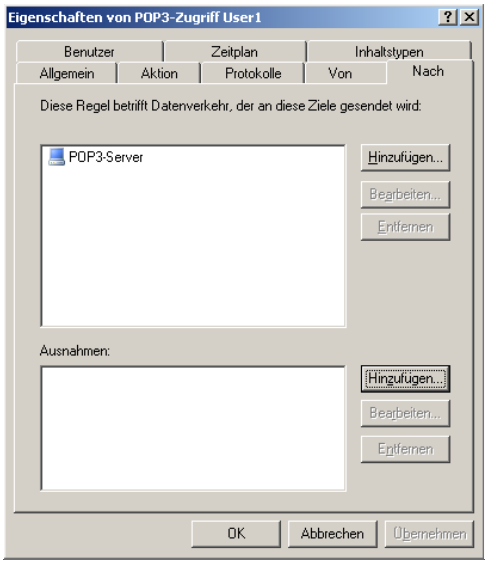
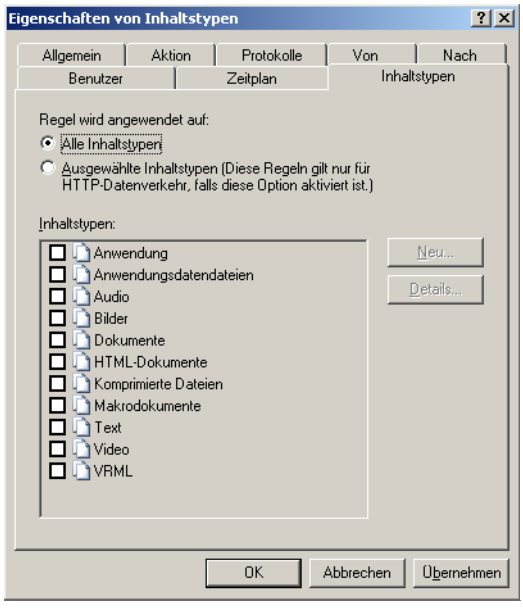


Abbildung 7.29: Einschränken der Ziele, an die Datenverkehr gesendet werden darf

Wie Sie bereits weiter oben gelesen haben, werden auch die Zeitpläne für die Ausnahmen einer Regel nicht über den Assistenten abgefragt. In der Grundeinstellung gilt die Regel immer. Über die Registerkarte ZEITPLAN können Sie nun den gewünschten Zeitplan auswählen.

Zusätzlich findet sich in den Eigenschaften die Registerkarte INHALTSTYPEN. Dort können Sie feiner abgestuft die Zugriffsregel für bestimmte Inhaltstypen wie Anwendungen, HTML-Dokumente oder Video verwenden. Über NEU können sogar zusätzliche Inhaltstypen hinzugefügt werden (siehe Abbildung 7.30).

Abbildung 7.30: Bestimmen von Inhaltstypen



7.2.5 Weitere Einsatzzwecke

Firewall-Richtlinien können zu diversen Zwecken erstellt werden. Um beispielsweise den Zugriff auf bestimmte Internetseiten zu unterbinden, können diese zum Regelelement *URL-Sätze* hinzugefügt werden.

Zeitsynchronisation des Domänencontrollers

Um zumindest für die Domänencontroller des Netzwerks eine Zeitsynchronisation zu ermöglichen, kann eine Richtlinie erstellt werden, in der der ausgehende Verkehr auf einen Zeitserver zugelassen wird. Mangelhaft eingestellte Synchronisationen zwischen Servern können nicht nur serverimmanent, z.B. bei der Replikation mehrerer Domänencontroller, zu Problemen führen, sondern auch bei weiteren im Netzwerk ausgeführten Programmen.

7.2.6 Weitere Firewall-Richtlinien-Funktionen

Über die Aufgabenliste der Firewall-Richtlinien sowie deren Kontextmenü können noch weitere Aufgaben an den Richtlinien durchgeführt werden.

Ändern der Reihenfolge

Abarbeitungsreihenfolge beachten

Sofern Sie mehrere Firewall-Richtlinien erstellt haben, wird automatisch die zuletzt erstellte Richtlinie an die oberste Stelle gesetzt. Unter *Reihenfolge* erhält diese den Wert 1. Die Standardregel befindet sich automatisch immer an der letzten Position. Sie kann von dieser Position auch nicht entfernt werden. Bei den anderen Richtlinien hingegen kann die Reihenfolge der Verarbeitung geändert werden. Wählen Sie dazu die Kontextmenüeinträge NACH OBEN bzw. NACH UNTEN, um die Richtlinie um jeweils eine Position höher oder niedriger zu verschieben. Alternativ können Sie auch in der Liste eine Regel markieren und im Aufgabenbereich AUSGEWÄHLTE REGEL NACH OBEN VERSCHIEBEN wählen.

Bedenken Sie immer, dass die Richtlinie, die an erster Stelle steht, zuerst abgearbeitet wird. Angenommen, in der ersten Richtlinie ist für eine bestimmte Verbindungsanfrage eine Regel mit dem Inhalt *Zulassen* konfiguriert, so wird lediglich diese Regel beachtet. Ist in einer späteren Richtlinie für dieselbe Verbindungsanfrage eine Regel mit dem Inhalt *Verweigern* eingerichtet, so wird diese nicht mehr abgearbeitet.

Import und Export

Im Aufgabenbereich befinden sich unter VERWANDTE AUFGABEN zwei Links, mit denen der Import bzw. Export der Firewall-Richtlinien durchgeführt werden kann. Weitere Hinweise zum Thema Import und Export finden Sie in Kapitel 6.

Richtlinien bearbeiten

Auf der Registerkarte AUFGABEN befinden sich weitere Links, über die die Regeln bearbeitet, gelöscht oder deaktiviert werden können. Diese Aufgaben können auch über das Kontextmenü aufgerufen werden.

Um mit einem Blick zu erkennen, ob eine Richtlinie deaktiviert ist oder nicht, schauen Sie auf das Symbol in der Spalte REIHENFOLGE. Das Deaktivieren bietet gegenüber dem Löschen den Vorteil, dass die Einstellungen erhalten bleiben. Gerade in einer Testumgebung oder bei der Fehlersuche kann das Deaktivieren bestimmter Regeln Sinn machen.

7.3 Die Systemrichtlinien

Richtlinie des ISA Server selbst

Eine Systemrichtlinie bestimmt nicht wie die Firewall-Richtlinien das Verhalten der Clients, sondern legt fest, welche Protokolle oder Verbindungen der ISA Server selbst nutzen darf oder nicht. Die Systemrichtlinien sind somit die Firewall-Richtlinien für den ISA Server selbst. Nach der Installation besitzt der ISA Server bereits 30 Systemrichtlinien. Allerdings sind diese nicht alle aktiviert.

Es ist nicht möglich, Systemrichtlinien zu löschen bzw. weitere Systemrichtlinien zum ISA Server hinzuzufügen. Lediglich das Deaktivieren bzw. Bearbeiten dieser Richtlinien ist möglich.

Sie finden diese Systemrichtlinien in der ISA-mmc, indem Sie dort unter FIREWALLRICHTLINIE im Aufgabenbereich auf der Registerkarte AUFGABEN auf SYSTEMRICHTLINIENREGELN EINBLENDEN klicken (siehe Abbildung 7.31).

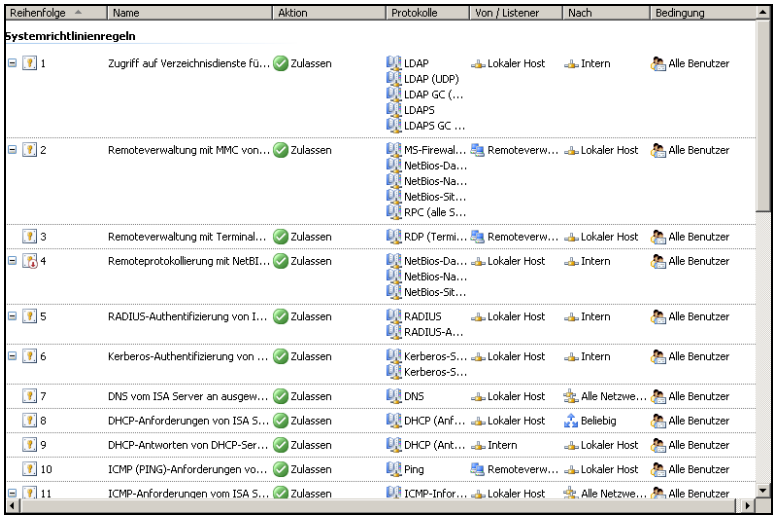


Abbildung 7.31: Übersicht über einen Teil der Systemrichtlinien

Um die Systemrichtlinien zu bearbeiten, wählen Sie entweder aus dem Kontextmenü von FIREWALLRICHTLINIE den Eintrag SYSTEMRICHTLINIE BEARBEITEN oder klicken auf den Link SYSTEMRICHTLINIE BEARBEITEN unter den Aufgaben der FIREWALLRICHTLINIE. Auf beiderlei Weise erhalten Sie das Fenster SYSTEMRICHTLINIEN-EDITOR (siehe Abbildung 7.32).

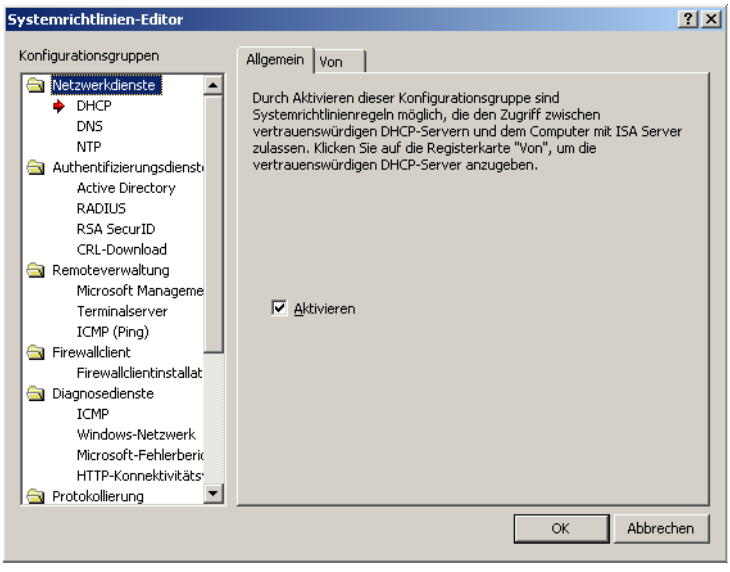


Abbildung 7.32: Systemrichtlinien-Editor zum Bearbeiten dieser Richtlinien

Insgesamt gibt es 30 Systemrichtlinien auf dem ISA Server. Die Bedeutung der einzelnen Richtlinien wird in Tabelle 7.2 beschrieben.

30 Systemrichtlinien

Tabelle 7.2: Auflistung der Systemrichtlinien des ISA Server und deren Bedeutung

Name der Richtlinie sowie Microsoft-Beschreibung in den Eigenschaften	Beschreibung
Authentifizierungsdienste: Zugriff auf Verzeichnisdienste für Authentifizierungszwecke zulassen	Der ISA Server kann auf das Active Directory des internen und damit vertrauenswürdigen Netzwerks zugreifen.
Remoteverwaltung: Remoteverwaltung mit MMC von ausgewählten Computern zulassen	Alle Computer, die zum Computersatz *Remoteverwaltungscomputer* gehören, können über die mmc auf die ISA-Konfiguration zugreifen.
Remoteverwaltung: Remoteverwaltung mit Terminalserver von ausgewählten Computern zulassen	Alle Computer, die zum Computersatz *Remoteverwaltungscomputer* gehören, können über den Remotedesktop auf die ISA-Konfiguration zugreifen.
Remoteverwaltung: Remoteprotokollierung auf vertrauenswürdigen Servern mit NetBIOS zulassen	Vom ISA Server dürfen NetBIOS-Anfragen und –Verbindungen zu allen Computern des internen Netzwerks hergestellt werden.

Name der Richtlinie sowie Microsoft-Beschreibung in den Eigenschaften	Beschreibung
Authentifizierungsdienste: RADIUS-Authentifizierung von ISA Server an vertrauenswürdige RADIUS-Server zulassen	Der ISA Server kann zur Authentifizierung auf einen RADIUS/IAS-Server des internen Netzwerks zugreifen.
Authentifizierungsdienste: Kerberos-Authentifizierung von ISA Server an vertrauenswürdige Server zulassen	Der ISA Server kann gegenüber Servern des internen Netzwerks die Kerberos-Authentifizierung durchführen.
Netzwerkdienste: DNS vom ISA Server an ausgewählte Server zulassen	Der ISA Server kann zur Namensauflösung in alle Netzwerke DNS-Anfragen senden und die Antworten empfangen.
Netzwerkdienste: DHCP-Anforderungen von ISA Server an alle Netzwerke zulassen	Der ISA Server kann eine oder mehrere IP-Adressen via DHCP erhalten.
Netzwerkdienste: DHCP-Antworten von DHCP-Servern an ISA Server zulassen	Die Clients des internen Netzwerks können DHCP-Anfragen an den ISA Server schicken und die Antworten empfangen.
Netzwerkdienste: ICMP (PING)-Anforderungen von ausgewählten Computern an ISA Server zulassen	Alle Computer, die zum Computersatz *Remoteverwaltungscomputer* gehören, können einen Ping-Befehl an den ISA Server senden.
Diagnosedienste: ICMP-Anforderungen vom ISA Server an ausgewählte Server zulassen	Der ISA Server kann einen Ping-Befehl in alle Netzwerke versenden.
VPN: VPN-Clientdatenverkehr auf ISA Server zulassen. VPN-Systemrichtlinienregeln basieren auf VPN-Eigenschaften und auf dem VPN-Knoten in der ISA Server-Verwaltung konfiguriert.	Clients des externen Netzwerks können eine PPTP-VPN-Verbindung zum ISA Server herstellen.
VPN: VPN-Standort-zu-Standort-Datenverkehr zum ISA Server zulassen. VPN-Systemrichtlinienregeln basieren auf VPN-Eigenschaften, die im VPN-Knoten der ISA Server-Verwaltung konfiguriert werden.	Über diese Richtlinie wird der Datenverkehr vom Remote-Standort zum ISA Server zugelassen.

Name der Richtlinie sowie Microsoft-Beschreibung in den Eigenschaften	Beschreibung
VPN: VPN-Standort-zu-Standort-Datenverkehr vom ISA Server zulassen. VPN-Systemrichtlinienregeln basieren auf VPN-Eigenschaften, die im VPN-Knoten der ISA Server-Verwaltung konfiguriert werden.	Über diese Richtlinie wird der Datenverkehr vom ISA Server zum Remote-Standort zugelassen.
Authentifizierungsdienste: Microsoft CIFS von ISA Server auf vertrauenswürdige Server zulassen	Der ISA Server kann auf das Dateisystem der internen Computer zugreifen.
Protokollierung: Remote-SQL-Protokollierung vom ISA Server an ausgewählte Server zulassen	Der ISA Server kann zur Protokollierung mit einem SQL Server kommunizieren.
Verschiedene: HTTP/HTTPS-Anforderungen von ISA Server an angegebene Sites zulassen	Der ISA Server kann über https auf die drei Seiten **.microsoft.com*, **.windows.com* und **.windowsupdate.com* zugreifen.
Netzwerkdienste: HTTP/HTTPS-Anforderungen vom ISA Server an ausgewählte Server für Konnektivitätsverifizierungen zulassen	Ist die Konnektivitätsverifizierung eingerichtet, kann der ISA Server aus sämtlichen Netzwerken Webseiten herunterladen.
Firewallclient: Zugriff von vertrauenswürdigen Computern auf die Firewallclient-Installationsfreigabe auf dem ISA Server zulassen	Befindet sich die Installationsfreigabe für den Firewallclient auf dem ISA Server, muss die Richtlinie aktiviert sein, so dass die Clients Zugriff auf diesen Ordner haben.
Remoteüberwachung: Remoteleistungsüberwachung von ISA Server von vertrauenswürdigen Servern zulassen	Alle Computer, die zum Computersatz *Remoteverwaltungscomputer* gehören, können zur Leistungsüberwachung NetBIOS-Sitzungen mit dem ISA Server herstellen.
Diagnosedienste: NetBIOS von ISA Server auf vertrauenswürdige Server zulassen	Der ISA Server kann zu allen Computern des internen Netzwerks NetBIOS-Anfragen und -Verbindungen herstellen.
Authentifizierungsdienste: RPC von ISA Server auf vertrauenswürdige Server zulassen	Der ISA Server kann zu allen Computern des internen Netzwerks RPC-Verbindungen herstellen.

Name der Richtlinie sowie Microsoft-Beschreibung in den Eigenschaften	Beschreibung
Diagnosedienste: HTTP/HTTPS von ISA Server an angegebene Microsoft-Fehlerberichterstattungs-Sites zulassen	Für die automatische Fehlerberichtsfunktion kann auf die Microsoft-Seite **.watson.microsoft.com* der Zugriff erfolgen.
Authentifizierungsdienste: SecurID-Authentifizierung von ISA Server an ausgewählte Server zulassen	Ist der SecureID-Filter aktiv, muss die Richtlinie zum Senden von Authentifizierungsanfragen an interne SecurID-Server aktiviert sein.
Remoteüberwachung: Remoteüberwachung von ISA Server auf vertrauenswürdigen Servern mithilfe des Microsoft Operations Manager-Agents zulassen	Diese Richtlinie ist erforderlich, wenn die Überwachung des ISA Server über einen MOM-Server erfolgen soll.
Authentifizierungsdienste: HTTP von ISA Server an ausgewählte Netzwerke für das Downloaden aktualisierter Zertifikatsperrlisten zulassen	Der ISA Server kann die jeweils aktuellsten Zertifikatsperrlisten über HTTP von allen Netzwerken abrufen.
Netzwerkdienste: NTP von ISA Server an vertrauenswürdige NTP-Server zulassen	Der ISA Server kann mit einem Zeitserver eine Zeitsynchronisation durchführen.
Remoteüberwachung: SMTP von ISA Server an vertrauenswürdige Server zulassen	Der ISA Server kann E-Mails über SMTP an das interne Netzwerk schicken, z.B. für Benachrichtigungen bei einem Alarm.
Verschiedenes: HTTP von ISA Server an ausgewählte Computer für Inhaltdownloadaufträge zulassen	Sind geplante Inhaltsdownload-Aufträge vorhanden, gestattet diese dann aktivierte Richtlinie den entsprechenden HTTP-Verkehr.
Remoteverwaltung: Remoteverwaltungscomputern gestatten, auf dem ISA Server-Computer ausgeführte Dienste zu verwalten	Sämtlicher Verkehr vom ISA Server zu allen Computern, die zum Computersatz *Remoteverwaltungscomputer* gehören, ist gestattet.

7.4 Authentifizierungsmechanismen

Regelgeltung für bestimmte Benutzer

Nachdem die Zugriffsregeln für die einzelnen Netzwerke konfiguriert worden sind, können die Benutzer anhand dieser Regeln z.B. auf das Internet zugreifen. Sollen die erstellten Zugriffsregeln für sämtliche Benutzer gelten, sind keine weiteren Einstellungen möglich. Möchten Sie hingegen, dass die Regeln nur für bestimmte Benutzer

gelten, so muss eine Benutzerauthentifizierung implementiert werden, damit der ISA Server erkennen kann, ob die Zugriffsregel angewendet werden soll oder nicht.

Wie Sie bereits gesehen haben, kann für eine Zugriffsregel der Benutzersatz *Alle Benutzer* gewählt werden. In diesem Fall erfordert der ISA Server keine Authentifizierungsinformationen. Der ISA Server kann in diesem Fall nicht feststellen, von welchem Benutzer der Zugriff durchgeführt wird. Lediglich die Protokollierung der anfragenden IP-Adresse des Computers ist möglich. So können Sie nicht verhindern, dass ein Benutzer, der über keinen eigenen Internetzugang an seinem Computer verfügt, die Anmeldung von einem anderen Gerät aus durchführt und so dennoch Zugriff auf für ihn eigentlich nicht genehmigte Ressourcen erlangt.

In der Überwachungsübersicht des ISA Server wird als Benutzername der Eintrag *anonymous* angezeigt, wenn der ISA Server keine Authentifizierungsinformationen angefordert hat. Bei einem SecureNAT-Client ist dies grundsätzlich der Fall. Weitere Hinweise zur Überwachung finden Sie in Kapitel 12.

Benutzersatz Alle Benutzer

Authentifizierungsinformationen werden vom ISA Server lediglich dann angefordert, wenn beim Erstellen der Zugriffsregel (oder zu einem späteren Zeitpunkt in deren Eigenschaften) der Benutzersatz *Alle Benutzer* durch einen anderen Benutzersatz ausgetauscht wird. In diesem Fall muss der Benutzer seine Authentifizierungsinformationen an den ISA Server übermitteln, bevor die Verbindung hergestellt werden kann.

Bedenken Sie, dass diese Konfiguration lediglich für Firewall- und Webproxy-Clients möglich ist. Ein SecureNAT-Client kann keine Authentifizierungsinformationen senden. Ist für diesen der Benutzersatz Alle Benutzer entfernt, kann der SecureNAT-Client für die entsprechenden Protokolle der Zugriffsregel keine Verbindung mehr herstellen.

Ein Sonderfall ist der Benutzersatz *Alle authentifizierten Benutzer*. Wird dieser Benutzersatz gewählt, werden automatisch alle Benutzer von Firewall- und WebProxy-Clients vom ISA Server identifiziert, so dass die Benutzerinformationen in der Überwachung und Protokollierung angezeigt werden. Selbstverständlich können Sie auch eigene Benutzersätze zu diesem Zweck festlegen.

Abhängig vom Client

Folgend finden Sie eine Übersicht über die Authentifizierungsmerkmale der drei Client-Typen des ISA Server:

- *Firewall-Client*: Für die Authentifizierung der Firewall-Clients ist keine besondere Konfigurationseinstellung notwendig, da diese automatisch über den Control Channel authentifiziert werden.
- *Webproxy-Client*: Eine Authentifizierung der Webproxy-Clients ist möglich, wenn der ISA Server diese erfordert. Allerdings muss

dazu eine Authentifizierungsmethode eingerichtet werden. Die dafür möglichen Verfahren werden in den folgenden Kapiteln näher vorgestellt.

- *SecureNAT-Client*: Diese Clients können keine Authentifizierungsinformationen senden, und deshalb können auf sie keine Zugriffsregeln angewendet werden, für die eine Authentifizierung notwendig ist.

7.4.1 Authentifizierung des Webproxy-Clients

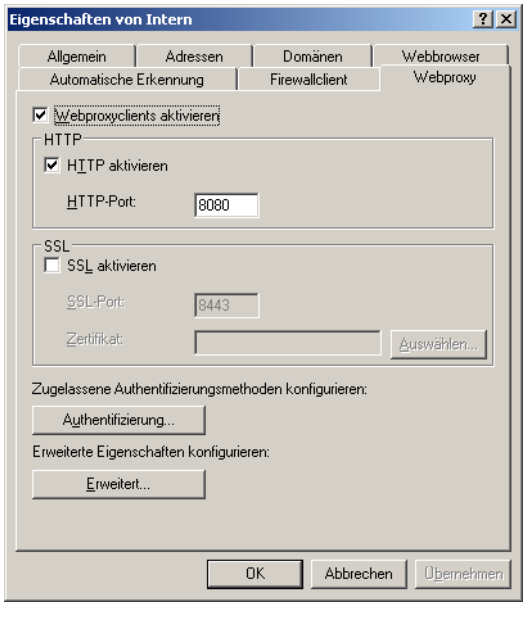
Um für einen Webproxy-Client die Authentifizierung festzulegen, müssen Sie die folgenden Schritte durchführen:

1. Navigieren Sie in der ISA-mmc zu KONFIGURATION/NETZWERKE und wählen Sie die EIGENSCHAFTEN des Netzwerks *Intern*.

In aller Regel gehören die Webproxy-Clients zu diesem Netzwerk. Ist dies in Ihrer Konfiguration nicht der Fall, wählen Sie das entsprechende andere Netzwerk aus.

2. Wechseln Sie auf die Registerkarte WEBPROXY (siehe Abbildung 7.33) und aktivieren zunächst diese Clients, sofern dies noch nicht geschehen ist. Des Weiteren können Sie wählen, ob für diese Clients das http- und/oder SSL-Protokoll aktiviert werden soll. Geben Sie jeweils den zugehörigen Port und für die SSL-Nutzung das zugehörige Zertifikat an.

Abbildung 7.33: Aktivierung der Webproxy-Clients



3. Über die Schaltfläche AUTHENTIFIZIERUNG können Sie zwischen verschiedenen Mechanismen wählen. Dabei stehen die folgenden Methoden zur Wahl (siehe Abbildung 7.34):
   - DIGEST
   - INTEGRIERT
   - STANDARD
   - SSL-ZERTIFIKAT
   - RADIUS

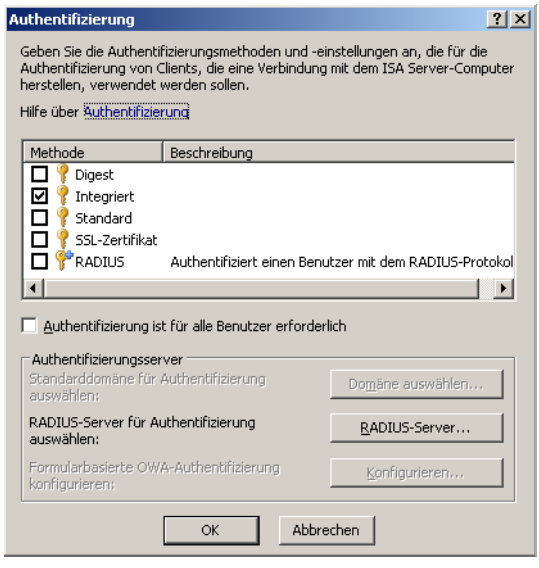


Abbildung 7.34: Die Auswahl und Konfiguration der Authentifizierungsmethode

Authentifizierung erzwingen

Über die Checkbox AUTHENTIFIZIERUNG IST FÜR ALLE BENUTZER ERFORDERLICH können Sie für sämtliche Webproxy-Clients des Netzwerks eine Authentifizierung erzwingen. Damit ist eine Authentifizierung immer notwendig, unabhängig davon, ob dies über eine entsprechende Zugriffsregel definiert ist oder nicht.

Haben Sie als Authentifizierungsmethode DIGEST, STANDARD oder RADIUS gewählt, müssen Sie über DOMÄNE AUSWÄHLEN die Domäne auswählen, an der die Benutzerauthentifizierung zu erfolgen hat. Bei Wahl der Methode RADIUS muss zusätzlich der RADIUS-Server angegeben werden. Nur bei der Veröffentlichung eines Webservers, nicht jedoch bei der Konfiguration ausgehender Zugriffe kann die formularbasierte OWA-Authentifizierung konfiguriert werden.

7.4.2 Hinweise zur Wahl der geeigneten Methode

Eine oder mehrere Methoden wählen

Sie können für die Authentifizierung eine oder mehrere der möglichen Methoden auswählen. Ist keine Methode ausgewählt, erhalten Sie ein Hinweisfenster, dass ohne Auswahl einer Methode die Zugriffsregeln, die eine Authentifizierung erfordern, nicht angewendet werden können und deshalb kein Zugriff für den Benutzer ermöglicht werden kann.

Heterogene Clients

Verfügen Sie über eine heterogene Client-Landschaft, die zudem unterschiedliche Webbrowser einsetzt, so müssen mehrere Authentifizierungsmethoden ausgewählt werden. Sobald die Verbindung hergestellt wird, wird zwischen dem ISA Server und dem Webproxy-Client automatisch das passende Protokoll ausgehandelt.

Nur Windows-Clients

Setzen Sie hingegen nur Windows-Clients in der Domäne ein, so sollten Sie die Windows-Authentifizierung verwenden, die mit geringem Aufwand einzurichten ist.

Verschiedene Domänen

Ist der ISA Server nicht Mitglied der Domäne oder einer vertrauenden Domäne, so sollte als Authentifizierungsmethode RADIUS verwendet werden, auch wenn damit ein gewisser Implementierungsaufwand verbunden ist und aus Gründen der Ausfallsicherheit mindestens zwei RADIUS-Server vorhanden sein sollten. Bei der Auswahl von RADIUS kann keine zweite Authentifizierungsmethode ausgewählt werden.

7.4.3 Digest-Authentifizierung des Webproxy-Clients

Die Digest-Authentifizierung kann nur verwendet werden, wenn sich das Benutzerkonto in einer Windows-2000/2003-Domäne befindet. Zudem müssen die Konten die Kennwörter mit umkehrbarer Verschlüsselung speichern können. Zudem müssen die Clients einen Webbrowser verwenden, der mindestens den http 1.1-Standard erfüllt. Die umkehrbare Verschlüsselung wird in der mmc ACTIVE DIRECTORY-BENUTZER UND COMPUTER über die EIGENSCHAFTEN des Benutzers auf der Registerkarte KONTO eingestellt (siehe Abbildung 7.35).

Bei der Digest-Authentifizierung werden die Anmeldeinformationen in einen Hash-Wert gewandelt. Dies geschieht in einem unidirektionalen Prozess.

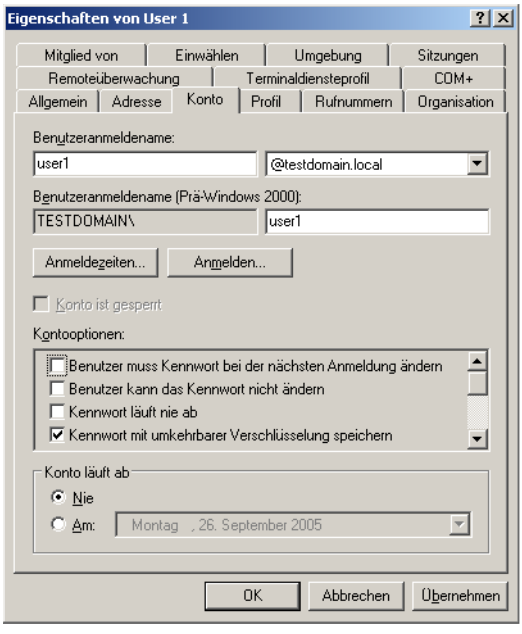


Abbildung 7.35: Das Kennwort des Benutzers muss mit umkehrbarer Verschlüsselung gespeichert werden können

7.4.4 Integrierte Windows-Authentifizierung des Webproxy-Clients

Die integrierte Authentifizierung ermöglicht es, dass ein Benutzer nicht erneut Anmeldeinformationen für den ISA Server eingeben muss, wenn die aktuellen Anmeldeinformationen des Computers oder der Domäne verwendet werden können. Lediglich wenn eine Authentifizierung über diese Informationen am ISA Server nicht möglich ist, muss der Benutzer einen anderen Benutzernamen mit zugehörigem Kennwort eingeben.

Kerberos oder NTLM

Zur Authentifizierung wird entweder *Kerberos* oder *NTLM (NT LAN-Manager)* verwendet. Dabei erfolgt keine Übertragung von Benutzernamen und Kennwort über das Netzwerk.

7.4.5 Standardauthentifizierung des Webproxy-Clients

Keine Verschlüsselung

Die Standardauthentifizierung ist als einzige Authentifizierungsmethode bereits auf der Registerkarte AUTHENTIFIZIERUNG vorgewählt. Dies liegt darin begründet, dass dieses Verfahren von nahezu allen Webbrowsern nativ unterstützt wird. Allerdings werden bei diesem Mechanismus der Benutzername und das Kennwort unverschlüsselt über das Netzwerk übertragen. Das Kennwort wird zwar durch eine Base64-Codierung geschützt, allerdings ist dies keine Verschlüsse-

lung, so dass das Kennwort z.B. über einen Netzwerksniffer ausgelesen werden könnte.

Sie sehen also, dass dieses Verfahren zwar eine breite Unterstützung, dafür aber keine hohe Sicherheit bietet.

7.4.6 SSL-Zertifikatsauthentifizierung des Webproxy-Clients

Damit sich ein Client über ein installiertes Zertifikat authentifizieren kann, muss dieses Zertifikat sowohl auf dem Client, als auch auf dem ISA Server vorhanden sein. Sobald der Client eine Verbindung zum ISA Server initiiert, wird das Zertifikat des Servers an den Client übertragen. Bei Anforderung der Authentifizierungsinformationen durch den ISA Server wird das Client-Zertifikat an den ISA Server geschickt.

7.4.7 RADIUS-Authentifizierung des Webproxy-Clients

Die Konfiguration der RADIUS-Authentifizierung ist von allen Methoden die aufwändigste. Sie müssen für diese Methode zunächst einen RADIUS-Server konfigurieren. An diesen werden vom ISA Server die Anmeldeinformationen über das RADIUS-Protokoll gesendet. Erst wenn der RADIUS-Server dem ISA Server mitgeteilt hat, dass diese Informationen erfolgreich geprüft worden sind, kann der Zugriff für den Client erfolgen.

Beim Einsatz eines RADIUS-Servers kann der ISA Server auch als allein stehender Server betrieben werden und muss nicht zu derselben oder einer vertrauenden Domäne gehören. Bei diesem Verfahren können auch Benutzer anderer Domänen authentifiziert werden.

Zwei Radius-Server zur Redundanz

Da jedoch beim Ausfall des RADIUS-Servers keine Authentifizierung durchgeführt werden kann, ist es sinnvoll, mindestens zwei RADIUS-Server im Netzwerk zu implementieren. Normalerweise wird das RADIUS-Verfahren verwendet, wenn die Authentifizierung für eingehende VPN- oder DFÜ-Verbindungen geprüft werden soll.

Wenn Sie die Methode RADIUS auswählen, darf keine andere Authentifizierungsmethode ausgewählt sein.

Einrichten des RADIUS-Servers

Um den RADIUS-Server einzurichten, führen Sie die folgenden Schritte aus. Der Server muss unter Windows 2000 oder 2003-Server betrieben werden und als Domänencontroller oder Mitgliederserver einer Windows 2000/2003-Domäne eingerichtet sein.

1. Zunächst muss der RADIUS-Dienst hinzugefügt werden. Klicken Sie dazu unter SYSTEMSTEUERUNG/SOFTWARE auf WINDOWS-KOMPONENTEN HINZUFÜGEN/ENTFERNEN. Markieren Sie den Eintrag NETZWERKDIENSTE und klicken auf DETAILS.
2. Wählen Sie dort den Eintrag INTERNETAUTHENTIFIZIERUNGSDIENST und klicken Sie auf OK. Die Installation des Dienstes erfolgt. Die Installations-CD ist dafür nicht erforderlich.
3. Starten Sie dann in der Verwaltung die neue mmc INTERNETAUTHENTIFIZIERUNGSDIENST. Markieren Sie dort den Eintrag INTERNETAUTHENTIFIZIERUNGSDIENST (LOKAL) und wählen Sie das Menü AKTION/SERVER IM ACTIVE DIRECTORY REGISTRIEREN. Dadurch wird der Server zur Gruppe *RAS- und IAS-Servers* im Active Directory hinzugefügt. Als Mitglied dieser Gruppe besitzt der Server die Berechtigung, aus den Benutzerkonten die Einwähleigenschaften des Benutzers zu lesen.
4. Markieren Sie dann den Eintrag RADIUS-CLIENTS und wählen Sie den Kontextmenüeintrag NEUER RADIUS-CLIENT. Der RADIUS-Client wird verwendet, um die Anmeldeinformationen der Benutzer an den RADIUS-Server weiterzuleiten. In unserem Beispiel fungiert der ISA Server als RADIUS-Client. In anderen Szenarien kann dies auch ein VPN- oder RAS-Server sein. Tragen Sie dazu im Fenster NEUER RADIUS-CLIENT unter ANGEZEIGTER NAME den Anzeigenamen und unter CLIENTADRESSE den FQDN oder die IP-Adresse des ISA Server ein (siehe Abbildung 7.36). Klicken Sie auf *Verifizieren*, um zu testen, ob der DNS-Name korrekt aufgelöst werden kann. Verfügt der ISA Server über mehrere IP-Adressen, muss hier die gewünschte ausgewählt werden.

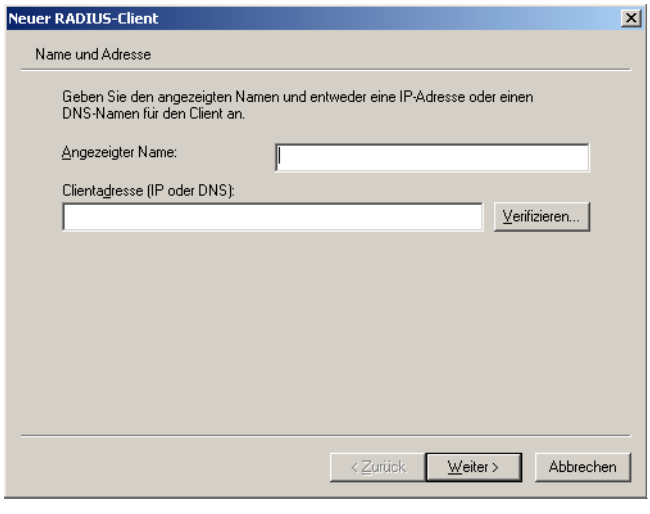
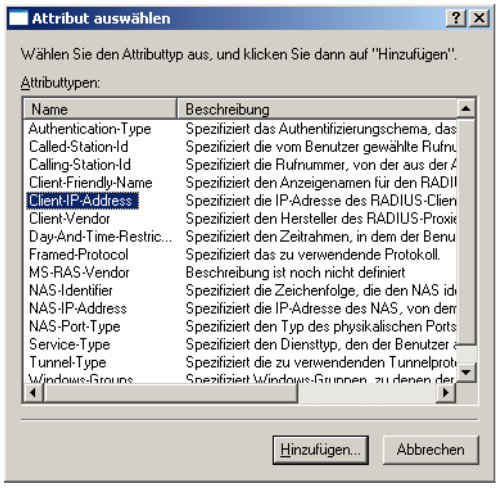


Abbildung 7.36: Konfiguration des RADIUS-Clients

5. Im folgenden Fenster ZUSÄTZLICHE INFORMATIONEN wird der auf dem ISA Server bestimmte RADIUS-Schlüssel angegeben (siehe Abbildung 7.39). Klicken Sie dann auf WEITER und beenden Sie den Assistenten. Der neue RADIUS-Client wird in der mmc angezeigt.
6. Als Nächstes werden RAS-Richtlinien erstellt. Über diese wird festgelegt, welche Benutzer wozu authentifiziert werden dürfen. Wählen Sie aus dem Kontextmenü von RAS-RICHTLINIEN den Eintrag NEUE RAS-RICHTLINIE.
7. Geben Sie der Richtlinie im Fenster RICHTLINIENKONFIGURATIONSMETHODE einen passenden Namen und wählen Sie BENUTZERDEFINIERTE RICHTLINIE EINRICHTEN.
8. Im Fenster RICHTLINIENBEDINGUNGEN klicken Sie auf HINZUFÜGEN. Wählen Sie dazu im Fenster ATTRIBUT AUSWÄHLEN (siehe Abbildung 7.37) den Eintrag CLIENT-IP-ADDRESS und klicken Sie erneut auf HINZUFÜGEN.

Abbildung 7.37: Wahl des Attributs für die Richtlinienbedingung



9. Sie erhalten dadurch das Fenster CLIENT-IP-ADDRESS. Geben Sie dort die IP-Adresse des ISA Server ein. Damit ist sichergestellt, dass nur Authentifizierungsanfragen von dieser Adresse vom RADIUS-Server verarbeitet werden. Klicken Sie danach auf WEITER.
10. Im Fenster BERECHTIGUNGEN wählen Sie die Option RAS-BERECHTIGUNG ERTEILEN und klicken Sie auf WEITER.
11. Klicken Sie dann im Fenster PROFIL auf PROFIL BEARBEITEN. Dadurch wird das Profil der RAS-Richtlinie modifiziert. Wechseln Sie dort auf die Registerkarte AUTHENTIFIZIERUNG (siehe Abbildung 7.38) und wählen Sie dort nur die Option UNVERSCHLÜSSELTE AUTHENTIFIZIERUNG (PAP, SPAP). Bestätigen Sie mit OK.

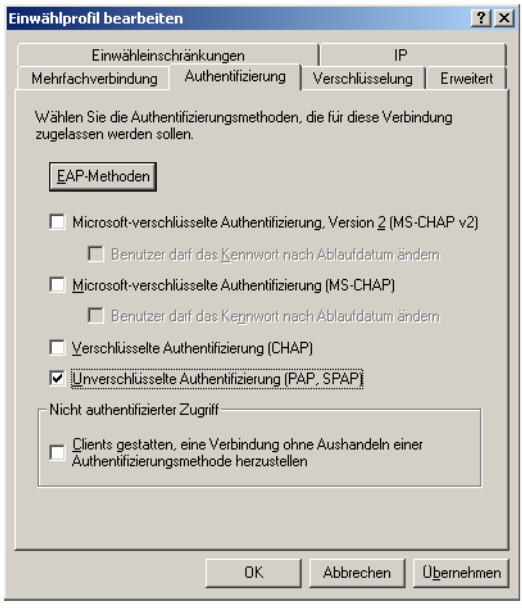


Abbildung 7.38: Wahl der Verschlüsselungsmethode für die Kommunikation zwischen RADIUS- und ISA Server

12. Klicken Sie dann auf WEITER und beenden Sie den Assistenten. Die neue Richtlinie wird unter RAS-RICHTLINIEN angezeigt. Befinden sich dort noch weitere Richtlinien, muss die neue Richtlinie über das Kontextmenü NACH OBEN oder NACH UNTEN an die gewünschte Position gebracht werden.
13. Damit diese neue Richtlinie korrekt umgesetzt werden kann, muss für sämtliche Benutzer der Domäne die Berechtigung zum Einwählen gegeben sein. Öffnen Sie dazu die mmc ACTIVE DIRECTORY-BENUTZER UND COMPUTER auf dem RADIUS-Server.
14. Zeigen Sie die Eigenschaften eines Benutzers an und wechseln Sie dort auf die Registerkarte EINWÄHLEN. Wählen Sie dort die Option ZUGRIFF ÜBER RAS-RICHTLINIEN STEUERN. Diese Option ist jedoch nur anwählbar, wenn die Domäne im Gesamtstrukturfunktionsmodus *Windows 2000 pur* oder *Windows Server 2003* ausgeführt wird. Ist dies nicht der Fall, wählen Sie die Option ZUGRIFF GESTATTEN.

Damit ist die Konfiguration auf Seiten des RADIUS-Servers abgeschlossen.

Wahl der RADIUS-Authentifizierungsmethode

Nachdem Sie den RADIUS-Server eingerichtet haben, wählen Sie auf der Registerkarte AUTHENTIFIZIERUNG diese Methode und klicken Sie auf DOMÄNE AUSWÄHLEN. Geben Sie hier die Domäne zur Authentifizierung des Benutzers an. Klicken Sie dann auf RADIUS-SERVER und geben den Namen bzw. die IP-Adresse des Servers sowie den Port und ein Zeitlimit an (siehe Abbildung 7.39)

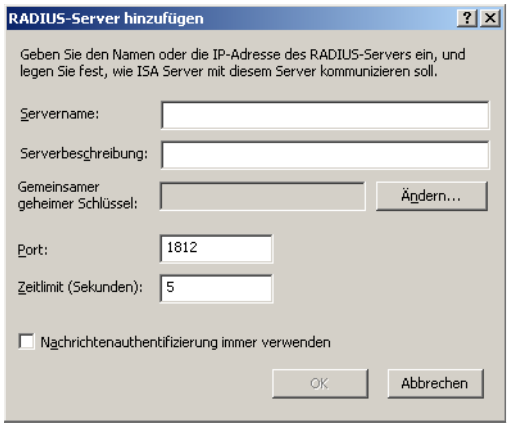


Abbildung 7.39: Konfiguration der Methode RADIUS

Anmeldefenster für den Client

Ist auch dieser Schritt erledigt, ist die RADIUS-Authentifizierung wirksam. Sobald ein Webproxy-Benutzer eine Webseite aufruft, erhält er ein Anmeldefenster, in dem er seinen Benutzernamen und sein Kennwort eingeben muss. Da in der RAS-Richtlinie die unverschlüsselte Kommunikation zwischen dem RADIUS- und ISA Server gewählt wurde, sollte unter Sicherheitsaspekten eine Verschlüsselung mit Hilfe von IPSec erfolgen.

7.4.8 Authentifizierung eines Servers

Sonderfall

Bei einem Client werden die Anmeldeinformationen des aktuellen Benutzers zur Authentifizierung an den ISA Server geschickt, allerdings ist bei einem Server in der Regel kein Benutzer angemeldet. Dennoch muss es möglich sein, dass der Server Authentifizierungsinformationen an den ISA Server sendet. Hierfür können Sie entweder das Programm *FWCCredts.exe* benutzen oder eine Zugriffsregel nur für den Server erstellen.

FWCCredts.exe

Programm bereits installiert

Dieses Kommandozeilenprogramm wird bei der Installation des Firewall-Clients automatisch mitinstalliert. Mit Hilfe dieses Programms kann eine Anwednung oder ein Dienst des internen Servers die Authentifizierung am ISA Server durchführen, ohne dass dazu am internen Server ein Benutzer angemeldet sein muss. Verwenden Sie dazu die folgende Kommandozeile:

```
Fwccredts.exe name_des_dienstes /s Benutzername Kennwort
Domäne ↵
```

Sie geben in dieser Kommandozeile zuerst den Namen der Anwendung oder des Dienstes an. Über den Parameter `/s` wird angezeigt, dass zusätzlich Anmeldeinformationen angegeben werden. Für diese Informationen werden der Benutzername, das zugehörige Kennwort sowie die Domäne des Benutzerkontos angegeben.

Zugriffsregel

Regel speziell für den Server

Alternativ können Sie auch eine Zugriffsregel erstellen, die ohne Authentifizierung ausgewählte Protokolle zulässt. In diesem Fall wird zunächst ein neuer Computersatz oder ein Computerobjekt angelegt, der bzw. das als einziges Objekt den internen Server enthält. Dieser Computersatz oder das Computerobjekt werden als Zugriffsregelquelle ausgewählt.

Damit diese Zugriffsregel auch korrekt umgesetzt werden kann, muss sie vor anderen Zugriffsregeln in der Reihenfolge stehen, die den Benutzern über eine Authentifizierung den Zugriff erlauben.

7.5 Web- und Firewall-Verkettungen

Eine Webverkettung kann nur dann angewendet werden, wenn im Unternehmen mehrere ISA Server an unterschiedlichen Standorten mit nur einem zentralen Internetzugang vorhanden sind. Befindet sich nur ein ISA Server im Unternehmen, werden alle Anfragen der Webproxy-Clients direkt an das Internet weitergeleitet. Bei der Webverkettung wird die Anfrage von einem ISA Server an einen anderen weitergeleitet, der dann seinerseits die Anfrage an das Internet weiterleitet.

Upstream- und Downstream-Server

In Abbildung 7.40 sehen Sie, dass für das Unternehmen die Internetverbindung nur über den ISA Server der Zentrale hergestellt wird. Der ISA Server der Zentrale fungiert in dieser Konstellation als Upstream-Server. Die beiden Standorte verfügen auch jeweils über einen ISA Server. Diese beiden sind Downstream-Server, da sie über keine direkte Internetverbindung verfügen, sondern die Anfragen an den Upstream-Server der Zentrale weiterleiten.

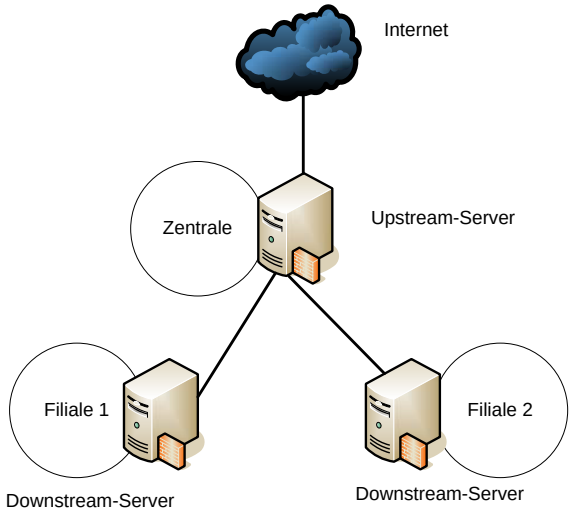


Abbildung 7.40: Übersicht über Upstream- und Downstream-Server

Sobald ein Client an einem der beiden Standorte eine Webanfrage sendet, werden die folgenden Schritte ausgeführt:

1. Der Webproxy-Client stellt an den ISA Server des Standorts seine Anfrage nach der gewünschten Webseite.
2. Der ISA Server am Standort schaut nach, ob sich die angeforderte Seite in seinem lokalen Cache befindet. Befinden sich dort alle Objekte, werden diese an den Client zurückgegeben. Befinden sich die Objekte nicht im lokalen Cache, stellt der ISA Server des Standorts die entsprechende Anfrage an den ISA Server der Zentrale.
3. Daraufhin durchsucht der ISA Server der Zentrale seinen lokalen Cache. Befinden sich dort die gewünschten Objekte, werden diese an den ISA Server des Standorts zurückgegeben, der sie seinerseits an den Client weitergibt.
4. Befinden sich die Objekte nicht im Cache des ISA Server der Zentrale, stellt dieser eine entsprechende Anfrage an einen Internetserver.
5. Der ISA Server der Zentrale speichert die Objekte in seinem Cache und sendet sie an den ISA Server des Standorts. Dieser gibt sie an den Client weiter.

Leistungsoptimierung

Durch die Anwendung dieser Form von Webverkettung wird die Leistung optimiert. Da mehrere Caches durchsucht werden, steigt die Wahrscheinlichkeit, dass die angeforderten Objekte dort bereits vorhanden sind, so dass sich die Antwortzeit für den Client verringert.

7.5.1 Webverkettung für Webproxy-Clients

Standardregel vorhanden

Nach der Installation des ISA Server ist bereits eine Regel zur Webverkettung vorhanden. Diese Webverkettungsregel besagt, dass alle Webanfragen direkt an das Internet weitergeleitet werden. Um weitere Regeln zu dieser hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Navigieren Sie in der ISA-mmc zu KONFIGURATION/NETZWERKE und wechseln zur WEBVERKETTUNG.
2. Wählen Sie aus dem Aufgabenbereich den Eintrag NEUE WEBVERKETTUNGSREGEL ERSTELLEN.
3. Geben Sie einen Namen für die neue Regel an und klicken Sie auf WEITER.
4. Im Fenster WEBVERKETTUNGSREGELZIEL bestimmen Sie, für welche Ziele die Weiterleitung an einen anderen ISA Server erfolgen soll. Normalerweise wird dort das Netzwerk *Extern* gewählt.
5. Dann gelangen Sie in das Fenster AKTION ANFORDERN. Dort wird bestimmt, wie das Ziel die Clientanfragen nach dem gewünschten Inhalt verarbeiten soll. Dazu stehen die folgenden Optionen zur Verfügung (siehe Abbildung 7.41):
   - ANFORDERUNGEN DIREKT VOM ANGEGEBENEN ZIEL ABRUFEN bzw. ANFORDERUNGEN AN ANGEGEBENEN UPSTREAMSERVER WEITERLEITEN: Mit der ersten Option erfolgt der Abruf direkt aus dem Inter-

net, mit der zweiten vom anzugebenen Upstream-Server. Nur für die zweite Option sind die folgenden weiteren verfügbar.

- DELEGIERUNG DER ANMELDEINFORMATIONEN FÜR BASISAUTHENTIFIZIERUNG ZULASSEN: Sofern nur am Upstream-Server eine Benutzerauthentifizierung notwendig ist, werden die Benutzerinformationen vom Downstream-Server an diesen weitergeleitet. Ist an beiden Servern eine Authentifizierung notwendig (man spricht in diesem Fall von verketteter Authentifizierung), ist eine doppelte Anmeldung des Benutzers notwendig. Ist diese Option aktiviert, muss jedoch nur eine einmalige Authentifizierung am Downstream-Server erfolgen. Die Anmeldeinformationen werden von diesem an den Upstream-Server weitergeleitet.
- ANFORDERUNGEN UMLEITEN AN: Die angeforderte Anfrage kann anstatt direkt an das Internet oder einen Upstream-Server auch an eine bestimmte Webseite weitergeleitet werden. Auf diese Weise können z.B. alle Anfragen an Webseiten, auf die kein Zugriff erfolgen soll, an eine spezielle Webseite weitergeleitet werden, die vom Administrator erstellt wurde und den Benutzer darüber aufklärt, warum die gewünschte Seite nicht verfügbar ist.
- AUTOMATISCHES EINWÄHLEN VERWENDEN: Der ISA Server kann bei Bedarf eine DFÜ-Verbindung herstellen.

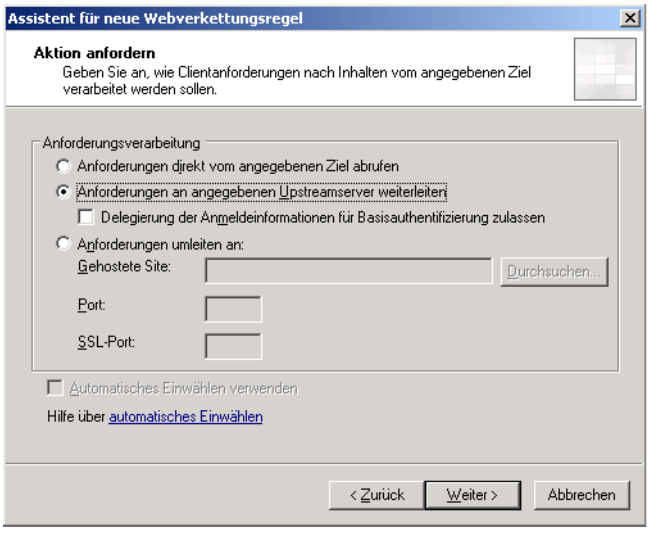


Abbildung 7.41: Konfiguration der Weiterleitung

6. Klicken Sie dann auf WEITER und geben Sie als Nächstes im Fenster PRIMÄRES ROUTING den Namen oder die IP-Adresse des ISA Server an, an den die Weiterleitung erfolgen soll. Zusätzlich ist der Port anzugeben (siehe Abbildung 7.42).

Wenn der vorgegebene Port geändert wird, müssen Sie auch auf dem Upstream-Server den Listener entsprechend ändern.

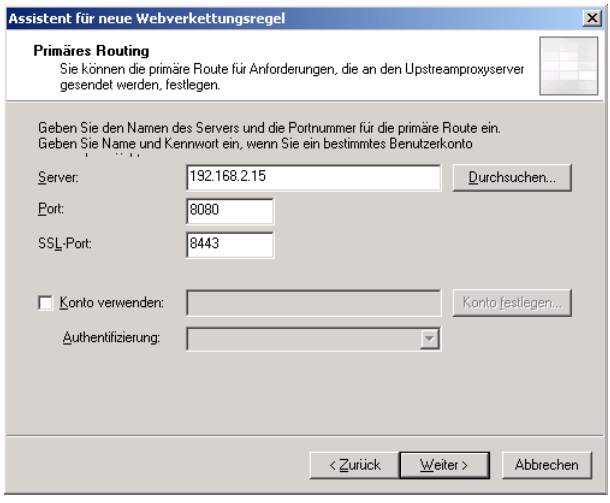


Abbildung 7.42: Wahl des Servers, an den die Weiterleitung erfolgen soll

Authentifizierung am Upstream-Server

Sofern am Upstream-Server eine Authentifizierung notwendig ist, markieren Sie die Checkbox KONTO VERWENDEN und klicken auf KONTO FESTLEGEN und geben das erforderliche Konto und Kennwort an. Klicken Sie dann auf WEITER.

7. Im Fenster RESERVEAKTION (siehe Abbildung 7.43) können Sie bestimmen, wie mit der Anfrage verfahren werden soll, wenn der Upstream-Server nicht verfügbar ist. Mit ANFORDERUNGEN IGNORIEREN wird die Anfrage nicht weitergeleitet und nicht bearbeitet. Ist ANFORDERUNGEN DIREKT VOM ANGEGEBENEN ZIEL ABRUFEN gewählt, erfolgt die Anfrage direkt an das Internet. Mit ANFORDERUNGEN AN ANDEREN UPSTREAM-SERVER WEITERLEITEN wird die Anfrage an einen anderen Upstream-Server gesendet. Klicken Sie dann auf WEITER und beenden Sie im nächsten Schritt den Assistenten. Übernehmen Sie dann die Konfigurationsänderungen.

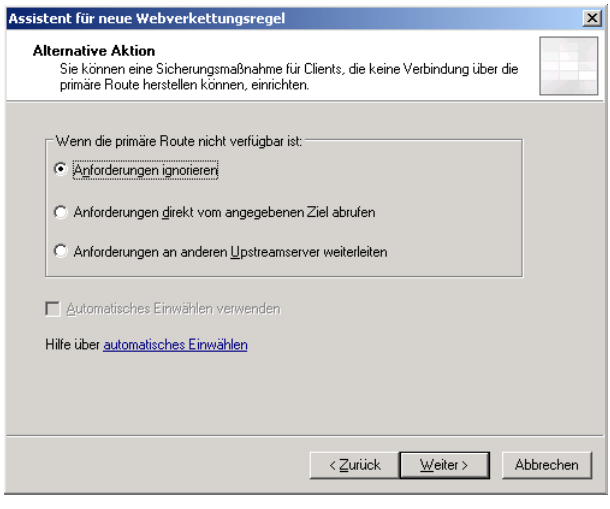


Abbildung 7.43: Wahl der Aktion, wenn der definierte Server nicht verfügbar ist

Definition von Ausnahmen

Sobald eine Webverkettung erstellt wurde, kann diese wie z.B. auch die Zugriffsrichtlinien über die EIGENSCHAFTEN bearbeitet werden. Dort sind einige weitere Optionen verfügbar, die über den Assistenten nicht eingestellt werden können. So können auf der Registerkarte NACH Ausnahmen für Zugriffsziele definiert werden, für die keine Weiterleitung erfolgen soll. Für eingehenden Verkehr können weitere Optionen auf der Registerkarte BRIDGING (siehe Abbildung 7.44) eingestellt werden. Dort sind die folgenden Einstellungen möglich:

- HTTP-ANFORDERUNGEN UMLEITEN ALS: Eine http-Anfrage kann vom ISA Server auch als https-Anfrage weitergeleitet werden. Wird von einem veröffentlichten Webserver eine http-Seite bereitgestellt, ist es möglich, dass die entsprechende Anfrage zur Weiterleitung vom ISA Server an den internen Webserver verschlüsselt wird.
- SSL-ANFORDERUNGEN UMLEITEN ALS: Eine https-Anfrage kann vom ISA Server auch als gewöhnliche http-Anfrage weitergeleitet werden. Wird von einem veröffentlichten Webserver eine http-Seite bereitgestellt, ist es möglich, dass die entsprechende Anfrage zur Weiterleitung vom ISA Server an den internen Webserver nicht verschlüsselt wird.
- SICHERER KANAL (SSL) IST ERFORDERLICH: Eine Anfrage muss über https erfolgen. Eine http-Anfrage wird nicht angenommen.
- 128-BIT-VERSCHLÜSSELUNG IST ERFORDERLICH: Die Verschlüsselungsstärke muss 128 Bit betragen. Anfragen mit anderen Verschlüsselungen werden nicht angenommen.
- ZERTIFIKAT FÜR AUTHENTIFIZIERUNG MIT DEM SSL-WEBSERVER VERWENDEN: Das Zertifikat muss angegeben werden, wenn der ISA Server zur Authentifizierung am internen Webserver ein Zertifikat benutzen muss.

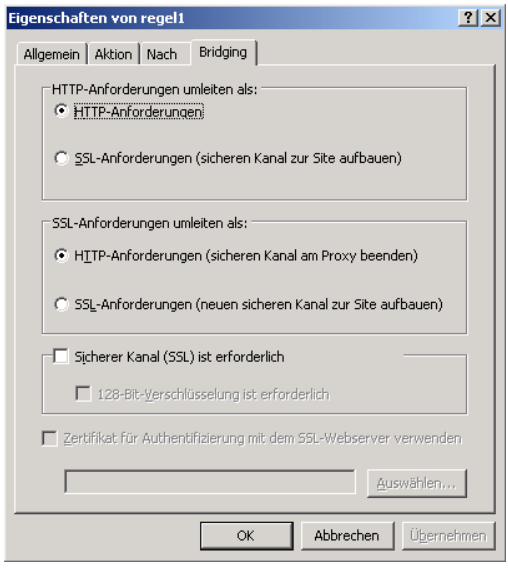


Abbildung 7.44: Weitere Optionen zur Umleitung von Anforderungen

7.5.2 Firewall-Verkettungen für SecureNAT- und Firewallclients

Firewall- statt Webverkettung

Eine Webverkettung kann nur für den Webproxyclient erfolgen. Für den Firewall- und SecureNAT-Client ist lediglich eine Firewall-Verkettung möglich. Über die Firewall-Verkettung ist zusammen mit der Webverkettung eine noch feiner konfigurierbare Weiterleitung der Anfragen möglich.

So ist es möglich, die Anfragen der Webproxyclients anders zu routen als die der beiden anderen Clients. Dies kann sinnvoll sein, wenn für die Anfragen verschiedene Internetverbindungen genutzt werden sollen.

Um eine Firewall-Verkettung einzurichten, führen Sie die folgenden Schritte durch:

1. Navigieren Sie in der ISA-mmc zu KONFIGURATION/ALLGEMEIN. Dort wählen Sie im Aufgabenbereich FIREWALLVERKETTUNG KONFIGURIEREN.
2. Tragen Sie auf der Registerkarte FIREWALLVERKETTUNG (siehe Abbildung 7.45) den Namen oder die IP-Adresse des Upstream-Servers ein. Wenn erforderlich, legen Sie auch noch das für die Authentifizierung erforderliche Benutzerkonto fest. Bestätigen Sie die Eingaben mit OK.

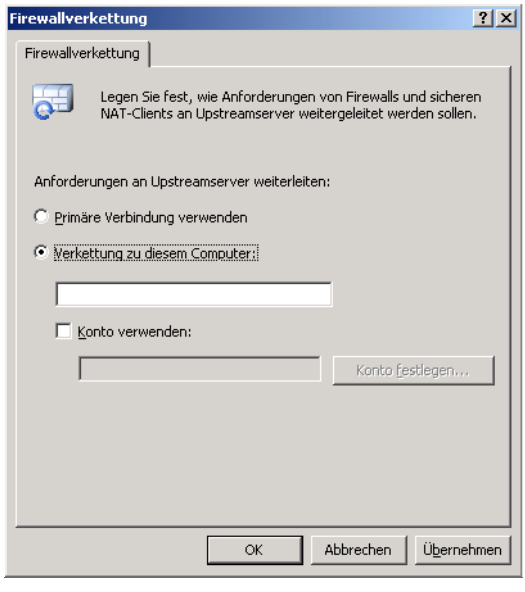


Abbildung 7.45: Die Webverkettung zum angegebenen Computer wählen

8 Veröffentlichen von Servern und Diensten

Dieses Kapitel beschäftigt sich mit der Veröffentlichung verschiedener Servertypen wie Websever, Mailserver, DNS-Server oder auch *OWA (Outlook Web Access)* durch den ISA Server, so dass Clients von außerhalb auf diese Server zugreifen können. Auch diese eingehenden Zugriffe sowie die für diese Zugriffe zu definierenden Zugriffsregeln werden in diesem Kapitel vorgestellt. Eine wichtige Grundlage für die Zugriffe ist auch das Auswählen und Konfigurieren des passenden Authentifizierungsmechanismus. Des Weiteren wird auch die Veröffentlichung von Diensten direkt auf dem ISA Server sowie die damit verbundene Problematik des Socket Pooling besprochen.

8.1 Eingehende Zugriffe und Veröffentlichung

Nachdem Sie im letzten Kapitel die ausgehenden Zugriffe kennengelernt haben, stehen in diesem Kapitel die eingehenden Zugriffe im Vordergrund. Unter eingehenden Zugriffen versteht man die Anfragen von Clients aus externen Netzwerken auf Server, die durch den ISA Server veröffentlicht wurden.

Hinter dem ISA Server befindliche Server veröffentlichen

Durch die Veröffentlichung kann auf interne Server und Dienste, die sich hinter dem ISA Server befinden und durch diesen geschützt werden, von anderen Netzwerken aus zugegriffen werden. Die Server oder Dienste können so im Internet oder in einem anderen Netzwerk veröffentlicht werden. Sobald von außen eine Anfrage an einen Server erfolgt, wird diese zunächst vom ISA Server angenommen. Die Pakete werden anhand von Filtern und Regeln bis hinunter auf die Anwendungsebene analysiert. Die Analyse wie auch generell die Annahme einer Verbindung wird über einen Listener (Abhörer) realisiert. Ist für eine Verbindung kein Listener vorhanden, so wird diese Verbindung vom ISA Server getrennt. Nur wenn eine Anfrage als gültig angesehen wird, werden die gesendeten Pakete an den internen veröffentlichten Server weitergeleitet. Die Anfrage wird vom Server beantwortet. Die Pakete dieser Antwort werden vom Server erst an den ISA Server und über diesen an den Client weitergeleitet. Auf diese Weise sind die internen Server durch den ISA Server geschützt, da ein externer Client niemals direkt mit dem internen Server kommunizieren kann.

Keine Auslagerung zum Internetdienstanbieter

Die Veröffentlichung kann natürlich nur dann durchgeführt werden, wenn sich der betreffenden Server im Unternehmensnetz befindet und nicht zu einem Internetdienstanbieter ausgelagert wurde, z.B. für die Internetpräsentation des Unternehmens. Durch eine selbstständige Verwaltung der Server können unternehmensspezifische Anforderungen wie z.B. bestimmte Zugriffsregeln oder die Anforderungen an die Hochverfügbarkeit eigenständig umgesetzt werden. Dies wäre bei der Verwaltung des Servers durch einen Internetprovider nicht oder nur in beschränktem Umfang gewährleistet. Allerdings müssen Sie bei der eigenen Verwaltung der Server immer bedenken, dass Sie nun allein für deren korrekte Konfiguration und Verfügbarkeit verantwortlich sind.

Für den laufenden Betrieb der veröffentlichten Server müssen also neben der Absicherung durch unbefugte Zugriffe über den ISA Server auch Maßnahmen zur laufenden Sicherung und Wiederherstellung der Systeme sowie der allgemeinen Administration durchgeführt werden. Für diese Aufgaben muss genügend und vor allen Dingen auch ausreichend geschultes Personal zur Verfügung stehen.

8.2 Zugriffs- und Webveröffentlichungsregeln

Um die veröffentlichten Server vor unbefugten Zugriffen zu schützen und den Zugriff kontrollieren und im Bedarfsfall blockieren zu können, müssen dazu Regeln definiert werden. Für diese Regeln gibt es zwei unterschiedliche Regeltypen, nämlich die Zugriffsregeln und die Webveröffentlichungsregeln. Der Einsatz dieser beiden Regeltypen ist davon abhängig, in welcher Form die Netzwerke miteinander verknüpft sind, zwischen denen eine Kommunikation erfolgen soll.

8.2.1 Webveröffentlichungsregeln

NAT-Übersetzung für eingehenden Verkehr

Webveröffentlichungsregeln können ausschließlich zwischen Netzwerken eingesetzt werden, die über eine NAT- oder eine Route-Verbindung miteinander verknüpft sind. Für sämtlichen eingehenden Datenverkehr findet dabei eine NAT-Übersetzung statt. Für folgende Szenarien von Netzwerken können die Webveröffentlichungsregeln eingesetzt werden:

- Internes Netzwerk mit privaten IP-Adressen und NAT-Beziehung
- Perimeternetzwerk mit öffentlichen IP-Adressen und Route-Beziehung
- Perimeternetzwerk mit öffentlichen IP-Adressen und NAT-Beziehung
- Perimeternetzwerk mit privaten IP-Adressen und NAT-Beziehung

Bei allen diesen Szenarien wird von außen eine Verbindung mit dem Netzwerkadapter für die externe Verbindung des ISA Server hergestellt. Durch eine Webveröffentlichungsregel wird diese Anfrage an die öffentliche IP-Adresse des veröffentlichten Servers weitergeleitet. Sofern die Webveröffentlichungsregel nicht anders konfiguriert ist, erfolgt dabei eine Übersetzung der Verbindung, wobei die IP-Adresse des ISA Server als Client-IP-Adresse angegeben wird.

Die Webveröffentlichungsregel kann jedoch auch so konfiguriert werden, dass die Client-IP-Adresse des externen Clients an den veröffentlichten Server gesendet wird.

8.2.2 Zugriffsregeln

Auch Zugriffsregeln können zwischen Netzwerken eingesetzt werden, die über eine Route- oder NAT-Verbindung miteinander verknüpft sind. Die Zugriffsregeln können in den folgenden beiden Szenarien eingesetzt werden:

- Perimeternetzwerk mit öffentlichen IP-Adressen und Route-Beziehung
- Perimeternetzwerk mit öffentlichen IP-Adressen und NAT-Beziehung

Allerdings unterscheidet es sich in beiden Szenarien, wie die Verbindung zum veröffentlichten Server hergestellt wird.

Keine NAT-Übersetzung

Beim Perimeternetzwerk mit öffentlichen IP-Adressen und einer Route-Beziehung wird eine eingehende Verbindung direkt mit der IP-Adresse des oder der DMZ-Server hergestellt. Dabei wird als IP-Adresse des Clients die des externen Clients erfasst und protokolliert.

Sofern jedoch eine http-Verbindung verwendet wird, wird diese über den Webproxy-Filter verarbeitet, so dass die IP-Adresse des ISA Server und nicht die des externen Clients protokolliert wird. Um in diesem Fall dennoch die IP-Adresse des externen Clients ermitteln zu können, darf keine Verknüpfung mehr zwischen dem http-Protokoll und dem Webproxy-Filter bestehen. Bedenken Sie jedoch, dass bei dieser Entkopplung keine http-Filterung sowie kein Reverse-Caching mehr möglich sind.

Direkte Weiterleitung

Anders liegt der Fall beim Perimeternetzwerk mit öffentlichen IP-Adressen und NAT-Beziehung. In diesem Szenario werden die eingehenden Verbindungen direkt an die externe Schnittstelle des ISA Server weitergeleitet. Über die Zugriffsregel wird die Anfrage des externen Clients an die öffentliche IP-Adresse des veröffentlichten Servers weitergeleitet. Durch die NAT-Übersetzung wird dabei die Adresse des ISA Server als Client-IP-Adresse angegeben.

Die Zugriffsregel kann jedoch auch so konfiguriert werden, dass die Client-IP-Adresse des externen Clients an den veröffentlichten Server gesendet wird.

8.2.3 Welcher Regeltyp soll verwendet werden?

Die Entscheidung, ob eine Zugriffsregel oder eine Webveröffentlichungsregel eingesetzt werden soll, richtet sich nicht nur nach dem Szenario des Einsatzes, sondern auch nach einigen weiteren Bedingungen, die folgend erläutert werden.

- *Filterung*: Wird eine Zugriffsregel verwendet, können nur Paketfilter verwendet werden. Beim Einsatz von Webveröffentlichungsregeln hingegen kann der eingehende Verkehr bis hin zur Anwendungsebene gefiltert werden.
- *Weblistener*: Beim Einsatz von Webveröffentlichungsregeln werden Weblistener eingesetzt, so dass bereits am ISA Server eine Authentifizierung (z.B. SecureID, RADIUS oder auch formularbasierte OWA-Authentifizierung) erfolgen kann. Wird hingegen eine Zugriffsregel verwendet, kann der ISA Server keine Authentifizierung durchführen. Die Authentifizierung muss stattdessen am veröffentlichten Server erfolgen.
- *Protokolle*: Bei Webveröffentlichungsregeln werden Inbound-Protokolle und bei Zugriffsregeln Outbound-Protokolle (auch für den eingehenden Netzwerkverkehr) verwendet.
- *Linkübersetzung*: Die Linkübersetzung ist nur bei Webveröffentlichungsregeln, nicht jedoch bei Zugriffsregeln verfügbar. Durch die Linkübersetzung werden Verweise auf interne Servernamen so übersetzt, dass die externen Clients eine Verknüpfung als zurückgegebenen Wert erhalten.
- *SSL-to-SSL-Bridging*: Bei der Verwendung von https-Seiten sollten Sie in jedem Fall auch auf Webveröffentlichungsregeln zurückgreifen, da bei Zugriffsregeln der ISA Server die Paketinhalte nicht analysiert werden, sondern direkt an den veröffentlichten Server weitergeleitet werden. Bei Webveröffentlichungsregeln hingegen ist es möglich, das so genannten SSL-to-SSL-Bridging einzurichten. Dabei wird die SSL-verschlüsselte Verbindung am ISA Server beendet, und die Pakete werden dort geprüft. Danach werden die Pakete wieder verschlüsselt und an den veröffentlichten Server weitergegeben.
- *FQDN und IP-Adressen*: Mit einer Webveröffentlichungsregel kann festgelegt werden, dass der eingehende Zugriff nur auf einen bestimmten vollqualifizierten Domänennamen (FQDN) und nicht auf eine IP-Adresse erfolgen darf. Bei einer Zugriffsregel hingegen kann der Zugriff immer auf eine IP-Adresse erfolgen. Dabei besteht die Gefahr, dass beispielsweise von Robots IP-Adressen verwendet werden, um Server auszuspionieren oder anzugreifen.

Höhere Sicherheit durch Webveröffentlichungsregeln

Sie sehen also anhand dieser Übersicht, dass Webveröffentlichungsregeln gegenüber Zugriffsregeln immer die höhere Sicherheit bieten, z.B. aufgrund der Möglichkeit, den eingehenden Verkehr bis hinunter zur Anwendungsebene zu prüfen. Wenn es also möglich ist, sollten Sie immer diesen Regeltyp bevorzugen.

Allerdings kann in einigen Szenarien auch der Einsatz von Zugriffsregeln durchaus ausreichend und sinnvoller sein. Dies ist beispielsweise dann der Fall, wenn Server in einer DMZ über öffentliche IP-Adressen verfügen. Existieren bereits umfangreiche DNS-Verweise auf diese Server, kann eine entsprechende Neu- bzw. Umkonfiguration der Einträge sehr aufwändig werden. In dieser Situation machen Zugriffsregeln durchaus Sinn, da mit ihnen keine Umkonfiguration notwendig ist. Allerdings kann nur noch für veröffentlichte Webserver die http-Filterung über den Webproxy-Filter erfolgen. Für alle anderen veröffentlichten Serverdienste können keine Filter mehr gesetzt werden, so dass für diese ein höheres Angriffs- und Gefahrenpotenzial besteht.

Zugriffsregeln für eingehenden Netzwerkverkehr werden genauso konfiguriert wie die Zugriffsregeln für ausgehenden Netzwerkverkehr. Diese Schritte wurden bereits in Kapitel 7.5 behandelt.

8.3 Veröffentlichen eines Webservers

http oder https

Dieses und die folgenden Kapitel beschäftigen sich mit der praktischen Umsetzung der Veröffentlichung. Bei einigen Arbeistsschritten gibt es Parallelen zwischen den verschiedenen Servertypen. Zunächst wird die Veröffentlichung eines Webservers beschrieben. Dabei wird unterschieden, ob es sich um eine herkömmliche (http) oder sichere (https) Webserver-Veröffentlichung handelt.

8.3.1 Herkömmliche Webserver-Veröffentlichung

http-Filter

Wird ein interner Webserver im Internet veröffentlicht, kann auf diesen von externen Quellen aus zugegriffen werden. Für die Prüfung der eingehenden Pakete verwendet der ISA Server den http-Filter. Damit werden die Pakete bis hinunter zur Anwendungsebene geprüft. Zusätzlich können die internen Webserver von der Reverse Caching-Funktion des ISA Server profitieren. Dadurch können Clientanfragen schneller beantwortet werden. Weitere Hinweise zum Reverse Caching finden Sie in Kapitel 11.

Um einen Webserver zu veröfentlichen, führen Sie die folgenden Schritte durch:

1. Navigieren Sie in der ISA-mmc zur FIREWALLRICHTLINIE und wählen aus dem Kontextmenü den Eintrag NEU/WEBSERVERVERÖFFENTLICHUNGSREGEL. Ein Assistent wird gestartet.
2. Geben Sie der Regel einen Namen und klicken Sie auf WEITER.
3. Im Fenster REGELAKTION wählen Sie ZULASSEN und klicken Sie auf WEITER.
4. Im folgenden Fenster ZU VERÖFFENTLICHENDE WEBSITE FESTLEGEN (siehe Abbildung 8.1) tragen Sie entweder den FQDN oder die IP-Adresse des internen Webservers ein. Wird der FQDN angegeben, müssen Sie sicherstellen, dass das interne DNS korrekt konfiguriert ist und der ISA Server den FQDN des internen Servers auflösen kann. Das Gleiche gilt auch, wenn sich der interne Webserver in einem Perimeternetzwerk befindet. Wichtig ist auch die Option URSPRÜNGLICHEN HOSTHEADER ANSTELLE DES AKTUELLEN (ODER ANGEGEBENEN) WEITERLEITEN. Ein Hostheader dient dazu, dass ein einziger Webserver mit nur einer IP-Adresse mehrere virtuelle Webserver betreiben kann. Jeder virtuelle Server besitzt einen individuellen Hostheader. Um die Clientanfragen an den korrekten virtuellen Server weiterleiten zu können, wird die vom Client im Browserfenster eingegebene Adresse des Servers mit dem Hostheader der einzelnen virtuellen Server verglichen. Die Checkbox muss in jedem Fall aktiviert sein, wenn der veröffentlichte Webserver mit Hostheadern arbeitet. Ansonsten wird bei einer Clientanfrage nicht der Hostheader verwendet, sondern der eingegebene Name in den Wert geändert, der unter COMPUTERNAME ODER IP-ADRESSE angegeben ist. Soll eine Clientanfrage direkt an ein virtuelles Verzeichnis des Webservers weitergeleitet werden, so tragen Sie dieses unter PFAD ein. Klicken Sie dann auf WEITER.

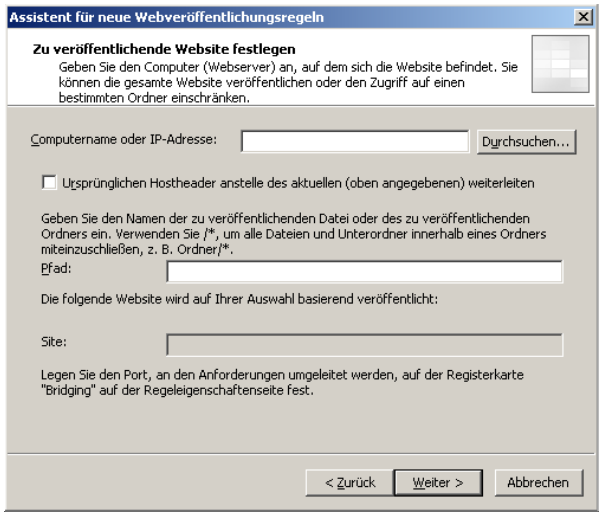


Abbildung 8.1: Festlegen des zu veröffentlichenden Webservers

Zugriff nur auf Webserver

5. Im folgenden Fenster DETAILS DES ÖFFENTLICHEN NAMENS (siehe Abbildung 8.2) bestimmen Sie, ob der Client für eine gültige Anfrage den FQDN oder auch die IP-Adresse des Webservers verwenden kann. Aus Sicherheitsgründen sollten Sie unter ANFORDERUNGEN ANNEHMEN FÜR die Option DIESEN DOMÄNENNAMEN (UNTEN EINGEBEN) wählen. Sobald nun bei einer Clientanfrage ein anderer Hostheader als der FQDN angegeben wird, z.B. die IP-Adresse, so wird die Anfrage vom ISA Server blockiert und nicht weitergeleitet. Wählen Sie die Option JEDEN DOMÄNENNAMEN, kann keine so explizite Kontrolle erfolgen. Mit der ersten Option ist sichergestellt, dass lediglich der Webserver angesprochen werden kann, mit der zweiten theoretisch auch ein anderer Server der Domäne, dessen Name bekannt ist. Klikken Sie dann auf WEITER.

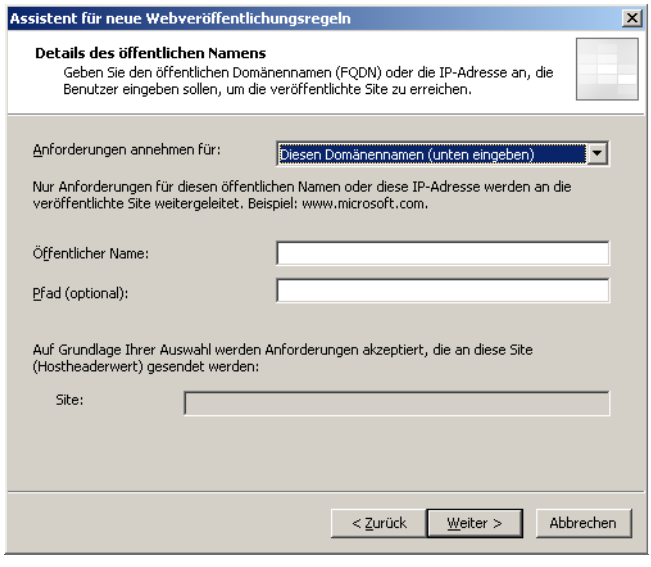


Abbildung 8.2: Festlegen des Namens, den die Benutzer für den Zugriff angeben müssen

6. Da die Anfrage der Clients zunächst vom ISA Server angenommen wird, muss auf diesem ein Weblistener konfiguriert werden. Mit Hilfe des Weblisteners kann der ISA Server bestimmen, wie mit einer eingehenden Verbindung verfahren werden soll. Klicken Sie dazu auf NEU, um einen neuen Weblistener zu erstellen und legen Sie dann einen Namen dafür fest. Klicken Sie dann auf WEITER.
7. Im Fenster IP-ADRESSEN (siehe Abbildung 8.3) bestimmen Sie das Netzwerk sowie mit einem Klicken auf ADRESSE die IP-Adresse(n), die der ISA Server auf eingehende Anfragen hin abhören soll (siehe Abbildung 8.4). Klicken Sie dann auf OK und WEITER.

