IT-ADMINISTRATOR.DE

05/2010

€ 12,60 ISSN 1614-2888

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

Remote Access, VPN und Gateway-Schutz

4 196583 212605 05

NetSupport

Fernwartung für jede IT-Umgebung

Die Verwendung von Fernwartungssoftware ist heute allgemein üblich, doch die große Vielfalt an IT-Plattformen mit ihren zahlreichen unterschiedlichen Betriebssystemen, Protokollen, Endgeräten und den vielen sich dadurch ergebenden Kombinationsmöglichkeiten stellt für viele Anbieter immer noch eine enorme Herausforderung dar.

Das Erfolgsrezept von NetSupport Manager liegt in seiner Anpassungsfähigkeit und der permanenten Weiterentwicklung seiner Funktionen. Denn schon seit 1989 unterstützt NetSupport Manager Unternehmen bei der IT-Fernwartung und optimiert ihre IT-Support-Services.

NetSupport Manager gibt Ihnen das gute Gefühl, dass Ihre komplexe IT-Infrastruktur allen Herausforderungen gewachsen ist! Denn NetSupport Manager kombiniert umfassenden Multi-Plattform-Support für Windows-, Linux-, MAC-, Solaris-, CE-, Pocket PC- und Windows Mobile-Systeme mit einer Vielzahl an Verwaltungs- und Steuerungswerkzeugen. Dadurch lässt es sich problemlos in praktisch jede heute übliche Systemumgebung integrieren.

Die komplett neu gestaltete Benutzeroberfläche des NetSupport Manager V11 erleichtert die Fernwartung komplexer Systemumgebungen noch wesentlicher. Die angeschlossenen Rechner lassen sich automatisch nach Betriebssystemen oder Systemfamilien sortieren und selbst die Prozessorausstattung von Laptops oder Desktop-PCs mit Intel® vPro™-Technologie ist problemlos darstellbar.

Selbst komplexe Software- und System-Upgrades oder die Umstellung auf neue Technologien sind jetzt mit wenigen Fingertipps möglich, dank perfekter Windows 7-Integration einschließlich Touchscreen-Unterstützung und zusätzlichen Task Bar-Funktionen!

www.pci-software.de
E-Mail: sales@pci-software.de Tel: +49 (0)89 550 508-10

EDITORIAL

Sicher in die Ferne schweifen

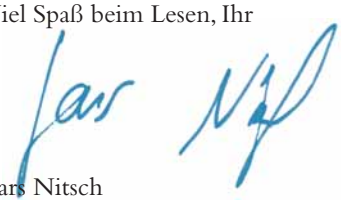
Liebe Leser,

ein guter Freund von mir, ein äußerst fähiger Admin, spricht das Wort "remote" stets so aus wie "remute". Immer wenn ich also aus seinem Mund so etwas wie *remjuut* vernehme, muss mein Gehirn erst einige Schalter umlegen, um zu verstehen, dass der gute Mann von Fernzugriff spricht und nicht etwa davon, seine Systeme zum Verstummen zu bringen. Dieses Verständigungsproblem bringt uns zu einer interessanten Frage: Was ist eigentlich remote? Ist jeder Zugriff, der von einem LAN ins andere geht, automatisch remote? Nicht unbedingt, befindet sich doch etwa ein KVM-Switch meist innerhalb eines Netzwerks, trotzdem wird die Verwendung eines solchen Geräts als Remote-Kontakt bezeichnet. Und was ist eigentlich mit der Administration eines virtuellen Servers irgendwo in den Tiefen eines Racks? Ist das nicht auch irgendwie remote?

Für die Arbeit eines Admins ist es hilfreich, zwei Arten von Fernverbindungen zu unterscheiden: Zum einen den Remote-Zugriff des Administrators, dessen Ziel meist die Systemkonfiguration und -pflege ist. Zum anderen die Anbindung eines externen Anwenders, der genau so arbeiten will wie auch innerhalb des LANs. Während es bei der ersten Art des Fernzugriffs darum geht, funktionsreiche, aber trotzdem schnelle Werkzeuge an der Hand zu haben, stehen bei der zweiten Gattung eher Sicherheitsaspekte im Vordergrund. So verwundert es nicht, dass die meisten Anbieter von VPN-Appliances ihre Geräte mit einem dicken Security-Paket ausstatten.

In unseren Tests ab den Seiten 22 und 26 erfahren Sie, wie sich die UTM-Appliances Cyberoam CR50ia und Clavister SG 4310 hinsichtlich Netzwerkschutz und Bedienbarkeit geschlagen haben. In einem unserer Workshops gehen wir ab Seite 40 darauf ein, wie Sie es sich mit Microsofts neuem SSTP-Protokoll leichter machen, einen VPN-Tunnel einzurichten. Beim Thema remote nicht zu vergessen sind natürlich die in Server 2008 R2 vorgestellten Features Direct Access und Branch Cache. Die Einrichtung von Letzterem erklären wir Ihnen in unserem Workshop ab Seite 35. Immer in dem Sinne, dass bei Ihrem Fernzugriff alles rund läuft – egal wie Sie "remote" aussprechen.

Viel Spaß beim Lesen, Ihr



Lars Nitsch
Redakteur IT-Administrator

P.S.: Wir würden uns sehr freuen, wenn Sie bei unserer großen Leserbefragung mitmachen. Es lohnt sich, gibt es doch viele attraktive Preise zu gewinnen. Mehr dazu gleich auf Seite 6.

LANCOM

. . . connecting your business

Made
in
Germany

Das beste WLAN aller Zeiten!

Die höchsten Datenraten aller Zeiten, die beste Funkfeldabdeckung, maximale Kompatibilität – 802.11n setzt neue Maßstäbe im Wireless LAN. Drinnen wie draußen.

Machen auch Sie Ihr Netz zukunftsfähig – und steigen Sie um auf die 802.11n Indoor & Outdoor Access Points, Clients und „11n-ready" WLAN-Controller von LANCOM.

Ob im kleinen Netz mit wenigen Access Points, im Controller-basierten WLAN mit Tausenden von Geräten, für den Hotspot-Betrieb oder im Freien: 802.11n WLAN von LANCOM sorgt überall für ungekannte Leistungsfähigkeit.

INNOVATIONSPREIS-IT
KATEGORIESIEGER
2009
initiative mittelstand
STORAGE/NETZWERKE

LANCOM OAP-310agn

802.11n WLAN von der dt. Nummer Eins

Kostenlose Lifetime-Updates inklusive

LANCOM
Systems

www.lancom.de

INHALT

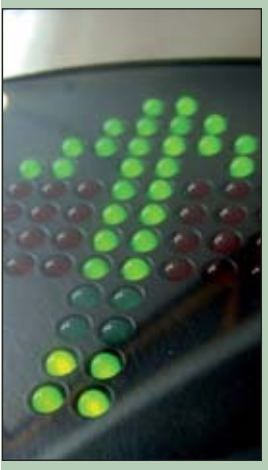
IT-Administrator – Ausgabe Mai 2010

Remote Access, VPN und Gateway-Schutz

Im Test: Clavister SG 4310

Die UTM-Appliance 4310 der SG 4300-Serie von Clavister bündelt die klassischen Sicherheitsfunktionen Intrusion Detection/Prevention, Gateway AntiVirus, Content Filtering und VPN in einer Hardware. Der Firewall-Hersteller mit Hauptsitz in Schweden schmückte sich noch bis vor kurzem mit dem Leitspruch "The platform techies will love". Und er könnte passender nicht sein, denn fast keine andere Firewall ist so administrationsfreundlich bei gleichzeitiger Erfüllung fast aller Sicherheitsanforderungen. Im IT-Administrator-Test zeigte sich anhand der Leistungsfähigkeit der untersuchten Sicherheitsfunktionen, dass sich Clavister keineswegs hinter den Großen verstecken muss.

Seite 26



Sichere Zugänge dank SSL-VPNs

Sollen externe Mitarbeiter effizient in interne Prozesse eingebunden werden, stehen vor allem Unternehmen mit mehreren Standorten vor großen Herausforderungen: Alle Nutzer müssen gleichzeitig auf die jeweils benötigten Anwendungen zugreifen können. Zudem erfordern reibungslose Arbeitsabläufe eine stabile und sichere Verbindung, unabhängig von den verwendeten Endgeräten oder Authentifizierungsverfahren. Hier bieten Web-basierte SSL-VPN-Portale eine unkomplizierte und sichere Alternative für den Netzwerkzugriff.