Abbildung 8.3: Bestimmen des Netzwerks, das der Weblistener abhören soll

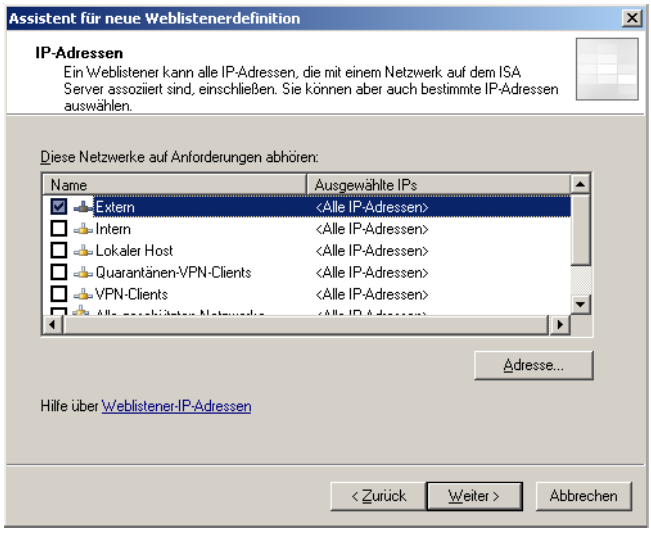
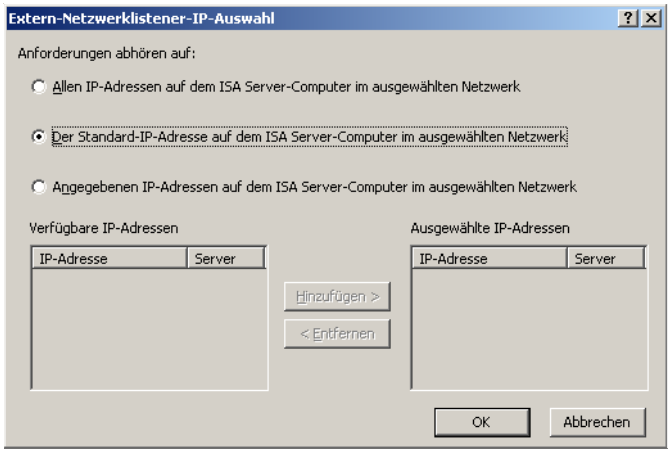


Abbildung 8.4: Das Abhören kann für alle, eine oder die angegebene IP-Adressen gewählt werden



Änderung des Ports

8. Unter PORTSPEZIFIZIERUNG (siehe Abbildung 8.5) wird der Port angegeben, auf dem die Anfragen abgehört werden sollen. Wird http verwendet, übernehmen Sie den Port 80. Theoretisch könnte auch ein anderer Port angegeben werden. Allerdings müsste dieser im Browserfenster mit der Adresse angegeben werden. Da dazu sämtlichen Benutzern der abweichende Port bekannt sein müsste, kann dies bei einem öffentlichen Webserver eigentlich nicht angewendet werden. Zusätzlich kann auch der SSL-Port angegeben werden. Weitere Hinweise zu SSL-Verbindungen finden Sie im folgenden Kapitel. Klicken Sie dann auf WEITER und beenden Sie den Assistenten zum Erstellen des Weblisteners.
9. Sie erhalten das Fenster WEBLISTENER AUSWÄHLEN. Dort wählen Sie den eben erstellten Listener für die Webveröffentlichungsregel aus. Klicken Sie dann auf WEITER.

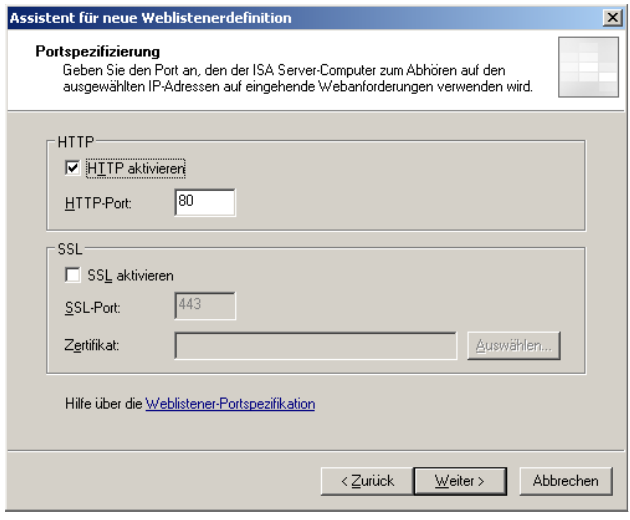


Abbildung 8.5: Angabe des Ports, auf dem der Weblistener arbeiten soll

10. Als Letztes wird festgelegt, welche Benutzer auf den veröffentlichten Webserver zugreifen dürfen (siehe Abbildung 8.6). Soll der Webserver als öffentlicher Webserver beliebigen Benutzern zur Verfügung stehen, wählen Sie den Benutzersatz ALLE BENUTZER aus. Damit ist sichergestellt, dass der ISA Server keine Authentifizierung der Benutzer fordert. Soll ein Webserver hingegen nur für Mitarbeiter des Unternehmens verfügbar sein, wählen Sie den passenden Benutzersatz. Damit ein Mitarbeiter auf den Webserver zugreifen kann, muss er sich zuvor an diesem authentifizieren. Klicken Sie dann auf WEITER und beenden Sie den Assistenten. Mit einem Klick auf ÜBERNEHMEN in der ISA-mmc wird die neue Webveröffentlichungsregel in Kraft gesetzt.

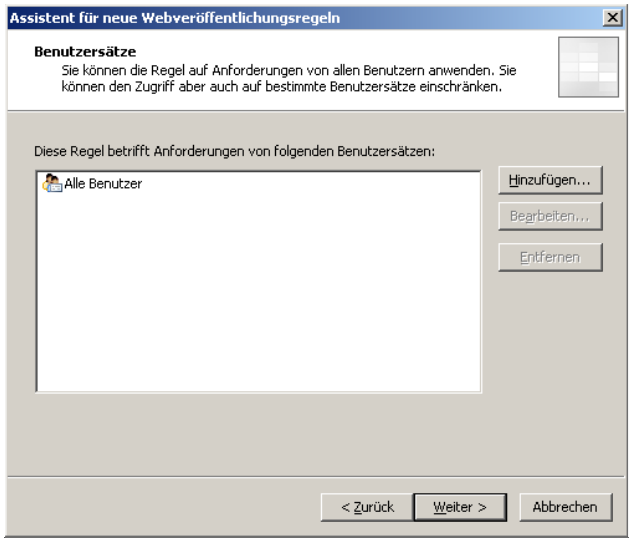


Abbildung 8.6: Auswahl der Benutzer, für die die Webveröffentlichungsregel gelten soll

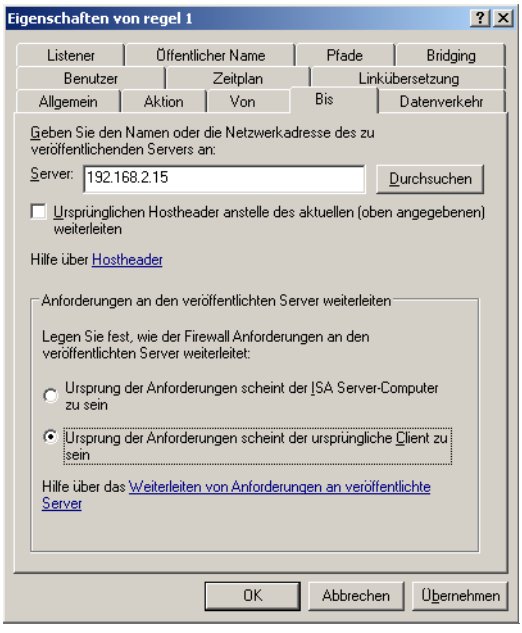
Zusätzliche Einstellungen

Nach der Fertigstellung der Regel können Sie über die Eigenschaften der Regel noch weitere Einstellungen vornehmen. Auf der Registerkarte VON ist standardmäßig der Computersatz BELIEBIG eingetragen. Soll ein Zugriff hingegen nicht von allen Computern aus möglich sein, kann dort ein anderer Computersatz ausgewählt werden.

Quelle der Anfrage

Auf der Registerkarte BIS (siehe Abbildung 8.7) kann festgelegt werden, ob in der Protokollierung der ISA Server oder der eigentlich anfragende Client als Quelle einer Anfrage aufgezeichnet werden soll. Selbstverständlich macht die zweite Option in der Regel mehr Sinn. Markieren Sie dazu die Option URSPRUNG DER ANFORDERUNGEN SCHEINT DER URSPRÜNGLICHE CLIENT ZU SEIN.

Abbildung 8.7: Weiterleitung von Client-Informationen an den veröffentlichten Server



Port-Weiterleitung

Weitere Einstellungen sind auf der Registerkarte BRIDGING (siehe Abbildung 8.8) möglich. Dort kann die Weiterleitung einer http-Anfrage an einen anderen Port als Port 80 eingestellt werden. Dies macht Sinn, wenn der interne Webserver nicht den Standardport verwendet. Soll die Anfrage vom ISA Server an einen FTP-Server weitergeleitet werden, wählen Sie die gleichnamige Option und tragen Sie gegebenenfalls einen abweichenden Port ein, wenn der interne Webserver nicht FTP-Port 21 verwendet.

Intene und externe Servernamen

Auf der Registerkarte LINKÜBERSETZUNG (siehe Abbildung 8.9) können interne Servernamen sowie deren externe Übersetzungsnamen angegeben werden. Daraus ergibt sich quasi ein Wörterbuch. Sobald eine ausgehende Antwort gesendet wird, untersucht der *Link Translation Filter* des ISA Server die festgelegten Einträge interner Servernamen des Wörterbuchs und ändert diese in die externen Namen ab.

Markieren Sie dazu die Checkbox ABSOLUTE LINKS IN WEBSEITEN ERSETZEN und erstellen über HINZUFÜGEN die Wörterbuchliste. Über INHALTSTYPEN kann festgelegt werden, für welche Inhalte wie z.B. Anwendungen, html-Dokumente usw. die konfigurierte Linkübersetzung gelten soll (siehe Abbildung 8.10). Damit die Linkübersetzung korrekt ausgeführt werden kann, muss auf der Registerkarte ÖFFENTLICHER NAME ein Domänenname eingetragen sein.

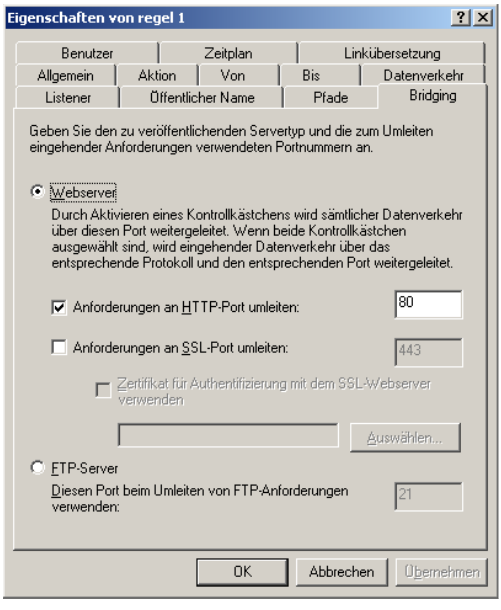


Abbildung 8.8: Weiterleitung an einen anderen Port des veröffentlichten Servers

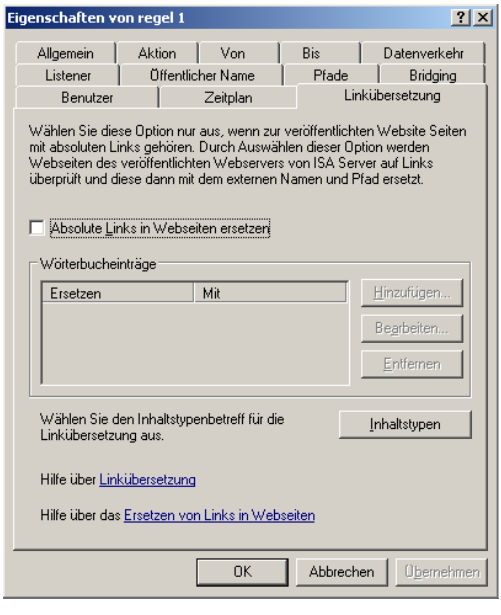


Abbildung 8.9: Konfiguration der Linkübersetzung

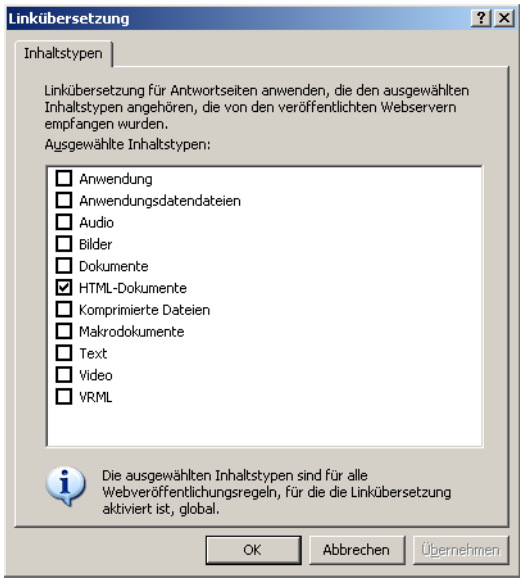


Abbildung 8.10: Auswahl der Inhaltstypen für die Linkübersetzung

http-Filter Wie für den ausgehenden Datenverkehr wird auch für den eingehenden Verkehr ein http-Filter verwendet. Dadurch werden die Anfragen an den Webserver bis hinunter zur Anwendungsebene analysiert und das Risiko eines Angriffs auf den Webserver stark minimiert. Der http-Filter wird über die Registerkarte DATENVERKEHR eingerichtet. Die Konfiguration von http-Filtern ist für eingehenden und ausgehenden Datenverkehr identisch. Die Filterkonfiguration wird ausführlich im eigenständigen Kapitel 9 beschrieben.

Reverse Caching Damit die Clientanfragen an den Webserver schneller beantwortet werden können, sollte das *Reverse-Caching* aktiviert werden. Ist dieses aktiviert, werden angefragte Objekte, die sich bereits im Cache des ISA Server befinden, direkt von diesem an den anfragenden Client gesendet und nicht erst vom Webserver angefordert. Eine detaillierte Beschreibung aller Cache-Funktionen des ISA Server finden Sie in Kapitel 11. Das Reverse Caching kann auch angewendet werden, wenn sich der Webserver in einer DMZ befindet. Die Netzwerke *DMZ* und *Extern* müssen dazu lediglich korrekt miteinander verknüpft worden sein.

8.3.2 Sichere Webserver-Veröffentlichung

https-Verbindungen Von einer sicheren Webserver-Veröffentlichung spricht man, wenn die Seiten des internen Webservers über gesicherte https-Verbindungen bereitgestellt werden. Die Verbindung zwischen dem externen Client und dem internen Server ist verschlüsselt und damit gesichert. Eine verschlüsselte Verbindung sollte immer dann gewählt werden, wenn sensible Daten übertragen werden, z.B. Daten von Kreditkarten

oder Bankverbindungen, wenn auf dem internen Webserver ein Internetshop betrieben wird.

Digitales Zertifikat

Damit https umgesetzt werden kann, muss ein digitales Zertifikat mit einem öffentlichen und einem privaten Schlüssel vorhanden sein. Dieses Zertifikat muss sich auf dem Webserver befinden. Ein Zertifikat kann entweder über eine eigene interne Zertifikatsinfrastruktur bereitgestellt werden oder kann von einem externen Anbieter wie VeriSign o.a. erworben werden.

Für den Einsatz von https kann der ISA Server in zwei verschiedenen Weisen verwendet werden: SSL-Bridging oder SSL-Tunneling.

SSL-Bridging

Wie schon weiter oben kurz erwähnt, wird beim SSL-Bridging oder genauer gesagt SSL-to-SSL-Bridging die verschlüsselte Verbindung am ISA Server beendet und zur Prüfung entschlüsselt. Sobald die Pakete hinsichtlich der Webveröffentlichungsregeln, Web- sowie Anwendungsfilter geprüft worden sind und die Verbindung aufgrund von Filtern und Regeln gestattet ist, wird ein neuer SSL-Tunnel zwischen dem ISA Server und dem internen Webserver hergestellt, über den die Daten erneut verschlüsselt übertragen werden.

SSL-Tunneling

Beim SSL-Tuneling wird ein direkter Tunnel vom externen Client zum veröffentlichten Webserver hergestellt. Am ISA Server erfolgt keine Kontrolle der Pakete, sondern eine direkte Weiterleitung an den Server. Dadurch ist nicht nur der interne Webserver, sondern das gesamte interne Netzwerk einer potenziell höheren Gefahr ausgesetzt. Allerdings ist die Konfiguration des SSL-Tunneling einfacher als die des SSL-Bridging.

8.3.3 Erstellen des Zertifikats

Um eine gesicherte SSL-Verbindung nutzen zu können, muss der Webserver für den SSL-Einsatz vorbereitet werden. Notwendig ist ein Zertifikat mit einem öffentlichen und einem privaten Schlüssel.

Um ein Zertifikat zu beziehen, haben Sie drei verschiedene Möglichkeiten:

1. Sie erwerben ein Zertifikat im Internet, z.B. bei *VeriSign*. Allerdings ist der Erwerb eines Zertifikats mit Kosten verbunden. Andererseits ist dies der schnellste Weg, um ein uneingeschränktes Zertifikat zu beziehen.
2. Sie verfügen bereits über eine Zertifikatsinfrastruktur mit einer eigenen Zertifizierungsstelle und stellen darüber ein Zertifikat bereit. Um nur für eine gesicherte Webserververöffentlichung ein Zertifikat zu beziehen, ist diese Methode jedoch völlig ungeeignet, da eine Zertifikatsinfrastruktur eine komplexe Verwaltung erfordert. Dafür können für sämtliche möglichen Einsatzgebiete eigene Zertifikate erstellt werden.

3. Sofern der Webserver auf IIS 6.0 basiert, also ab Windows Server 2003, können Sie mit Hilfe des Programms *selfssl.exe* selbst Zertifikate erstellen. Dieses Programm ist ein Bestandteil des *IIS6-Resource Kit* und befindet sich auf der Begleit-CD. Dieses Tool kann jedoch keine anderen Zertifikatstypen, z.B. für E-Mail, erstellen und ist damit in seinem Funktionsumfang eingeschränkt, dafür auch kostenlos.

Eigene Zertifikatserstellung

Im folgenden Beispiel wird die dritte Methode verwendet. Um mit Hilfe von *selfssl.exe* ein Zertifikat zu erstellen, führen Sie die folgenden Schritte aus:

1. Installieren Sie entweder das komplette *IIS6-Resource Kit* oder in der benutzerdefinierten Installation nur das Programm *selfssl.exe* auf dem Webserver.
2. Verwenden Sie die folgende Kommandozeile, um auf dem Webserver ein Zertifikat mit dem zugehörigen Schlüsselpaar zu erstellen:

   ```
   Selfssl.exe /T /N:cn=Name des virtuellen Webservers /
   K:4096 /V:500 ↵
   ```

   Diese Parameter haben folgende Bedeutung:

Tabelle 8.1: Die Parameter von selfssl.exe

Parameter	Beschreibung
`/T`	Das ausgestellte Zertifikat wird den vertrauenswürdigen Zertifizierungsstellen hinzugefügt.
`/N:cn=Name des virtuellen Webservers`	Gibt den FQDN des virtuellen Webservers an, für den das Zertifikat erstellt wird. Unter diesem FQDN sollte der Webserver im Webbrowser angesprochen werden.
`/K:4096`	Bestimmt die Länge des asymmetrischen Schlüssels und sollte eine Mindestlänge von 4.096 Bit besitzen.
`/V:500`	Bestimmt in Tagen die Gültigkeitsdauer des Zertifikats. Nach Ablauf dieser Frist muss das Zertifikat erneuert werden.
`Optional /S:`	Diese Option ist nur erforderlich, wenn mehrere virtuelle Webserver vorhanden sind, und gibt den betreffenden virtuellen Server an. Existiert nur ein einziger virtueller Webserver, muss diese Option nicht gesetzt werden.

Wird das Zertifikat über *selfssl.exe* oder auch über eine eigene Zertifizierungsstelle bereitgestellt, so erhält der Benutzer beim Zugriff auf den Server die Warnmeldung, dass das Zertifikat von einer Zertifizierungsstelle stammt, die als nicht vertrauenswürdig eingestuft wird. Der Benutzer kann zwar die Warnmeldung bestätigen und die Verbindung dennoch herstellen, dennoch sollten Sie diese Form der Zertifikate nur für den SSL-Zugriff interner Mitarbeiter auf einen Webserver verwenden. Außenstehende Benutzer könnten im schlimmsten Fall von diesem Hinweis abgeschreckt werden. Dieser Sicherheitshinweis basiert auf einer Liste des jeweiligen Betriebssystems, in der eine Reihe vertrauenswürdiger Zertifikatsanbieter enthalten ist. Sie sollten dann darüber nachdenken, ob Sie nicht lieber ein Zertifikat von *VeriSign* o.a. beziehen sollten oder aber die Zertifizierungsstelle des Unternehmens ebenfalls zertifizieren zu lassen. Besonders Letzteres ist jedoch mit deutlichen Kosten verbunden.

3. Egal, in welcher der drei Arten Sie das Zertifikat erstellt oder bezogen haben, sollten Sie prüfen, ob der Zugriff per https problemlos funktioniert.

8.3.4 SSL-Bridging

Höhere Sicherheit als SSL-Tunneling

Um das SSL-Bridging zu konfigurieren, sind zahlreiche Konfigurationsschritte erforderlich. Bedenken Sie jedoch, dass Sie nur einmalig diese recht aufwändige Konfiguration vornehmen müssen, dafür aber eine dauerhaft wesentlich höhere Sicherheit als beim Einsatz des SSL-Tunneling erhalten.

1. Als Erstes muss das Zertifikat vom virtuellen Webserver exportiert werden. Der ISA Server muss dasselbe Zertifikat mit denselben Schlüsseln besitzen wie der Webserver, da der ISA Server die https-Verbindung von außen annimmt. Starten Sie dazu auf dem Webserver in der Verwaltung den INTERNETINFORMATIONSDIENSTE-MANAGER.
2. Öffnen Sie den Kontextmenüeintrag EIGENSCHAFTEN des virtuellen Servers und wechseln Sie auf die Registerkarte VERZEICHNISSICHERHEIT. Über ZERTIFIKAT ANZEIGEN wird das Zertifikat angezeigt.
3. Wechseln Sie dann auf die Registerkarte DETAILS. Über IN DATEI KOPIEREN wird der Export-Assistent gestartet.
4. Im Fenster PRIVATE SCHLÜSSEL EXPORTIEREN wählen Sie JA, PRIVATEN SCHLÜSSEL EXPORTIEREN und klicken auf WEITER.

5. Geben Sie dann den Pfad zur Speicherung an. Im Fenster EXPORTDATEIFORMAT wählen Sie PRIVATER INFORMATIONSAUSTAUSCH und darunter die Option WENN MÖGLICH, ALLE ZERTIFIKATE IM ZERTIFIZIERUNGSPFAD EINBEZIEHEN. Klicken Sie dann auf WEITER und beenden Sie den Assistenten.
6. Als Nächstes muss das exportierte Zertifikat auf dem ISA Server importiert werden. Verwenden Sie dazu die mmc ZERTIFIKATE. Navigieren Sie zum Eintrag EIGENE ZERTIFIKATE und wählen aus dem Kontextmenü ALLE TASKS/IMPORTIEREN.

Ist diese mmc noch nicht auf dem ISA Server vorhanden, fügen Sie das Snap-In ZERTIFIKATE des lokalen Computers zu einer leeren mmc hinzu.

7. Geben Sie dann den Speicherpfad sowie das Kennwort an. Markieren Sie hier *nicht* die Option SCHLÜSSEL ALS EXPORTIERBAR MARKIEREN. Auf diese Weise ist es nicht möglich, dass ein Angreifer oder eine andere unbefugte Person den privaten Schlüssel des ISA Server exportieren und dadurch den eingehenden https-Verkehr entschlüsseln kann. Klicken Sie dann auf WEITER.
8. Im Fenster ZERTIFIKATSSPEICHER wählen Sie ALLE ZERTIFIKATE IN FOLGENDEM SPEICHER SPEICHERN und wählen als Speicher EIGENE ZERTIFIKATE. Klicken Sie dann auf WEITER und beenden Sie den Assistenten.
9. Sobald das Zertifikat importiert ist, wird es angezeigt. Sie müssen es jetzt noch nach VERTRAUENSWÜRDIGE STAMMZERTIFIZIERUNGSSTELLEN kopieren, damit der ISA Server dem Zertifikat ebenfalls vertraut. Anderenfalls gilt das importierte Zertifikat nicht als vertrauenswürdig und Sie können kein SSL-Bridging durchführen. Wird eine Zertifizierungsstelle verwendet, so müssen Sie das Zertifizierungsstellenzertifikat nach VERTRAUENSWÜRDIGE STAMMZERTIFIZIERUNGSSTELLEN kopieren.
10. Nachdem das Zertifikat auf dem ISA Server importiert wurde, müssen Sie nun eine sichere Webserververöffentlichungsregel erstellen. Dies erledigen Sie über den entsprechenden Kontextmenüeintrag von FIREWALLRICHTLINIE in der ISA-mmc.
11. Geben Sie der neuen Regel einen Namen und klicken Sie auf WEITER.
12. Im Fenster VERÖFFENTLICHUNGSMODUS (siehe Abbildung 8.11) wählen Sie SSL-BRIDGING und klicken auf WEITER.

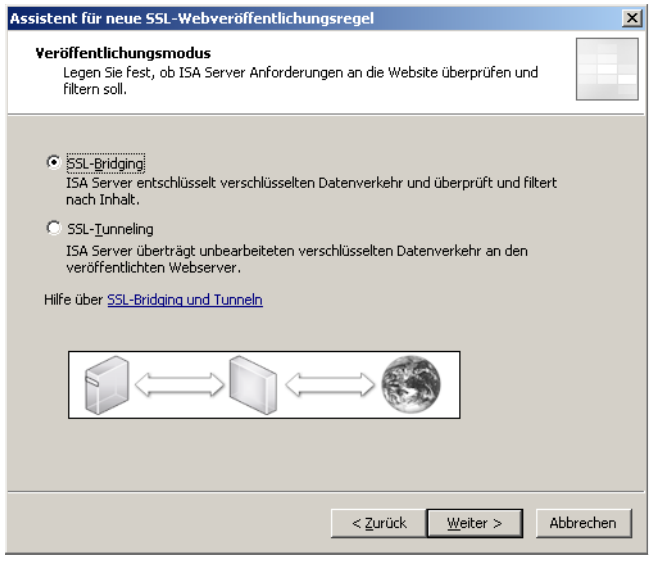


Abbildung 8.11: Auswahl des SSL-Bridging als Veröffentlichungsmodus

13. Als Nächstes wählen Sie ZULASSEN, damit die eingehenden Verbindungen gestattet werden. Klicken Sie dann auf WEITER.
14. Im Fenster BRIDGINGMODUS (siehe Abbildung 8.12) wählen Sie die dritte Option SICHERE VERBINDUNG MIT CLIENTS UND WEBSERVER und klicken dann auf WEITER.

Abbildung 8.12: Auswahl des Bridgingmodus für die sichere Webserververöffentlichung

15. Danach wird im Fenster ZU VERÖFFENTLICHENDE WEBSITE FESTLEGEN der Name des Webservers angegeben. Es *muss* sich hierbei um denselben Namen handeln, der bei der Erstellung des Zertifi-

kats angegeben wurde. Wichtig ist auch die Option URSPRÜNGLICHEN HOSTHEADER ANSTELLE DES AKTUELLEN (ODER ANGEGEBENEN) WEITERLEITEN. Ein Hostheader dient dazu, dass ein einziger Webserver mit nur einer IP-Adresse mehrere virtuelle Webserver betreiben kann. Jeder virtuelle Server besitzt einen individuellen Hostheader. Um die Clientanfragen an den korrekten virtuellen Server weiterleiten zu können, wird die vom Client im Browserfenster eingegebene Adresse des Servers mit dem Hostheader der einzelnen virtuellen Server verglichen. Die Checkbox muss auf jeden Fall aktiviert sein, wenn der veröffentlichte Webserver mit Hostheadern arbeitet. Ansonsten wird bei einer Clientanfrage nicht der Hostheader verwendet, sondern der eingegebene Name in den Wert geändert, der unter COMPUTERNAME ODER IP-ADRESSE angegeben ist. Soll eine Clientanfrage direkt an ein virtuelles Verzeichnis des Webservers weitergeleitet werden, so tragen Sie dieses unter PFAD ein. Klicken Sie dann auf WEITER.

16. Danach wird ein neuer Weblistener über NEU erstellt. Geben Sie für diesen einen Namen an und klicken Sie auf WEITER.
17. Im Fenster PORTSPEZIFIZIERUNG wählen Sie SSL und tragen den Port ein (Standardport = 443). Zusätzlich muss das Zertifikat für die Kommunikation angegeben werden. Der private Schlüssel dieses Zertifikats wird vom ISA Server verwendet, um den eingehenden verschlüsselten Verkehr zur Kontrolle der Pakete zu entschlüsseln. Klicken Sie danach auf WEITER und beenden Sie den Assistenten zur Erstellung des Weblisteners
18. Als Letztes wird für die Webserververöffentlichungsregel bestimmt, welche Benutzer auf den Webserver zugreifen dürfen. Lediglich bei der Auswahl des Benutzersatzes ALLE BENUTZER erfordert der ISA Server keine Authenitifizierung. Diese Einstellung sollten Sie verwenden, wenn beliebige Benutzer über das Internet auf den Webserver zugreifen dürfen. Sollen beispielsweise nur Mitarbeiter des Unternehmens auf den Webserver zugreifen dürfen, wählen Sie einen anderen Benutzersatz aus. Für diese Benutzer ist dann eine Authentifizierung am ISA Server notwendig. Klicken Sie dann auf WEITER und beenden Sie den Assistenten. Mit einem Klick auf ÜBERNEHMEN in der ISA-mmc werden die aktuellen Änderungen in die Konfiguration übernommen.
19. Weitere Einstellungen können über die Eigenschaften der sicheren Webserververöffentlichungsregel vorgenommen werden. Die Einstellungen sind nahezu identisch mit den Eigenschaften einer herkömmlichen Webserververöffentlichungsregel und wurden bereits in Kapitel 8.2.1 erläutert. Lediglich die Registerkarte DATENVERKEHR weist andere Optionen auf. Dort ist es möglich, die http-Filterung einzurichten, obwohl zwischen Client und Webserver eine verschlüsselte Kommunikation stattfindet. Dies liegt darin begründet, dass der ISA Server den SSL-Tunnel mit sei-

nem privaten Schlüssel öffnen kann. Des Weiteren kann festgelegt werden, ob für die Verschlüsselung ein Schlüssel von 128 Bit verwendet werden muss.

Bedenken Sie, dass es ältere Webbrowser gibt, die noch keine 128-Bit-Verschlüsselung beherrschen. Diese können keine Verbindung herstellen, wenn die 128-Bit-Verschlüsselung erzwungen ist.

Abgesicherte FTP-Zugriffe

Über das SSL-Bridging des ISA Server ist es auch möglich, die Verbindung zwischen einem externen Client und einem veröffentlichten FTP-Server zu verschlüsseln. Diese Funktion bietet der IIS nativ nicht. Dabei wird zunächst über Port 443 eine https-Verbindung zum ISA Server hergestellt, der dann die Anfrage an den Server auf Port 21 des internen FTP-Servers umleitet.

8.3.5 SSL-Tunneling

Weniger Sicherheit als SSL-Bridging

Das SSL-Tunneling ist zwar einfacher zu konfigurieren als das SSL-Bridging, allerdings geht diese Vereinfachung in der einmaligen Einrichtung zu Lasten der dauerhaften Sicherheit des internen Netzwerks. Zur Konfiguration des SSL-Tunneling sind lediglich die folgenden Schritte erforderlich:

1. Wählen Sie in der ISA-mmc aus dem Kontextmenü von FIREWALLRICHTLINIE den Eintrag NEU/SICHERE WEBSERVERVERÖFFENTLICHUNGSREGEL. Ein Assistent wird gestartet.
2. Geben Sie einen Namen für die Regel an und klicken Sie auf WEITER.
3. Im Fenster VERÖFFENTLICHUNGSMODUS wählen Sie SSL-TUNNELING und klicken Sie auf WEITER.
4. Tragen Sie dann die IP-Adresse des Webservers ein und klicken Sie auf WEITER.
5. Wählen Sie dann das Netzwerk und über die Schaltfläche ADRESSE die IP-Adresse(n), für die der ISA Server die Anfragen entgegennehmen soll. Klicken Sie auf WEITER und beenden Sie den Assistenten.
6. Über die Eigenschaften der Regel können Sie noch weitere Einstellungen vornehmen. Diese sind nahezu deckungsgleich mit den Einstellungen einer Webserververöffentlichungsregel, siehe Kapitel 8.2.1.

8.4 Veröffentlichen eines Mailservers

Zugriff für mobile Benutzer

Neben Webservern dürften Mailserver die am häufigsten zu veröffentlichenden Server sein. Auch für diese Funktionalität leistet der ISA Server umfassende Unterstützung. Durch eine Veröffentlichung eines Mailservers ist es möglich, dass mobile Benutzer über unterschiedliche Protokolle auf den Mailserver zugreifen können. Ferner kann ein veröffentlichter Mailserver eine Verbindung zu anderen Mailservern im Internet herstellen und mit diesem E-Mails austauschen.

Auch hierbei steht der Sicherheitsaspekt wieder an erster Stelle. Der ISA Server kann die Authentifizierung der Benutzer durchführen, so dass diese nicht am Mailserver direkt erfolgen muss. Erst wenn sich ein Benutzer erfolgreich authentifiziert hat, kann dieser die Verbindung zum Mailserver herstellen. Ein nicht authentifizierter Benutzer kann dies in keinem Fall.

Zusammenarbeit mit zahlreichen Mailservern

Der ISA Server 2004 arbeitet nicht nur mit einem Microsoft Exchange Server, sondern auch mit anderen veröffentlichten Mailservern problemlos zusammen.

Das Veröffentlichen eines Mailservers kann zu insgesamt drei verschiedenen Zwecken vorgenommen werden:

1. Konfiguration des Webclient-Zugriffs
2 Konfiguration des Client-Zugriffs
3 Kommunikation zwischen Servern

Diese drei Zwecke werden in den folgenden Kapiteln ausführlich beschrieben.

8.4.1 Konfiguration des Webclient-Zugriffs

Zugriff per http oder https

Die Konfiguration des Webclient-Zugriffs ist erforderlich, wenn Internet-Clients über http oder https auf ihr Postfach auf dem veröffentlichten Mailserver zugreifen. Verwenden Sie Exchange als Mailserver, gibt es drei verschiedene Methoden für den Webclient-Zugriff:

- *Outlook Web Access (OWA)* für Internetbenutzer über einen Webbrowser
- *Outlook Mobile Access (OMA)* für den Zugriff mit mobilen Geräten wie Handys oder PDAs
- *ActiveSync* zur Synchronisation von Postfachinhalten über das Internet auf ein mobiles Gerät

Das Veröffentlichen eines Mailservers für den Webclient-Zugriff ähnelt der Veröffentlichung eines Webservers. Führen Sie die folgenden Schritte aus:

1. Starten Sie über den entsprechenden Kontextmenüeintrag von FIREWALLRICHTLINIE in der ISA-mmc die Veröffentlichung des Mailservers.
2. Geben Sie der Richtlinie einen passenden Namen und klicken Sie auf WEITER.
3. Auf der Seite WEBCLIENTZUGRIFF (siehe Abbildung 8.13) wählen Sie die Option WEBCLIENTZUGRIFF: OUTLOOK WEB ACCESS (OWA), OUTLOOK MOBILE ACCESS (OMA), EXCHANGE SERVER ACTIVESYNC und klicken Sie dann auf WEITER.

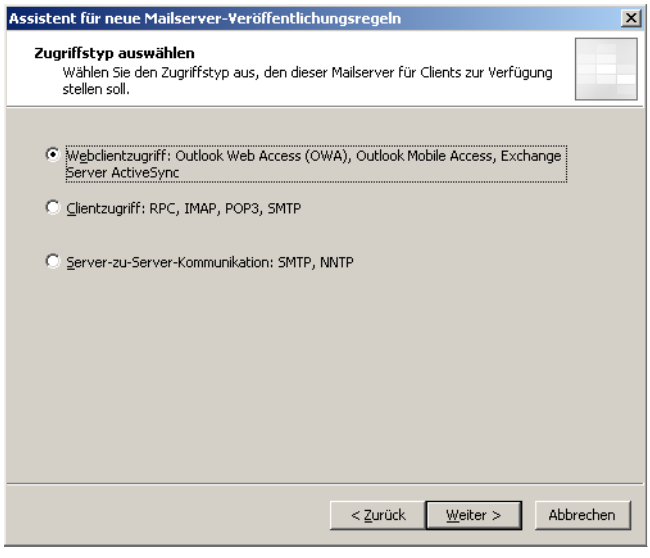


Abbildung 8.13: Auswahl des Zugriffstyps für die Veröffentlichung des Mailservers

4. Als Nächstes werden unter DIENSTE AUSWÄHLEN (siehe Abbildung 8.14) die E-Mail-Dienste OUTLOOK WEB ACCESS, OUTLOOK MOBILE ACCESS und/oder EXCHANGE ACTIVESYNC ausgewählt. Wählen Sie hier nur die Dienste aus, die auch tatsächlich benötigt werden. Je nach Auswahl werden die folgenden virtuellen Verzeichnisse veröffentlicht:

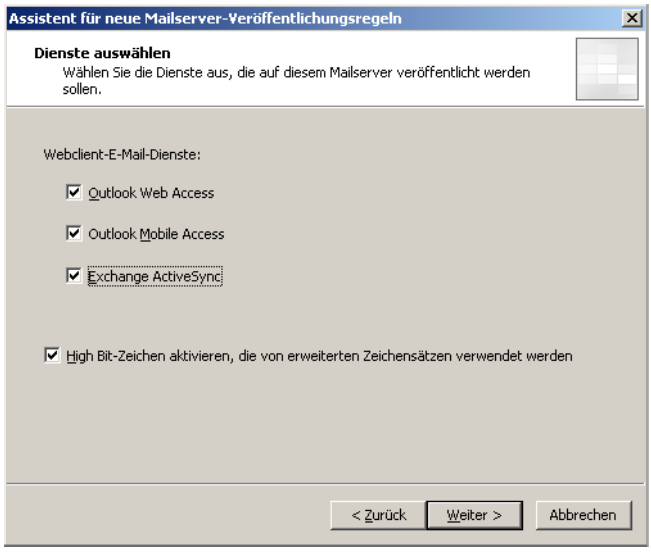
Dienst	Veröffentlichte virtuelle Verzeichnisse
Outlook Web Access	▶ /exchange/* ▶ /exchweb/* ▶ /public/*
Outlook Mobile Access	/OMA/*
Exchange Active Sync	/Microsoft-Server-ActiveSync/*

Tabelle 8.2: Übersicht über die jeweils veröffentlichten virtuellen Verzeichnisse bei der Wahl der Exchange-Dienste

Erweiterter Zeichensatz

Ist die Checkbox HIGH BIT-ZEICHEN AKTIVIEREN, DIE VON ERWEITERTEN ZEICHENSÄTZEN VERWENDET WERDEN aktiviert, können OWA sowie andere Webclient-Dienste einen erweiterten Zeichensatz verwenden, der zwei Byte für die Darstellung eines Zeichens verwendet. Klicken Sie dann auf WEITER.

Abbildung 8.14: Auswahl der unterstützten Dienste des Mailservers



5. Im folgenden Fenster BRIDGINGMODUS (siehe Abbildung 8.15) wählen Sie den gewünschten Modus, in der Regel also SICHERE VERBINDUNG MIT CLIENTS UND MAILSERVER. Die Auswahl des Bridging-Modus ist möglich, weil der Webclient-Zugriff per http oder https erfolgen kann. Klicken Sie dann auf WEITER.

Abbildung 8.15: Auswahl des Bridgingmodus für die Veröffentlichung

6. Danach geben Sie im Fenster WEBMAILSERVER FESTLEGEN den Namen oder die IP-Adresse des zu veröffentlichenden Mailservers an. Haben Sie im vorangehenden Fenster die Option SICHERE VERBINDUNG MIT CLIENTS UND MAILSERVER gewählt, so müssen Sie hier den Namen des Mailservers angeben, der im Zertifikat des virtuellen Webservers angegeben ist. Geben Sie einen anderen Namen oder nur die IP-Adresse an, kann die Verbindung nicht hergestellt werden. Wurde einer der beiden anderen Optionen im vorherigen Fenster gewählt, kann auch der FQDN oder die IP-Adresse des Servers angegeben werden. Klicken Sie dann auf WEITER.
7. Im folgenden Fenster WEBLISTENER AUSWÄHLEN wählen Sie den http- oder https-Listener aus oder erstellen einen neuen, der die Anfragen der externen Clients entgegennimmt. Klicken Sie dann auf WEITER.
8. Abschließend werden noch die Benutzer ausgewählt, die auf den Mailserver zugreifen dürfen. Abweichend von der Konfiguration bei der Veröffentlichung eines Webservers erfolgt auch dann eine Authentifizierung, wenn Sie den Benutzersatz ALLE BENUTZER ausgewählt haben. Klicken Sie dann auf WEITER und beenden den Assistenten.
9. Über die EIGENSCHAFTEN der neu erstellten Regel kann diese noch weiter bearbeitet werden. Diese Einstellungen entsprechen den bereits in Kapitel 8.2.1 beschriebenen Eigenschaften einer Webserververöffentlichungsregel.

8.4.2 Konfiguration des Client-Zugriffs

Zugriff über SMTP oder POP3

Der Client-Zugriff wird für solche externen Clients konfiguriert, die nicht über das Internet erfolgen, sondern über Protokolle wie POP3 oder SMTP. Um diese Form von Zugriff zu konfigurieren, sind die folgenden Schritte erforderlich:

1. Wählen Sie aus dem Kontextmenü der FIREWALLRICHTLINIE den Assistenten zur Veröffentlichung eines Mailservers.
2. Geben Sie der Richtlinie einen passenden Namen und klicken Sie auf WEITER.
3. Im Fenster ZUGRIFFSTYP AUSWÄHLEN markieren Sie die Option CLIENTZUGRIFF: RPC, IMAP, POP3, SMTP. Klicken Sie dann auf WEITER.
4. Im folgenden Fenster DIENSTE AUSWÄHLEN (siehe Abbildung 8.16) können Sie die Unterstützung der Protokolle RPC, POP3, IMAP4 und/oder SMTP wählen und für jedes Protokoll (außer RPC) entscheiden, ob der Standardport und/oder der sichere Port verwendet werden sollen. Die folgende Tabelle gibt Ihnen eine Entscheidungshilfe zur Aktivierung der korrekten Protokolle und Ports:

Abbildung 8.16: Auswahl der Protokolle und Ports für den Clientzugriff

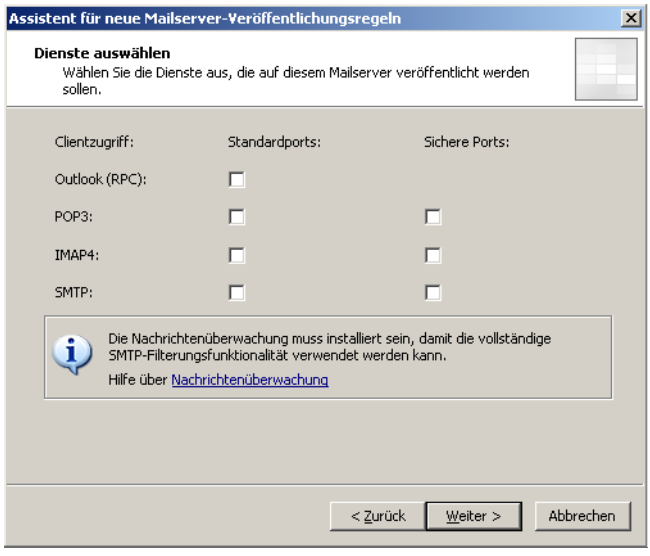


Tabelle 8.3: Entscheidungshilfe zur Auswahl der richtigen Protokolle und Ports

Protokoll und Port	Beschreibung
Outlook (RPC)	RPC wird verwendet, wenn mobile Benutzer über Outlook auf ihre Postfächer zum Abholen von E-Mails zugreifen. Ein Benutzer merkt keinen Unterschied, ob der Zugriff per RPC oder direkt auf den Exchange Server erfolgt. Bei dieser Auswahl werden der TCP-Port 135 sowie die UUIDs für die RPC-Kommunikation mit Exchange veröffentlicht.
POP3	Über POP3 können lediglich die Postfachinhalte auf den Client übertragen werden. Dies geschieht unverschlüsselt. Andere Funktionen wie Aufgaben oder Kalender sind nicht verfügbar. Bei dieser Option wird Port 110 veröffentlicht.
POP3 sicherer Port	Diese Option entspricht POP3, allerdings erfolgt die Übertragung der E-Mails verschlüsselt. Es wird dabei Port 995 veröffentlicht.
IMAP4	Auch über IMAP4 können die Benutzer E-Mails aus ihren Postfächern übertragen. Dies geschieht unverschlüsselt. Zusätzlich können noch weitere Ordner der Mailbox sowie öffentliche Ordner angezeigt werden. Es wird dabei Port 143 veröffentlicht.
IMAP4 sicherer Port	Diese Option entspricht IMAP4, allerdings erfolgt die Übertragung der E-Mails verschlüsselt. Es wird dabei Port 993 veröffentlicht.

Protokoll und Port	Beschreibung
SMTP	Soll auch das Versenden von E-Mails für einen Benutzer möglich sein, der über POP3 oder IMAP4 auf sein Postfach zugreift, muss auch der SMTP-Dienst veröffentlicht werden. Das Senden der E-Mails erfolgt unverschlüsselt. Dazu wird der Port 25 veröffentlicht.
SMTP sicherer Port	Diese Option entspricht SMTP, allerdings erfolgt das Versenden der E-Mails verschlüsselt. Es wird dabei Port 465 veröffentlicht.

Die drei verschlüsselten Verbindungen können vom ISA Server nicht analysiert werden. Die verschlüsselten Daten werden vom ISA Server angenommen und direkt an den Mailserver weitergeleitet.

Klicken Sie dann auf WEITER.

5. Geben Sie dann im Fenster SERVER AUSWÄHLEN die IP-Adresse des Mailservers an und klicken Sie auf WEITER.
6. Dann wird unter IP-ADRESSEN die Netzwerkverbindung ausgewählt, an der der ISA Server den eingehenden Verkehr abhören soll. Klicken Sie danach auf WEITER und beenden den Assistenten.
7. Sie sehen, dass für jedes gewählte Protokoll eine eigene Firewall-Richtlinie hinzugefügt worden ist (siehe Abbildung 8.17). Den drei Protokollen RPC, POP3 und SMTP ist automatisch ein Anwendungsfilter beigefügt worden.

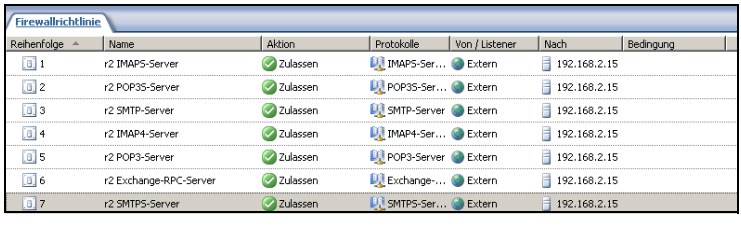


Abbildung 8.17: Für jedes Protokoll ist eine eigene Firewall-Richtlinie erstellt worden

8.4.3 Kommunikation zwischen Servern

Austausch von E-Mails

Soll zwischen dem veröffentlichten Mailserver und weiteren Mailservern eine Kommunikation stattfinden, so muss auch dies separat konfiguriert werden. Eine Kommunikation kann z.B. im Austausch von E-Mails bestehen. Zur Einrichtung sind die folgenden Schritte notwendig:

1. Starten Sie über das Kontextmenü von FIREWALLRICHTLINIE den Assistenten zum Veröffentlichen eines Mailservers.
2. Geben Sie einen passenden Namen für die Richtlinie an und klicken Sie auf WEITER.

3. Wählen Sie dann im Fenster ZUGRIFFSTYP AUSWÄHLEN die Option SERVER-ZU-SERVER-KOMMUNIKATION: SMTP, NNTP und klicken Sie danach auf WEITER.
4. Unter DIENSTE AUSWÄHLEN können Sie SMTP, SICHERES SMTP und/oder NNTP auswählen (siehe Abbildung 8.18). Die einzelnen Dienste sollten in den folgenden Fällen ausgewählt werden:

Abbildung 8.18: Auswahl der Dienste für die Server-zu-Server-Kommunikation

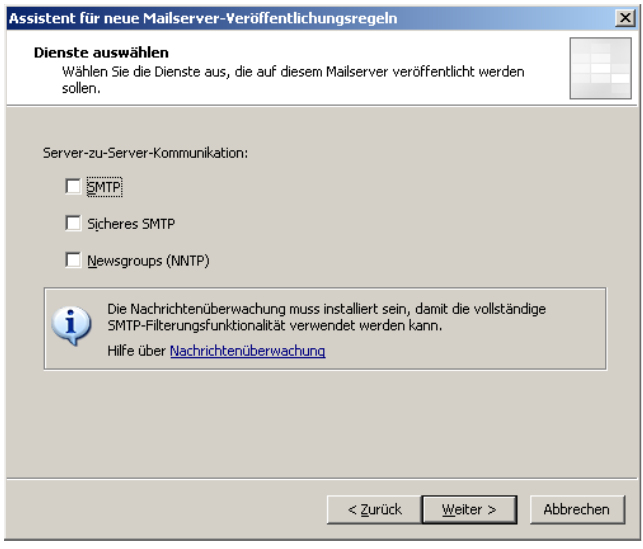


Tabelle 8.4: Auswahl der Dienste für die Server-zu-Server-Kommunikation

Dienst	Beschreibung
SMTP	Über den SMTP-Dienst kann der interne Mailserver E-Mails von Mailservern aus dem Internet empfangen. Dies geschieht unverschlüsselt. Es wird dabei Port 25 veröffentlicht.
Sicheres SMTP	Das sichere SMTP entspricht der Funktion des herkömmlichen SMTP. Allerdings erfolgt der E-Mail-Empfang verschlüsselt. Es wird dabei Port 465 veröffentlicht.
NNTP	Der NNTP-Dienst wird benötigt, damit der Mailserver aus Newsgroups Nachrichten empfangen kann. Es wird dabei Port 119 veröffentlicht.

Klicken Sie dann auf WEITER.

5. Geben Sie dann die IP-Adresse des Mailservers an und klicken auf WEITER.
6. Bestimmen Sie dann abschließend die Netzwerkschnittstelle, auf der der eingehende Verkehr empfangen werden soll. Klicken Sie dann auf WEITER und beenden Sie den Assistenten.

Pro Dienst eine Zugriffsrichtlinie

Sie sehen, dass auch jetzt für jeden gewählten Dienst eine separate Zugriffsrichtlinie hinzugefügt worden ist.

8.5 Veröffentlichen weiterer Server

Zahlreiche vordefinierte Inbound-Protokolle

Außer mit den bisher beschriebenen Verfahren zur Veröffentlichung von mailservern und Webservern können auch noch weitere Server veröffentlicht werden. Bei der Veröffentlichung können sämtliche Inbound-Protokolle verwendet werden. Dazu stellt der ISA Server bereits verschiedene Inbound-Protokolle zur Verfügung. Benötigen Sie noch zusätzliche dieser Protokolle, so fügen Sie diese zunächst über die Toolbox hinzu. Die folgenden Protokolle für die Veröffentlichung weiterer Server sind bereits vorhanden:

- DNS-Server
- Exchange-RPC-Server
- FTP-Server
- HTTPS-Server
- IKE-Server
- IMAP4-Sever
- IMAPS-Server
- IPSec-ESP-Server
- IPSec-NAT-T-Server
- L2TP-Server
- Microsoft SQL Server
- MMS-Server
- NNTP-Server
- NNTPS-Server
- PNM-Server
- POP3-Server
- POP3S-Server
- PPTP-Server
- RDP-(Terminaldienste-)Server
- RPC-Server (alle Schnittstellen)
- RTSP-Server
- SMTP-Server
- SMTPS-Server
- Telnetserver

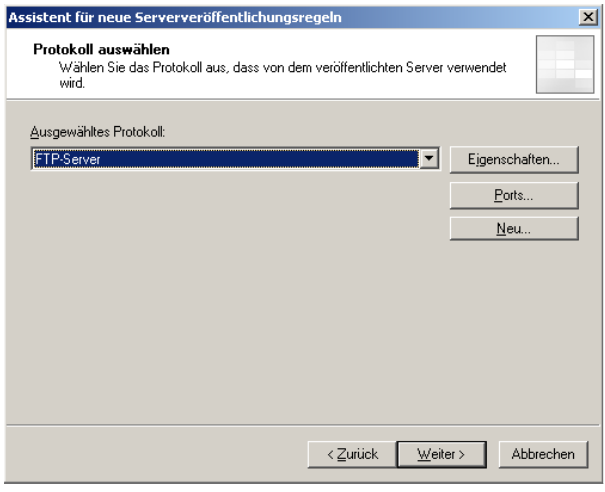
Beispiel FTP-Server

Um beispielsweise einen FTP-Server zu veröffentlichen, führen Sie die folgenden Schritte aus:

1. Starten Sie aus dem Kontextmenü von FIREWALLRICHTLINIE den Link NEUE SERVERVERÖFFENTLICHUNGSREGEL ERSTELLEN.
2. Geben Sie einen passenden Namen für die Regel an und klicken dann auf WEITER.

3. Tragen Sie im Fenster SERVER AUSWÄHLEN die IP-Adresse des Servers ein, auf dem der FTP-Dienst veröffentlicht werden soll, und klicken Sie auf WEITER.
4. Im Fenster PROTOKOLL AUSWÄHLEN wählen Sie aus der Liste den Eintrag FTP-SERVER (siehe Abbildung 8.19) und klicken dann auf WEITER.

Abbildung 8.19: Veröffentlichen eines FTP-Servers



5. Bestimmen Sie danach die Netzwerkschnittstelle und die IP-Adresse (n), auf der der eingehende Verkehr abgehört werden soll. Klicken Sie auf WEITER und beenden Sie den Assistenten.

8.6 Authentifizierungsmechanismen

Nachdem Sie nun die Veröffentlichung verschiedener Server und Dienste kennen gelernt haben, müssen Sie entscheiden, in welcher Form sich die Benutzer dazu authentifizieren sollen. Insgesamt gibt es vier verschiedene Möglichkeiten, wie die Authentifizerung erfolgen kann:

- Keine Authentifizierung
- Authentifizierung am veröffentlichten Server
- Authentifizierung am ISA Server
- Authentifizierung am veröffentlichten Server und am ISA Server

8.6.1 Keine Authentifizierung

Benutzersatz Alle Benutzer

Ist für einen Dienst keine Authentifizierung erforderlich, so wird diese weder vom ISA Server, noch vom veröffentlichten Server verlangt. Damit keine Authentifizierung notwendig wird, muss in der Veröffentlichungsregel der Benutzersatz *Alle Benutzer* gewählt sein. Bei allen anderen Benutzersätzen ist eine Authentifizierung notwendig. Ist keine Authentifizierung nötig, prüft der ISA Server lediglich das Paket

der Anfrage und leitet dieses an den internen Server weiter. Sinnvoll ist diese Form der Authentifizierung z.B. bei öffentlichen Webseiten.

8.6.2 Authentifizierung am veröffentlichten Server

Keine Authentifizierung am ISA Server

In dieser Form verlangt nicht der ISA Server, wohl aber der interne, veröffentlichte Server eine Authentifizierung. Der ISA Server prüft nur das Paket und leitet es an den internen Server weiter. Dieser fordert dann vom Benutzer die Authentifizierungsinformationen. Erst wenn diese korrekt erfolgt sind, wird die Verbindung hergestellt.

8.6.3 Authentifizierung am ISA Server

Weiterleiten der Benutzerinformationen

Ist diese Form der Authentifizierung gewählt, muss sich der Benutzer am ISA Server authentifizieren. Erst wenn dort die korrekten Informationen eingegeben wurden, werden die Pakete an den internen Server weitergeleitet und die Verbindung zu diesem hergestellt. Hierzu darf in der Veröffentlichungsregel nicht der Benutzersatz *Alle Benutzer* gewählt sein. Diese Form ist sicherer als die eben beschriebene, da so die Verbindung zum internen Netzwerk für den externen Benutzer erst hergestellt wird, wenn der ISA Server die Authentifizierung durchgeführt hat.

Eine Authentifizierung am ISA Server ist nur für Veröffentlichungsregeln für die Protokolle http und https beim Bridging möglich. Bei anderen Protokollen wie POP3, FTP usw. kann die Authentifizierung nur am veröffentlichten Server erfolgen.

8.6.4 Authentifizierung am veröffentlichten Server und am ISA Server

Doppelte Authentifizierung

Bei dieser Methode verlangen beide Server eine Authentifizierung vom externen Benutzer. Möglicherweise ist für den Benutzer für den Zugriff auf denselben Dienst eine zweimalige Eingabe der Benutzerinformationen erforderlich. Damit keine zweimalige Authentifizierung erforderlich wird, muss in den Eigenschaften der Regel auf der Registerkarte BENUTZER die Checkbox ANMELDEINFORMATIONEN FÜR BASISAUTHENTIFIZIERUNG WEITERLEITEN (EINFACHE DELEGIERUNG) aktiviert sein. Diese Delegierung ist allerdings nur dann notwendig, wenn am virtuellen Webserver und dem ISA Server die Standardauthentifizierung gewählt ist.

Eine Authentifizierung kann nur bei der Veröffentlichung von http- und https-Protokollen im Bridging-Modus eingestellt werden. Bei der Veröffentlichung anderer Protokolle wie z.B. FTP, POP3 usw. erfolgt die Authentifizierung grundsätzlich am veröffentlichten Server. Die Registerkarte BENUTZER ist bei den Veröffentlichungsregeln dieser Protokolle nicht verfügbar.

8.6.5 Authentifizierungsmethoden

Damit sich der externe Benutzer authentifizieren kann, können unterschiedliche Methoden verwendet werden. Eine kurze Beschreibung dieser Methoden finden Sie in der folgenden Tabelle.

Tabelle 8.5: Übersicht über die verschiedenen Authentifizierungsprotokolle

Authentifizierungsmethode	Beschreibung
Integrierte Windows-Authentifizierung	Die Windows-Authentifizierung erfolgt entweder über Kerberos oder NTLM. Ist der Benutzer bereits lokal oder an der Domäne angemeldet, werden diese Anmeldeinformationen weitergeleitet. Diese Informationen werden nie über das Netzwerk übertragen. Nur wenn eine Authentifizierung mit den aktuellen Informationen nicht möglich ist, wird der Benutzer zur Eingabe aufgefordert.
Standardauthentifizierung	Dieses Verfahren wird oft verwendet, da es von nahezu allen Webbrowsern unterstützt wird. Die Anmeldeinformationen werden in ein Fenster eingegeben und im Klartext an den ISA Server übertragen. Bedenken Sie, dass die Base64-Codierung des Kennworts dabei *keiner* Verschlüsselung entspricht und z.B. mit einem Netzwerksniffer ausgelesen werden kann.
Digest-Authentifizierung	Die Digest-Authentifizierung ähnelt der Standardauthentifizierung, allerdings werden die Informationen der Authentifizierung im einem unidirektionalen Vorgang in einen Hash-Wert umgesetzt. Das Benutzerkonto muss zu einer Windows-Domäne gehören und umkehrbar verschlüsselt sein. Der Webbrowser muss dem http-Standard 1.1 entsprechen.
OWA-formularbasiert	Die OWA-formularbasierte Authentifizierung ist ab Exchange Server 2003 verfügbar. Der Benutzer muss seinen Namen und sein Kennwort in ein Formular eintragen. Danach erhält er ein Cookie, der nach einem definierbaren Zeitraum wieder ungültig wird. Dadurch wird verhindert, dass unbefugte Personen Zugriff auf das Postfach erhalten.

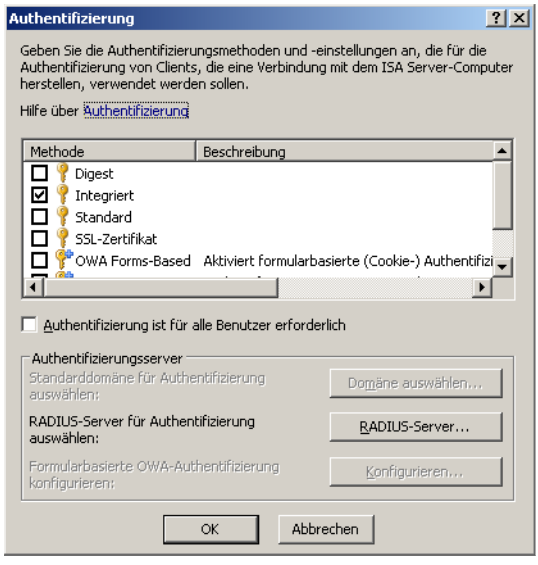
Authentifizierungs-methode	Beschreibung
SSL-Zertifikat	Für diese Methode müssen der Server und Client über ein Zertifikat verfügen. Sobald die Verbindung vom Client initiiert wird, wird an diesen das Zertifikat des Servers übertragen. Verlangt der Server eine Client-Authentifizierung, übermittelt der Client dem Server sein Zertifikat. Diese Form der Authentifizierung kann auch für ältere Exchange-Versionen oder auch für den Zugangsschutz herkömmlicher Webseiten verwendet werden.
RADIUS	Der ISA Server fordert vom Benutzer den Namen und das Kennwort an. Diese beiden Informationen werden an einen RADIUS-Server über das RADIUS-Protokoll weitergeleitet. Der RADIUS-Server teilt dem ISA Server mit, ob es sich um gültige Anmeldeinformationen handelt und somit die Verbindung hergestellt werden kann. In diesem Szenario müssen der RADIUS-Server und der ISA Server nicht zu derselben Domäne gehören. Dies Verfahren kann auch verwendet werden, wenn es sich um einen allein stehenden ISA Server handelt.
SecureID	Diese Form der Authentifizierung bietet auch dann noch Schutz, wenn eine unbefugte Person den Benutzernamen und das Kennwort herausbekommen hat. Für die SecureID-Authentifizierung ist zusätzlich eine Karte erforderlich, die in einem Intervall von 60 Sekunden eine bestimmte Ziffer herausgibt, die außer den Anmeldeinformationen ebenfalls anzugeben ist. Man spricht bei diesem Verfahren auch von einer Multifaktor-Authentifizierung. Zum Einsatz dieser Methode ist der Einsatz von RSA SecureID Authentication zwingend erforderlich. Weitere Hinweise dazu finden Sie unter dem Link *http://www.rsasecurity.com*.

Authentifizierungsmethode festlegen

Um zu bestimmen, welche Form der Authentifizierung verwendet werden soll, wechseln Sie über die Eigenschaften der entsprechenden Regel auf die Registerkarte BENUTZER. Entfernen Sie dort den Benutzersatz *Alle Benutzer*, so dass keine anonyme Authentifizierung mehr

möglich ist, und fügen Sie einen anderen Benutzersatz hinzu. Wechseln Sie dann auf die Registerkarte LISTENER und klicken Sie auf EIGENSCHAFTEN. Auf der Registerkarte EINSTELLUNGEN klicken Sie auf AUTHENTIFIZIERUNG. Dort kann die gewünschte Authentifizierungsmethode gewählt werden (siehe Abbildung 8.20).

Abbildung 8.20: Auswahl der Authentifizierungsmethode



8.7 Veröffentlichen von Diensten direkt auf dem ISA Server

Dienste direkt auf dem ISA Server

Bisher wurden veröffentlichte Server besprochen, deren Dienst auf einem separaten Computer und nicht direkt auf dem ISA Server ausgeführt wurden. Eine Veröffentlichung von Diensten ist theoretisch auch direkt auf dem ISA Server möglich oder sogar unumgänglich, wenn man an einen Small Business Server (SBS) in der Premium Version denkt. Allerdings macht hierbei das standardmäßig aktivierte Socket Pooling Probleme. Ist das Socket Pooling aktiviert, wird von den IIS-Listenern der gesamte Datenverkehr aller Netzwerkschnittstellen und IP-Adressen abgehört. Sehen wir uns dieses Problem einmal im Detail an.

8.7.1 Das Problem des Socket Pooling

Problem IP-Adresse 0.0.0.0

Angenommen, auf dem ISA Server selbst soll eine Website veröffentlicht werden. Dazu wird ein Weblistener für die externe Schnittstelle benötigt, der auf Port 80 den eingehenden Verkehr abhört. Dieser entgegengenommene Verkehr wird mittels der Veröffentlichungsregel

an den virtuellen Webserver auf dem ISA Server weitergeleitet, genauer gesagt an die interne IP-Adresse auf Port 80. Sobald das Socket Pooling jedoch aktiviert ist, hört der IIS nicht nur einzelne IP-Adressen, sondern auch die IP-Adresse 0.0.0.0 für Port 80 ab, da er sämtliche Schnittstellen in das Abhören miteinbezieht.

Um die aktiven Bindungen anzuzeigen, geben Sie an der Eingabeaufforderung den Befehl `netstat -na` ↵ ein (siehe Abbildung 8.21).

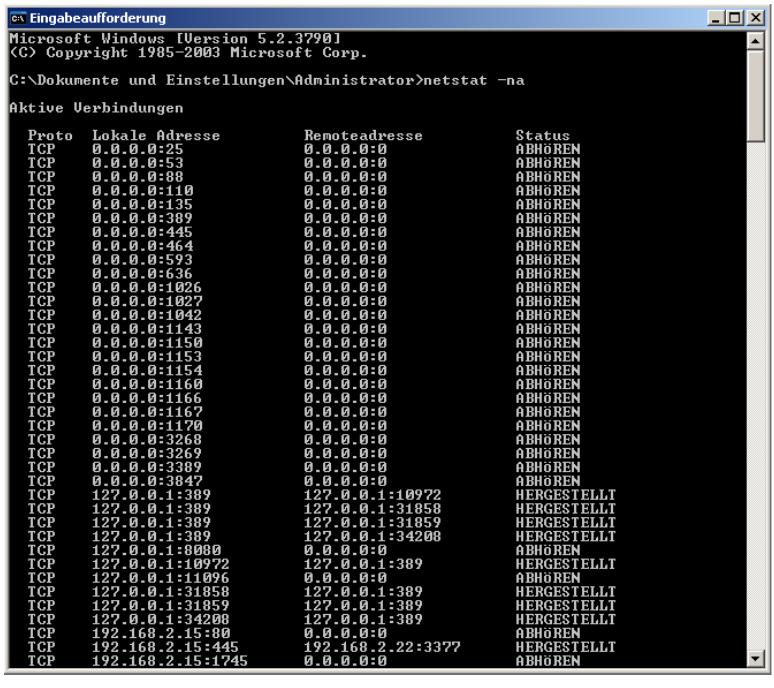


Abbildung 8.21: Anzeige der aktiven Verbindung über den Befehl netstat -na

An dieser Stelle kommt es zu einem Problem mit dem Listener für die Veröffentlichungsregel. Dieses Problem lässt sich auch nicht lösen, indem der virtuelle Webserver nur für eine einzige IP-Adresse konfiguriert wird.

Eine Lösung ist nur möglich, wenn für ein bestimmtes Protokoll das Socket Pooling deaktiviert wird. So kann der Listener von der IP-Adresse 0.0.0.0 entkoppelt werden. Allerdings sind einige Dienste wie z.B. IIS mit dem http-Protokoll auf Port 80 an die IP-Adresse 0.0.0.0 gebunden und können auch nicht entkoppelt werden.

8.7.2 Deaktivieren des Socket Pooling

Für die meisten Protokolle möglich

Wenn das Socket Pooling auch nicht für alle Protokolle entkoppelt werden kann, so ist dies dennoch für die meisten möglich und behebt damit auch nahezu sämtliche Probleme. Die folgenden Kapitel zeigen Ihnen, wie das Socket Pooling für die gebräuchlichsten Protokolle deaktiviert wird. Dabei wird auf Unterschiede zwischen Windows Server 2000 und 2003 hingewiesen.

http-Protokoll

Unter Windows Server 2000 verwenden Sie die folgenden Befehle:

```
Net stop w3svc ↵
```

Cscript.exe adsutil.vbs set w3svc/disablesocketpooling true ↵

```
Net start w3svc ↵
```

Unter Windows 2003 ist das Deaktivieren des Socket Pooling ein wenig aufwändiger.

1. Sie müssen zunächst von der Betriebssystem-CD die Support Tools installieren. Danach beenden Sie den http-Dienst mit dem folgenden Befehl:

   ```
   Net stop http /y ↵
   ```

2. Wechseln Sie an der Eingabeaufforderung zum Installationsverzeichnis der Support Tools und geben Sie folgenden Befehl ein:

   ```
   Httpcfg.exe delete iplisten -i 0.0.0.0 ↵
   ```

   ```
   Httpcfg.exe set iplisten -i interne IP-Adresse des
   ISA Server ↵
   ```

3. Danach prüfen Sie mit dem Befehl httpcfg.exe query iplisten ↵ , ob die Listener-Konfiguration nun korrekt ist.
4. Starten Sie wieder den Dienst mit net start http ↵.
5. Mit dem Befehl `netstat -na` ↵ überprüfen Sie, ob für die IP-Adresse 0.0.0.0 auf Port 80 kein Listener mehr konfiguriert ist.

FTP-Protokoll

Zum Deaktivieren des Socket Pooling für das FTP-Protokoll verwenden Sie sowohl unter Windows Server 2000 als auch unter Windows Server 2003 die folgenden Befehle:

```
Net stop mstfpsvc ↵
```

```
Cscript.exe adsutil.vbs set mstfpsvc /
disablesocketpooling true ↵
```

```
Net start mstfpsvc ↵
```

SMTP-Protokoll

Um unter Windows Server 2000 das Socket Pooling für den SMTP-Dienst zu deaktivieren, müssen Sie zunächst von der Betriebssystem-CD das Programm *MDUtil.exe* extrahieren. Verwenden Sie dazu den folgenden Befehl:

```
Expand.exe CD-Laufwerk\i386\mdutil.ex_ c:\inetpub\
adminscripts\mdutil.exe ↵
```

Geben Sie danach die folgenden Befehle ein:

```
Net stop smtpsvc ↵
```

```
Mdutil.exe set -path smtpsvc/1 -value 1 -dtype 1 -prop
1029 -attrib 1 ↵
```

```
Net start smtpsvc ↵
```

Unter Windows Server 2003 beenden Sie den SMTP-Dienst zunächst mit dem Befehl `net stop smtpsvc ↵`.

Wechseln Sie dann zum Verzeichnis `c:\inetpub\adminscripts`.

Mit folgendem Befehl wird das Socket Pooling für den SMTP-Dienst deaktiviert:

```
cscript.exe adsutil.vbc set smtpsvc /disablesocketpooling
true ↵
```

Starten Sie dann den Dienst wieder über `net start smtpsvc ↵`

Für sämtliche Deaktivierungen gilt, dass die Einstellungen möglicherweise erst nach einem Neustart des ISA Server korrekt übernommen werden. Sollten also nach der Deaktivierung des Socket Pooling dennoch Probleme bestehen, starten Sie den ISA Server neu.

9 Filter

Dieses Kapitel beschäftigt sich mit den zahlreichen Filtern, die der ISA Server zur Analyse von Paketen bereitstellt. Zunächst erhalten Sie einen Einblick in die Filtermethoden der Stateful Inspection und der Application-Layer-Filterung. Danach werden die drei verschiedenen Typen von Filtern vorgestellt. Dabei handelt es sich um Anwendungsfilter, Webfilter und IP-Filter. Im Rest des Kapitels werden die einzelnen Filter jeder Kategorie in ihrer Funktion und Konfiguration näher vorgestellt.

9.1 Stateful Inspection und Application Layer-Filterung

Gleichwertig einer Hardware-Firewall

Über den ISA Server 2004 können Sie gleichermaßen eine Stateful Inspection wie auch die Application Layer-Filterung durchführen. Durch das Feature der Stateful Inspection wird der ISA Server zu einer Netzwerk-Layer Stateful Firewall mit denselben Fähigkeiten wie eine Hardware-Firewall. Die Filterung wird auf den Netzwerk- und Transport-Layern durchgeführt.

Die Stateful-Filterung wird vielfach auch als Stateful Packet Filtering bezeichnet. Allerrdings ist diese Bezeichnung streng genommen falsch, da sich die Pakete auf Layer 3 des OSI-Modells beziehen. Um jedoch den Verbindungsstatus zu prüfen, müssen Informationen des Layers 4 geprüft werden.

Der ISA Server ist in der Lage, die kompletten Kommunikationsströme zu überprüfen, die über die ISA-Firewall von einem Netzwerk zu einem anderen fließen. Beim Stateful Filtering werden lediglich die Informationen der Netzwerk- und Transport-Layer gefiltert, allerdings erfordert ein wahres Stateful Filtering, dass sämtliche Layer der Kommunikation analysiert werden können. Besonders die Applikations-Layer sind hier von Bedeutung.

Web- und Anwendungsfilter

Auch Web-Filter führen ein Stateful Applikations-Layer Filtering der Proxy-Komponenten-Kommunikation durch. Hierbei handelt es sich um http-, https- sowie http-getunnelte ftp-Verbindungen. Die Anwendungsfilter sind für die Durchführung der Stateful Applikations-Layer Filtering von nicht http-basierten Protokollen zuständig. Dazu zählen Protokolle wie POP3, SMTP oder DNS.

Protokollzugriff und -sicherheit

Beide Arten von Filtern können für den Zugriff und die Sicherheit von Protokollen verwendet werden. Unter Protokollzugriff versteht man Zugriff auf Protokolle, die sekundäre Verbindungen erfordern. Dies ist entweder bei komplexen Protokollen oder auch z.B. bei dynamisch zugewiesenen Ports einer FTP-Verbindung der Fall. Im Rahmen der Protokollsicherheit werden die Verbindungen, die über den ISA Server hergestellt werden, abgesichert. Z.B. wird mit Hilfe von SMTP- oder DNS-Filtern der entsprechende Verkehr analysiert und blockiert, sobald eine Sicherheitsverletzung des Systems wahrgenommen wird, z.B. ein Speicherüberlauf.

Eine Übersicht über die Anwendungs- und Webfilter des ISA Server 2004 finden Sie, indem Sie in der ISA-mmc auf KONFIGURATION/ADD-INS klicken. Über die EIGENSCHAFTEN des jeweiligen Filters kann eine Bearbeitung oder Einstellung durchgeführt werden. Dort können auch die einzelnen Filter aktiviert oder deaktiviert werden.

9.2 Anwendungsfilter

In der ISA-Firewall sind mehrere Anwendungsfilter enthalten. Anwendungsfilter werden auch als Applikationsfilter bezeichnet. Beide Begriffe sind deckungsgleich. Dabei handelt es sich um die folgenden Typen:

- FTP-Zugriffsfilter
- RPC-Filter
- SMTP-Filter
- POP Intrusion Detection-Filter
- DNS-Filter
- SOCKS V4-Filter
- PPTP-Filter
- H.323-Filter
- MMS-Filter
- PNM-Filter
- RTSP-Filter

9.2.1 FTP-Zugriffsfilter

Mit Hilfe des FTP-Zugriffsfilters wird die Kommunikation zwischen dem FTP-Client und dem FTP-Server verfolgt. Der Filter kann einerseits über den Befehl `PORT` zugewiesene Ports dynamisch öffnen und andererseits auch unzulässige Schreibversuche auf den FTP-Server blockieren.

Dynamische Ports, sekundäre Verbindungen

Das FTP-Protokoll verwendet für den Aufbau der Verbindung Port 21. Sobald diese Verbindung erfolgreich hergestellt wurde, werden für die Übertragung der Daten ein oder mehrere dynamische Ports benutzt. Diese werden als sekundäre Verbindungen bezeichnet und können für eine Firewall zu Problemen führen, weil nicht nur ein einzelner dynamischer Port für die FTP-Antworten eingerichtet werden kann.

Der FTP-Zugriffsfilter ist jedoch in der Lage, die Kommunikation zwischen dem FTP-Server und FTP-Client zu verfolgen und so dynamisch die jeweilserforderlichen Ports zu öffnen. Des Weiteren kann auch das Schreiben auf einem FTP-Server blockiert werden. So können die Clients lediglich Daten vom FTP-Server downloaden, jedoch dort keine Daten speichern. Dazu ist bereits standardmäßig die Option NUR LESEN für den Filter gewählt.

Schreibzugriffe

Um die Schreibzugriffe zu blockieren, wechseln Sie über die Eigenschaften der Veröffentlichungsregel auf die Registerkarte DATENVERKEHR. Dort klicken Sie auf FILTERUNG und aktivieren die Checkbox NUR LESEN (siehe Abbildung 9.1). Um bei einer Zugriffsregel diese Option einzustellen, wechseln Sie in den EIGENSCHAFTEN der betreffenden Regel auf die Registerkarte PROTOKOLLE, markieren das FTP-Protokoll und klicken auf FILTERUNG/FTP KONFIGURIEREN.

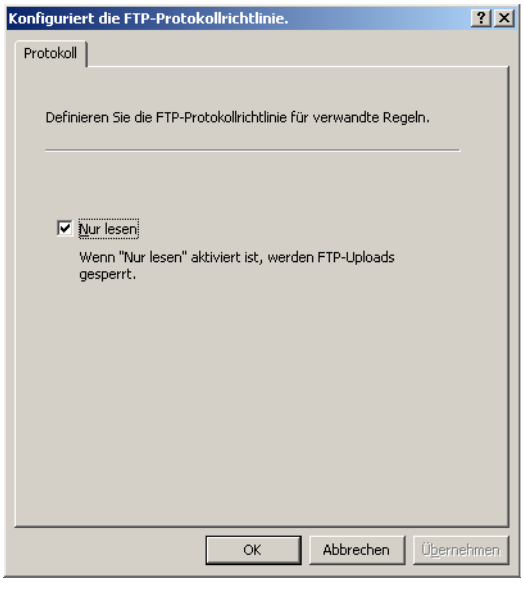


Abbildung 9.1: Konfiguration des FTP-Zugriffsfilters

9.2.2 RPC-Filter

Externer Zugriff auf internen Server

Das RPC-Protokoll wird verwendet, um von einem externen Client, z.B. einem *Outlook*-Client, vom veröffentlichten Server, in diesem Beispiel also Exchange, Dienste aufzurufen. Eine RPC-Verbindung wird zunächst über Port 135 hergestellt. Danach werden dem Client abhängig davon, welche UUID angefordert wurde, vom Server dynamisch Ports zugewiesen. Diese werden für die gesamte folgende Kommunikation benutzt.

Im Gegensatz zu einigen anderen Firewall-Lösungen kann der ISA Server die dynamisch zugewiesenen Ports verarbeiten. Der RPC-Filter kann die dynamischen Ports erkennen und diese je nach Bedarf sogar öffnen.

Dynamische Port-Öffnung

Zunächst wird vom ISA Server die Verbindung auf Port 135 entgegengenommen. Dann fragt der ISA Server beim veröffentlichten Exchange-Server an, welche Ports für den eingehenden Verkehr benutzt werden. Der vom Exchange Server angegebene Port wird vom ISA Server dynamisch geöffnet. Dadurch kann der Client die Verbindung herstellen. Sobald der Client die Verbindung beendet hat, werden sämtliche dynamisch geöffneten Ports automatisch wieder geschlossen.

Authentifizierung

Sobald der externe Benutzer auf ein Exchange-Postfach zugreifen möchte, fordert der Exchange-Server Authentifizierungsinformationen vom Benutzer an. Handelt es sich beim Exchange-Server um einen Domänencontroller, erfolgt die Authentifizierung direkt am Exchange-Server. Ist dieser jedoch nur Mitglied einer Domäne, so erfolgt ein Verweis zur Authentifizierung des Clients an den Domänencontroller. Dieser Verweis kann jedoch nicht durch den ISA Server hindurch erfolgen. Deshalb muss der Exchange-Server als Domänenmitglied selbst in der Lage sein, die Authentifizierungsinformationen für den Benutzer am Domänencontroller zu prüfen. Man spricht hierbei von Authentication Proxy. Um dieses Feature zu aktivierem, ist auf dem Exchange-Server im Registry-Schlüssel `HKEY_LOCAL_MACHINE\CurrentControlSet\Services\MSExchangeSA\Parameters` ein Eintrag namens `No RFR Service` vom Typ `REG_DWORD` mit dem Wert 1 erforderlich.

Für den RPC-Filter kann die Option STRIKTE RPC-EINHALTUNG ERZWINGEN (siehe Abbildung 9.2) gewählt werden, so dass keine zusätzlichen RPC-Typprotokolle wie z.B. DCOM erlaubt werden. Sie stellen diese Option auf der Registerkarte PROTOKOLLE unter FILTERUNG/RPC-PROTOKOLL KONFIGURIEREN ein.

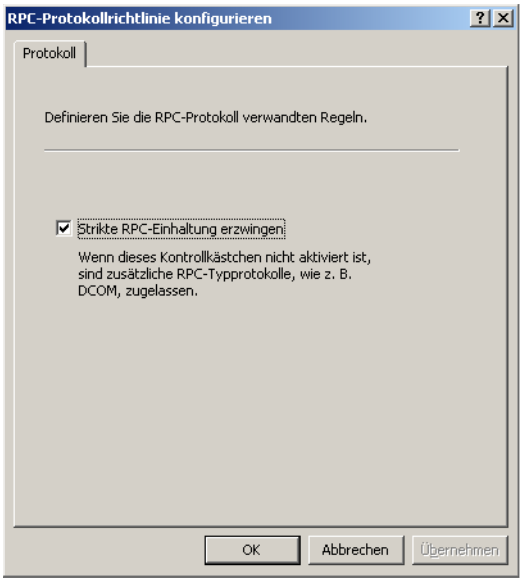


Abbildung 9.2: Konfiguration des RPC-Filters

9.2.3 SMTP-Filter

Über den SMTP-Filter werden die E-Mails geprüft, die an einen veröffentlichten Mailserver gesendet werden. Dabei werden sämtliche enthaltenen SMTP-Befehle ausgelesen und bedarfsweise blockiert. Es kann festgelegt werden, welche SMTP-Befehle erlaubt sind und welche maximale Länge diese besitzen dürfen. Enthält ein Paket unerlaubte Befehle, so kann eine Aktion festgelegt werden.

Nachrichtenüberwachung

Ist auf dem ISA Server auch die Komponente *Nachrichtenüberwachung (SMTP Message Screener)* installiert, erhält der SMTP-Filter automatisch weitere Funktionen. Es können nun Filterungen von Sendern und Empfängern sowie Filterungen der E-Mail-Anhänge und nach bestimmten Schlüsselwörtern durchgeführt werden.