Seite 60

Themenübersicht

- Server- und Systemmanagement
- Clientmanagement
- Storage
- Sicherheit
- Messaging
- Virtualisierung
- Netzwerkmanagement
- Job/Weiterbildung
- Recht

IT-Administrator Leserumfrage 2010

Sagen Sie uns Ihre Meinung!

Um unser Magazin noch besser auf die Bedürfnisse Ihrer täglichen Arbeit zuzuschneiden, bitten wir Sie diesen Monat um Ihre Unterstützung bei unserer Leserumfrage 2010. Mit der Beantwortung von weniger als 20 Fragen zum IT-Administrator und zu Ihrem beruflichen Umfeld gestalten Sie Ihre monatliche Lieblingslektüre aktiv mit und haben gleichzeitig die Chance auf einen wertvollen Gewinn. Durch die freundliche Unterstützung zahlreicher Sponsoren sind wir in der Lage, unter den Einsendern einen ganzen Korb attraktiver Preise zu verlosen. Zur Teilnahme faxen Sie uns entweder den beiliegenden Fragebogen zu oder füllen unseren Fragebogen im Internet unter www.it-administrator.de/ita2010 aus. Unabhängig davon, ob Sie zu den glücklichen Gewinnern gehören, bedanken wir uns für Ihre Mühe auf jeden Fall mit einem IT-Administrator-Sonderheft. Und nicht lange zögern: Einsendeschluss ist der 28. Mai 2010.

Für Ihre Mühe und Zeit, unseren Fragebogen auszufüllen, belohnen wir Sie auf jeden Fall mit einem Exemplar unseres Sonderhefts "Windows-Systemtuning und -Optimierung". Jeder Einsender des Fragebogens erhält dieses oder ein gleichwertiges Sonderheft im Wert von 35 Euro von uns.

Belohnung für jeden Teilnehmer

Um an der IT-Administrator-Leserumfrage und der Verlosung der Preise teilzunehmen, füllen Sie einfach den beiliegenden Fragebogen aus und faxen ihn an die Rufnummer 089-4445408-99. Oder Sie füllen den Fragebogen aus und senden ihn uns auf dem Postweg zu – das Porto übernehmen wir!

Sollten Sie den Fragebogen nicht in dieser Ausgabe vorgefunden haben, laden Sie ihn sich einfach als PDF [1] herunter, drucken ihn aus und verfahren wie oben beschreiben. Unabhängig davon können Sie den Fragebogen auch online [2] ausfüllen.

Pro Teilnehmer ist selbstverständlich nur die Einsendung eines Fragebogen gestattet und die Verlosung der Gewinne erfolgt ohne Gewähr.

[1] Download des Fragebogens als PDF
www.it-administrator.de/downloads/fragebogen/

[2] Online-Fragebogen
www.it-administrator.de/ITA2010/

So geht's

Der Hauptgewinn:

Gewinnen Sie eine 8MAN-Lizenz für 100 User inklusive Installationsunterstützung und Einweisung im Wert von 3.500 Euro.

8MAN und Berechtigungen bleiben sauber: Mit 8MAN wird Ihr Job zu einem Kinderspiel. Endlich können Sie wie noch nie grafisch durch die Active Directory-User und -Gruppen browsen und Zusammenhänge erkennen. Sie durchleuchten und verstehen Fileserver-Berechtigungen und administrieren diese per Drag & Drop. So sind Sie in der Lage, Fragen zu beantworten, bei denen Sie mit Windows-Bordmitteln keine Chance haben. Mit wenigen Klicks erstellen Sie in Sekunden einen einfachen Bericht über die Berechtigungslage eines Dateiablagebaums, den auch ein Abteilungsleiter versteht und lesen kann. 8MAN ermöglicht es, Fileserver-Rechte oder Gruppenmitgliedschaften mit automatischem Ablauf-Datum zu vergeben. Das ist zum Beispiel bei Azubis, Urlaubsvertretungen und Projektmitarbeitern notwendig und sinnvoll. So sehen Sie der nächsten Revision oder Wirtschaftsprüfung entspannt entgegen, da alles dokumentiert ist und reportet werden kann.

Der **SafeStick** sichert alle gespeicherten Daten durch Passwort und 256-Bit AES-Hardwareverschlüsselung. Zur Nutzung ist keine Software oder Admin-Berechtigung notwendig. SafeStick kann sofort unter Windows und MAC OS genutzt werden. Die optionale SafeConsole ermöglicht die zentrale Konfiguration und unternehmensweite Verwaltung aller SafeSticks.

Die neue **ProSecure UTM Appliance** von **Netgear** garantiert ein Höchstmaß an Sicherheit und Performance zu einem äußerst attraktiven Preis für kleine Unternehmen. Die UTM10 integriert die führende Stream-Scanning-Technologie von Netgear. Mit der Appliance können umfassende Viren- und Malware-Datenbanken eingesetzt werden, ohne auf eine hohe Arbeitsgeschwindigkeit verzichten zu müssen. Ein hohes Maß an Durchsatz bleibt erhalten und die durch das Scanning bedingten Latenzen sind minimiert. Die flexible, modulare Architektur der UTM-Linie überprüft Dateien und Datenverkehr bis zu fünfmal schneller als konventionelle Methoden. So können den immer größeren Sicherheitsrisiken von Web 2.0- und Cloud Computing-Technologien entgegengetreten werden. Die ProSecure UTM-Plattformen können problemlos bestehende Firewalls oder Router ersetzen. Eine intuitive browserbasierte Administration macht Einrichtung und Betrieb äußerst einfach.

Der **Funkwerk bintec R1200** ist ein vielseitig ausgestatteter und flexibel einsetzbarer Multiprotokoll-Router mit automatischem ISDN-Backup. Er wurde speziell für den High Speed Internet-Zugang entwickelt und kann zudem als Remote Access in kleinen bis mittleren Unternehmen oder Remote Offices eingesetzt werden. Das Gerät ist mit einem 4-Port-Switch und einem Ethernet-Port für den WAN-Zugang ausgestattet und verfügt ab Werk bereits über 10 IPSec-Tunnel inklusive Hardwarebeschleunigung. Bis zu 100 zusätzliche IPSec-Tunnel lassen sich per Lizenz freischalten. Die integrierte zweite ISDN S0-Schnittstelle kann ebenfalls optional per Lizenz aktiviert werden. Für den Einsatz als VoIP Media Gateway ist ein 4-Kanal-DSP-Steckplatz vorgesehen. Mit eingesetztem DSP-Modul unterstützt das Media Gateway maximal vier gleichzeitige Hybrid-Rufe.

IT-Dokumentation mit **Docusnap 5.0** vereinfacht für Administratoren die aktuelle Abbildung von IT-Infrastrukturen. Von Docusnap 5.0 automatisiert erstellte Netzwerkpläne, Datenblätter, Übersichtslisten und Berichte unterstützen das IT-Team bei seinen Aufgaben. Zudem sind die visualisierten Werte durch optionale Module wie die Lizenzverwaltung oder die Rechteanalyse eine sichere Basis für anstehende Entscheidungen im IT-Bereich, für Lizenzmanagement, Datenschutz- und Sicherheitsbeauftragte, Controller, Budgetplaner, Revisoren sowie Steuerberater.

Microsoft Flight Simulator X bietet eine beispielhafte Realitätstreue, die von echten Piloten in aller Welt geschätzt wird. Dank der extrem detaillierten 3D-Grafik fühlt sich der Hobbypilot mitten in die perfekt simulierte Welt hinein versetzt. Dutzende Flugzeugmodelle, darunter eine Vielzahl neuer Maschinen, sowie spannende Missionen und innovative Online-Features sorgen für grenzenlose Abwechslung.

PC Tools Spyware Doctor mit AntiVirus bietet vollständige Anti-Virus- und Anti-Spyware-Erkennung und -Entfernung in einer Anwendung und schützt damit vor allen Arten von Bedrohungen wie beispielsweise Spyware, Adware, Viren, Trojaner, Würmer oder Keylogger. Mit Hilfe einer verhaltensbasierten Erkennungstechnologie erkennt, entfernt und blockiert Spyware Doctor mit AntiVirus auch neue Bedrohungen wie Zero-Day-Attacken, die durch herkömmliche Verfahren auf Signatur-Basis nicht sofort erkannt werden.

TeamViewer ist die Allround-Lösung für Fernwartung/Remote-Support, Online-Präsentationen und Teamarbeit. Innerhalb weniger Sekunden wird mit der Software über das Internet eine Verbindung zu einem anderen Rechner aufgebaut. Der Anwender sieht die Benutzeroberfläche des entfernten PCs auf seinem Monitor und kann damit arbeiten, als säße er selbst direkt davor. Der Zugriff funktioniert schnell und unkompliziert auch durch Firewalls hindurch oder bei PCs hinter Routern.

Der Hauptgewinn

Eine 8MAN-Lizenz für 100 User inklusive Installationsunterstützung und Einweisung im Wert von 3.500 Euro.

Weitere Gewinne

- 1x **bintec R1200 VoIP-Gateway** im Wert von 620 Euro
- 1x **Netgear UTM 10** im Wert von 300 Euro
- 10x **Sandberg Wireless Keyboard** im Wert von jeweils 35 Euro
- 1x **SonicWall TZ 100** im Wert von 500 Euro
- 5x **Spyware Doctor 2010** mit AntiVirus im Wert von jeweils 40 Euro
- 10x **Microsoft Flight Simulator X Pro Edition** im Wert von jeweils 30 Euro
- 3x **8 GByte Safesticks** im Wert von jeweils 124 Euro
- 1x **Docusnap 5.0** im Wert von 500 Euro
- 3x **Teamviewer Premiumlizenzen** im Wert von jeweils 835 Euro

Alle Gewinne im Überblick

Das **Sandberg Wireless Keyboard-Set** ist eine schwarze Tastatur in schönem Design, die sich hervorragend auf Ihrem Schreibtisch macht, ohne dass Ihnen Kabel in die Quere kommen. Die Tastatur verfügt über präzise, geräuscharme Tasten, Schnellstarttasten für Ihre Anwendungen und eine leicht zu verwendende Multimedia-Abspielfunktion. Die drahtlose optische Maus bietet präzise Steuerung, schnelles Scrollen und zwei Schnelltasten. Sowohl die Maus als auch die Tastatur verfügen über eine bequeme schwarze Gummioberfläche für mehr Griffigkeit. Die Mausbatterie wird automatisch geladen, wenn sie die Maus in der Ladestation platzieren.

Als Einstiegsgerät bietet das **TZ 100 Wireless TotalSecure** von **SonicWall** ein leistungsstarkes Unified Threat Management zum erschwinglichen Preis. Die umfassende Anti-Spam-Lösung ergänzt dabei die bestehenden Schutzmechanismen um Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention und Content Filtering. Der integrierte SSL VPN-Remote Access ist leistungsfähig und einfach zu nutzen. Selten in seiner Klasse: Den Datenverkehr unterzieht das Gerät einer ständigen Deep Packet Inspection.

Business-PCs für Anspruchsvolle

Acer bietet zwei neue **Business-PCs** an. Der **Veriton M680** besitzt ein Micro-Tower-Gehäuse, während der **Veriton S680** durch seinen platzsparenden Formfaktor unter dem Display positioniert werden kann. Die Modelle sind mit den Intel Core i3-, i5- oder i7-Prozessoren ausgestattet. Für 3D-Anwendungen und die Wiedergabe von High Definition-Inhalten verfügt der Chipsatz Intel Q57 Express über eine integrierte HD-Grafikkarte. Bis zu 16 GByte DDR3-Arbeitsspeicher stellen die PCs dabei zur Verfügung. PCI-Express 2.0 optimiert die Funktion von Komponenten wie High-End Discrete-Grafik- und Netzwerkkarten für die höchste gegenwärtig mögliche Leistung. Ausreichend Speicherplatz und erhebliche Verbesserungen bei den Zugriffs- und Abrufgeschwindigkeiten soll die SATA-Festplatte mit bis zu 1 TByte Speicherplatz bieten. RAID 0, 1, 5 und 10 (nur RAID 0 und 1 beim Veriton S680G) sorgen dabei für Datensicherheit, optimierten Durchsatz sowie höhere Speicherkapazität mit mehreren Festplatten. Eine schraubenlose Gerätekonstruktion ermöglicht schnellen Zugriff auf die internen Komponenten. An Betriebssystemen unterstützen die Geräte Windows 7 Professional, Linpus Linux sowie FreeDOS. Das Modell M680G ist ab 671 Euro zu haben, die Variante S680G kostet 587 Euro. *(dr)*

Acer: www.acer.de

Die neuen Business-PCs von Acer bieten RAID-Sicherheit für die gespeicherten Daten

Applikationsvirtualisierung unterwegs

Citrix Systems bringt die **Applikationsvirtualisierung Citrix XenApp** in **Version 6** auf den Markt. Die neue Version soll die zentrale Verwaltung dank der Managementkonsole "AppCenter" sowie die unternehmensweite Skalierbarkeit verbessern. Zudem ermöglicht XenApp nun die Integration von Microsoft-Technologien wie App-V und Windows Server 2008 R2. Über die Funktion "Citrix Dazzle" können Administratoren ihren Nutzern einen Pool von Anwendungen aus XenApp oder Microsoft App-V, sowie SaaS- oder Web-Anwendungen zur Verfügung stellen. Die User wählen hierfür die angebotenen Applikationen nach Bedarf aus und können diese dann in ihrer Umgebung nutzen. Dabei unterstützt XenApp auch Mac OS-Rechner, Laptops und Smartphones. Durch Verbesserungen der HDX-Technologie können Nutzer zudem in Echtzeit beispielsweise Sprache oder Audio in CD-Qualität übertragen. Außerdem unterstützt XenApp 6 jetzt verschiedene USB-Endgeräte wie Webcams, Mikrofone, Digitalkameras und Scanner. XenApp 6 ist ab sofort erhältlich. Die Preise beginnen bei 350 US-Dollar pro Concurrent User. *(dr)*

Citrix: www.citrix.de/produkte/schnellsuche/xenapp

Firewall für reale und virtuelle Umgebungen

SonicWALL bietet die Network **Security-Appliance** SonicWALL **NSA E8500** an. Die Firewall verfügt über eine erweiterte **Intrusion Prevention** (IPS) und umfassende Kontroll- und Überwachungsmechanismen für Daten und Anwendungen im Netzwerk. Einsetzen lässt sich das Gerät als Security-Gateway oder inline im Datenstrom. Vier GBit-Ethernet-Ports sowie vier SFP Fibre Channel-Ports sorgen für Anschluss ans Netzwerk. Während der Firewall-Durchsatz dabei 8 GBit/s betragen soll, überprüft das IPS laut Hersteller 3,5 GBit/s an Daten. Über verschiedene Kontrollmechanismen kann der IT-Verantwortliche detaillierte Sicherheitspolicies konfigurieren und Richtlinien für User, Anwendungen, Zeitfenster oder IP-Subnetze festlegen. So lässt sich etwa definieren, wie auf Bandbreitenengpässe zu reagieren ist, welche Dateien nicht übermittelt werden dürfen und nach welchen Kriterien angehängte Dateien geprüft werden sollen. Auch Anwenderberechtigungen sowie die Kontrolle des internen wie externen Internetzugriffs können die IT-Verantwortlichen im Detail bestimmen. Benutzerfreundliche Tools für die Visualisierung ermöglichen es zudem, die Anwendungen im Netzwerk an verschiedenen Datenpunkten darzustellen und zu überwachen. Dies umfasst auch Informationen zu den jeweiligen Anwendern und dem möglichen Einfluss auf die Sicherheit. Eine "Terminal Services Authentication" und Citrix-Unterstützung erlaubt den Einsatz der Appliance in virtuellen Umgebungen. Im zweiten Quartal 2010 soll die Firewall für rund 31.000 US-Dollar erhältlich sein. *(dr)*

SonicWALL:
www.sonicwall.com/us/products/NSA_E8500.html

Die SonicWALL NSA E8500 schützt virtualisierte Systeme

NETGEAR ProSecure UTM:
WEB- UND E-MAIL-SICHERHEIT FÜR KMUs

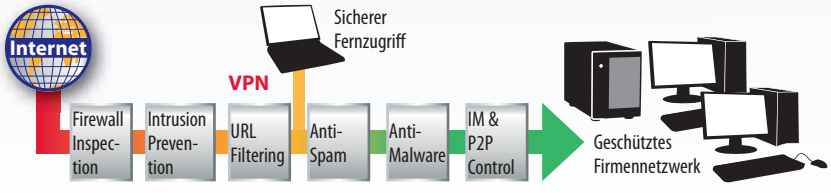
NETGEAR ProSecure UTM5/UTM10/UTM25:

Router, Application, Proxy Firewall, VPN, IPsec & SSL VPN für bis zu 30 User

Die neuen ProSecure Unified Threat Management Appliances garantieren als All-in-one-Lösung ein Höchstmaß an Sicherheit und Performance für Web- und Mailanwendungen in kleinen und mittleren Unternehmen zu einem äußerst attrraktiven Preis.