Damit die Nachrichtenüberwachung (nach)installiert werden kann, muss zuvor auf dem ISA Server der SMTP-Dienst installiert werden.

Beliebiger Installationsort

Die Nachrichtenüberwachung muss nicht direkt auf dem ISA Server installiert werden, sondern kann auch auf dem Mailserver oder einem SMTP-Relay-Server installiert werden. In dieser Konstellation muss nicht der ISA Server selbst die SMTP-Filterung durchführen und wird dadurch entlastet. Außer der Filterung kann der SMTP-Relay-Server die eingehenden E-Mails auch auf Spam-Mails und Viren hin untersuchen.

Die Konfiguration des SMTP-Filters geschieht in der ISA-mmc unter KONFIGURATION/ADD-INS über die EIGENSCHAFTEN von SMTP-ANWENDUNGSFILTER.

Schlüsselwörter

Auf der Registerkarte SCHLÜSSELWÖRTER können Sie bestimmte Begriffe hinzufügen, nach denen eine E-Mail durchsucht werden soll. Es kann entweder in der Betreffszeile oder im Textfeld oder in beiden Bereichen nach dem entsprechenden Begriff gesucht werden. Zusätzlich kann eine Aktion bestimmt werden, die beim Finden einer solchen E-Mail durchgeführt werden soll. Dafür stehen drei Aktionen zur Wahl:

- NACHRICHT LÖSCHEN: Sofern der SMTP-Filter die Weiterleitung einer E-Mail verhindert, wird diese gelöscht.
- NACHRICHT HALTEN: Auf dem ISA Server befindet sich ein spezieller Ordner \BADMAIL. In diesem wird die E-Mail vorgehalten.
- NACHRICHT WEITERLEITEN AN: Die vom SMTP-Filter blockierten E-Mails können zur weiteren Kontrolle an eine bestimmte E-Mail-Adresse weitergeleitet werden, z.B. an den Administrator.

SMTP-Befehle

Auf der Registerkarte SMTP-BEFEHLE (siehe Abbildung 9.3) befindet sich eine Liste von SMTP-Befehlen. Sie können über BEARBEITEN jeden einzelnen Befehl zulassen oder verbieten und für ihn eine maximale Länge bestimmen. Zudem können weitere SMTP-Befehle hinzugefügt und gelöscht werden.

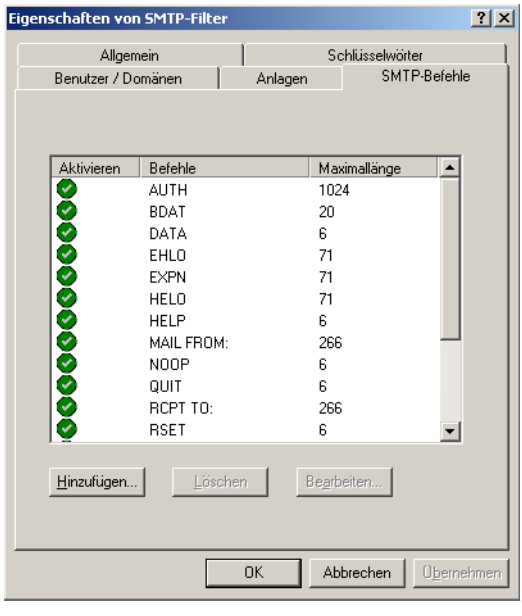


Abbildung 9.3: Übersicht über die SMTP-Befehle, die zugelassen oder blockiert werden sollen

E-Mail-Anhänge filtern

Über die Registerkarten ANLAGEN und BENUTZER/DOMÄNEN können die Filterfunktionen für bestimmte E-Mail-Anhänge sowie Benutzer und Domänen, die keine E-Mails an den SMTP-Server senden dürfen, konfiguriert werden. In Abbildung 9.4 sehen Sie ein Beispiel für die Konfiguration einer Regel zum Umgang mit einem E-Mail-Anhang.

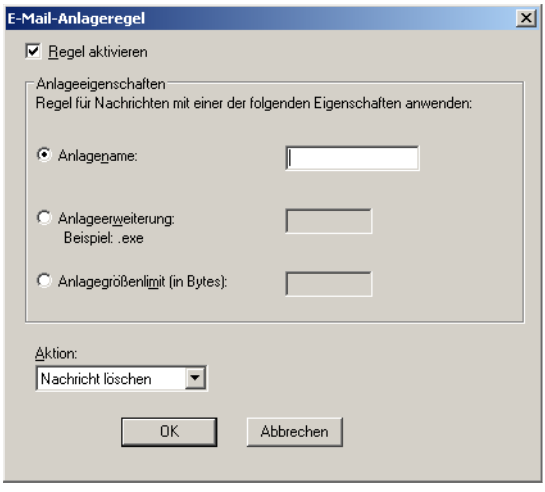


Abbildung 9.4: Konfiguration einer Regel für den Umgang mit E-Mail-Anhängen

9.2.4 POP3-Eindringversuchs-Erkennungsfilter

Veröffentlichte Mailserver

Dieser Filter prüft die Verbindungen, die von externen Benutzern zum veröffentlichten Mailserver über das POP3-Protokoll zum Herunterladen von E-Mails hergestellt werden. Eine Verbindung wird bereits beendet, bevor sie den Mailserver erreichen kann, wenn durch sie ein Pufferüberlauf verursacht wird. Es gibt für diesen Filter keine weiteren Möglichkeiten zur Konfiguration.

9.2.5 DNS-Filter

DNS notwendig im Active Directory

Ein DNS-Server ist Voraussetzung für den Betrieb einer Active Directory-Domäne und die komplette Namensauflösung im Netzwerk. Aufgrund dieser gewichtigen Funktion des Servers sind DNS-Server oftmals Ziel von Angriffen. Über einen DNS-Filter kann eine eingehende Verbindung zu einem veröffentlichten DNS-Server verfolgt und überprüft werden.

Um den DNS-Filter zu konfigurieren, navigieren Sie in der ISA-mmc zu KONFIGURATION/ALLGEMEIN und wählen ERKENNEN VON EINDRINGVERSUCHEN UND DNS-ANGRIFFEN AKTIVIEREN. Wechseln Sie dann auf die Registerkarte DNS-ANGRIFFE (siehe Abbildung 9.5).

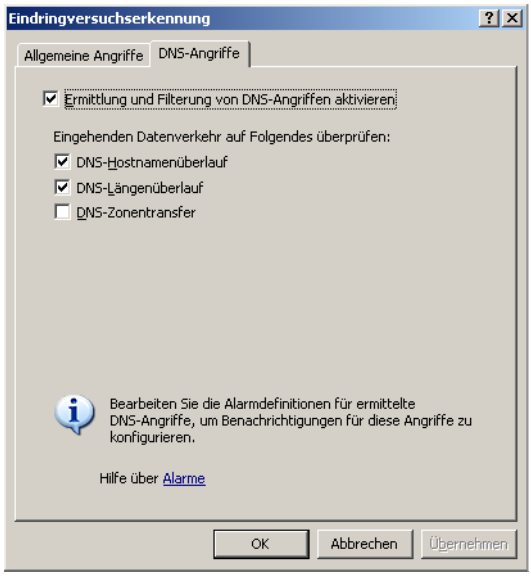


Abbildung 9.5: Konfiguration des DNS-Filters

Ist die Checkbox ERMITTLUNG UND FILTERUNG VON DNS-ANGRIFFEN AKTIVIEREN markiert, wird generell der eingehende DNS-Netzwerkverkehr gefiltert. Dabei sind die folgenden Filterungen möglich:

- DNS-HOSTNAMENÜBERLAUF: Geht die DNS-Anfrage über eine bestimmte Länge hinaus, kann dies zu einem Pufferüberlauf des DNS-Servers führen. Wird eine solche Anfrage vom ISA Server ermittelt, kann die Antwort verweigert werden.
- DNS-LÄNGENÜBERLAUF: Es kann auch ein Pufferüberlauf entstehen, wenn die IP-Adresse einer DNS-Anfrage oder –Antwort länger als 4 Byte ist. Wird eine solche Anfrage vom ISA Server entdeckt, wird die Verbindung getrennt.
- DNS-ZONENTRANSFER: Fordert ein externer Computer die vollständige Übertragung einer DNS-Zone an, so verhindert der ISA Server diese Übertragung.

9.2.6 PPTP-Filter

Eingehende VPN-Verbindungen

Befindet sich im internen Netzwerk ein PPTP-Server, prüft der PPTP-Filter die eingehenden VPN-Verbindungen. Da die VPN-Pakete jedoch verschlüsselt sind, kann der ISA Server diese nicht prüfen. Anders verhält es sich, wenn der VPN-Server direkt auf dem ISA Server ausgeführt wird. In diesem Fall wird der VPN-Tunnel am ISA Server beendet und die Pakete können über den Filter bis hinunter zur Anwendungsebene analysiert werden.

SecureNAT-Client

Der Filter wird sowohl für Firewall-, als auch für SecureNAT-Clients benötigt. Ein Computer im ISA Server-geschützten Netzwerk muss

als SecureNAT-Client konfiguriert sein, um einen PPTP-Filter für die Verbindung zu PPTP-VPN-Servern nutzen zu können. Dies liegt darin begründet, dass der Firewall-Client keine Nicht-TCP/UDP-Protokolle vermitteln kann. Für das PPTP-VPN-Protokoll sind jedoch das GRE-Protokoll (Generic Routing Encapsulation, IP-Protokollnummer 47) und das TCP-Protokoll 1723 notwendig. Die TCP-Verbindung wird zur Verwaltung des Tunnels verwendet.

Es gibt keine weiteren Einstellmöglichkeiten für diesen Filter.

9.2.7 SOCKS V4-Filter

Nur für Nicht-Windows-Clients

Mit Hilfe des SOCKS V4-Filters kann die SOCKS V4-Kommunikation aktiviert werden. Dieser Filter ist standardmäßig deaktiviert. Auf Windows-Betriebssystemen sollten diesen Filter nicht benötigen, da auf diesen der Firewall-Client installiert werden kann, über den die Authentifizierung am ISA Server sowie die Protokollaushandlung erfolgen. Dieser Filter sollte deshalb nur in heterogenen Netzwerken aktiviert werden, wenn z.B. MacOS- oder Linux-Clients eingesetzt werden.

Nachdem der Filter aktiviert wurde, wählen Sie auf der Registerkarte NETZWERKE (siehe Abbildung 9.6) diejenigen aus, die der Filter nach entsprechenden zu akzeptierenden Verbindungen abhören soll. Optional kann auch der standardmäßig verwendete Port 1080 bearbeitet werden.

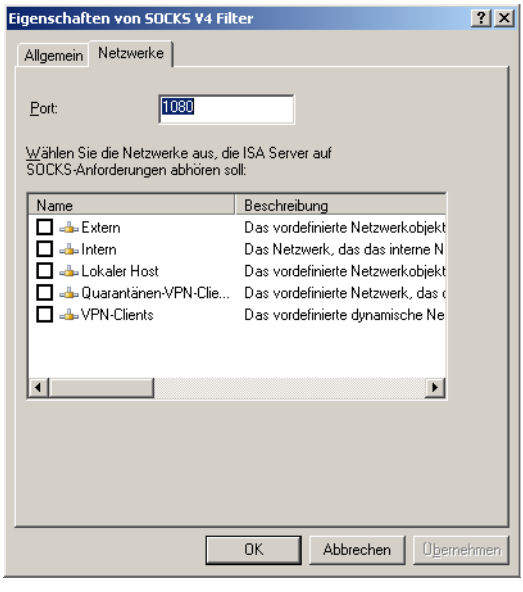


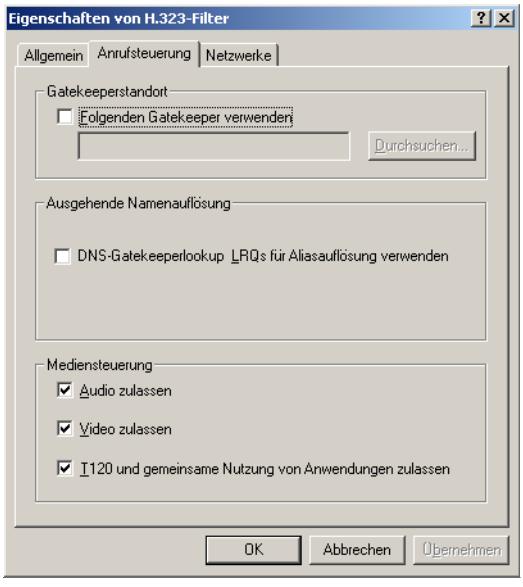
Abbildung 9.6: Konfiguration des SOCKS V4-Filters

Über diesen Filter werden sämtliche Applikationen unterstützt, die den SOCKS V4.3-Spezifikationen entsprechen.

9.2.8 H.323-Filter

Über diesen Filter werden H.323-Verbindungen durch die ISA-Firewall zugelassen. Auf der Registerkarte ANRUFSTEUERUNG (siehe Abbildung 9.7) wird der Filter konfiguriert. Sie können dort den zu verwendenden Gatekeeper angeben, die ausgehende Namensauflösung konfigurieren und bestimmen, welche Optionen für die Mediensteuerung erlaubt sind.

Abbildung 9.7: Konfiguration des H.323-Filters



Auf der Registerkarte NETZWERKE werden die Netzwerke ausgewählt, für die der H.323-Filter Verbindungsanfragen akzeptieren soll.

9.2.9 MMS-Filter

Microsoft Media Services

Über den MMS-Filter werden *Microsoft Media-Services* über die entsprechenden Zugriffsregeln und Veröffentlichungsregeln zugelassen bzw. blockiert. Dieser Filter ist nur für SecureNAT-Clients notwendig, damit diese die komplexen Protokolle und sekundären Verbindungen verarbeiten können. Der Firewallclient benötigt diesen Filter nicht. Es gibt keine weiteren Einstellmöglichkeiten für diesen Filter.

9.2.10 PNM-Filter

Progressive Networks Media Protocol

Der PNM-Filter ist für die Unterstützung des *Progressive Networks Media- Protokolls* der Firma *Real Networks* zuständig. Er dient ebenfalls dazu, den SecureNAT-Clients den Zugriff auf die komplexen Protokolle und sekundären Verbindungen zu ermöglichen. Es gibt keine weiteren Konfigurationsmöglichkeiten für diesen Filter.

9.2.11 RTSP-Filter

Microsoft Real Time Streaming Protocol

Über den RTSP-Filter werden Verbindungen des *Microsoft Real Time Streaming-Protokolls* über die entsprechenden Zugriffsregeln und Veröffentlichungsregeln zugelassen bzw. blockiert. Dieser Filter ist nur für SecureNAT-Clients notwendig, damit diese die komplexen Protokolle und sekundären Verbindungen verarbeiten können. Der Firewall-Client benötigt diesen Filter nicht. Es gibt keine weiteren Einstellmöglichkeiten für diesen Filter.

9.3 Webfilter

Webfilter werden zur Vermittlung von http-, https- und http-getunnelten ftp-Verbindungen eingesetzt. Die folgenden Filter zählen zu den Webfiltern:

- http-Filter
- Link Translation-Filter
- Webproxy-Filter
- SecureID-Filter
- OWA-formularbasierte Filter

9.3.1 http-Filter

Mächtigster aller Filter

Der http-Filter ist von allen Filtern der umfassendste. Er greift, sofern in einer Veröffentlichungsregel das http-Protokoll verwendet wird. Über diesen Filter kann der komplette http-Verkehr zwischen zwei Computern bis hinunter auf die Anwendungsebene analysiert werden. Dabei können die folgenden Prüfungen durchgeführt werden:

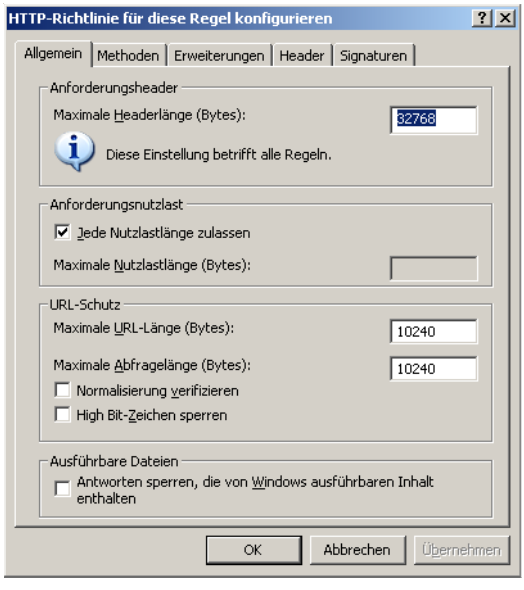
- Blockade ausführbarer Dateien
- Erkennung und Blockade bestimmter Dateitypen
- Erkennung und Blockade von http-Signaturen
- Prüfung von http-Methoden
- Prüfung und Änderung von http-Headern
- Längenbegrenzung von Anforderungsheadern, Anforderungsnutzlasten und URLs

Dieser Filter kann eingesetzt werden, wenn in einer Zugriffsregel das http-Protokoll eingesetzt wird. Mit Hilfe des http-Filters kann z.B. zwischen dem Webserver und dem internen Client der komplette Datenverkehr bis hinunter zur Anwendungsebene analysiert werden.

Um den http-Filter in einer Zugriffsrichtlinie zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die Eigenschaften der Zugriffsrichtlinie und wechseln Sie auf die Registerkarte PROTOKOLLE.
2. Markieren Sie dort das Protokoll HTTP und klicken Sie auf FILTERUNG/HTTP KONFIGURIEREN.
3. Auf der Registerkarte ALLGEMEIN (siehe Abbildung 9.8) ist als MAXIMALE HEADERLÄNGE der Wert 32.768 Byte angegeben. Mit der Beschränkung auf diesen Wert können bereits im Vorfeld Attacken abgewehrt werden, die mit einem überlangen Anforderungsheader den Computer zum Absturz bringen können, z.B. Buffer-Overflow- oder DoS-Angriffe. Die Microsoft-Empfehlung für diesen Wert liegt bei 10.000 Byte. Allerdings kann dieser Wert zu Problemen führen, die ein Heraufsetzen des Werts erzwingen.

Abbildung 9.8: Allgemeine Einstellungen am http-Filter



Eine Änderung dieses Werts hat Auswirkungen auf *alle* Regeln und *nicht nur* die *aktuell* bearbeitete.

Nutzlastlänge

Des Weiteren können Sie auch eine MAXIMALE NUTZLASTLÄNGE bestimmen. Unter Nutzlast versteht man die Maximalgröße des Paketinhalts. Für ausgehenden Verkehr ist eine Beschränkung dieses Linits in aller Regel nicht notwendig, Sie können dabei die Option JEDE NUTZLASTLÄNGE ZULASSEN wählen. Jedoch sollte für eingehenden Verkehr ein Limit gesetzt werden, so dass beispielsweise ein veröffentlichter Webserver nicht durch Pakete in Übergröße angegriffen wird.

URL-Abfragelänge

Im Abschnitt URL-SCHUTZ kann die maximal erlaubte Länge einer URL festgelegt werden. Der vorgegebene Wert sollte dabei nur geändert werden, wenn spezielle Bedürfnisse dies erzwingen, da dieser Wert den Mittelweg zwischen Schutz und Funktionalität gewährleistet. Auch hier hilft eine Begrenzung gegen mögliche Angriffe. Mit Hilfe einer überlangen URL kann beispielsweise auf einen veröffentlichten Webserver ungewünschter Programmcode übertragen werden. In der Regel wird der hier gesetzte Wert auch unter MAXIMALE ABFRAGELÄNGE verwendet. Darüber wird festgelegt, bis zu welcher Länge eine URL vom Client abgefragt werden darf.

URL-Codierung

Die Option NORMALISIERUNG VERIFIZIEREN bezieht sich auf die Fähigkeit des ISA Server, URLs zweifach zu codieren. Anfragen an einen Webserver sind grundsätzlich URL-codiert. Bestimmte Zeichen der URL werden dabei durch einen festgelegten Wert ersetzt. So erhält das Leerzeichen in der URL-Codierung den Wert %20. Diese Codierung kann von einem Angreifer missbraucht werden, so dass eine URL durch ihn weiter geändert wird. Kann der Webserver lediglich eine einfache Codierung anwenden, kann über eine manipulierte, doppelt codierte URL unerlaubter Programmcode auf das System gespielt werden. Durch die Aktivierung der Option NORMALISIERUNG VERIFIZIEREN erfolgt eine doppelte Codierung durch den ISA Server. Dabei werden die beiden Codierungen miteinander verglichen und blockiert, falls diese beiden nicht übereinstimmen.

Erweiterte Zeichensätze

Wird die Option HIGH BIT-ZEICHEN SPERREN aktiviert, werden in URLs alle Zeichen blockiert, die pro Zeichenanzeige mehr als ein Byte verwenden, so dass 256 Zeichen angezeigt werden können. Darunter fallen DBCS- (Double Byte Character Set)- oder Latin1-Zeichensätze, die die Erweiterungen zur Darstellung z.B. asiatischer Schriftzeichen nutzen.

Ausführbare Dateien

Über die Option ANTWORTEN SPERREN, DIE VON WINDOWS AUSFÜHRBAREN INHALT ENTHALTEN werden auf Webseiten ausführbare Dateien wie z.B. *.exe*-Dateien blockiert. So kann der Download der entsprechenden Dateien verhindert werden. Die Option ist sinnvoll, wenn Benutzern, die über keinen FTP-Zugang verfügen, die Möglichkeit genommen werden soll, die Dateien stattdessen per http herunterzuladen.

http-Kommunikationsmethoden

Auf der zweiten Registerkarte METHODEN werden die http-Methoden festgelegt, die für die Kommunikation zwischen dem Webserver und dem Client verwendet werden. Sie können entweder ALLE METHODEN ZULASSEN oder nur bestimmte Methoden für die Kommunikation gestatten. Um diese Methoden festzulegen, klicken Sie auf HINZUFÜGEN (siehe Abbildung 9.9). Umgekehrt können Sie auch nur die angegebenen Methoden zulassen und alle übrigen sperren.

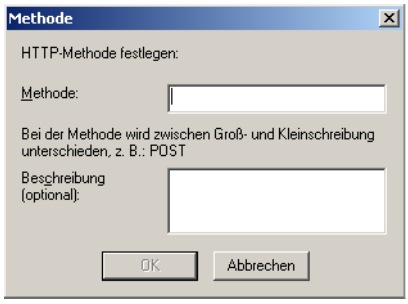


Abbildung 9.9: Die angegebenen Methoden können entweder zugelassen oder blockiert werden

Im Folgenden finden Sie eine Auflistung über die meistgebrauchten http-Methoden.

Tabelle 9.1: Übersicht über einige http-Methoden

Methode	Beschreibung
DELETE	Auf dem Zielsystem können Objekte gelöscht werden.
GET	Diese Methode wird zum Anfordern von Informationen vom Webserver verwendet.
HEAD	Es werden ebenfalls Informationen vom Webserver angefordert, allerdings handelt es sich nur um Header-Informationen.
OPTIONS	Über diese Methode teilt der Webserver dem Client mit, welche http-Methoden verfügbar sind.
POST	Über diese Methode sendet der Client Informationen an den Webserver, z.B. wenn ein Webformular ausgefüllt wird.
PUT	Die Methode PUT wird zum Laden von Dateien auf dem Zielsystem benutzt.
TRACE	Diese Methode wird in der Regel nur zur Fehlersuche oder Diagnose verwendet. Über sie können Clientanfragen verfolgt werden.

Tragen Sie jeweils die gewünschte http-Methode in das Eingabefenster METHODE ein und bestätigen Sie mit OK. Achten Sie dabei auf die Großschreibung der Methoden. Für interne Clients sollten die beiden Methoden *GET* und *HEAD* zugelassen werden. Soll zudem auch das Ausfüllen von Formularen ermöglicht werden, so ist zusätzlich die Methode *POST* zuzulassen.

Dateierweiterungen sperren

Ähnlich wie bei den Methoden können Sie auf der Registerkarte ERWEITERUNGEN (siehe Abbildung 9.10) bestimmen, welche Dateiendungen wie z.B. *.exe* usw. vom http-Filter gesperrt werden sollen. Auf diese Weise können für den Benutzer Musikdateien wie *.mp3* oder auch Animationen gesperrt werden. Ist zusätzlich die Option ANFORDERUNGEN SPERREN, DIE MEHRDEUTIGE ERWEITERUNGEN ENTHALTEN aktiviert, werden sämtliche Erweiterungen gesperrt, die der ISA Server nicht eindeutig zuordnen kann.

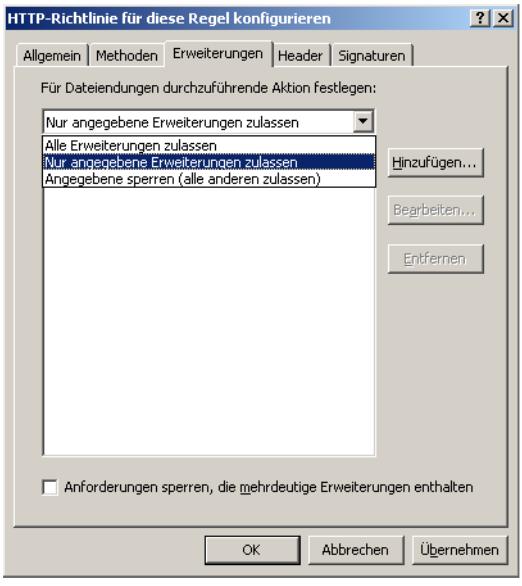


Abbildung 9.10: Festlegen von Dateierweiterungen, die zugelassen oder blockiert werden sollen

Sobald die Filterung für eine oder mehrere Dateiendungen aktiviert wurde, wird jede Anfrage bezüglich dieser Erweiterung(en) durchsucht. Als Dateiendung wird vom ISA Server die Zeichenfolge angesehen, die nach dem letzten Zeichen „.“, „/“ oder „?“ steht. Auch Zeichen, die einem Punkt („.“) folgen, werden versuchsweise als Dateierweiterung gelesen. Befinden sich innerhalb einer URL mehrere Zeichen wie „/“ oder „.“, so wird jeweils die erste Zeichenkette dahinter als Dateierweiterung angesehen. Der restliche Teil wird ignoriert.

Beispielsweise wird in der URL h*ttp://www.servername/pfad/datei.exe* die Erweiterung *.exe* blockiert, wenn dies so konfiguriert ist. Lautet die URL hingegen *http://www.servername/datei.exe/anderedatei.xyz*, so wird ebenfalls lediglich die *.exe*-Datei blockiert, da der Rest der URL vom http-Filter ignoriert wird. Um dennoch auch die Dateierweiterung *.xyz* blockieren zu können, muss dies über die Registerkarte SIGNATUR zur Verweigerung dieses Dateityps erstellt werden.

http-Header

Über die vierte Registerkarte HEADER (siehe Abbildung 9.11) können bestimmte Header blockiert werden. Die zu blockierenden Header werden über HINZUFÜGEN angegeben. Ein Header ist immer der Teil, der nach dem Senden einer http-Anfrage oder einer http-Antwort zwischen Server und Client gesendet wird. Im Header befinden sich Informationen über den Client, z.B. die Version des Betriebssystems, Informationen zur Autorisierung oder zum verwendeten Webbrowser. Mit Hilfe dieser Informationen kann sich ein potenzieller Angreifer ein Bild vom Zustand des Webservers machen und gezielt bestimmte Angriffe planen.

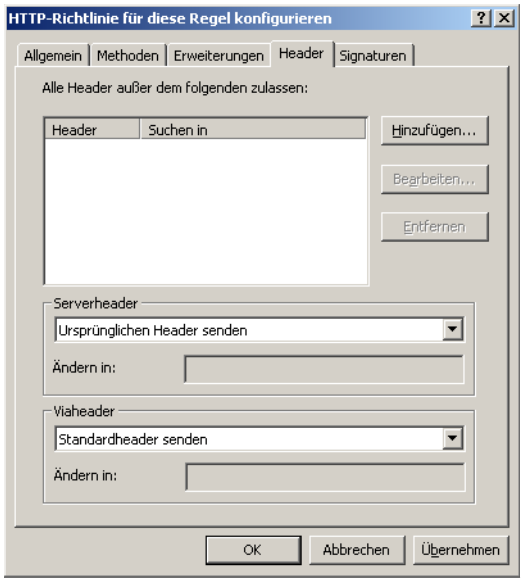


Abbildung 9.11: Die Konfiguration der Header-Informationen

Header-Informationen ändern

In den Abschnitten SERVERHEADER und VIAHEADER können Sie verschiedene Optionen festlegen, wie mit dem Header verfahren werden soll. Mit URSPRÜNGLICHEN HEADER SENDEN wird der ursprüngliche Header in der Antwort zurückgegeben. Über HEADER AUS DER ANTWORT LÖSCHEN wird in der Antwort kein Header zurückgegeben und mit ANTWORT BEARBEITEN/HEADER IN DER ANTWORT BEARBEITEN wird in der Antwort ein modifizierter Header zurückgegeben. Tragen Sie bei Wahl dieser Option unter ÄNDERN IN den geänderten Wert ein. Das Löschen bzw. Ändern des Antwortheaders dient dem Schutz des Webservers, da ein Angreifer nun nicht mehr die kompletten Informationen über die Betriebssystemversion usw. des Webservers erhält.

http-Signaturen

Auf der letzten Registerkarte SIGNATUREN (siehe Abbildung 9.12) werden Einstellungen für Signaturen vorgenommen. Bei einer Signatur kann es sich um jedes Zeichen im http-Header und http-Body handeln. Damit die http-Signatur ermittelt werden kann (z.B. um dadurch das Ausführen einer bestimmten Anwendung zu verhindern), muss bekannt sein, welches Muster die Anwendung unter Request Header, Response Header sowie Body benutzt. Dann können Sie anhand dieser verwendeten Zeichenkette eine Signatur erstellen, die das Ausführen der Anwendung blockiert.

Das Problem beim Definieren von Signaturen besteht darin, die geeignete Zeichenkette zu ermitteln, über die tatsächlich nur unerwünschte Aufrufe blockiert werden.

Zusätzlich zum Blockieren bestimmter Aufrufe kann auch bestimmter bösartiger Code unterbunden werden. Z.B. wird über die Zeichenfolge `<iframe src=“?“ />` der Internet Explorer aufgefordert, CPU-

Ressourcen zu benutzen. Mit Hilfe einer Signatur kann dieses Codefragment blockiert werden.

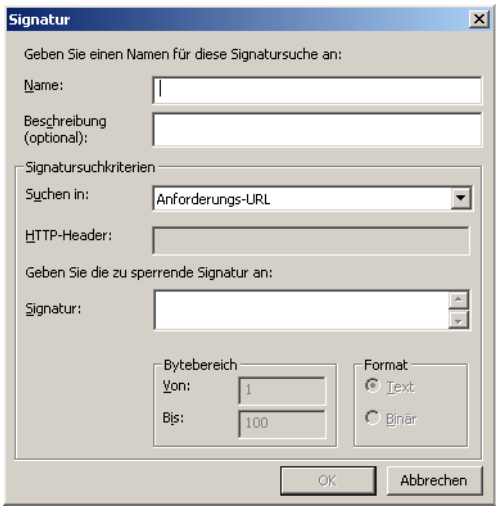


Abbildung 9.12: Festlegen von Signaturinformationen

Die Filterung nach http-Signaturen kann nur durchgeführt werden, wenn die Anfragen und Antworten mit Hilfe von UTF-8 codiert worden sind. UTF-8 ist eine Abwandlung von Unicode. Wird eine andere Codierung verwendet, kann keine Blockade von http-Signaturen durchgeführt werden.

Quellen für http-Signaturen

Wenn Sie die Informationen für eine http-Signatur nicht selbst ermitteln wollen, können Sie auf zahlreiche bereits vorhandene Filter-Signaturen im Internet zurückgreifen. Eine Übersicht über wichtige Signaturen bestimmter Applikationen finden Sie unter dem Link *http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/commonapplicationsignatures.mspx*. Spezielle Filtersignaturen für den ISA Server 2004 finden Sie auch unter dem Link *http://www.msisafaq.de/Tools/HTTPFilter.htm*.

Um beispielsweise eine Signatur für *Bearshare* zu erstellen, tragen Sie im Fenster SIGNATUR die folgenden Werte ein:

- NAME: Bearshare blockieren
- BESCHREIBUNG: Blockiert die Nutzung von Bearshare
- SUCHEN IN: Antwortheader
- HTTP-HEADER: Server
- SIGNATUR: Bearshare

Standardmäßig durchsucht der http-Filter nur die Bytes von eins bis 100 im Anforderungs- und Antwortbody. Sie können diesen Wert jedoch heraufsetzen. Bedenken Sie jedoch, dass dabei die Performance des ISA Server deutlich abnehmen kann.

Sofern der Aufruf über eine http-Signatur blockiert wurde, erhält der Benutzer im Webbrowser den Hinweis, dass die Seite nicht angezeigt werden kann. Als Quelle der Blockade ist dort der Filter angegeben.

Selbst Signaturen ermitteln

Um für weitere Anwendungen die http-Signatur zu ermitteln, können Sie mit Hilfe des Windows-Netzwerkmonitors oder mit einem anderen Netzwerksniffer die entsprechenden Informationen auslesen und anhand derer eine neue Signatur erstellen.

http-Filter importieren und exportieren

Auf der Installations-CD des ISA Server 2004 finden Sie im Ordner `\SDK\SAMPLES\ADMIN` das Skript *httpfilterconfig.vbs*. Mit Hilfe dieses Skripts können Sie http-Filter importieren und exportieren (siehe Abbildung 9.13).

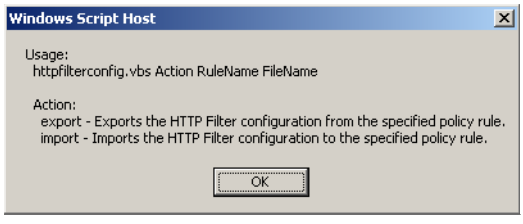


Abbildung 9.13: Per Skript können http-Filter importiert und exportiert werden

Nicht für https anwendbar

Ein http-Filter kann grundsätzlich nur für das http-Protokoll, jedoch nicht für https verwendet werden, da https-Pakete verschlüsselt sind und deshalb vom Filter nicht analysiert werden können. Da der Filter in diesem Fall nicht eingesetzt werden kann, besteht die Gefahr, dass durch eine https-Verbindung unerwünschter Netzwerkverkehr ermöglicht wird. Um auch dieses Risiko zu vermeiden, sollte generell https-Verkehr blockiert werden. Nur mit Hilfe von Ausnahmen werden in einer Regel bestimmte Webseiten zugelassen, mit denen eine https-Verbindung hergestellt werden darf.

9.3.2 Link Translation-Filter

Namensauflösung von Servernamen

Wenn ein interner Webserver veröffentlicht ist, kann es zu Problemen bei der Namensauflösung kommen, wenn Verknüpfungen auf Server verweisen, die lediglich über den internen Namen erreichbar sind. Ein externer Benutzer könnte in diesem Fall nicht auf den Server zugreifen. Zur Lösung dieses Problems kommt der Link Translation-Filter zum Einsatz. Dieser Filter prüft die Pakete der externen Clients auf bestimmte Namen hin und kann die internen Namen anhand der vom Administrator definierten Wörterbuchliste in für den externen Benutzer erreichbare Namen übersetzen. Die Konfiguration des Filters sowie das Erstellen der Wörterbuchliste geschieht über die Eigenschaften der Veröffentlichungsregel. Wechseln Sie dazu auf die Registerkarte LINKÜBERSETZUNG (siehe Abbildung 9.14).

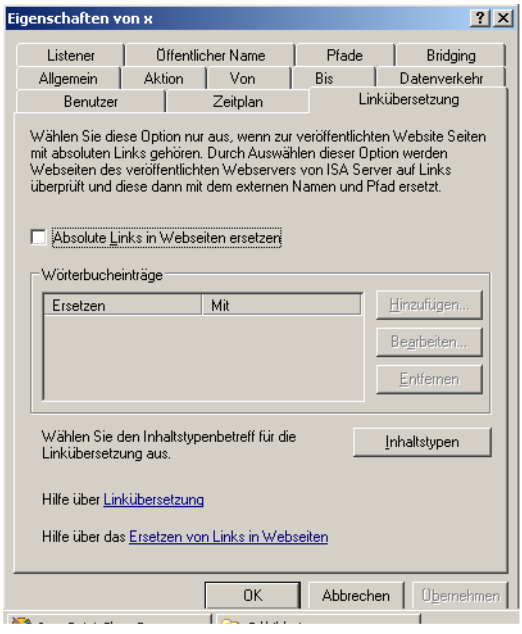


Abbildung 9.14: Konfiguration der Linkübersetzung

Eigene Einträge

Um neue Wörterbucheinträge hinzuzufügen, aktivieren Sie zunächst die Checkbox ABSOLUTE LINKS IN WEBSEITEN ERSETZEN und klicken dann auf HINZUFÜGEN.

Die Linkübersetzung kann nur konfiguriert werden, wenn Sie in der Veröffentlichungsregel einen expliziten Domänennamen angegeben haben. Bei der Wahl von JEDER DOMÄNENNAME kann die Linkübersetzung nicht angewendet werden.

Geben Sie in dem Fenster WÖRTERBUCHELEMENT HINZUFÜGEN/BEARBEITEN den originalen und den zu ersetzenden Text ein (siehe Abbildung 9.15).

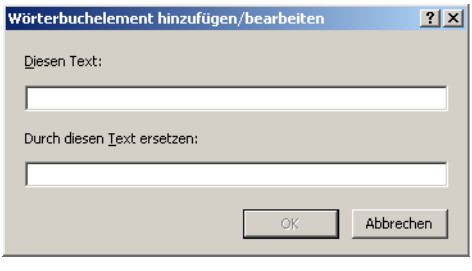


Abbildung 9.15: Hinzufügen eines Wörterbucheintrags

9.3.3 Formularbasierter OWA-Authentifizierungsfilter

Auch ältere Exchange-Versionen

Über diesen Filter wird die OWA-formularbasierte Authentifizierung bereitgestellt. Obwohl dieser Authentifizierungsmechanismus für Exchange Server 2003 entwickelt wurde, kann er auch für ältere Exchange-Versionen oder für die Authentifizierung an herkömmlichen Webseiten verwendet werden.

Damit die formularbasierte OWA-Authentifizierung zusammen mit der RADIUS-Authentifizierung eingesetzt werden kann, muss sichergestellt sein, dass auf dem ISA Server das Hotfix KB884560 installiert ist. Dieses Hotfix ist Bestandteil des Service Pack 1 für den ISA Server 2004.

9.3.4 RADIUS-Filter

RADIUS-Authentifizierungsmethode

Über diesen Filter wird RADIUS als zusätzliche Authentifizierungsmethode für eingehenden und ausgehenden Netzwerkverkehr zur Verfügung gestellt. Dieser Filter wird von Weblistenern verwendet, wenn diese Listener für die RADIUS-Authentifizierung konfiguriert sind. Ist die RADIUS-Authentifizierung gewählt, kann nur diese und keine andere Form der Authentifizierung wie z.B. die Digest- oder integrierte Authentifizierung gleichzeitig durchgeführt werden.

9.3.5 SecureID-Filter

Dieser Filter kann nur im Zusammenhang mit *RSA SecureID Authentication* verwendet werden. Dadurch wird die Multifaktor-Authentifizierung ermöglicht.

9.3.6 Webproxy-Filter

Eingehende Webanfragen

Über den Webproxy-Filter werden die eingehenden Webanfragen geprüft. Zusätzlich wird auch der Cache des ISA Server für die externen Clients bereitgestellt, damit deren Anfragen schneller beantwortet werden und die Zugriffe auf die veröffentlichten Server minimiert werden. Auch die Webfilter werden dem Firewall-Dienst über den Webproxy-Filter bereitgestellt.

9.4 IP-Filter

Erkennen von Angriffen

Die dritte Gruppe der vom ISA Server bereitgestellten Filter sind die IP-Filter. Diese dienen ausschließlich der Intrusion Detection sowie dem Erkennen und Verhindern von DNS-Attacken.

Detaillierte Hinweise zu den verschiedenen Angriffsszenarien, die der ISA Server 2004 automatisch erkennen kann, finden Sie in Kapitel 12.9.

9.4.1 IP-Optionen

Zusätzlich können auch noch verschiedene IP-Optionen zur Gefahrenabwehr eingestellt werden. Klicken Sie dazu in der ISA-mmc unter KONFIGURATION/ALLGEMEIN auf den Link IP-EINSTELLUNGEN DEFINIEREN.

IP-Optionen zum Sammeln von Informationen

Auf der Registerkarte IP-OPTIONEN (siehe Abbildung 9.16) finden Sie eine Liste von IP-Optionen. Mit Hilfe dieser Optionen kann der IP-Protokollstack beeinflusst werden. Der ISA Server ist in der Lage, bestimmte IP-Optionen zu blockieren. Dabei handelt es sich um die Optionen, die ein Angreifer benutzen kann, um weitere Informationen über das Netzwerk *Intern* zu sammeln und das Routing von Paketen nachzuverfolgen. Sobald alle oder einige der IP-Optionen ausgewählt sind, werden vom ISA Server alle IP-Pakete abgelehnt, in deren Header ein Flag für IP-Optionen gesetzt ist.

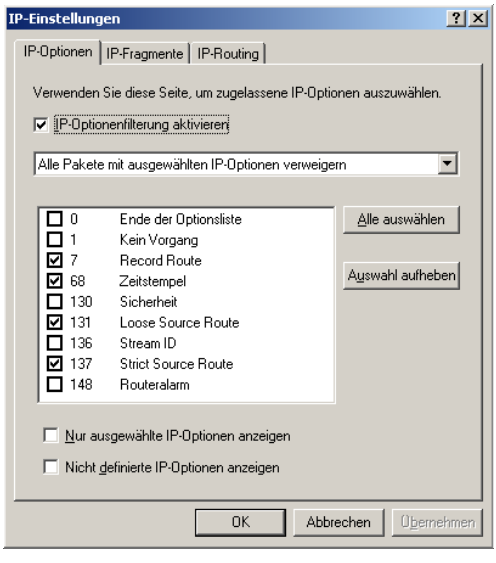


Abbildung 9.16: Konfiguration der IP-Optionen

IP-Fragmente können gefährlichen Code importieren

Auf der Registerkarte IP-FRAGMENTE kann festgelegt werden, ob IP-Fragmente gesperrt werden sollen oder nicht. Ein einzelnes IP-Datagramm kann in mehrere Teile zerlegt werden. Diese Teile werden als IP-Fragmente bezeichnet. Die einzelnen Fragmente werden alle an einen Server gesendet, der diese in der richtigen Reihenfolge wieder

zusammensetzt. Allerdings besteht bei dieser Technik auch die Gefahr, dass ein IP-Datagramm mit bösartigem Inhalt in mehrere Fragmente geteilt wird. Bei der Prüfung der einzelnen Fragmente kann der ISA Server noch nicht feststellen, dass es sich um bösartigen Code handelt, da dieser erst nach dem Zusammenfügen als solcher funktioniert. Da das Zusammensetzen des Pakets erst auf dem Zielserver geschieht, kann dort ungehindert das bösartige Paket mit seiner Wirkung beginnen.

Standarmäßig werden die IP-Fragmente nicht gesperrt, da dadurch auch Netzwerkverkehr wie z.B. bei der RADIUS-Authentifizierung betroffen sein könnte.

IP-Routing verbessert die Performance

Auf der dritten Registerkarte IP-ROUTING kann diese Funktion aktiviert oder deaktiviert werden. Ist das IP-Routing aktiviert, kann der ISA Server die Pakete der sekundären Verbindung im Kernelmodus weiterleiten, was zu einer Verbesserung der Leistung führt. Die auf dem Client erstellten IP-Pakete werden direkt an den Zielserver weitergeleitet. Wird das IP-Routing deaktiviert, werden vom ISA Server nur die IP-Daten des Pakets, nicht jedoch das gesamte IP-Paket weitergesendet. Damit ist sichergestellt, dass einige Clientinformationen nicht aus dem internen Netzwerk herausgelangen können.

9.4.2 Verbindungslimits

Maximale Anzahl gleichzeitiger Verbindungen

Des Weiteren haben Sie die Möglichkeit, die Anzahl aktiver Verbindungen einzuschränken. Damit wird unterbunden, dass der Server durch eine zu große Anzahl von Verbindungen arbeitsunfähig wird. Sobald das gesetzte Limit erreicht ist, werden vom ISA Server keine neuen Verbindungen mehr bereitgestellt. Diese Einstellung geschieht über KONFIGURATION/ALLGEMEIN über den Link VERBINDUNGSLIMITS FESTLEGEN (siehe Abbildung 9.17).

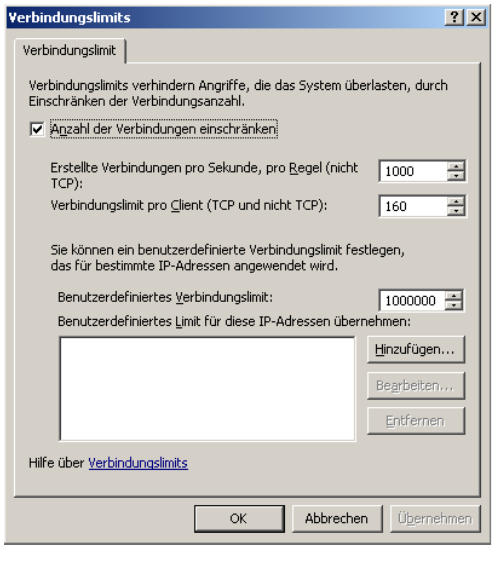


Abbildung 9.17: Festlegen von Verbindungslimits

Ausnahmen für interne Server

Sie können entweder die maximale Anzahl der Verbindungen pro Regel oder die maximale Anzahl von Verbindungen (TCP und nicht-TCP), die ein Client gleichzeitig aufbauen darf, einschränken. Zusätzlich kann auch für bestimmte IP-Adressen ein benutzerdefiniertes Limit von Verbindungen festgelegt werden. Dieses benutzerdefinierte Limit macht z.B. für interne Server Sinn, die ein höheres Limit als die Clients besitzen sollen. Sie können beispielsweise die internen Server zu einem bestimmten Computersatz zusammenfassen und für diesen das benutzerdefinierte Limit festlegen.

10 Remotezugriff und VPN

Dieses Kapitel beschäftigt sich mit den Themen Remotezugriff und VPN (Virtual Private Network). Immer häufiger ergibt sich für Unternehmen das Bedürfnis oder auch die Notwendigkeit, nicht nur vom lokalen Standort auf Daten und Applikationen zuzugreifen. Beispiele dafür sind Benutzer, die von einem Arbeitsplatz von zu Hause arbeiten, Mitarbeiter, die von unterwegs aus, z.B. bei einem Kunden, mit einem mobilen Gerät wie einem Notebook oder PDA auf Daten zugreifen, oder auch Mitarbeiter eines Partnerunternehmens, die auf bestimmte Teile von Ressourcen zugreifen dürfen.

Der Bedarf für ein VPN ist heutzutage sehr hoch

Zur Erfüllung dieser Ansprüche eigent sich der Einsatz eines VPN. Das VPN ist quasi eine Erweiterung des bestehenden Firmennetzwerks, so dass auch externen Clients Zugriff, z.B. über das Internet, auf dieselben Ressourcen wie den internen Clients gewährt werden kann. Nachdem die VPN-Verbindung aufgebaut worden ist, besitzt der Benutzer im Rahmen seiner Berechtigungen Zugriff auf das interne Netzwerk. Bestenfalls anhand der Zugriffsgeschwindigkeit bemerkt der Benutzer, dass er sich nicht direkt im internen Netzwerk befindet. Clients, die eine solche VPN-Verbindung herstellen, werden als Remote VPN-Clients bezeichnet.

Für die Zugriffssteuerung sind nicht nur die Berechtigungen des Benutzers an den Netzwerkressourcen, sondern auch die Richtlinieneinstellungen des ISA Server wichtig.

Bevor es an die Konfiguration des ISA Server geht, werden als Einführung oder Wiederholung die verschiedenen Typen von VPNs vorgestellt.

10.1 VPN-Typen

Beim Einsatz einer VPN-Verbindung wird über das Internet ein sicherer Tunnel zwischen dem Client und dem Server aufgebaut, so dass der Client auf die Ressourcen des internen Netzwerks zugreifen kann. Eine VPN-Verbindung besitzt eine Reihe von Vorteilen:

- Verwenden Sie eine DSL-Flatrate, entstehen für die Einwahl keine weiteren Kosten.
- In der Regel ist eine VPN-Verbindung deutlich schneller als eine Internetanbindung über eine Telefonleitung.
- Die VPN-Verbindung kann von jedem beliebigen Ort aus, an dem eine Internetverbindung verfügbar ist, aufgebaut werden. Selbst mit einem PocketPC kann eine VPN-Verbindung hergestellt werden.

Tunneling-Protokolle

Für die Einrichtung des VPN-Zugriffs können Sie verschiedene Typen von VPNs verwenden. Anhand dieser Erläuterungen sollen Sie ermitteln können, welchen Typ Sie am besten einsetzen. Bei allen VPN-Verbindungen handelt es sich um so genannte Tunneling-Protokolle. Dabei werden Daten in verschlüsselter Form von einem Ende des Tunnels zum anderen übertragen. Eine Seite des Tunnels bildet das Firmennetzwerk, die andere Seite der Standort des Benutzers. Als Verbindungsnetzwerk zwischen diesen beiden Enden wird in aller Regel das Internet verwendet.

Für die Übertragung des Pakets wird ein spezieller Header am Paket verwendet. In diesen Header werden Datenrahmen mit Hilfe des jeweiligen VPN-Protokolls gekapselt. Sobald das Paket am Endpunkt des Tunnels angelangt ist, wird das Paket wieder entkapselt, d.h. der Header entfernt. Der verbleibende Datenrahmen wird an das entsprechende Zielgerät weitergeleitet. Die verschiedenen Tunneling-Protokolle, die der ISA Server anbietet, werden im Folgenden vorgestellt.

Die praktische Umsetzung der Konfiguration am ISA Server wird danach erläutert.

10.1.1 Point-To-Point Tunneling Protocol (PPTP)

Nur IP-basierte Netzwerke

Die Abkürzung PPTP steht für Point-to-Point Tunneling Protocol. Beim Einsatz dieses Protokolls kann der Datenverkehr verschiedener Netzwerkprotokolle (TCP/IP, IPX/SPX usw.) für die Übertragung in einen IP-Header gekapselt werden, so dass die Übertragung verschlüsselt ist. Die Übertragung erfolgt über ein IP-basierendes Netzwerk. Das verschlüsselte Paket kann über ein internes Netzwerk oder auch über das Internet versendet werden. Es wird bei Verbindungen von Router-zu-Router-VPNs sowie Benutzer-zu-Router-VPNs eingesetzt.

PPTP besitzt die folgenden Features:

- Benutzerauthentifizierung über Windows, RADIUS und EAP
- Datenverschlüsselung mit MPPE (Microsoft Point-to-Point Encryption, Schlüssellänge 40, 56 oder 128 Bit)
- Dynamische IP-Zuweisung
- Datenkomprimierung

Die Sicherheit des PPTP beruht auf der Komplexität des Benutzerkennworts

Sobald eine erfolgreiche Authentifizierung des Benutzers erfolgt ist, werden die Daten verschlüsselt. Dies liegt darin begründet, dass der für die Verschlüsselung des Datenverkehrs erforderliche gemeinsame Schlüssel aus einem Hash abgeleitet wird, der auf dem Kennwort des Benutzers basiert. Je sicherer dieses Kennwort ist, desto sicherer ist letztendlich auch die PPTP-Verbindung.

10.1.2 Layer 2 Tunneling Protocol (L2TP)

Kein IP-basiertes Netzwerk nötig

L2TP steht als Abkürzung für Layer 2 Tunneling Protocol. Auch beim Einsatz dieses Protokolls erfolgt wie bei PPTP die Einkapselung des Datenverkehrs verschiedener Netzwerkprotokolle. Allerdings kann die Übertragung über ein beliebiges Netzwerk erfolgen und ist nicht an ein IP-basiertes Netzwerk gebunden. Für den Transport kann jedes Medium wie IP, X.25, Frame Relay oder ATM (Asynchronous Transfer Mode) verwendet werden, das die Übertragung von Point-to-Point-Datagrammen unterstützt. Bei der Konfiguration für IP kann L2TP als Tunneling-Protokoll über das Internet verwendet werden. Für die Tunnelverwaltung werden verschiedene L2TP-Messages sowie UDP (User Datagram Protocol) verwendet. Es wird wie PPTP bei Verbindungen von Router-zu-Router-VPNs sowie Benutzer-zu-Router-VPNs eingesetzt.

L2TP besitzt die folgenden Features:

- Benutzerauthentifizierung über Windows, RADIUS und EAP
- Datenverschlüsselung mit IPSec (Schlüssellänge 56 Bit – DES - oder 3 x 56 Bit - 3DES)
- Gegenseitige Authentifizierung der Geräte über IPSec-Schlüssel oder Zertifikate
- Dynamische IP-Zuweisung
- Datenkomprimierung

L2TP over IPSec bietet höhere Sicherheit als PPTP

Im Gegensatz zu PPTP setzt die Verschlüsselung des Datenverkehrs bereits vor der Authentifizierung ein. Zwischen den beiden Seiten des Tunnels wird eine auf IPSec basierende Sicherheitszuordnung ausgehandelt, die nicht an das Benutzerkennwort gebunden ist. Zur erfolgreichen Authentifizierung muss auf beiden Seiten des Tunnels zwingend eine Form der Authentifizierung wie z.B. ein IPSec-Schlüssel oder ein Zertifikat vorhanden sein.

10.1.3 IPSec

Die Abkürzung IPSec steht für IP Security. Über diesen Mechanismus werden IP-Pakete verschlüsselt und danach in einen Header gekapselt. Die Übertragung der Pakete kann wie bei PPTP nur über ein IP-basiertes Netzwerk erfolgen. IPSec unterstützt im Gegensatz zu den beiden anderen Protokollen kein Verfahren für die Benutzerauthentifizierung und IP-Zuweisung. In der Regel wird diese Methode bei Router-zu-Router-VPNs eingesetzt.

IPSEc kann im Transport- und Tunnelmodus benutzt werden. Im Transportmodus werden die Applikations-, TCP- sowie UDP-Header und Paketdaten verschlüsselt, jedoch nicht der IP-Header. Im Tunnelmodus wird das komplette Paket verschlüsselt.

ESP unter NAT-T

Es gibt zwei verschiedene IPSec-Protokolle, die sich jedoch hinsichtlich der Authentifizierung und Integrität unterscheiden: *Authentication Header (AH)* sowie *Encapsulating Security Payload (ESP)*. ESP ist das einzige Protokoll, das mit NAT-T verwendet werden kann.

IPSec-Tunnelmodus

Normalerweise wird das IPSec-Protokoll für die Verschlüsselung im Zusammenhang mit L2TP verwendet. Dennoch kann IPSec auch als Tunneling-Protokoll verwendet werden. Dabei werden die IP-Pakete verschlüsselt und in IP-Header eingekapselt. Diese Pakete können über das Unternehmensnetzwerk oder auch das Internet gesendet werden. Allerdings muss es sich dabei um ein IP-basiertes Netzwerk handeln. IPSec kann für die Interoperabilität mit anderen Routern oder Gateways verwendet werden, die nicht L2TP über IPSec oder PPTP-Tunneling unterstützen.

10.1.4 Wann soll welches Protokoll verwendet werden?

Protokollanforderungen

Der Einsatz eines bestimmten Protokolls ist an bestimmte Voraussetzungen, z.B. beim Einsatz des Betriebssystems, gebunden. Auch je nach gewünschter Anforderung z.B. an Verschlüsselung oder NAT-Unterstützung kann sich entscheiden, welches Protokoll eingesetzt werden sollte. Anhand von Tabelle 10.1 werden verschiedene Kriterien in Bezug auf die beiden Protokolle PPTP und L2TP over IPSec miteinander verglichen.

Tabelle 10.1: Übersicht über die Features der Protokolle PPTP und L2TP over IPSec

Feature	PPTP	L2TP over IPSec
Betriebssysteme	Windows 98, ME, NT 4.0, 2000, XP, 2003	Windows 2000, XP, 2003. Softwareaktualisierung für ältere Windows-Clients erforderlich
NAT-Unterstützung	Die NAT-Geräte müssen einen PPTP-NAT-Editor besitzen.	Beide Tunnelseiten müssen NAT-T unterstützen.
Verschlüsselung	MPPE 40, 56 oder 128 Bit	IPSec (56Bit – DES - oder 3 x 56 Bit - 3DES)

Der ISA Server 2004 bietet zahlreiche Funktionen, die den Windows RRAS-Dienst (Routing und RAS) erweitern. Die wichtigsten dieser Unterstützungen und Features sind:

- VPN-Unterstützung für Remote-Client-VPN und Standort-zu-Standort-VPN
- Überwachung von VPN-Clientsitzungen
- Standort-zu-Standort-VPNs unter Benutzung von PPTP, L2TP und IPSec.
- Behandlung von VPN-Clients und Quarantäne-Clients als eigenes Netzwerk
- VPN-Quarantäne
- Zugriffsregeln für die Steuerung der Verbindung zwischen den Netzwerken und VPN-Netzwerken.

10.1.5 Anforderungen an die Protokolle

Tabelle 10.2 zeigt, welche Anforderungen an die VPN-Protokolle von welchem Protokoll unterstützt werden.

Feature	PPTP	L2TP über IPSec	IPSec-Transport-modus	IPSec-Tunnel-modus
VPN-Verbindung Client-Standort	x	x	-	-
VPN-Verbindung Standort-Standort	x	x	-	x
Datenver-schlüsselung	x	x	x	x
Benutzerauthen-tifizierung	x	x	-	-
Computer-authentifizierung	-	x	x	x
Adresszuweisung	x	x	-	-
Schlüsselverwaltung	-	x	x	x

Tabelle 10.2: Übersicht über die Funktionsunterstützung für bestimmte Features durch die verschiedenen VPN-Protokolle

10.1.6 Möglichkeiten der Veröffentlichung

Verschiedene Veröffentlichungs-möglichkeiten

Die folgende Tabelle gibt eine Übersicht über die Veröffentlichungsmöglichkeiten der VPN-Protokolle unter ISA Server 2004 sowie Hinweise und Einschränkungen dabei.

Tabelle 10.3: Übersicht über Veröffentlichungsmöglichkeiten der VPN-Protokolle durch den ISA Server 2004

Protokoll	Veröffentlichung	Anmerkungen
PPTP	Wird unterstützt	Vom PPTP-Filter werden eingehende Verbindungen unterstützt, während unter ISA Server 2000 lediglich ausgehende Verbindungen unterstützt wurden.
IPSec-Tunnelmodus	Wird zwischen Netzwerken mit Routenverbindung unterstützt, jedoch nicht zwischen Netzwerken mit NAT-Verbindung, wenn der VPN-Server im IPSec-Tunnelmodus nicht NAT-T unterstützt	Ein NAT-Gerät wie ein ISA Server setzt die Validierung der IPSec-Pakete während der Adressauflösung außer Kraft. Befinden sich in einem ISA Server-2004-Perimeter-Netzwerk lediglich öffentliche Adressen und besteht eine Routenverbindung zwischen dem Front-End-ISA Server, der direkt mit dem Internet verbunden ist, und dem Perimeter-Netzwerk, so können VPN-Server hinter dem Front-End-Server mit IPSec im Tunnelmodus ohne NAT veröffentlicht werden. Enthält das Perimeter-Netzwerk private Adressen, kann lediglich eine NAT-Verbindung zwischen den Netzwerken eingerichtet werden.
L2TP über IPSec ohne NAT-T	Wird nicht zwischen Netzwerken mit NAT-Verbindung unterstützt, wenn der VPN-Server im IPSec-Tunnelmodus nicht NAT-T unterstützt	Keine
L2TP über IPSec NAT-T	Wird unterstützt	Keine

Der ISA Server 2000 unterstützt keine Veröffentlichung von PPTP sowie L2TP über IPSec ohne NAT-T. IPSec im Tunnelmodus ist nur dann möglich, wenn der VPN-Server NAT-T unterstützt.

10.2 Eingehende VPN-Verbindungen einrichten

Sobald sich ein VPN-Client nach erfolgreicher Authentifizierung mit dem Firmennetzwerk verbunden hat und verschlüsselt Daten übertragen kann, wird dieser Remote VPN-Client wie ein interner Netzwerk-Client behandelt. Allerdings würde der völlig uneingeschränkte Zugriff wie durch einen richtigen internen Client ein zu hohes Risiko für das Firmennetzwerk bedeuten. Deshalb sollte der Zugriff immer nur auf die Ressourcen beschränkt werden, die der VPN-Client tatsächlich benötigt.

Einschränken der Ressourcen für den VPN-Zugriff

Server, Dienste, Netzwerke und weitere Ressourcen, für die der jeweilige Client keinen Zugriff besitzen muss, sollten für ihn auch nicht erreichbar sein. Über die internen Clients besitzt der Administrator des Unternehmens einen Überblick. So kann er diese gemäß den Standards des Unternehmens konfigurieren und über Patches und Updates sowie geeignete Programme absichern. Bei einem VPN-Client ist dies nicht oder nur bedingt möglich. Arbeitet ein Mitarbeiter beispielsweise von zu Hause und verwendet dazu seinen privaten Computer oder sein Notebook, so ist dieses Gerät gemäß den eigenen Wünschen des Benutzers eingerichtet. Auch wenn der Zugriff von einem öffentlichen Computer, z.B. von einem Internetcafe aus erfolgt, entspricht dieser Computer nicht den Richtlinien des Unternehmens.

Anhand dieser Beispiele sollte bereits deutlich sein, dass eine Minimierung der zugriffsberechtigten Ressourcen für VPN-Clients eine Maximierung der Sicherheit darstellt.

Das spezielle Netzwerk VPN-Clients

Sobald ein VPN-Client eine Verbindung zum Firmennetzwerk hergestellt hat, wird dieser zu dem bereits vordefinierten Netzwerk VPN-CLIENTS hinzugefügt. Für dieses Netzwerk müssen Zugriffsregeln definiert werden. Diese bestimmen, auf welche Ressourcen in welchen anderen Netzwerken zugegriffen werden darf und auf welche nicht. Zur Umsetzung der Zugriffsregeln wird der RRAS-Dienst verwendet, an den die Einstellungen der Zugriffsregeln übergeben werden.

Der ISA Server 2004 ist in der Lage, die Zugriffe auf das Firmennetzwerk bis auf die Anwendungsebene zu verfolgen und zu analysieren.

10.3 VPN-Server veröffentlichen

Wahl des Protokolls

Über die Serververöffentlichungsregeln des ISA Server 2004 wird der Zugriff auf Ressourcen des internen Netzwerks ermöglicht, ohne dabei die Sicherheit des Netzwerks zu reduzieren. Als neues Feature ermöglicht es der ISA Server, auch VPN-Server zu veröffentlichen. Dieser veröffentlichte Server kann als Endpunkt für die eingehenden Verbindungen dienen. Als VPN-Verbindung können die folgenden Typen verwendet werden:

- PPTP (Point-to-Point Tunneling Protocol)
- L2TP (Layer 2 Tunneling Protocol
- IPSec (L2TP over Internet Protocol Security) in Verbindung mit NAT oder NAT-T (Network Address Translation/NAT-Traversal)

Der ISA Server 2004 kann selbst als VPN-Server agieren. Es ist jedoch ebenso möglich, einen anderen Server als VPN-Server zu veröffentlichen, der sich im Netzwerk hinter dem ISA Server befindet. Für die Veröffentlichung sind verschiedene Lösungen möglich. Die folgenden drei Lösungen sind die am häufigsten eingesetzten:

- Veröffentlichen eines PPTP-VPN-Servers über PPTP
- Veröffentlichen eines L2TP over IPSec-NAT-T-Servers über NAT-T. (hierzu muss der VPN-Server unbedingt unter Windows Server 2003 ausgeführt werden).
- Veröffentlichen eines L2TP-VPN-Servers ohne IPSec

10.3.1 Voraussetzungen für die Veröffentlichung

Um einen VPN-Server veröffentlichen zu können, müssen die folgenden Voraussetzungen erfüllt sein:

- Es muss ein ISA Server eingerichtet sein, der über zwei Netzwerkkarten verfügt. Über eine Netzwerkkarte erfolgt die Verbindung zum internen Netzwerk, über die andere die Verbindung zum externen Netzwerk, also dem Internet.
- Die externe Netzwerkkarte muss über eine statische IP-Adresse verfügen und eine dauerhafte Verbindung zum Internet herstellen.
- Ein Computer muss als VPN-Endpunkt fungieren. Dieser sollte lediglich über den ISA Server seine Verbindung zum Internet herstellen und muss über mindestens eine Verbindung zum internen Netzwerk verfügen.
- Soll L2TP over IPSec als VPN-Verbindung genutzt werden, muss auf dem VPN-Server ein digitales Zertifikat installiert sein. Alle Clients, die die L2TP over IPSec-VPN-Verbindung benutzen, müssen dieser CA vertrauen. Weitere Hinweise zum Einsatz von Zertifikaten unter ISA Server 2004 finden Sie im Artikel unter dem

Link *http://go.microsoft.com/fwlink/?LinkId=20794*. sowie dem Artikel *Digital Certificates* auf der Begleit-CD.

- Auf allen L2TP over IPSec-Clients muss das NAT-T-Update installiert sein. Weitere Hinweise zu diesem Update finden Sie in der Microsoft Knowledge Base unter dem Link *http://support.microsoft.com/kb/818043/de*.

Detaillierte Hinweise für die Installation und Grundkonfiguration des VPN-Servers unter Windows Server 2003 finden Sie unter dem Link *http://go.microsoft.com/fwlink/?LinkId=28085*.

10.3.2 Grundkonfiguration des VPN-Servers

Bevor der VPN-Server veröffentlicht werden kann, muss er noch konfiguriert werden. Dazu muss der VPN-Server bereits auf dem Windows Server 2003 installiert sein.

Standardgateway

Als Standardgateway tragen Sie auf dem VPN-Server die Adresse des Netzwerkadapters ein, der auf dem ISA Server die Verbindung zum internen Netzwerk herstellt.

Die weitere Konfiguration ist abhängig davon, in welcher Weise der VPN-Server veröffentlicht werden soll. In den drei folgenden Kapiteln werden die Verfahren für die Veröffentlichung von VPN über PPTP, VPN über L2TP/IPSec mit NAT-T sowie eines L2TP-Servers beschrieben.

10.4 Eingehende PPTP-Verbindungen einrichten

Für die VPN-Remoteeinwahl unterstützt der ISA Server 2004 die beiden Tunnelprotokolle PPTP und L2TP/IPSec. In diesem Kapitel wird die Einrichtung des PPTP-Protokolls auf dem ISA Server beschrieben. Die zweite Variante wird im folgenden Kapitel näher vorgestellt.

Unterstützung für NAT-Geräte

PPTP ist einserseits einfach zu konfigurieren und bietet andererseits den Vorteil, dass es problemlos mit Geräten funktioniert, die NAT verwenden. Allerdings bietet PPTP nicht so hohe Sicherheitsmaßstäbe wie L2TP/IPSec.

Um die Einrichtung des PPTP-Protokolls durchzuführen, sind die folgenden Schritte erforderlich:

1. Klicken Sie in der ISA-mmc auf den Eintrag VIRTUELLE PRIVATE NETZWERKE. Ihnen werden in der Übersicht die fünf Schritte angezeigt, die für die Konfiguration erforderlich sind (siehe Abbildung 10.1). Um einen dieser Schritte auszuführen, klicken Sie jeweils auf den Link.

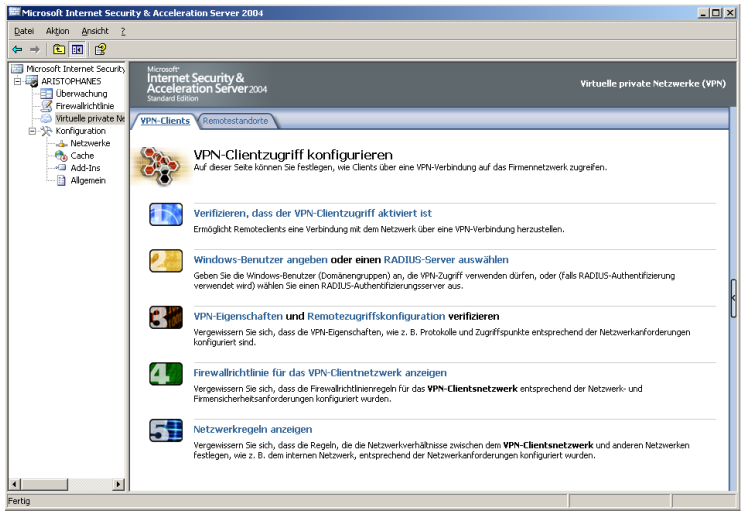


Abbildung 10.1: Übersicht über die einzelnen Schritte der VPN-Konfiguration auf dem ISA Server

2. Als Erstes müssen Sie prüfen, ob der Clientzugriff aktiviert ist. Dazu können Sie bestimmen, wieviele VPN-Verbindungen der ISA Server gleichzeitig verarbeiten soll. Klicken Sie dazu auf den Link VERIFIZIEREN, DASS DER CLIENTZUGRIFF AKTIVIERT IST. Markieren Sie die Checkbox VPN-CLIENTZUGRIFF AKTIVIEREN (siehe Abbildung 10.2) und geben Sie die maximale Anzahl der gleichzeitigen Verbindungen an. Je nach Wert werden im RRAS-Dienst zusätzliche Ports für PPTP- und L2TP-Verbindungen hinzugefügt.

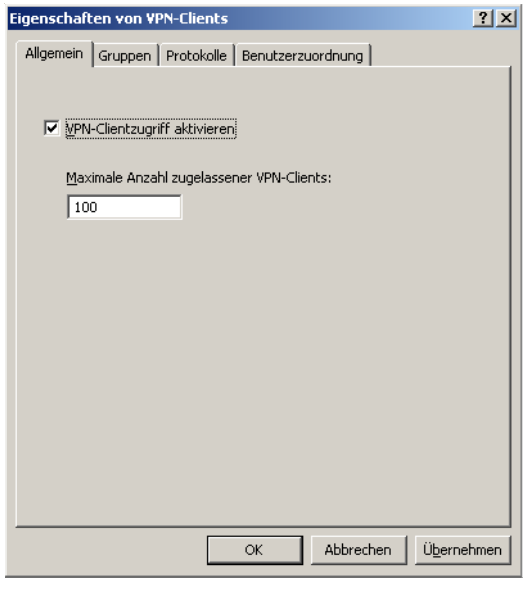


Abbildung 10.2: Aktivieren des VPN-Clientzugriffs

3. Im nächsten Schritt WINDOWS-BENUTZER ANGEBEN ODER RADIUS-SERVER WÄHLEN wird die Authentifizierungsmethode für die VPN-Benutzer bestimmt. Die Benutzerauthentifizierung kann entweder auf dem ISA Server selbst über RAS-Richtlinien erfolgen oder aber die Authentifizierung wird über RADIUS vorgenommen und an einen RADIUS-Server weitergeleitet.

Der Einsatz eines RADIUS-Servers ist immer anzuraten

Die erste Form ist nur dann sinnvoll, wenn der ISA Server Mitglied einer Active Directory-Domäne ist. Durch den Zugriff auf die Datenbank des Active Directory kann die Benutzerauthentifizierung durchgeführt werden. Ist der ISA Server kein Domänenmitglied, was aus Sicherheitserwägungen auch häufig der Fall ist, müssen die Anmeldeinformationen des Benutzers an einen RADIUS-Server weitergeleitet werden, der Mitglied der Domäne ist. Über diesen Umweg ist der Zugriff auf die Konteninformationen über einen Domänencontroller des Active Directory möglich. Das Ergebnis der Kontenprüfung gibt der RADIUS-Server an den ISA Server zurück. Diese Methode ist sinnvoller und sicherer, da auf die Domänenmitgliedschaft des ISA Server verzichtet werden kann.

Gruppen und Benutzer hinzufügen

Nachdem Sie auf den Link geklickt haben, klicken Sie auf der Registerkarte GRUPPEN auf HINZUFÜGEN. In der Liste werden sämtliche globalen Benutzergruppen aus der Benutzerdatenbank des ISA Server und der Domäne angezeigt, zu der der ISA Server gehört, sowie der vertrauenden Domäne (siehe Abbildung 10.3). Die Gruppen der Domänen werden natürlich nur angezeigt, wenn der ISA Server Domänenmitglied ist. Wählen Sie die gewünschte Gruppe oder mehrere Gruppen aus.

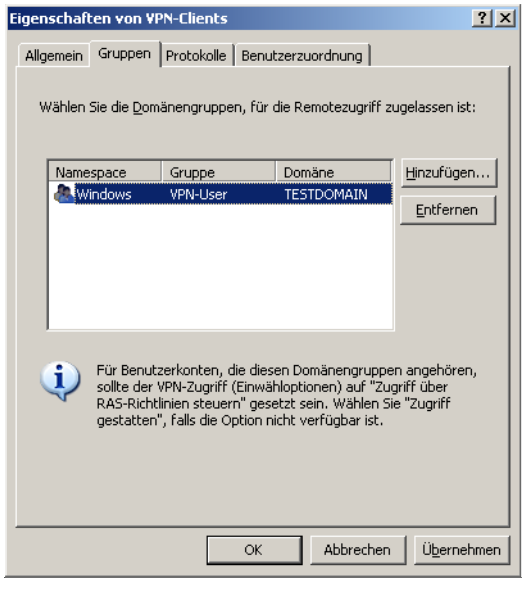


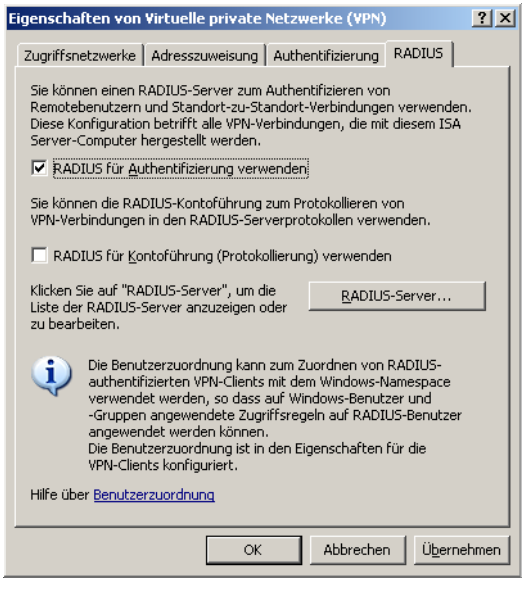
Abbildung 10.3: Auswahl der Benutzergruppen, die VPN-Verbindungen herstellen dürfen

Der VPN-Zugriff ist ausschließlich den Mitgliedern der hier gewählten Gruppen möglich. Diese Gruppen werden in die lokale RAS-Richtlinie integriert.

Soll statt der manuellen Auswahl der Benutzergruppen ein RADIUS-Server eingesetzt werden, muss dieser zusätzlich konfiguriert werden. Soll kein RADIUS-Server verwendet werden, können Sie mit dem folgenden Schritt fortfahren.

- Klicken Sie unter Schritt 2 auf RADIUS-SERVER AUSWÄHLEN.
- Auf der Registerkarte RADIUS (siehe Abbildung 10.4) markieren Sie die Checkbox RADIUS FÜR AUTHENTIFIZIERUNG VERWENDEN.
- Sollen zusätzlich auch die Protokollinformationen der VPN-Verbindungen an den RADIUS-Server weitergeleitet werden, markieren Sie auch die Checkbox RADIUS FÜR KONTOFÜHRUNG (PROTOKOLLIERUNG) VERWENDEN.

Abbildung 10.4: Auswahl der RADIUS-Authentifizierung



Diese Option ist besonders dann sinnvoll, wenn mehrere ISA Server den RADIUS-Server verwenden. So wird es möglich, die Protokollierungen sämtlicher ISA Server zentral in einer Datei auf dem RADIUS-Server zur Auswertung zu erfassen.

- Um den RADIUS-Server auszuwählen, klicken Sie auf die Schaltfläche RADIUS-SERVER. Über HINZUFÜGEN wird der Server ausgewählt und konfiguriert. Dieser Server ist sowohl für eingehende als auch für ausgehende Verbindungen zuständig.

Achten Sie darauf, dass auch die Regel der Systemrichtlinien zur Weiterleitung von RADIUS-Authentifizierungspaketen an das interne Netzwerk aktiviert ist. Dies ist standardmäßig der Fall.

4. Klicken Sie als Nächstes auf den Link für Schritt 3 VPN-EIGENSCHAFTEN UND REMOTEZUGRIFFSKONFIGURATION VERIFIZIEREN, um weitere Eigenschaften der VPN-Verbindung zu konfigurieren. Auf der Registerkarte PROTOKOLLE bestimmen Sie, dass das PPTP-Protokoll als VPN-Protokoll benutzt werden soll (siehe Abbildung 10.5).

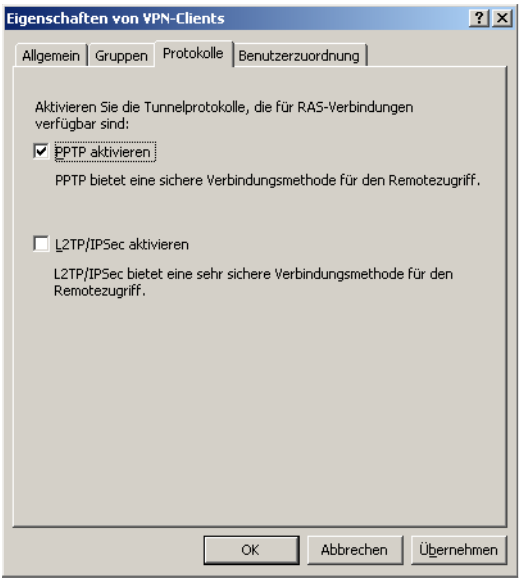


Abbildung 10.5: Auswahl des PPTP-Protokolls

Klicken Sie dann auf OK und auf REMOTEZUGRIFFSKONFIGURATION unter Schritt 3. Auf der Registerkarte ZUGRIFFSNETZWERKE (siehe Abbildung 10.6) wählen Sie die Netzwerke aus, von denen aus VPN-Verbindungen hergestellt werden dürfen. Da die Zugriffe in der Regel über das Internet erfolgen, wählen Sie hier das Netzwerk EXTERN. Es können jedoch noch weitere Netzwerke ausgewählt werden.

Adressvergabe via DHCP für die VPN-Clients

Auf der Registerkarte ADRESSZUWEISUNG (siehe Abbildung 10.7) kann für die Zuweisung der IP-Adressen DHCP oder ein statischer Adresspool eingesetzt werden. Der Einsatz von DHCP macht insbesondere dann Sinn, wenn auch die internen Netzwerkclients ihre Adressen via DHCP erhalten. Sobald der ISA Server bzw. der RRAS-Dienst gestartet wird, wird ein DHCP-Server über einen DHCP-Broadcast gesucht. Es werden von diesem IP-Adressen angefordert. Der DHCP-Server nimmt diese Anforderung entgegen und reserviert standardmäßig zehn IP-Adressen für den ISA Server, die er VPN-Clients zuweisen kann.

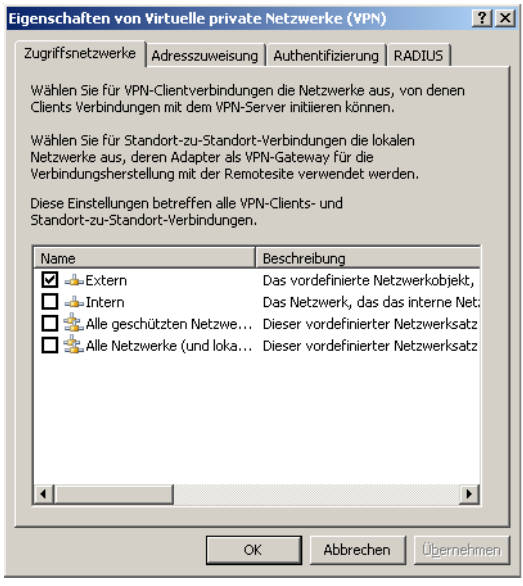


Abbildung 10.6: Auswahl der Netzwerke, von denen aus VPN-Verbindungen zugelassen werden

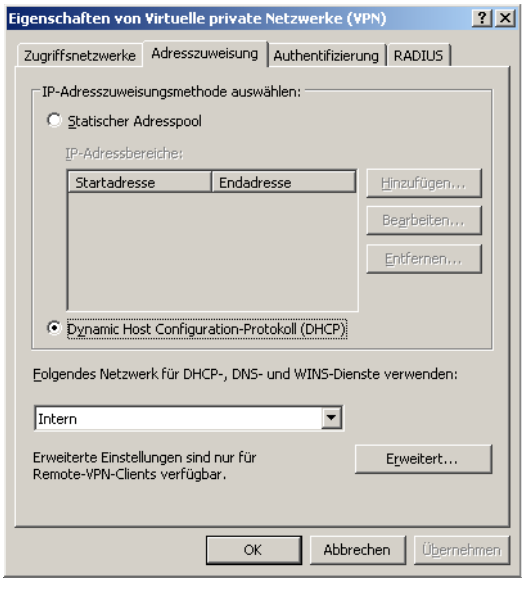


Abbildung 10.7: Methode der Adresszuweisung für die VPN-Clients

DHCP-Relay-Agent

Der ISA Server kann auf diese Weise den VPN-Clients lediglich eine IP-Adresse zuweisen. Weitere Informationen der DHCP-Bereichsoptionen wie DNS-Server oder Standardgateway erhält der VPN-Client auf diese Weise nicht. Damit auch diese Informationen vom DHCP-Server bezogen werden können, muss der ISA Server als DHCP-Relay-Agent konfiguriert werden.

Mit einem Klick auf ERWEITERT können Sie zusätzlich auch bestimmen, welche DNS- und WINS-Server den VPN-Clients zugeteilt werden (siehe Abbildung 10.8).