Sie können umfassende Viren- und Malware-Datenbanken von NETGEAR und Sophos bei hoher Performance einsetzen. Die flexible, modulare Architektur der UTM-Linie überprüft Dateien und Datenverkehr bis zu fünf mal schneller als konventionelle Methoden.

- Mail-, Web-, FTP- und Netzwerksicherheit bei hoher Performance.
- Real Time Protection durch stündliche Updates
- Einfaches Management und unkomplizierte Konfiguration
- Keine nutzerabhängigen Lizenzgebühren
- Über 1.000.000 Antivirus Signaturen
- ICSA Labs certified



Mehr Infos unter:
www.prosecure.netgear.de

PROSECURE™
SECURITY ARCHITECTURE BY NETGEAR

ALL-IN-ONE SECURITY. REALTIME.

NETGEAR Green

PROSUPPORT™

Das NETGEAR Serviceportfolio. Sichern Sie Ihr Netzwerk mit OnCall 24x7 oder mit dem XPressHW Hardwareaustausch.

NETGEAR® SMB SOLUTIONS

Alle NETGEAR® ProSecure-Produkte sind auf Basis von Enterprise-Technologien nach strengsten Qualtitätsmaßstäben hergestellt, um höchste Performance und Funktionssicherheit für kleine und mittlere Firmennetzwerke zu bieten – kostengünstig und bedarfsgerecht erweiterbar.

NETGEAR®

BUILT FOR BUSINESS

+++TICKER+++TICKER+++TICKER+++

Trend Micro hat sein **gehostetes E-Mailsecurity-Angebot** überarbeitet und verspricht Kunden nun 100 Prozent Verfügbarkeit sowie 99 Prozent Spamblockade. Ansonsten will der Anbieter mit "hohen Geldzahlungen" als Vertragsstrafe geradestehen. Zudem garantiert Trend Micro nun, nicht mehr als drei von einer Million E-Mails fälschlicherweise als Spam zu klassifizieren. Auch sollen Nutzer weltweit künftig nicht mehr als eine Minute auf ihre E-Mailzustellung warten müssen. Der Preis für die Hosted Email Security beginnt bei 45,14 Euro pro Anwender, für das Hosted Email Security Inbound Filtering liegen die Kosten bei 29,80 Euro pro Anwender (jeweils ab 5 User). *(dr)*
http://de.trendmicro.com/de/solutions/hosted-security/

Mit dem **EZ Connect N** bietet **SMC** einen WLAN Access Point/Repeater mit Ethernet-Client-Modus an. Hierdurch kann der Access Point mehrere Ethernet-fähige Geräte miteinander verbinden. Der EZ Connect N arbeitet in den WLAN-Modi 802.11b/g/n und unterstützt über mehrere Antennen das MIMO-Verfahren (Multiple In, Multiple Out). Daneben verfügt das Gerät über einen Vier-Port 10/100 LAN-Switch und mehrere SSIDs, die es dem Anwender ermöglichen, einzelne drahtlose Netzwerke mit unterschiedlichen Einstellungen und Sicherheitsstufen zu konfigurieren. Für rund 58 Euro ist der Access Point ab sofort auf dem Markt. *(dr)*
www.smc.de

Mit dem **CompactHiL II** bietet **COSATEQ** ein weiteres Komplettsystem für Hardware-in-the-Loop (HiL)-Anwendungen an. Mit dem Gerät lassen sich Embedded-Systeme wie Steuergeräte testen und absichern oder Maschinen und Anlagen vorzeitig in Betrieb nehmen. Auch eignet es sich zum Erfassen und Visualisieren von Messdaten. Der CompactHiL beinhaltet die ME-Neuron XL mit sechs Steckplätzen für CompactPCI, eine PCI-Karte mit 32 AI-, vier AO-, 16 DIO- und vier PWM OUT- und IN-Kanälen bis 8 MHz. Die concert-Version von **SCALE-RT**, der Linux-basierten Echtzeitsimulationssoftware, ist bereits installiert. Ein komfortabler BNC-Anschlussblock ermöglicht den schnellen Wechsel von Testaufbauten. Ab 7.490 Euro ist das Gerät einschließlich einer Schulung verfügbar. *(dr)*
www.cosateq.com

Die webbasierte Helpdesk-Software **ServiceDesk Plus** von **ManageEngine** unterstützt mit Version 7.6 den Zugriff über mobile Endgeräte wie das iPhone, Blackberry oder mobile Windows-Webbrowser. Darüber hinaus ist ServiceDesk Plus jetzt auch in der Lage, die Apple-Betriebssysteme Mac OS Leopard und Snow Leopard zu überwachen. Somit können alle Arten von Workstations und deren Applikationen gescannt werden, egal ob diese Windows, Linux oder Apple basiert sind. Ab rund 440 Euro ist die Software erhältlich. *(dr)*
www.manageengine.de/produkte/helpdesk/itservicedesk/uebersicht.html

Neue Server für KMUs

transtec stellt die **CALLEO 340-Serverreihe** mit neuem **Intel Xeon 5600-Prozessor**, bekannt unter dem Codenamen "Westmere", vor. Die Prozessoren werden als Quad- oder als Six-Core-Version angeboten. Die Server kommen im **Rack- sowie Tower-Format** daher und sind für übliche Geschäftsanwendungen sowie für rechenintensivere Einsätze konzipiert, etwa Multimedia- oder Datenbank-Anwendungen. Zudem eignen sich die neuen Server zur Virtualisierung oder als Teil eines High-Performance-Clusters. Je nach Einsatzgebiet lassen sich die Rechner mit SATA-, SAS II- oder SSD-Festplatten ausstatten. Die maximale Speichergröße beträgt dabei 72 TByte. Die CALLEO 340-Modelle sind standardmäßig mit einem "Intelligent Plattform Management Interface" (IPMI 2.0) ausgerüstet. Damit verwaltet, steuert und repariert der Administrator alle funktions- und leistungsrelevanten Elemente zentral über das Netzwerk. Nur bei Hardware-Ausfällen ist die Vor-Ort-Präsenz eines Admins notwendig. Ein für den Fernzugriff dedizierter LAN-Port und umfassende Sicherheitsstandards stellen sicher, dass nur autorisierte Personen Zugriff haben. Die Einstiegsversion des CALLEO 342-Servers ist für rund 1.800 Euro erhältlich. *(dr)*

transtec: www.transtec.de/D/D/products/servers/CALLEO300/calleo_340_Intel.html

Die neuen CALLEO 340-Server von transtec sind als Rack- und Tower-Variante erhältlich

Steuerzentrale für VMware-Umgebungen

NetIQ erweitert seine **Management-Software NetIQ Aegis** auf **VMware-Umgebungen**. Durch Erweiterung der IT-Prozessautomatisierung und integrierte, virtuell-physische Management- und Steuerungsfunktion unterstützt NetIQ Aegis Unternehmen dabei, die nötige Konsistenz zwischen virtuellen und physischen Managementprozessen herzustellen. Mit der Software können nun auch VMware-Administratoren Workflows auf der Grundlage vorhandener Verfahren entwerfen, die Ausführung technischer Richtlinien und Sicherheitseinstellungen standardisieren und das Snapshot-Management automatisieren. Die vorkonfigurierte Integration in Ticketing-Systeme, wie BMC Remedy, Configuration Management Databases (CMDBs) und andere Enterprise-Management-Tools, ermöglicht IT-Verantwortlichen dabei eine bessere Steuerung der virtuellen Umgebungen, ein konsistentes virtuell-physisches Management und eine Reduzierung der Speicherkosten, sodass mehr Ressourcen für die eigentlichen Kernaufgaben zur Verfügung stehen. NetIQ Aegis und der NetIQ Aegis-Adapter für VMware vCenter Server sind ab sofort verfügbar. Die Preise beginnen bei 21.125 Euro. *(dr)*