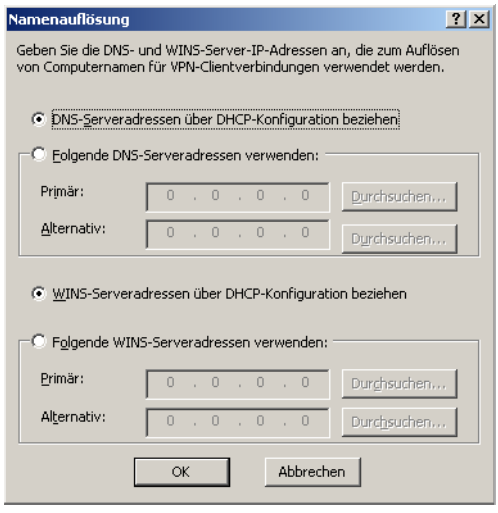


Abbildung 10.8: Optionales Zuweisen von IP-Adressen des DNS- und WINS-Servers für die VPN-Clients

Die Konfiguration des ISA Server als DHCP-Relay-Agent ist auch dann notwendig, wenn sich der ISA Server in einem anderen Netzwerksegment befindet als der DHCP-Server, da diesen sonst die DHCP-Broadcasts des ISA Server nicht erreichen.

Konfiguration des ISA Server als DHCP-Relay-Agent

Um den ISA Server als DHCP-Relay-Agent zu konfigurieren, sind die folgenden Schritte erforderlich:

1. Öffnen Sie auf dem ISA Server die mmc ROUTING UND RAS.
2. Wählen Sie unter IP-ROUTING das Kontextmenü NEUES ROUTING-PROTOKOLL des Eintrags ALLGEMEIN.
3. Nachdem das Protokoll DHCP-RELAY-AGENT hinzugefügt worden ist, wählen Sie dessen Kontextmenüeintrag EIGENSCHAFTEN.
4. Tragen Sie auf der Registerkarte ALLGEMEIN die IP-Adresse des DHCP-Servers ein. Es können auch mehrere Adressen eingetragen werden, wenn mehrere DHCP-Server eingesetzt werden (siehe Abbildung 10.9).

Verwechseln Sie die hier angegebene Netzwerkschnittstelle *Intern* nicht mit der physikalischen Schnittstelle des ISA Server, die eine Verbindung zum internen Netzwerk herstellt.

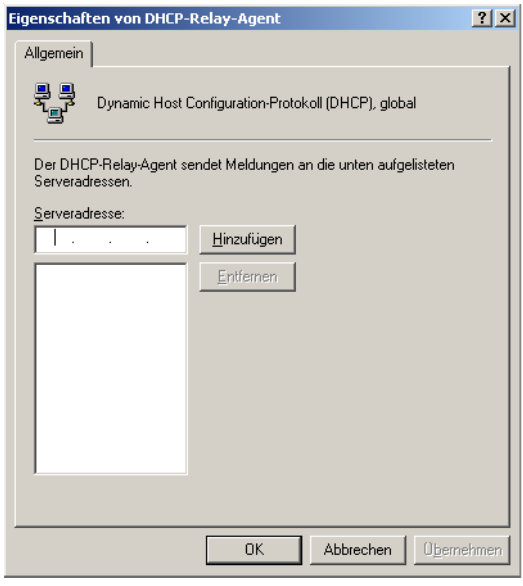


Abbildung 10.9: Hinzufügen von IP-Adressen von DHCP-Servern

5. Klicken Sie dann auf das Kontextmenü NEUE SCHNITTSTELLE des DHCP-Relay-Agent und wählen Sie die Schnittstelle INTERN aus. Unter NEUSTARTSCHWELLENWERT (SEKUNDEN) muss der Wert von 4 auf 1 abgeändert werden (siehe Abbildung 10.10).

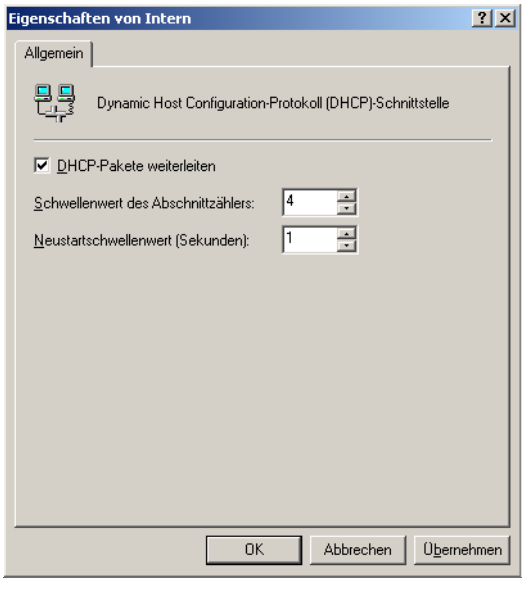


Abbildung 10.10: Konfiguration der Netzwerkschnittstelle Intern

6. Des Weiteren muss unter Schritt 3, Remotezugriffskonfiguration noch eine Authentifizierungsform gewählt werden. Die geschieht auf der Registerkarte AUTHENTIFIZIERUNG (siehe Abbildung 10.11).

Voreingestellt ist dort die Authentifizierungsmethode MS-CHAP V2. Diese Einstellung sollten Sie so belassen, da diese eine sichere Methode für die Authentifizierung mit Benutzername und Kennwort ist.

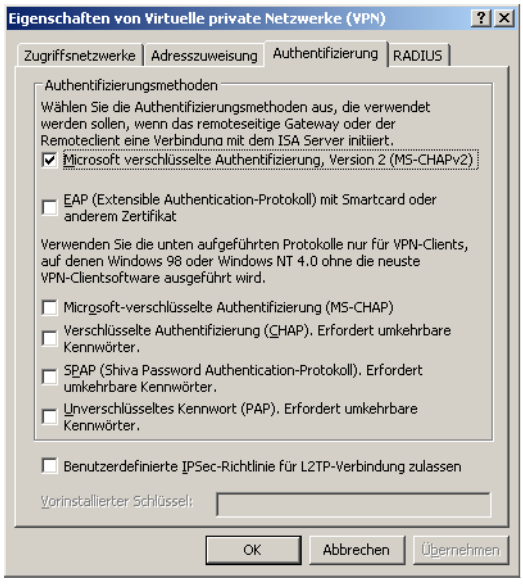


Abbildung 10.11: Auswahl der Authentifizierungsmethoden für die VPN-Clients

Mehrere Authentifizierungsmethoden

Die Sicherheit der einzelnen genannten Methoden ist von oben nach unten absteigend:

- MICROSOFT VERSCHLÜSSELTE AUTHENTIFIZIERUNG, VERSION 2 (MS-CHAPv2): Dieses Verfahren ist eine Erweiterung von MS-CHAP. Zusätzlich zu den Features von MS-CHAP findet eine gegenseitige Authentifizierung der Geräte statt. Außerdem werden unterschiedliche Sitzungsschlüssel zum Versenden und Empfangen verschlüsselter Pakete verwendet.

Sicherste Methode

- EAP (EXTENSIBLE AUTHENTICATION PROTOKOLL): Über EAP werden verschiedene Mechanismen zur Authentifizierung unterstützt (digitale Zertifikate, Smardcards usw.). Allerdings ist für alle diese Methoden eine spezielle Infrastruktur notwendig. Ist diese vorhanden, ist EAP die sicherste aller aufgeführten Mechanismen.
- MICROSOFT VERSCHLÜSSELTE AUTHENTIFIZIERUNG (MS-CHAP): Dieses Authentifizierungsverfahren wird nur von Microsoft-basierten Betriebssystemen unterstützt. Sobald die Verbindung aufgebaut wird, sendet der VPN-Server an den Client einen Challenge. Dabei handelt es sich um eine Sitzung-ID und eine zufällige Zeichenfolge. Aus diesen Challenge-Informationen und dem Kennwort des Benutzers wird über einen bestimmten Algorithmus (MD4) ein Hashwert gebildet. Da an den Server dieser Hashwert vom Client

gesendet wird, kann ein Angreifer keine Informationen über das Benutzerkennwort erhalten. Sobald der VPN-Server diesen Hashwert erhält, berechnet er anhand der Challenge und des in der Benutzerdatenbank gespeicherten Kennworts ebenfalls einen Hashwert. Nur wenn diese beiden Hashwerte übereinstimmen, ist die Authentifizierung gültig. Damit der VPN-Server ebenfalls einen Hashwert berechnen kann, müssen die Kennwörter im Gegensatz zur CHAP-Authentifizierung nicht mit umkehrbarer Verschlüsselung gespeichert sein. Zusätzlich kann der Benutzer über MS-CHAP aufgefordert werden, ein neues Kennwort einzugeben, wenn sein altes Kennwort abgelaufen ist. Lediglich der Benutzername wird bei dieser Form der Authentifizierung unverschlüsselt im Klartext an den VPN-Server übertragen.

- VERSCHLÜSSELTE AUTHENTIFIZIERUNG (CHAP): Sobald die Verbindung aufgebaut wird, sendet der VPN-Server an den Client einen Challenge. Dabei handelt es sich um eine Sitzung-ID und eine zufällige Zeichenfolge. Aus diesen Challenge-Informationen und dem Kennwort des Benutzers wird über einen bestimmten Algorithmus (MD5) ein Hashwert gebildet. Da an den Server dieser Hashwert vom Client gesendet wird, kann ein Angreifer keine Informationen über das Benutzerkennwort erhalten. Sobald der VPN-Server diesen Hashwert erhält, berechnet er anhand der Challenge und des in der Benutzerdatenbank gespeicherten Kennworts ebenfalls einen Hashwert. Nur wenn diese beiden Hashwerte übereinstimmen, ist die Authentifizierung gültig. Damit der VPN-Server ebenfalls einen Hashwert berechnen kann, müssen die Kennwörter mit umkehrbarer Verschlüsselung gespeichert sein. Lediglich der Benutzername wird bei dieser Form der Authentifizierung unverschlüsselt im Klartext an den VPN-Server übertragen.
- SHAP (SHIVA PASSWORD AUTHENTICATION PROTOKOLL): Es handelt sich um ein proprietäres Protokoll, das für die Kommunikation zwischen Shiva-Client und –Server eingesetzt wird. Dabei ist eine umkehrbare Verschlüsselung verfügbar, die zumindest einen geringen Sicherheitsanspruch erfüllt.

Nicht zu empfehlen

- UNVERSCHLÜSSELTES KENNWORT (PAP): Der Benutzername und das Kennwort werden unverschlüsselt vom VPN-Client an den Server übertragen. Auf diese Weise können die Benutzerinformationen von einem Angreifer sehr leicht ermittelt werden. Es ist nicht anzuraten, die Methode zur Authentifizierung zu verwenden.

7. Klicken Sie als Nächstes auf Schritt 4, FIREWALLRICHTLINIE FÜR DAS CLIENTNETZWERK ANZEIGEN. Sie können nun eine oder mehrere Zugriffsregeln für die VPN-Clients einrichten. Auch hier können Sie wie bei jeder anderen Zugriffsregel den Zugriff auf bestimmte Protokolle beschränken. Stellen Sie sicher, dass Sie unter ZUGRIFFSREGELQUELLEN (siehe Abbildung 10.12) das Netzwerk *VPN-Clients* wählen, als ZUGRIFFSREGELZIEL wird in der Regel das interne Netzwerk angegeben.

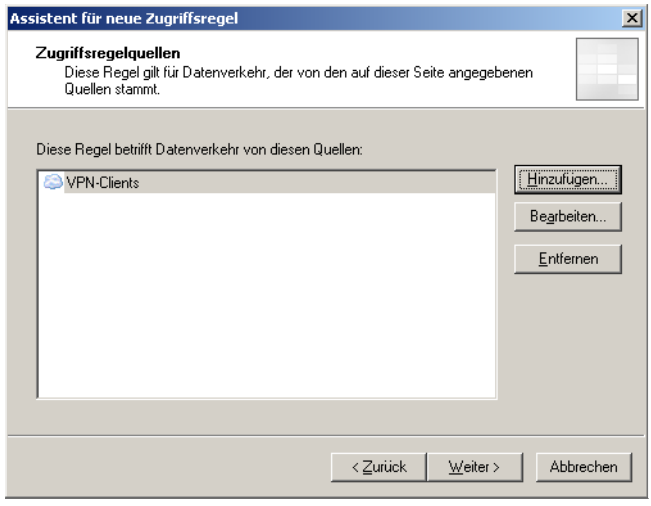


Abbildung 10.12: Auswahl des Netzwerks VPN-Clients als Zugriffsregelquelle

Bedenken Sie, dass Firewall- und Webproxy-Clients, die als VPN-Clients verwendet werden, für die Kommunikation mit dem ISA Server TCP-Port 1745 (Firewall-Clients) oder TCP-Port 8080 (Webproxy-Clients) verwenden. Diese Ports können nicht geändert werden und müssen für die Kommunikation zugelassen werden.

8. Der letzte Schritt der VPN-Konfiguration lautet NETZWERKREGELN ANZEIGEN. Prüfen Sie unter den Netzwerkregeln (siehe Abbildung 10.13), wie Verbindungen des Netzwerks *VPN-Clients* mit den anderen Netzwerken hergestellt werden. Die Verbindung kann über Route oder NAT hergestellt werden.

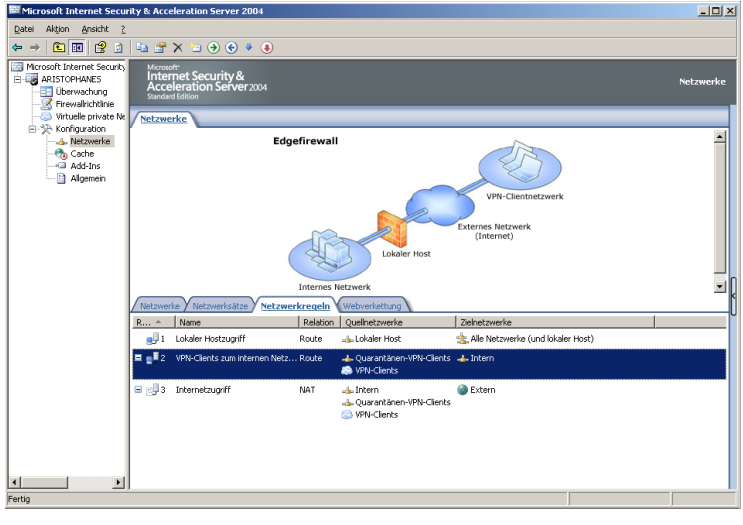


Abbildung 10.13: Prüfen der Netzwerkregeln für das Netzwerk VPN-Clients

Änderungen am Routing- und RAS-Dienst

Konfigurationsänderungen

Beim Konfigurieren des VPN-Zugriffs wurden auch einige Änderungen am Routing- und RAS-Dienst vorgenommen. Sie finden nun in der Routing- und RAS-mmc unter RAS-Richtlinien den neuen Eintrag ISA SERVER-STANDARDRICHTLINIE (siehe Abbildung 10.14).

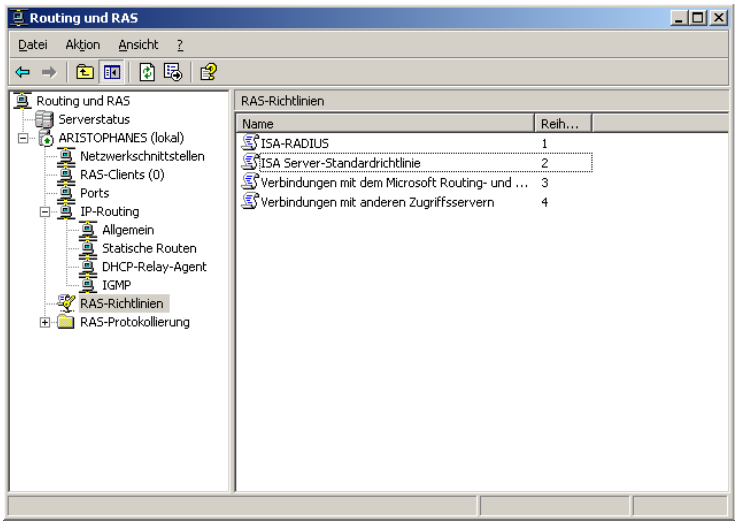


Abbildung 10.14: Die neue ISA Server-Standardrichtlinie

Einwählprofil

Wechseln Sie in die Eigenschaften dieser Richtlinie, sehen Sie, dass diese lediglich für die Benutzergruppe der VPN-Benutzer gilt. Über die Schaltfläche PROFIL BEARBEITEN können Sie noch weitere Einstellungen vornehmen wie z.B. den VPN-Zugriff auf bestimmte Zeiträume beschränken (siehe Abbildung 10.15).

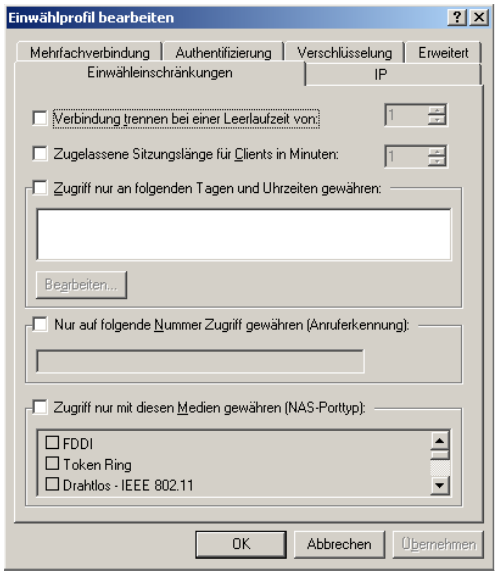


Abbildung 10.15: Weitere Konfigurationsmöglichkeiten für das Routing- und RAS-Einwählprofil

10.5 Eingehende L2TP über IPSec-Verbindungen mit NAT-T einrichten

Der ISA Server wendet NAT auf sämtliche eingehende Pakete an. Dies bedeutet, dass Sie beim Einsatz von L2TP NAT-T verwenden müssen.

NAT-T-Update der Clients

Dazu muss auf sämtlichen Clients ein NAT-T-Update installiert sein. Weitere Hinweise zu diesem Update finden Sie im Artikel 818043 der Microsoft Knowlegdebase. Zusätzlich muss der VPN-Server unter Windows Server 2003 betrieben werden.

Das Einrichten einer L2TP-Verbindung für den VPN-Zugriff gleicht in weiten Teilen dem eben beschriebenen Verfahren zur Konfiguration einer PPTP-Verbindung. Allerdings werden hier zwei Veröffentlichungsregeln benötigt. Über die erste Regel wird die IKE-Aushandlung (Internet Key Exchange) veröffentlicht, über die zweite NAT-T. In diesem Kapitel wird das Erstellen dieser beiden Regeln aufgezeigt. Die weitere Konfiguration des VPN-Servers wurde bereits in den vergangenen Kapiteln beschrieben.

NAT-T

L2TP/IPSEC hingegen bietet einen höheren Sicherheitsstandard als PPTP und funktioniert mittlerweile auch, durch NAT-T (NAT-Traversal), mit Geräten, die NAT anwenden. Hierbei ist allerdings zu beachten, dass die Router L2TP/IPSEC Passthrough unterstützen müssen.

10.5.1 Veröffentlichen der IKE-Aushandlung

Um eine Regel zur Veröffentlichung der IKE-Aushandlung zu erstellen, sind die folgenden Schritte erforderlich:

1. Klicken Sie in der ISA-mmc unter FIREWALLRICHTLINIE auf den Link NEUE SERVERVERÖFFENTLICHUNGSREGEL ERSTELLEN im Aufgabenbereich.
2. Geben Sie der Regel einen passenden Namen, z.B: *IKE veröffentlichen* und klicken Sie auf WEITER.
3. Geben Sie dann die IP-Adresse des zu veröffentlichenden Servers an und klicken Sie auf WEITER.
4. Im Fenster PROTOKOLL AUSWÄHLEN wählen Sie das Protokoll IKE-SERVER und klicken auf WEITER (siehe Abbildung 10.16).

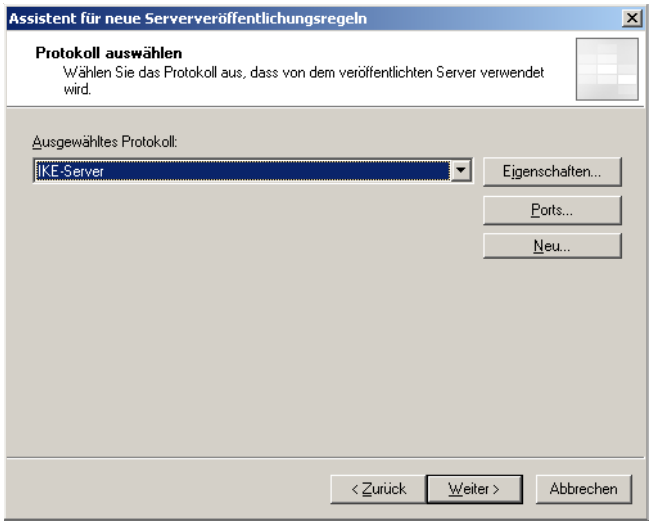


Abbildung 10.16: Auswahl des Protokolls IKE-Server

5. Unter IP-ADRESSEN wählen Sie das Netzwerk EXTERN. Klicken Sie danach auf WEITER. Beenden Sie danach den Assistenten.

Standardmäßig hört der ISA Server alle externen IP-Adressen nach VPN-Verbindungen ab. Möchten Sie lediglich eine einzelne IP-Adresse für die Abhörung verwenden, klicken Sie auf ADRESSE und wählen Sie die gewünschte IP-Adresse aus.

6. Bestätigen Sie dann die Konfigurationsänderung mit einem Klick auf ÜBERNEHMEN. Änderungen dieser Regel sind über die Eigenschaften möglich.

10.5.2 Veröffentlichen von NAT-T

Um NAT-T zu veröffentlichen, müssen Sie die folgenden Schritte durchführen:

1. Klicken Sie in der ISA-mmc unter FIREWALLRICHTLINIE auf den Link NEUE SERVERVERÖFFENTLICHUNGSREGEL ERSTELLEN im Aufgabenbereich.
2. Geben Sie der Regel einen passenden Namen, z.B: *NAT-T veröffentlichen*, und klicken Sie auf WEITER.
3. Geben Sie dann die IP-Adresse des zu veröffentlichenden Servers an und klicken Sie auf WEITER.
4. Im Fenster PROTOKOLL AUSWÄHLEN wählen Sie das Protokoll IPSEC-NAT-T-SERVER und klicken auf WEITER (siehe Abbildung 10.17).
5. Unter IP-ADRESSEN wählen Sie das Netzwerk EXTERN. Klicken Sie danach auf WEITER. Beenden Sie danach den Assistenten.

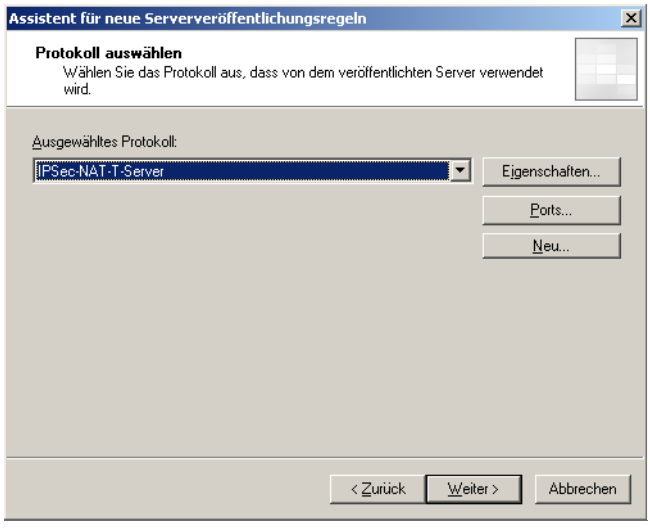


Abbildung 10.17: Auswahl des Protokoll IPSec-NAT-T-Server

Standardmäßig hört der ISA Server alle externen IP-Adressen nach VPN-Verbindungen ab. Möchten Sie lediglich eine einzelne IP-Adresse für die Abhörung verwenden, klicken Sie auf ADRESSE und wählen die gewünschte IP-Adresse aus.

6. Bestätigen Sie dann die Konfigurationsänderung mit einem Klick auf ÜBERNEHMEN. Änderungen dieser Regel sind über die Eigenschaften möglich.

10.6 Eingehende L2TP-Verbindungen einrichten

Kein NAT-T bei L2TP

Verwenden Sie L2TP ohne IPSec, muss NAT-T nicht eingesetzt werden. Das L2TP-Protokoll ohne IPSec bietet keinerlei Datenverschlüsselung. Auch für L2TP-Verbindungen muss eine Zugriffsregel erstellt werden.

Bevor Sie mit diesen Schritten beginnen, müssen Sie die L2TP über IPSec-Richtlinie deaktivieren. Weitere Hinweise dazu finden Sie im Artikel 310109 *HOW TO: Disable the Automatic L2TP/IPSec Policy* in der Microsoft Knowledgebase.

Server veröffentlichen

Um die Serververöffentlichungsregel zu erstellen, sind die folgenden Schritte erforderlich:

1. Klicken Sie in der ISA-mmc unter FIREWALLRICHTLINIE auf den Link NEUE SERVERVERÖFFENTLICHUNGSREGEL ERSTELLEN im Aufgabenbereich.
2. Geben Sie der Regel einen passenden Namen, z.B: *L2TP ohne IPSec*, und klicken Sie auf WEITER.

3. Geben Sie dann die IP-Adresse des zu veröffentlichenden Servers an und klicken Sie auf WEITER.
4. Im Fenster PROTOKOLL AUSWÄHLEN wählen Sie das Protokoll L2TP-SERVER und klicken Sie auf WEITER .
5. Unter IP-ADRESSEN wählen Sie das Netzwerk EXTERN. Klicken Sie danach auf WEITER. Beenden Sie danach den Assistenten.

Standardmäßig hört der ISA Server alle externen IP-Adressen nach VPN-Verbindungen ab. Möchten Sie lediglich eine einzelne IP-Adresse für die Abhörung verwenden, klicken Sie auf ADRESSE und wählen die gewünschte IP-Adresse aus.

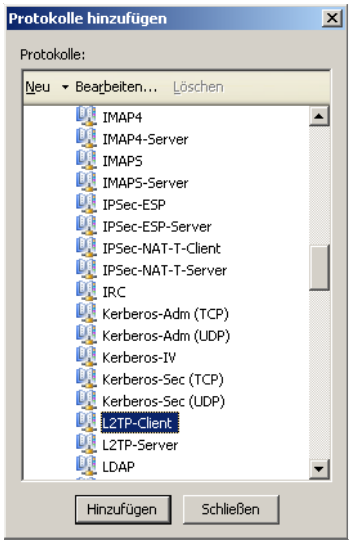
6. Bestätigen Sie dann die Konfigurationsänderung mit einem Klick auf ÜBERNEHMEN. Änderungen dieser Regel sind über die Eigenschaften möglich.

Zugriffsregel

Danach müssen Sie eine Zugriffsregel für das L2TP-Protokoll erstellen.

1. Klicken Sie in der ISA-mmc unter FIREWALLRICHTLINIE auf den Link NEUE ZUGRIFFSREGEL ERSTELLEN im Aufgabenbereich.
2. Geben Sie der Regel einen passenden Namen, z.B. *L2TP zulassen*, und klicken Sie auf WEITER.
3. Wählen Sie die Regelaktion ZULASSEN und klicken Sie auf WEITER.
4. Im Fenster PROTOKOLLE wählen Sie AUSGEWÄHLTE PROTOKOLLE und klicken auf HINZUFÜGEN. Öffnen Sie dort ALLE PROTOKOLLE und wählen Sie den Eintrag L2TP-CLIENT (siehe Abbildung 10.18).

Abbildung 10.18: Auswahl des Protokolls L2TP-Client



5. Im Fenster ZUGRIFFSREGELQUELLEN klicken Sie auf HINZUFÜGEN und wählen unter COMPUTER den L2TP-VPN-Server aus. Klicken Sie dann auf WEITER.

6. Im Fenster ZUGRIFFSREGELZIELE wählen Sie das Netzwerk EXTERN und klicken auf WEITER.
7. Unter BENUTZERSÄTZE lassen Sie den Eintrag ALLE BENUTZER unverändert. Klicken Sie auf WEITER und beenden Sie den Assistenten. Übernehmen Sie danach die Konfigurationsänderungen.

10.7 Die VPN-Clientkonfiguration

Breite Client-Unterstützung

Nachdem Sie nun die serverseitige Clientkonfiguration kennen gelernt haben, geht es daran, die Clients für den VPN-Einsatz zu konfigurieren. Dieser Vorgang wird für Windows XP/2000-Clients sowie Windows 98-Clients beschrieben. Auch für Pocket-PC-Clients kann eine VPN-Unterstützung eingerichtet werden.

10.7.1 VPN-Clients unter Windows XP und 2000

Um einen VPN-Client unter den Betriebssystemen Windows XP oder Windows 2000 einzurichten, führen Sie die folgenden Schritte aus:

1. Klicken Sie unter NETZWERKVERBINDUNGEN auf NETZWERKAUFGABEN und wählen Sie den Eintrag NEUE VERBINDUNG ERSTELLEN.
2. Auf der Seite NETZWERKVERBINDUNGSTYP (siehe Abbildung 10.19) wählen Sie VERBINDUNG MIT DEM NETZWERK AM ARBEITSPLATZ HERSTELLEN und klicken Sie auf WEITER.

Abbildung 10.19: Auswahl des Netzwerkverbindungstyps

3. Auf der Seite NETZWERKVERBINDUNG (siehe Abbildung 10.20) wählen Sie VPN-VERBINDUNG und klicken auf WEITER.

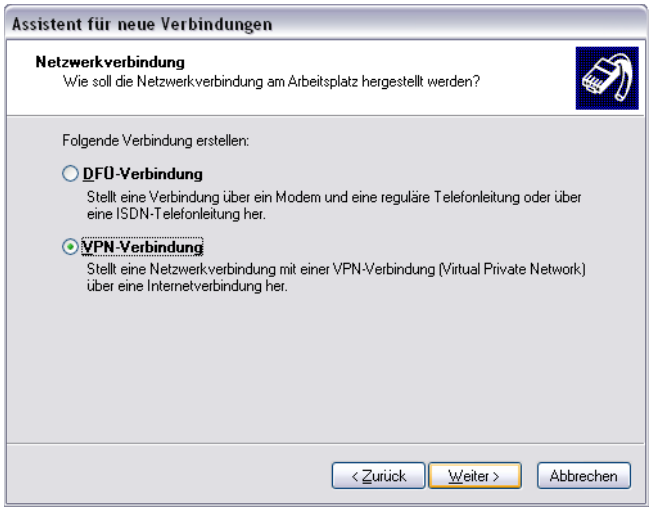


Abbildung 10.20: Auswahl der VPN-Verbindung

4. Im Fenster VERBINDUNGSNAME tragen Sie einen Namen für die VPN-Verbindung ein und klicken auf WEITER.
5. Unter ÖFFENTLICHES NETZWERK können Sie bestimmen, ob vor dem Herstellen der Verbindung eine bestimmte Internetverbindung aufgebaut werden muss. Klicken Sie dann auf WEITER.
6. Unter VPN-SERVERAUSWAHL tragen Sie entweder die IP-Adresse oder den Hostnamen des VPN-Servers ein. Klicken Sie dann auf WEITER.
7. Im Fenster VERFÜGBARKEIT DER VERBINDUNG bestimmen Sie, ob die Verbindung für ALLE BENUTZER oder nur für den aktuellen Benutzer (EIGENE VERWENDUNG) zur Verfügung stehen soll. Klicken Sie dann auf WEITER und im folgenden Fenster auf FERTIG STELLEN.

Verbindungsdetails

Um die Verbindung herzustellen, muss der Benutzer seinen Benutzernamen und das Kennwort angeben. Über den Status der Verbindungsherstellung zum Server sowie die Prüfung von Benutzernamen und Kennwort werden Sie in zwei Statusfenstern informiert. Sobald die VPN-Verbindung hergestellt ist, können Sie über das Statusfenster auf der Registerkarte DETAILS Einzelheiten zur Verbindung einsehen.

10.7.2 VPN-Clients unter Windows 98

Aufwändigere Konfiguration

Für die Konfiguration eines Windows 98-Clients ist ein wenig mehr Aufwand erforderlich als für Windows 2000 oder XP. Die Unterstützung einer L2TP-über-IPSec-Verbindung muss dem Windows 98-Client zuerst hinzugefügt werden. Führen Sie nacheinander die folgenden Schritte aus:

1. Öffnen Sie die Eigenschaften der NETZWERKUMGEBUNG und klicken dort auf HINZUFÜGEN und wählen Sie NETZWERKKARTE.
2. Im Fenster NETZWERKARTEN AUSWÄHLEN markieren Sie unter HERSTELLER den Eintrag MICROSOFT und wählen die Karte MICROSOFT VIRTUAL PRIVATE NETWORKING ADAPTER. Klicken Sie dann auf OK. Für die Installation wir u.U. die Windows 98-Installations-CD benötigt.
3. Fügen Sie dann wie eben beschrieben die Netzwerkkarte DFÜ-ADAPTER des Herstellers MICROSOFT hinzu.
4. Öffnen Sie dann ARBEITSPLATZ/DFÜ-NETZWERK. Wird das DFÜ-Netzwerk erstmalig aufgerufen, müssen Sie einige Stammdaten angeben. Dies ist auch erforderlich, wenn keine Wählverbindungen konfiguriert werden sollen. Folgen Sie für diese Erstkonfiguration den Anweisungen des Assistenten.
5. Danach wird die VPN-Verbindung eingerichtet. Wählen Sie dazu NEUE VERBINDUNG ERSTELLEN. Tragen Sie im Fenster NEUE VERBINDUNG ERSTELLEN den Namen der Verbindung ein und wählen Sie als Netzwerkkarte den MICROSOFT VPN-ADAPTER aus. Klicken Sie dann auf WEITER.
6. Geben Sie dann den Hostnamen oder die IP-Adresse des VPN-Servers an und klicken Sie auf WEITER. Schließen Sie dann die Einrichtung der Verbindung ab.
7. Öffnen Sie das Fenster DFÜ-VERBINDUNGEN, markieren Sie die VPN-Verbindung und wählen Sie das Menü VERBINDUNGEN/EINSTELLUNGEN.
8. Wechseln Sie auf die Registerkarte SICHERHEIT und markieren dort die beiden Checkboxen SENDEN VON LAN MANAGER-KENNWÖRTERN DEAKTIVIEREN und SICHERE VPN-VERBINDUNGEN ANFORDERN. Bestätigen Sie mit OK.
9. Öffnen Sie das Kontextmenü EIGENSCHAFTEN der VPN-Verbindung und wechseln Sie auf die Registerkarte SERVERTYPEN. Markieren Sie dort die folgenden Checkboxen: AM NETZWERK ANMELDEN, SOFTWAREKOMPRIMIERUNG AKTIVIEREN, VERSCHLÜSSELTES KENNWORT FORDERN sowie TCP/IP. Bestätigen Sie mit OK.
10. Danach kann die Anmeldung am VPN-Server erfolgen. Geben Sie den Benutzernamen und das Kennwort ein. Über den Status der Verbindungsherstellung werden Sie in einem Fenster informiert. Wurde die Verbindung erfolgreich hergestellt, erhalten Sie im Fenster VERBUNDEN MIT weitere Informationen zur Verbindung.

10.8 Ausgehende VPN-Verbindungen

Seltener, aber realisierbar

In aller Regel ist das Erstellen eingehender VPN-Verbindungen die weitaus weiter verbreitete Methode. Jedoch können auch ausgehende VPN-Verbindungen eingerichtet werden, wenn die Clients des internen Netzwerks VPN-Verbindungen zu einem anderen Netzwerk herstellen sollen. Je nachdem, ob Sie dazu PPTP oder L2TP verwenden, muss eine Zugriffsregel erstellt werden.

Für eine PPTP-Verbindung wählen Sie beim Erstellen der Zugriffsrichtlinie das Protokoll PPTP, bei einer L2TP-Verbindung entsprechend das Protokoll L2TP. Auch diese ausgehenden Verbindungen werden in der Überwachung angezeigt.

10.9 Standort-zu-Standort-VPN

Verbinden zweier Netzwerke

Unter einem Standort-zu-Standort-VPN versteht man die Verbindung zweier Netzwerke. Diese Verbindung kann beispielsweise über das Internet hergestellt werden. Ein häufiges Szenario für den Einsatz von Standort-zu-Standort-VPNs ist die Anbindung einer Zweigstelle an den Hauptsitz des Unternehmens oder die Verbindung von zwei Standorten des Unternehmens untereinander.

ISA Server als VPN-Gateway

In diesem Szenario befindet sich an jedem der Standorte ein ISA Server, der als VPN-Gateway fungiert. Die Verbindung zwischen den beiden Netzwerken wird über einen Tunnel zwischen den beiden Gateways hergestellt. Die Übertragung der Daten erfolgt in verschlüsselter Form.

Sobald ein Client Daten an einen Computer am anderen VPN-Standort versenden möchte, werden diese an das VPN-Gateway des Standorts geleitet, da dieses für die internen Computer als Standardgateway eingerichtet ist. Das VPN-Gateway baut den Tunnel zum Gateway des anderen VPN-Standorts auf. Dort werden die verschlüsselt eintreffenden Daten wieder entschlüsselt und an den Zielcomputer weitergeleitet. Da der Tunnel am VPN-Gateway endet, können die übertragenen Daten vom ISA Server bis hinunter zur Anwendungsebene geprüft werden, so dass ein hohes Maß an Sicherheit gewährleistet ist.

Keine besondere Konfiguration an Client und Server

Für den Einsatz solcher VPN-Tunnel ist weder am Server noch an den Clients der beiden Standorte eine besondere Konfiguration erforderlich, da der ISA Server den VPN-Standort als Remote-Standort, also als ein eigenständiges Netzwerk, behandelt. Der Zugriff auf die Ressourcen des Netzwerks kann wie bei jedem anderen Netzwerk über Zugriffsregeln gesteuert werden.

Selbstverständlich sollte auch bei Standort-zu-Standort-VPNs wie bei einem Remote-VPN grundsätzlich nur der VPN-Verkehr gestattet werden, der auch wirklich notwendig ist.

Nach der Installation des Service Pack 1 besteht bei der Konfiguration eines VPN-Standort-zu-Standort-Netzwerks die Einschränkung, dass für die Verbindung vom lokalen zum Remotestandort der Domänenname, der bei der ausgehenden Anmeldeinformation angegeben wird, nicht länger als 15 Zeichen sein darf. Für die Authentifizierung werden NetBIOS-Namen verwendet, die dieser 15 Zeichen-Regelung unterliegen.

10.9.1 Anlegen des Remote-Standorts

Eigenständiges Netzwerk

Wie bereits erwähnt, sieht der ISA Server den Remote-Standort des Standort-zu-Standort-VPNs als ein eigenständiges Netzwerk an. Dieses neue Netzwerk muss zunächst angelegt werden. Dazu sind die folgenden Schritte erforderlich:

1. Navigieren Sie in der ISA-mmc zum Eintrag VIRTUELLE PRIVATE NETZWERKE (VPN) und wechseln Sie auf die Registerkarte REMOTESTANDORTE.
2. Klicken Sie im Aufgabenbereich auf den Link REMOTESTANDORTNETZWERK HINZUFÜGEN. Ein Assistent wird gestartet.
3. Geben Sie einen passenden Namen für das Netzwerk an und klicken Sie auf WEITER.
4. Im folgenden Fenster VPN-PROTOKOLL (siehe Abbildung 10.21) wählen Sie das Protokoll, über das der VPN-Tunnel bereitgestellt werden soll. Je nach gewählter Option unterscheiden sich die folgenden Schritte.

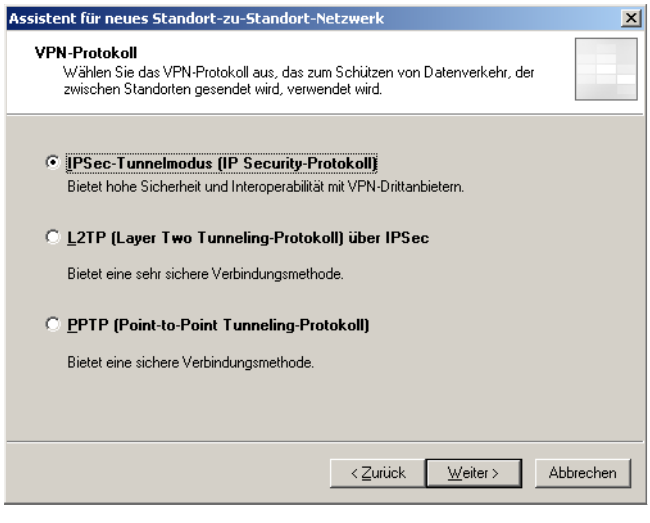


Abbildung 10.21: Auswahl des VPN-Protokolls für die Verbindung zum Remote-Standort

IPSec-Tunnelmodus

5. Haben Sie die erste Option gewählt, geben Sie im Fenster VERBINDUNGSEINSTELLUNGEN die IP-Adresse des ISA Server am Remote-Standort an. Zusätzlich geben Sie auch die lokale IP-Adresse dieses ISA Server an, zu der der VPN-Tunnel aufgebaut wird. Klicken Sie dann auf WEITER.
6. Als Nächstes wählen Sie die Authentifizierungsmethode aus. Sie können im Fenster IPSEC-AUTHENTIFIZIERUNG zwischen der Zertifikatesauthentifizierung oder der Benutzung eines vorinstallierten Schlüssels wählen. Die erste Methode ist die sicherere von beiden. Stellen Sie bei der Auswahl dieser Methode sicher, dass beide VPN-Gateways über ein IPSec-Zertifikat verfügen müssen, das von derselben Zertifizierungsstelle ausgestellt ist. Klicken Sie danach auf WEITER.
7. Geben Sie dann die IP-Adressen an, die am Remote-Standort verwendet werden sollen. Hierzu können Sie Bereiche von IP-Adressen, private Adressbereiche oder mit einem Netzwerkadapter verknüpfte Adressen hinzufügen. Klicken Sie dann auf WEITER und beenden Sie den Assistenten.

L2TP

8. Bei der Wahl von L2TP erhalten Sie zunächst ein Hinweisfenster mit den Voraussetzungen, die erfüllt sein müssen. Bestätigen Sie dieses und geben Sie im Fenster REMOTESTANDORTGATEWAY den Namen oder die IP-Adresse des VPN-Servers am Remotestandort an. Klicken Sie danach auf WEITER.
9. Im Fenster REMOTEAUTHENTIFIZIERUNG geben Sie die Informationen eines Benutzerkontos an. Auf dem Remote-Server muss sich ein Benutzerkonto befinden, das die Berechtigung zum Einwählen besitzt. Um auch dem Remote-VPN-Gateway Verbindungen zum lokalen Netzwerk zu ermöglichen, muss ein Benutzerkonto erstellt werden. Dabei muss der Benutzername für die Authentifizierung dem Namen des Remote-Standorts entsprechen. Klicken Sie danach auf WEITER.
10. Sie können dann für die gegenseitige Authentifizierung die Zertifikatsauthentifizierung (Standardeinstellung) oder einen vorinstallierten Schlüssel verwenden. Klicken Sie dann auf WEITER.
11. Zum Schluss werden die am Remote-Standort verwendeten IP-Adressen festgelegt. Klicken Sie dann auf WEITER und beenden Sie den Assistenten. Übernehmen Sie die Konfigurationsänderungen.

PPTP

Die Konfiguration ist nahezu identisch mit der Konfiguration von L2TP. Lediglich eine Computerauthentifizierung ist bei einer PPTP-Verbindung nicht notwendig.

10.9.2 Abschließende Konfiguration

Zusätzliche Konfigurationen

Nachdem Sie den neuen Remote-Standort erstellt haben, wird dieser in der Liste der Standorte angezeigt. Über die Aufgabenliste können noch vier weitere Konfigurationseinstellungen für diesen Standort vorgenommen werden.

- ZUGRIFFSNETZWERKE AUSWÄHLEN: Bestimmt die Netzwerke, von denen aus ein Remote-VPN-Gateway eine Verbindung zum ISA Server herstellen darf
- ADRESSZUWEISUNG KONFIGURIEREN: Bestimmt die IP-Konfiguration für ein Remote-VPN-Gateway
- AUTHENTIFIZIERUNGSMETHODEN AUSWÄHLEN: Hier werden ein oder mehrere Protokolle für die Authentifizierung festgelegt.
- RADIUS-KONFIGURATION ANGEBEN: Es kann ein RADIUS-Server zur Weiterleitung der Anmeldeinformationen angegeben werden.

10.9.3 Der Routing- und RAS-Dienst

Verbindungsprobleme prüfen

Kommt es bei der Herstellung der VPN-Verbindung zu Problemen, sollten Sie diese in der mmc ROUTING UND RAS überprüfen und beheben.

Unter NETZWERKSCHNITTSTELLEN wird die Schnittstelle für den Remote-Standort angezeigt. Der Status muss AKTIVIERT lauten. Um die Verbindung zu testen, rufen Sie den Kontextmenüeintrag VERBINDEN auf. Soll die Verbindung mit anderen Anmeldeinformationen hergestellt werden, so können diese über den Kontextmenüeintrag ANMELDEINFORMATIONEN FESTLEGEN modifiziert werden.

Über statische Routen wird vom Routing- und RAS-Dienst festgelegt, wann die Netzwerkschnittstelle eine Verbindung zum Wählen bei Bedarf aufbauen soll. Der Aufbau der Verbindung hängt davon ab, in welches Netzwerk die Pakete weitergeleitet werden müssen. Um das Routing zu prüfen, markieren Sie IP-ROUTING/STATISCHE ROUTEN. In der Spalte SCHNITTSTELLE ist erkennbar, dass zur Weiterleitung von IP-Paketen das Wählen bei Bedarf aktiviert wird.

10.9.4 Systemrichtlinien

Aktivierung zweier Richtlinien

Um dem ISA Server die Annahme der eingehenden VPN-Fragen zu ermöglichen, werden im Zuge der VPN-Konfiguration zwei Systemrichtlinien aktiviert. Dabei handelt es sich um die Systemrichtlinien Nummer 13 und 14 (siehe Abbildung 10.22). Über eine dieser Richtlinien wird der Verbindungsaufbau zum Remote-VPN-Gateway zugelassen, über die andere werden eingehende VPN-Verbindungen akzeptiert.

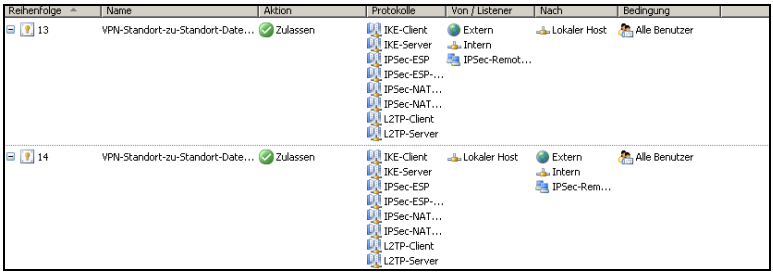


Abbildung 10.22: Aktivierung zweier zusätzlicher Systemrichtlinien

In den dynamischen Computersatz *IPSec-Remotegateways* werden automatisch alle Computerobjekte geschrieben, die durch die IP-Adresse eines Remote-VPN-Gateways klassifiziert werden. Das Hinzufügen der Objekte zu diesem Computersatz erfolgt ausschließlich anhand der Regeln und kann nicht manuell erfolgen.

10.9.5 Netzwerk- und Zugriffsregeln zur Paketweiterleitung

Damit zwischen den beiden Netzwerken des Unternehmens Pakete versendet werden können, müssen die Netzwerke *Intern* sowie das Netzwerk des Remote-Standorts miteinander verknüpft sein. Prüfen Sie dies unter KONFIGURATION/NETZWERKE auf der Registerkarte NETZWERKREGELN.

Als Letztes muss noch festgelegt werden, welche Protokolle zwischen den beiden Standorten verwendet werden dürfen. Dazu wird eine Zugriffsregel erstellt. Dabei ist eine Regel für den Datenverkehr vom Remote-Standort zur Zentrale und eine für den Verkehr von der Zentrale zum Remote-Standort anzulegen. Damit ist die Konfiguration des Remote-Standorts abgeschlossen.

10.10 VPN-Quarantäne

Funktion auch unter Windows Server 2003

Die VPN-Quarantänefunktion ist ein neues Feature des ISA Server 2004. Verfügbar ist dieses Feature jedoch schon seit der Einführung des Windows Server 2003. Über die VPN-Quarantäne ist es möglich, VPN-Clients den Zugriff auf die Netzwerkressourcen zu verwehren, wenn die Clients nicht bestimmte Richtlinien erfüllen. Diese Anforderungen kann der Administrator festlegen. Sie beziehen sich beispielsweise auf den Einsatz eines Virenscanners, einer Firewall oder Windows-Updates.

Spezielles Quarantäne-Netzwerk

Bevor ein VPN-Client Zugriff auf das interne Netzwerk erhält, wird er zunächst dem Netzwerk *Quarantänen-VPN-Clients* hinzugefügt. Die Mitglieder dieses Netzwerks verfügen über nur sehr eingeschränkte Berechtigungen, so dass sie kein Sicherheitsrisiko für das interne Netzwerk darstellen können. In der Regel darf der Zugriff auf

nur einen einzigen Server erfolgen, der die Komponenten wie z.B. Hotfixes oder Service Packs bereitstellt, die der Client zunächst installieren muss. Sobald sich ein Client in diesem speziellen Netzwerk befindet, wird dessen Konfiguration mit Hilfe eines vom Administrator definierten Skripts geprüft. Verläuft diese Überprüfung erfolgreich und hat der Benutzer zusätzlich korrekte Anmeldeinformationen eingegeben, erfolgt der Aufbau der Verbindung. Der Client gehört nun dem Netzwerk *VPN-Clients* an.

Skriptbasierte Konfigurationsprüfung des Clients

Damit ein Client die Quarantänefunktion des ISA Server unterstützen kann, muss auf diesem ein Prüfskript ablaufen können. In diesem Skript kann der Administrator beispielsweise ermitteln, ob bestimmte Hofixes installiert sind oder ob ein Virenscanner mit einer aktuellen Virendefinition vorhanden ist. Damit diese Prüfung durchgeführt werden kann, muss sich auf dem Client die Komponente *rqc.exe* befinden, die den auf dem ISA Server laufenden Dienst *rqs.exe* darüber informiert, ob der Quarantänestatus aufgehoben werden kann oder nicht.

10.10.1 Quarantänefunktion auf dem ISA Server aktivieren

Um die Quarantänefunktion auf dem ISA Server zu aktivieren, müssen Sie die folgenden Schritte durchführen:

1. Navigieren Sie in der ISA-mmc zu KONFIGURATION/NETZWERKE.
2. Auf der Registerkarte NETZWERKE rufen Sie die Eigenschaften des Netzwerks QUARANTÄNEN-VPN-CLIENTS auf.
3. Markieren Sie dort die Checkbox QUARANTÄNENSTEUERUNG AKTIVIEREN. Legen Sie zusätzlich fest, ob die Quarantänefunktion über RADIUS- oder ISA Server-Richtlinien zur Verfügung gestellt werden soll (siehe Abbildung 10.23). Die RADIUS-Funktion kann nur gewählt werden, wenn der ISA Server unter Windows Server 2003 installiert ist. Aktivieren Sie zusätzlich die Checkbox VERBINDUNG WIRD GETRENNT NACH und geben Sie einen Wert in Sekunden ein. Nach Ablauf dieser Zeit wird die VPN-Verbindung getrennt, wenn keine Verschiebung aus dem Quarantänenetzwerk heraus erfolgen kann. Sollen bestimmte Benutzer oder Gruppen von der Quarantäneregelung ausgeschlossen werden, so wählen Sie diese über HINZUFÜGEN aus.

Überlegen Sie sich, zu welchem Zeitpunkt Sie diese Einstellung vornehmen. Sobald die eben beschriebene Konfiguration durchgeführt wurde, jedoch noch nicht die komplette Quarantänekonfiguration abgeschlossen worden ist, bleiben sämtliche VPN-Clients für den angegebenen Zeitraum unter Quarantäne, bis die VPN-Verbindung wieder getrennt wird. Auch ein Client, der die Anforderungen theoretisch bereits erfüllt, erlangt noch keinen Zugriff auf den VPN-Server.

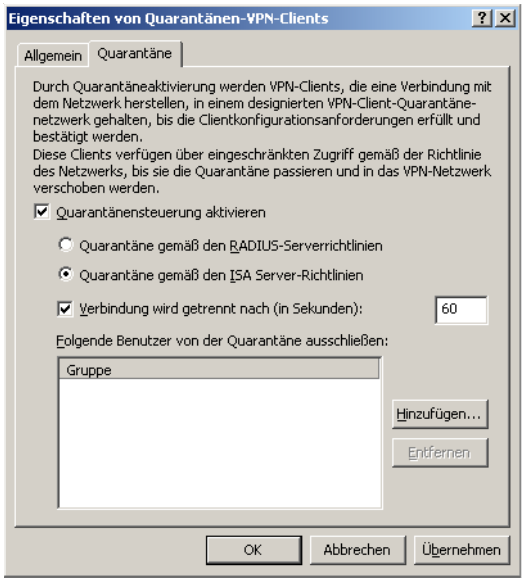


Abbildung 10.23: Konfiguration der Quarantänefunktion

10.10.2 Zugriff der Quarantäne-Clients

Server für Hotfixes u.ä.

Über eine Zugriffsregel kann festgelegt werden, ob den Quarantäne-Clients der Zugriff auf z.B. einen Server gestattet werden soll, der die erforderlichen Komponenten wie Hotfixes, Service Packs usw. für die Installation bereitstellt. Auf diese Weise wird sichergestellt, dass die Clients die korrekten erforderlichen Ressourcen installieren und sie danach vollen VPN-Zugriff besitzen können.

Erstellen Sie dazu eine Zugriffsregel, die als Zugriffsregelquelle das Quarantäne-Netzwerk und als Zugriffsregelziel den entsprechenden Server beinhaltet. Als Benutzersatz ist *Alle Benutzer* zu wählen.

10.10.3 Einrichten des RQS-Listeners

Client- und Server-Komponente

Auf dem ISA Server muss die Komponente *rqs.exe* installiert sein. Diese bildet den Listener für die Client-Komponente *rqc.exe*, die an *rqs.exe* ein Signal sendet, sobald der VPN-Client die Anforderungen für das VPN-Netzwerk erfüllt.

Beide Dateien sind Bestandteil des *Windows Server 2003 Resource Kit*. Die dort enthaltene Komponente *rqs.exe* muss jedoch für den Einsatz unter ISA Server 2004 noch aktualisiert werden.

Auf der Begleit-CD finden Sie beide Komponenten in der aktuellen Version. Es ist keine Aktualisierung mehr notwendig.

Auf dem ISA Server wird mit Hilfe des Programms *rqs.exe* ein neuer Dienst hinzugefügt. Wechseln Sie dazu an der Eingabeaufforderung in das Installationsverzeichnis des Resource Kit-Tools und geben Sie folgenden Befehl ein (siehe Abbildung 10.24):

```
Rqs_setup.bat /install ↵
```

Um den Dienst später wieder zu entfernen, fügen Sie stattdessen den Parameter `/remove` hinzu.

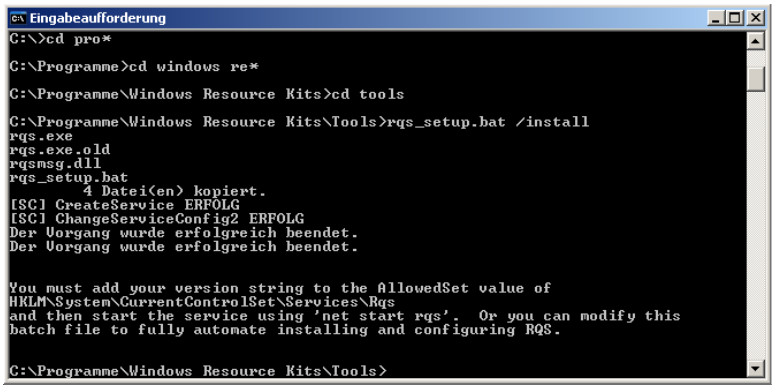


Abbildung 10.24: Installation des RQS-Dienstes

Zusätzliche Registry-Einstellungen

Sie sehen bereits anhand der Hinweismeldung, dass die Konfiguration noch nicht komplett abgeschlossen ist. Als Nächstes müssen Sie dafür sorgen, dass die auf den VPN-Clients ausgeführten Prüf-Skripte mit einer Liste erlaubter Skripte übereinstimmen. Dazu muss folgender Eintrag in der Registry vorgenommen werden: Im Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RQS` geben Sie einen neuen Wert mit dem Namen *AllowedSet* vom Typ `REG_MULTI_SZ` ein. Als Wert wird der Name des Skripts oder der Skripte angegeben.

Sobald der ISA Server von der Client-Komponente *rqc.exe* die Aufforderung erhält, den VPN-Client aus dem Quarantäne-Netzwerk zu verschieben, wird eine *.dll*-Datei aufgerufen, über die die erforderlichen Schritte aufgerufen werden. Im eben genannten Registry-Schlüssel befindet sich im Wert *Authenticator* bereits ein Eintrag für diese *.dll*-Datei. Allerdings gilt diese Version für den Windows Server 2003 und muss durch den folgenden Wert für ISA Server 2004 ersetzt werden: `C:\Programme\Microsoft ISA Server\vpnlgin.dll`.
Nach diesen beiden Änderungen am Registry-Schlüssel sollte dieser folgendermaßen aussehen (siehe Abbildung 10.25):

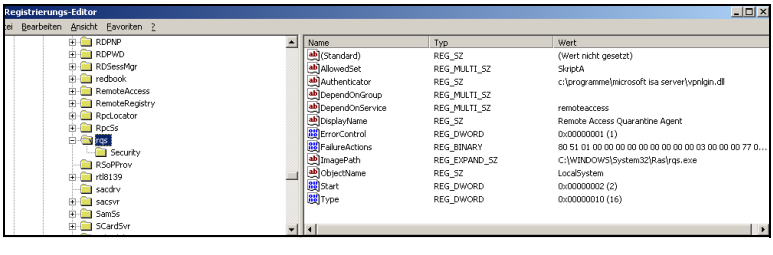


Abbildung 10.25: Die geänderten Registry-Einträge für den RQS-Dienst

Dienststart

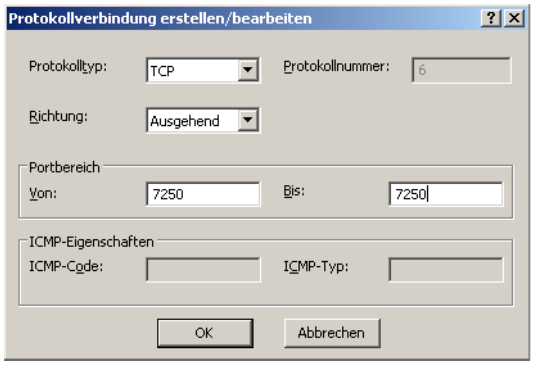
Nachdem Sie diese Änderungen vorgenommen haben, starten Sie über die mmc DIENSTE den Dienst REMOTE ACCESS QUARANTINE AGENT. An der Kommandozeile können Sie auch den Befehl `net start rqs` ↵ verwenden.

Zugriffsregel für Listener-Kommunikation

Als Nächstes wird eine neue Zugriffsregel erstellt, über die die Kommunikation zwischen den Komponenten *rqs.exe* und *rqc.exe* ermöglicht wird. Für diese Regel müssen Sie über die Toolbox zunächst ein neues Protokoll definieren. Dieses Protokoll muss die folgenden Eigenschaften besitzen (siehe Abbildung 10.26):

- NAME: RQC-Benachrichtigungen
- PROTOKOLLTYP: TCP
- RICHTUNG: Ausgehend
- PORT: 7250

Abbildung 10.26: Definition eines neuen Protokolls



Nach der Erstellung des neuen Protokolls wird eine neue Zugriffsregel angelegt. Geben Sie dieser einen Namen wie *RQC-Benachrichtigungen*, wählen die Aktion ZULASSEN und geben das eben erstellte Protokoll an. Als Zugriffsregelquelle wird das Quarantäne-Netzwerk angegeben, als Zugriffsregelziel das Netzwerk *Lokaler Host*. Als Benutzersatz wird der Satz *Alle Benutzer* ausgewählt.

10.10.4 Die Client-Skripte

Skripte zum Prüfen der Client-Konfiguration

Nachdem die Konfiguration auf Seiten des Servers abgeschlossen ist, muss nun ein Client-Skript konfiguriert werden, das die Konfiguration des VPN-Clients prüft und den Listener auf dem ISA Server benachrichtigt, ob die Quarantäne für den Client aufgehoben werden kann. Das Skript muss dazu eine der folgenden Dateiendungen besitzen:

- *.bat*
- *.cmd*
- *.exe*
- *.vbs*

Sobald das Skript auf dem Client die Konfiguration erfolgreich überprüft hat, muss dieses noch den Listener auf dem Server informieren, dass der Client die Quarantänezone verlassen darf. Dazu muss am Ende des Skripts die folgende Befehlszeile stehen:

```
Rqc.exe Verbindungsname Tunnelname TCPPort Domäne
Benutzername SkriptVersion ↵
```

Die einzelnen Parameter der Befehlszeile haben die folgenden Bedeutungen:

Tabelle 10.4: Übersicht über die Parameter von rqs.exe für die Benachrichtigung des Listeners

Parameter	Beschreibung
Verbindungs-name	Name der verwendeten Remote-Verbindung. Dieser Wert kann auch über die Variable %*DialRASEntry*% des Profils im Verbindungs-Manager ausgelesen werden.
Tunnelname	Name der Tunnelverbindung. Dieser Wert kann auch über die Variable %*TunnelRASEntry*% des Profils im Verbindungs-Manager ausgelesen werden.
TCPPort	Standardmäßig wird der Port 7250 für die Kommunikation zwischen dem VPN-Client und dem Listener benutzt.
Domäne	Gibt die Domäne des Benutzers an. Dieser Wert kann auch über die Variable %*Domain*% ausgelesen werden.
Benutzer-name	Gibt den Benutzernamen des verbundenen Benutzers an. Dieser Wert kann auch über die Variable %*User-name*% ausgelesen werden.
Skript-version	Bestimmt die Version des Skripts, damit dieses vom ISA Server als gültig angesehen werden kann.

Von Microsoft werden verschiedene Beispielskripte für die Konfiguration bereitgestellt. Sie finden diese Skripte auf der Begleit-CD im Ordner \TOOLS.

10.10.5 Der Verbindungsmanager

Verbindungs-manager-Verwaltungskit

Damit die Clients die Quarantäne-Funktion korrekt verwenden können, müssen Sie das Verbindungsmanager-Verwaltungskit einsetzen. Mit Hilfe dieses Kits können Sie beispielsweise die Installation des VPN-Clients mit den zugehörigen VPN-Verbindungen sowie weiteren Komponenten und Skripten automatisieren. Dieses Verwaltungskit muss als zusätzliche Komponente unter Windows Server 2000 und 2003 hinzugefügt werden. Führen Sie dazu die folgenden Schritte aus:

1. Klicken Sie unter SYSTEMSTEUERUNG/SOFTWARE auf WINDOWS-KOMPONENTEN HINZUFÜGEN/ENTFERNEN.
2. Klicken Sie unter VERWALTUNGS- UND ÜBERWACHUNGSPROGRAMME auf DETAILS.
3. Fügen Sie den Eintrag VERBINDUNGS-MANAGER-VERWALTUNGSKIT hinzu (siehe Abbildung 10.27).

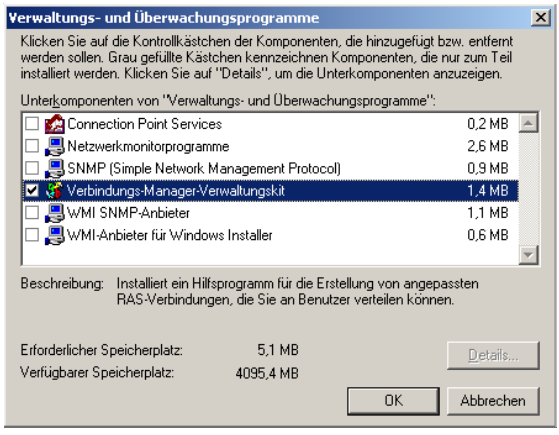


Abbildung 10.27: Hinzufügen des Verbindungsmanager-Verwaltungskits

Installationspaket erstellen

Das neue Programm wird nach der Installation über die Verwaltung aufgerufen. Ein Assistent führt Sie durch die erforderlichen Schritte zum Erstellen eines neuen Installationspakets für die VPN-Clients.

1. Im Willkommensfenster klicken Sie auf WEITER und wählen danach die Option NEUES PROFIL.
2. Geben Sie im Fenster DIENST- UND DATEINAMEN (siehe Abbildung 10.28) einen Namen für den Dienst, z.B. den der Firma, sowie den der Datei an. Klicken Sie dann auf WEITER.

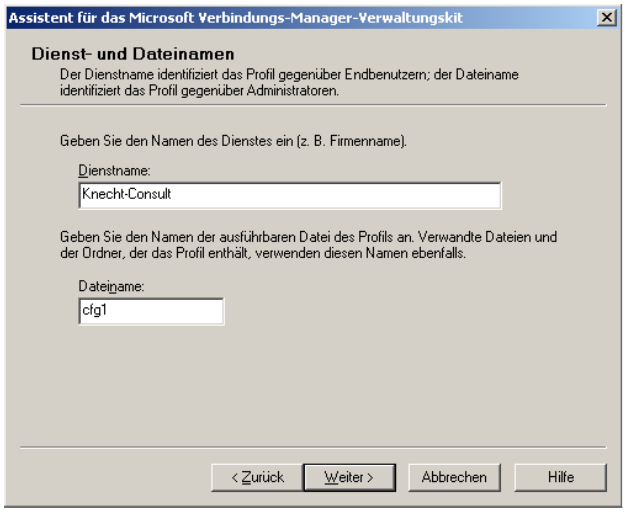


Abbildung 10.28: Angabe des Dienstnamens

3. In den beiden Fenstern BEREICHSNAME und PROFILINFORMATIONEN ZUSAMMENFÜHREN belassen Sie jeweils die Voreinstellungen.
4. Im Fenster VPN-UNTERSTÜTZUNG (siehe Abbildung 10.29) markieren Sie die Checkbox TELEFONBUCH AUS DIESEM PROFIL. Wählen Sie dazu die Option IMMER DENSELBEN VPN-SERVER VERWENDEN und tragen Sie die IP-Adresse des ISA Server ein, der ja als VPN-Gateway fungiert. Klicken Sie danach auf WEITER.

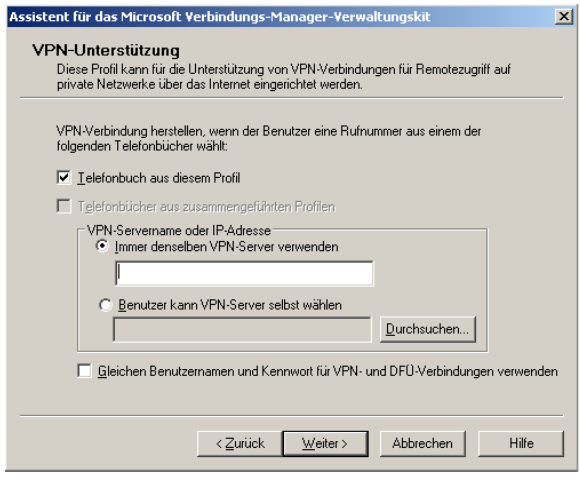


Abbildung 10.29: Auswahl des VPN-Servers

5. Als Nächstes wird im Fenster VPN-EINTRÄGE der eben erstellte Eintrag gewählt. Klicken Sie dann auf WEITER.
6. Im Fenster TELEFONBUCH deaktivieren Sie die Checkbox AUTOMATISCHER DOWNLOAD VON TELEFONBUCHUPDATES. Klicken Sie auf WEITER.
7. Unter DFÜ-NETZWERKEINTRÄGE wählen Sie den angezeigten Eintrag. Klicken Sie hier und in den beiden folgenden Fenstern auf WEITER, bis Sie das Fenster BENUTZERDEFINIERTE AKTIONEN erreicht haben. Unter AKTIONSTYP können Sie für verschiedene Stadien der Verbindung Aktionen definieren. An dieser Stelle klicken Sie auf NEU, um einen neuen Typ anzulegen.
8. Tragen Sie dazu im Fenster NEUE BENUTZERDEFINIERTE AKTION (siehe Abbildung 10.30) eine Beschreibung (z.B. VPN-Quarantäne) ein. Geben Sie Des Weiteren den Namen des Skripts und optional Parameter dazu an. Unter AKTIONSTYP wählen Sie NACH HERSTELLEN DER VERBINDUNG und als Letztes ALLE VERBINDUNGEN.

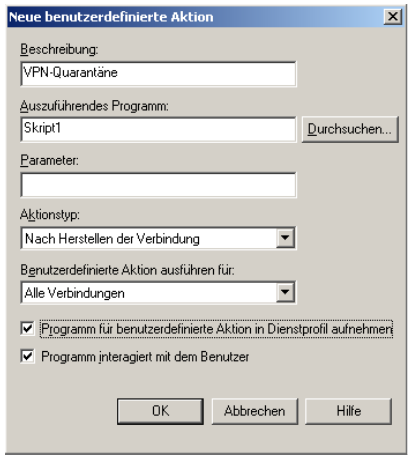


Abbildung 10.30: Erstellen einer benutzerdefinierten Aktion

9. Danach kann für die Anmeldung ein eigenes Bitmap gewählt werden. Klicken Sie nach der optionalen Auswahl auf WEITER. Dasselbe gilt auch für das Telefonbuch-Bitmap sowie die weiteren Symbole. Optional können Sie auch in den folgenden drei Fenstern Einstellungen vornehmen. Relevant ist jedoch erst wieder das Fenster VERBINDUNGS-MANAGER-SOFTWARE. Stellen Sie sicher, dass dort die Checkbox VERBINDUNGS-MANAGER-1.3-SOFTWARE MIT DIESEM DIENSTPROFIL INSTALLIEREN aktiviert ist.
10. Nehmen Sie optional Einstellungen in den letzten Fenstern vor und beenden Sie dann den Assistenten.

Nachdem das Profil erstellt wurde, wird dieses im Ordner `C:\Programme\CMAK\Profiles` gespeichert. Über die dort befindliche *.exe*-Datei werden die Konfigurationseinstellungen am VPN-Client vorgenommen.

10.10.6 Installation des Profils auf dem Client

Um das eben erstellte Profil auf dem Client zu installieren, führen Sie die folgenden Schritte aus:

1. Installieren Sie das Profil auf einem VPN-Client.
2. Stellen Sie von diesem Client aus eine VPN-Verbindung her. Dabei wird das Skript zur Prüfung der Clientkonfiguration ausgeführt. Ist die Konfiguration in Ordnung, wird der Listener informiert, dass der Client aus dem Quarantäne-Netzwerk in das Netzwerk *VPN-Clients* verschoben werden darf. Dazu muss das Skript mit einem der Skripte übereinstimmen, die auf dem ISA Server im Registry-Schlüssel *AllowedSet* aufgezählt sind. Ist dies nicht der Fall, kann die VPN-Verbindung nicht hergestellt werden.
3. Sobald die Verbindung erfolgreich hergestellt wurde, finden Sie einen entsprechenden Eintrag in der Protokollierung des ISA Server.

11 Die Cache-Funktion

Zweite Funktion des ISA Server

In allen bisherigen Kapiteln lag der Schwerpunkt auf der Firewall-Funktionalität des ISA Server. Dieses Kapitel widmet sich ausschließlich der zweiten Funktion, nämlich der Cache-Funktion des ISA Server. Über die Cache-Funktion werden von den Clients häufig angeforderte Internetinhalte in den Cache des ISA Server gespeichert und von dort aus abgerufen. Dies bedeutet für die Clients schnellere Antwortzeiten, da die Inhalte nicht erst aus dem Internet abgerufen werden müssen. Auch für eingehende Zugriffe kann die Cache-Funktion genutzt werden, so dass die veröffentlichten Webserver entlastet werden.

11.1 Die Technik des Caching

Verbesserte Techniken zur Zwischenspeicherung

Bereits seit der frühesten Version des Proxy-Servers ist in diesem die Funktion des Caching integriert. Die Techniken zur Optimierung des Caching wurden in jeder Version bis hin zum ISA Server 2004 verbessert.

Im Folgenden finden Sie eine Übersicht über die Techniken, die der ISA Server für das Caching anwendet.

Tabelle 11.1: Übersicht über die Techniken des Caching

Technik	Beschreibung
Speicherort des Cache	Die Zwischenspeicherung der Webobjekte kann sowohl auf einer Festplatte als auch im Arbeitsspeicher erfolgen. Beide Verfahren können auch miteinander kombiniert werden, so dass eine höhere Performance entsteht. Bei einer Kombination dieser beiden Methoden werden die Objekte zunächst im RAM vorgehalten und erst später auf der Festplatte gespeichert. Werden Objekte sehr häufig verwendet, können sie auch dauerhaft im Arbeitsspeicher behalten werden. Für das Vorhalten von Objekten im RAM sind standardmäßig 10 % dessen reserviert. Dieser Wert kann jedoch individuell angepasst werden. Soll ein Objekt nicht mehr im RAM behalten, sondern auf die Festplatte geschrieben werden, so geschieht dies zu einem Zeitpunkt, zu dem der ISA Server nicht stark ausgelastet ist.

Technik	Beschreibung
Cache-Datei	Werden für die Speicherung auf der Festplatte mehrere Partitionen benutzt, so wird auf jeder dieser Partitionen eine eigene Cache-Datei angelegt. Durch diese Datei wird immer die zugewiesene Dateigröße reserviert, so dass eine Fragmentierung der Inhalte möglichst verhindert wird. Damit die gecachten Objekte innerhalb der Cache-Datei schnell aufgefunden werden können, besitzt der ISA Server einen Objekt-Index, in dem alle aktuell zwischengespeicherten Objekte und ihr Speicherort verzeichnet sind.
Gültigkeitsdauer	Wenn ein Objekt im Cache gespeichert ist, bleibt es dort nur eine bestimmte Zeit gültig. Anderenfalls könnte dies dazu führen, dass bei einer zwischenzeitlichen Aktualisierung der Quell-Webseite dem Benutzer nicht das aktualisierte, sondern das veraltete Objekt angeboten wird. Ein nach dem Zeitablauf ungültiges Objekt wird nicht mehr bei einer Anfrage zurückgegeben, sondern wieder neu aus dem Internet angefordert und in den Cache geschrieben. Hierbei kommt nun die Technik des Active Caching zum Zuge. Mittels Active Caching kann der ISA Server ermitteln, welche Objekte am häufigsten angefragt worden sind, und diese bereits erneut zwischenspeichern, bevor die Gültigkeitsdauer abgelaufen ist. So sind diese Objekte zu jedem Zeitpunkt im Cache vorhanden.
Löschen nicht mehr benötigter Objekte	Sobald die maximale Größe der Cache-Datei erreicht ist, beginnt der ISA Server damit, nicht mehr benötigte Objekte zu löschen. Dabei werden zunächst ältere Objekte sowie seit Längerem nicht mehr aufgerufene Objekte gelöscht. Objekte, die regelmäßig benutzt werden, bleiben im Cache und werden nicht gelöscht, sondern lediglich durch das Active Caching aktualisiert.

11.2 Lokales Client-Caching

Verwendet ein Internetclient für den Webzugriff keinen ISA Server, so werden Objekte im lokalen Cache des Webbrowsers des Clients zwischengespeichert. Erfolgt auf einige Seiten ein besonders häufiger Zugriff, so werden die Objekte dieser Seiten direkt aus dem Cache und nicht aus dem Internet geladen. Die Seiten werden schneller aufgebaut, und zusätzlich ergibt sich eine Entlastung der Internetverbindung, was sich besonders bei geringerer Bandbreite positiv auswirkt.

Nur für den lokalen Benutzer nutzbar

Allerdings besitzt das lokale Caching die eben genannten Vorteile nur für den lokal angemeldeten Benutzer. Greift ein anderer Benutzer am selben Computer auf dieselben Objekte häufig zu, so kann dazu nicht der Cache des anderen Benutzers verwendet werden, sondern die Objekte müssen für ihn in einem zweiten Cache separat gespeichert werden. Auch für andere Netzwerkbenutzer sind die Inhalte des lokalen Cache nicht verfügbar.

11.3 ISA Server-Caching-Methoden

Wenn man von der Cache-Funktion des ISA Server spricht, müsste man streng genommen hinzufügen, welche Art des Caching gemeint ist, da dieser insgesamt fünf verschiedene Arten des Caching unterstützt.

Für alle ISA Server-Clients nutzbar

Beim ISA Server-Caching erfolgt die Speicherung der Objekte nicht wie beim lokalen Caching im Zwischenspeicher des Webbrowsers, sondern in einem zentralen Speicher der Festplatte und des RAMs. Durch diese zentrale Speicherung können sämtliche Benutzer, die ihre Internetverbindung über den ISA Server herstellen (also alle Webproxy-Clients), auf die dort gespeicherten Objekte zugreifen, was wiederum kürzere Antwortzeiten auf ihre Anfragen zur Folge hat. Außer den Webproxy-Clients ermöglicht der ISA Server über seinen Webproxy-Filter auch den Firewall- und SecureNAT-Clients den Zugriff auf den zentralen Cache, da dieser Filter die Anfragen dieser beiden Clienttypen abgreift.

Separat von der Firewall-Funktion betreibbar

Die Cache-Funktion des ISA Server kann auch entkoppelt von dessen Firewall-Funktion eingesetzt werden. In diesem Szenario muss der ISA Server lediglich über eine einzige Netzwerkkarte verfügen und wird in das interne Netzwerk platziert. Beim gleichzeitigen Einsatz als Firewall- und Cache-Server muss der ISA Server über zwei Netzwerkkarten verfügen. Bei diesem Verfahren wendet der ISA Server das Forward-Caching an, wodurch die Zugriffszeiten für die Internetclients bei Webzugriffen verkürzt werden. Alternativ kann der ISA Server auch zum Reverse-Caching eingesetzt werden. Dabei arbeitet er umgekehrt zum Forward-Caching, so dass für externe Clients die Zugriffszeiten auf die internen veröffentlichten Server verkürzt werden und diese Server zudem entlastet werden.

In den folgenden Kapiteln werden die fünf möglichen Arten des ISA Server-Caching detailliert vorgestellt.

11.3.1 Forward-Caching

Die wohl häufigste Methode

Das Forward-Caching dürfte wohl die am häufigsten eingesetzte Form der Zwischenspeicherung sein. Hierbei werden die folgenden Schritte durchlaufen:

1. Das Forward-Caching wird automatisch angewendet (natürlich nur, sofern es konfiguriert ist), sobald ein Internet-Client eine http-, https- oder auch ftp-Verbindung zu einem beliebigen Server im Internet aufbauen möchte.
2. Die entsprechende Anfrage des Clients wird vom ISA Server zunächst beendet und nicht an den Webserver weitergeleitet. Bei dieser Unterbrechung schaut der ISA Server nach, ob sich die angeforderten Objekte in seinem Cache befinden.
3. Sollte dies nicht der Fall sein, fordert der ISA Server im Auftrag des Clients die gewünschten Objekte beim Webserver an.
4. Der Webserver sendet die vom ISA Server angeforderten Objekte an diesen zurück.
5. Die vom Webserver gesendeten Objekte werden vom ISA Server in seinen Cache geschrieben.
6. Der ISA Server sendet die gewünschten Objekte an den anfragenden Client. Auch wenn in Schritt 2 festgestellt wird, dass sich die angeforderten Objekte bereits im Cache befinden, werden diese von dort an den Client zurückgegeben, ohne dass die in den Schritten 3 bis 5 beschriebene Anforderung vom Webserver stattfindet.

Die einzelnen Schritte werden in dem folgenden Schaubild (Abbildung 11.1) verdeutlicht:

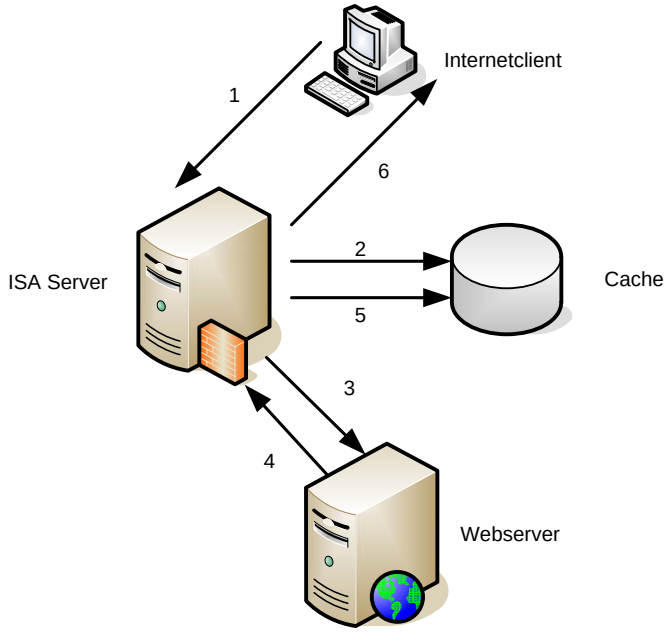


Abbildung 11.1: Schematischer Ablauf des Forward-Caching

11.3.2 Reverse-Caching

Forward-Caching in umgekehrter Richtung

Das Reverse-Caching bildet quasi das Gegenstück zum Forward-Caching und wird verwendet, um für externe Clients den Zugriff auf interne veröffentlichte Server zu beschleunigen und diese gleichzeitig zu entlasten. Die einzelnen Schritte des Reverse-Caching ähneln denen des Forward-Caching.

1. Das Reverse-Caching wird automatisch angewendet (natürlich nur, sofern es konfiguriert ist), sobald ein externer Client eine http-, https- oder auch ftp-Verbindung zu einem veröffentlichten Server im Unternehmensnetzwerk aufbauen möchte.
2. Die entsprechende Anfrage des Clients wird vom ISA Server zunächst beendet und nicht an den internen Server weitergeleitet. Bei dieser Unterbrechung schaut der ISA Server nach, ob sich die angeforderten Objekte in seinem Cache befinden.
3. Sollte dies nicht der Fall sein, fordert der ISA Server im Auftrag des Clients die gewünschten Objekte beim internen Server an.
4. Der interne Server sendet die vom ISA Server angeforderten Objekte an diesen zurück.
5. Die vom internen Server gesendeten Objekte werden vom ISA Server in seinen Cache geschrieben.
6. Der ISA Server sendet die gewünschten Objekte an den anfragenden externen Client. Auch wenn in Schritt 2 festgestellt wird, dass sich die angeforderten Objekte bereits im Cache befinden, werden diese von dort an den Client zurückgegeben, ohne dass die in den Schritten 3 bis 5 beschriebene Anforderung vom internen Server stattfindet.

Die einzelnen Schritte des Reverse-Caching werden in Abbildung 11.2 dargestellt.