NetIQ: www.netiq.de

Schweizer WLAN-Taschenmesser

Fluke bringt das WLAN-Analysegerät **OptiView Network Analyzer** in **Version 5.4** auf den Markt. Eine neue Wireless-Option bietet IT-Mitarbeitern bei der Installation und **Wartung von WLANs** nun Transparenz auf beiden Seiten des Access Points. Durch diese kombinierte Analysefähigkeit ist laut Hersteller nur noch ein Tool für den gesamten Lebenszyklus der Wireless-Implementierung erforderlich. Dank des 802.11a/b/g/n-Toolsets können Administratoren dabei Probleme entdecken, diagnostizieren, beheben und melden. Gleichzeitig soll sich so die Sicherung des Netzwerks gewährleisten lassen, da Sicherheitsbedrohungen und auch andere Schwachstellen automatisch erkannt würden. Mit Version 5.4 können Administratoren nun auch 10-GBit-Schnittstellen über eine SNMP-basierte Infrastrukturanalyse überwachen und den Datenfluss von kritischen Verbindungen einfacher analysieren. Die Netzwerkerkennungsfunktion des Analyzers wurde dabei laut Hersteller verbessert, um schnellere und tiefere Einblicke in WLANs zu ermöglichen. Außerdem enthält die VoIP-Analyse eine neue Funktion, die es ermöglicht, beim Testen der Anrufqualität gleichzeitig VoIP-Anrufe vom Analyzer aus zu tätigen. Für 19.995 Euro ist das Gerät erhältlich. *(dr)*

Fluke Networks: www.flukenetworks.com/optiview/

Der OptiView Network Analyzer von Fluke ermöglicht nun Voice over WLAN-Analysen

Datenträgerverwaltung auf Servern

Mit **Version 3** lässt sich der **PartitionManager** von **O&O Software** nun auch auf **Windows-Servern** einsetzen. Das Tool dient der **Datenträgerverwaltung** und umfasst hierfür mehrere Software-Pakete von O&O wie Defrag, SafeErase oder FileExplorer. Mit Version 3 können übergreifende, mirrored oder auch RAID-5-Volumes eingerichtet und verwaltet werden. Die Software zeigt zudem die Eigenschaften von physikalischen Datenträgern an, beispielsweise auch, ob diese fehlerhaft sind. Die zusätzlich ausgelesenen S.M.A.R.T.-Werte liefern dabei **Informationen zu den Fehlern einer Festplatte**. Durch die Umwandlung von primären in logische Partitionen kann daneben eine zuvor getroffene Zuordnung aufgehoben werden. Dies bietet sich an, wenn etwa auf einem Basisdatenträger zusätzlicher Speicherplatz für eine Systempartition benötigt wird oder eine Partition verschoben werden soll, aber keine freie aufzulösende primäre Partition oder logisches Laufwerk vorhanden ist. Neben MBR-Datenträgern werden nun auch dynamische Datenträger sowie Wechseldatenträger, USB-Sticks und Speicherkarten erkannt und unterstützt. Dies ermöglicht es, verschiedene Datenträgertypen anzulegen und untereinander zu konvertieren. Start- oder Wiederherstellungspartitionen sind Benutzern dabei normalerweise nicht zugänglich. Mit dem PartitionManager 3 können diese nun im "O&O FileExplorer"-Fenster geöffnet und durchsucht werden. Ab 99 Euro ist die Software erhältlich. *(dr)*

O&O Software: www.oo-software.com

Bietet sich nun auch für den Server-Einsatz an: O&O PartitionManager 3

Monitoring mit Failover

Ipswitch bietet **Version 14.2** der Überwachungs- und Management-Software **WhatsUp Gold** an. Zu den neuen Leistungsmerkmalen zählen automatisches Failover sowie die Möglichkeit, Linux- und Unix-Systeme zu überwachen. Die wesentliche Neuerung in Version 14.2 ist dabei laut Hersteller der **WhatsUp Gold Failover Manager**. Er ermöglicht einen automatischen bidirektionalen Failover des produktiven Systems auf ein Standby-System, wenn das primäre System ausfällt. Steht das primäre System wieder zur Verfügung, kann es ebenfalls automatisch wieder die Verantwortung für die Überwachung des Netzwerks übernehmen (Failback). Bei geplanten Ausfallzeiten, etwa bei der Systemwartung, können Failover und Failback auch manuell vorgenommen werden. Bei der Überwachung und dem Management von Unix/Linux-Systemen stehen zudem neue aktive Performance-Monitore sowie ein neuer Aktionstyp zur Verfügung. Das integrierte SSH-Monitoring ermöglicht die Überwachung beliebiger Geräte, die SSH unterstützen, und damit ein umfassendes Monitoring von Unix- und Linux-Systemen. Das Plug-in "FlowMonitor" unterstützt daneben nun auch das IPFIX-Protokoll sowie NetFlow in Cisco ASA-Firewalls, auch als "NetFlow Security Event Logging" (NSEL) bezeichnet. Weitere Verbesserungen will der Hersteller bei der Usability und der Performance vorgenommen haben; so könne Flow Monitor nun doppelt so viele Flows pro Minute verarbeiten wie bisher. Ab 1.166 Euro ist die Software zu haben. *(dr)*

Ipswitch: www.whatsupgold.com

IT-Administrator-Workshop "Exchange Disaster Recovery" am 10. Juni 2010 in München

ITANet Workshop-Partner:

Katastrophenschutz

von John Pardey

Steht der Exchange-Server still, geht im Unternehmen nichts mehr: Bestellungen bei Lieferanten, Kundenaufträge und auch Rechnungen werden heutzutage per E-Mail abgewickelt. Daher ist im Problemfall eine möglichst kurze Ausfallzeit des Mailservers geschäftskritisch. Die Verantwortlichen in der IT sind daher gefordert, Konzepte und Absicherungen der Infrastruktur zu entwickeln und Know-how zur schnellen Wiederherstellung der Systemumgebung aufzubauen. In unserem Juni-Workshop zeigen wir für den Exchange-Server mögliche Disaster Recovery-Konzepte bei Teil- oder Totalausfall.

Unser Workshop im Juni wendet sich den wichtigsten Exchange-Vorsorgemaßnahmen zu, um so rasch wie möglich wieder einen produktiven Betrieb herstellen zu können. Zunächst zeigen Ihnen unsere Dozenten sinnvolle Vorsorgemaßnahmen auf, die entweder die Wahrscheinlichkeit eines Exchange-Ausfalls oder im Fall der Fälle die Wideranlaufzeiten reduzieren. Denn wie so oft im Leben gilt auch für Exchange: Vorsorge ist besser als Nachsorge. So betrachten wir in diesem Themengebiet etwa die physische Umgebung des Servers. Dazu zählt neben den Kabeln auch die Klimaanlage im Serverraum. Ein weiteres Problem ist der mögliche Ausfall eines zentralen Switch: Diese Komponente kann unter Umständen sehr kritisch sein, insbesondere wenn der Ausfall am Freitagabend passiert und bis Montag niemand den Ausfall bemerkt.

Natürlich muss der IT-Verantwortliche auch die Hardware des Servers selber im Auge behalten. Was es hier zu beachten gilt, vermittelt der Workshop ebenso wie Gedanken zu Hochverfügbarkeitslösungen für Exchange.

Um nach einem Ausfall möglichst rasch wieder in den Produktivbetrieb zu gehen, sollten Sie wissen, welche Komponenten für den Betrieb wiederhergestellt werden müssen und wo Exchange welche Daten ablegt. Und natürlich muss sichergestellt sein, dass auch die zuvor erfolgte Datensicherung erfolgreich war. Ein Teil der Exchange-Daten wird allerdings nicht direkt auf dem Exchange-Server selbst abgelegt.

Das Active Directory nicht vergessen

So sind im Active Directory viele Einstellungen, wie beispielsweise die Datenbanken, hinterlegt. Und in der Domänenpartition werden direkt am Benutzerobjekt die Beschränkungen der Mailboxgröße oder auch die E-Mailadressen gesichert. Sie müssen daher für eine umfassende Disastervorsorge nicht nur eine Sicherung der Exchange-Mailboxdatenbanken und der Datenbanken für die Öffentlichen Ordner vornehmen, sondern auch das Active Directory sollte regelmäßigen Datensicherungen unterzogen werden.

Schließlich rundet das Thema, wie korrupte Exchange-Datenbanken zu reparieren sind, den Workshopnachmittag ab. Darüber hinaus stellen wir Ihnen noch nützliche Bordmittel und Zusatztools vor. So sind die Teilnehmer gut gerüstet, einen Exchange-Notfallplan zu entwickeln, den bestehenden zu aktualisieren oder einfach mal wieder den Ernstfall zu üben. Wir würden uns auf jeden Fall freuen, Sie in München begrüßen zu dürfen.

iTANet
Die System und Netzwerk User Group

Die Agenda des Workshops

13.00 Uhr: Begrüßung

13.15 Uhr: Exchange Disaster Recovery

- Präventive Maßnahmen der Infrastruktur
- Backup und Recovery von Exchange
- Datenbankfehler beheben
- Sinnvolle Bordmittel und Zusatztools

Dozenten: Henry Schleichardt und Jürgen Haßlauer, Senior Consultants, infoWAN, Unterschleißheim

17.30 Uhr: Ende des Workshops

Ort: Global Knowledge Germany Training GmbH
Kistlerhofstraße 75
81379 München

Teilnahmegebühren:
Für IT-Administrator Abonnenten kostenlos.

Anmeldung bis zum 28. Mai unter
www.it-administrator.de/workshops/

Workshop "Exchange Disaster Recovery" am 10. Juni

1&1 SERVER

DYNAMIC CLOUD SERVER

FLEXIBLE SERVER-KONFIGURATION WANN IMMER SIE WOLLEN!

1&1 DYNAMIC CLOUD SERVER BASIS-PAKET:

- 1 Core: Quad-Core AMD Opteron™ Prozessor 2352 (auf 4 Cores erweiterbar)
- 1 GB RAM (auf 15 GB erweiterbar)
- 100 GB Festplatte (auf 800 GB erweiterbar)

~~39,99~~

0,– €/Monat*

Für 3 Monate, danach 39,99 €/Monat*

AMD Opteron 64

1&1

MEMBER OF united internet

Jetzt informieren und bestellen:[1]

0180 5 / 001 535

0800 / 100 668

www.1und1.info

* z. B. 1&1 DynamicCloud Server Basis-Paket jetzt zum Aktionspreis 3 Monate für 0,– €/Monat, danach für 39,99 €/Monat. Einrichtungsgebühr 39,– € bei 12 Monaten Mindestvertragslaufzeit. Preise inkl. MwSt.

[1] DE: 14 ct/Min. dt. Festnetz, Mobilfunk höchstens 42 ct/Min. AT: Anrufe aus dem österr. Festnetz und Mobilfunknetz kostenfrei.

IT Admin Tech Talk 2010, 27.-28. September 2010, Stadthalle Oberursel bei Frankfurt/Main

Terminblocker

von John Pardey

Am 27. und 28. September veranstaltet IT-Administrator in Kooperation mit der IIR Deutschland GmbH den "IT Admin Tech Talk 2010". An diesen zwei Tagen bietet die neue Veranstaltung eine Kombination aus technischen Vorträgen, Workshops und offenen Diskussionsrunden. So werden herstellerneutral wichtige Themen wie Virtualisierung, Sicherheit und Servermanagement erörtert. Darüber hinaus stellt die Konferenz die Person des Admins in den Mittelpunkt und wendet sich Rechts- und Karrierefragen zu. Abonnenten des IT-Administrator profitieren dabei von einem Sonderpreis.

Bis Ende September geht zwar noch einige Zeit ins Land und zum Zeitpunkt der Drucklegung unserer Mai-Ausgabe stand nur ein vorläufiges Programm [1] für den IT Admin Tech Talk 2010 fest, aber es spricht einiges dafür, sich den Termin schon einmal im Kalender zu blockieren. Denn zu den spannenden Inhalten, auf die wir im Folgenden noch kurz eingehen, werden sich zahlreiche namhafte Sprecher gesellen.

Technik erleben und erfragen

Die zwei Tage in Oberursel bei Frankfurt/M. stehen inhaltlich natürlich voll im Zeichen tiefgehender technischer Sessions. In fast 40 Vorträgen, Mini-Workshops und Diskussionsrunden erhalten die Teilnehmer praxisnahes Wissen zu Virtualisierung, Windows Server-Technologien, IT-Sicherheit, Storage und mehr.

Die Details der Agenda verrät Ihnen ein Blick in das Programm – hier die Fülle der Themen darzustellen würde den Rahmen sprengen. Es sei jedoch angemerkt, dass die Veranstaltung in allen Sessions Wert auf einen hohen Praxisbezug legt. Zudem liegt besonderes Augenmerk auf der Diskussion von Problemen mit und unter den Teilnehmern und den Experten.

Darüber hinaus wenden sich die Sprecher auch Themen zu, die jeder Admin abseits vom Tagesgeschäft im Auge behalten sollte. So etwa die Entwicklung der Chiptechnologie, die ja insbesondere für die Virtualisierung von großer Bedeutung ist. Wir werfen aber auch einen Blick auf die Zukunft der Betriebssysteme und die damit verbundene Frage, was die Cloud leisten kann und wird. Denn Investitionssicherheit ist für Administratoren schon lange kein Fremdwort mehr

.

Der Administrator im Fokus

Und obwohl technisches Know-how natürlich die zentrale Qualifikation des Administrators ist, muss er sich – in zunehmenden Maße – auch anderen Anforderungen stellen. So eröffnet die Konferenz denn auch mit einem Ausblick auf den "Admin 2020", dem Versuch, ein sich wandelndes Berufsbild zu skizzieren. Diese Keynote verdeutlicht den Fokus der Veranstaltung auf eine ganzheitliche Sicht des Administrators.

Darüber hinaus haben die Teilnehmer in einem Expertengespräch die Gelegenheit, sich über aktuelle Rechtsfragen zu informieren, die im Berufsalltag relevant sind. Sei es nun das Thema E-Mail, Archivierung oder der Umgang mit personenbezogenen Daten – der Admin arbeitet an einer sensiblen Schnittstelle im Unternehmen und steht nicht selten bei Verstößen persönlich in der Haftung. Erfreulichere Szenarien zeigt hingegen der Beitrag zum aktuellen Stand in Sachen "Zertifizierungen" auf. Hier beleuchten die Experten, welche Zertifizierungen am Arbeitsmarkt besonders gefragt sind und geben damit wertvolle Tipps zur Karriereplanung.

Preisvorteil für Abonnenten

Als Kooperationspartner des Tech Talk 2010 bietet IT-Administrator seinen Lesern besonders günstige Konditionen für die Teilnahme an der Veranstaltung an. Bei einer Anmeldung über unsere Website [2] bis zum 20. Juli sichern Sie sich neben dem Leser-Rabatt auch noch die Vergünstigung für Frühbucher. Blockieren Sie sich also schon jetzt diesen Termin.

[1] Vorläufiges Programm
www.iir.de/ad/

[2] Anmeldung zum Vorzugspreis für IT-Administrator-Abonnenten
www.it-administrator.de/fachkongresse/

Links zum IT Admin Tech Talk 2010

1&1 SERVER

HEXA-CORE TECHNOLOGIE

NEU: 12 PROZESSORKERNE FÜR MAXIMALE SERVER-LEISTUNG!