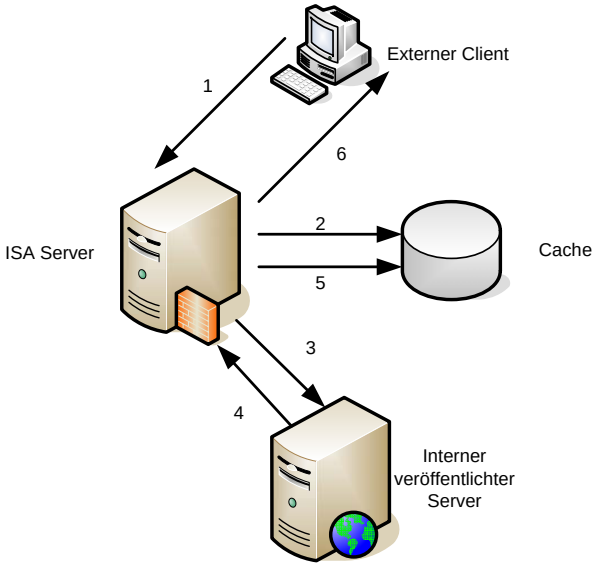


Abbildung 11.2: Schematischer Ablauf des Reverse-Caching

11.3.3 Hierarchisches Caching

Nur bei mehreren ISA Servern anwendbar

Das hierarchische Caching kann nur angewendet werden, wenn sich mehrere ISA Server im Unternehmen befinden. In diesem Fall kann ein ISA Server, der die Anfrage nicht aus seinem eigenen Cache heraus beantworten kann, die Anfrage an den Cache eines anderen ISA Server weiterleiten. Dieser zweite ISA Server wird auch als Upstreamserver bezeichnet. Bei dieser Art des Caching werden die folgenden Schritte durchlaufen:

1. Das hierarchische Caching wird automatisch angewendet (natürlich nur, sofern es konfiguriert ist und entsprechend mehrere ISA Server vorhanden sind), sobald ein Client eine http-, https- oder auch ftp-Verbindung zu einem beliebigen Server im Internet aufbauen möchte.
2. Die entsprechende Anfrage des Clients wird vom ersten ISA Server zunächst beendet und nicht an den Webserver weitergeleitet. Bei dieser Unterbrechung schaut der ISA Server nach, ob sich die angeforderten Objekte in seinem Cache befinden.
3. Befinden sich dort nicht die angeforderten Objekte, so leitet der ISA Server die Anfrage an den Upstreamserver weiter.
4. Auch dieser schaut nach, ob sich die Objekte in seinem Cache befinden.
5. Sollte dies nicht der Fall sein, fordert der Upstreamserver im Auftrag die gewünschten Objekte beim Webserver an.
6. Der Webserver sendet die vom Upstreamserver angeforderten Objekte an den ISA Server zurück.
7. Die vom Webserver gesendeten Objekte werden vom Upstreamserver in seinen Cache geschrieben.
8. Der Upstreamserver sendet die Objekte an den ISA Server weiter.
9. Auch der erste ISA Server schreibt die Objekte in seinen Cache.
10. Der ISA Server sendet die gewünschten Objekte an den anfragenden Client. Befindet sich ein Objekt bereits zuvor im Cache der einen der beiden Server, so werden von dort aus die Objekte an den Client zurückgesendet.

Die Abbildung 11.3 zeigt den Ablauf des hierarchischen Caching.

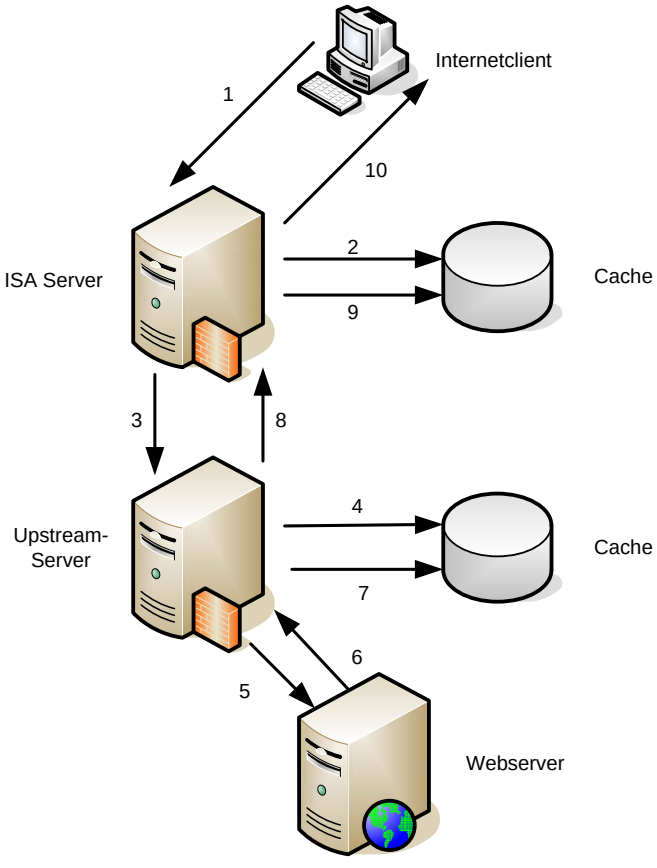


Abbildung 11.3: Der schematische Ablauf des hierarchischen Caching

11.3.4 Verteiltes Caching

Nur in der Enterprise-Version anwendbar

Das verteilte Caching kann nur angewendet werden, wenn sich mehrere ISA Server in einem Array befinden. Es ist jedoch nur möglich, ISA Server der Enterprise-, nicht der Standardversion in einem Array zu installieren.

Der Unterschied zum hierarchischen Caching besteht darin, dass beim verteilten Caching nicht mehrere Server jeweils einen einzelnen Cache besitzen, in dem dasselbe Objekt vorgehalten wird, sondern das Array über einen gemeinsamen Cache aller darin enthaltenen ISA Server verfügt. Ein Objekt wird beim verteilten Caching nur einmal im zentralen Array-Cache gespeichert.

Beim verteilten Caching werden die folgenden Schritte durchgeführt:

1. Das verteilte Caching wird automatisch angewendet (natürlich nur, sofern es konfiguriert ist), sobald ein Internet-Client eine http-, https- oder auch ftp-Verbindung zu einem beliebigen Server im Internet aufbauen möchte.

2. Die entsprechende Anfrage des Clients wird von einem ISA Server des Arrays zunächst beendet und nicht an den Webserver weitergeleitet. Bei dieser Unterbrechung schaut der ISA Server nach, ob sich die angeforderten Objekte im Cache des Arrays befinden.
3. Sollte dies nicht der Fall sein, fordert der ISA Server im Auftrag des Clients die gewünschten Objekte beim Webserver an.
4. Der Webserver sendet die vom ISA Server angeforderten Objekte an diesen zurück.
5. Die vom Webserver gesendeten Objekte werden vom ISA Server in den Cache des Arrays geschrieben.
6. Der ISA Server sendet die gewünschten Objekte an den anfragenden Client. Auch wenn in Schritt 2 festgestellt wird, dass sich die angeforderten Objekte bereits im Cache befinden, werden diese von dort an den Client zurückgegeben, ohne dass die in den Schritten 3 bis 5 beschriebene Anforderung vom Webserver stattfindet.

Abbildung 11.4 zeigt den Ablauf des verteilten Caching.

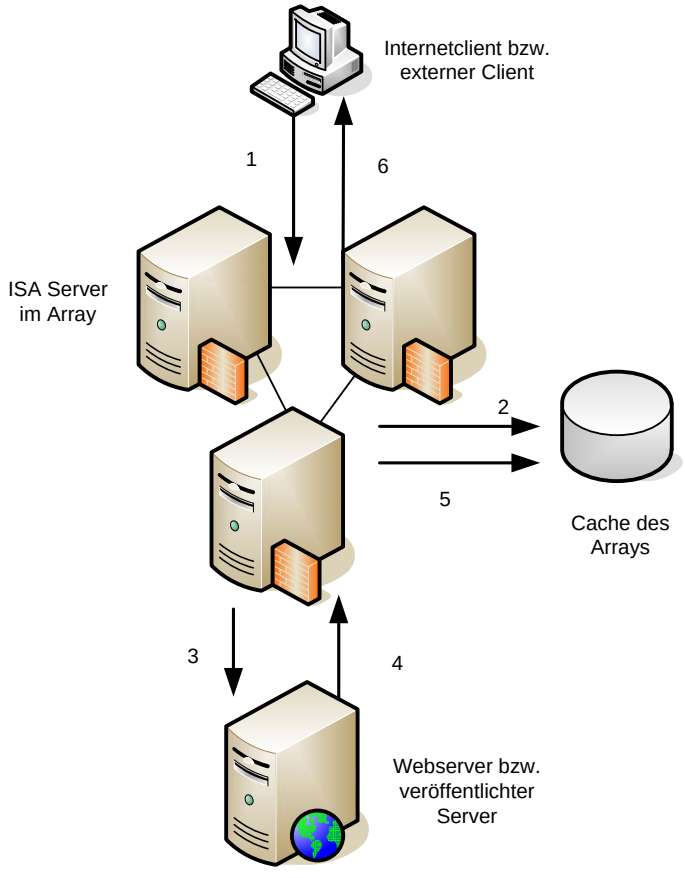


Abbildung 11.4: Der schematische Ablauf des verteilten Caching

11.3.5 Automatische Downloadaufträge von Inhalten

Diese Form des Caching ist keine Funktion, die wie die anderen vier vom jeweils anfordernden Client aus angestoßen wird, sondern eine, die zuvor vom Administrator explizit konfiguriert wird, damit die Funktion später den Clients zur Verfügung steht.

Inhaltsdownload häufig besuchter Webseiten anhand von Zeitplänen

Diese Methode sollte angewendet werden, wenn es bestimmte Webseiten gibt, die von den Clients regelmäßig aufgerufen werden. Es ist möglich, dass die kompletten Inhalte dieser Seiten automatisch in den Cache des ISA Server geladen werden. Damit dort immer die aktuellen Informationen der Webseite vorliegen, können Zeitpläne erstellt werden, nach denen die Inhalte automatisch von den erforderlichen Webseiten in den Cache des ISA Server geladen werden. Diese Funktion ist auch umgekehrt möglich, so dass die Inhalte von veröffentlichten internen Servern komplett in den Cache geladen werden.

11.4 Cache-Konfiguration

Nach diesen theoretischen Vorbetrachtungen wird nun beschrieben, wie in der Praxis der Cache konfiguriert wird. Dazu zählen das Festlegen des Cache-Laufwerks, das Anlegen von Cache-Regeln oder die Einrichtung des Active Caching.

11.4.1 Bestimmen der Cache-Laufwerke

Wie Sie bereits gelesen haben, werden die Objekte nicht nur im Arbeitsspeicher, sondern auch auf einer oder mehreren Festplatten bzw. Partitionen gespeichert. Damit dort Objekte zwischengespeichert werden können, müssen zwei Voraussetzungen erfüllt sein:

- Es muss sich um ein lokales Laufwerk handeln, ein Netzlaufwerk kann nicht benutzt werden.
- Die Partition muss mit dem Dateisystem NTFS formatiert sein.

Um eine höhere Performance zu erzielen, sollten auch nicht die Partitionen gewählt werden, auf denen sich das Betriebssystem und die Auslagerungsdatei befinden. Dies ist jedoch nur ein Hinweis, die Einrichtung auf diesen beiden Partitionen ist technisch möglich.

Optimale Größe der Cache-Datei ist von verschiedenen Faktoren abhängig

Es ist schwierig, als Anhaltspunkt, wie groß die Cache-Datei ausfallen soll, einen Wert anzugeben. Auch Microsoft verzichtet seit der Version des ISA Server 2004 bewusst auf die Angabe. Bestand für den ersten Proxy-Server noch die Empfehlung von 100 MB fester Größe sowie

zusätzlich 0,5 MB pro internem Benutzer, so würde diese Größe heute keinesfalls mehr ausreichen, da sich in der Zwischenzeit die Dimensionen des Internets entscheidend verändert haben. Zudem ist der benötigte Wert abhängig von den Surfgewohnheiten und dem Umfang der besuchten Seiten. So kann es leicht notwendig werden, dass ein deutlich performanteres Arbeiten der Benutzer erst spürbar wird, wenn pro Benutzer 30 oder 40 MB Cache-Speicher bereitgestellt wurden.

Um das Cache-Laufwerk einzurichten, führen Sie die folgenden Schritte durch:

1. Navigieren Sie in der ISA-mmc zum Eintrag KONFIGURATION/CACHE und wählen CACHELAUFWERKE DEFINIEREN.
2. Im Fenster CACHELAUFWERKE FESTLEGEN (siehe Abbildung 11.5) markieren Sie die gewünschte Partition und tragen in MB die gewünschte Größe ein. Klicken Sie auf FESTLEGEN, um die Einstellung zu übernehmen. Klicken Sie dann auf OK.

Selbstverständlich können Sie hier auch mehrere Partitionen auswählen und darauf in jeweils unterschiedlicher Größe eine Cache-Datei erstellen. Eine Spaltung in mehrere Cache-Dateien wird auch notwendig, wenn die Maximalgröße von 64 GB für eine Cache-Datei nicht ausreicht. In diesem Fall müssen Sie auf einer zweiten oder gegebenenfalls weiteren Partitionen weitere Cache-Dateien anlegen.

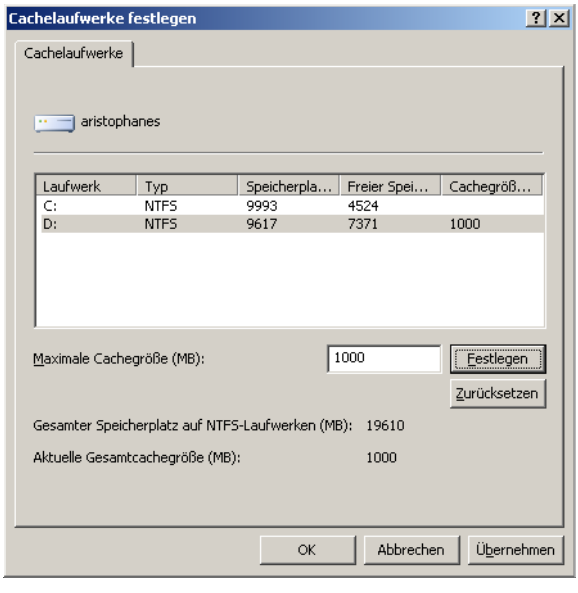


Abbildung 11.5: Auswahl der Partitionen für den Cache

3. Damit der ISA Server diese Änderung übernehmen kann, klicken Sie auf ÜBERNEHMEN und wählen die Option ÄNDERUNGEN SPEICHERN UND DIENSTE NEU STARTEN.

Ordner mit einer Datei

Durch das Anlegen der Cache-Datei wird auf der jeweiligen Partition ein Ordner Namens \URLCACHE in der festgelegten Größe erstellt. In diesem befindet sich eine Datei namens *dir1.cdat* (siehe Abbildung 11.6).

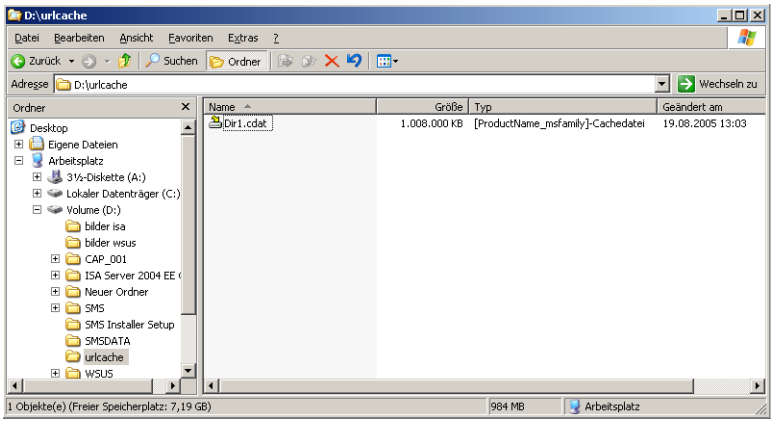


Abbildung 11.6: Der Inhalt des Cache-Ordners

11.4.2 Festlegen von Cache-Regeln

Eine Standardregel ist vorhanden

Sobald mindestens ein Cache-Laufwerk bestimmt worden ist, existiert automatisch eine standardmäßige Cache-Regel, über die das Cachen der Objekte geregelt wird. Über diese Regel werden alle http- und ftp-Objekte aus den unterschiedlichen Netzwerken des Forward- und Reward-Caching in den Zwischenspeicher geschrieben. Um die Zwischenspeicherung jedoch besser gestalten zu können, sollten Sie eigene angepasste Cache-Regeln bestimmen. Dazu sind die folgenden Schritte erforderlich:

1. Navigieren Sie in der ISA-mmc zum Eintrag KONFIGURATION/CACHE und wählen Sie CACHEREGEL ERSTELLEN über das Menü des Aufgabenbereichs. Ein Assistent wird gestartet.
2. Geben Sie der Regel einen passenden Namen und klicken Sie auf WEITER.
3. Im Fenster CACHEREGELZIEL (siehe Abbildung 11.7) bestimmen Sie die Netzwerke, URL-Sätze usw., für deren Anforderungen die Regel gelten soll. Soll das Forward-Caching eingesetzt werden, wählen Sie typischerweise das Netzwerk *Extern* aus. Klicken Sie danach auf WEITER.

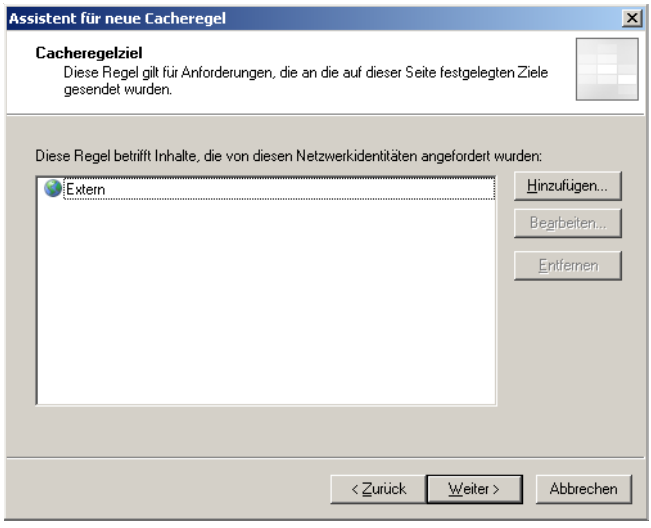


Abbildung 11.7: Auswahl des Ziels, für das die Cache-Regel gelten soll

4. Als Nächstes wird die Versionierung für die an den Benutzer aus dem Cache zurückzugebenden Objekte bestimmt. Hierzu gibt es im Fenster INHALTSABRUF (siehe Abbildung 11.8) die drei folgenden Optionen:

- NUR WENN EINE GÜLTIGE VERSION DES OBJEKTS IM CACHE VORHANDEN IST. ANFORDERUNGEN AN DEN SERVER WEITERLEITEN, FALLS KEINE VORHANDEN IST: Befindet sich im Cache ein gültiges Objekt, dessen Gültigkeitsdauer noch nicht abgelaufen ist, so wird dieses an den Benutzer gegeben. Befindet sich kein oder nur ein ungültiges Objekt im Cache, so wird das Objekt vom ISA Server neu aus dem Internet angefordert und danach im Cache gespeichert.
- FALLS IRGENDEINE VERSION DES OBJEKTS IM CACHE VORHANDEN IST. ANFORDERUNG AN DEN SERVER WEITERLEITEN, FALLS KEINE VORHANDEN IST: Sofern das Objekt im Cache vorhanden ist, wird es unabhängig von seiner Version an den Benutzer gesendet. Dabei ist es möglich, dass der Benutzer eine nicht mehr aktuelle Version des Objekts erhält. Nur nicht vorhandene Objekte werden direkt angefordert.
- FALLS IRGEDEINE VERSION DES OBJEKTS IM CACHE VORHANDEN IST. ANFORDERUNG VERWERFEN, FALLS KEINE VORHANDEN IST: Sofern das Objekt im Cache vorhanden ist, wird es unabhängig von seiner Version an den Benutzer gesendet. Dabei ist es möglich, dass der Benutzer eine nicht mehr aktuelle Version des Objekts erhält. Ist ein Objekt nicht im Cache vorhanden, wird dieses auch nicht vom ISA Server angefordert. Dies kann jedoch dazu führen, dass bestimmte Teile oder sogar komplette Webseiten dem Benutzer nicht angezeigt werden.

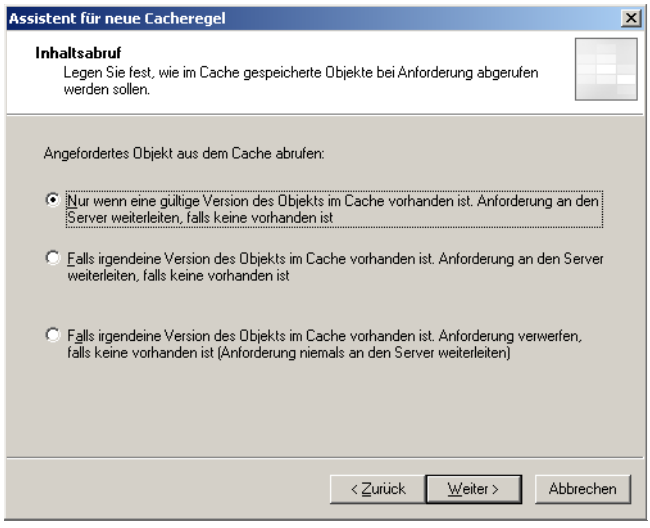


Abbildung 11.8: Festlegen von Versionszuständen für die Zwischenspeicherung

5. Im Fenster CACHEINHALT (siehe Abbildung 11.9) wird festgelegt, ob und wenn ja, welche Inhalte zwischengespeichert werden sollen. Mit der Option NIEMALS, KEIN INHALT WIRD ZWISCHENGESPEICHERT wird vom Ziel kein Objekt zwischengespeichert. Diese Option ist nur sinnvoll, wenn sie für eine Ausnahmeregel verwendet werden soll, die z.B. für bestimmte URL-Sätze kein Caching zulässt. Das Caching wird über die Option FALLS QUELL- UND ANFORDERUNGSHEADER ZWISCHENSPEICHERN INDIZIEREN aktiviert. Für die genaue Art des Caching können Sie zwischen den drei zusätzlichen folgenden Einstellungen wählen:

Keine Zwischenspeicherung für Ausnahmeregeln

- DYNAMISCHEN INHALT: Bei dynamischen Inhalten handelt es sich um Objekte, die nur eine geringe Gültigkeitsdauer besitzen und schnell veraltet sind. Über diese Option können derartige Objekte dennoch gecacht werden.
- INHALT FÜR OFFLINEBROWSING (302, 307 ANTWORTEN): Sofern eine Webseite vorübergehend umgeleitet wird (z.B. während einer umfangreichen Aktualisierung oder Wartung), wird die Seite vollständig angezeigt und der Webbrowser gleichzeitig angewiesen, beim nächsten Verbindungsaufbau wieder auf die ursprüngliche Adresse und nicht die umgeleitete Adresse zuzugreifen. Ist diese Option aktiviert, werden auch die Webobjekte, die nur vorübergehend umgeleitet sind, in den Zwischenspeicher des ISA Server geschrieben.
- INHALT, DER BENUTZERAUTHENTIFIZIERUNG FÜR DEN ABRUF ERFORDERT: Ist diese Option aktiviert, werden auch alle Objekte aus geschützten Bereichen einer Webseite zwischengespeichert, auf die die Benutzer nur nach einer gültigen Authentifizierung Zugriff besitzen.

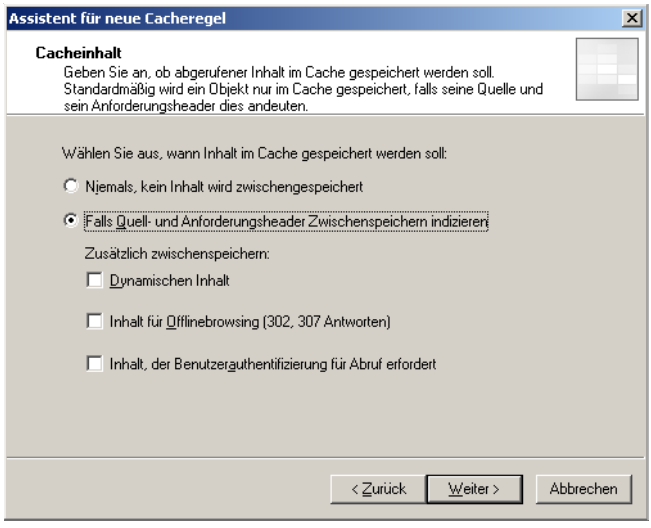


Abbildung 11.9: Bestimmen der Objekte, die zwischengespeichert werden sollen

6. Im folgenden Fenster ERWEITERTE CACHEKONFIGURATION (siehe Abbildung 11.10) bestimmen Sie, wie groß ein Objekt maximal sein darf, das in den Cache geladen werden kann. Ist ein Objekt größer als der angegebene Wert, wird dieses nicht in den Cache geschrieben. Sollen auch Objekte von SSL-basierten Webseiten zwischengespeichert werden, so wählen Sie die Option SSL-ANTWORTEN ZWISCHENSPEICHERN. Klicken Sie dann auf WEITER.

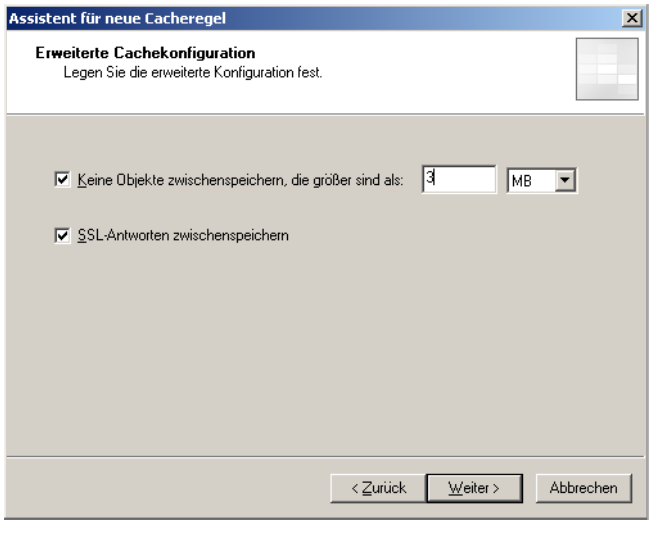


Abbildung 11.10: Objekte, die größer als der festgelegte Wert sind, werden nicht gecacht

Gültigkeitsdauer von Objekten

7. Danach wird die Gültigkeitsdauer (TTL, Time to live) der zwischengespeicherten Objekte im Cache festgelegt (siehe Abbildung 11.11). Ist die Checkbox HTTP-ZWISCHENSPEICHERUNG AKTIVIEREN nicht markiert, kann auch kein Caching stattfinden. Nur wenn diese Option gesetzt ist, können die folgenden Einstellungen getroffen werden:

- GÜLTIGKEITSDAUER DER OBJEKTE FESTLEGEN (PROZENTSATZ DES INHALTSALTERS): Das Inhaltsalter wird berechnet, indem der Zeitraum von der Erstellung bzw. letzten Änderung des Webobjekts bis hin zum Zeitpunkt der Anforderung berechnet wird. Angenommen, ein Webobjekt wurde das letzte Mal vor fünf Tagen modifiziert und als Wert sind 20 % gesetzt, so ergibt sich eine Gültigkeitsdauer von vier Tagen. Erfolgte die Modifikation vor zehn Tagen bei einem gesetzten Wert von 20 %, so resultiert daraus eine Gültigkeitsdauer von zwei Tagen. Wird vom Quellserver eine Gültigkeitsdauer des Webobjekts bestimmt, so gilt stattdessen diese.
- NICHT WENIGER BZW. MEHR ALS: Da sich anhand der Inhaltsdauer teilweise sehr kurze oder auch sehr lange Intervalle für die Gültigkeitsdauer ergeben, können zusätzlich minimale und maximale Grenzwerte für die Gültigkeit bestimmt werden.
- GÜLTIGKEITSDAUER-GRENZWERTE AUCH AUF QUELLEN ANWENDEN, DIE EINE ABLAUFZEIT FESTLEGEN: Wird für Webobjekte die Gültigkeitsdauer vom Webserver bestimmt, so lässt sich über diese Option diese Dauer stattdessen auf die konfigurierten Werte umsetzen.

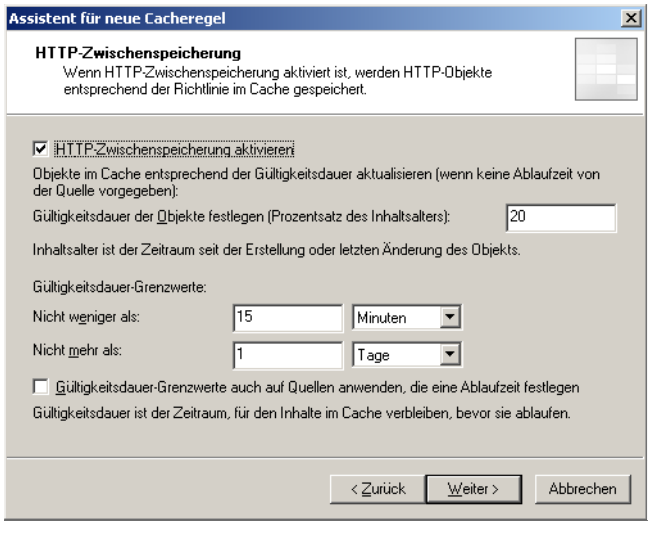


Abbildung 11.11: Bestimmen der Gültigkeitsdauer für zwischengespeicherte Objekte

8. Als Letztes kann im Fenster FTP-ZWISCHENSPEICHERUNG (siehe Abbildung 11.12) auch für FTP das Caching generell aktiviert und eine Gültigkeitsdauer für FTP-Objekte festgelegt werden. Klicken Sie dann auf WEITER und schließen Sie den Assistenten ab. Mit ÜBERNEHMEN wird die neue Cache-Regel in die ISA-Konfiguration eingepflegt.

Separate FTP-Option

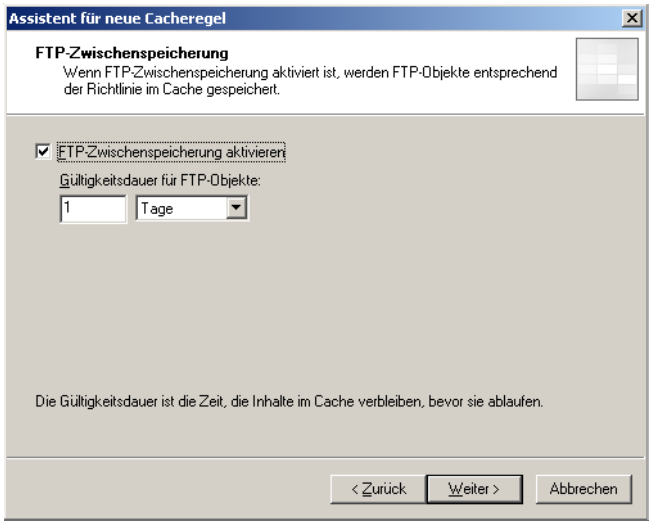


Abbildung 11.12: Optional können auch FTP-Objekte zwischengespeichert werden

Reihenfolge mehrerer Regeln

Auch Cache-Regeln werden wie die anderen Regeln des ISA Server in der Reihenfolge ausgeführt, in der sie in der Liste der Regeln angegeben sind. Diese Reihenfolge kann in der gleichnamigen Spalte geändert werden. Des Weiteren kann die Regel über ihre Eigenschaften weiter bearbeitet werden. Auch hierbei ist als zusätzliche Option das Einrichten von Ausnahmen verfügbar, für die die Regel nicht angewendet werden soll, z.B. für bestimmte URL-Sätze. Für die unter AUSNAHMEN (siehe Abbildung 11.13) gewählten Ziele wird die Zwischenspeicherung nicht verwendet. Diese Einstellung erfolgt über die Registerkarte NACH.

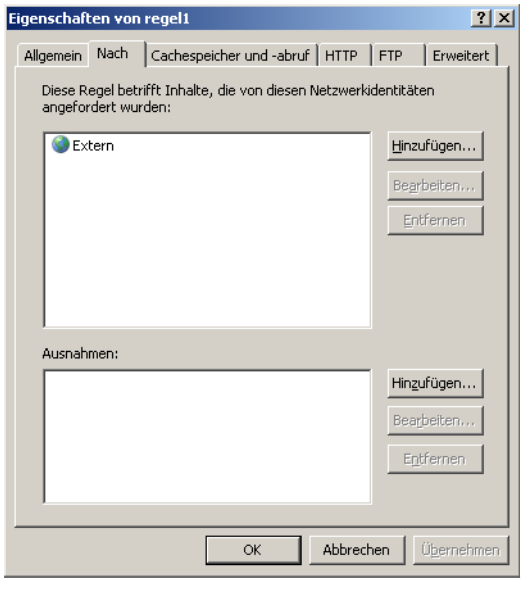


Abbildung 11.13: Für das Ziel der Regel können Ausnahmen definiert werden, für die keine Objekte zwischengespeichert werden sollen

11.4.3 Cache-Regeln importieren und exportieren

Die erstellten Cache-Regeln können unabhängig von weiteren Konfigurationseinstellungen separat importiert und exportiert werden. Auch diese Regeln werden in Form einer *.xml*-Datei exportiert und importiert. Klicken Sie dazu auf den Link CACHEREGELN EXPORTIEREN oder CACHEREGELN IMPORTIEREN im Aufgabenbereich der markierten Cache-Regel und geben Sie den Namen und Speicherort der Datei an. Optional kann auch eine Verschlüsselung beim Export erfolgen. Dabei muss ein Kennwort angegeben werden, das beim Import wiederum einzugeben ist.

11.5 Einrichten des Active Caching

Überwachung der gecachten Objekte und deren eigenständige Aktualisierung

Das Active Caching ist für die Überwachung der im Cache gespeicherten Webobjekte zuständig. So wird einerseits anhand der festgelegten Gültigkeitsdauer geprüft, ob ein Objekt noch gültig ist, bevor dies an den Benutzer zurückgegeben wird, andererseits wird ermittelt, welche Objekte besonders häufig aus dem Cache aufgerufen werden. Für diese Objekte ist eine ständige Aktualität notwendig. Solche häufig benötigten Objekte können über das Active Caching schon vor Ablauf der Gültigkeitsdauer automatisch vom Webserver downgeloadet und wieder in den Zwischenspeicher geschrieben werden. Auf diese Weise ist sichergestellt, dass die Objekte immer im Cache vorliegen und die Benutzer diese nicht erst vom Server aus dem Internet anfordern müssen.

Wird von einem Client ein Objekt innerhalb einer bestimmten Zeit angefordert, das im Zwischenspeicher jedoch schon ungültig ist, wird dieses Objekt zur Update-Liste des ISA Server hinzugefügt. Der Zeitpunkt der Aufnahme des Objekts in die Update-Liste ist sowohl von dessen Gültigkeitsdauer, als auch von der festgelegten Active Caching-Einstellung anhängig.

Um das Active Caching zu konfigurieren, navigieren Sie in der ISA-mmc zum Eintrag KONFIGURATION/CACHE und klicken auf CACHEEINSTELLUNGEN KONFIGURIEREN. Auf der Registerkarte AKTIVE ZWISCHENSPEICHERUNG können Sie die Häufigkeit für das Active Caching bestimmen.

- HÄUFIG: Die Anforderung ist nicht später als dreimal die Gültigkeitsdauer des Objekts eingetroffen. Das Objekt wird der Update-Liste hinzugefügt.
- NORMAL: Die Anforderung ist nicht später als zweimal die Gültigkeitsdauer des Objekts eingetroffen. Das Objekt wird der Update-Liste hinzugefügt.
- SELTEN: Die Anforderung ist nicht später als einmal die Gültigkeitsdauer des Objekts eingetroffen. Das Objekt wird der Update-Liste hinzugefügt.

Über die Schaltfläche WIEDERHERSTELLEN wird die Einstellung wieder auf den ursprünglichen Wert zurückgesetzt.

11.5.1 Die Update-Liste

Update-Liste zur Umsetzung der Aktualisierung

Diese Einstellung soll an einem Beispiel verdeutlicht werden. Angenommen, ein Objekt hat eine Gültigkeitsdauer von 24 Stunden und als Active Caching-Option ist normal gewählt, so wird dieses Objekt der Update-Liste hinzugefügt, wenn es innerhalb von zweimal 24 Stunden, also 48 Stunden, erneut von einem Client angefordert wird. Sofern innerhalb dieses Intervalls erneut auf das Objekt zugegriffen wird, bleibt dieses in der Update-Liste erhalten. Erfolgt innerhalb dieses Zeitraums kein Zugriff mehr auf das Objekt, so wird dieses wieder aus der Update-Liste gelöscht.

Die in der Update-Liste enthaltenen Objekte werden vor Ende ihrer Gültigkeitsdauer automatisch vom ISA Server aktualisiert. Die Häufigkeit der Aktualisierung basiert auf der Auslastung des ISA Server. Je nachdem, zu wie viel Prozent der ISA Server ausgelastet ist, erfolgt die Aktualisierung gemäß Tabelle 11.2. Die aktuelle Last des ISA Server wird seit dem jeweils letzten Neustart aus der maximalen Anzahl von gleichzeitigen Websitzungen und der aktuellen Anzahl von Websitzungen berechnet.

Tabelle 11.2: Basierend auf der Auslastung des ISA Server treten unterschiedliche Aktualisierungsverhalten auf

Auslastung	Aktualisierung
0 – 25 %	Es werden alle Objekte der Update-Liste aktualisiert, bei denen schon über 50 % der Gültigkeitsdauer abgelaufen ist.
26 – 75 %	Es werden alle Objekte der Update-Liste aktualisiert, bei denen schon über 75 % der Gültigkeitsdauer abgelaufen ist. Außerdem werden auch die Objekte aktualisiert, deren Gültigkeitsdauer innerhalb der nächsten 7,2 Minuten ablaufen wird.
76 – 100 %	Es werden alle Objekte der Update-Liste aktualisiert, bei denen schon über 95 % der Gültigkeitsdauer abgelaufen ist. Außerdem werden auch die Objekte aktualisiert, deren Gültigkeitsdauer innerhalb der nächsten 3,6 Minuten ablaufen wird.

Eine Patentlösung, welche Einstellungen für das Active Caching optimal sind, kann an dieser Stelle nicht gegeben werden. Allerdings kann das Anwenden des Active Caching auch zu negativen Effekten führen, z.B. wenn der ISA Server zur Aktualisierung der zwischengespeicherten Objekte eine Wählverbindung benutzt oder wenn sich im Cache zahlreiche Objekte mit einer extrem kurzen Gültigkeitsdauer befinden. In diesem Fall könnte der ISA Server mehr mit dem Beschaffen der aktualisierten Objekte als mit dem Beantworten der

Client-Anfragen ausgelastet sein. Da für die Aktualisierung die Verbindung zum Internet hergestellt sein muss, sollten Sie darauf achten, wann der Zugriff zur Aktualisierung auf diese Verbindung erfolgt. Sofern Sie keine Standleitung oder Flat-Rate verwenden, kann dies bei einer Wählverbindung dazu führen, dass diese nahezu 24 Stunden am Tag geöffnet ist und dadurch beträchtliche Kosten verursachen kann.

11.5.2 Weitere Cache-Einstellungen

Zusätzlich zu den eben beschriebenen Grundeinstellungen können noch weitere Einstellungen am Zwischenspeicher vorgenommen werden, um dessen Nutzung weiter zu optimieren. Für diese Einstellungen wechseln Sie auf die Registerkarte ERWEITERT (siehe Abbildung 11.14) der CACHEEINSTELLUNGEN.

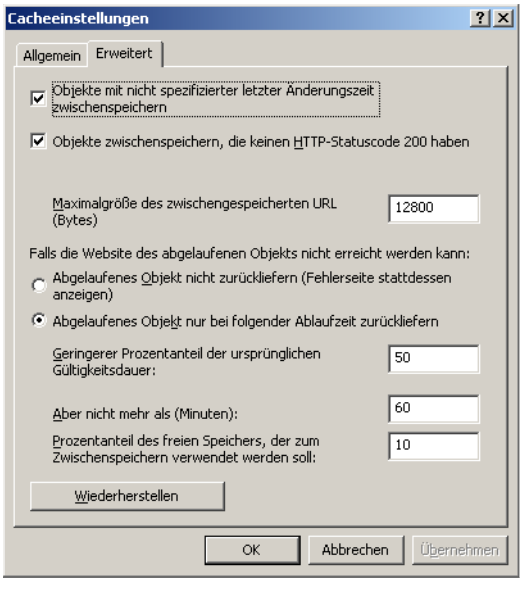


Abbildung 11.14: Die erweiterten Einstellungen am Cache

Auf dieser Registerkarte stehen die folgenden Optionen zur Verfügung:

- OBJEKTE MIT NICHT SPEZIFIZIERTER LETZTER ÄNDERUNGSZEIT ZWISCHENSPEICHERN: Auch wenn ein Objekt kein Erstelldatum besitzt oder das Datum der letzten Objektänderung nicht ermittelt werden kann, werden diese Objekte zwischengespeichert, wenn diese Option aktiviert ist.

- OBJEKTE ZWISCHENSPEICHERN, DIE KEINEN HTTP-STATUSCODE 200 HABEN: Über den http-Statuscode 200 wird angegeben, dass eine Anfrage korrekt durchgeführt und die Webseite angezeigt werden kann. Wird der Statuscode nicht ausgegeben, z.B. weil der Web-

Anzeige einer Fehlermeldung statt eines ungültigen Objekts

server nicht erreichbar ist, kann die Seite auch nicht angezeigt werden. Ist diese Option aktiviert, wird anstelle des gewünschten Objekts bei der Nicht-Verfügbarkeit des Webservers die negative Antwort des Servers vermerkt, so dass bei einer weiteren Anfrage nach diesem Objekt eine entsprechende Fehlermeldung aus dem Zwischenspeicher direkt ausgegeben werden kann. Allerdings sollten Sie diese Option mit Vorsicht behandeln, da es bei einer auch nur kurzen Störung des Webservers zu einer Anzeige des Fehlers kommen wird, bis das Objekt im Zwischenspeicher nicht mehr gültig ist, obwohl das Objekt in Wirklichkeit im Internet schon wieder zur Verfügung steht.

- MAXIMALGRÖßE DES ZWISCHENGESPEICHERTEN URL (BYTES): Objekte, die größer sind als hier festgelegt, werden nicht im Arbeitsspeicher, sondern direkt auf der Festplatte zwischengespeichert. Auch wenn ein großes Objekt sehr häufig verwendet wird, wird dieses nicht im Arbeitsspeicher abgelegt. Dadurch wird verhindert, dass der Arbeitsspeicher nicht mit nur wenigen großen Objekten belegt wird. Da die Antwortzeiten für dort gespeicherte Objekte geringer sind als für die auf der Festplatte gespeicherten, sollten sich im Arbeitsspeicher immer so viele Objekte wie möglich befinden.

Zusätzlich wird auf dieser Seite noch bestimmt, ob ein bereits abgelaufenes Objekt dennoch an den Benutzer zurückgegeben werden soll, wenn der Webserver zum eigentlichen Zeitpunkt der notwendigen Aktualisierung nicht verfügbar ist. Würde in diesem Moment nicht das veraltete Objekt dargestellt, so erhielte der Benutzer eine Fehlermeldung, dass die Objekte oder die komplette Webseite nicht verfügbar sind. Für die Konfiguration dieses Verhaltens stehen die folgenden Optionen zur Verfügung:

- ABGELAUFENES OBJEKT NICHT ZURÜCKLIEFERN (FEHLERSEITE STATTDESSEN ANZEIGEN): Ist diese Option aktiviert, werden keine bereits abgelaufenen Objekte an den Client zurückgegeben. Anstelle des Objekts erhält der Client eine Fehlermeldung mit dem Hinweis, dass entweder die komplette Webseite oder das angeforderte Objekt nicht angezeigt werden kann.
- ABGELAUFENES OBJEKT NUR BEI FOLGENDER ABLAUFZEIT ZURÜCKLIEFERN: Es wird ein bereits abgelaufenes Objekt gemäß einer der folgenden Einstellungen zurückgeliefert. Eine Fehlermeldung wird nicht angezeigt.
- GERINGERER PROZENTANTEIL DER URSPRÜNGLICHEN GÜLTIGKEITSDAUER: Dieser Wert gibt die Prozentzahl der ursprünglichen Gültigkeitsdauer an. Der vordefinierte Wert liegt bei 50 Prozent. Bis zum Erreichen dieses Werts werden auch veraltete Objekte zurückgegeben, erst danach wird eine Fehlermeldung angezeigt.

- ABER NICHT MEHR ALS (MINUTEN): Ist für ein Objekt eine sehr hohe Gültigkeitsdauer gesetzt, so kann dieser Wert stattdessen durch eine bestimmte Anzahl von Minuten definiert werden. Der vordefinierte Wert liegt bei 60 Minuten.

Zuweisung des Cache-Anteils am Arbeitsspeicher

Zusätzlich kann der Anteil des freien Arbeitsspeichers für die Zwischenspeicherung festgelegt werden.

- PROZENTANTEIL DES FREIEN SPEICHERS, DER ZUM ZWISCHENSPEICHERN VERWENDET WERDEN SOLL: Der Standardwert liegt bei zehn Prozent. Wird ein höherer Anteil des Arbeitsspeichers für die Zwischenspeicherung zugewiesen, kann diese zwar performanter durchgeführt werden, es ist jedoch darauf zu achten, dass auch für andere Serverdienste bzw. deren Prozesse weniger Arbeitsspeicher verfügbar ist. Dies kann dazu führen, dass die vollständige Leistung inklusive der Zwischenspeicherung rapide abfällt. Wird ein ISA Server ausschließlich als Cacheserver eingesetzt, kann dieser Wert deutlich höher gesetzt werden, je nach Ausstattung mit RAM auf 70 bis 80 Prozent. Generell gilt auch beim Modifizieren dieses Werts, dass die Leistungsfähigkeit des gesamten Systems solange geprüft und überwacht werden sollte, bis ein optimaler Wert gefunden ist.

Auch für diese Einstellungen gilt, dass sie sich nicht zwangsläufig positiv auf die Leistung des ISA Server auswirken müssen. Sie sollten also in jedem Fall nach der Konfiguration der Zwischenspeicherung diese eine Zeit lang beobachten, um so möglicherweise notwendige Konfigurationsänderungen noch einpflegen zu können.

11.6 Planen von Inhalts-Downloads

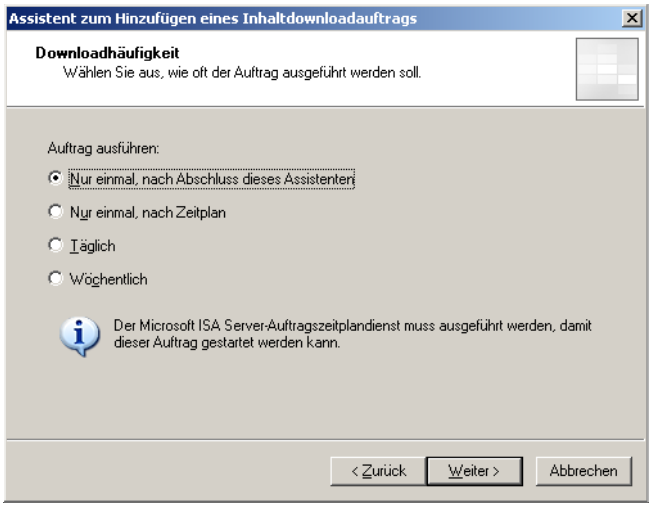
Automatischer Download zu festen Zeiten von häufig besuchten Webseiten

Außer dem automatischen Download häufig besuchter Webseiten und deren Objekte mittels URL-Liste kann der ISA Server auch automatisch anhand von frei definierbaren Zeitplänen bestimmte Inhalte in seinen Zwischenspeicher downloaden. Auf diese Weise können Sie z.B. täglich vor Beginn der regulären Arbeitszeit die kompletten Inhalte der am häufigsten besuchten Webseiten automatisch downloaden lassen, so dass die Inhalte vollständig aus dem Cache bezogen werden können, wodurch die Internetverbindung entlastet und die Antwortzeiten für die Clients verkürzt werden.

1. Um dieses Feature einzurichten, navigieren Sie in der ISA-mmc zum Eintrag KONFIGURATION/CACHE und wechseln auf die Registerkarte INHALTSDOWNLOADAUFTRÄGE.
2. Klicken Sie dann im Aufgabenbereich auf INHALTSDOWNLOADAUFTRAG PLANEN.

3. Sie erhalten zunächst ein Hinweisfenster, dessen Inhalt Sie mit JA bestätigen müssen. Durch diese Bestätigung wird auf dem ISA Server die Systemrichtlinie aktiviert, die die geplanten Downloads zulässt. Außerdem wird für das Netzwerk *Lokaler Host*, also den ISA Server selbst, der Webproxy-Listener eingerichtet.
4. Klicken Sie dann auf ÜBERNEHMEN, damit die neue Systemrichtlinie und der Weblistener aktiviert werden können.
5. Danach müssen Sie abermals auf den Link INHALTSDOWNLOADAUFTRAG PLANEN klicken und einen passenden Namen für diesen Auftrag angeben. Klicken Sie dann auf WEITER.
6. Im Fenster DOWNLOADHÄUFIGKEIT (siehe Abbildung 11.15) bestimmen Sie, wann der neue Auftrag ausgeführt werden soll. Die Ausführung kann entweder nur einmalig oder in täglichen bzw. wöchentlichen Abständen erfolgen. Klicken Sie dann auf WEITER.

Abbildung 11.15: Auswahl der Häufigkeit für den Inhaltsdownload



7. Haben Sie sich für die Option WÖCHENTLICH entschieden, können Sie die einzelnen Wochentage, das Startdatum sowie die Startzeit bestimmen (siehe Abbildung 11.16). Außerdem wird festgelegt, ob der Download einmal am Tag zur gewünschten Startzeit oder in einem bestimmten Abstand erneut durchgeführt werden soll. Geben Sie dazu die Anzahl der Minuten an, nach deren Ablauf erneut ein Inhalts-Download erfolgen soll. Zudem kann eine Uhrzeit festgelegt werden, nach der an einem Tag kein Download mehr erfolgen soll. Haben Sie im vorigen Fenster eine der anderen Optionen gewählt, geben Sie lediglich die Startzeit und das Startdatum an. Klicken Sie danach auf WEITER.

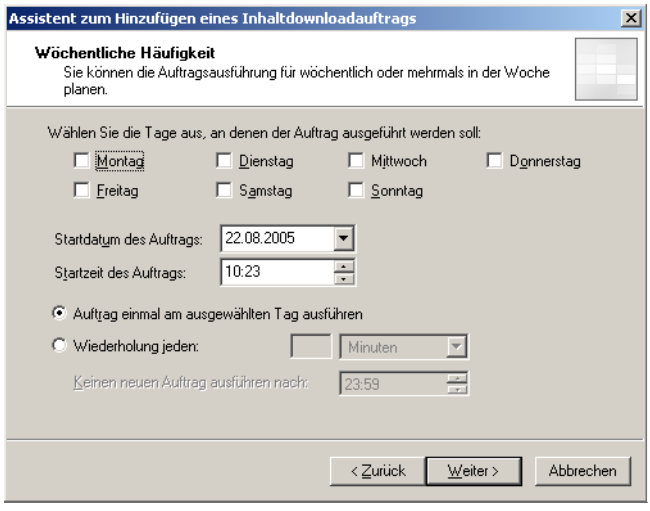


Abbildung 11.16: Beispielkonfiguration der Häufigkeitsoption Wöchentlich

8. Im Fenster INHALTSDOWNLOAD (siehe Abbildung 11.17) wird in das Feld INHALTSDOWNLOAD VON DIESEM URL die vollständige URL der downzuloadenden Inhalte angegeben. Zusätzlich sind dort die folgenden Optionen verfügbar:

- LINK NICHT AUßERHALB DES ANGEGEBENEN URL-DOMÄNENNAMENS FOLGEN: Verweist ein Objekt auf eine andere Webseite, so wird diese nicht downgeloadet.
- MAXIMALE LINKTIEFE PRO SEITE: Bestimmt die maximale Linkverzweigung, die für den Download verfolgt werden soll. Tiefer liegende Links werden nicht heruntergeladen.
- ANZAHL DER ABGERUFENEN OBJEKTE EINSCHRÄNKEN AUF: Über diesen Wert wird bestimmt, wie viele Objekte über den Download-Auftrag in den Zwischenspeicher geschrieben werden sollen. Sobald dieser Wert erreicht ist, werden keine weiteren Objekte mehr heruntergeladen, auch wenn sich der URL-Inhalt noch nicht komplett im Cache befindet. Auf diese Weise ist es möglich, den Cache so zu verteilen, dass dieser nicht komplett durch nur eine einzige große Webseite belegt wird.
- MAXIMALE ANZAHL GLEICHZEITIGER TCP-VERBINDUNGEN FÜR DIESEN AUFTRAG: Bestimmt die Anzahl der gleichzeitigen TCP-Verbindungen zum Server. Über jede TCP-Verbindung kann immer nur ein Objekt zur Zeit heruntergeladen werden.

Maximal ein Objekt pro TCP-Verbindung downloadbar

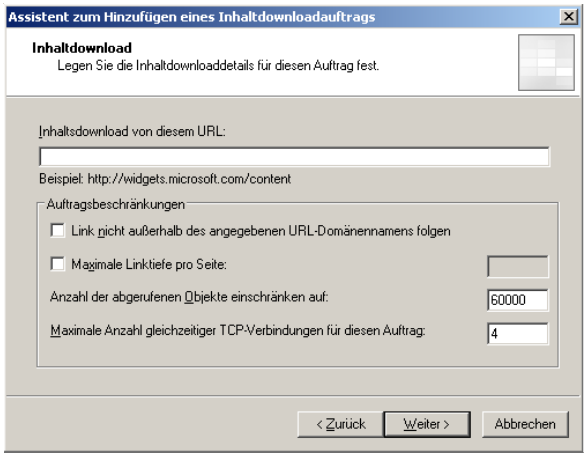


Abbildung 11.17: Bestimmen der URL, von der der Inhalt downgeloadet werden soll

9. Danach werden im Fenster INHALTSZWISCHENSPEICHERUNG (siehe Abbildung 11.18) Optionen für den Cache-Inhalt und die Gültigkeitsdauer festgelegt.

Globale Cache-Einstellungen können andere außer Kraft setzen

Optionen für den Cache-Inhalt:

- ALLE INHALTE ZWISCHENSPEICHERN: es werden ausnahmslos alle Objekte im Zwischenspeicher abgelegt. Dies gilt auch für Objekte, bei denen im Quell- oder Anforderungsheader festgelegt ist, dass diese nicht zwischengespeichert werden sollen, sowie für Objekte, die vorübergehend umgeleitet worden sind, und für Offline-Inhalte.
- WENN QUELL- UND ANFORDERUNGSHEADER ZWISCHENSPEICHERN INDIZIEREN BZW. WENN DER INHALT DYNAMISCH IST, DANN WIRD DER INHALT ZWISCHENGESPEICHERT: Objekte werden nur zwischengespeichert, wenn die Quell- und Anforderungsheader dies zulassen oder wenn es sich um dynamische Inhalte handelt.
- INHALT WIRD ZWISCHENGESPEICHERT, WENN QUELL- UND ANFORDERUNGSHEADER DIES INDIZIEREN: Objekte werden nur zwischengespeichert, wenn die Quell- und Anforderungsheader dies zulassen. Dagegen werden dynamische Inhalte nicht in den Zwischenspeicher geschrieben.
- Optionen für die Gültigkeitsdauer:
- INHALT LÄUFT GEMÄß DER CACHEREGEL AB: Die Gültigkeitsdauer wird nur über die festgelegten Cache-Regeln bestimmt.
- GÜLTIGKEITSDAUER FESTLEGEN, FALLS DIES NICHT IN DER ANTWORT DEFINIERT IST: Die Gültigkeitsdauer wird entweder entsprechend dem im Header gesetzten Wert übernommen oder, wenn dort kein Wert festgesetzt ist, auf einen in Minuten anzugebenden Wert festgelegt.
- GÜLTIGKEITSDAUER DES OBJEKTS AUßER KRAFT SETZEN: Es werden nicht die im Header angegebenen Gültigkeitswerte übernommen, sondern alle angegebenen Werte durch den in Minuten zu spezifizierenden Wert überschrieben.

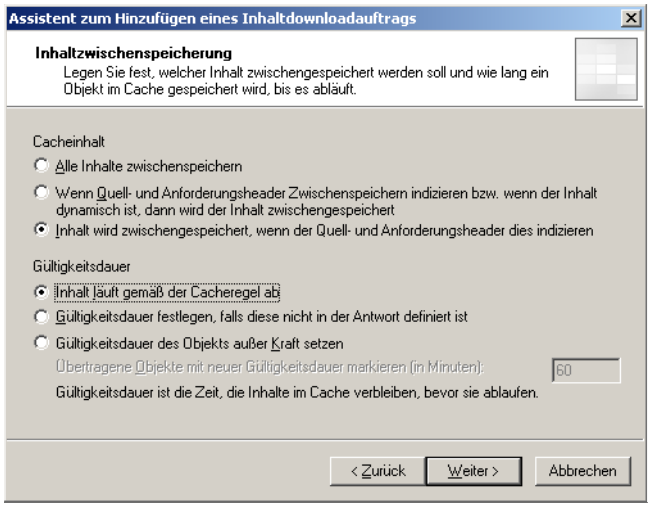


Abbildung 11.18: Weitere Optionen für den Cache-Inhalt und die Gültigkeitsdauer

Wählen Sie die gewünschte Option und klicken Sie auf WEITER. Beenden Sie dann den Assistenten und übernehmen mit einem Klick auf die gleichnamige Schaltfläche die Konfigurationsänderungen.

Auch wenn ein Download-Auftrag an einen bestimmten Zeitplan gebunden ist, so kann der Auftrag auch jederzeit manuell gestartet werden. Markieren Sie dazu den gewählten Auftrag in der Liste und klicken Sie im Aufgabenbereich auf AUSGEWÄHLTE AUFTRÄGE JETZT STARTEN. Zusätzlich können über die Aufgabenliste vorhandene Aufträge gelöscht, bearbeitet oder vorübergehend deaktiviert werden.

11.7 Deaktivieren der Cache-Funktion

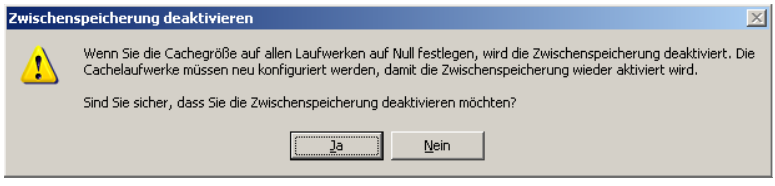
Deaktivierung und spätere Aktivierung

Es ist möglich, die Cache-Funktion des ISA Server zu jedem beliebigen Zeitpunkt zu deaktivieren.

Ist der ISA Server gleichzeitig auch als Firewall eingerichtet, so wird diese Funktion durch das Deaktivieren des Cache selbstverständlich nicht aufgehoben. Lediglich beim reinen Einsatz als Cacheserver erfüllt der ISA Server nach der Deaktivierung keinen Zweck mehr.

1. Um das Caching zu deaktivieren, markieren Sie in der ISA-mmc den Eintrag KONFIGURATION/CACHE, wechseln auf die Registerkarte CACHEREGELN und klicken im Aufgabenbereich auf ZWISCHENSPEICHERUNG DEAKTIVIEREN.
2. Sie erhalten ein Hinweisfenster, das Sie über die Auswirkung dieser Aktion informiert (siehe Abbildung 11.19). Bestätigen Sie dieses mit JA.

Abbildung 11.19: Hinweisfenster, das beim Deaktivieren der Cache-Funktion angezeigt wird



3. Klicken Sie dann auf ÜBERNEHMEN und wählen dabei die Option ÄNDERUNGEN SPEICHERN UND DIENSTE NEU STARTEN. Bestätigen Sie dies mit OK.

Sobald die Zwischenspeicherung deaktiviert ist, wird automatisch der zugewiesene Speicherplatz auf allen Laufwerken auf Null MB gesetzt.

Die Cache-Dateien selbst werden dadurch jedoch nicht gelöscht. Diese müssen bei Bedarf manuell gelöscht werden.

Spätere Weiterverwendung

Auch die bereits konfigurierten Cache-Regeln sowie Inhalts-Downloads bleiben erhalten. Dies bietet den Vorteil, dass diese Konfigurationen bei einer späteren Reaktivierung der Zwischenspeicherung wieder vorhanden sind und nicht erneut eingerichtet werden müssen.

12 Überwachung und Protokollierung

Dieses Kapitel beschäftigt sich mit der Überwachungsfunktion des ISA Server sowie der Protokollierung von ISA-relevanten Ereignissen. Unter der Überwachung werden nicht nur zu überwachende Ereignisse verstanden, die auf Angriffen oder anderen Attacken auf das Netzwerk resultieren, sondern auch die Überwachung des ISA Server selbst auf einwandfreie Funktionalität. Dessen reibungsloser Funktionalität kommt im Netzwerk eine enorme Bedeutung zu, da ausschließlich über den ISA Server die Verbindung aller angeschlossenen Clients zum Internet erfolgt und dieser allein für den Schutz des Netzwerks vor Angriffen zuständig ist.

Deshalb müssen Probleme, die sich aufgrund von falschen Konfigurationen oder auch Hardwarefehlern ergeben, schnellstmöglich erkannt und beseitigt werden. Hierzu ist eine Überwachung des ISA Server unerlässlich.

Zur Überwachung der Leistungsdaten des ISA Server selbst dient der Leistungsmonitor. Auch dessen Konfigurationsoptionen werden in diesem Kapitel behandelt.

Der zweite Teil dieses Kapitels beschäftigt sich mit der Protokollierung. Die Protokolldaten können entweder in eine MSDE- oder SQL-Server-Datenbank oder in eine simple Textdatei geschrieben werden. Die dazu erforderlichen Konfigurationen werden alle erläutert.

Den Abschluss des Kapitels bildet das Thema Intrusion Detection. Dort lernen Sie zum einen die häufigsten Angriffsmethoden kennen, zum anderen, wie Sie über die entstandenen Angriffe schnell informiert werden.

12.1 Die Überwachungsfunktion

Zentrale Übersicht über verschiedene Kategorien

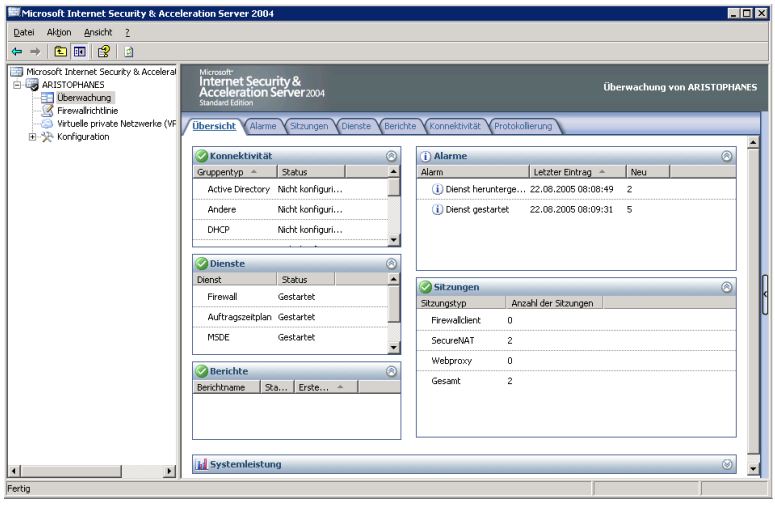
In der ISA-mmc steht für die Überwachung das gleichnamige Snap-In zur Verfügung. Dort sind die Überwachungsfunktionen nach verschiedenen Bereichen geordnet abzulesen (siehe Abbildung 12.1). Dabei handelt es sich um die folgenden Kategorien:

- Übersicht
- Alarme
- Sitzungen
- Dienste

- Berichte
- Konnektivität
- Protokollierung

Die folgende Gliederung dieses Kapitels orientiert sich an der Reihenfolge dieser Registerkarten.

Abbildung 12.1: Überblick über die Überwachungsfunktion des ISA Server



Unter ÜBERSICHT sehen Sie eine komprimierte Zusammenfassung sämtlicher Kategorien. Wo es möglich ist, werden die Überwachungsdaten dort in Echtzeit dargestellt. Diese Seite sollte also immer ihr erster Anlaufpunkt sein, wenn Sie eine schnelle Übersicht über den Status des ISA Server benötigen. So können Sie schnell erkennen, ob Alarme aufgelaufen sind, Dienste beendet sind oder Verbindungsprobleme vorliegen. Zusätzlich werden im Leistungsmonitor die zugelassenen und verworfenen Pakete pro Sekunde dargestellt. Sofern Sie in dieser komprimierten Übersicht an einer bestimmten Stelle Fehler oder Probleme feststellen, können Sie diese auf der entsprechenden Registerkarte weiter nachvollziehen bzw. dort Konfigurationseinstellungen vornehmen.

Übersichtliche Symbole

Für die Darstellung des Status verwendet der ISA Server vier verschiedene Symbole:

- Weißes Häkchen in grünem Kreis: Es liegen keine Probleme oder Fehler vor.
- Blaues „i“ in weißem Kreis: zeigt an, dass eine nicht sicherheitskritische Information vorliegt, z.B. unter DIENSTE der Start eines Dienstes
- Schwarzes Ausrufezeichen in gelbem Dreieck: Dieses Symbol bezeichnet eine Warnung. Dieses Ereignis nimmt zwar keinen Einfluss auf die Funktion oder die Konfiguration des ISA Server

und stellt auch kein sicherheitsrelevantes Problem dar, dennoch sollten Sie den Inhalt dieser Warnung zeitnah prüfen.

- Weißes Kreuz in rotem Kreis: Das Symbol kennzeichnet einen schwer wiegenden Fehler, der sich negativ auf die Funktion des ISA Server auswirken kann. Derartige Einträge müssen sofort geprüft und die aufgetretenen Probleme behoben werden.

12.2 Alarme

56 vordefinierte Alarme

Auf der Registerkarte ALARME kann festgelegt werden, bei welchem Ereignis welche Art von Alarm ausgelöst werden soll. Dazu bietet der ISA Server bereits 56 vordefinierte Definitionen für Alarme, für die jeweils unterschiedliche Aktionen festgelegt werden können. Diese reichen von der Information des Administrators per E-Mail bis hin zum Herunterfahren des ISA Server.

Auf der Registerkarte ALARME (siehe Abbildung 12.2) finden Sie eine Übersicht über alle aufgetretenen Alarme. Sämtliche Alarme sind aus Gründen der Übersichtlichkeit nach Kategorien geordnet. Für jeden der Alarme ist das Datum des Auftretens, die Kategorie sowie der Status angegeben.

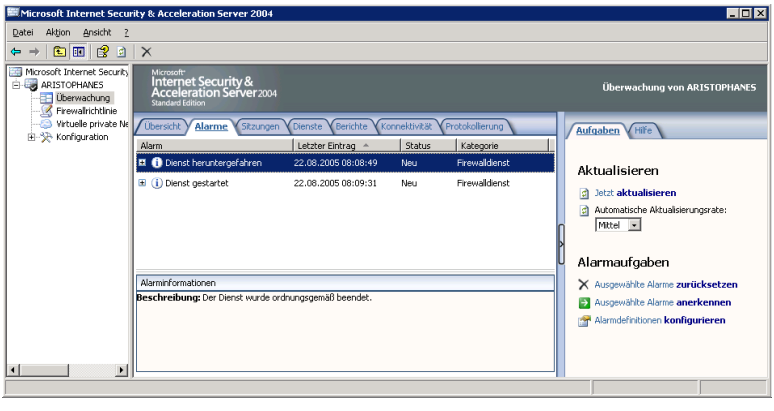


Abbildung 12.2: Übersicht über die nach Kategorien geordneten Alarme

Zurücksetzen von Alarmen

Als Status ist entweder der Wert NEU oder ANERKANNT angegeben. Ein neu hinzugekommener Alarm besitzt logischerweise zunächst den Status NEU. Sobald Sie jedoch einen Alarm überprüft und die Ursache dafür beseitigt haben, markieren Sie diesen und klicken im Aufgabenbereich auf AUSGEWÄHLTE ALARME ANERKENNEN. Insbesondere wenn mehrere Administratoren für die Pflege des ISA Server verantwortlich sind, ist für die jeweils anderen Administratoren schnell ersichtlich, welche Alarme zurückgesetzt und damit beseitigt sind. Alternativ zur Anerkennung kann auch eine Zurücksetzung eines Alarms durchgeführt werden. Dabei wird der Alarm komplett aus der Liste entfernt.

Im Aufgabenbereich können Sie über den entsprechenden Link jederzeit eine Aktualisierung der Alarmanzeige vornehmen. Des Weiteren können Sie auch die Aktualisierungsrate für die Anzeige bestimmen. Standardmäßig ist eine mittlere Wiederholungsrate vorgegeben, sie kann jedoch herauf- oder herabgesetzt werden.

Alarmaktionen festlegen

Des Weiteren werden im Aufgabenbereich über den Link ALARMDEFINITIONEN KONFIGURIEREN die Aktionen für einen bestimmten Alarm festgelegt. Mit einem Klick auf diesen Link erhalten Sie das Fenster EIGENSCHAFTEN DER ALARME (siehe Abbildung 12.3). Dort sehen Sie anhand der Checkbox vor dem Namen des Alarms, ob der jeweilige Alarm aktiv ist oder nicht. Zusätzlich wird für jeden Alarm der Schweregrad des Auftretens als Symbol dargestellt (Fehler, Warnung, Hinweis). Zusätzlich ist für jeden der Alarme die zugehörige Kategorie angegeben.

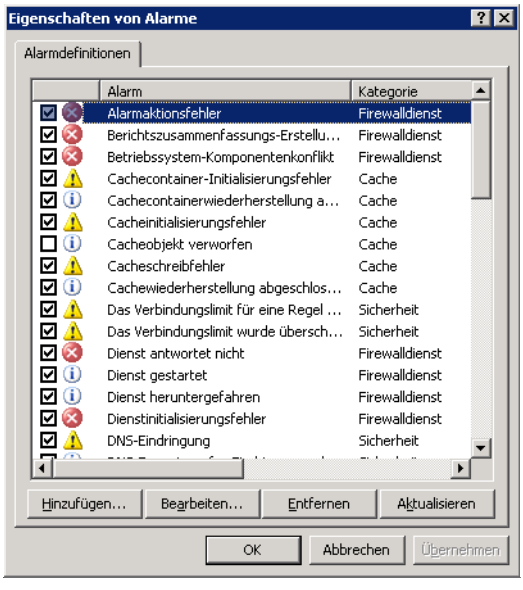


Abbildung 12.3: Die Eigenschaften der auf dem ISA Server konfigurierten Alarme

Hinzufügen von Alarmen

Aus der Liste können auch Alarme über ENTFERNEN gelöscht werden. Um diese zu einem späteren Zeitpunkt wieder verfügbar zu machen, klicken Sie auf HINZUFÜGEN. Dabei führt Sie ein Assistent durch den Vorgang. Sie haben jedoch nur die Möglichkeit, darin als Ereignis eines der vom ISA Server vordefinierten Ereignisse auszuwählen. Zudem darf sich dieses Ereignis noch nicht in der Liste der Alarme befinden, da jedes Ereignis dort nur einmal vorhanden sein darf. Andernfalls erhalten Sie eine Fehlermeldung des Assistenten.

Im Assistenten werden dieselben Einträge abgefragt, die auch über das Bearbeiten eines Alarms vorgenommen werden können. Das Bearbeiten eines Alarms wird im weiteren Verlauf dieses Kapitels beschrieben.

Alarmereignisse

In der folgenden Tabelle finden Sie eine Übersicht über alle vordefinierten Alarmereignisse des ISA Server:

Alarmereignis	Beschreibung
Alarmaktionsfehler	Eine Aktion, die einem Alarm zugeordnet ist, konnte nicht ausgeführt werden.
Berichtzusammenfassungs-Erstellungsfehler	Das Erstellen einer Berichtszusammenfassung aus bestehenden Protokolldaten ist fehlgeschlagen.
Betriebssystem-Komponentenkonflikt	Bei einer der Betriebssystem-Komponenten NAT-Editor, ICS oder RRAS besteht ein Konflikt mit dem Betriebssystem.
Cachecontainer-Initialisierungsfehler	Die Initialisierung des Cache-Containers ist fehlgeschlagen.
Cachecontainerwiederherstellung abgeschlossen	Ein einzelner Cache-Container wurde wiederhergestellt.
Cacheinitialisierungsfehler	Der Cache des Webproxy wurde deaktiviert, da ein globaler Fehler vorlag.
Cacheobjekt verworfen	Bei der Wiederherstellung des Cache wurde das Fehler verursachende Objekt verworfen.
Cacheschreibfehler	Es ist ein Fehler aufgetreten, während Objekte in den Cache geschrieben wurden.
Cachewiederherstellung abgeschlossen	Die Cache-Wiederherstellung ist erfolgreich abgeschlossen worden.
Das Verbindungslimit für eine Regel wurde überschritten.	Die maximale Anzahl der Verbindungen pro Sekunde, die für eine Regel konfiguriert wurde, wurde überschritten.
Das Verbindungslimit wurde überschritten.	Das Verbindungslimit wurde durch eine IP-Adresse oder einen Benutzer überschritten.
Dienst antwortet nicht	Der Dienst des ISA Server ist nicht mehr verfügbar oder wurde beendet.
Dienst gestartet	Ein Dienst wurde korrekt gestartet.
Dienst heruntergefahren	Ein Dienst wurde korrekt beendet.
Dienstinitialisierungsfehler	Bei der Initialisierung eines Dienstes ist ein Fehler aufgetreten.
DNS-Eindringung	Es wurde vom ISA Server ein DNS-Eindringung, z.B. ein Hostnamenüberlauf, ermittelt.
DNS-Zonentransfer Eindringversuch	Eine unerlaubte Übertragung einer DNS-Zone wurde ermittelt.
Ein Neustart des ISA Server-Computers ist erforderlich.	Der Neustart ist notwendig, damit bestimmte Konfigurationsänderungen am ISA Server übernommen werden können.
Eindringversuch festgestellt	Es wurde vom ISA Server ein Eindringversuch durch einen externen Benutzer festgestellt.

Tabelle 12.1: Übersicht über die vordefinierten Alarm-Ereignisse des ISA Server

Alarmereignis	Beschreibung
Ergebnisprotokollfehler	Die Ereignisprotokollierung in das Windows-Systemprotokoll hat Fehler verursacht.
Ermittlungsmechanismus gegen bösartige DHCP-Eindringversuche wurde deaktiviert	Dieser Ermittlungsmechanismus ist deaktiviert worden.
Fehler bei der Cachedateigrößenänderung	Bei einer Änderung der Cache-Dateigröße ist es zu einem Problem gekommen.
Fehler bei Wählen bei Bedarf	Es konnte keine DFÜ-Verbindung vom ISA Server aufgebaut werden.
Firewall-Kommunikationsfehler	Es gab ein Problem in der Kommunikation zwischen ISA Server und Firewallclient.
FTP-Filter-Initialisierungswarnung	Vom FTP-Filter konnten die gestatteten FTP-Befehle nicht geprüft werden.
IP-Spoofing	Der Quellcomputer besitzt eine ungültige IP-Adresse.
Keine Konnektivität	Vom ISA Server konnte keine Verbindung mit dem angegebenen Server hergestellt werden.
Keine Ports verfügbar	Weil kein Port verfügbar ist, konnte kein Socket erstellt werden.
Komponentenladefehler	Fehler beim Laden einer Erweiterungskomponente
Konfigurationsfehler	Die Konfigurationsinformationen konnten nicht korrekt gelesen werden.
Langsame Konnektivität	Ein Server, für den eine Konnektivitätsprüfung erstellt wurde, hat nicht innerhalb der festgelegten Zeit dem ISA Server geantwortet.
Nicht registriertes Ereignis	Ein unbekanntes Ereignis ist aufgetreten.
POP-Eindringung	Es wurde ein POP-Pufferüberlauf festgestellt.
POP-Eindringversuch	Es wurde ein POP-Pufferüberlauf festgestellt.
Protokollierungsfehler	Eine Dienstprotokollierung hat nicht korrekt funktioniert.
Protokollspeicherlimits	Für ein Protokoll wurde das Speicherlimit erreicht.
Ressourcenzuweisungsfehler	Es gab einen Fehler bei der Zuweisung von Ressourcen.
Routing(verkettungs)-fehler	Eine Anfrage an einen Upstreamserver konnte nicht korrekt durchgeführt werden.

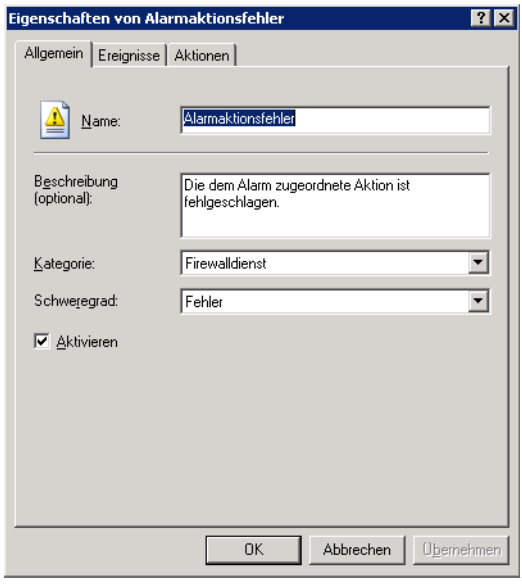
Alarmereignis	Beschreibung
Routing(verkettungs)-wiederherstellung	Die Weiterleitung von Anfragen an einen Upstreamserver funktioniert wieder.
RPC-Filter: Konnektivität wurde geändert	Es wurde die Konnektivität zum RPC-Veröffentlichungs-Dienst modifiziert.
RPC-Filter-Bindungsfehler	Da der Port bereits verwendet wird, kann der RPC-Filter den ihm zugewiesenen Port.
Serververöffentlichung ist unzutreffend	Eine Serververöffentlichungsregel ist fehlerhaft konfiguriert.
Serververöffentlichungs-Wiederherstellung	Eine Serververöffentlichungsregel, die nicht funktionierte, läuft jetzt wieder.
Serververöffentlichungs-fehler	Eine Serververöffentlichungsregel arbeitet nicht fehlerfrei.
SMTP-Filterereignis	Es wurde ein SMTP-Befehl bzw. eine SMTP-Protokollverletzung verweigert oder blockiert.
SOCKS-Konfigurations-fehler	Es wurde in den SOCKS-Eigenschaften ein bereits von einem anderen Dienst oder Protokoll verwendeter Port konfiguriert.
SYN-Angriff	Ein SYN-Angriff wurde festgestellt.
Ungültige Anmeldeinformationen für Wählen bei Bedarf	Die Anmeldeinformationen für eine Wählen-bei-Bedarf-Verbindung sind ungültig.
Ungültige ODBC-Protokoll-Anmeldeinformationen	Die Anmeldeinformationen für eine ODBC-Datenquelle sind ungültig.
Ungültige Zertifikatsliste gefunden	Aufgrund einer Zertifikatssperrliste wurde ein Zertifikat blockiert.
Ungültiges DHCP-Angebot	Eine vom DHCP-Server angebotene IP-Adresse ist ungültig.
Upstream-Verkettungs-Anmeldeinformationen	Die Anmeldeinformationen an einem Upstreamserver sind nicht gültig.
Veränderte Netzwerk-konfiguration	Es wurde eine Änderung an der Konfiguration des Netzwerks ermittelt.
VPN-Verbindungsfehler	Ein VPN-Client konnte keine Verbindung herstellen.
Zu großes UDP-Paket	Die festgelegte Maximalgröße für ein UDP-Paket wurde überschritten und das Paket vom ISA Server verworfen.
Änderungen des Quarantänen-Clientnetzwerks	Ein Benutzer des Quarantäne-VPN-Netzwerks hat dieses verlassen.

Anpassen von Alarmen

Um einen vordefinierten Alarm anzupassen, klicken Sie auf die Schaltfläche BEARBEITEN. Auf drei verschiedenen Registerkarten können nun Einstellungen von der Kategorie des Alarms über die Definition des Ereignisses bis hin zur Wahl der gewünschten Aktion geändert werden.

Auf der Registerkarte ALLGEMEIN (siehe Abbildung 12.4) können der Name, die Beschreibung, die Kategorie sowie der Schweregrad des Alarms eingestellt werden. Zusätzlich ist über die Checkbox AKTIVIEREN zu entscheiden, ob der betreffende Alarm scharf geschaltet werden soll.

Abbildung 12.4: Die allgemeinen Eigenschaften eines Alarms



Bedingungen für Alarme

Komplexer sind schon die Einstellungen auf der Registerkarte EREIGNISSE (siehe Abbildung 12.5). Unter EREIGNIS und BESCHREIBUNG sehen Sie die Einträge der Registerkarte ALLGEMEIN. Für einige Ereignisse kann unter ZUSÄTZLICHE BEDINGUNG eine zweite Bedingung aus einer Liste ausgewählt werden. Erst wenn auch die dort gesetzte Bedingung erfüllt ist, wird das Ereignis als Alarm gewertet. Ist für ein Ereignis keine zusätzliche Bedingung verfügbar, ist dieses Feld nicht anwählbar.

Häufigkeit des Auftretens

Des Weiteren wird festgelegt, bei welcher Häufigkeit des Ereignisses ein Alarm ausgelöst werden soll. Dazu können Sie entweder unter WIEDERHOLUNGSANZAHL oder unter ANZAHL DER EREIGNISSE PRO SEKUNDE einen Grenzwert bestimmen. Für zahlreiche Ereignisse ist jedoch die Angabe einer Häufigkeit nicht erforderlich oder würde keinen Sinn ergeben.

Der Alarm wird nur ausgelöst, wenn das Ereignis (und gegebenenfalls dessen zusätzliche Bedingung) zusammen mit der definierten Häufigkeit auftritt. Eine Ausnahme besteht nur, wenn für das Ereignis keine Häufigkeit definiert ist.

Im Bereich ALARM BEIM ÜBERSCHREITEN DER SCHWELLENWERTE WIE FOLGT AUSLÖSEN legen Sie fest, wann der Alarm ausgelöst werden soll. Dieses kann entweder sofort oder auch nach einem in Minuten zu definierenden Intervall geschehen. Soll verhindert werden, dass

derselbe Alarm zu häufig ausgelöst wird, so wählen Sie die Option NUR NACH MANUELLEM ZURÜCKSETZEN DES ALARMS. So kann derselbe Alarm erst wieder ausgelöst werden, wenn der Alarmeintrag vom Administrator in der Liste zurückgesetzt wurde.