1&1 DEDICATED HEXA-CORE SERVER XXL:

- 2x Six-Core AMD Opteron™ Prozessoren 2423HE
- 16 GB Arbeitsspeicher
- Bis zu 2 TB nutzbarer Speicherplatz mit RAID 5
- Stromsparend: High Efficency

0,– €/Monat* ~~299,99 €/Monat~~

Für 3 Monate, danach 299,99 €/Monat*

1&1

MEMBER OF united internet

Jetzt informieren und bestellen:[1]

0180 5 / 001 535

0800 / 100 668

www.1und1.info

* z. B. 1&1 Hexa-Core XXL jetzt 3 Monate für 0 €/Monat, danach für 299,99 €/Monat. Einrichtungsgebühr 99,– € bei 12 Monaten Mindestvertragslaufzeit. Preise inkl. MwSt.

[1] DE: 14 ct/Min. dt. Festnetz, Mobilfunk höchstens 42 ct/Min. AT: Anrufe aus dem österr. Festnetz und Mobilfunknetz kostenfrei.

Im Test: HOB RD VPN 1.3

Flexibles SSL-VPN

von Jürgen Heyer

Für SSL-VPNs kommen häufig Gateways in Form von Hardware-Appliances zum Einsatz. Diese sind allerdings funktional meist recht statisch. Flexibler präsentiert sich die Software-Lösung "RD VPN" von HOB. Mit ihr verspricht der Hersteller eine vielseitige Betriebssystem- sowie Plattformunterstützung und ein breites Einsatzspektrum. IT-Administrator hat die Software in verschiedenen Szenarien getestet – und kam dabei nicht ganz um den Hersteller-Support herum.

Die Remote Access-Lösung RD VPN 1.3 ist ein zentrales Produkt von HOB, dem die langjährige Entwicklung und Erfahrung, die in die einzelnen Module geflossen ist, sofort anzumerken ist. So lassen sich neben den üblichen Funktionen wie Zugriffe auf Dateien und die Bereitstellung von Applikationen über Terminalserver auch eher ausgefallene Anforderungen abbilden, wie etwa Fernzugriffe auf Großrechnerterminals oder das Durchreichen von Datenverkehr auf individuellen Ports. HOB RD VPN gehört dabei zur Sparte der SSL-VPN-Lösungen, bei denen im Gegensatz zu IPSec-VPN auf der Anwenderseite kein spezieller Client nötig ist. Die zentrale Komponente von RD VPN ist der so genannte "WebSecure-Proxy" (WSP), der als Gateway die Clientanfragen aus dem Internet annimmt und seinerseits die Verbindung zu den Zielsystemen im Firmennetz herstellt.

Prinzipiell gehört das System, auf dem der WSP installiert wird, in eine DMZ mit entsprechendem Firewallschutz zum Internet und zum Firmennetz. Sehr positiv fällt hier auf, dass der WSP nicht nur für Windows verfügbar ist, sondern auch für Linux, Sun Solaris, HP-UX, AIX und Open-Unix, und das wiederum in Verbindung mit jeweils passender Hardware, also mit x86- und EM64T-Unterstützung sowie für Itanium, Sparc und PA-Risc. Außerdem ist RD VPN in Kombination mit dem HOB Secure Communication Server (SCS) erhältlich. Der SCS ist ein von HOB verschlanktes und gehärtetes Unix, das speziell auf den Einsatz als Plattform für den WSP zugeschnitten ist. SCS hat einen geringen Ressourcenbedarf und weist vom Betriebssystem her keine zusätzlichen offenen Ports auf. Letztendlich kann sich der Administrator für die für seine schon bestehende Umgebung am besten geeignete Plattform entscheiden und auch wählen, ob er den WSP von RD VPN zusätzlich auf einem schon bestehenden Server mit installiert oder alleinstehend womöglich mit SCS betreibt.

Einfache Grundinstallation

Für unseren Test installierten wir RD VPN 1.3 auf einem Windows Server 2008. Neben RD VPN, das auch die Komponente "HOB Enterprise Access" enthält (hierzu später mehr), gibt es die etwas schlankere Lösung "RD VPN Compact" ohne Enterprise Access (EA). HOB EA ist eine übergeordnete Benutzeradministration und speichert die Konfiguration wahlweise in einer integrierten Datenbank oder kommuniziert mit einem LDAP-Server für eine Koppelung beispielsweise mit einem Active Directory. So kann der Administrator bei der großen Lösung für jeden Benutzer individuelle Einstellungen vornehmen, während bei der auf 100 Benutzer (Named User) begrenzten Compact-Version die benutzerspezifische Konfiguration wegfällt. Dann wird der WSP zentral für alle Benutzer gleich eingerichtet.

Das Setup ist 157 MByte groß und stellt keine besonderen Voraussetzungen an den darunter liegenden Server. Im Rahmen der Installation wird ein Webserver eingerichtet, und der Administrator kann gleich einen Terminalserver für eine spätere Verbindung angeben. Außerdem möchte das Setup wissen, ob nur ein reiner RDP-Client benötigt wird, oder ob auch die Terminal-Emulations-Protokolle 3270, 5250, VT, HP700, Siemens 97801 und Siemens 9750 eingerichtet werden sollen. Zuletzt kann der Administrator noch entscheiden, ob der WSP nur lokal oder auch remote konfigurierbar sein soll. Die lokale Variante ist dabei die sicherste, setzt aber voraus, dass der Administrator einen Konsolenzugriff auf den VPN-Server, also den WSP, hat. Andernfalls kann er den Server von jedem System innerhalb des Netzwerks konfigurieren. Für den Test beschränkten wir uns auf den RDP-Client und wählten die Variante für eine Remote-Konfiguration. Nach dem Abschluss der Installation ist darauf zu achten, dass der SSL-Port 443 auf den be-

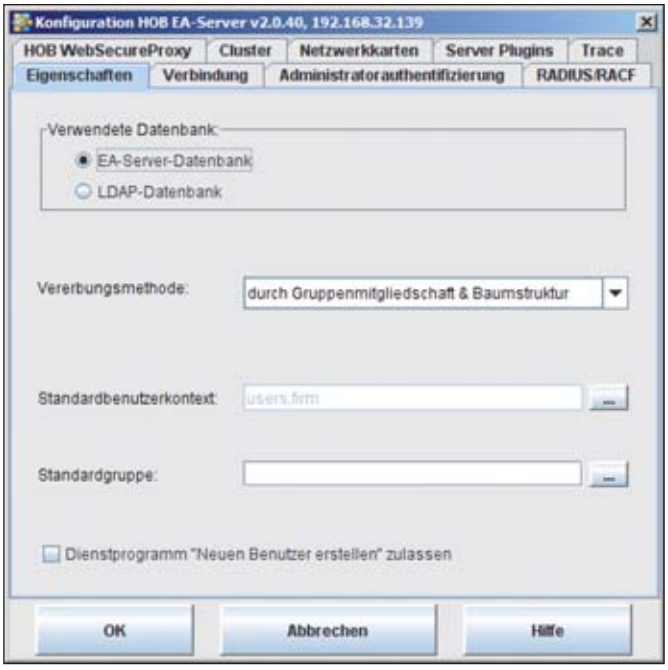


Bild 1: RD VPN lässt sich wahlweise mit einer eigenen Benutzerdatenbank oder einer LDAP-Anbindung, beispielsweise Active Directory, betreiben

teiligten Firewalls freigeschaltet ist. Falls gewünscht, lässt sich der Kommunikationsport beliebig ändern und beispielsweise einer der Highports verwenden. Bezüglich der Sicherheit ist noch anzumerken, dass der installierte Webserver, der auch IPv6 unterstützt, eine Eigenentwicklung von HOB ist. Dies hat den Vorteil, dass er hinsichtlich möglicher Sicherheitslücken nicht im Fokus der Hacker steht wie beispielsweise ein IIS oder Apache Webserver. Ähnliches gilt für die Verschlüsselung, denn hier verwendet HOB zwar anerkannte Verfahren wie AES, programmiert aber alle Routinen selbst.

Um nun im Test über den WSP Dienste für Anwender bereitstellen zu können, stellten wir ein Firmennetz nach, in dem wir noch zusätzliche Windows 2003 Server einrichteten. Sie dienten als Terminalserver sowie als Webserver für das Intranet und zur Bereitstellung von Freigaben für einen Dateizugriff. Für die Authentifizierung nutzt die VPN-Lösung RADIUS+ in Verbindung mit User-ID und Passwort, Zertifikaten, Smartcards oder Tokens wie RSA SecurID, Safeword PremierAccess und Vasco Digipass.