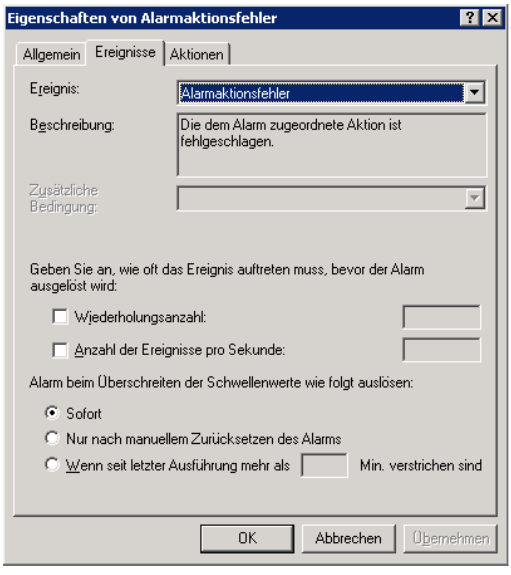


Abbildung 12.5: Für jeden Alarm können die Ereignisse bestimmt werden, durch die ein Vorfall auch als Alarm gekennzeichnet wird

Reaktion durch Aktion

Auf der dritten Registerkarte AKTIONEN (siehe Abbildung 12.6) schließlich legen Sie fest, welche Aktion beim Eintreten des Alarms ausgelöst werden soll. Sie können insgesamt bis zu fünf verschiedene Aktionen für jeden Alarm auswählen. Jedoch wird es in der Praxis wenig Sinn machen, für jeden Alarm alle Aktionen auslösen zu lassen.

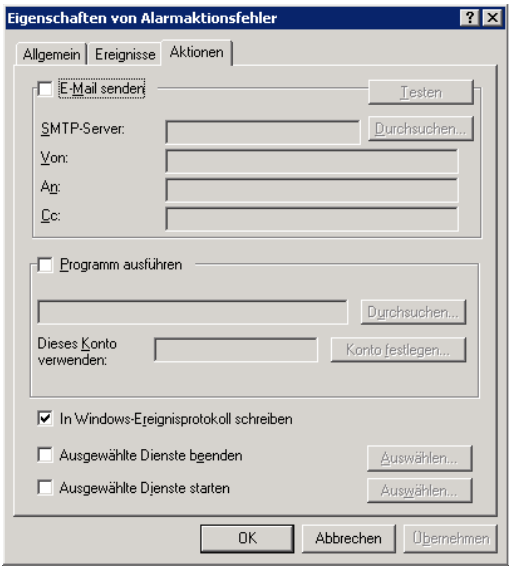


Abbildung 12.6: Sie können mehrere Aktionen wählen, die beim Auftreten eines Alarms ausgeführt werden sollen

Senden einer E-Mail

Soll beim Auslösen des Alarms ein Administrator oder eine andere Person per E-Mail benachrichtigt werden, so markieren Sie die Checkbox E-MAIL SENDEN. Zusätzlich müssen Sie den SMTP-Server, die Adresse des Absenders sowie den oder die Empfänger angeben.

Damit das Senden der E-Mail funktioniert, muss entweder die Systemrichtlinie das Senden von E-Mails vom ISA Server zum internen Netzwerk zulassen, sofern sich der SMTP-Server im internen Netzwerk befindet. Befindet sich der SMTP-Server hingegen im externen Netzwerk, muss zuvor eine Zugriffsregel erstellt worden sein. Außerdem muss sichergestellt sein, dass der SMTP-Server E-Mails vom ISA Server empfangen kann.

Programmausführung

Über PROGRAMM AUSFÜHREN können Sie eine Applikation bestimmen, die bei einem Alarm ausgeführt werden soll. Wählen Sie dazu unter DURCHSUCHEN die ausführbare Datei dieser Applikation aus und geben Sie gegebenenfalls ein Benutzerkonto für die Programmausführung an.

Ereignisprotokoll

Die Option IN WINDOWS-EREIGNISPROTOKOLL schreiben ist bei den meisten Ereignissen bereits standardmäßig aktiviert. Es wird dabei ein Eintrag in das Windows-Ereignisprotokoll vorgenommen.

Dienste starten oder beenden

Außerdem können beim Eintreten des Alarmfalls auch bestimmte Dienste beendet oder gestartet werden. Markieren Sie dazu die gewünschte(n) Checkbox(en) und klicken Sie auf AUSWÄHLEN, um einen oder mehrere Dienste zum Start oder zum Beenden auszuwählen.

12.3 Sitzungen

Auf der Registerkarte SITZUNGEN (siehe Abbildung 12.7) sehen Sie eine Übersicht über alle aktiven Sitzungen, die mit dem ISA Server hergestellt sind. Die Anzeige wird in Echtzeit wiedergegeben.

Fünf verschiedene Sitzungstypen

In der Spalte AKTIVIERUNG sehen Sie, wann die Sitzung mit dem ISA Server hergestellt wurde. Unter SITZUNGSTYP wird angegeben, welcher Client oder welcher Typ von VPN-Verbindung die Sitzung durchführt. Dabei können die folgenden Sitzungstypen angezeigt werden:

- SecureNAT-Client-Sitzungen
- Webproxy-Client-Sitzungen
- Firewallclient-Sitzungen
- VPN-Client-Sitzungen
- Standort-zu-Standort-VPN-Sitzungen

Des Weiteren werden die IP-Adresse des Clients sowie dessen Quellnetzwerk und Hostname angezeigt. Da bei einem SecureNAT-Client

keine Authentifizierung durchgeführt wird, befindet sich auch kein Eintrag in der Spalte CLIENTBENUTZERNAME. Bei anderen Verbindungstypen wird dort der Name des angemeldeten authentifizierten Benutzers angegeben.

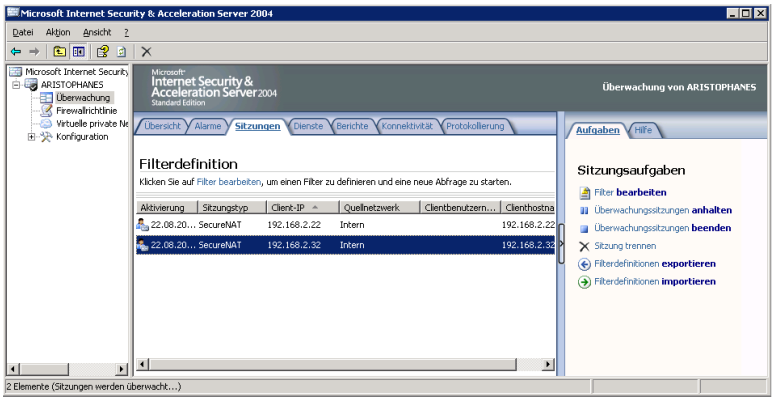


Abbildung 12.7: Echtzeitanzeige der aktiven Sitzungen des ISA Server

Filtern von Einträgen

Im Beispiel befinden sich zwar lediglich zwei Einträge in der Liste, in einem großen produktiven System kann die Liste jedoch schnell sehr lang und damit auch unübersichtlich werden. Aus diesem Grund können Filter angewendet werden, um lediglich eine Teilmenge der aktiven Sitzungen betrachten zu können. Um einen solchen Filter zu erstellen, klicken Sie im Aufgabenbereich auf den Link FILTER BEARBEITEN.

Wählen Sie dort (siehe Abbildung 12.8) unter FILTERN NACH die Kategorie wie *Clientbenutzername*, *Quellnetzwerk* usw. aus. Zusätzlich geben Sie eine der verfügbaren Bedingungen sowie den Wert an. Klicken Sie dann auf ZUR LISTE HINZUFÜGEN. Auf diese Weise können Sie mehrere Abfragen zu einem Filter hinzufügen. Sind alle Abfragen erstellt, klicken Sie auf ABFRAGE STARTEN.

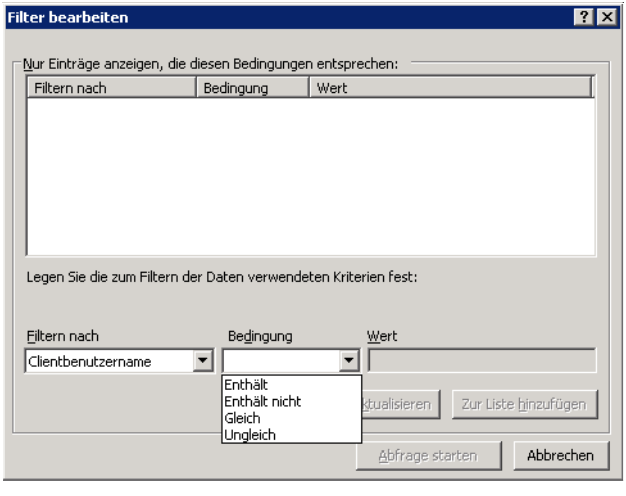


Abbildung 12.8: Anlegen eines Filters zur Abfrage einer Teilmenge der aktiven Sitzungen

Die erstellten Filter können über die entsprechenden Links im Aufgabenbereich auch exportiert und auf einem anderen ISA Server wieder importiert werden.

Beenden von Sitzungen

Des Weiteren befinden sich dort noch die beiden Links ÜBERWACHUNGSSITZUNGEN ANHALTEN und ÜBERWACHUNGSSITZUNGEN BEENDEN. Über den erstgenannten Link wird die Aktualisierung der Anzeige unterbrochen und der aktuelle Status beibehalten. Erst durch einen Klick auf ÜBERWACHUNGSSITZUNGEN FORTSETZEN wird die Anzeige wieder aktualisiert. Mit ÜBERWACHUNGSSITZUNGEN BEENDEN werden sämtliche aktuellen Einträge gelöscht und erst durch einen Klick auf ÜBERWACHUNGSSITZUNGEN STARTEN wieder neu dargestellt.

Im Kontextmenü jeder Sitzung befindet sich der Eintrag SITZUNG TRENNEN. Darüber kann der Administrator manuell die Verbindung eines Benutzers trennen. Allerdings bedeutet dies nicht, dass der Benutzer nicht mehr weiterarbeiten kann, solange für ihn noch eine Zugriffsregel existiert. Über diese Regel wird bedarfsweise sofort wieder eine neue Verbindung hergestellt. Es macht also nur Sinn, die Verbindung über den Kontextmenüeintrag zu trennen, wenn gleichzeitig auch die Zugriffsregel geändert wurde und dem Benutzer kein Zugriff mehr gestattet werden soll.

12.4 Dienste

Dienste des ISA Server

Auf der Registerkarte DIENSTE (siehe Abbildung 12.9) werden die Dienste des ISA Server, deren Status sowie die Dienstbetriebszeit angezeigt. Zusätzlich zu den ISA-Diensten werden auch weitere für diesen wichtige Dienste wie z.B. der RAS-Dienst angezeigt. Über den Link im Aufgabenbereich können die Dienste auch beendet und wieder neu gestartet werden. Bedenken Sie, dass nach verschiedenen Konfigurationsänderungen ein Neustart von Diensten erforderlich ist.

Zusätzlich kann auch hier die Aktualisierungsrate für die Anzeige auf die gewünschte Stufe angepasst werden.

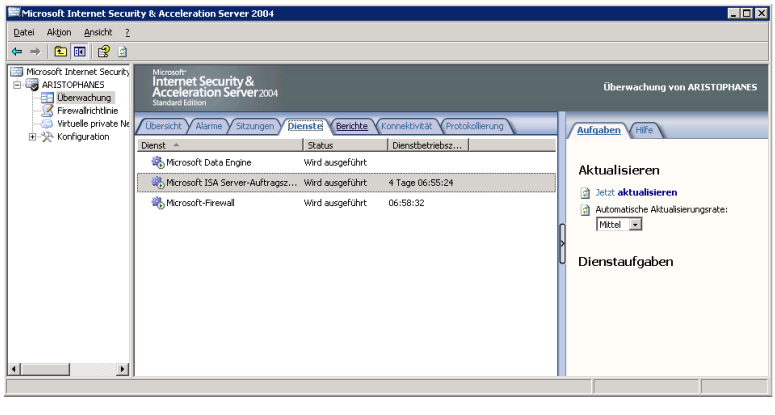


Abbildung 12.9: Übersicht über die aktuellen Dienste des ISA Server

12.5 Berichte

Detaillierte und graphische Berichte

Der ISA Server ist nicht nur in der Lage, Informationen in Protokolle zu schreiben, sondern kann diese Informationen auch zu Zusammenfassungsinhalten zusammenstellen und aus mehreren Zusammenfassungsinhalten Berichte generieren. Basierend auf den Inhalten der Berichtsdatenbank können auch graphische Berichte bereitgestellt werden. Dies geschieht über die Registerkarte BERICHTE (siehe Abbildung 12.10). Standardmäßig befinden sich dort noch keine Einträge, da die Berichte erst nach Ihren Vorstellungen erstellt werden müssen. Die Erstellung kann manuell oder auch über einen Zeitplan gesteuert erfolgen.

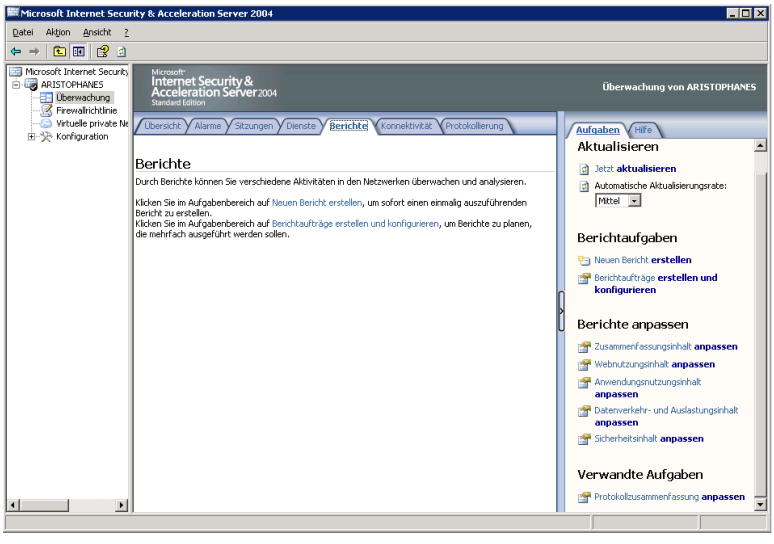


Abbildung 12.10: Über diese Registerkarte können Berichte konfiguriert werden

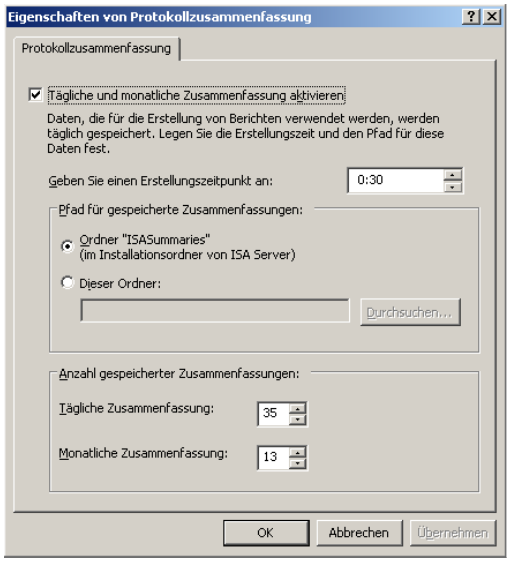
Bevor Sie mit der Konfiguration einzelner Berichte beginnen, sollten Sie über den Link PROTOKOLLZUSAMMENFASSUNG ANPASSEN im Aufgabenbereich globale Einstellungen für das Anlegen dieser Berichte treffen (siehe Abbildung 12.11). Damit tägliche und monatliche Zusammenfassungen erstellt werden können, muss diese Funktion auf der Registerkarte PROTOKOLLZUSAMMENFASSUNG aktiviert sein. Anderenfalls sind auch die anderen Optionen dieser Seite nicht wählbar. Unter ANZAHL GESPEICHERTER ZUSAMMENFASSUNGEN geben Sie jeweils die Anzahl der Zusammenfassungen an, die täglich und monatlich gespeichert werden sollen. In einer monatlichen Zusammenfassung werden sämtliche täglichen Zusammenfassungen des vergangenen Monats gespeichert. Je größer die Anzahl dieser Zusammenfassungen ist, desto mehr historische Daten können in die zu generierenden Berichte einbezogen werden. Allerdings ist für eine größere Anzahl historischer Daten auch mehr Speicherkapazität erforderlich.

Zeitpunkt der Erstellung

Über GEBEN SIE DEN ERSTELLUNGSZEITPUNKT AN wird der Zeitpunkt festgelegt, an dem die Zusammenfassungsdateien angelegt werden

sollen. Zusätzlich können Sie den standardmäßigen oder einen benutzerdefinierten Ordner für die Speicherung der Zusammenfassungsdateien auswählen. Diese Dateien tragen die Dateiendung *.ils*.

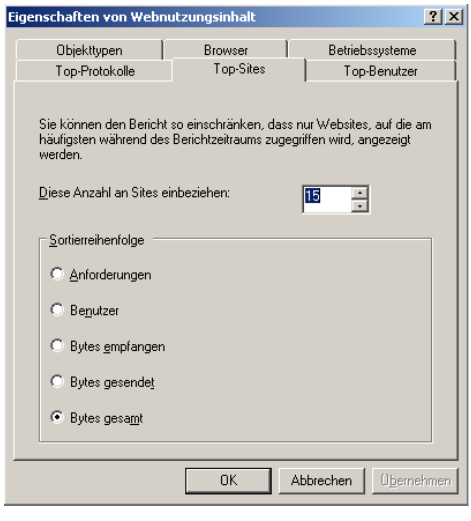
Abbildung 12.11: Globale Einstellungen für die Protokollzusammenfassung



Anpassen der Berichte

Als Nächstes können Sie die fünf verschiedenen Arten von Berichten noch individuell anpassen, bevor Sie schließlich Berichte erstellen. Wählen Sie dazu den gewünschten Link unter BERICHTE ANPASSEN. Im Beispiel in Abbildung 12.12 sehen Sie die Optionen, die für den Bericht zur Webnutzung eingestellt werden können. Weitere Informationen zu den jeweils einstellbaren Optionen erhalten Sie, indem Sie auf das Fragezeichen-Symbol klicken. Die Struktur ist für die Konfiguration sämtlicher Berichte ähnlich.

Abbildung 12.12: Optionen für den Webnutzungsbericht



12.5.1 Manuelles Erstellen von Berichten

Anlegen des Berichts

Nachdem Sie nun quasi als Vorarbeit die globalen Protokollzusammenfassungen und die Optionen für die einzelnen Berichte konfiguriert haben, können Sie darangehen, Berichte zu erstellen. Dies geschieht über den gleichnamigen Link im Aufgabenbereich. Ein Assistent führt Sie durch den Konfigurationsvorgang.

1. Zunächst geben Sie einen Namen für den Bericht an und klicken auf WEITER.
2. Im Fenster BERICHTSINHALT (siehe Abbildung 12.13) bestimmen Sie, welche der fünf verschiedenen Berichtskategorien in diesen Bericht eingeschlossen werden sollen. Klicken Sie dann auf WEITER.

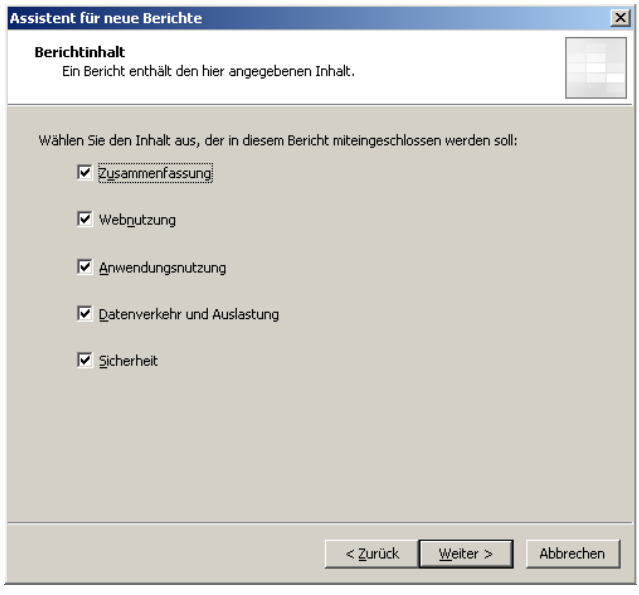


Abbildung 12.13: Auswahl der einzelnen Inhalte, die in den Bericht aufgenommen werden sollen

3. Danach wird im Fenster BERICHTSZEITRAUM (siehe Abbildung 12.14) das Start- und das Enddatum für den Bericht bestimmt. Da die Berichte immer die Zusammenfassungen der Tagesprotokolle enthalten, können in einem Bericht niemals die Daten des aktuellen Tages, sondern maximal des vorherigen Tages dargestellt werden. Klicken Sie dann auf WEITER.

Veröffentlichung in einer Freigabe ist möglich

4. Danach können Sie festlegen, ob die Berichte in einem freigegebenen Ordner gespeichert werden sollen. Markieren Sie dazu im Fenster BERICHTVERÖFFENTLICHUNG (siehe Abbildung 12.15) die Checkbox BERICHTE IN EINEM VERZEICHNIS VERÖFFENTLICHEN und geben dann einen freigegebenen Ordner an. Optional kann die Veröffentlichung auch unter einem bestimmten Benutzerkonto erfolgen. Achten Sie jedoch darauf, dass das gewählte Konto entsprechende Schreibberechtigungen besitzt, um die Berichtsdatei in den Ordner zu schreiben. Klicken Sie dann auf WEITER.

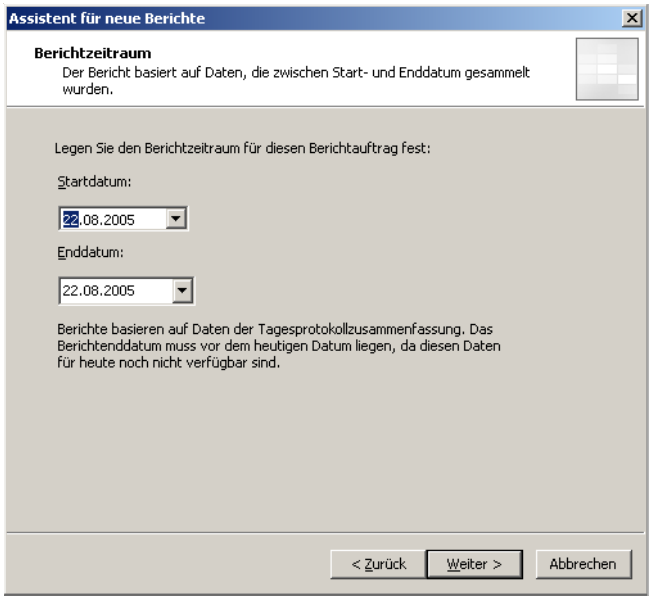


Abbildung 12.14: Auswahl des Zeitraums, der in den Bericht einbezogen werden soll

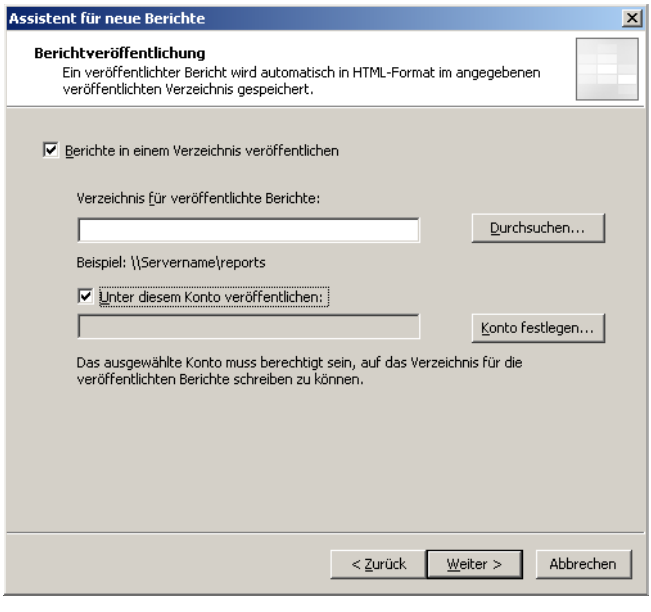


Abbildung 12.15: Optional kann der Bericht in einer Freigabe veröffentlicht werden

5. Im Fenster E-MAIL-BENACHRICHTIGUNG SENDEN (siehe Abbildung 12.16) können Sie optional nach Abschluss des Berichts zur Information eine E-Mail an einen oder mehrere Benutzer schicken lassen. Auch der Text dieser Nachricht ist frei wählbar. Klicken Sie dann auf WEITER und beenden Sie den Assistenten.

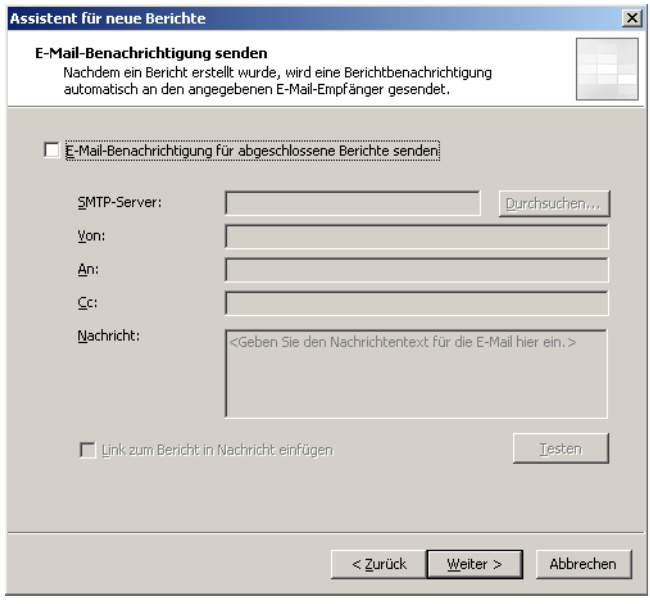


Abbildung 12.16: Über den Abschluss der Berichtserstellung kann per E-Mail informiert werden

Status des Berichts

Nachdem der Bericht erstellt wurde, wird dieser auf der Registerkarte BERICHTE angezeigt. Warten Sie ab, bis in der Spalte STATUS nicht mehr *Erstellungsvorgang*, sondern *Abgeschlossen* steht. Dies kann nach Umfang des Berichts und Auslastung des ISA Server einen Moment dauern. Um die Inhalte dieses Berichts zu sehen, wählen Sie aus dem Aufgabenbereich AUSGEWÄHLTEN BERICHT ANZEIGEN. Die Anzeige des Berichts erfolgt im Webbrowser. Auf der linken Seite sind die Inhalte der einzelnen Berichte aufgelistet, so dass Sie schnell zum gewünschten Teil des Berichts navigieren können.

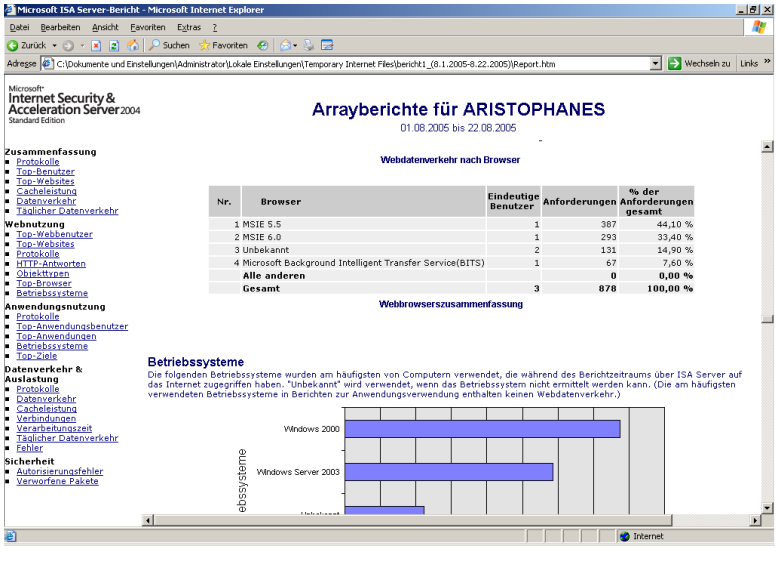


Abbildung 12.17: Ausschnitt aus einem ISA Server-Bericht

12.5.2 Zeitgesteuerte Berichtserstellung

Nutzen eines Zeitplans

Neben der eben beschriebenen manuellen Erstellung von Berichten kann dieser Vorgang auch automatisch zu festen Zeiten erfolgen. Um diese Zeitplanung festzulegen, klicken Sie im Aufgabenbereich auf BERICHTSAUFTRÄGE ERSTELLEN UND KONFIGURIEREN. Der Vorgang entspricht bis auf ein zusätzliches Fenster dem manuellen Erstellen von Berichten.

1. Sie erhalten zunächst die leere Seite BERICHTAUFTRÄGE, auf der über HINZUFÜGEN ein neuer Auftrag erstellt werden kann. Es wird ein Assistent gestartet.
2. Geben Sie zunächst den Namen des Berichts an und wählen dann die Inhalte des Berichts aus.
3. Danach erhalten Sie das zusätzliche Fenster BERICHTAUFTRAGSZEITPLAN (siehe Abbildung 12.18). Dort können Sie wählen, zu welchem Zeitpunkt der Bericht erstellt werden soll. Beachten Sie, dass Sie bei der Auswahl *Monatlich, an folgendem Tag* nur einen Tag auswählen, der in jedem Monat vorkommt. Ist zum Beispiel der 31. gewählt, würde dies in Monaten mit 30 Tagen oder im Februar zu Problemen führen. Klicken Sie dann auf WEITER.

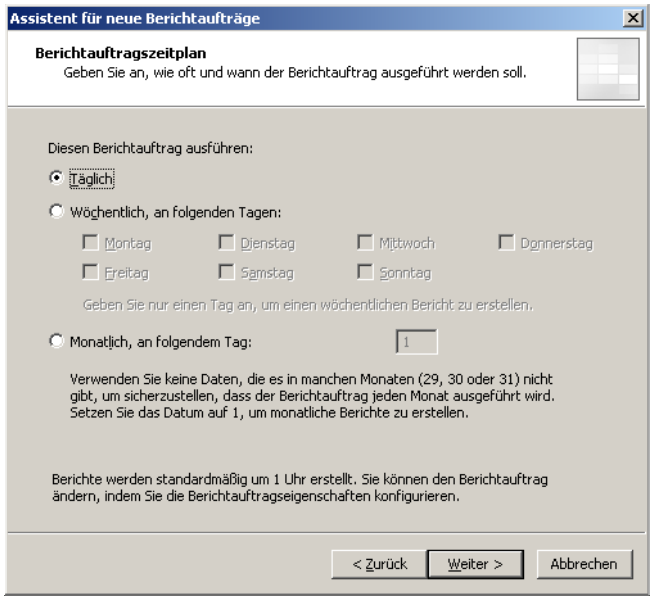


Abbildung 12.18: Bestimmen des Zeitplans, nach dem Berichte erstellt werden sollen

4. Führen Sie den Assistenten wie im letzten Kapitel beschrieben zu Ende.

Berichtsaufträge

Sobald der Assistent abgeschlossen ist, befindet sich der neue Auftrag in der Liste BERICHTSAUFTRÄGE (siehe Abbildung 12.19). Hier kann er später modifiziert oder gelöscht werden. Auch die sofortige Ausführung eines geplanten Auftrags ist über JETZT AUSFÜHREN möglich.

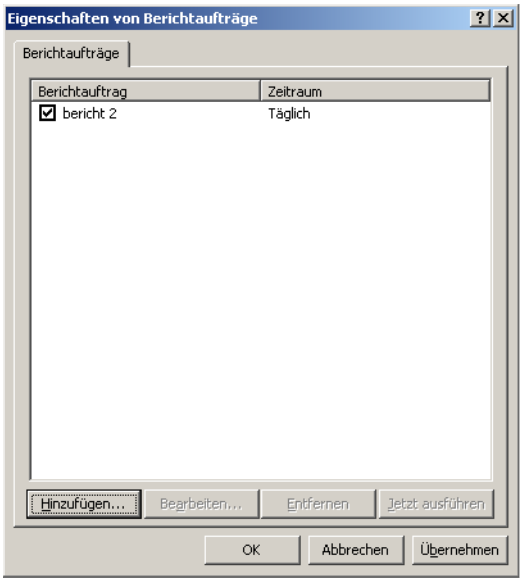


Abbildung 12.19: Übersicht über die geplanten Berichtsaufträge

Wird für die Protokollierung (siehe Kapitel 12.7) die Option zur Speicherung auf einem SQL-Server gewählt, können auf dem ISA Server selbst nicht mehr wie eben beschrieben Berichte erstellt werden, da sämtliche Auswertungsdaten direkt an den SQL-Server gesendet werden.

12.6 Konnektivität

Regelmäßige Prüfung von Verbindungen

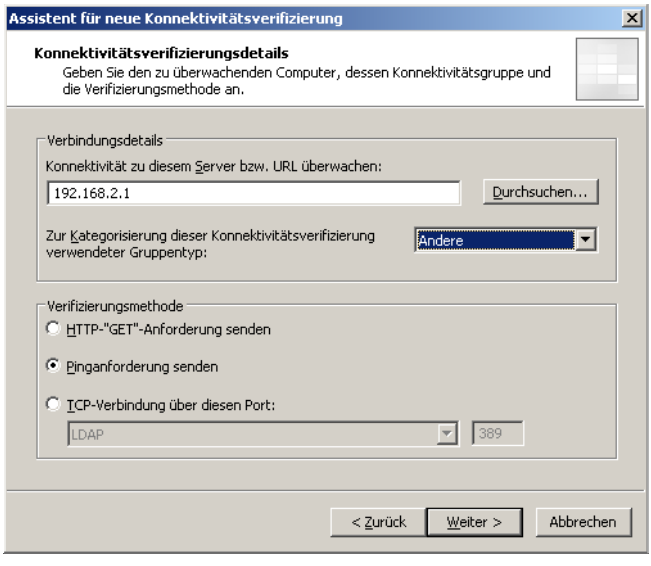
Mit Hilfe der Konnektivität können Verbindungen zwischen dem ISA Server und ausgewählten anderen Servern des internen oder externen Netzwerks geprüft werden. In regelmäßigen Abständen wird dabei geprüft, ob die Verbindung zwischen den beiden Servern noch besteht. Standardmäßig sind keine Konnektivitätsverifizierungen vorhanden, sondern müssen erst manuell erstellt werden. Klicken Sie dazu im Aufgabenbereich auf NEUE KONNEKTIVITÄTSVERIFIZIERUNG ERSTELLEN. Ein Assistent geleitet Sie durch den Vorgang.

1. Geben Sie zunächst einen passenden Namen für die Konnektivitätsverifizierung an und klicken auf WEITER.
2. Im Fenster KONNEKTIVITÄTSVERIFIZIERUNGSDETAILS (siehe Abbildung 12.20) tragen Sie zunächst den Namen des Servers, dessen IP-Adresse oder dessen URL ein. Fügen Sie diesen Server zu einer der

folgenden Gruppentypen hinzu, um so in der Übersicht schneller erkennen zu können, in welchem Bereich Verbindungsprobleme aufgetreten sind:

- ACTIVE DIRECTORY
- ANDERE
- DHCP
- DNS
- VERÖFFENTLICHTE SERVER
- WEB (INTERNET)

Abbildung 12.20: Festlegen der Konnektivitäts-verifizierung



Verifizierung und Prüfmethode

Zusätzlich müssen Sie noch eine Verifizierungsmethode bestimmen. Je nach gewählter Kategorie des zu prüfenden Servers wird jeweils die geeignetste Methode automatisch markiert. Dazu stehen die drei folgenden Optionen zur Verfügung, von denen jeweils nur eine pro Assistent gewählt werden kann:

- HTTP-„GET"-ANFORDERUNG SENDEN: Diese Anfrage wird zu einem Server gesendet um herauszufinden, ob dieser Webanfragen beantworten kann. Sobald diese Option gewählt wird, wird automatisch die Systemrichtlinie aktiviert, die dem ISA Server den http/https-Zugang zu sämtlichen Netzwerken gestattet.
- PING-ANFORDERUNG: Das Senden einer ICMP-Anforderung ist der simpelste der drei Tests. Durch das Senden einer Antwort auf diese Anfrage bestätigt der Server lediglich, dass zu ihm eine Verbindung hergestellt werden kann. Dies bedeutet jedoch noch nicht, dass auf diesem auch sämtliche Dienste korrekt konfiguriert sind.

- TCP-ANFORDERUNG: Es wird eine TCP-Verbindung zu dem anzugebenden Port hergestellt. So kann gezielt geprüft werden, ob ein bestimmter Dienst korrekt auf dem Server ausgeführt wird.

3. Klicken Sie dann auf WEITER und beenden Sie den Assistenten. Übernehmen Sie anschließend die Konfigurationsänderungen. Die neue Verifizierung und ihr Status werden auf der Registerkarte KONNEKTIVITÄT angezeigt.

Schwellwert zum Auslösen eines Alarms

Über die Eigenschaften der Verifizierung können noch zwei zusätzliche Optionen bestimmt werden, die über den Assistenten nicht eingestellt werden können. Wechseln Sie dazu auf die Registerkarte EIGENSCHAFTEN (siehe Abbildung 12.21). Sie können dort zum einen unter SCHWELLENWERT ein Zeitlimit in Millisekunden definieren, innerhalb dessen die Antwort vom Server erfolgen muss. Zum anderen können Sie noch festlegen, dass ein Alarm ausgelöst wird, wenn die Antwort des Servers nicht innerhalb des festgelegten Limits erfolgt. Wurden hier Änderungen vorgenommen, muss diese Konfigurationsänderung übernommen werden.

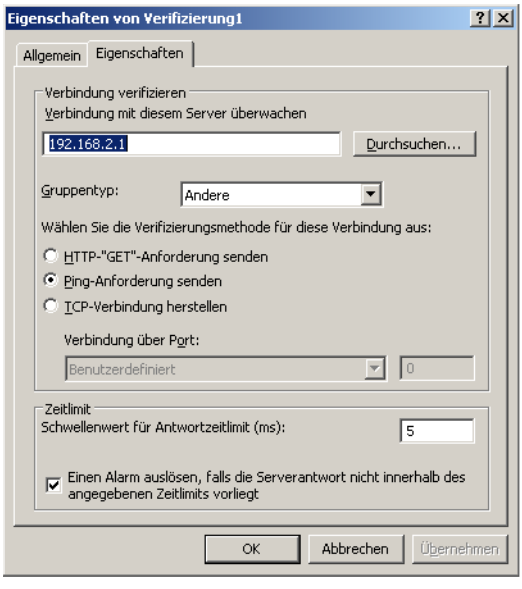


Abbildung 12.21: Zusätzliche Optionen für die Konnektivitätsverifizierung

Der jeweils aktuelle Status sowie die Optionen der Konnektivitätsverifizierung werden in der Liste angezeigt (siehe Abbildung 12.22).

Abbildung 12.22: Übersicht über eine Konnektivitätsverifizierung und deren Ergebnis

12.7 Protokollierung

Standardmäßig aktiviert

Nach der Installation des ISA Server ist standardmäßig die Protokollierung für die ein- und ausgehenden Pakete über die Firewall-, Webproxy- und Nachrichtenüberwachungsprotokollierung aktiviert. Jeder dieser drei Dienste kann jedoch separat deaktiviert werden. Die Protokolldaten können entweder als Textdatei oder in eine MSDE- bzw. SQL-Server Datenbank gespeichert werden.

Damit die Protokollierung nicht durch ein zu hohes Maß an protokollierten Daten unüberschaubar wird und Daten möglicherweise nicht mehr ordentlich ausgewertet werden können, müssen Sie bei der Konfiguration der Protokolle genau bestimmen, welche Ereignisse protokolliert werden sollen. Dies ist unabhängig von der Art der Speicherung.

12.7.1 Protokolle als Textdatei

Simpelste Speichermethode

Wird eine Textdatei für die Protokolle verwendet, so können die Informationen in Echtzeit in der ISA-mmc angezeigt werden. Allerdings besteht nicht die Möglichkeit, per Abfrage auf ältere Protokolldaten zuzugreifen. Sollen die Protokolle als Textdatei gespeichert werden, können dazu zwei verschiedene Formate benutzt werden:

- *ISA Server-Dateiformat*: Alle Werte werden kommasepariert aufgezeichnet. Die Aufzeichnung betrifft jedoch nur ausgewählte Felder. Es sind Daten und Direktiven enthalten. Sämtliche Zeitangaben werden als GMT angegeben.
- *Erweitertes W3C-Protokollierungsdateiformat*: Alle Werte werden tabulatorsepariert aufgezeichnet. Leere Felder werden durch einen Strich kenntlich gemacht. Es sind nur Daten und keine Direktiven enthalten. Für sämtliche Zeitangaben wird die lokale Zeit verwendet.

12.7.2 Protokolle in der MSDE-Datenbank

Zugriff auf Daten des lokalen ISA Server

Bei einer Aufzeichnung der Daten in einer MSDE-Datenbank können diese in Echtzeit in der ISA-mmc angezeigt werden oder die Abfrage historischer Daten ist möglich. Für diese Abfragen können Filter eingesetzt werden. In der MSDE-Datenbank können lediglich die Protokollierungen des Firewall- und Webproxy-Dienstes vorgenommen werden. Die Einträge der Nachrichtenüberwachung können nur in eine Datei geschrieben werden.

Wird die Protokollierung in der MSDE gewählt, so beansprucht diese Form der Protokollierung mehr Ressourcen als die Speicherung in einer Textdatei. Dies gilt für die Ressourcen Prozessor und Festplatte.

12.7.3 Protokolle in der SQL-Server-Datenbank

Zugriff auf Daten mehrerer ISA Server

Damit die Protokollierung in der SQL-Server-Datenbank erfolgen kann, muss sich selbstverständlich ein SQL-Server im Netzwerk befinden. Im Gegensatz zu den beiden anderen Verfahren kann ein SQL-Server auch die Protokolldaten mehrerer ISA Server speichern. Zusätzlich können die Daten über wesentlich komplexere Abfragen als bei der Speicherung in der MSDE-Datenbank ausgewertet werden.

12.7.4 Erstellen von Protokollen

Über den Aufgabenbereich der Überwachung können die Protokolle für Firewall-, Webproxy- und SMTP-Nachrichtenüberwachung erstellt und konfiguriert werden. Standardmäßig sind alle drei Protokolle aktiviert, können aber deaktiviert werden.

Firewallprotokollierung

32 vordefinierte Felder

Um die Firewall-Protokollierung zu konfigurieren, klicken Sie auf den entsprechenden Link im Aufgabenbereich. Auf der Registerkarte PROTOKOLLIERUNG können Sie die Art der Protokollierung bestimmen. Weitere Hinweise dazu finden Sie in Kapitel 12.7.5. Auf der Registerkarte FELDER (siehe Abbildung 12.23) können Sie aus 32 Feldern auswählen, die in die Protokollierung eingeschlossen werden können. Die Bedeutung der einzelnen Felder finden Sie in der folgenden Tabelle.

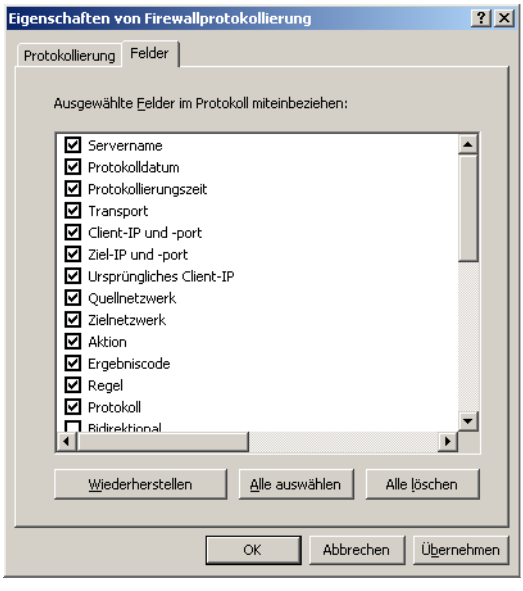


Abbildung 12.23: Die Felder der Firewall-Protokollierung

Tabelle 12.2: Die Felder für die Firewall-Protokollierung

Feld	Beschreibung
Servername	Name des ISA Server
Protokolldatum	Datum des Eintrags
Protokollierungszeit	Zeitpunkt des Eintrags
Transport	Gibt das Transportprotokoll (TCP oder UDP) an.
Client-IP und –Port	IP-Adresse und Port des Quellcomputers
Ziel-Ip und –Port	IP-Adresse und Port des Zielcomputers
Ursprüngliche Client-IP	IP-Adresse des die Anfrage stellenden Clients
Quellnetzwerk	Netzwerk des Quellcomputers
Zielnetzwerk	Netzwerk des Zielcomputers
Aktion	Die Aktion beschreibt die Verarbeitung eines Pakets oder die Behandlung einer Verbindung durch den ISA Server. Eine Verbindung kann z.B. hergestellt oder getrennt sein.
Ergebniscode	Detaillierte Information über den Statuscode der jeweiligen Anforderung
Regel	Für die Herstellung bzw. Verweigerung der Verbindung benutzte Regel. Bei der Blockade des Netzwerkverkehrs vor Prüfung einer Regel wird keine Regel angezeigt.
Protokoll	Gibt das benutzte Protokoll an. Kann dieses nicht ermittelt werden, wird als Wert *Nicht identifizierter IP-Datenverkehr* eingetragen.
Bidirektional	Bei einer bidirektionalen Abfrage (DNS-Abfrage) wird eine Antwort erwartet, bei einer unidirektionalen Abfrage (Broadcast) nicht.
Bytes gesendet	Anzahl der Bytes, die bei der aktuellen Sitzung an den externen Server gesendet werden
Delta der gesendeten Bytes	Anzahl der während der aktuellen Sitzung schon an den externen Server gesendeten Bytes
Bytes empfangen	Anzahl der Bytes, die bei der aktuellen Sitzung an vom internen Client empfangen werden
Delta der empfangenen Bytes	Anzahl der während der aktuellen Sitzung schon vom internen Client empfangenen Bytes
Verarbeitungszeit	Angabe der Zeit in Millisekunden, die vom ISA Server für die Verarbeitung der Anfrage benötigt werden
Verarbeitungszeitdelta	Bisherige Verbindungsdauer
Quellproxy	Wird momentan nicht benutzt

Feld	Beschreibung
Zielproxy	Wird momentan nicht benutzt
Clienthostname	Wird momentan nicht benutzt
Zielhostname	Wird momentan nicht benutzt
Clientbenutzer-name	Erfordert der ISA Server eine Authentifizierung, wird der Name des Benutzers angegeben, ansonsten wird der Name *anonymous* gesetzt.
Client-Agent	Clientanwendungstyp
Sitzungskennung	Kennung der Verbindungen einer Sitzung
Verbindungs-kennung	Kennung von zum gleichen Socket gehörenden Paketen
Netzwerkschnitt-stelle	Primäre IP-Adresse des Netzwerkadapters, der die Verbindung entgegennimmt
Roh-IP-Header	Roh-IP-Header des Pakets
Rohnutzlast	Daten der Rohnutzlast des Pakets
Client-IP	IP-Adresse des Clients, der die Anforderung stellt

Webproxy-Protokollierung

28 vordefinierte Felder

Um die Webproxy-Protokollierung zu konfigurieren, klicken Sie auf den entsprechenden Link im Aufgabenbereich. Auf der Registerkarte PROTOKOLLIERUNG können Sie die Art der Protokollierung bestimmen. Weitere Hinweise dazu finden Sie in Kapitel 12.7.5. Auf der Registerkarte FELDER (siehe Abbildung 12.24) können Sie aus 28 Feldern auswählen, die in die Protokollierung eingeschlossen werden können. Die Bedeutung der einzelnen Felder finden Sie in der folgenden Tabelle.

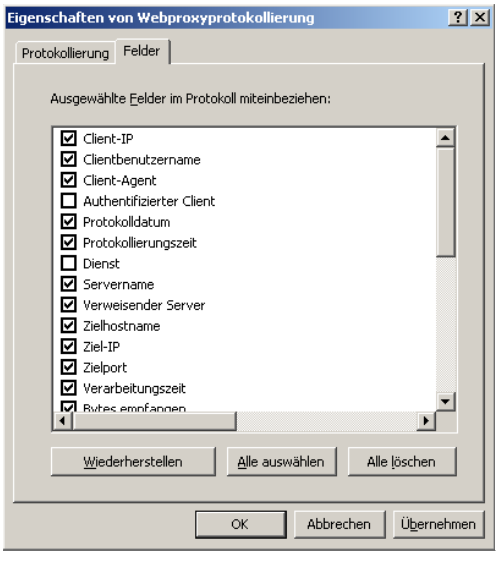


Abbildung 12.24: Die Felder der Webproxy-Protokollierung

Tabelle 12.3: Die Felder für die Webproxy-Protokollierung

Feld	Beschreibung
Clientbenutzer-name	Erfordert der ISA Server eine Authentifizierung, wird der Name des Benutzers angegeben, ansonsten wird der Name *anonymous* gesetzt.
Client-Agent	Clientanwendungstyp
Authentifizierter Client	Beschreibt, ob der Client am ISA Server authentifiziert wurde oder nicht
Protokolldatum	Datum des Protokolleintrags
Protokollierungs-zeit	Zeitpunkt des Protokolleintrags
Dienst	W3proxy = ausgehende Anfrage, w3reverseproxy = eingehende Anfrage
Servername	Name des ISA Server
Verweisender Server	Wird momentan nicht benutzt
Zielhostname	FQDN des Zielcomputers, an den die Anfrage gerichtet ist
Ziel-IP	IP-Adresse des Zielcomputers
Zielport	Port des Zielcomputers
Verarbeitungszeit	Angabe der Zeit in Millisekunden, die vom ISA Server für die Verarbeitung der Anfrage benötigt wird
Bytes empfangen	Anzahl der Bytes, die bei der aktuellen Sitzung vom internen Client empfangen werden
Bytes gesendet	Anzahl der Bytes, die bei der aktuellen Sitzung an den externen Server gesendet werden
Protokoll	Benutztes Protokoll, z.B. http oder ftp
Transport	Gibt das Transportprotokoll (TCP oder UDP) an
http-Methode	Die in der Anfrage benutzte http-Methode, z.B. GET, POST usw.
URL	Gibt die URL der angeforderten Webseite oder des Objekts an.
MIME-Typ	MIME-Typ des angeforderten Objekts
Objektquelle	Bezugsquelle des Objekts (Internet, Cache des ISA Server)
http-Statuscode	Statuscode der http-Verbindung
Cacheinforma-tionen	Der Cache-Status des Objekts besagt, aus welchem Grund ein Objekt in den Cache des ISA Server geschrieben wurde oder nicht

Feld	Beschreibung
Regel	Für die Herstellung bzw. Verweigerung der Verbindung benutzte Regel. Bei der Blockade des Netzwerkverkehrs vor Prüfung einer Regel wird keine Regel angezeigt.
Filterinformationen	Zusätzliche Informationen zum Webfilter, z.B. warum eine Verbindung nicht hergestellt wurde
Quellnetzwerk	Netzwerk des Quellcomputers
Zielnetzwerk	Netzwerk des Zielcomputers
Fehlerinformationen	Fehlernummer des Webproxy
Aktion	Die Aktion beschreibt die Verarbeitung eines Pakets oder die Behandlung einer Verbindung durch den ISA Server. Eine Verbindung kann z.B. hergestellt oder getrennt sein.

SMTP-Nachrichtenüberwachung

Acht vordefinierte Felder

Um die SMTP-Nachrichtenüberwachung zu konfigurieren, klicken Sie auf den entsprechenden Link im Aufgabenbereich. Auf der Registerkarte PROTOKOLLIERUNG können Sie die Art der Protokollierung bestimmen. Weitere Hinweise dazu finden Sie in Kapitel 12.7.5. Auf der Registerkarte FELDER (siehe Abbildung 12.25) können Sie aus acht Feldern auswählen, die in die Protokollierung eingeschlossen werden können. Die Bedeutung der einzelnen Felder finden Sie in der folgenden Tabelle.

Tabelle 12.4: Die Felder für die Nachrichtenüberwachung

Feld	Beschreibung
Protokolldatum	Datum des Protokolleintrags
Protokollierungszeit	Zeit des Protokolleintrags
Sender	Absender der E-Mail
Empfänger	Empfänger der E-Mail
Betreff	Betreff der E-Mail
Nachrichtenkennung	Die vom versendenden SMTP-Server generierte eindeutige Kennung einer E-Mail
Aktion	Vom ISA Server ausgeführte Aktion (z.B. Weiterleiten, Löschen) beim Erhalt der E-Mail
Ursache	Grund für den Protokollierungseintrag, z.B. Verletzung einer SMTP-Regel, auf Grund derer eine E-Mail gelöscht wird

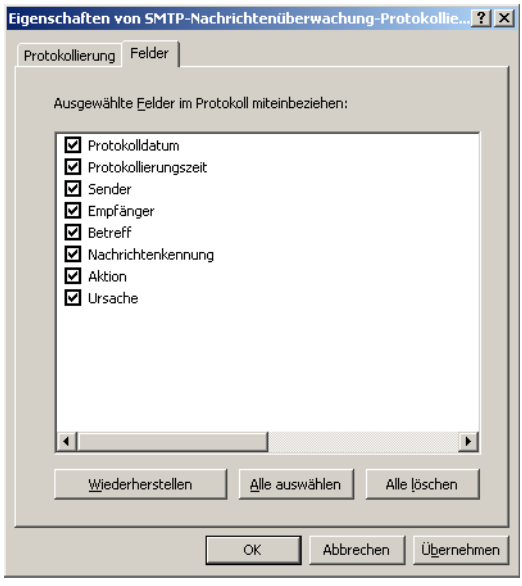


Abbildung 12.25: Die Felder der SMTP-Nachrichtenüberwachung

12.7.5 Speicherung der Protokolldateien

Speicheroptionen

Bei der Konfiguration aller drei Protokolldateien wird auf der Registerkarte PROTOKOLLIERUNG (siehe Abbildung 12.26) festgelegt, in welcher Form die Daten gespeichert werden sollen.

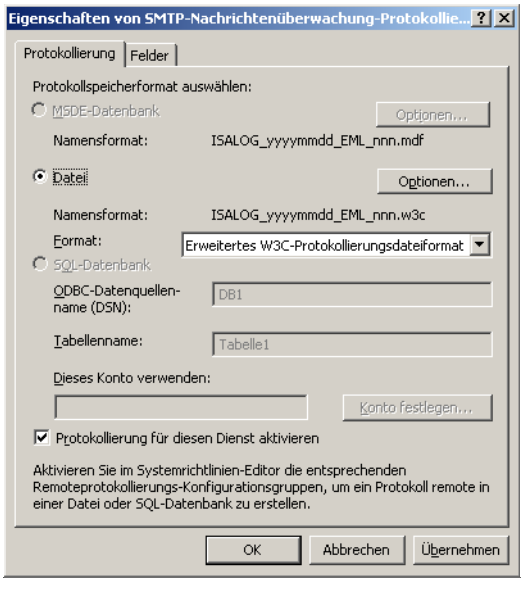


Abbildung 12.26: Auswahl der Speichermethode für die Protokolldateien

MSDE-Datenbank und Textdatei

Speicherzeit und Dateigröße

Soll die Speicherung in der MSDE-Datenbank erfolgen, muss auf dem ISA Server die MSDE installiert sein und der zugehörige SQL-Server-Dienst Manager gestartet sein. Das Protokoll wird bei der Speicherung in der MSDE-Datenbank als *.mdf*-Datei gespeichert. Mit einem Klick auf OPTIONEN wird eine weitere Registerkarte verfügbar (siehe Abbildung 12.27). Dort können Sie den vordefinierten Ordner \ISALOGS oder einen anderen Ordner zur Speicherung der Protokolldatei angeben. Ferner kann eine maximale Größe für die Protokolldatei festgelegt werden. Die Maximalgröße der Protokolldatei liegt bei acht GB. Sofern diese Größe überschritten wird, werden neue Dateien angelegt. Bei der Protokollierung wird für jeden Tag eine neue Protokolldatei angelegt. Um sicherzustellen, dass wegen der Protokolldatei nicht der gesamte Speicher eines Laufwerks verbraucht wird, können Sie unter BEIZUBEHALTENDER FREIER SPEICHERPLATZ einen Wert bestimmen, der nicht für die Protokolldateien verwendet werden darf. Ist die Maximalgröße der Protokolldatei erreicht, können entweder alte Protokolldaten gelöscht oder aber keine neuen Dateien hinzugefügt werden. In aller Regel dürfte die Wahl der ersten Option mehr Sinn machen, da auf diese Weise immer die aktuellen Protokolleinträge vorhanden sind. Um die Protokolldatei nicht zu groß werden zu lassen, kann unter DATEIEN LÖSCHEN, DIE ÄLTER SIND ALS (TAGE) die Anzahl der Tage angegeben werden, für die nur die Protokolldateien beibehalten werden sollen. Nur wenn die Speicherung der Datei auf einem mit NTFS formatierten Datenträger erfolgt, ist die Option PROTOKOLLDATEIEN KOMPRIMIEREN verfügbar. Dadurch werden sämtliche Dateien komprimiert, um zusätzlich Speicherplatz zu sparen. Bestätigen Sie die Optionen mit OK.

Die Schaltfläche OK ist nicht verfügbar, wenn der Dienst *MSSQLServerADHelper* nicht gestartet ist. Sie erkennen dies daran, dass das MSDE-Symbol im Systemtray keinen Status anzeigt.

Dieselben Optionen sind auch verfügbar, wenn Sie für die Speicherung eine Textdatei auswählen.

Zwei Speicherformate der Textdatei

Soll die Speicherung in einer Textdatei erfolgen, müssen Sie festlegen, ob die Protokolldatei im ISA Server-Dateiformat (*.iis*-Datei) oder als erweitertes W3C-Protokollierungsdateiformat (*.w3c*-Datei) gespeichert werden soll. Die Unterschiede zwischen diesen beiden Formen wurden bereits in Kapitel 12.7.1 dargestellt.

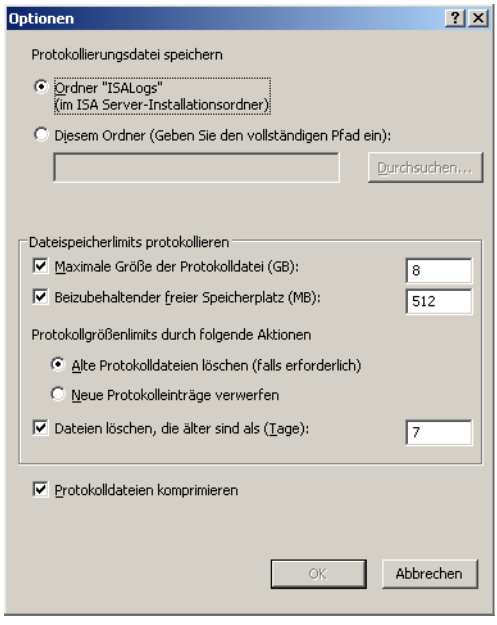


Abbildung 12.27: Weitere Optionen für die Protokollierung

SQL-Server-Datenbank

Am aufwendigsten ist die Konfiguration für die Speicherung der Protokolldateien in einer SQL-Server-Datenbank. Die folgenden Beschreibungen beziehen sich auf den SQL-Server 2000.

Sofern die Protokollierung auf einem SQL-Server erfolgt, können auf dem ISA Server nicht mehr wie in Kapitel 12.5 beschrieben Berichte erstellt werden, da sämtliche Daten direkt auf den SQL-Server geschickt werden.

Für die Konfiguration sind zahlreiche Schritte erforderlich.

1. Als Erstes muss auf dem SQL-Server eine Datenbank eingerichtet werden. Starten Sie dazu den ENTERPRISE MANAGER des SQL-Servers aus dem Startmenü.
2. Erstellen Sie dort eine neue Datenbank, z.B. namens ISA-Protokollierung und bestimmen Sie für diese die Datendateien und das Transaktionsprotokoll.

Vordefinierte Skripte

3. Legen Sie dann die Installations-CD des ISA Server 2004 ein. Auf dieser CD befinden sich zwei Skripte, über die die neu erstellte SQL-Datenbank für die Protokollierung der Firewall-Protokollierung und der Webproxy-Protokollierung vorbereitet wird.
4. Wählen Sie dann aus dem Startmenü den QUERY ANALYZER des SQL-Server. Authentifizieren Sie sich und wählen dann das Menü DATEI/ÖFFNEN.

5. Navigieren Sie dort zum folgenden Pfad: `CD-Laufwerk:\FPC\Program Files\Microsoft ISA Server\fwsrv.sql`. Es werden die Inhalte der gewählten Konfigurationsdatei angezeigt.
6. Wählen Sie dann die Datenbank für die ISA-Protokollierung aus und starten Sie das Skript über die entsprechende Schaltfläche (siehe Abbildung 12.28).

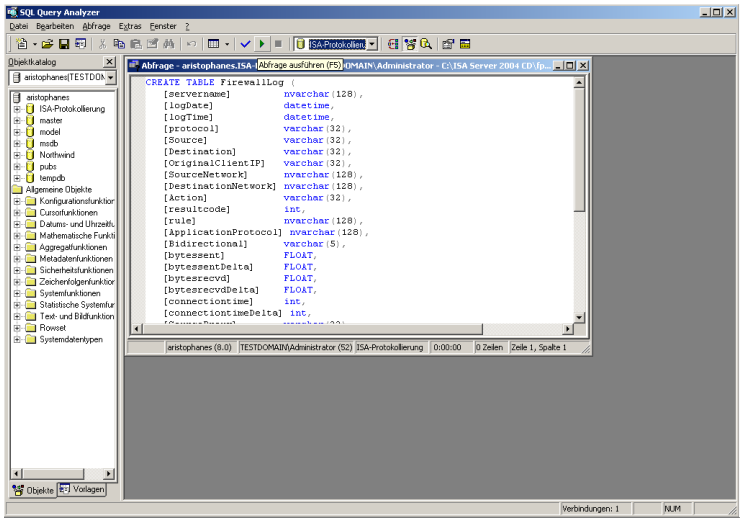
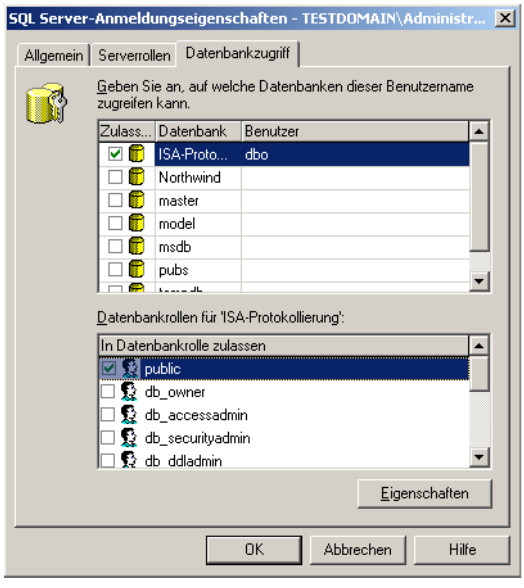


Abbildung 12.28: Ausführen des Konfigurationsskripts

7. Wählen Sie danach die zweite Konfigurationsdatei aus. Diese befindet sich im Verzeichnis `CD-Laufwerk:\FPC\Program Files\Microsoft ISA Server\w3proxy.sql`.
8. Als Nächstes sollten Sie ein Benutzerkonto bestimmen, über das der Zugriff auf die Daten in den SQL-Server-Datenbanken erfolgen darf. Damit die ISA-Protokollierungsdaten in die Datenbank geschrieben werden dürfen, muss ein Benutzerkonto mit einem Kennwort angegeben werden. Starten Sie dazu den ENTERPRISE MANAGER und navigieren Sie zum Eintrag SICHERHEIT/BENUTZERNAMEN. Fügen Sie hier das gewünschte Benutzerkonto hinzu. Wichtig hierbei ist die Wahl der Authentifizierungsmethode. Sie haben dazu zwei Möglichkeiten:
   - WINDOWS-AUTHENTIFIZIERUNG: Es werden nur Benutzerkonten der Windows-Domäne verwendet. So kann der Zugriff mit Hilfe dieser Benutzerdaten erfolgen, ohne dass eine erneute Authentifizierung für den Zugriff auf die SQL-Datenbank erforderlich ist.
   - SQL SERVER-AUTHENTIFIZIERUNG: Bei dieser Form können auch Benutzerkonten verwendet werden, die sich nicht in der Domäne befinden. Dadurch kann einer zweite Authentifizierung für den Zugriff auf die SQL-Daten erforderlich werden.

9. Stellen Sie sicher, dass der gewählte Benutzer für die Datenbank ISA-Protokollierung Zugriff besitzt (siehe Abbildung 12.29). Dies geschieht über die EIGENSCHAFTEN des Benutzerkontos auf der Registerkarte DATENBANKZUGRIFF.

Abbildung 12.29: Konfiguration des Datenbankzugriffs für den Benutzer



10. Des Weiteren muss es dem Benutzer ermöglicht werden, Daten in der Datenbank aktualisieren zu können. Navigieren Sie dazu zum Eintrag DATENBANKEN/ISA-PROTOKOLLIERUNG/TABELLEN und wählen Sie die Eigenschaften von FIREWALLLOG. Klicken Sie dann auf BERECHTIGUNGEN und stellen Sie sicher, dass für den Benutzer die Berechtigungen *SELECT* sowie *INSERT* aktiviert sind.
11. Wiederholen Sie Schritt 10 für die Tabelle WEBPROXYLOG. Damit sind die Datenbankkonfigurationen abgeschlossen.
12. Als Nächstes muss auf dem ISA Server eine ODBC-Schnittstelle eingerichtet werden, über die eine Verbindung zum SQL-Server hergestellt wird. Öffnen Sie dazu auf dem ISA Server in der VERWALTUNG die mmc DATENQUELLEN (ODBC).
13. Wechseln Sie dort auf die Registerkarte SYSTEM-DSN und klicken auf HINZUFÜGEN. Im Fenster NEUE DATENQUELLE ERSTELLEN wählen Sie den Eintrag SQL SERVER und klicken auf FERTIG STELLEN.
14. Im Fenster NEUE DATENQUELLE FÜR SQL SERVER ERSTELLEN (siehe Abbildung 12.30) geben Sie einen Namen für den Datenquellenverweis, eine Beschreibung sowie den Namen des SQL-Servers an und klicken auf WEITER.

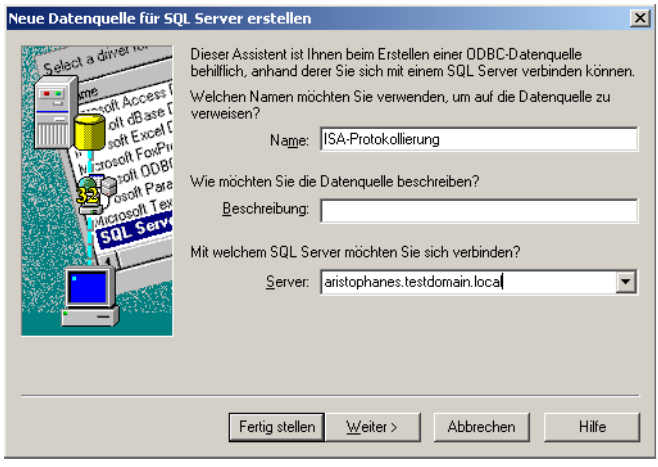


Abbildung 12.30: Wahl des SQL-Servers für die ODBC-Datenquelle

15. Danach wird die Authentifizierungsmethode gewählt. Wählen Sie dort die SQL-Server-Authentifizierung aus (siehe Abbildung 12.31). Klicken Sie danach auf WEITER.

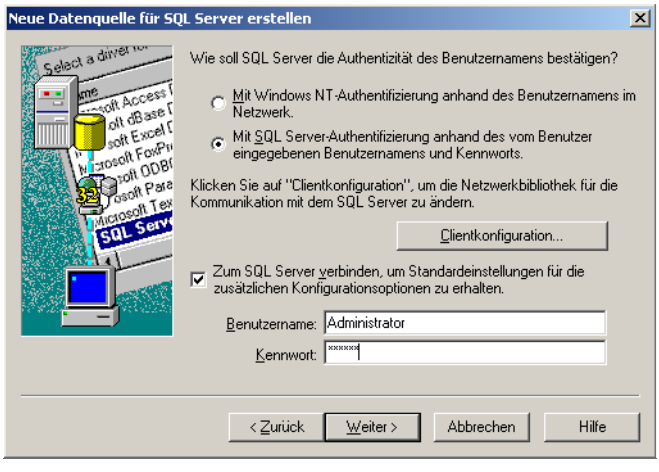


Abbildung 12.31: Auswahl der Authentifizierungsmethode

16. Im nächsten Fenster wird die Datenbank ausgewählt. Tragen Sie hier die Datenbank *ISA-Protokollierung* ein (siehe Abbildung 12.32). Klicken Sie dann auf WEITER. In dem danach folgenden Fenster können die Einstellungen beibehalten werden. Klicken Sie dann auf FERTIG STELLEN.

Testen der Konfiguration

17. Klicken Sie dann auf DATENQUELLE TESTEN (siehe Abbildung 12.33), um zu prüfen, ob der ISA Server eine Verbindung mit der SQL-Datenbank herstellen kann. Erhalten Sie das Ergebnis TESTS ERFOLGREICH ABGESCHLOSSEN, wurde die Konfiguration korrekt durchgeführt. Klicken Sie auf OK.

Abbildung 12.32: Auswahl der Datenbank

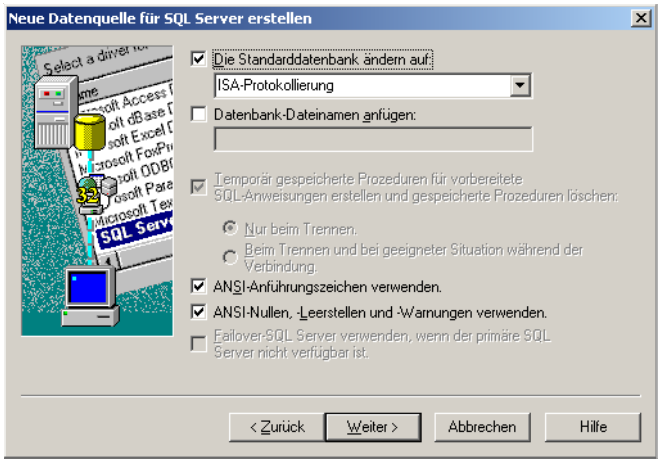
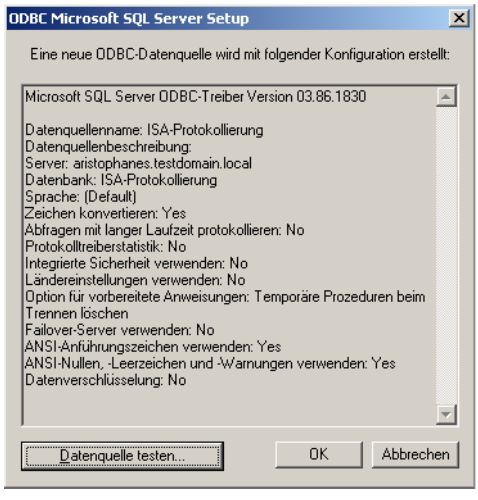


Abbildung 12.33: Vor der endgültigen Erstellung sollte die Datenquelle getestet werden



18. Nach diesen Schritten sind zum Schluss noch Änderungen am ISA Server durchzuführen. Dort wird das Speicherformat für die Firewall- und Webproxy-Protokollierung angepasst. Navigieren Sie dazu in der ISA-mmc zur ÜBERWACHUNG und wechseln Sie auf die Registerkarte PROTOKOLLIERUNG.
19. Klicken Sie dann im Aufgabenbereich auf den Link FIREWALLPROTOKOLLIERUNG KONFIGURIEREN. Wählen Sie dort den Eintrag SQL-DATENBANK und tragen unter ODBC-DATENQUELLENNAME (DSN) den Namen der Datenquelle ein, in unserem Beispiel *ISA-Protokollierung* und unter TABELLENNAME *FirewallLog* (siehe Abbildung 12.34). Über KONTO FESTLEGEN wird das gewünschte Benutzerkonto gewählt. Klicken Sie dann auf OK.

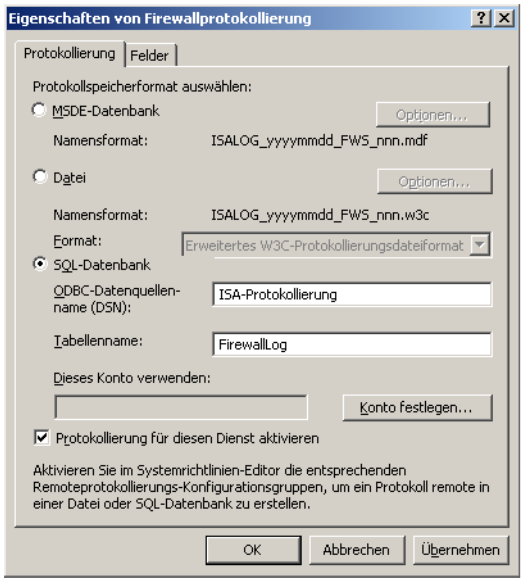


Abbildung 12.34: Konfiguration der Firewallprotokollierung für den SQL-Server

20. Klicken Sie dann auf WEBPROXYPROTOKOLLIERUNG KONFIGURIEREN. Führen Sie dort dieselben Schritte durch. Allerdings muss hier unter TABELLENNAME *WebProxyLog* eingetragen werden.
21. Als Letztes muss noch die Systemrichtlinie modifiziert werden, so dass die SQL-Protokollierung zu einem internen SQL-Server möglich ist. Navigieren Sie in der ISA-mmc zu FIREWALLRICHTLINIE und wählen das Kontextmenü SYSTEMRICHTLINIE BEARBEITEN. Wechseln Sie dort zu PROTOKOLLIERUNG/REMOTEPROTOKOLLIERUNG (SQL) und aktivieren Sie diese Richtlinie.
22. Übernehmen Sie dann die Änderungen an der Konfiguration des ISA Server.

12.7.6 Abfragen und Filter

Einsatz von Filtern zur Abfrage

Nachdem Sie die Optionen für die Protokollierung festgelegt haben, klicken Sie im Aufgabenbereich auf ABFRAGE STARTEN. Je nachdem, welche Speichermethode gewählt wurde, werden die Daten in Echtzeit oder historische Daten angezeigt. Um aus der möglichen Fülle der Informationen die gewünschten zu finden, können Filter verwendet werden.

Um einen neuen Filter zu erstellen oder einen vorhandenen zu ändern, klicken Sie im Aufgabenbereich auf FILTER BEARBEITEN. Dort können Sie für die vordefinierten Filter eine Bedingung und einen Wert auswählen (siehe Abbildung 12.35).

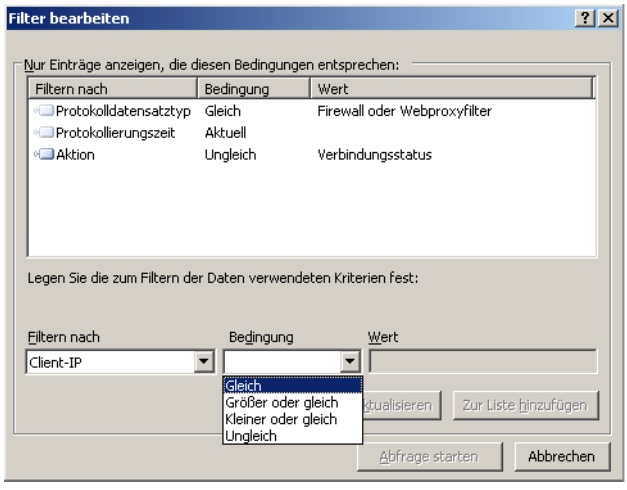


Abbildung 12.35: Konfiguration eines neuen Filters

Anpassen der angezeigten Spalten

Für die Anzeige der Protokollierungsdaten werden in der ISA-mmc die am häufigsten benutzten Felder verwendet. Möchten Sie noch zusätzliche Felder zur Anzeige bringen oder vorhandene Felder dort entfernen, so wählen Sie das Menü ANSICHT/SPALTEN HINZUFÜGEN/ENTFERNEN und passen die Anzeige gemäß Ihren Wünschen an.

Haben Sie ein bestimmtes Ereignis markiert, können Sie dieses über den Link AUSGEWÄHLTE ERGEBNISSE IN ZWISCHENABLAGE KOPIEREN dorthin kopieren und in einem anderen Programm, z.B. Excel, weiterbearbeiten. Ebenso können auch sämtliche Ereignisse in die Zwischenablage kopiert werden.

12.8 Leistungsmonitor

Echtzeitanzeige und historische Daten

Ein weiteres wichtiges Hilfsmittel zur Überwachung des ISA Server ist der Leistungsmonitor. Über diesen werden nicht die Überwachungsfunktionen des ISA Server, sondern dessen Leistungsdaten selbst kontrolliert. Der Leistungsmonitor ist Ihnen sicherlich schon aus der Arbeit mit Windows Server 2000 oder Windows Server 2003 geläufig. Prinzipiell funktioniert der Leistungsmonitor des ISA Server genau wie der des Betriebssystems. Der einzige Unterschied besteht darin, dass hier spezielle Leistungsindikatoren für den ISA Server vorhanden sind.

12.8.1 Echtzeitanzeige der Daten

Über den Leistungsmonitor können einerseits Daten in Echtzeit angezeigt werden, andererseits diese Daten aber auch in einer Datenbank gespeichert und zu einem späteren Zeitpunkt ausgewertet werden.

1. Um den Leistungsmonitor zu starten, öffnen Sie im Startmenü den Programmeintrag MICROSOFT ISA SERVER/ISA SERVER-LEISTUNGSMONITOR.
2. Sie sehen, dass dort bereits einige wichtige Leistungsindikatoren angezeigt werden. Um weitere Indikatoren hinzuzufügen, klicken Sie auf das Kreuz-Symbol.
3. Im Fenster LEISTUNGSINDIKATOREN HINZUFÜGEN (siehe Abbildung 12.36) können Sie unter LEISTUNGSOBJEKT für verschiedene ISA-Bereiche wie z.B. ISA Server-Cache, ISA Server-Firewalldienst usw. Leistungsindikatoren auswählen.

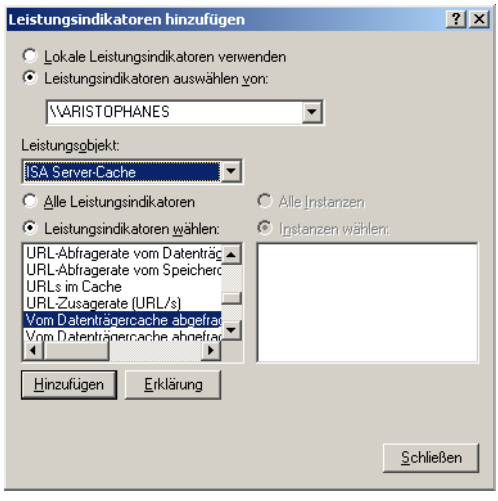


Abbildung 12.36: Hinzufügen neuer Leistungsindikatoren

4. Sobald ein neuer Indikator hinzugefügt wurde, werden dessen Daten in Echtzeit dargestellt.

Leistungsindikatoren und -objekte

Über LEISTUNGSINDIKATOR AUSWÄHLEN VON geben Sie den Namen des zu überwachenden Servers an, hier also den des ISA Server. Unter LEISTUNGSOBJEKT wird die zu überwachende Kategorie gewählt. An jedes dieser Leistungsobjekte sind verschiedene Leistungsindikatoren geknüpft. Der Leistungsindikator beschreibt einen Zustand oder gibt Auskunft über eine bestimmte Aktivität. Eine Übersicht über die dort verfügbaren Indikatoren und deren Bedeutung finden Sie, indem Sie bei einem Indikator auf die Schaltfläche ERKLÄRUNG klicken.

Soll die Überwachung des ISA Server von einem anderen Computer aus erfolgen, so beachten Sie die Hinweise zur Remote-Verwaltung in Kapitel 6.

12.8.2 Datenaufzeichnung in einer Datenbank

Historische Daten

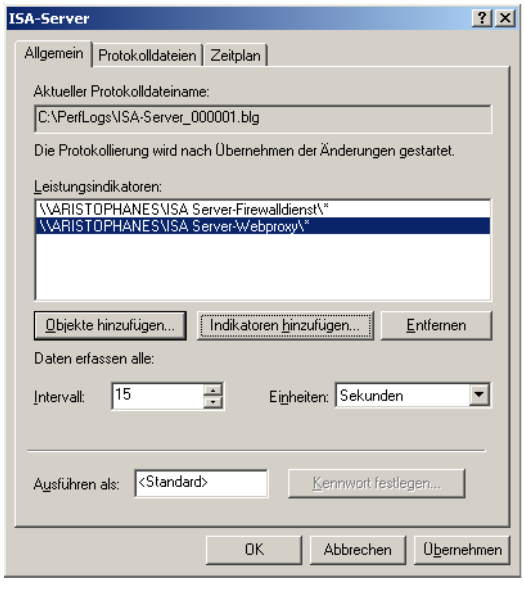
Neben der Anzeige der Leistungsdaten in Echtzeit kann auch eine Speicherung dieser Daten in eine Datenbank erfolgen. Auf diese Weise können über einen längeren Zeitraum Daten gesammelt und ausgewertet werden. So können z.B. Trends in der Auslastung des ISA Server erkannt werden, die z.B. eine Aktualisierung der Hardware zur Folge haben können.

Datenbank

Um die Leistungsdaten in einer Datenbank zu speichern, führen Sie die folgenden Schritte aus:

1. Öffnen Sie in der Verwaltung die mmc LEISTUNG und navigieren Sie zum Eintrag LEISTUNGSPROTOKOLLE UND WARNUNGEN.
2. Wählen Sie aus dem Kontextmenü von LEISTUNGSINDIKATOREN-PROTOKOLLE den Eintrag NEUE PROTOKOLLEINSTELLUNGEN.
3. Geben Sie einen passenden Namen für diese Einstellungen an, in unserem Beispiel *ISA Server*.
4. Auf der Registerkarte ALLGEMEIN (siehe Abbildung 12.37) wählen Sie die gewünschten Leistungsobjekte oder einzelnen Leistungsindikatoren dieser Objekte aus. Des Weiteren geben Sie das Intervall für die Messung an. Bedenken Sie aber, dass ein niedriges Intervall zwar mehr Daten liefert, insgesamt aber den ISA Server wesentlich stärker belastet.

Abbildung 12.37: Auswahl der zu protokollierenden Objekte und Indikatoren



5. Über die Registerkarte ZEITPLAN können Sie festlegen, ob die Protokollierung manuell über das Kontextmenü oder nach einem bestimmten Zeitplan ausgeführt werden soll.

6. Sie können die Aufzeichnung der Daten nun entweder manuell über das Kontextmenü bzw. die entsprechende Schaltfläche oder gemäß dem Zeitplan starten. Die Leistungsdaten werden in die gewählte Protokolldatei geschrieben.
7. Ist das Sammeln der Daten beendet (zu erkennen am roten Symbol der Datenbank anstelle des grünen), navigieren Sie zum Eintrag SYSTEMMONITOR. Wählen Sie über das Symbol PROTOKOLLDATEN ANZEIGEN oder die Tastenkombination Strg + L die Datenbankansicht und geben Sie auf der Registerkarte QUELLE den Pfad zur Datei über HINZUFÜGEN an (siehe Abbildung 12.38).

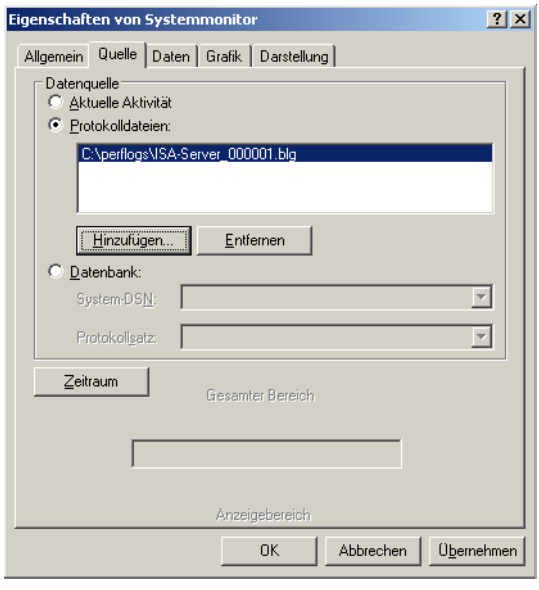


Abbildung 12.38: Auswahl der Quell-Protokolldatei

8. Soll aus Gründen der Übersichtlichkeit nur ein Teil der aufgezeichneten Protokolldateien angezeigt werden, so können über ENTFERNEN bzw. HINZUFÜGEN die gewünschten Elemente gewählt werden.
9. Wurden die Daten über einen längeren Zeitraum gesammelt, so können Sie im Abschnitt ZEITRAUM über den Schieberegler den gewünschten Ausschnitt wählen. Die gewählten Inhalte werden dann im Systemmonitor angezeigt. Die Anzeige unterscheidet sich lediglich dadurch, dass die Daten hier nicht in Echtzeit aktualisiert, sondern in einer festen Kurve angezeigt werden.

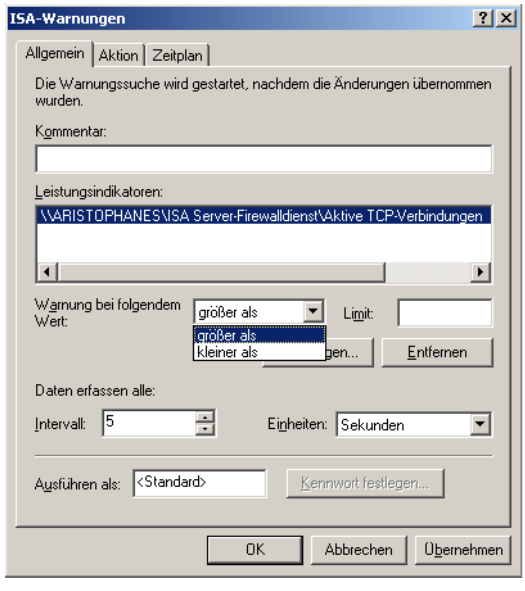
12.8.3 Warnungen des Systemmonitors

Auch über den Systemmonitor können Warnungen eingerichtet werden, wenn bestimmte Ereignisse eintreten. Dies ist sinnvoller, als wenn erst bei der Betrachtung der historischen Daten festgestellt wird, dass es zu einem Problem oder einem außergewöhnlichen Ereignis kam.

So kann beim Über- oder Unterschreiten eines Werts für einen Leistungsindikator beispielsweise ein Hinweis gesendet oder ein bestimmtes Programm ausgeführt werden. Um diese Warnfunktion einzurichten, führen Sie die folgenden Schritte durch:

1. Navigieren Sie in der mmc LEISTUNG zum Eintrag LEISTUNGSPROTOKOLLE UND WARNUNGEN.
2. Wählen Sie aus dem Kontextmenü von WARNUNGEN den Eintrag NEUE WARNEINSTELLUNGEN.
3. Geben Sie der neuen Warneinstellung einen passenden Namen, z.B. *ISA-Warnungen*.
4. Auf der Registerkarte ALLGEMEIN wählen Sie die gewünschten Leistungsindikatoren aus. Zusätzlich legen Sie dort den passenden Grenzwert fest, bei dessen Über- oder Unterschreiten eine Aktion ausgelöst werden soll (siehe Abbildung 12.39).

Abbildung 12.39: Definition eines Limits für einen Leistungsindikator, bei dessen Über/Unterschreiten ein Alarm ausgelöst werden soll



5. Markieren Sie je einen Indikator und wechseln Sie auf die Registerkarte AKTION (siehe Abbildung 12.40). Dort können Sie eine oder mehrere der folgenden Optionen wählen: Eintrag in das Ereignisprotokoll, Senden einer Netzwerkmeldung an einen bestimmten Benutzer, Starten eines Leistungsdatenprotokolls oder Ausführen eines Programms mit optionalen Kommandozeilenparametern. Bestätigen Sie die Auswahl(en) mit OK.

Damit eine Nachricht an einen Benutzer gesendet werden kann, muss auf dem ISA Server und dem Computer des Benutzers der Nachrichtendienst aktiviert sein. Des Weiteren muss über eine der Systemrichtlinien DIAGNOSEDIENSTE/WINDOWS NETZWERK oder PROTOKOLLIERUNG/REMOTEPROTOKOLLIERUNG ZULASSEN (NETBIOS) der NetBIOS-Verkehr für das Senden der Nachrichten vom ISA Server an das interne Netzwerk zugelassen werden.

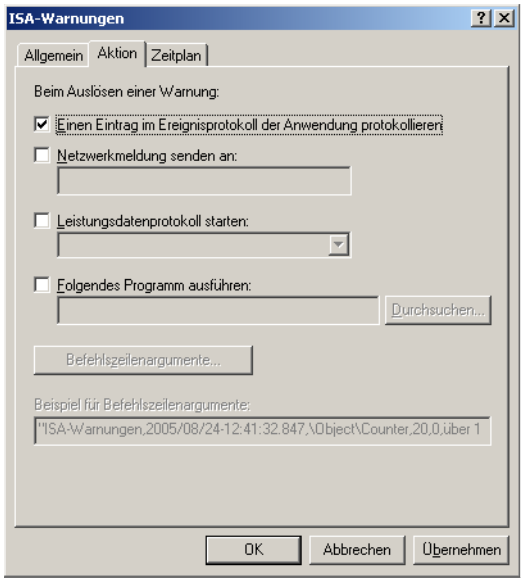


Abbildung 12.40: Wahl der Aktion, die als Alarm ausgeführt werden soll

6. Um die Überwachung der Leistungsindikatoren zu beginnen, starten Sie die konfigurierte Warneinstellung.

12.9 Intrusion Detection

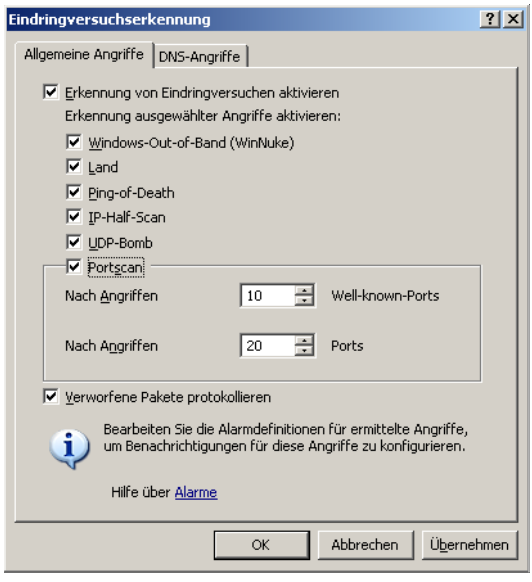
Unter Intrusion Detection oder der Eindringversuchserkennung versteht man die Fähigkeit des ISA Server, Angriffe bereits im Vorfeld zu erkennen und nicht an das geplante Ziel des Angriffs durchzulassen. Dabei ist es gleichgültig, ob es sich um einen geplanten und gezielten Angriff mit einem bestimmten Zweck handelt oder ob der Angriff über einen Robot bzw. ein Programm eine Reihe von Servern im Internet heimsucht.

Natives Abwehrverhalten gegen bekannte Angriffe

Der ISA Server besitzt bereits nativ die Fähigkeit, eine Reihe bekannter Angriffe und Eindringversuche zu erkennen und abzuwehren. Selbstverständlich kann auch dieses Feature auf die Gegebenheiten und Bedürfnisse Ihres Netzwerks abgestimmt werden. Zur Konfiguration sind die folgenden Schritte erforderlich:

1. Navigieren Sie in der ISA-mmc zu KONFIGURATION/ALLGEMEIN und wählen Sie ERKENNUNG VON EINDRINGVERSUCHEN UND DNS-ANGRIFFEN AKTIVIEREN.
2. Auf der Registerkarte ALLGEMEINE ANGRIFFE finden Sie eine Übersicht über die wichtigsten und am häufigsten durchgeführten Angriffe. Markieren Sie dort alle Angriffe, die der ISA Server abwehren soll (siehe Abbildung 12.41).

Abbildung 12.41: Übersicht über die Angriffe, die der ISA Server automatisch erkennen kann



Die Erkennung von DNS-Angriffen und deren Bedeutung wurde bereits im Zusammenhang mit dem DNS-Filter in Kapitel 9 vorgestellt.

Im Folgenden werden die verschiedenen Angriffe und deren Bedeutung kurz vorgestellt.

- WINDOWS-OUT-OF-BAND (WINNUKE): Ein WinNuke-Angriff ist eine DoS-Attacke (Denial of Service), bei der – in der Regel auf Port 139- ein TCP-Paket, bei dem das URG-Flag gesetzt ist, an den Server gesendet wird und diesen so zum Absturz bringen kann.
- LAND: Bei einer Land-Attacke werden manipulierte IP-Pakete versendet, bei denen die Absenderadresse der Zieladresse entspricht. Sobald ein solches Paket sein Ziel erreicht, versucht der Computer das Paket zuzustellen und läuft dabei in eine endlose Schleife. Nach dem Versenden eines für eine Land-Attacke modifizierten Pakets werden die Ziel-IP-Adresse und der Zielport geprüft. Genau diese beiden Informationen werden dann auch als gefälschter Absender benutzt.

- PING-OF-DEATH: Bei einem Ping-of-Death wird einem Computer oder einem Router o.Ä. ein IP-Paket zugesendet, das größer ist als die maximal erlaubte Größe von 65.535 Byte. Damit ein derartiges Paket überhaupt versendet werden kann, wird dieses in einzelnen Teilen verschickt und erst auf dem Zielsystem wieder zu einem (über)großen Paket zusammengefügt. Der Zusammenbau und der Versuch der Verarbeitung dieses übergroßen Pakets kann zum Absturz des Geräts führen.
- IP-HALF-SCAN: Um eine TCP-Sitzung zwischen zwei Geräten zu initiieren, wird zwischen diesen zunächst ein Drei-Wege-Handschlag (Three-Way-Handshake) durchgeführt. Dieser besteht aus den drei folgenden Handlungen.
  1. Um einen bestimmten Port des Zielsystems zu kontaktieren, sendet der Client eine Nachricht, die ein SYN-Flag enthält.
  2. In der Antwortnachricht des Servers ist das Flag SYN/ACK gesetzt.
  3. Der Client antwortet darauf mit einer Nachricht, in der das Flag ACK gesetzt ist.

     Erst wenn dieser Handshake abgeschlossen ist, beginnt der eigentliche Transfer der Daten. Dieses Verfahren machen sich Hacker zu Nutze, indem sie dieses nur zum Teil ausführen, um herauszufinden, ob auf dem Server ein bestimmter Dienst aktiv ist. Dazu wird die Verbindung nach dem zweiten Schritt abgebrochen (Flag RST, Reset), sobald der Server dem Client auf seine Anfrage hin geantwortet hat.
- UDP-BOMB: Eine UDP-Bomb-Attacke besteht aus dem Senden von ungültigen UDP-Paketen, um damit einen Server zum Absturz zu bringen.
- PORTSCAN: Mit Hilfe eines Portscans wird auf einem Computer nach der Existenz bestimmter Dienste gesucht, indem ein Bereich von Ports abgesucht wird. Auf der Registerkarte können Sie unter PORTSCAN für die Well-known-Ports und für die übrigen Ports bestimmen, wie viele jeweils abgefragt werden dürfen, ohne dass dies als Angriff gewertet wird. Ein Portscan ist der einzige Angriff in der Liste, der per se noch kein Angriff ist, sondern nur nach Informationen sucht, die für einen späteren Angriff verwendet werden können.

Alle Eindringversuche aktivieren

In der Regel sollten Sie alle Eindringversuche für die Erkennung aktivieren und zusätzlich für jeden Versuch wie weiter oben beschrieben einen Alarm einrichten, der beim Administrator oder einer anderen zuständigen Person aufläuft. Auch die Option VERWORFENE PAKETE PROTOKOLLIEREN sollte aktiviert werden, um auch im Protokoll Informationen über den versuchten Angriff zu erhalten.

Zusätzlich zu diesen Optionen helfen auch Anwendungsfilter, den Netzwerkverkehr bis hinunter zur Anwendungsebene zu untersuchen und gegebenenfalls eine Verbindung zu unterbrechen. Hierzu zählen die Anwendungsfilter:

- SMTP-Filter
- POP3-Eindringversuch-Erkennungsfilter
- DNS-Filter

13 ISA-Tools

Dieses Kapitel beschreibt zahlreiche Werkzeuge und Programme, die die Verwaltung des ISA Server erleichtern oder sogar erweitern. Es wird sowohl auf Microsoft-eigene Programme als auch auf Tools von Drittanbietern eingegangen. Weiterhin werden auch verschiedene hilfreiche Skripte vorgestellt.

13.1 Microsoft-Tools

In diesem Kapitel werden einige von Microsoft herausgebrachte Programme für den ISA Server 2004 vorgestellt. Sie finden diese Tools alle auf der beiliegenden CD.

13.1.1 Firewall Client-Tool

Konfiguration und Test des Firewall-Clients

Das Firewall Client-Tool (*FwcTool.exe*) ist ein Kommandozeilenprogramm, mit dem der ISA Server angegeben werden kann, den die Firewall-Clients verwenden sollen. Zusätzlich können Optionen für die automatische Erkennung angegeben werden sowie Einstellungen für den Webbrowser des Clients gesetzt werden.

Zusätzlich können Tests für die Verfügbarkeit des ISA Server sowie der automatischen Erkennung durchgeführt werden. Die Konfiguration des Firewall-Clients kann auch ausgegeben werden.

Die mit *FwcTool.exe* festgelegten Einstellungen können entweder für sämtliche Benutzer des Firewall-Clients, für den aktuellen oder für ausgewählte Benutzer umgesetzt werden.

Das Programm verwendet die folgende Syntax:

```
Fwctool.exe Befehl Parameter ↵
```

Die folgenden Parameter sind verfügbar, eine Übersicht über die Parameter der einzelnen Befehle erhalten Sie über den Aufruf des jeweiligen Befehls mit der Option `/?`.

Tabelle 13.1: Übersicht über die Befehle von FwcTool.exe

Befehl	Beschreibung
Info	Anzeige der Installationsinformationen
Enable	Aktivieren des Firewall-Clients
Disable	Deaktivieren des Firewall-Clients
SetManualServer	Angabe des zu benutzenden ISA Server
SetAutoDetect-Server	Aktivieren der automatischen Erkennung des ISA Server
PrintConfig	Ausgabe der aktuellen Konfigurationseinstellungen
PrintServerConfig	Ausgabe der aktuellen Konfigurationseinstellungen des ISA Server
PrintUserConfig	Ausgabe der aktuellen Konfigurationseinstellungen für den aktuellen Benutzer
PrintGlobalConfig	Ausgabe der aktuellen Konfigurationseinstellungen für alle Benutzer
TestAutoDetect	Testen des Mechanismus zur automatischen Erkennung
PingServer	Ping-Konnektivitätsprüfung an den ISA Server
EnableBrowser-Config	Aktivieren der automatischen Konfiguration des Webbrowsers
DisableBrowser-Config	Deaktivieren der automatischen Konfiguration des Webbrowsers
PrintBrowser-Config	Ausgabe der aktuellen Konfigurationseinstellungen des Webbrowsers

Wurde ein Befehl erfolgreich ausgeführt, gibt das Programm den Wert 0 zurück, bei einem Fehler wird der Wert 1 oder höher ausgegeben.

13.1.2 RAS-Quarantäne-Tool

Als RAS-Quarantäne-Tool werden zwei verschiedene Programme für die Quarantäne-Kontrolle zusammengefasst, nämlich *rqs.exe* und *rqc.exe*.

Diese beiden Programme gehören auch zum Lieferumfang des *Windows Server 2003 Resource Kit*.

Zwei Komponenten für Client und Server

Mit Hilfe der Quarantäne-Kontrolle können Remote-Clients nach ihrer Authentifizierung in Quarantäne gehalten werden, bis die Konfiguration des Clients den Richtlinien des Unternehmens entspricht. Solange stehen dem Remote-Client aus Sicherheitsgründen nur sehr

eingeschränkte Berechtigungen zu. Das Programm *rqc.exe* wird als Benachrichtigungsprogramm auf dem Remote-Computer ausgeführt. Dieses informiert die Listener-Komponente *rqs.exe* auf dem ISA Server, sobald der Remote-Client den Anforderungen entspricht.

Nach der Installation von *rqs.exe* auf dem ISA Server erhält dieser die zusätzliche RQS-Protokolldefinition. Es wird eine Instanz des RQS-Dienstes angelegt. Gleichzeitig wird auch eine Zugriffsregel erstellt, die das RQS-Protokoll zulässt.

ISA Server per Skript vorbereiten

Nachdem die beiden Komponenten *rqs.exe* und *rqc.exe* als Bestandteil des Windows Server 2003 Resource Kit installiert worden sind, sollten Sie die aktualisierte Version von *rqs.exe* installieren. Führen Sie dann das Skript *RQSForISA.vbs* aus. Dieses befindet sich im Installationsverzeichnis von *rqs.exe*. Dieses Skript bereitet den ISA Server als RQS-Listener vor. Dabei werden die RQS-Protokolldefinition, die Instanz des RQS-Dienstes sowie die Zugriffsregel zum Zulassen des RQS-Protokolls erstellt.

13.1.3 Firewall Kernel Mode-Tool

Fweng.sys

Das Firewall Kernel Mode-Tool für ISA Server 2004 (*FwEngMon.exe*) dient zur Analyse und Fehlersuche der Firewall-Konnektivität, indem der Kernel Mode-Treiber des ISA Server (*fweng.sys*) überwacht wird. Mit Hilfe dieses Kommandozeilenprogramms können Sie beispielsweise die Aktivität von Low-Level-Treibern überwachen, die Firewall für einen bestimmten Bereich von IP-Adressen öffnen oder schließen, Informationen über verschiedene Verbindungselemente ausgeben lassen sowie die jeweiligen Ausgabedaten in eine *.xml*-Datei exportieren.

Weitere Hinweise zu den genauen Abläufen der Kernel Mode-Treiber finden Sie im Abschnitt Useful Information in der Dokumentationsdatei des Programms *fwengmon.doc*.

Das Programm unterstützt den Aufruf der folgenden Parameter:

Tabelle 13.2: Parameter des Kommandozeilenprogramms fwengmon.exe

Parameter	Beschreibung
`/session oder /s`	Liste der aktiven Sitzungen
`/creations oder /c`	Liste der aktiven Creation-Objekte
`/allow oder /a <von> <bis>`	Öffnet die Firewall für den angegebenen Bereich von IP-Adressen. Es gibt für diese IP-Adressen keine Zugriffsbeschränkungen durch die Firewall.
`/NoAllow`	Der eben genannte Befehl wird wieder außer Kraft gesetzt.

Parameter	Beschreibung
`/v`	Ausgabe der Informationen im ausführlichen Modus (Verbose Mode)
`/ID <id>`	Auswahl einer Verbindung oder eines Creation-Objekts, über das ausführliche Informationen angezeigt werden
`/Organize oder /o`	Als Sortierreihenfolge der Ergebnisliste ist eine der folgenden Optionen anzugeben: ▶ `By_Src_Ip` ▶ `By_Dst_Ip` ▶ `By_Src_Port` ▶ `By_Dst_Port` ▶ `By_Protocol`
`/filter oder /f`	Filterung der Ergebnisliste nach einer der folgenden Einträge: ▶ `Src_Ip <ip>` ▶ `Dst_Ip <ip>` ▶ `Src_Port <port>` ▶ `Dst_Port <port>`
`/E <pfad>`	Export der Ausgabedaten in eine *.xml*-Datei

13.1.4 ISA Server 2004 SDK

Eigenes ISA Server-SDK

Microsoft stellt für den ISA Server 2004 ein eigenes SDK (Software Development Kit) zur Verfügung. Mit Hilfe dieses SDK können Entwickler die Funktionen des ISA Server erweitern und anpassen. Auch eine Automatisierung der Konfiguration von z.B. Firewall-Dienst, Paketfilterung, VPN-Unterstützung, Caching, Überwachung, Protokollierung und der Alarmfunktion ist realisierbar.

Zusätzlich können mit Hilfe des SDK Anwendungsfilter, Webfilter, Konfigurationsskripte und Erweiterungen der Benutzeroberfläche erstellt werden.

13.2 Drittanbieter-Tools

Auch von verschiedenen Drittanbietern sind Programme verfügbar, die den Funktionsumfang des ISA Server 2004 erweitern oder dessen Verwaltung erleichtern. Zur besseren Übersicht sind die Programme nach Einsatzgebieten geordnet. Beachten Sie, dass die Liste der Programme keinen Anspruch auf Vollständigkeit erhebt.

13.2.1 Überwachung

Protokollierung von URLs statt IP-Adressen

Um in der Protokollierung des ISA Server in der Spalte URL anstelle der IP-Adressen die eigentliche URL anzuzeigen, die der Client in seinen Webbrowser eingegeben hat, verwenden Sie das Programm *LogHostname* der Firma Collective Software. Dieses Programm integriert sich nahtlos in die Protokollierung des ISA Server 2004. Sie haben damit die Möglichkeit, bei Proxy-Clients, die den SecureNAT-Client verwenden, oder bei Firewall-Clients, für die die automatische Konfiguration nicht möglich ist, anstelle der IP-Adresse in der Protokollierung die komplette URL zu sehen, die der Client in seinen Webbrowser eingetragen hat.

Weitere Informationen zu diesem Programm finden Sie unter *https://www.collectivesoftware.com/Products/*.

Echtzeitüberwachung aufgerufener Webseiten

Zur Überwachung der Internetseiten in Echtzeit, die von den Netzwerkclients aufgerufen werden, können Sie das Programm *GFI WebMonitor* verwenden. Zusätzlich zu den aktuell aufgerufenen Webseiten können auch die downgeloadeten Dateien betrachtet werden. Des Weiteren ist es auch möglich, aus dem Programm heraus Internetverbindungen zu blockieren. Bei diesem Programm handelt es sich um Freeware.

Weitere Informationen zu diesem Produkt finden Sie unter dem Link *http://www.gfisoftware.de/webmon/*.

13.2.2 Reporting

Visualisiertes Reporting

Für die Analyse der Internetnutzung im Unternehmen bietet sich das Programm *Proxy Inspector* der Firma ADV Soft an. In visualisierter Darstellung erhalten Sie Informationen über besuchte Internetseiten, gesperrte Seiten, versuchte Zugriffe sowie Benutzeraktivitäten.

Weitere Informationen zu diesem Produkt finden Sie unter dem Link *http://www.advsoft.info/de/products/proxyinspector/.*

Logkonverter

Die Protokolldateien des ISA Server können mit Hilfe des Logconverters *ISALogToHTML* vom ASCII-Format in html-Dateien konvertiert werden. Bei diesem Programm handelt es sich um Freeware.

Weitere Informationen zu diesem Produkt finden Sie unter dem Link *http://www.ulrichlennartz.de/tools/isalogtohtml.html.*

13.2.3 Verschiedene Programme

Internetdownload-Kontingent

Über das Programm *TrafficQuota* der Firma Digirain Technologies kann der Internetzugang eines Benutzers zugelassen oder blockiert werden, abhängig von seinem Kontingent der downloadbaren Datenmenge. Darf ein Benutzer beispielsweise im Monat 100 MB downloaden, so besteht für ihn kein Zugang mehr zum Internet, sobal er dieses

Limit überschritten hat. Für bis zu fünf Benutzer ist das Programm kostenlos. Bei mehr Benutzern richtet sich der Preis nach der Anzahl der Benutzer.

Weitere Informationen zu diesem Programm finden Sie unter dem Link *http://www.digirain.com/tquota/*.

Bedingungen für den Internetzugriff bestimmen

Soll entweder vor dem Zugriff der internen Benutzer auf das Internet oder vor dem der externen Benutzer auf veröffentlichte Server ein spezielles Dialogfeld angezeigt werden, in dem der Benutzer vom Administrator frei definierbaren Bedingungen für den Zugriff auf die jeweiligen Systeme zustimmen muss, so bietet sich dazu das Programm *WebTOS (Terms of Services)* der Firma Collective Software an. Dieses Verfahren bietet sich an, wenn die Benutzer z.B. vor dem Zugriff auf das Internet zustimmen müssen, dass sie gemäß Unternehmensrichtlinien keine Seiten für den privaten Gebrauch aufrufen.

Weitere Hinweise zu diesem Produkt finden Sie unter dem Link *http://www.collectivesoftware.com/products*.

Datenkontrolle für das interne Netzwerk

Für eine Kontrolle der Dateien, die in das interne Netzwerk per http oder ftp gelangen dürfen sowie eine Prüfung dieser Daten auf Viren können Sie das Programm *DownloadSecurity for ISA Server* der Firma GFI verwenden. Sie können weiterhin festlegen, welche Art von Dateien von welchem Urheber in das interne Netzwerk gestellt werden dürfen.

Weitere Informationen zu diesem Produkt finden Sie unter dem Link *http://www.gfisoftware.de/de/dsec/index.html*.

14 ISA Server 2004 Enterprise

Wesentlich erweiterter Funktionsumfang

In diesem Kapitel wird auf die Funktionen des ISA Server 2004 in Multi-Netzwerkumgebungen eingegangen. Die hier genannten Features und Funktionen sind lediglich in dieser Version, nicht jedoch in der Standardversion verfügbar und anwendbar. Die Enterprise Version des ISA Server wird in den allermeisten Fällen sicher nur in großen Unternehmen eingesetzt, die höhere Anforderungen an Verfügbarkeit, Verwaltungsaufwand und Flexibilität stellen.

Gegenüber der Standardversion verfügt die Enterprise-Version über die folgenden zusätzlichen Features:

- Die ISA Server können in einem ISA Server 2004 Enterprise-Array betrieben werden.
- Zur Konfiguration stehen zusätzliche Array- und Enterprise-Richtlinien zur Verfügung.
- Zentrale Übersicht über Protokollierung und Überwachung
- Unterstützt Network Load Balancing (NLB)
- Unterstützt das Cache Array Routing Protocol (CARP)

In den folgenden Kapiteln lernen Sie die ersten Schritte speziell im Umgang mit der Enterprise Version. Die Inhalte der bisherigen Kapitel, die sich auf die Standardversion beziehen, werden dabei vorausgesetzt.

Beispielszenario

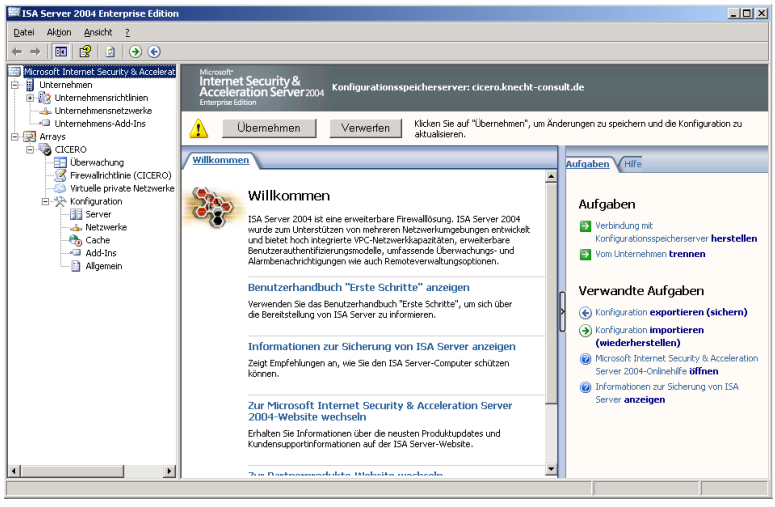
Das Szenario, das den Konfigurationsanleitungen zu Grunde liegt, besteht aus dem Unternehmen mit einer Filiale. Im internen Netzwerk der Unternehmenszentrale befindet sich ein ISA Server-Konfigurationsspeicherserver. Das Firewallarray dort besteht aus drei Computern. In der Filiale befindet sich ebenfalls ein ISA Server-Konfigurationsspeicherserver und ein Computer im Firewallarray. Die Zentrale und Filiale gehören zu derselben Domäne. Der Domänencontroller befindet sich in der Zentrale.

14.1 Die ISA Server Enterprise-mmc

Die ISA-mmc der Enterprise-Version weicht in der Gliederung von der der Standardversion ab. In der Enterprise ISA-mmc finden sich die beiden übergeordneten Snap-Ins UNTERNEHMEN und ARRAYS. Unter ARRAYS finden Sie dann die bereits aus der Standardversion bekannte Struktur. Unter dem Snap-In UNTERNEHMEN befinden sich dessen

untergeordnete Einträge UNTERNEHMENSRICHTLINIEN, UNTERNEHMENSNETZWERKE und UNTERNEHMENS-ADD-INS (siehe Abbildung 14.1).

Abbildung 14.1: Die ISA-mmc der Enterprise-Version



Direkt nach der Installation finden sich dort die folgenden zu beachtenden Punkte:

- In den UNTERNEHMENSRICHTLINIEN findet sich eine Richtlinie, die Standardrichtlinie, die sämtliche Zugriffe verweigert, die nicht explizit erlaubt worden sind.
- Wenn Sie den Eintrag UNTERNEHMENSNETZWERKE öffnen, sehen Sie, dass dort keine expliziten Netzwerke definiert sind, wie z.B. in der Standardversion das Netzwerk *Intern*.
- Unter ARRAY sehen Sie, dass sich dort noch kein Eintrag befindet, solange kein Array erstellt worden ist.

14.2 Benutzer zum Active Directory hinzufügen

Administrationshierarchien

Zur Verwaltung des ISA Server werden verschiedene Rollen von Administratoren definiert, die jeweils unterschiedliche Aufgaben erledigen sollen. So gibt es beispielsweise Administratoren für das Unternehmen und untergeordnete Administratoren für bestimmte Arrays. Damit weitere Konfigurationsschritte durchgeführt werden können, müssen zunächst drei verschiedene Benutzer im Active Directory angelegt werden. Dies sind:

- *EnterpriseAdmin*: Unternehmensadministrator
- *ArrayAdmin*: Administrator des Arrays in der Unternehmenszentrale
- *FilialarrayAdmin*: Administrator des Arrays in der Filiale

Einige der Verwaltungsaufgaben werden nicht direkt vom Unternehmensadministrator ausgeführt, sondern an den Array-Administrator delegiert. Dazu zählen das Anlegen eines Arrays sowie das Hinzufügen von Computern zum Array, das Erstellen der Array-Richtlinie sowie die Einrichtung des Netzwerklastenausgleichs (Network Load Balancing, NLB) oder des CARP-Protokolls.

Um die Benutzer dem Active Directory zuzufügen, öffnen Sie die mmc ACTIVE DIRECTORY-BENUTZER UND –COMPUTER. Erstellen Sie die Benutzer im Container der Domäne.

Beachten Sie, dass diese drei Benutzer auch über lokale Administratorenrechte auf allen Computern verfügen müssen, auf denen mit Ausnahme der ISA-Verwaltung Komponenten des ISA Server installiert werden.

14.3 Konfigurationsspeicherserver installieren

Separate Installation oder gemeinsam mit ISA Server

Der Konfigurationsspeicherserver kann während der Installation des ISA Server entweder direkt auf diesem System mitinstalliert werden oder auch nach der Installation des ISA Server 2004 auf einem separaten Computer installiert werden.

1. Entscheiden Sie sich für die zweite Variante, legen Sie die Installations-CD ein und folgen Sie zunächst den Anweisungen des Installationsassistenten.
2. Sobald das Fenster SETUP-SZENARIEN erscheint, wählen Sie die zweite Option KONFIGURATIONSSPEICHERSERVER INSTALLIEREN.
3. Im Fenster UNTERNEHMENSINSTALLATIONSOPTIONEN wählen Sie die Option NEUES ISA SERVER-UNTERNEHMEN ERSTELLEN.
4. Danach geben Sie einen Namen für das neue Unternehmen an.
5. Im Fenster BEREITSTELLUNGSUMGEBUNG FÜR DAS UNTERNEHMEN kann wahlweise ein digitales Zertifikat für die verschlüsselte Kommunikation zwischen dem ISA Server und dem Konfigurationsspeicherserver angegeben werden. Sie sollten die dafür notwendige Option BEREITSTELLUNG IN EINER ARBEITSGRUPPE ODER IN DOMÄNEN, ZWISCHEN DENEN KEINE VERTRAUENSSTELLUNG BESTEHT wählen, wenn ein derartiges Szenario vorliegt. Befinden sich wie in unserem Beispiel der ISA Server und der Konfigurationsspeicherserver in derselben Domäne, kann die Standardoption dafür beibehalten werden.
6. Schließen Sie dann in den restlichen Schritten die Installation ab.

14.4 Den Unternehmensadministrator hinzufügen

Ranghöchster Admin

Ein Unternehmensadministrator besitzt die höchsten Verwaltungsrechte am ISA Server. Er kann zusätzlich zum Unternehmen auch die darin enthaltenen Arrays administrieren. Ein Array-Administrator hingegen kann keine Verwaltungsaufgaben am Unternehmen durchführen.

1. Öffnen Sie in der ISA-mmc den Kontextmenüeintrag EIGENSCHAFTEN von UNTERNEHMEN.
2. Wechseln Sie auf die Registerkarte ROLLEN ZUWEISEN. Dort ist als Benutzer derjenige angezeigt, der zum Zeitpunkt der Installation als aktueller Benutzer angemeldet war (siehe Abbildung 14.2). Löschen Sie diesen Benutzer und fügen Sie stattdessen den Benutzer *EnterpriseAdmin* hinzu. Achten Sie dabei darauf, diesem die Rolle *ISA Server-Unternehmensadministrator* zuzuweisen.

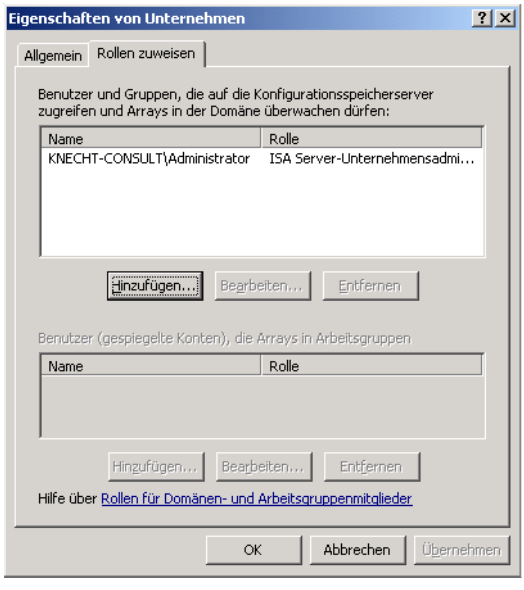


Abbildung 14.2: Hinzufügen des Benutzers EnterpriseAdmin als ISA-Unternehmensadministrator

3. Die geänderten Einstellungen müssen mit einem Klick auf ÜBERNEHMEN in der ISA-mmc gespeichert werden.

14.5 Anlegen eines Unternehmensnetzwerks

Unternehmensweite Zugriffsregeln

Als Nächstes steht das Erstellen eines Unternehmensnetzwerks an. Für ein Unternehmensnetzwerk können unternehmensweite Zugriffsregeln erstellt werden. Danach können von den einzelnen Array-Administratoren Array-Netzwerke erstellt werden. Im Unternehmensnetzwerk sind sämtliche IP-Adressen des internen Netzwerks enthalten.

1. Navigieren Sie in der ISA-mmc zu UNTERNEHMEN/UNTERNEHMENSNETZWERKE.
2. Klicken Sie unter AUFGABEN auf NEUES NETZWERK ERSTELLEN. Ein Assistent wird gestartet.
3. Geben Sie zunächst einen Namen für das Netzwerk ein, z.B. *internes Netzwerk*. Klicken Sie dann auf WEITER.
4. Im Fenster NETZWERKADRESSEN (siehe Abbildung 14.3) klicken Sie auf HINZUFÜGEN. Geben Sie dann einen IP-Adressbereich ein, der das neue Unternehmensnetzwerk umfasst, und bestätigen Sie mit OK.

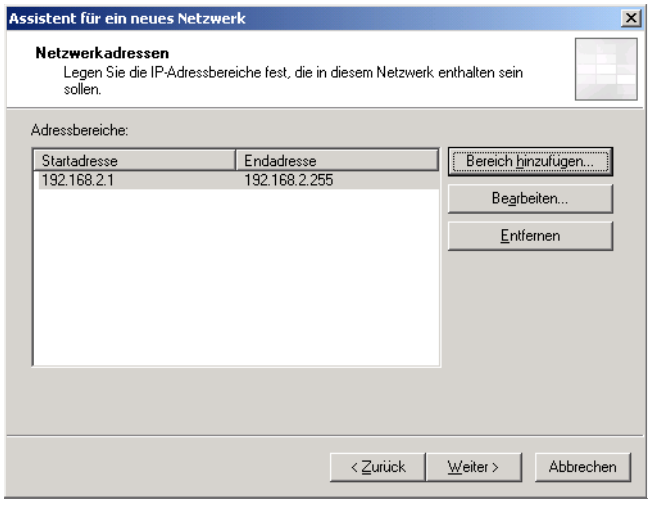


Abbildung 14.3: Auswahl des Netzwerkbereichs für das Unternehmensnetzwerk

5. Beenden Sie dann den Assistenten und bestätigen Sie die Konfigurationsänderung mit ÜBERNEHMEN.

14.6 Unternehmensrichtlinien definieren

Nur eine Standardrichtlinie vorhanden

Da für das Unternehmen nur die Standardrichtlinie definiert ist, müssen dafür weitere Unternehmensrichtlinien erstellt werden. In unserem Beispiel soll eine Richtlinie so definiert werden, dass sämtliche Benutzer der Unternehmenszentrale die Protokolle http, https und ftp benutzen dürfen und die ftp-Nutzung der Zweigstellenbenutzer vom Array-Administrator lediglich auf bestimmte Zeiten beschränkt ist. Die zweite Richtlinie besagt, dass die Benutzer der Zweigstelle grundsätzlich kein http-Protokoll verwenden dürfen, sondern nur https-Verbindungen.

Um die erste Richtlinie zu erstellen, führen Sie die folgenden Schritte aus:

1. Melden Sie sich als *EnterpriseAdmin* an der Domäne an.
2. Navigieren Sie zu UNTERNEHMEN/UNTERNEHMENSRICHTLINIEN und klikken Sie auf NEUE UNTERNEHMENSRICHTLINIE ERSTELLEN.
3. Geben Sie der Regel einen Namen, z.B. *eingeschränkter ftp-Zugriff*. Klicken Sie auf WEITER und beenden Sie den Assistenten. Übernehmen Sie dann die Änderungen.
4. Als Nächstes werden für diese Richtlinie Zugriffsregeln hinzugefügt. Navigieren Sie dazu zu der eben erstellten Unternehmensrichtlinie und klicken Sie auf UNTERNEHMENSZUGRIFFSREGEL ERSTELLEN. Es wird erneut ein Assistent gestartet.

Weitere Details zu den hier beschriebenen Assistenten finden Sie in Kapitel 7, das das Erstellen von Zugriffsregeln erläutert.

5. Geben Sie der Zugriffsregel einen Namen, z.B. *http/https-Unternehmenszugriff*.
6. Als Regelaktion wird ZULASSEN gewählt.
7. Wählen Sie die Option AUSGEWÄHLTE PROTOKOLLE und fügen Sie die Protokolle http sowie https hinzu.
8. Im Fenster ZUGRIFFSREGELQUELLEN klicken Sie auf HINZUFÜGEN. Wählen Sie aus den NETZWERKSÄTZEN den Eintrag ALLE GESCHÜTZTEN NETZWERKE (siehe Abbildung 14.4) aus und klicken Sie auf HINZUFÜGEN und SCHLIEßEN.

Durch die Auswahl von ALLE GESCHÜTZTEN NETZWERKE sind alle Netzwerke impliziert, die auch zu einem späteren Zeitpunkt als Unternehmensnetzwerk hinzugefügt werden. Dadurch verringert sich der Konfigurationsaufwand erheblich.

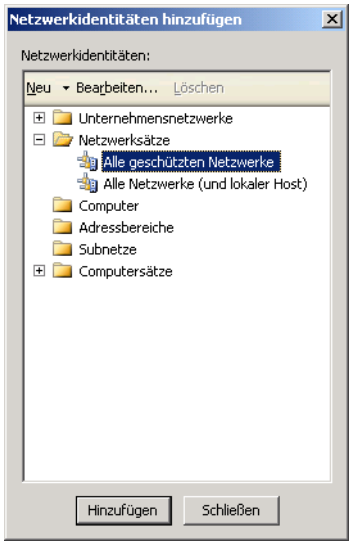


Abbildung 14.4: Auswahl des Netzwerksatzes Alle geschützten Netzwerke

9. Im Fenster ZUGRIFFSREGELZIELE klicken Sie auf HINZUFÜGEN und wählen unter UNTERNEHMENSNETZWERKE den Eintrag EXTERN.
10. Unter BENUTZERSÄTZE wählen Sie den Eintrag ALLE BENUTZER. Beenden Sie dann den Assistenten und übernehmen Sie die Konfigurationsänderung.
11. Wiederholen Sie die Schritte 4 bis 10 und erstellen Sie dabei eine Zugriffsregel namens *ftp-Zugriff des Unternehmens*. Dabei ist der ftp-Zugriff zulässig.
12. Nach Erstellung dieser Richtlinien befinden sich beide im Abschnitt NACH DER ARRAYRICHTLINIE ANGEWENDETE UNTERNEHMENSRICHTLINIENREGELN. Verschieben Sie über den Kontextmenüeintrag NACH OBEN die Regel *http/https-Unternehmenszugriff* in den Bereich VOR DER ARRAYRICHTLINIE ANGEWENDETE UNTERNEHMENSRICHTLINIENREGELN (siehe Abbildung 14.5). Übernehmen Sie diese Änderung.

Reihenfolgen unbedingt bearbeiten

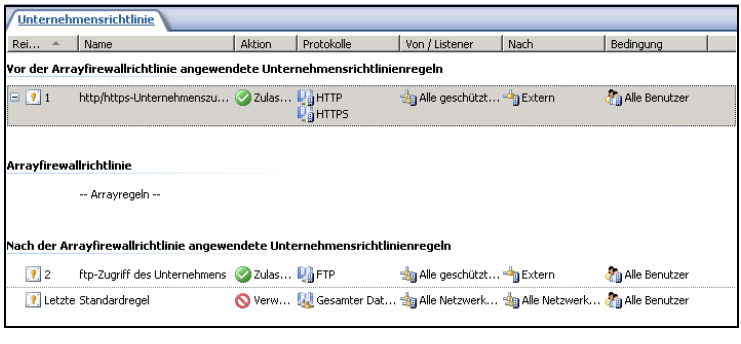


Abbildung 14.5: Die geänderte Reihenfolge der Unternehmenszugriffsregeln

13. Als Nächstes wird eine Richtlinie erstellt, die den ftp-Zugriff immer gestattet. Melden Sie sich dazu als *EnterpriseAdmin* an der Domäne an und navigieren Sie zu UNTERNEHMEN/UNTERNEHMENSRICHTLINIEN.
14. Klicken Sie auf NEUE UNTERNEHMENSRICHTLINIE ERSTELLEN und geben dieser den Namen *permanenter ftp-Zugriff*. Übernehmen Sie diese Änderung.
15. Nun werden für diese Richtlinie Zugriffsrichtlinien hinzugefügt. Wählen Sie dazu für diese Richtlinie den Link UNTERNEHMENSZUGRIFFSREGEL ERSTELLEN im Aufgabenbereich.
16. Geben Sie der Zugriffsregel den Namen *http/https/ftp-Unternehmenszugriff*.
17. Wählen Sie die drei Protokolle *http*, *https* und *ftp* aus. Alle weiteren Einstellungen erfolgen wie in den Schritten 4 bis 10. Übernehmen Sie danach die Änderung.
18. Die neue Zugriffsregel wird über das Kontextmenü NACH OBEN bis in den Abschnitt VOR DER ARRAYRICHTLINIE ANGEWENDETE UNTERNEHMENSRICHTLINIENREGELN verschoben. Übernehmen Sie abermals die Änderungen.

14.7 Anlegen eines Arrays

Mehrere ISA Server im Array

Unter einem ISA Server 2004 Enterprise-Array versteht man eine Sammlung mehrerer ISA Server. Alle im Array enthaltenen Server benutzen einen gemeinsamen Konfigurationsspeicherserver und werden zusammen verwaltet. Innerhalb des Arrays werden beispielsweise auch dieselben Richtlinien eingesetzt. Zentral erfolgt auch die Protokollierung und Überwachung. Auch eine Delegierung der Verwaltung für das ISA Server-Array ist möglich.

ADAM

In einem ISA Server 2000-Array wurde noch das Active Directory zur Speicherung der Konfiguration verwendet. Aufgrund höherer Flexibilität und erweiterter Konfigurationsmöglichkeiten, aber weniger Konfigurationsaufwand wird nun *ADAM* (*Active Directory Application Mode*) als zentraler Konfigurationsspeicher verwendet. Zur Erhöhung der Fehlertoleranz können auch mehrere Konfigurationsspeicherserver eingesetzt werden, die ihre jeweiligen Inhalte miteinander synchronisieren. Auf der Registerkarte KONFIGURATIONSSPEICHER des Arrays können Sie einen alternativen Konfigurationsspeicherserver sowie den Intervall, in dem dieser auf Aktualisierungen geprüft werden soll, einstellen (siehe Abbildung 14.6).

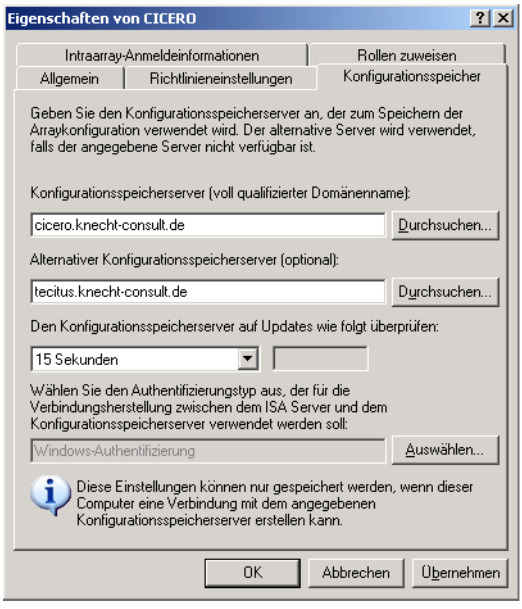


Abbildung 14.6: Einstellen des Intervalls, in dem der Konfigurationsspeicherserver auf Updates geprüft werden soll

Der Vorteil des ADAM gegenüber dem Active Directory besteht darin, dass die ISA Server nicht zwangsläufig Mitglied einer Domäne sein müssen.

Nachdem der Konfigurationsspeicherserver installiert wurde, können Sie mit der Berechtigung des Unternehmensadministrators dort ein Array erstellen. Der Unternehmensadministrator kann das Zusammenspiel von Unternehmens- und Array-Richtlinien verwalten, bevor der untergeordnete Array-Administrator Zugriff auf sein Array bekommt.

Eingeschränkte Regeltypen für das Array

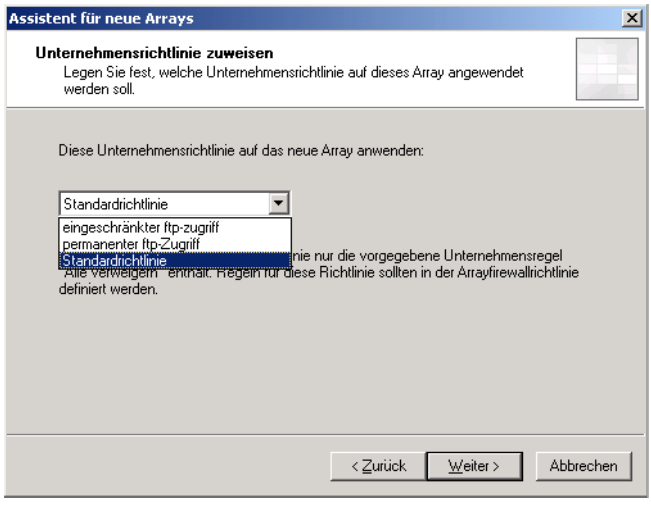
Es ist auch möglich, dass der Array-Administrator selbst ein Array einrichtet, indem er bei der Installation des ISA Server im Fenster ARRAYMITGLIEDSCHAFT ein neues Array anlegt. Sobald dieses Array erstellt wurde, kann der Unternehmensadministrator jedoch die Regeltypen für dieses Array beschränken. Allerdings können keine Regeltypen eingeschränkt werden, für die der Array-Administrator bereits Regeln erstellt hat.

Um als Unternehmensadministrator ein Array zu installieren, sind die folgenden Schritte erforderlich:

1. Markieren Sie den Eintrag ARRAYS und klicken Sie auf NEUES ARRAY ERSTELLEN.
2. Geben Sie einen neuen Namen für das Array an, z.B. *Unternehmenszentrale*. Geben Sie den DNS-Namen an, den die Clients für die Verbindung mit dem entsprechenden ISA Server benutzen.

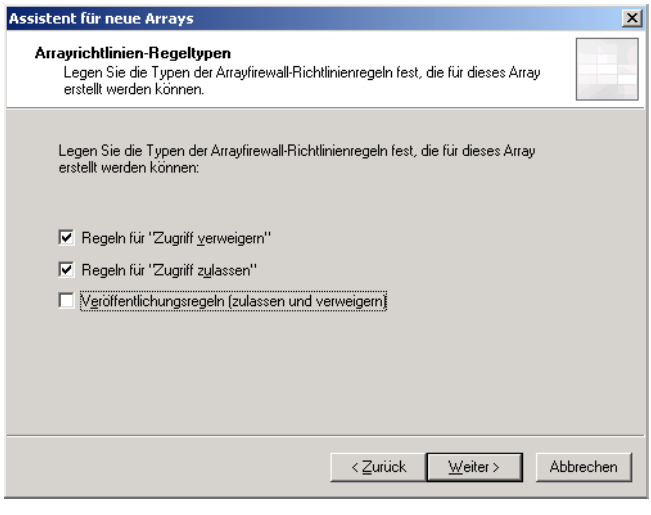
3. Im Fenster UNTERNEHMENSRICHTLINIE ZUWEISEN können Sie zwischen der Standardregel und den beiden eben erstellten Richtlinien *eingeschränkter ftp-Zugriff* und *permanenter ftp-Zugriff* wählen. Für das Unternehmen wird die Richtlinie *permanenter ftp-Zugriff* ausgewählt (siehe Abbildung 14.7).

Abbildung 14.7: Auswahl der Unternehmensrichtlinie für das Array



4. Danach legen Sie im Fenster ARRAYRICHTLINIEN-REGELTYPEN (siehe Abbildung 14.8) fest, welche Regeltypen der Array-Administrator verwenden darf. Sie sollten diesem untergeordneten Administrator lediglich die Regeln *Zugriff verweigern* und *Zugriff gestatten* zugestehen.

Abbildung 14.8: Auswahl der Regeltypen, die der Array-Administrator verwenden darf



5. Beenden Sie dann den Assistenten und wählen aus dem Kontextmenü des neuen Arrays den Eintrag EIGENSCHAFTEN.
6. Wechseln Sie auf die Registerkarte ROLLEN ZUWEISEN und klicken Sie auf HINZUFÜGEN. Wählen Sie den Benutzer *ArrayAdmin* aus und erteilen Sie diesem die Rolle ISA SERVER-ARRAYADMINISTRATOR. Bestätigen Sie die Einstellungen und übernehmen Sie die Konfigurationsänderung.

14.8 Installation weiterer ISA Server im Array

Nachdem das Array erstellt wurde, können diesem ISA Server hinzugefügt werden. Dazu müssen die folgenden Schritte auf jedem ISA Server durchgeführt werden, der zu dem Array hinzugefügt werden soll.

1. Die Installation wird wie gewohnt durchgeführt. Im Fenster SETUP-SZENARIEN wählen Sie die Option ISA SERVER-DIENSTE INSTALLIEREN.
2. Im Fenster KONFIGURATIONSSPEICHERSERVER SUCHEN geben Sie entweder den vollständigen Namen dieses Servers an oder wählen diesen über DURCHSUCHEN aus.
3. Wählen Sie dann im Fenster ARRAYMITGLIEDSCHAFT die Option VORHANDENEM ARRAY BEITRETEN.
4. Im Fenster VORHANDENEM ARRAY BEITRETEN geben Sie das Array *Unternehmenszentrale* an.
5. Als Authentifizierungsmethode wählen Sie im Fenster AUTHENTIFIZIERUNGSOPTIONEN FÜR KONFIGURATIONSSPEICHERSERVER dieselbe Option aus, die auch für die Authentifizierung zwischen Konfigurationsspeicherserver und ISA Server gewählt wurde. Da sich in unserem Beispiel die Server in derselben Domäne befinden, wählen Sie die Option WINDOWS-AUTHENTIFIZIERUNG.
6. Dieser Schritt muss nur auf dem ersten ISA Server durchgeführt werden, der dem Array beitreten soll: Geben Sie im Fenster INTERNES NETZWERK den IP-Adressbereich des internen Netzwerks für dieses Array an.

Nur einmal notwendig

7. Folgen Sie den weiteren Schritten des Installationsassistenten und schließen Sie die Installation ab. Danach muss der Server neu gestartet werden.

Wenn Sie danach in der ISA-mmc den Eintrag KONFIGURATION/SERVER öffnen, sehen Sie, dass dort alle dem Array hinzugefügten Server vorhanden sind.

14.9 Anlegen eines zweiten Arrays

Zweites Array z.B. für eine Filiale

Die Unternehmenszentrale und der Konfigurationsspeicherserver werden in diesem Szenario in einem Array abgebildet. Ein zweites Array wird nun für die Filiale angelegt. Damit dies funktioniert, muss eine Verbindung zwischen den beiden Standorten bestehen. In einer Testumgebung wird dies eine reine LAN-Verbindung sein, später in der produktiven Umgebung wahrscheinlich eine VPN-Verbindung (Standort-zu-Standort-VPN).

Wie schon in früheren Kapiteln erwähnt, kann der ISA Server in beiden Versionen auf einem Domänencontroller oder einem Mitgliedserver bzw. allein stehenden Server installiert werden. Hinsichtlich von Sicherheitsaspekten ist die Installation auf einem Domänencontroller nicht unbedingt sinnvoll, kann jedoch in einigen Szenarien nicht verhindert werden.

14.9.1 Replikations-Konfigurationsspeicherserver zum Computersatz Replikations-Konfigurationsspeicherserver hinzufügen

1. Ist der erste ISA Server 2004 Enterprise auf einem Domänencontroller installiert worden, müssen Sie auf diesem zunächst eine Firewall-Regel erstellen, bevor ein neuer Server zum Array hinzugefügt werden kann. Dies ist erforderlich, damit der neue Server zur Namensauflösung auf das DNS sowie auf das Active Directory und den Konfigurationsspeicherserver zugreifen kann. Diese Richtlinie muss folgendermaßen konfiguriert sein:
   - Name: Installationszugriff auf das Array
   - Aktion: Zulassen
   - Protokolle: DNS, Kerberos-Sec (UDP), LDAP (UDP), LDAP GC (Global Catalog), LDAP
   - Von: Intern
   - Nach: Lokaler Host
2. Der neu zu erstellende ISA Server muss außerdem dem Computersatz *Konfigurationsspeicherserver replizieren* hinzugefügt werden. Dies ist jedoch nur dann notwendig, wenn auf jedem ISA Server auch ein Konfigurationsspeicherserver installiert werden soll. Navigieren Sie in der ISA-mmc zum Snap-In UNTERNEHMEN/UNTERNEHMENSRICHTLINIEN/STANDARDRICHTLINIE. In der Toolbox wählen Sie KONFIGURATIONSSPEICHERSERVER REPLIZIEREN und fügen den zweiten oder einen weiteren ISA Server hinzu. Erst wenn diese Schritte abgeschlossen sind, können Sie im Installationsfenster des zweiten ISA Server den Namen des ersten Konfigurationsspeicherservers angeben.

Um die Ausfallsicherheit zu maximieren, sollten innerhalb eines Arrays mindestens zwei ISA Server als Konfigurationsspeicherserver eingerichtet werden.

14.9.2 Replikations-Konfigurationsspeicherserver erstellen

Replikat des Konfigurationsspeicherservers

Um diese Aufgabe auszuführen, muss eine Verbindung zwischen den beiden Konfigurationsspeicherservern der Unternehmenszentrale und der Filiale bestehen.

1. Die Installation dieser zusätzlichen Server verläuft zunächst analog zur Erstinstallation. Allerdings müssen Sie dann im Fenster UNTERNEHMENSINSTALLATIONSOPTIONEN die Option REPLIKAT DER UNTERNEHMENSKONFIGURATION ERSTELLEN auswählen.
2. Sie erhalten dann ein Hinweisfenster, dass Sie nach der Installation die IP-Adressen dieses und des primären Konfigurationsspeicherservers dem Computersatz *Konfigurationsspeicherserver replizieren* hinzufügen. Diese Meldung können Sie jedoch ignorieren, weil der neu installierte Konfigurationsspeicherserver bereits zum entsprechenden Computersatz hinzugefügt worden ist.
3. Im Fenster ISA SERVER-KONFIGURATIONSREPLIKATIONSQUELLE müssen Sie festlegen, in welcher Weise die Daten des primären Konfigurationsspeicherservers repliziert werden sollen. Verwenden Sie eine schnelle LAN-Verbindung, so wählen Sie die Option ÜBER DAS NETZWERK REPLIZIEREN. Sind die Server hingegen nur über eine langsame Verbindung miteinander verbunden, wählen Sie die zweite Option VON DEN WIEDERHERGESTELLTEN SICHERUNGSDATEIEN KOPIEREN.
4. Über das Fenster BEREITSTELLUNGSUMGEBUNG FÜR DAS UNTERNEHMEN wird die Authentifizierung für die Kommunikation bestimmt. Ist der ISA Server Mitglied in einer Domäne, so wählen Sie die Option BEREITSTELLUNG IN EINER EINZELNEN DOMÄNE ODER IN DOMÄNEN, ZWISCHEN DENEN EINE VERTRAUENSSTELLUNG BESTEHT. Ist der ISA Server nicht Mitglied in einer Domäne oder in einer Domäne, die keine Vertrauensstellung zur Domäne des primären Konfigurationsspeicherservers besitzt, so wählen Sie die zweite Option BEREITSTELLUNG IN EINER ARBEITSGRUPPE ODER IN DOMÄNEN, ZWISCHEN DENEN KEINE VERTRAUENSSTELLUNG BESTEHT. Im zweiten Fall muss zur Authentifizierung ein Serverzertifikat angegeben werden. Klicken Sie dann auf WEITER.
5. Im Fenster ARRAYMITGLIEDSCHAFT wählen Sie die zweite Option VORHANDENEM ARRAY BEITRETEN, dass Sie ja kein neues Array erstellen wollen. Klicken Sie dann auf WEITER.

6. Als Nächstes wird unter VORHANDENEM ARRAY BEITRETEN der Name des Arrays angegeben oder über DURCHSUCHEN gesucht. Klicken Sie dann auf WEITER.
7. Danach müssen für den Konfigurationsspeicherserver die Authentifizierungsoptionen festgelegt werden. Ist der ISA Server Mitglied in einer Domäne, wählen Sie die Option WINDOWS-AUTHENTIFIZIERUNG. Bei der Mitgliedschaft in einer Arbeitsgruppe oder nicht vertrauenswürdigen Domäne ist die zweite Option AUTHENTIFIZIERUNG ÜBER SSL-VERSCHLÜSSELTEN KANAL zu wählen. Die beiden anderen Optionen können gewählt werden, wenn die Authentifizierung über Zertifikate erfolgen soll. Klicken Sie dann auf WEITER.
8. Folgen Sie dann den weiteren Schritten des Installationsassistenten und schließen Sie die Installation ab.

Replikation des Konfigurationsspeicherservers

Um nach der Installation des zweiten Servers zu prüfen, ob sich dieser korrekt mit dem ersten Konfigurationsspeicherserver repliziert hat, wechseln Sie in der Überwachung auf die Registerkarte KONFIGURATION.

14.9.3 Array-Erstellung

Um das Array zu erstellen, sind die folgenden Schritte notwendig:

1. Navigieren Sie auf dem Konfigurationsspeicherserver der Zentrale oder Filiale in der ISA-mmc zu ARRAYS und klicken Sie auf NEUES ARRAY ERSTELLEN.
2. Geben Sie dem Array den Namen *Filiale*.
3. Wählen Sie dann die Unternehmensrichtlinie *eingeschränkter ftp-Zugriff*.
4. Bestimmen Sie die Regeltypen für den Array-Administrator. In diesem Beispiel sind alle drei Regeltypen für ihn verfügbar. Stellen Sie dann den Assistenten fertig.
5. In den Eigenschaften des Arrays fügen Sie auf der Registerkarte ROLLEN ZUWEISEN den *FilialarrayAdmin* hinzu und geben diesem die Rolle *ISA Server-Arrayadministrator*. Übernehmen Sie dann die Konfigurationsänderungen.

14.9.4 Computer zum neuen Array hinzufügen

Zum neuen Array kann nun ein Computer hinzugefügt werden.

1. Die Installation wird wie gewohnt durchgeführt. Im Fenster SETUP-SZENARIEN wählen Sie die Option ISA SERVER-DIENSTE INSTALLIEREN.
2. Im Fenster KONFIGURATIONSSPEICHERSERVER SUCHEN geben Sie entweder den vollständigen Namen dieses Servers an oder wählen diesen über DURCHSUCHEN aus.

3. Wählen Sie dann im Fenster ARRAYMITGLIEDSCHAFT die Option VORHANDENEM ARRAY BEITRETEN.
4. Im Fenster VORHANDENEM ARRAY BEITRETEN geben Sie das Array *Filiale* an.
5. Als Authentifizierungsmethode wählen Sie im Fenster AUTHENTIFIZIERUNGSOPTIONEN FÜR KONFIGURATIONSSPEICHERSERVER dieselbe Option aus, die auch für die Authentifizierung zwischen Konfigurationsspeicherserver und ISA Server gewählt wurde. Da sich in unserem Beispiel die Server in derselben Domäne befinden, wählen Sie die Option WINDOWS-AUTHENTIFIZIERUNG.
6. Dieser Schritt muss nur auf dem ersten ISA Server durchgeführt werden, der dem Array beitreten soll: Geben Sie im Fenster INTERNES NETZWERK den IP-Adressbereich des internen Netzwerks für dieses Array an.

Nur einmal notwendig

7. Folgen Sie den weiteren Schritten des Installationsassistenten und schließen Sie die Installation ab. Danach muss der Server neu gestartet werden.

Wenn Sie dach in der ISA-mmc den Eintrag KONFIGURATION/SERVER öffnen, sehen Sie, dass dort alle dem Array hinzugefügten Server vorhanden sind.

14.10 Anlegen einer Array-Richtlinie

Eingeschränkte Array-Richtlinien

Nachdem dem Array ein Server hinzugefügt wurde, können Array-Richtlinien definiert werden. Für diese Richtlinien gelten die Einschränkungen, die der Unternehmensadministrator für das Array bestimmt hat.

14.10.1 Zugriffsregel für das Zweigstellen-Array

Um für das Array der Filiale eine Zugriffsregel zu erstellen, sind die folgenden Schritte notwendig, die auf einem Mitglied des Zweigstellen-Arrays vorgenommen werden:

1. Navigieren Sie zu ARRAYS/FILIALE und klicken Sie auf FIREWALLRICHTLINIE.
2. Im Aufgabenbereich klicken Sie auf ARRAYZUGRIFFSREGEL ERSTELLEN. Ein Assistent wird gestartet.
3. Geben Sie der Regel den Namen *kein ftp-Zugriff von Zweigstelle*.
4. Wählen Sie die Aktion VERWEIGERN.
5. Wählen Sie das Protokoll FTP aus.
6. Im Fenster ZUGRIFFSREGELQUELLEN wählen Sie das Netzwerk INTERNES NETZWERK aus.

7. Unter ZUGRIFFSREGELZIELE wird das Netzwerk EXTERN gewählt.
8. Wählen Sie als Benutzersatz ALLE BENUTZER aus. Beenden Sie den Assistenten und übernehmen Sie die Einstellungen.

14.10.2 Test der Richtlinie

Einstellungen überprüfen

Um zu testen, ob die Richtlinien korrekt erstellt wurden, versuchen Sie, von einem Client der Zentrale aus Daten von einer FTP-Seite downzuloaden. Dies sollte funktionieren. Versuchen Sie dann, FTP-Daten von einem Client der Filiale aus downzuloaden. Dabei sollte der Zugriff verweigert werden.

14.11 Network Load Balancing

Speziell für ISA Server 2004 angepasst

Network Load Balancing (Netzwerklastenausgleich) oder kurz *NLB* erhöht die Ausfallsicherheit der ISA Server. Diese Technik wurde bereits unter Windows Server 2000 eingeführt und liegt hier nun in einer speziell für ISA Server 2004 Enterprise angepassten Variante bereit. In der Standardversion ist dieses Feature nicht enthalten. Um auch hier auf eine Redundanz zugreifen zu können, müssen Sie auf zusätzliche Programme zurückgreifen.

Beim Einsatz des NLB werden die Anfragen der Netzwerkclients an die Mitglieder des Arrays über einen festen Algorithmus an sämtliche Mitglieder des Arrays gleichmäßig aufgeteilt. Dies ermöglicht eine gleichmäßige Auslastung aller Array-Mitglieder. Sofern eines der Array-Mitglieder ausfällt, werden die Anfragen automatisch an die noch verbliebenen Mitglieder gleichmäßig verteilt.

Zur Konfiguration des *NLB* steht ein eigener Assistent zur Verfügung.

1. Navigieren Sie in der ISA-mmc zu ARRAYS/UNTERNEHMENSZENTRALE/KONFIGURATION/NETZWERKE.
2. Klicken Sie im Aufgabenbereich auf NETZWERKLASTENAUSGLEICHS-INTEGRATION AKTIVIEREN.
3. Im Fenster LASTENAUSGLEICHSNETZWERKE AUSWÄHLEN (siehe Abbildung 14.9) wählen Sie die Netzwerke aus, für die die Funktion aktiviert werden soll. Das Netzwerk INTERN wird gewählt, wenn der Lastenausgleich für die Anfragen interner Clients ausgeglichen werden soll. Das Netzwerk EXTERN ist zu wählen, um aus dem Internet eingehenden Verkehr auszugleichen. Wählen Sie hier diese Option.

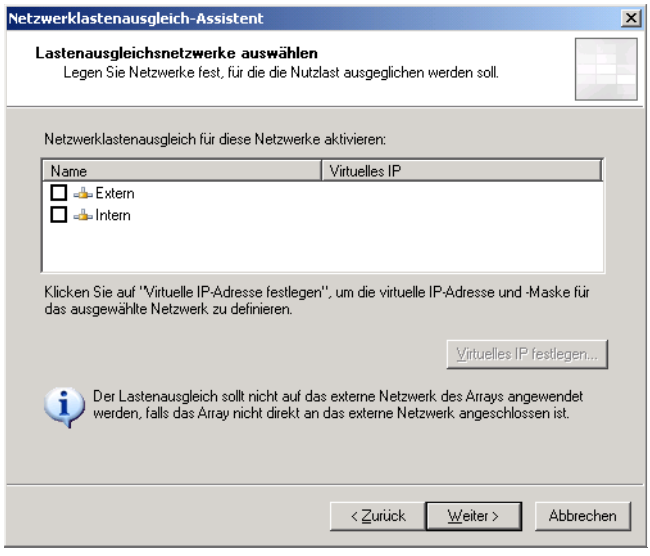


Abbildung 14.9: Auswahl des Netzwerks, für das der Lastenausgleich aktiviert werden soll

4. Sie müssen dann eine virtuelle IP-Adresse mit Subnetz angeben (siehe Abbildung 14.10). Dieses muss eine statische IP-Adresse sein, die sich in demselben Bereich wie das konfigurierte Netzwerk befindet. Beenden Sie dann den Assistenten.

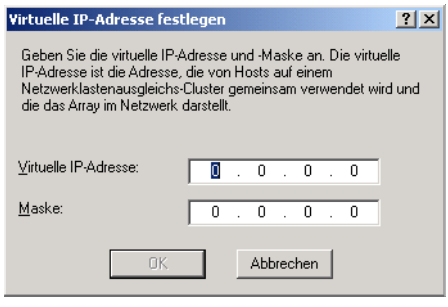


Abbildung 14.10: Angabe der virtuellen IP-Adresse für den Lastenausgleich

14.12 Cache Array Routing Protocol (CARP)

Verteilen der Cache-Inhalte

Das *Cache Array Routing Protocol* oder abgekürzt *CARP* ist ein Hash-Verfahren, über das die Cache-Inhalte gleichmäßig auf alle Array-Mitglieder verteilt werden und ebenso auch die Abfragen gleichmäßig an alle Mitglieder weitergeleitet werden. Standardmäßig besitzt auch ein ISA Server der Enterprise-Version einen lokalen Cache – wie auch der ISA Server der Standardversion. Mit Hilfe von CARP können jedoch sämtliche lokalen Cache-Speicher der Array-Mitglieder zu einem einzigen zentralen Cache zusammengeführt werden. Im Gegensatz zu NLB ermöglicht CARP keine Redundanz. Fällt bei Anwendung von

CARP ein Array-Mitglied aus, steht der gecachte Inhalt dieses Servers auf keinem anderen mehr zur Verfügung, sondern muss wieder neu aus dem Internet abgefragt werden. Der CARP-Algorithmus ist lediglich für die Cache-Einträge und Abfragen zuständig, wodurch sich die Performance für den Zugriff und auch die Wahrscheinlichkeit, Inhalte bereits im Cache zu finden, deutlich erhöht.

Bevor CARP verwendet werden kann, müssen zunächst der Cache und CARP für das Netzwerk aktiviert werden. Standardmäßig sind nach der Installation keine Cache-Laufwerke definiert, so dass keine Zwischenspeicherung stattfindet.

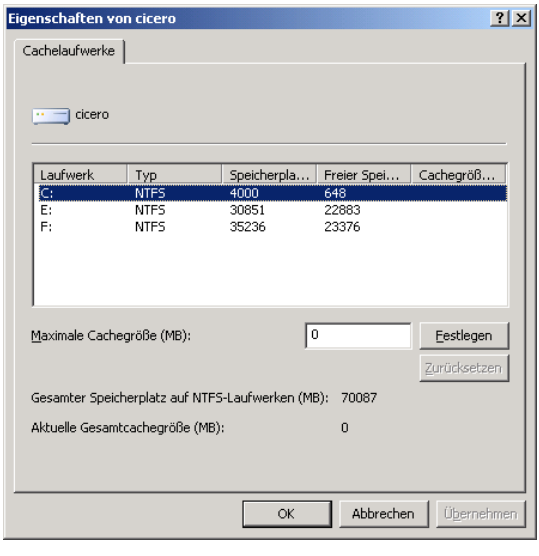
14.12.1 Cache-Aktivierung

Um den Cache für den ISA Server zu aktivieren, führen Sie die folgenden Schritte aus:

1. Navigieren Sie in der ISA-mmc beim gewünschten Server zu ARRAYS/ARRAYNAME/KONFIGURATION/CACHE.
2. Wechseln Sie auf die Registerkarte CACHELAUFWERKE.
3. Markieren Sie den Server und klicken Sie im Aufgabenbereich auf CACHELAUFWERKE DEFINIEREN (ZWISCHENSPEICHERUNG AKTIVIEREN).
4. Wählen Sie ein Laufwerk aus und bestimmen Sie über FESTLEGEN die Größe des Cache (siehe Abbildung 14.11).

Als Cache-Laufwerk kann nur ein Laufwerk oder eine Partition ausgewählt werden, die mit dem Dateisystem NTFS formatiert ist.

Abbildung 14.11: Auswahl des Cache-Laufwerks



5. Bestätigen Sie die Eingabe mit OK. Übernehmen Sie danach die Änderung dieser Konfiguration.

14.12.2 CARP aktivieren

Die Aktivierung von CARP erfolgt auf einem Computer des Arrays. Sie müssen mit der Berechtigung eines Array-Administrators angemeldet sein.

1. Navigieren Sie in der ISA-mmc beim gewünschten Server zu ARRAYS/ARRAYNAME/KONFIGURATION/NETZWERK.
2. Markieren Sie das interne Netzwerk und klicken Sie im Aufgabenbereich auf AUSGEWÄHLTES NETZWERK BEARBEITEN.
3. Wechseln Sie auf die Registerkarte CARP und markieren die Checkbox CARP AUF DIESEM NETZWERK AKTIVIEREN. Im unteren Bereich können einzelne Websites hinzugefügt werden, für die kein CARP-gestützter Datenverkehr angewendet werden soll (siehe Abbildung 14.12).

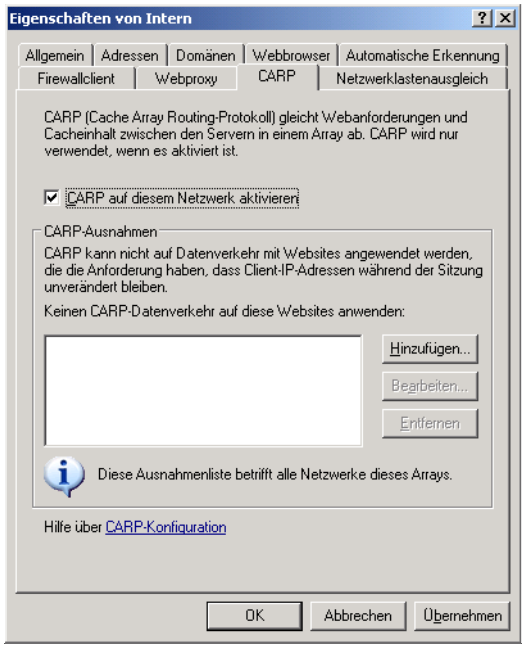


Abbildung 14.12: Aktivieren von CARP für das Netzwerk

4. Bestätigen Sie die Auswahl mit OK und übernehmen Sie danach die Änderungen an der Konfiguration.

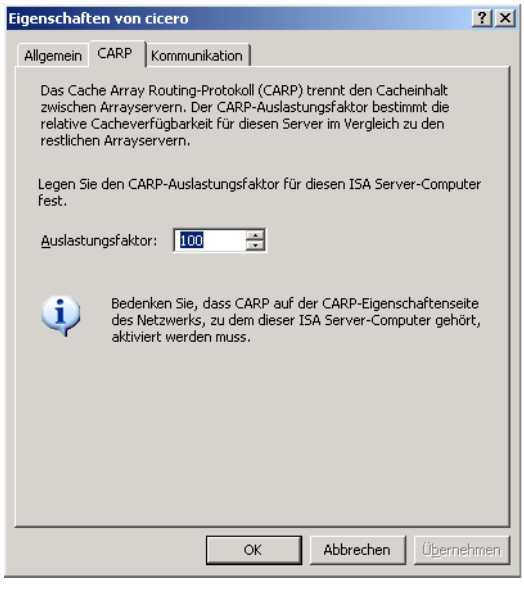
14.12.3 CARP konfigurieren

Auslastungsfaktor

Abschließend wird noch der CARP-Auslastungsfaktor konfiguriert. Über diesen Auslastungsfaktor wird die relative Cacheverfügbarkeit des gewählten Servers in Bezug zu den anderen Servern des Arrays dargestellt. Dazu sind die folgenden Schritte erforderlich:

1. Navigieren Sie in der ISA-mmc beim gewünschten Server zu ARRAYS/ARRAYNAME/KONFIGURATION/SERVER.
2. Markieren Sie den Server und klicken Sie im Aufgabenbereich auf AUSGEWÄHLTEN SERVER KONFIGURIEREN.
3. Wechseln Sie auf die Registerkarte CARP (siehe Abbildung 14.13) und setzen Sie dort einen Wert für den Auslastungsfaktor fest. Der Standardwert liegt bei 100.

Abbildung 14.13: Festlegen des CARP-Auslastungsfaktors



4. Bestätigen Sie den Wert mit OK und übernehmen Sie danach die Änderungen an der Konfiguration.

14.13 Weitere Aufgaben

Konfigurationseinstellungen sichern

Nachdem Sie diese Konfigurationsaufgaben am ISA Server durchgeführt haben, sollten diese Einstellungen gesichert werden. Dazu wird die Exportfunktion des ISA Server verwendet. Die exportierten Daten werden in einer *.xml*-Datei gespeichert. Beim Export kann entweder die komplette Konfiguration oder ein bestimmter Teil der Konfigurationselemente wie z.B. Richtlinien oder Regeln gewählt werden. Grundsätzliche Anmerkungen dazu finden Sie in Kapitel 6.

Soll das gesamte Unternehmen oder ein komplettes Array gesichert werden, so ist der Vorgang auf dem Konfigurationsspeicherserver selbst oder einem Computer mit der ISA Server-Verwaltung, der mit dem Konfigurationsspeicherserver verbunden ist, vorzunehmen. Ein Array kann auch von einem Mitglied des Arrays aus oder von einem

Computer mit der ISA Server-Verwaltung, der mit dem Array-Mitglied verbunden ist, gesichert werden.

Überwachung

Der zweite wichtige Punkt für den laufenden Betrieb ist die Überwachung. Für sämtliche Mitglieder des ISA-Arrays kann von zentraler Stelle aus die Überwachung und Protokollierung überblickt werden. Sie finden im Eintrag *Überwachung* in der ISA-mmc dieselben Punkte wie auch in der Standardversion (Übersicht, Alarme, Sitzungen, Dienste, Berichte, Konnektivität und Protokollierung). Eine detaillierte Übersicht über diese Funktionen finden Sie in Kapitel 12.

Zusätzlich ist in der Enterprise-Version noch die Registerkarte KONFIGURATIONSSTATUS verfügbar. Dort erhalten Sie Informationen darüber, ob (Spalte STATUS) und wann (Spalte AKTUALISIERT AM) der ISA Server mit dem Konfigurationsspeicher synchronisiert wurde (siehe Abbildung 14.14).

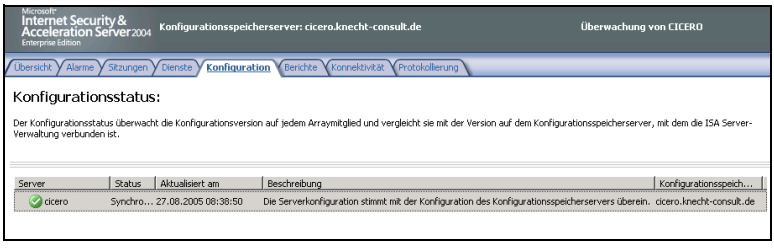


Abbildung 14.14: Überwachung der Synchronisation zwischen ISA Server und Konfigurationsspeicherserver

15 Rechtliche Aspekte zur Angriffserkennung und Beweissicherung

In diesem Kapitel werden Ihnen hier nun einige, beispielsweise auch rechtliche Informationen im Zusammenhang mit Angriffen, Gegenmaßnahmen und Beweissicherung vorgestellt.

Die im Rahmen der Angriffserkennung (Intrusion Detection, ID) gesammelten Daten müssen zwei wesentliche Kriterien erfüllen: Sie müssen einerseits datenschutzrechtlich behandelt sein und andererseits auch rechtsverwertbar in der späteren Beweisführung sein.

15.1 Signaturanalyse und Anomalieerkennung

Erkennen von Angriffsmustern

Bei der Signaturanalyse, wie sie auch für einige Angriffsformen im ISA Server 2004 integriert ist, wird ein Angriffsmuster anhand spezifischer Parameter erfasst, die in einer Datenbank als so genannte Signatur hinterlegt sind. Gibt es zu einem Angriff eine Signatur, so wächst der zu betreibende Aufwand zur Erkennung des Angriffs exponenziell in Abhängigkeit vom Effektivitätsgrad des Angriffs. Um einen hohen Effektivitätsgrad zu erreichen, muss der Angreifer hier einen hohen Aufwand betreiben. Gelingt ihm dies, steigt der Aufwand, einen Missbrauch trotzdem zu erkennen, unproportional an.

Darum ist es sinnvoll, neben der Signaturanalyse evetuell auch eine Anomalieerkennung zu betreiben. Bei diesem Verfahren steigt der Aufwand bei der Erkennung logarithmisch mit der Effektivität des Angriffs.

Der Ursprung der Anomalieerkennung lag in dem Bedarf, Benutzer, die unter einem falschen Account agieren, zu erkennen. Dabei wird sich ein Eindringling unter dem Benutzerkonto der Sekräterin anders im Netzwerk verhalten als diese selbst. Es gilt mit der Anomalieerkennung, dies zu erkennen. Hier zeigt sich schon das Problem. Vom Intrusion-Detection-Standpunkt aus bedeutet anomales Verhalten lediglich ein vom üblichen Benutzerverhalten abweichendes Verhalten, wobei folgende Parameter zur Analyse herangezogen werden:

- Seitenwechselrate
- CPU-Last

- Netzwerkdienstanforderungen (Sessions) während eines Zeitraumes (z.B. TELNET)
- Anzahl offener Ports etc.

Generell ist der Aufwand gegen den Nutzen abzuwägen

Letztendlich bedeutet dies die statistische Auswertung und Überwachung von Benutzer-Aktivitäten. Ein Punkt, der etwas schwierig zu realisieren ist, sind die Erhebung dieser Daten an sich, ihre Speicherung und Auswertung sowie letztendlich die Kosten für eine solche Analyse. Darüber hinaus entstünde so etwas wie der „gläserne Arbeitnehmer", was derzeit rechtlich umstritten ist und in den meisten Fällen der Zustimmung der gesamten Belegschaft bedarf. Auch wenn zu einer Anomalieanalyse kein gesondertes Instrumentarium eingesetzt wird, sollten die Administratoren Abweichungen in der Netzwerkauslastung oder CPU-Last auch unter dem Aspekt eines möglichen Angriffes betrachten.

15.2 Datenschutzrechtliche Grundlagen

Zu beachtende Paragraphen

Auch die im Rahmen der Intrusion Detection gesammelten Daten müssen datenschutzrechtlichen Grundsätzen entsprechen. Hierbei sind besonders die folgenden Paragraphen zu beachten:

- Bundesdatenschutzgesetz (BDSG) § 14,4 sowie §31
- Betriebsverfassungsgesetz (BtrVG) § 87,1 für nicht-öffentliche sowie öffentlich-rechtliche Wettbewerbsunternehmen
- Personalvertretungsrecht des Bundes oder Landes für öffentliche Stellen
- Gesetz über die Nutzung von Telediensten (TDG)
- Gesetz über den Datenschutz bei Telediensten (TDSG) § 4 bis 6

15.2.1 Rechtsverwertbarkeit

Rechtsgültige Beweismittel

Die von einem ID-System gesammelten Audit-Daten sind kein rechtsverbindliches Beweismittel wie beispielsweise Urkunden nach § 416 der Zivilprozessordnung (ZPO), sondern werden im Rahmen der freien Beweisführung, ähnlich wie eine Zeugenaussage, verwendet. Der Wert dieser Daten liegt damit im Ermessensbereich des Gerichts oder eines Sachverständigen.

Der vermeintlich geringere Beweiswert der Audit-Daten liegt darin begründet, dass diese theoretisch nachträglich modifiziert oder auch unvollständig dargebracht werden können. Dieses Problem stellt sich weniger, wenn Sie ein ID-System verwenden, das über eine automatische Integritätssicherung verfügt, z.B. eine digitale Signatur der

Audit-Daten. Allerdings muss dann auch sichergestellt sein, dass der Schlüssel für die Signatur vertraulich behandelt wird.

Folgende Rechtnormen sind anwendbar:

- Strafprozessordung (stopp), § 72 ff.
- Zivilprozessordung (ZPO), § 415

Verwertbare Audit-Daten

Um den rechtlichen Ansprüchen zu genügen, müssen in jedem Fall die folgenden Voraussetzungen erfüllt sein:

- Sind die Auditdaten personenbezogen, so muss die Person darüber informiert werden, dass diese Daten gesammelt werden.
- Nach Beendigung der Nutzung der personenbezogenen Daten müssen diese gelöscht werden.
- Die Nutzungsdaten müssen zusätzlich pseudonomisiert werden.
- Die Audit- und Nutzungsdaten müssen fälschungssicher zertifiziert sein. Nach Sammlung der Daten muss deren Integrität gewährt bleiben, z.B. durch Ausdruck, Speichern auf CD usw.

15.2.2 Gegenmaßnahmen bei einem Angriff

Intrusion Response

Die Gegenmaßnahmen bei einem Angriff werden auch als Intrusion Response (IR) bezeichnet. Die zu ergreifenden Maßnahmen auf einen Angriff müssen vom Unternehmen im Betriebsführungshandbuch in den Gesamtsicherheitsrichtlinien festgelegt sein. Sie sollten dort ein eigenes Kapitel mit IR-Richtlinien bilden.

Um eine Gegenmaßnahme einleiten zu können, müssen zunächst Informationen über den Angreifer bekannt sein. Es ist also nicht immer ratsam, die Verbindung zum Angreifer sofort zu trennen. Es kann durchaus sinnvoll sein, ihn zunächst kontrolliert seine Angriffe durchführen zu lassen. Es muss dabei eine Regelung geben, welche Angriffe zumindest temporär gestattet werden sollen. Dies mag zwar auf den ersten Blick wenig sinnvoll scheinen, hat aber durchaus seine Berechtigung.

Identifikation des Angreifers

Das wichtigste Ziel der Identifikation besteht darin, die richtige IP-Adresse des Angreifers zu ermitteln. Diese Aufgabe ist umso anspruchsvoller, als ein Angreifer in den seltensten Fällen den Angriff direkt von seinem Rechner aus starten wird, sondern entweder einen anderen Computer quasi als Sprungbrett benutzt oder IP-Adressen-Spoofing anwendet.

Der Zweck der IR liegt in zwei Zielen: Den Angreifer ausfindig machen und weitere Schäden abwenden bzw. bereits entstandene Schäden beheben.

Insgesamt gibt es drei Möglichkeiten, die Maßnahmen der IR umzusetzen:

- Automatische Maßnahmen, die vom verwendeten IR-System automatisch ausgeführt werden,
- Halbautomatische Maßnahmen, bei denen automatische IR-Maßnahmen sowie weitere manuelle Schritte zusammenspielen sowie
- Rein manuelle IR-Maßnahmen.

Wahl der Gegenmaßnahmen

Die Kunst besteht darin, im Einzelfall des Angriffs zu entscheiden, welche Maßnahmenstrategie die beste ist. Dies ist abhängig vom Angriffsverhalten sowie den betroffenen Computern und den darauf gespeicherten Dateien. Zudem müssen die Maßnahmen mit den vom Unternehmen definierten Sicherheitsrichtlinien in Einklang stehen.

Schadensbegrenzung durch Abschottung

Zeitpunkt zum Abbruch der Verbindung

Sobald ein Computer angegriffen worden ist, sollte der folgende Katalog von Sofortmaßnahmen angewendet werden. Bedenken Sie jedoch bei jedem Schritt, dass ein Ziel der IR auch die Identifikation des Angreifers sein soll und deshalb die Verbindung nicht zu schnell unterbrochen werden darf.

- Schließen Sie die betroffenen TCP/UDP-Ports.
- Lehnen Sie sämtliche Datagramme ab, die von der IP-Adresse des Angreifers stammen.
- Beenden Sie Programme und Dienste.
- Sofern der Angriff aus einer internen Quelle stammt, muss das betreffende Benutzerkonto sofort gesperrt werden.

Das Ablehnen der Datagramme sollte immer der erste Schritt sein, bevor Dienste oder Anwendungen beendet werden. Hierzu muss kurzfristig eine Konfigurationsänderung auf der Firewall oder dem Router vorgenommen werden. Während dieser Rekonfiguration muss natürlich gewährleistet sein, dass Firewall oder Router weiterhin ihre Funktion wahrnehmen können. Zudem muss sich das IR-System auch gegenüber dem rekonfigurierten System wieder authentifizieren können.

Sobald ein Dienst beendet wurde, muss sichergestellt sein, dass dieser nach einer gewissen Zeit wieder neu gestartet werden kann. Ansonsten wäre es dem Angreifer möglich, gegen diesen Dienst oder sogar das gesamte System DoS-Attacken zu starten.

Schadensbegrenzung durch Gegenangriff

Automatische Gegenangriffe

Im Gegensatz zur Abschottungsstrategie ist diese Maßnahme vor allen Dingen rechtlich wesentlich brisanter. Sobald ein System angegriffen wird, kann dieses einen automatischen Gegenangriff starten. Ziel dieses Angriffs ist in aller Regel eine DoS-Attacke (Denial of service), um dadurch den Angriffsrechner außer Gefecht zu setzen. Diese Angriffsform hört sich zwar recht einfach umzusetzen an, dennoch müssen in jedem Fall folgende Punkte bedacht werden:

- Es ist zunächst sicherzustellen, dass der angreifende Computer der wirkliche Angreifer ist und nicht nur für diesen Zweck mißbraucht wird.
- Es ist die richtige IP-Adresse des Angreifers ermittelt worden. Bedenken Sie, dass IP-Spoofing als probates Mittel zur Verschleierung der IP-Adresse angewendet worden sein kann.
- Der Gegenangriff muss gerechtfertigt sein. Bedenken Sie hier Punkte wie Verhältnismäßigkeit sowie die Gefahr von Selbstjustiz.

Nicht jeder rein technisch durchführbare Gegenangriff ist auch juristisch vertretbar. Und die Durchführung des automatischen Gegenangriffs sollte nicht unbedingt im Gerichtssaal mit einer Klage gegen Ihr Unternehmen enden.

Identifikation des Angreifers

Zur Identifikation des Angreifers ist eine umfassende Protokollierung notwendig. Das eingesetze Intrusion Detection-System (IDS) sollte in der Lage sein, diese Protokollierung im Falle eines Angriffs selbsttätig zu starten.

Festhalten des Benutzers auf präpariertem Computer

Während der Identifikation sind dem Angreifer zunächst weitere Aktionen möglich. Allerdings sollte man ihn hierzu in eine Art „Gummizelle“ locken, in der er keinen weiteren Schaden anrichten kann. Hierbei handelt es sich um einen vordem für derartige Zwecke präparierten Computer.

Sofern der Angreifer weitere Computer als Sprungbrett benutzt, muss auch auf diesen eine ausführliche Protokollierung aktiviert werden. Folgende weiteren Identifikationsmöglichkeiten bieten sich an:

- DNS-Suche nach dem betreffenden Computer. Dies wird jedoch in den seltensten Fällen zum Erfolg führen, da der Angreifer eigene Schutzmechanismen verwendet.
- Benachrichtigen eines CERT (Computer Emergency Response Team)
- Alarmierung der Administratoren der Computer, die als Sprungbrett benutzt werden. Der schnellste und sinnvollste Weg ist hier das Telefon und nicht die E-Mail. Auf diese Weise kann auch auf diesen Computern die Protokollierung aktiviert werden.

Nachverfolgung bei Telefonleitung

Sofern der Angreifer seine Aktionen jedoch über eine Telefonleitung oder einen X.25-Zugang ausübt, wird seine Nachverfolgung wesentlich schwieriger. Um Telefonleitungen abzuhören, ist in jedem Fall eine richterliche Genehmigung erforderlich.

Schadensbegrenzung und –beseitigung

Sicherungskopien

Das weitere Ziel der IR ist die Schadensbegrenzung und -beseitigung auf den betroffenen Systemen. Die hier einzuleitenden Maßnahmen sind abhängig von der Art des Angriffs sowie der dadurch entstandenen Schäden. Ein wichtiges Mittel sind Sicherungskopien, um wieder den Status von vor Beginn des Angriffs herstellen zu können. Hierbei sind jedoch zwei Punkte entscheidend: Wurde der Angriff frühzeitig genug erkannt, so dass die Aktualität der Sicherungskopie gewährleistet ist? Und kann zudem sichergestellt sein, dass die Inhalte der Sicherung nicht vom Angreifer verfälscht worden sind? Befindet sich auf dem System ein Trojanisches Pferd, so muss sichergestellt sein, dass dieses auch nach Einspielen der Sicherung nicht mehr vorhanden ist. Ansonsten kann der Angreifer nach wie vor auf den Computer zugreifen.

Entstandene Schäden lassen sich in die folgenden Schadensklassen einteilen:

- *Integritätsverlust*: Der Angreifer konnte auf dem System auf Daten zugreifen und diese manipulieren. Auch geänderte Konfigurationseinstellungen fallen in diese Kategorie.
- *Verfügbarkeitsverlust*: Auf dem System wurden Daten gelöscht oder durch andere Daten ersetzt.
- *Authentizitätsverlust*: Der Angreifer kann seine Handlungen unter einem anderen Benutzernamen ausführen. Ihm ist es möglich gewesen, Informationen wie den Autor einer E-Mail oder eines Dokuments zu fälschen.
- *Vertraulichkeitsverlust*: Der Angreifer hat Zugriff auf vertrauliche, geschützte Dateien erlangt, die nur bestimmten Personen zugänglich sind, z.B. Passwortdateien oder sensible Bilanzdaten. Bei dieser Form handelt es sich um die schwerwiegendste Schadensklasse, da die Vertraulichkeit im Gegensatz zu den übrigen Punkten nicht wiederhergestellt werden kann.

15.2.3 Testen der Sicherheit durch eigene Angriffe

Ein sehr probates Mittel zum Testen der Sicherheitseinstellungen ist der eigene Angriff auf das Netzwerk und die Computer.

Bevor derartige Maßnahmen durchgeführt werden, muss in jedem Fall Rücksprache mit der Geschäftsführung gehalten werden. Diese muss den Angriffsversuchen auf das Unternehmen aus den eigenen Reihen vorher unbedingt zustimmen. Anderenfalls könnten die Angriffe falsch interpretiert werden, und der im guten Glauben handelnde Administrator wird zu einem Verdächtigen oder Sündenbock.

Selbst den Angreifer spielen

Um vielschichtige Angriffe ausführen zu können, sollten Sie natürlich auch über die Programme und Werkzeuge verfügen, die ein potenzieller Hacker einsetzt. Besonders hilfreich ist in diesem Zusammenhang die Zusammenstellung derartiger Hackertools auf der Sicherheits-CD *Hackers best friend*. Diese CD wird ca. einmal jährlich aktualisiert herausgegeben.

Sie enthält eine umfangreiche Sammlung von Tools und Programmen mit ausführlichen Anleitungen, so dass der Administrator rasch in die Rolle des Hackers schlüpfen kann, um zu versuchen, in sein eigenes Netzwerk zu gelangen und dieses anzugreifen.

16 Sicherheitsstrategie für den ISA Server 2004

Das letzte Kapitel beschäftigt sich mit einer Sicherheitsstrategie für den ISA Server selbst. Selbstverständlich sollte für diese Komponente, die für die Bereitstellung von Sicherheit im internen Netzwerk verantwortlich ist, ebenfalls eine umfassende Absicherung gewährleistet sein. Ein ungeschützter ISA Server stellt ein hohes Risiko für die übrigen Ressourcen des Unternehmensnetzwerks dar. Zum Schutz des ISA Server gehört auch der Schutz des zugrunde liegenden Server-Betriebssystems.

Bei der Absicherung des Systems spricht man auch vom System Hardening. Hierzu gehören verschiedene Verfahrensweisen und Vorgehen, die in diesem Kapitel näher vorgestellt werden.

16.1 Sicherheitsrichtlinienkatalog für Maßnahmen und Zuständigkeiten

Richtlinien für den laufenden Betrieb

Mit dieser Form von Sicherheitsrichtlinie ist nicht die Richtlinie gemeint, die direkt am Betriebssystem konfiguriert werden kann, sondern vielmehr ein umfassendes Regelwerk für das Unternehmen, in dem Regeln und Maßnahmen für die Organisation, Einrichtung, den laufenden Betrieb und natürlich auch die Wartung und Schritte für einen Notfallplan zur Absicherung des Systems beschrieben werden. Zusätzlich müssen in dieser Richtlinie auch Regelerklärungen für die Mitarbeiter definiert werden, z.B. eindeutige Regelungen für die private Nutzung des Internets oder Hinweise zur Datenschutzerklärung oder zu sonstigen durch die Mitarbeiter nicht offen zu legenden Informationen.

Notfallpläne

Auch für den Notfall müssen Pläne definiert werden. So muss z.B. vorab gereglt sein, welche Schritte durchzuführen sind, wenn ein Angreifer in das interne Netzwerk gelangt ist. Dabei sind nicht nur die einzuleitenden technschen Maßnahmen (Abschottung oder Gegenangriff), sondern auch Regularien darüber, welche Personen zu informieren sind und wer über die Durchführung einer bestimmten Maßnahme zu entscheiden hat, zu dokumentieren.

Eine solche Sicherheitsrichtlinie macht natürlich wenig Sinn, wenn die dort beschriebenen Verfahrensweisen isoliert betrachtet werden.

Was ist damit gemeint? Der ISA Server ist ein Bestandteil des Netzwerks. Er selbst basiert auf einem Windows Server-Betriebssystem. Einige Verfahren erfordern nicht nur Maßnahmen am ISA Server selbst, sondern auch an anderen Komponenten des Netzwerks. So machen z.B. festgelegte Verfahren für die Sicherung des ISA Server nur dann Sinn, wenn gleichzeitig auch dieselben Verfahren für das Betriebssystem festgelegt sind.

Lohnender Konfigurationsaufwand

Sie sehen also schon anhand dieses kleinen Beispiels, dass die Implementierung und Festlegung von Kriterien für die Sicherheitsrichtlinien einen nicht zu unterschätzenden Konfigurationsaufwand bedeuten. Behalten Sie allerdings dabei immer den folgenden Gedanken im Hinterkopf: Die sorgfältige einmalige Planung der entsprechenden Richtlinien wird später im laufenden Betrieb viel Zeit und damit auch Kosten einsparen, da auf festgeschriebene Regeln und Verfahrensabläufe zurückgegriffen werden kann.

16.2 Personal-Qualifikation

Nicht nur für die Verwaltung des ISA Server, sondern auch für die Verwaltung weiterer Server und anderer Netzwerkkomponenten muss qualifiziertes Personal eingesetzt werden. Auch wenn z.B. Schulungen des Personals mit Kosten verbunden sind, so sollte dennoch immer darüber nachgedacht werden, dass eine Fortbildung des zuständigen Mitarbeiters möglicherweise auf die Dauer Folgekosten einspart, die z.B. durch Behebungen von Fehlbedienung oder -konfiguration entstehen könnten.

Ein weiterer wichtiger Punkt ist es auch, den Administratoren immer nur die Berechtigungen zuzuweisen, die für seine Aufgaben notwendig sind. Der ISA Server bietet hierzu verschiedene Verwaltungsrollen. In der Enterprise-Version des ISA Server können Sie sogar auf verschiedenen Ebenen wie dem übergeordneten Unternehmen oder nur einem einzelnen Array Administrationsrechte zuweisen.

Outsourcing

Sollte Ihr Unternehmen weder über das notwendige Know-how noch über Kosten (und Zeit) verfügen, Mitarbeiter ausreichend ausbilden und schulen zu lassen bzw. einen neuen Mitarbeiter einzustellen, so sollten Sie über die Auslagerung der Verwaltung an ein externes Consulting-Unternehmen nachdenken. Hiermit sind zwar auch laufende Kosten verbunden, allerdings erhalten Sie dafür ein auf Ihre Bedürfnisse angepasstes funktionierendes System, für das sie selbst keinen Verwaltungsaufwand aufbringen müssen und für das der externe Dienstleister die Verantwortung trägt. Selbstverständlich hängt dies vom Umfang des Outsourcing-Vertrags mit dem Dienstleister ab, inwieweit die Betriebsverantwortung ebenfalls abgegeben wird.

16.3 Physikalische Absicherung

Eine Absicherung des ISA Server 2004 muss auf zweierlei Ebenen erfolgen. Zunächst einmal muss der Server selbst physikalisch abgesichert werden. Dazu muss der Server auch hinsichtlich der Software sicher gestaltet werden.

16.3.1 Physikalische Absicherung des Servers

Serverraum

Zur physikalischen Absicherung zählt, dass sich der Server in einem abgeschlossenen Raum befindet, so dass kein Zugriff auf den Server erfolgen kann. Die Schlüssel für diesen Raum sollte nur der Personenkreis der Administratoren erhalten. Ansonsten besteht die Gefahr, die Festplatte des Servers zu entfernen und auszulesen, den Computer mit einer Diskette zu starten und die Festplatte zu formatieren oder auch die Tastatur durch eine speziell präparierte Tastatur auszutauschen, die sämtliche Eingaben inklusive des Passworts aufzeichnen kann. Zusätzlich sollten Sie das BIOS des Servers mit einem Passwort schützen. Achten Sie also darauf, das Gehäuse des Servers immer verschlossen zu halten und den Schlüssel an einem sicheren Ort zu deponieren. Um die Server gegen Diebstahl zu schützen, können diese beispielsweise in abschließbaren Racks aufbewahrt werden. Weitere Sicherheitsmaßnahmen sind eine Zugangskontrolle zum Serverraum oder auch ein Bewegungsmelder innerhalb dieses Raums.

Backup-Medien

Zusätzlich sollten Sie die Backup-Bänder des ISA Server sowie natürlich auch anderer Server grundsätzlich an einem anderen Ort als dem Standort des Servers aufbewahren. Auch der Einsatz einer USV (Unterbrechungsfreie Stromversorgung) kann den Server vor Schäden bei einem Stromausfall schützen.

Unterschätzen Sie niemals die physikalische Sicherung der Server. Sobald es einem Angreifer gelingt, sich unbemerkt Zutritt zu einem Gerät zu verschaffen, bedeutet dies in aller Regel den Anfang vom Ende der Sicherheit im Netzwerk.

16.3.2 Softwareinstallation auf dem Server

Als Grundregel sollte für einen Server immer gelten, dass Sie auf diesem nicht mehr Applikationen als notwendig installieren. Keinesfalls darf der ISA Server 2004 bezüglich der Softwareinstallation wie ein Clientcomputer behandelt werden. Somit schließen Sie aus, dass ein Angreifer über mögliche Sicherheitslücken in den installierten Applikationen Zugriff auf den Server erhält.

Backup-Programm

Auf jeden Fall sollten Sie auf dem Server ein Backup-Programm ausführen, sofern Sie nicht das integrierte Windows-Backup benutzen. Des Weiteren sollte es selbstverständlich sein, dass auf dem Server auch ein Antivirenprogramm installiert ist. Dabei müssen Sie entscheiden, ob Sie sich für eine serverbasierte Lösung entscheiden, die sämtliche Clients im Netzwerk ebenfalls vor Viren schützt, oder ob Sie für jeden Client einzeln eine Antivirensoftware einsetzen möchten.

Kein Applikationsserver

Des Weiteren sollte der ISA Server auch nicht als Applikationsserver fungieren. Es sollten also weder für das interne noch für das externe Netzwerk Programme auf dem ISA Server bereitgestellt werden. Jede auf dem ISA Server installierte Anwendung ist eine potenzielle Sicherheitslücke für das System. Stattdessen stellen Sie Applikationen für externe Benutzer auf veröffentlichten Servern bereit oder installieren Sie die Programme auf Servern, die sich in der DMZ befinden.

16.3.3 Antiviren-Software

Es sollte eigentlich nicht notwendig sein zu erwähnen, dass auch der ISA Server durch einen Virenscanner geschützt werden muss. Insbesondere da der ISA Server die Schnittstelle zwischen Firmennetzwerk und Internet bildet, müssen an dieser Stelle Viren abgewehrt werden, bevor diese in das interne Netzwerk gelangen können. Ebenso sollte selbstverständlich sein, dass der Virenscanner durch automatische Updates stets auf dem aktuellen Stand zu halten ist.

Auch Gateway-basiert

Zusätzlich zum Virenscanner können auf dem ISA Server auch Intrusion Detection-Systeme (ID-Systeme) oder Gateway-basierte Virenscanner (zur Prüfung des gesamten Datenverkehrs von extern nach intern) oder Content Management-Systeme installiert werden: alle ebenfalls zu dem Zweck, einen Angreifer quasi vor den Pforten des internen Netzwerks bereits abzufangen.

Eine Übersicht über Drittanbieterlösungen – nicht nur für den Virenschutz – finden Sie unter dem Link *http://www.microsoft.com/isaserver/partners/default.mspx*.

16.4 Absichern des Betriebssystems

Als Grundlage für die Absicherung des ISA Server muss die Absicherung des zugrunde liegenden Betriebssystems Windows Server 2000 oder Windows Server 2003 gewährleistet sein. Auch im Betriebssystem müssen potenzielle Sicherheitslücken geschlossen werden und möglichst kein Ziel für Angriffe bestehen. Um dies sicherzustellen, sollten auf dem Server möglichst alle nicht benötigten Dienste deakti-

viert werden. Des Weiteren sollten auch nur die Windows-Komponenten installiert sein, die unbedingt zur Funktion des Servers notwendig sind. Ferner ist auch die Arbeit mit Sicherheitsvorlagen ein wichtiger Punkt.

16.4.1 Deaktivieren unnötiger Dienste

Sicherheitsrisiko Dienste

Eine weitere wichtige Aufgabe ist das Deaktivieren aller nicht vom Betriebssystem und dem ISA Server benötigten Dienste. Ein deaktivierter Dienst kann kein potenzielles Sicherheitsrisiko mehr darstellen. Die folgende Tabelle gibt Ihnen eine Übersicht über alle vom Betriebssystem bzw. vom ISA Server benötigten Dienste sowie die empfohlene Startart für den jeweiligen Dienst.

Tabelle 16.1: Übersicht über die vom Betriebssystem und dem ISA Server benötigten Dienste sowie deren empfohlener Startart

Name	Funktion	Empfohlene Startart
COM+	Betriebssystem	Manuell
Kryptographische Dienste	Betriebssystem/ Sicherheit	Automatisch
Ereignisanzeige	Betriebssystem	Automatisch
IPSec-Dienste	Betriebssystem/ Sicherheit	Automatisch
Logischer Festplattenmanager	Betriebssystem/ Festplatten	Automatisch
Logischer Festplattenmanager Verwaltungsdienst	Betriebssystem/ Festplatten	Manuell
Microsoft Firewall	ISA Server	Automatisch
Microsoft ISA Server Control	ISA Server	Automatisch
Microsoft ISA Server Job Scheduler	ISA Server	Automatisch
Microsoft ISA Server Storage	ISA Server	Automatisch
MSSQL$MSFW	ISA Server/MSDE-Logging	Automatisch
Netzwerkverbindungen	Betriebssystem/ Netzwerk	Manuell
NTLM Security Support Provider	Betriebssystem/ Sicherheit	Manuell
Plug&Play	Betriebssystem	Automatisch
Protected Storage	Betriebssystem/ Sicherheit	Automatisch

Name	Funktion	Empfohlene Startart
Remote Access Connection Manager	ISA Server	Manuell
RPC	Betriebssystem	Automatisch
Secondary Logon	Betriebssystem/ Sicherheit	Automatisch
Sam Security Accounts Manager	Betriebssystem	Automatisch
Server	ISA Server/Client Freigabe	Automatisch
Smartcard	Betriebssystem/ Sicherheit	Manuell
SQLAgent$MSFW	ISA Server/MSDE-Logging	Manuell
System Event Notification	Betriebssystem	Automatisch
Telefonie	ISA Server	Manuell
VDS Virtual Disc Service	Betriebssystem/ Festplatten	Manuell
WMI (Windows Management Instrumentation)	Betriebssystem/WMI	Automatisch
WMI Performance Adapter	Betriebssystem/WMI	Manuell

16.4.2 Auswahl der installierten Windows-Komponenten

Nicht benutzte Server-Komponenten

Grundsätzlich sollten auf dem Windows Server immer nur die Windows-Komponenten installiert werden, die für die Funktion und Dienstbereitstellung des Servers unverzichtbar sind. Deshalb sollten Sie unter der Systemsteuerung/Software unter WINDOWS-KOMPONENTEN HINZUFÜGEN/ENTFERNEN überprüfen, ob dort verzichtbare Komponenten vorhanden sind. Häufig installierte Komponenten, die jedoch in der produktiven Umgebung auf dem Server nicht benötigt werden, sind z.B. DHCP-Server, WINS-Server, Terminalserver oder RIS-Server (Remote Installation Service).

16.4.3 Arbeiten mit Sicherheitsvorlagen

Standardisierte Einstellungen

Über Sicherheitsvorlagen werden sicherheitsrelevante Einstellungen z.B. für Kontenrichtlinien, Überwachungsrichtlinien, Dienstekonfiguration, Registry-Konfiguration usw. vorgenommen. Sicherheitsvorlagen können sowohl auf Windows Server 2000 als auch auf Windows Server 2003 angewendet werden. Bei der Konfigurationsdatei für eine Sicherheitsvorlage handelt es sich immer um eine *.inf*-Datei.

13 vordefinierte Vorlagen

Insgesamt stellt Windows 13 verschiedene Sicherheitsvorlagen bereit. Selbstverständlich können alle diese Vorlagen nach dem Import in ein GPO noch weiter angepasst werden. Sämtliche Vorlagen befinden sich im Verzeichnis `%Systemroot%\Security\Templates`. Tabelle 16.2 gibt Ihnen eine Übersicht über die Sicherheitsvorlagen und deren Einsatzgebiet.

Tabelle 16.2: Die Sicherheitsvorlagen und ihre Bedeutungen

Sicherheitsvorlage	Beschreibung
Basicdc.inf	Basis-Sicherheitseinstellungen für Domänen controller
Basicsv.inf	Basis-Sicherheitseinstellungen für Server
Basicwk.inf	Basis-Sicherheitseinstellungen für Client-Computer
Compatws.inf	Kompatible Sicherheitseinstellungen für Server und Client-Computer
DC security.inf	Aktualisierte Basis-Sicherheitseinstellungen für Domänencontroller
Hisecdc.inf	Hochsicherheitseinstellungen für Domänen controller
Hisecws.inf	Hochsicherheitseinstellungen für Server und Client-Computer
Notssid.inf	Die Benutzer-SID des Terminalservers wird vom Windows 2000 Server entfernt.
Ocfiless.inf	Optionale Komponentendateisicherheit für Server
Ocfilesw.inf	Optionale Komponentendateisicherheit für Client-Computer
Securedc.inf	Sichere Sicherheitseinstellungen für Domänencontroller
Securews.inf	Sichere Sicherheitseinstellungen für Server und Client-Computer
Setup security.inf	Vordefinierte standardmäßige Sicherheitseinstellungen

Sobald eine Sicherheitsvorlage definiert ist, können Sie darüber das Betriebssystem konfigurieren. Auf diese Weise ist eine Homogenität der Konfigurationen der Betriebssysteme sichergestellt.

Mit den Basis-Sicherheitseinstellungen (*basic*.inf*) werden alle Sicherheitsbereiche abgedeckt bis auf die Bereiche, die mit speziellen Benutzerrechten verknüpft sind. Diese Bereiche können beispielsweise durch die Installation einer Applikation mit den entsprechenden Benutzerrechten angepasst werden.

Die kompatible Sicherheitseinstellung (*compat*.inf*) schränkt die Berechtigungen der Gruppe *Hauptbenutzer* ein. Dieser Gruppe gehören unter Windows standardmäßig alle authentifizierten Benutzer an. Allerdings kann diese Gruppenzugehörigkeit ein zu hohes Risiko bedeuten, sodass die Benutzer lieber nur mit den Berechtigungen der Gruppe Benutzer ausgestattet werden sollten. Die Berechtigungen werden für Dateien, Ordner oder auch Registry-Schlüssel so eingestellt, dass die Benutzer zwar noch ihre Applikationen ausführen können, aber keine darüber hinaus gehenden Rechte besitzen.

Die Hochsicherheitseinstellungen (*hisec*.inf*) sorgen für hohe Sicherheit im Netzwerkverkehr. Deshalb können die Windows 2000/XP-Computer, die eine Hochsicherheitsvorlage benutzen, nur mit anderen Windows 2000/XP-Computern kommunizieren. Ein Austausch mit Computern, die das Betriebssystem Windows 9x oder NT ausführen, ist nicht möglich.

Über die sicheren Sicherheitsvorlagen (*secure*.inf*) werden sichere, empfohlene Einstellungen an allen Bereichen außer Dateien, Ordnern und Registry-Schlüsseln durchgesetzt. Die Bereiche der Registry und des Dateisystems sind bereits standardmäßig sicher konfiguriert.

16.4.4 Arbeiten mit einer Sicherheitsvorlage

Eigene mmc

Um mit den Sicherheitsvorlagen arbeiten zu können, sollten Sie zunächst eine eigene mmc einrichten. Fügen Sie dazu das Snap-In SICHERHEITSVORLAGEN zu einer leeren mmc hinzu. In dieser mmc können Sie nun darangehen, die eben beschriebenen Vorlagen zu bearbeiten.

Wenn Sie eine Vorlage öffnen, befinden sich darin die Knoten, die auch in der Sicherheitsrichtlinie enthalten sind (siehe Abbildung 16.1). Sie können hier nun beliebige Änderungen und Anpassungen durchführen.

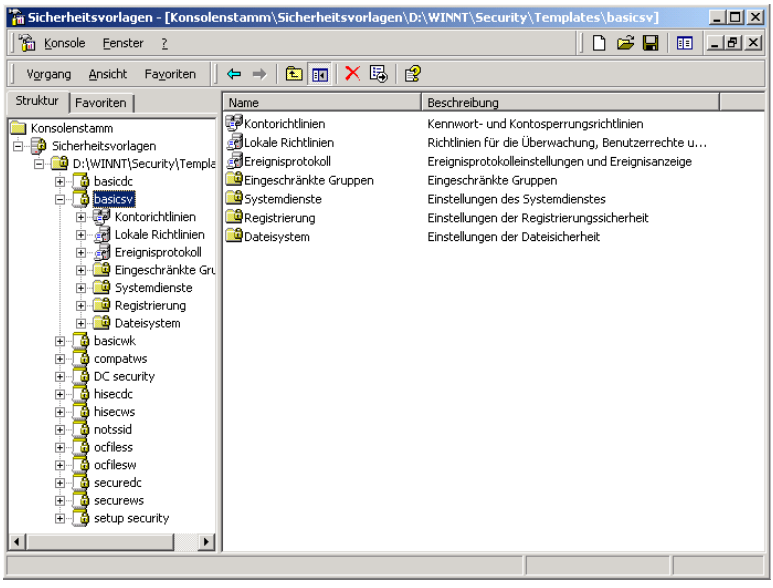


Abbildung 16.1: Die mmc-Sicherheitsvorlagen

Nach Abschluss der Änderungen sollten Sie die neue Vorlage unter einem anderen Namen speichern. Diese neue Vorlage erscheint dann ebenfalls in der mmc. Wählen Sie aus dem Kontextmenü der neuen Vorlage BESCHREIBUNG FESTLEGEN und geben Sie dann eine Beschreibung für die neue Vorlage an. So werden Sie immer schnell den Überblick über die Inhalte der selbst definierten Vorlagen behalten.

Neue Sicherheitsvorlage

Um eine neue Sicherheitsvorlage zu erzeugen, wählen Sie aus dem Kontextmenü des Pfades NEUE VORLAGE. Geben Sie der neuen Vorlage einen Namen und eine Beschreibung. Die neue Vorlage enthält alle Knoten, die auch die übrigen Sicherheitsvorlagen enthalten. Sie können hier nun die gewünschten Richtlinien einrichten.

Sämtliche Vorlagen können auch importiert bzw. Einstellungen daraus exportiert werden.

1. Um eine Sicherheitsvorlage in ein GPO zu importieren, wählen Sie in der mmc des GPO den Knoten COMPUTERKONFIGURATION/WINDOWS-EINSTELLUNGEN/SICHERHEITSEINSTELLUNGEN und aus dessen Kontextmenü den Eintrag RICHTLINIE IMPORTIEREN.
2. Im folgenden Fenster sehen Sie dann alle Vorlagen, die im Pfad `%Systemroot%\Security\Templates` abgelegt sind. Wählen Sie dort die gewünschte Vorlage aus.

Die neue Sicherheitsvorlage wird erst ab dem Moment gültig, in dem das GPO auf den Computer angewendet wird. Die Richtlinienübertragung findet standardmäßig alle acht Stunden statt. Wollen Sie nicht so lange warten, starten Sie entweder den Computer neu oder

geben an der Eingabeaufforderung folgenden Befehl ein:
`secedit /refreshpolicy machine_policy` ↵.

Des Weiteren besteht auch die Möglichkeit, Einstellungen an den Sicherheitsrichtlinien zu exportieren. Wählen Sie dazu STARTMENÜ/PROGRAMME/VERWALTUNG/LOKALE SICHERHEITSRICHTLINIE. Aus dem Kontextmenü des Knotens SICHERHEITSEINSTELLUNGEN wählen Sie RICHTLINIE EXPORTIEREN. Sie können dann entscheiden, ob Sie die lokale oder effektive Richtlinie exportieren möchten. Als Zielverzeichnis zum Speichern wird Ihnen der Ordner `%Systemroot%\Security\Templates` angegeben. Das Exportieren der lokalen Richtlinie kann sinnvoll sein, um diese Einstellungen zu einem späteren Zeitpunkt wieder zurückzuspielen, da das lokale GPO von domänenbasierten GPOs außer Kraft gesetzt wird.

16.4.5 Die Sicherheitskonfiguration

Prüfen der Sicherheitseinstellungen

Die Sicherheitskonfiguration und -analyse wird zum Überprüfen und Einstellen der Sicherheit verwendet. Hierzu wird eine eigene Sicherheitsdatenbank benutzt. Zur Einrichtung und Steuerung kann die mmc SICHERHEITSKONFIGURATION UND –ANALYSE eingerichtet werden. Fügen Sie dazu einer leeren Konsole das gleichnamige Snap-In hinzu.

Sobald Sie die neue mmc erstellt haben, befinden sich noch keine untergeordneten Knoten darin. Als Erstes müssen Sie eine Sicherheitsdatenbank anlegen. Diese Datenbank ist das Arbeitsverzeichnis für sämtliche Konfigurations- und Analysevorgänge. Wählen Sie aus dem Kontextmenü DATENBANK ÖFFNEN. Sie können nun entweder eine neue Sicherheitsdatenbank (*.sdb*-Datei) anlegen oder eine bereits bestehende öffnen. Wenn Sie eine neue Datenbank angelegt haben, müssen Sie im Fenster VORLAGE IMPORTIEREN eine Sicherheitsvorlage auswählen, die in die Datenbank geladen werden soll. Sie haben alle Vorlagen des Verzeichnisses `%Systemroot%\Security\Templates` zur Auswahl. Sobald die Datenbank angelegt ist, erscheinen die Knoten mit ihren Einstellungen in der mmc.

Vorlagenimport

Sie haben auch die Möglichkeit, mehrere Datenbanken anzulegen und in jede Datenbank eine Vorlage zu importieren. Die Inhalte der verschiedenen Arbeitsdatenbanken werden automatisch zu einer Verbundvorlage zusammengefasst. Wollen Sie hingegen in eine bestehende Datenbank eine neue Vorlage importieren, die die bereits geladene Vorlage überschreiben soll, so wählen Sie aus dem Kontextmenü VORLAGE IMPORTIEREN und aktivieren Sie die Checkbox DATENBANK VOR DEM IMPORTIEREN AUFRÄUMEN bei der Auswahl der Vorlage (siehe Abbildung 16.2).

Abbildung 16.2: Importieren von Vorlagen in die Sicherheitsdatenbank

Wird die Checkbox nicht aktiviert, so gelten bei Unterschieden zwischen den Vorlagen die Einstellungen der zuletzt importierten Sicherheitsvorlage. Außerdem wird keine Verbundvorlage angelegt, wenn das Überschreiben aktiviert ist.

16.4.6 Die Sicherheitsanalyse

Analyse der aktuellen Sicherheitseinstellungen

Anhand der in die Arbeitsdatenbank importierten Sicherheitsvorlagen können Sie die Sicherheit des Systems analysieren. Dabei wird der aktuelle Sicherheitsstand des Computers mit der importierten Sicherheitsvorlage verglichen. Bei der Wahl der geladenen Vorlagen sollten Sie immer darauf achten, dass diese zum Typ des zu prüfenden Rechners passen. Es macht wenig Sinn, Vorlagen für Domänencontroller auf einem Client-Computer zu testen oder umgekehrt. Um die Analyse zu starten, wählen Sie aus dem Kontextmenü COMPUTER JETZT ANALYSIEREN. Geben Sie dann den Pfad an, in dem das Protokoll der Analyse gespeichert werden soll. Während der Durchführung der Analyse erhalten Sie Statusinformationen über den gerade analysierten Bereich (siehe Abbildung 16.3).

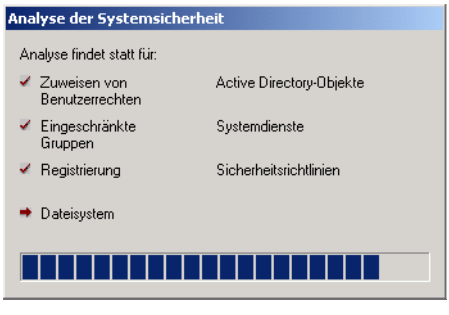


Abbildung 16.3: Statusanzeige der Sicherheitsanalyse

Ergebnisauswertung

Um die Ergebnisse zu betrachten, wählen Sie aus dem Kontextmenü PROTOKOLLDATEI ANSEHEN. Im Detailbereich der mmc sehen Sie alle getesteten Bereiche. Wollen Sie für spezielle Richtlinien die Ergebnisse sehen, so markieren Sie diese Richtlinie. Sie finden eine Gegenüberstellung der Datenbankeinstellung und der aktuellen Computereinstellung. Dabei werden übereinstimmende Werte mit einem grünen Häkchen gekennzeichnet, während Fehler ein rotes Kreuz aufweisen. Sind an einigen Richtlinieneinstellungen keine Symbole vorhanden, befand sich diese Richtlinie nicht in der importierten Vorlage und konnte deshalb nicht analysiert werden.

Die in die Arbeitsdatenbank importierten Vorlagen können nach der Analyse auf den Computer angewendet werden. Wählen Sie dazu aus dem Kontextmenü SYSTEM JETZT KONFIGURIEREN. Geben Sie einen Pfad für die Protokolldatei an. Während der Konfiguration sehen Sie wie bei der Analyse einen Statusbalken mit dem aktuellen Fortschritt. Die bei der Konfiguration vorgenommenen Änderungen werden jedoch nicht in der Sicherheitsvorlage, sondern in der Verbundvorlage in der Arbeitsdatenbank gespeichert. Um die Sicherheitsvorlage endgültig zu überschreiben, müssen Sie die Konfiguration unter demselben Namen wie dem der ursprünglichen Sicherheitsvorlage abspeichern.

Alternativ können Sie die Verbundvorlage der Arbeitsdatenbank auch als neue Sicherheitsvorlage exportieren. Wählen Sie dazu aus dem Kontextmenü VORLAGE EXPORTIEREN und geben Sie einen Namen und einen Pfad für die Datei an.

16.5 Implementieren sicherer Kennwörter

Das Implementieren sicherer Kennwörter, die die Windows-Komplexitätsanforderungen erfüllen, ist ein weiterer Schritt zur Sicherung des Netzwerks. Neben der Implementierung der entsprechenden Richtlinien ist hier auch die Schulung der Benutzer im Umgang mit dem Kennwort erforderlich. Es soll ja immer noch genügend Benutzer geben (selbst Administratoren), die ihr Kennwort auf einem Zettel unter der Tastatur oder an den Monitor geklebt aufbewahren. Insbesondere der Nutzen des regelmäßigen Änderns des Kennworts sowie der Anforderungen sollten den Benutzern eingehend nahe gebracht werden. Erklären Sie den Benutzern, dass sie ihr Kennwort genauso geheim halten sollten wie beispielsweise die PIN ihrer Kreditkarte.

Schlechte Kennwörter

Für die Wahl des Passworts sollten die Benutzer keine Begriffe wählen, die ein potenzieller Angreifer entweder durch persönliche Kenntnis des Benutzers oder durch andere Suchmethoden herausfinden könnte. Dazu zählen die folgenden Begriffe:

- Der Name von Kindern, Ehegatte, Haustier oder Freunden,
- ein beliebiges Wort, das sich in einem Wörterbuch finden lässt,
- ein Geburtsdatum, eine Telefonnummer oder weitere persönliche Nummern wie KFZ-Kennzeichen oder Kontonummern,
- ebenso wenig sollte ein Kennwort wieder benutzt werden, das bereits früher benutzt worden ist.

Sie erhalten den Hinweis für die Implementierung sicherer Kennwörter, nachdem Sie den Assistenten für die Herstellung der Internetverbindung abgeschlossen haben.

16.6 Einschränken der Benutzerrechte

Beabsichtigter und unbeabsichtigter Schaden

Indem den Benutzern zu hohe Berechtigungen zugewiesen werden, besteht eine Gefahr in zweierlei Weise. So können einerseits die Benutzer selbst ohne böse Absicht oder wider besseres Wissen schnell Schaden anrichten. Zudem besteht auch die Gefahr, dass im Falle des unberechtigten Zugriffs auf das Konto der Angreifer bereits über umfassende Berechtigungen verfügt.

Beim Erstellen der Benutzerkonten sollten Sie darauf achten, den Benutzern lediglich die notwendigsten Berechtigungen zu gewähren. Fügen Sie Benutzer mit denselben Berechtigungen immer zu Benutzergruppen zusammen. Auch für Netzwerkfreigaben sollten Sie immer nur die wirklich notwendigen Benutzerrechte und Dateirechte vergeben.

16.6.1 Sicherheitsaspekte für Administratoren

Anmeldung mit einem anderen Konto

Aus Sicherheitsaspekten sollte der Administrator nur dann unter dem Benutzerkonto *Administrator* oder unter einem anderen Konto mit Administratorrechten angemeldet sein, wenn er Aufgaben erledigen muss, für die er die entsprechenden Rechte unbedingt benötigt. Ansonsten sollte der Administrator sich mit einem Benutzerkonto mit weniger privilegierten Rechten anmelden. Ist der Administrator mit vollen Admin-Rechten angemeldet und holt er sich während eines Internet-Besuches einen Virus oder Trojaner, so werden alle Tätigkeiten des Virus ermöglicht, die dem aktuellen Benutzerkonto möglich sind. Bei Administratorrechten können so Daten gelöscht oder Festplatten formatiert werden. Melden Sie sich deshalb über ein Konto an, dem nur minimale Rechte zugewiesen sind.

Achten Sie ferner darauf, dass nicht mehr Konten als notwendig über administrative Berechtigungen verfügen.

Sollte es dabei jedoch vorkommen, dass unvorhergesehen das Ausführen einer bestimmten Aufgabe die Administratorrechte verlangt, so kann diese Aktion dennoch unter dem gerade aktuellen Benutzerkonto ausgeführt werden, ohne dass eine Abmeldung und Neuanmeldung als Administrator am Computer erfolgen muss. Hierzu gibt es die Optionen *Ausführen als* in der grafischen Oberfläche sowie die Kommandozeilenoption *RUNAS*.

16.6.2 Die Option Ausführen als

Programmausführung mit anderen Berechtigungen

Sie können jede ausführbare Datei, jede mmc und jedes Element der Systemsteuerung mit der Option *Ausführen als* starten. Dazu müssen Sie lediglich über einen Benutzernamen und ein Passwort verfügen, womit das gewünschte Programm ausgeführt werden darf. Es kann jedoch möglich sein, dass diese Option fehlschlägt, wenn Sie über das Netzwerk ein Programm auf einem anderen Computer ausführen möchten. Dies ist der Fall, wenn das Benutzerkonto, das Sie bei *Ausführen als* angeben, nicht mit dem Konto identisch ist, von dem das Programm ursprünglich gestartet wurde, selbst wenn die Rechte des Ausführen-Kontos ausreichend sind.

Um diese Option zu benutzen, führen Sie die folgenden Schritte aus:

1. Stellen Sie fest, ob unter DIENSTE der Dienst DIENST AUSFÜHREN ALS gestartet ist. Falls dies nicht der Fall ist, starten Sie den Dienst manuell.
2. Markieren Sie die Programmdatei, Verknüpfung, mmc oder das Systemsteuerungselement, das Sie ausführen möchten. Halten Sie die Umschalt-Taste ⇧ gedrückt und wählen Sie dann aus dem Kontextmenü AUSFÜHREN ALS.
3. Geben Sie nun an, unter welchem Konto Sie das Programm ausführen möchten. Dazu sind Angaben über Benutzername, Kennwort und Domäne notwendig (siehe Abbildung 16.4).

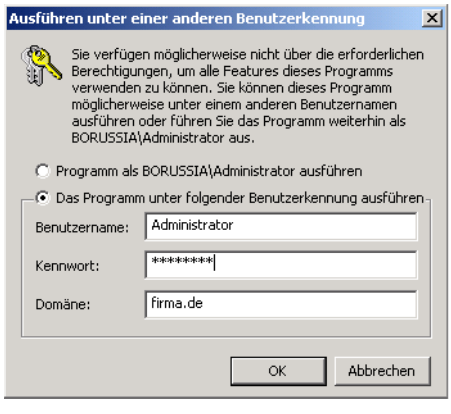


Abbildung 16.4: Die Option Ausführen als

16.6.3 Verwenden von RUNAS

„Ausführen als“ an der Kommandozeile

Das Programm *RUNAS* wird von der Kommandozeile aus gestartet. Es erfüllt denselben Zweck wie das eben beschriebene *Ausführen als*. Prüfen Sie auch hier zuvor, ob unter Dienste der Dienst DIENST AUSFÜHREN ALS gestartet ist. *RUNAS* bietet die folgenden Optionen:

```
runas [/profile] [/env] [/netonly] /user:Kontoname
Programmpfad
```

Die optionalen Parameter haben folgende Bedeutung:

`/profile`: Profilpfad des Benutzerkontos, nur nötig, wenn ein Profil geladen werden muss

`/env`: wenn die Netzwerkumgebung statt der lokalen Umgebung verwendet werden soll

`/netonly`: wenn die Benutzerinformationen nur für den Remotezugriff gültig sind

`/user`: im Format Computername\Konto bzw. unter 2000 Konto@Computername

Programmpfad: Pfad zur ausführbaren Datei. Befinden sich Leerzeichen im Programmpfad, müssen die Angaben in Anführungszeichen gesetzt werden.

Eine RUNAS-Befehlszeile könnte folgendermaßen aussehen:

```
runas /user: Administrator@hippokrates.firma.de "mmc
%windir%\system32\Konsole1.msc" ↵
```

Das Passwort für das Konto können Sie nach der Aufforderung eingeben.

Des Weiteren sollten für die Benutzung des Administratorkontos folgende, eigentlich selbstverständliche Regeln gelten:

- Benutzen Sie auf jeden Fall ein sicheres Kennwort für das Konto
- Geben Sie das Kennwort niemals weiter und notieren Sie dieses nicht in der Nähe des Computers
- Melden Sie sich für tägliche Aufgaben nicht mit dem Administratorkonto an
- Lassen Sie den Computer nicht unbeaufsichtigt, wenn Sie unter dem Administratorkonto angemeldet sind. Sperren Sie den Computer, wenn Sie ihn auch nur kurzzeitig verlassen.

16.6.4 Sichern der Netzwerkfreigaben

Restriktive Berechtigungen festlegen

Bei sämtlichen Netzwerkfreigaben, die vom System automatisch eingerichtet werden, sind die Berechtigungen sehr restriktiv gesetzt, um die Unternehmensdaten vor unberechtigtem Zugriff zu schützen. Diesem Prinzip sollten Sie auch bei allen weiteren Freigaben treu bleiben.

Um zu ermitteln, welche Freigaben auf dem Server vorhanden sind, geben Sie an der Eingabeaufforderung den Befehl \\Servername ein.

Bei den aufgelisteten Freigaben handelt es sich sicherlich teilweise um selbst erstellte Freigaben, deren Berechtigungen Sie überprüfen sollten. Öffnen Sie dazu über die EIGENSCHAFTEN die Registerkarte SICHERHEIT und prüfen Sie die Berechtigungen, die den Benutzern und Gruppen für die Freigabe zugewiesen worden sind, und schränken Sie diese notfalls ein.

16.6.5 Ändern des Administratorkontonamens

Ändern des Kontonamens

Ein weiterer Schritt zur Absicherung des Administratorkontos ist das Umbenennen des vordefinierten Kontos Administrator. Da das Administratorkonto nicht gesperrt werden kann, während mit denselben Berechtigungen ein anderes Konto benutzt wird, kommt nur ein Umbenennen des Kontos in Frage. So hat ein potenzieller Angreifer keine Chance, wenn er sich mit dem Konto *Administrator* anmeldet und versucht, das Kennwort zu erraten, da es ein Konto diesen Namens nicht mehr gibt.

Nachdem Sie das Administratorkonto umbenannt haben, müssen Sie sich unbedingt neu am ISA Server 2004 anmelden, da Ihnen ansonsten der Zugriff auf Verwaltungswerkzeuge oder weitere Ressourcen verweigert wird, solange Sie noch unter dem alten Administratorkonto angemeldet sind.

1. Um den Kontonamen zu ändern, öffnen Sie in der Serververwaltung den Eintrag BENUTZER. Wählen Sie aus dem Kontextmenü die EIGENSCHAFTEN und öffnen Sie die Registerkarte ALLGEMEIN. Im Textfeld ANZEIGENAME tragen Sie den neuen Namen für das Konto ein.
2. Wechseln Sie dann auf die Registerkarte KONTO und tragen Sie unter BENUTZERANMELDENAME denselben neuen Kontonamen ein. Dieser Name muss auch unter BENUTZERANMELDENAME (PRÄ-WINDOWS 2000) eingetragen werden. Klicken Sie dann auf OK.

Des Weiteren können Sie auch auf den Clients das lokale Administratorkonto umbenennen.

1. Unter Windows 2000 und XP öffnen Sie SYSTEMSTEUERUNG/VERWALTUNG/COMPUTERVERWALTUNG.
2. Öffnen Sie in der Konsole LOKALE BENUTZER UND GRUPPEN und darunter BENUTZER. Wählen Sie aus dem Kontextmenü von *Administrator* den Eintrag UMBENENNEN und ändern Sie den Namen.

Um auf sämtlichen Clientcomputern den Namen des Administratorkontos zu ändern, verwenden Sie die GPMC (Group Policy Management Console).

Deaktivieren des Administrator-Kontos

Es kann auch sinnvoll sein, ein anderes Benutzerkonto mit den vollständigen administrativen Berechtigungen auszustatten und das ursprüngliche Administrator-Konto zu deaktivieren. Als zusätzlichen Schutz können Sie überwachen, ob Anmeldeversuche mit dem Konto *Administrator* stattfinden.

16.7 Aktualisierung durch Updates

Ein weiterer Schritt zur Sicherung des Netzwerks ist die rechtzeitige Aktualisierung der Betriebssystem-Software durch die von Microsoft bereitgestellten Service Packs, Updates und Patches, um bekannte Sicherheitslücken zu schließen. Dieses gilt gleichermaßen sowohl für den ISA Server 2004 sowie das zugrunde liegende Serversystem selbst als auch für die einzelnen Clientcomputer.

WSUS oder SUS

Der beste Weg hierzu ist der Einsatz der *Software Update Services (SUS)* bzw. dessen Nachfolger *WSUS* (*Windows Server Update Services*). Alternativ dazu können Sie auch das automatische Windows-Update verwenden.

16.7.1 Aktualisierung weiterer Applikationen

Microsoft Office

Des Weiteren sollten Sie darauf achten, dass Sie auch Applikationen wie Microsoft Office oder Applikationen anderer Hersteller regelmäßig auf Updates hin prüfen und sich für diese eine Verteilstrategie überlegen. Für Microsoft Office-Produkte ist die automatische Verteilung der Updates in die aktuelle Version des *WSUS* implementiert. Für ein automatisches Update verwenden Sie den Link *http://office.microsoft.com/OfficeUpdate/default.aspx*. Für das Update werden ausschließlich die Office-Versionen 2000, XP und 2003 unterstützt.

Um nach Updates für weitere Applikationen zu suchen, schauen Sie auf den entsprechenden Websites nach oder lassen Sie sich automatisch über neue Updates informieren, sofern der Hersteller dieses anbietet.

ISA Server-Updates

Speziell für die Updates des ISA Server finden Sie die gewünschten Informationen und Dateien unter dem Link *http://www.microsoft.com/isaserver/downloads/2004/default.mspx*.

Um sich regelmäßig über Updates informieren zu lassen, können Sie im Microsoft Subscription Center Newsletter abonnieren, die Sie mit aktuellen Informationen zu Patches-Sicherheitslücken versorgen.

http-Filtersignaturen

Auch das regelmäßige Prüfen von http-Filtersignaturen ist ein Bestandteil zur softwareseitigen Absicherung des ISA Server. Eine stets aktuelle Auflistung wichtiger http-Filtersignaturen finden Sie unter dem Link *http://www.msisafaq.de/Tools/HTTPFilter.htm*.

16.7.2 Updates der Betriebssysteme und Applikationen

Aktualisierung von Windows 9x und NT

Bei Clients, die noch unter Windows 9x oder NT 4.0 oder früher betrieben werden, sollten Sie über ein Update auf Windows 2000 oder XP Professional nachdenken. Diese Betriebssysteme garantieren eine bessere Leistung und Sicherheit im Windows-Netzwerk. Zudem werden zunehmend mehr Applikationen wie z.B. Office 2003 als Betriebssystem Windows 2000 Professional mit mindestens Service Pack 3 oder Windows XP erfordern und sind unter früheren Windows-Versionen nicht mehr lauffähig.

16.8 Absichern des ISA Server

Auch für die Absicherung des ISA Server selbst stehen verschiedene Möglichkeiten zur Verfügung. Generell sollte der ISA Server nach Möglichkeit auf dem Betriebssystem Windows Server 2003 installiert werden, da dieses gegenüber dem Windows Server 2000 zahlreiche Verbesserungen (auch in der Beseitigung von Sicherheitslücken) bietet.

16.8.1 Wahl der Serverrolle

Domänencontroller

Wie bereits in Kapitel 2 diskutiert, kann der ISA Server sowohl auf einem Domänencontroller als auch auf einem Mitgliedserver oder als allein stehender Server eingerichtet werden. Aus Sicherheitsgründen, insbesondere zum Schutz der Domäne, sollte der ISA Server nach Möglichkeit nicht direkt auf dem Domänencontroller installiert werden. Obwohl dies technisch gesehen durchaus möglich ist (beim Einsatz des SBS 2003 wird die ISA-Komponente schließlich auch direkt auf dem Domänencontroller installiert), sollte dies nach Möglichkeit nicht umgesetzt werden.

Mitgliedserver

Eine Installation als Mitgliedserver ist nicht sinnvoll, wenn der ISA Server direkt mit dem Internet verbunden wird (in der Konstellation als Front-Firewall oder Edge-Firewall). Sofern der ISA Server jedoch in der Konstellation als Backend-Server ausgeführt wird, kann dieser dennoch auf einem Mitgliedserver der Domäne installiert werden.

Separate Gesamtstruktur

In Microsoft-Whitepapern ist zu lesen, dass die Installation des ISA Server in einer separaten Gesamtstruktur erfolgen sollte. Diese Konfiguration macht bei der Installation eines einzelnen ISA Server keinen Sinn und sollte nur verwendet werden, wenn zahlreiche ISA Server eingesetzt werden sollen. Bei der Einrichtung einer separaten Gesamtstruktur können Sie für diesen Gruppenrichtlinien bestimmen und beim Einsatz der ISA Server Enterprise-Version die Informationen der Arrays im Active Directory speichern.

Generell sollte die Installation des ISA Server erst erfolgen, nachdem wie in dem vergangenen Kapitel beschrieben das zugrunde liegende Betriebssystem abgesichert wurde sowie auch die weiteren Faktoren (physikalische Absicherung, Personalschulung, Maßnahmenkatalog und Unternehmensrichtlinien) entsprechend organisiert sind.

16.8.2 Erstellen von Zugriffsregeln

Der ISA Server sollte auch erst mit dem Internet verbunden werden, nachdem er vollständig eingerichtet und konfiguriert wurde. In der Grundkonfiguration verfügt der ISA Server lediglich über eine Standardregel, die sämtlichen Netzwerkverkehr verweigert. Auf diese Weise wird sichergestellt, dass der Administrator zunächst mit hoffentlich überlegten Schritten die Firewall öffnen muss, anstatt eine nach der Installation bereits offene Firewall nach und nach wieder schließen zu müssen, wobei er wichtige Punkte übersehen könnte, die wiederum ein Sicherheitsrisiko darstellen.

Übersichtliches Regelwerk erstellen

Generell gilt für die Erstellung von Zugriffsregeln, dass deren Inhalte immer nur so wenig Handlungsspielraum wie möglich zulassen sollten. Erstellen Sie dabei insgesamt so wenig Regeln wie möglich. In einem umfangreichen Regelwerk kann selbst der Administrator schnell den Überblick verlieren, wenn in diesem anstelle von Ausnahmen für eine Regel eigene Regeln als Ausnahmen definiert werden.

Bevor Sie mit dem Erstellen von Regeln beginnen, sollten Sie ermitteln, welche Kommunikationstypen, d.h. welche Protokolle zwischen dem internen und externen Netzwerk sowie zum ISA Server benötigt werden. Benötigen Sie dabei noch nicht im ISA Server vordefinierte Protokolle, so erstellen Sie diese. Legen Sie danach Des Weiteren alle benötigten Regelelemente wie Computersätze, Benutzersätze oder URL-Sätze an.

Systemrichtlinie Nach diesen Vorkonfigurationen sollte die Systemrichtlinie des ISA Server angepasst werden. Hier können Sie festlegen, welche Protokolle beispielsweise für den Zugriff auf den ISA Server selbst zugelassen sind. Über die Systemrichtlinie werden sämtliche Zugriffe, die auf den ISA Server selbst erfolgen dürfen, definiert.

Dokumentation Sowohl bei der Konfiguration der Systemrichtlinie als auch besonders bei der Erstellung der Firewallrichtlinien sollten Sie eine korrekte Dokumentation der einzelnen Schritte vornehmen. So sollte für jede Regel angegeben werden, zu welchem Zweck sie erstellt wurde und was über sie zugelassen bzw. verweigert werden soll. So behalten Sie auch bei einem komplexeren Richtlinienumfang immer noch den Überblick.

Reihenfolge der Abarbeitung Sofern Sie mehrere Richtlinien erstellen (was eigentlich immer der Fall sein wird), müssen Sie auch unbedingt auf die Abarbeitungsreihenfolge der einzelnen Regeln achten. Bedenken Sie, dass eine falsche Reihenfolge der Regeln zu Problemen beim Zugriff führen kann. Einen versehentlich verweigerten Zugriff werden Sie bzw. Ihre Mitarbeiter sicherlich schnell bemerken. Anders verhält es sich jedoch, wenn versehentlich zu viele Zugriffsberechtigungen erteilt worden sind. Wenn es die Konfiguration zulässt, sollten Sie aus Gründen der Performance die am häufigsten benutzten Firewall-Richtlinien an den Anfang der Abarbeitungsreihenfolge stellen.

16.8.3 Aktivieren von Komponenten

Nicht benötigte ISA-Komponenten deaktivieren Für den ISA Server selbst gilt wie auch für das Betriebssystem, dass dort nur die Komponenten aktiviert sein sollten, die für den Betrieb zwingend notwendig sind. Dies beginnt schon bei der Auswahl der gewünschten Komponenten während der Installation. Aber auch ein späteres Deaktivieren von Komponenten ist immer noch möglich. Wird der ISA Server beispielsweise nicht auch als VPN-Server eingesetzt, sollten Sie keine VPN-Verbindungen zulassen. Ist auf dem ISA Server keine Zwischenspeicherung vorgesehen, so sollten Sie die Cache-Funktion des ISA Server ebenfalls deaktivieren. Dasselbe gilt auch für Webfilter und Anwendungsfilter, die in Ihrer Konfiguration nicht benötigt werden.

16.8.4 Delegierung der Verwaltung

Gerade in einem größeren Unternehmen kommt der Delegierung von Verwaltungsaufgaben eine entscheidende Rolle zu, da der übergeordnete Administrator nicht sämtliche Konfigurationseinstellungen selbst vornehmen kann. Eine Delegierung der Verwaltung ist nicht nur für die Aufgaben am ISA Server, sondern auch für Verwaltungsaufgaben am Active Directory möglich.

Der ISA Server verfügt über insgesamt drei verschiedene Rollen für die Verwaltungsdelegierung. Dies sind:

Drei Verwaltungsrollen

- *ISA Server Hauptadministrator*: Diese Benutzer dürfen sämtliche Verwaltungsaufgaben am ISA Server durchführen und diesen komplett überwachen.
- *Erweiterte ISA Server-Überwachung*: Diese Benutzer können sowohl den ISA Server überwachen als auch im Rahmen der Überwachung Protokolle konfigurieren und Alarme festlegen.
- *ISA Server-Standardüberwachung*: Diese Benutzer können lediglich den ISA Server passiv überwachen, jedoch nicht aktiv Überwachungsfunktionen hinzufügen.

16.9 Überwachen

In Kapitel 12 wurde bereits umfassend die Überwachungs- und Protokollfunktion des ISA Server 2004 beschrieben. Um so schnell wie möglich über Angriffe informiert zu werden, sollten Sie für möglichst viele Punkte Alarme definieren und diesen die geeigneten Aktionen zur Reaktion zuweisen. Auch eine regelmäßige Überprüfung der Überwachungsseite kann Sie schnell über Probleme mit dem ISA Server aufklären, die nicht alle zwangsläufig aus Angriffen resultieren müssen. Sie erkennen hier auch, wenn z.B. eine Festplatte ausgefallen ist und deshalb keine Zwischenspeicherung mehr erfolgen kann oder wenn es Konnektivitätsprobleme zwischen dem ISA Server und anderen Servern oder Geräten des Netzwerks gibt.

Im Rahmen der Überwachung sollte der Administrator die folgenden Aufgaben durchführen:

Regelmäßige Aufgaben

- Täglich sollten die Protokolldateien des ISA Server auf ungewöhnliche und damit verdächtige Aktivitäten hin untersucht werden.
- Die Meldungen in der Ereignisanzeige sollten ebenfalls mindestens einmal pro Tag durchsucht werden.
- Speichern Sie die Inhalte der Protokolldateien und der Ereignisanzeige. Allerdings sollte immer eine andere physikalische Maschine als Speicherort gewählt werden, da es bei einem Angriff auch zu einer Manipulation dieser Dateien kommen kann.
- Prüfen Sie in regelmäßigen Abständen die Speicherkapazität der Festplatte. Ein Aufräumen der Festplatte kommt immer günstiger als die Anschaffung einer neuen zusätzlichen Festplatte. Bedenken Sie auch, dass der ISA Server nicht als Dateiserver oder Applikationsserver missbraucht werden sollte.

16.10 Absichern des Routers

Verwenden Sie für die Internetverbindung einen Router, der gleichzeitig noch als Firewall und als Wireless Access Point dient, so müssen Sie eine korrekte, sichere Konfiguration dieses Geräts sicherstellen.

16.10.1 Absichern des Wireless Access Point (Basisstation)

WLAN deaktivieren

Verfügt der Router zugleich über das Feature eines Wireless Access Point und werden in Ihrem Unternehmen keine Wireless-Geräte eingesetzt, sollten Sie die Funktionalität des Routers unbedingt abschalten. Ansonsten besteht das Risiko, dass sich fremde Benutzer unautorisiert Zugang zu Ihrem Netzwerk verschaffen können. Genaue Hinweise zum Deaktivieren dieses Features finden Sie in der Dokumentation Ihres Routers. Benutzen Sie hingegen Wireless-Geräte, so müssen Sie den Access Point entsprechend absichern, um den unauthorisierten Zugriff auszuschließen oder zumindest stark zu minimieren.

Passwortschutz für die Konfiguration

Dazu zählt, dass Sie zunächst ein Passwort für die Konfiguration des Routers vergeben. Dabei sollte es sich nicht um das Standard-Passwort handeln, das die Hersteller für ihre Geräte vergeben. Als Nächstes sollten Sie die Verschlüsselung aktivieren. Dazu können Sie entweder die *WEP-Verschlüsselung (Wired Equivalent Privacy)* oder die *802.1x-Authentifizierung* anwenden. Die 802.1x-Authentifizierung ist neuer und sicherer als WEP. Bei beiden Verfahren handelt es sich um ein Sicherheitsprotokoll, bei dem die Daten bei der Übertragung über die Radiowellen von einem Gerät zum anderen verschlüsselt werden. Bei der WEP-Verschlüsselung müssen Sie manuell einen Sicherheitsschlüssel erstellen, der dann zwischen dem Access Point und den Wireless-Geräten ausgetauscht wird. Unter 802.1x wird dieser Sicherheitsschlüssel automatisch generiert. Wenn Sie bei der WEP-Verschlüsselung die Wahl zwischen einem 64 Bit- und einem 128 Bit-Schlüssel haben, sollten Sie immer den längeren Schlüssel benutzen.

MAC-Filterung

Für höhere Sicherheit sollten Sie die *MAC-Filterung (Media Access Control)* aktivieren. Hierzu müssen Sie die MAC-Adressen der im Netzwerk verwendeten Wireless-Karten herausfinden und die Liste der Adressen im Router eintragen. Damit wird sichergestellt, dass nur die Karten mit den aufgelisteten MAC-Adressen Zugriff auf den Access Point haben.

Um die MAC-Adresse einer Netzwerkkarte auszulesen, geben Sie an der Eingabeaufforderung den Befehl `ipconfig /all` ein. Die MAC-Adresse wird unter `Physikalische Adresse` (siehe Abbildung 16.5) angezeigt.

Abbildung 16.5: Das Ermitteln der MAC-Adresse einer Wireless-Netzwerkkarte

Haben Sie die MAC-Filterung aktiviert, müssen Sie die Liste auf dem Router aktualisieren, sobald Sie eine neue Wireless-Karte im Netzwerk hinzufügen oder eine Karte entfernen.

16.10.2 Die Firewallkonfiguration auf dem Router beim Einsatz des SBS 2003

Router und SBS 2003

In diesem Kapitel wird die Konfiguration einer Firewall für den Einsatz mit SBS 2003 beschrieben. Auf dem SBS 2003 werden automatisch sämtliche Ports konfiguriert, nachdem Sie in der Aufgabenliste den Assistenten HERSTELLEN DER INTERNETVERBINDUNG abgeschlossen haben.

Das Öffnen von Ports auf einer Firewall wird in den entsprechenden Dokumentationen auch als Port Forwarding oder Weiterleitung bezeichnet. Im Folgenden finden Sie eine Übersicht über die im SBS 2003-Netzwerk möglicherweise benötigten Ports. Wird ein Port nicht benötigt, so sperren Sie diesen auf der Firewall des Routers.

Sofern Sie nicht die Premium Edition des SBS 2003 erworben haben und somit nicht den ISA Server 2000 als Firewall einsetzen, dürfte in den meisten kleineren Unternehmen ein separates Firewallgerät vorhanden sein. Dieses kann unter bestimmten Umständen auch gemeinsam mit der in den SBS 2003 integrierten Firewall betrieben werden. Oftmals handelt es sich dabei um eine Kombination aus Firewall und DHCP-Server.

UPnP-fähiges Gerät

Ist dieses Gerät UPnP-fähig (Universal Plug&Play), so wird die Konfiguration der verschiedenen vom SBS 2003 benötigten Ports über den Assistenten E-MAIL UND INTERNETVERBINDUNG vorgenommen. Ist das Gerät nicht UPnP-fähig, so müssen Sie die Konfiguration der Firewall manuell durchführen.

Dient die Firewall zusätzlich als Router und ist der SBS über eine Netzwerkkarte mit dem lokalen Netzwerk, über die andere mit dem Internet verbunden, so können Sie sowohl die Firewall des SBS 2003 oder die Firewallfunktionalität des Kombigeräts oder auch beide gemeinsam nutzen.

Tabelle 16.3 zeigt Ihnen eine Übersicht über die vom SBS 2003 für die verschiedenen Dienste genutzten Portnummern. Bei sämtlichen Diensten handelt es sich um TCP-Protokolle.

Tabelle 16.3: Übersicht über die im SBS 2003-Netzwerk erforderlichen Ports

Portnummer	Dienst	Beschreibung
21	FTP (File Transfer Protocol)	Bevor Sie den Server als FTP-Server einrichten, müssen Sie zunächst den FTP-Dienst hinzufügen und einrichten.
25	E-Mail	Maileingang und –ausgang über das SMTP-Protokoll (Simple Mail Transfer Protocol)
80 (http)	Webserver	Internetzugriff, Outlook Web Access (OWA), Outlook Mobile Access (OMA), Aufruf von Leistungs- und Nutzungsberichten des SBS, Firmenwebseite (wwwroot) sowie Outlookzugriff über das Internet (RPC) ohne VPN-Verbindung
443 (https)	Webserver; Remote-Webarbeitsplatz	http-Anfragen über SSL (Secure Sockets Layer); Webarbeitsplatz siehe die betreffende Spalte dieser Tabelle
444	SharePoint Services Intranet-Webseite	Sicherung der Client-Server-Kommunikation beim Zugriff auf die Intranet-Webseite der Firma sowie weitere unter *http://companyweb* bereitgestellte Seiten
1723	VPN (Virtual Private Network)	Aufbau einer sicheren Verbindung von Remote-Clients zum Firmennetzwerk
3389	Terminaldienste	Benutzung der Terminaldienste des SBS 2003 durch Remote-Clients
4125	Remote-Webarbeitsplatz	Verbindung über Outlook Web Access (OWA) zum lokalen Netzwerk, Remotedesktopverbindung zu Clients des lokalen Netzwerks, Zugriff auf die Intranet-Webseite der SharePoint-Services sowie Herunterladen des Verbindungsmanagers für die Konfiguration des Remotezugriffs

Benötigen Sie für bestimmte Applikationen weitere Ports, so müssen Sie diese ebenfalls auf der Firewall freischalten. Eine Übersicht über alle verfügbaren und von bestimmten Applikationen oder Diensten benutzten Ports finden Sie unter *http://www.iana.org/assignments/port-numbers*.

Sofern der Router auch die Funktionalität des Logging unterstützt, sollten Sie dieses ebenfalls aktivieren und die Logdateien auswerten.

A Microsoft-Zertifizierung

Microsoft stellt zur Zertifizierung im Bereich ISA Server 2004 zwei verschiedene Kurse zur Verfügung. Dabei handelt es sich um das Examen 70-350, das sich auf den ISA Server 2004 bezieht, sowie 70-298 zur Sicherheitsimplementierung unter Windows Server 2003. Diese beiden Examen sind zum aktuellen Zeitpunkt erst in englischer, aber noch nicht in deutscher Sprache verfügbar.

A.1 70-350

Examen 70-350, *Implementing Microsoft Intenet Security and Acceleration Server 2004.*

Als Vorbereitung zu diesem Examen kann der MOC-Kurs 2824 belegt werden. Die Durchführung dieses Kurses dauert fünf Tage. Die Kursunterlagen sind momentan nur in englischer Sprache verfügbar. Dieser MOC-Kurs gliedert sich in die folgenden Teile:

- Module 1: Overview of Microsoft ISA Server 2004
- Module 2: Installing and Maintaining ISA Server
- Module 3: Enabling Access to Internet Resources
- Module 4: Configuring ISA Server as a Firewall
- Module 5: Configuring Access to Internal Resources
- Module 6: Integrating ISA Server 2004 and Microsoft Exchange Server
- Module 7: Advanced Application and Web Filtering
- Module 8: Configuring Virtula Private Network Access for Remote Clients and Networks
- Module 9: Implementing Caching
- Module 10: Monitoring ISA Server 2004
- Module 11: Implementing ISA Server 2004 Enterprise Edition
- Module 12: Implementing ISA Server 2004 Enterprise Edition: Back-to-Back-Firewall Scenario
- Module 13: Implementing ISA Server 2004 Enterprise Edition: Site-to-Site VPN Scenario

A.2 70-298

Examen 70-298, *Designing Security for a Microsoft Windows Server 2003 Network*

Vorbereitend auf dieses Examen kann der MOC-Kurs 2830 besucht werden. Weitere Informationen zu diesem MCSE-Examen finden Sie unter dem Link *http://www.microsoft.com/learning/exams/70-298.asp*.

B Adressbereiche

In der Regel wird für das interne Firmennetzwerk ein Satz von IP-Adressen aus dem privaten Bereich verwendet. Im Gegensatz zu einer öffentlichen IP-Adresse kann eine private IP-Adresse nicht direkt von einem externen Netzwerk aus angesprochen werden. Zudem ist keine kostenpflichtige Reservierung wie bei einer öffentlichen IP-Adresse notwendig. Auch für Geräte, die sich in der DMZ befinden, können private IP-Adressen verwendet werden. Je nach eingesetzter Adressklasse können die folgenden Adressbereiche als private IP-Adressen genutzt werden:

- Klasse A: 10.0.0.0 bis 10.255.255.255
- Klasse B: 172.16.0.0. bis 172.16.31.255
- Klasse C: 192.168.0.0 bis 192.168.255.255

Bei allen anderen hier nicht aufgeführten IP-Adressen handelt es sich um öffentliche IP-Adressen, die nicht für das interne Netzwerk benutzt werden sollten.

C Übersicht über die wichtigsten TCP- und UDP-Ports

Im Folgenden finden Sie eine Übersicht über die wichtigsten TCP-Ports und UDP-Ports, die Sie für die Konfiguration der Firewallfunktion des ISA Servers oder auch einer zusätzlichen Firewall benötigen.

Eine komplette Aufstellung aller Ports finden Sie im Internet unter der Adresse *http://www.iana.org/assignments/port-numbers*. Dort sind auch sämtliche Ports verzeichnet, die von Applikationen bestimmter Hersteller reserviert sind.

Die folgende Tabelle zeigt eine Übersicht über die gebräuchlichsten TCP- und UDP-Ports.

Tabelle C.1: Übersicht über die gebräuchlichsten TCP- und UDP-Ports

Port	Name	Protokoll
7	echo	TCP, UDP
9	discard	TCP, UDP
11	systat	TCP, UDP
13	daytime	TCP, UDP
17	qotd	TCP, UDP
19	chargen	TCP, UDP
20	ftp-data	TCP
21	ftp	TCP
23	telnet	TCP
25	smtp	TCP
37	time	TCP, UDP
39	rlp	UDP
42	nameserver	TCP, UDP
43	nicname	TCP
53	domain	TCP, UDP
67	bootps	UDP
68	bootpc	UDP
69	tftp	UDP
70	gopher	TCP
79	finger	TCP
80	http	TCP

Port	Name	Protokoll
88	kerberos	TCP, UDP
101	hostname	TCP
102	iso-tsap	TCP
107	telnet	TCP
109	pop2	TCP
110	pop3	TCP
111	sunrpc	TCP, UDP
113	auth	TCP
117	uucp-path	TCP
119	nntp	TCP
123	ntp	TCP
135	epmap	TCP, UDP
137	netbios-ns	TCP, UDP
138	netbios-dgm	UDP
139	netbios-ssn	TCP
143	imap	TCP
158	pcmail-srv	TCP
161	snmp	UDP
162	snmptrap	UDP
170	print-srv	TCP
179	bgp	TCP
194	irc	TCP
213	ipx	UDP
389	ldap	TCP
443	https	TCP, UDP
445	microsoft-ds	TCP, UDP
464	kpaswd	TCP, UDP
500	isakmp	UDP
512	a. exec, b. biff	a. TCP, b. UDP
513	a. login, b. who	a. TCP, b. UDP
514	a. cmd, b. syslog	a. TCP, b. UDP
515	printer	TCP
517	talk	UDP
518	ntalk	UDP
520	a. efs, b. router	a. TCP, b. UDP

Port	Name	Protokoll
525	timed	UDP
526	tempo	TCP
530	courier	TCP
531	conference	TCP
532	netnews	TCP
533	netwall	UDP
540	uucp	TCP
543	klogin	TCP
544	kshell	TCP
550	new-rwho	UDP
556	remotefs	TCP
560	rmonitor	UDP
561	monitor	UDP
636	ldaps	TCP
666	doom	TCP, UDP
749	kerberos-adm	TCP, UDP
750	kerberos-iv	UDP
1109	kpop	TCP
1167	phone	UDP
1433	ms-sql-s	TCP, UDP
1434	ms-sql-m	TCP, UDP
1512	wins	TCP, UDP
1524	ingreslock	TCP
1701	l2tp	UDP
1723	pptp	TCP
1812	radius	UDP
1813	radacct	UDP
2049	nfsd	UDP
2053	knetd	TCP
9535	man	TCP

D Übersicht über IP-Protokollnummern

Die folgende Tabelle zeigt eine Übersicht über die IP-Protokollnummern und deren Bedeutung:

Tabelle D.1: Übersicht über die gebräuchlichsten IP-Protokollnummern

Nummer	Protokoll	Nummer	Protokoll	Nummer	Protokoll
0	HOPOPT	46	RSVP	95	MICP
1	ICMP	47	GRE	96	SCC-SP
2	IGMP	48	MHRP	97	ETHERIP
3	GGP	49	BNA	98	ENCAP
4	IP	50	ESP	100	GMTP
5	ST	51	AH	101	IFMP
6	TCP	52	I-NLSP	102	PNNI
7	CBT	53	SWIPE	103	PIM
8	EGP	54	NARP	104	ARIS
9	IGP	55	MOBILE	105	SCPS
10	BBN-RCC-MON	56	TLSP	106	QNX
11	NVP-II	57	SKIP	107	A/N
12	PUP	58	IPv6-ICMP	108	IPComp
13	ARGUS	59	IPv6-NoNxt	109	SNP
14	EMCON	60	IPv6-Opts	110	Compaq-Peer
15	XNET	62	CFTP	111	IPX-in-IP
16	CHAOS	64	SAT-EXPAK	112	VRRP
17	UDP	65	KRYPTO-LAN	113	PGM
18	MUX	66	RVD	115	L2TP
19	DCN-MEAS	67	IPPC	116	DDX
20	HMP	69	SAT-MON	117	IATP
21	PRM	70	VISA	118	STP

Nummer	Protokoll	Nummer	Protokoll	Nummer	Protokoll
22	XNS-IDP	71	IPCV	119	SRP
23	TRUNK-1	72	CPNX	120	UTI
24	TRUNK-2	73	CPHB	121	SMP
25	LEAF-1	74	WSN	122	SM
26	LEAF-2	75	PVP	123	PTP
27	RDP	76	BR-SAT-MON	124	ISIS
28	IRTP	77	SUN-ND	125	FIRE
29	ISO-TP4	78	WB-MON	126	CRTP
30	NETBLT	79	WB-EXPAK	127	CRUDP
31	MFE-NSP	80	ISO-IP	128	SSCOPMCE
32	MERIT-INP	81	VMTP	130	SPS
33	SEP	82	SECURE-VMTP	131	PIPE
34	3PC	83	VINES	132	SCTP
35	IDPR	84	TTP	133	FC
36	XTP	85	NSFNET-IGP	255	Reserviert
37	DDP	86	DGP		
38	IDPR-CMTP	87	TCF		
39	TP++	88	EIGRP		
40	IL	89	OSPFIGP		
41	IPv6	90	Sprite-RPC		
42	SDRP	91	LARP		
43	IPv6-Route	92	MTP		
44	IPv6-Frag	93	AX.25		
45	IDRP	94	IPIP		

Stichwortverzeichnis

Z