Eine Konsole für mehrere Module

Da in HOB RD VPN mehrere Module kombiniert sind, die teilweise eigenständig programmiert und auch getrennt vermarktet wurden, erlaubt EA unter anderem die Konfiguration des WSP, der Benutzereinstellungen und der verschiedenen Session-Arten, wobei die Rechte auf verschiedene Objekte innerhalb der Organisation vergeben werden können. Leider verfolgen die Module etwas unterschiedliche Bedienkonzepte und es ist auch nicht immer ganz klar, wo genau welche Funktion zu finden ist. Wer anfangs ohne ausreichende Planung loslegt, wird anschließend seine Mühe haben, alles nachzuvollziehen. Hier wäre eine Vereinheitlichung wünschenswert.

Letztendlich lassen sich die üblichen Standardfunktionen durchweg recht einfach konfigurieren, sobald aber jemand tiefer in Spezialfunktionen einsteigen muss, erscheint uns eine umfassende Einarbeitung unumgänglich. Vor allem muss hinsichtlich der Rechtevergabe alles korrekt konfiguriert werden, da es sich hier um das Eingangstor aus dem Internet in ein Firmennetz und somit um ein sicherheitskritisches Produkt handelt.

Zugriff mittels Browser und Java

Wie eingangs erwähnt, ist beim Einsatz von RD VPN auf der Clientseite nichts zu installieren oder zu konfigurieren. Benötigt wird nur ein beliebiger Browser. Damit sind auf dem Client auch keine Administrator-Rechte für eine Einrichtung erforderlich. Sofern bei der Konfiguration des WSP der SSL-Standard-Port beibehalten wurde, ist im Browser nur die IP-Adresse oder der DNS-Name als sichere HTTPS-Verbindung anzugeben. Daraufhin wird ein Java-Applet heruntergeladen und anschließend erscheint die RD VPN-Anmeldemaske.

Nach erfolgreicher Anmeldung öffnet sich im Browser ein individuelles Auswahlmenü mit den frei geschalteten Funktionen. Bei einer Anmeldung als Administrator erscheinen, sofern die Remote-Administration gewählt wurde, auch entsprechende Einträge für den Zugriff auf die HOB EA-Administration. Dort erfolgen letztendlich alle benutzerspezifischen Einstellungen inklusive der Konfiguration des WSP.

Konfiguration nach Maß

Wurde bei der Installation ein Terminalserver angegeben, so sollte nach deren Abschluss bereits ein erster Zugriff auf dessen Desktop möglich sein, wozu in der Datenbank neben dem Administrator noch ein Gast-Benutzer angelegt wurde. Für einen produktiven Einsatz sind in der EA-Administration allerdings noch weitere Einstellungen erforderlich. Zuerst ist es wichtig, die Standardpasswörter zu ändern. Hierbei ist zu beachten, dass es sowohl in der lokalen Benutzerdatenbank von HOB EA einen Administrator gibt, als auch einen Administrator für die Konfiguration des EA-Servers selbst. Beide Administratoren haben anfangs das gleiche Passwort. Wird nun eines ohne Verständnis der Zuordnung geändert, kann es später zu Verwirrungen kommen, wenn die Anmeldung nicht mehr klappt.

Zusätzlich muss der Administrator festlegen, ob er die Benutzer in der mitgelieferten Datenbank verwalten möchte oder RD VPN per LDAP beispielsweise mit dem Active Directory verknüpft. Wählt er die EA-Datenbank, so ist für einen erhöhten Ausfallschutz ein Clustering durch den Betrieb von zwei EA-Servern sinnvoll. Eine automatische Synchronisation der beiden Datenbanken ist allerdings nicht vorgesehen. Vielmehr muss der Administrator den

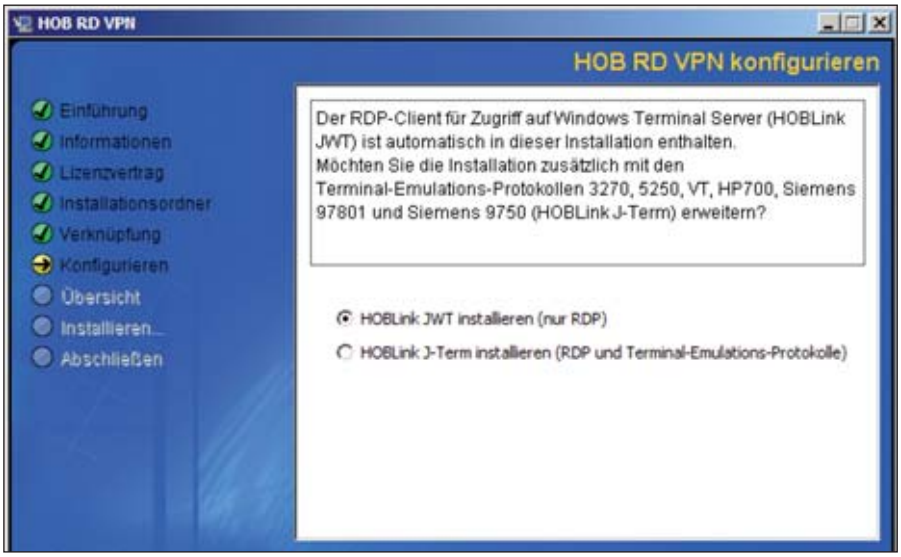


Bild 2: RD VPN unterstützt wahlweise nur RDP-Zugriffe oder auch die Nutzung spezieller Terminal-Emulations-Protokolle

Inhalt eines Ordners auf beiden Systemen abgleichen oder dieses anderweitig automatisieren. Ein Benutzerimport aus einer Datei oder aus LDAP ist auch möglich.

Nach den Grundeinstellungen sind nun für einzelne Benutzer oder auch Benutzergruppen die benötigten Zugriffe einzurichten. Idealerweise konfiguriert der Administrator den Zugang so, dass sich ein Benutzer am Client durch möglichst wenige Fenster hindurchklicken muss. Soll also ein Anwender beispielsweise Zugriff auf verschiedene Applikationen von Terminalservern haben, so sollte bei diesem nach der Anmeldung an RD VPN sofort die Session-Seite erscheinen. Benötigt ein Anwender aber nur den Zugriff auf eine bestimmte Applikation, so kann der Administrator diese automatisch starten lassen. Meldet sich nun ein Benutzer an RD VPN an, öffnet sich sofort das Fenster mit seiner zugewiesenen Applikation. Im Folgenden haben wir nun einige typische Zugriffe konfiguriert, um die verschiedenen Möglichkeiten aufzuzeigen.

Typische Szenarien in der Praxis

Die wohl häufigste Aufgabe von RD VPN dürfte das WTS-Computing auf Basis des Windows Terminalservers sein – neuerdings auch RDS-Computing (Remote Desktop Services) genannt. Bereits vorkonfiguriert ist dabei der Zugriff auf den Desktop eines bei der Installation angegebenen Terminalservers. Wir hinterlegten im Test noch entsprechende Anmeldeinformationen, so dass sich das Fenster beim Anklicken der Session sofort öffnete. Anschließend richteten wir die Bereitstellung einiger dedizierter Applikationen ein. Hierzu ist in der Session der Aufruf der gewünschten Applikation anzugeben. Über eine Suchfunktion ließ sich der Pfad komfortabel festlegen. Für jede Sitzung konnten wird individuelle Einstellungen hinsichtlich Anmeldung, Bildschirmanzeige, Tastatur, Audio- und Twain-Geräte sowie Smartcards, Drucker, lokalen Laufwerkszuordnungen und Port-Umleitungen definieren.

Dateizugriffe über den Browser

Für einen reinen Dateizugriff dient die Funktion "Web File Access", mit der der Anwender Dateien über den Browser hoch- und herunterladen kann. Hierzu sind Namen oder die IP-Adressen der Server, die sichtbar sein sollen, in eine Liste einzutragen. Sie erscheinen dann remote ebenso aufgelistet und der Anwender kann sich durch die Freigaben klicken und einzelne Dateien für den Up- und Download markieren. Auch lassen sich neue Verzeichnisse für einen Upload anlegen. Zu beachten ist, dass Up- und Download nur mit einzelnen Dateien möglich ist, nicht mit ganzen Verzeichnissen. Letztendlich ist der Web File Access nicht für den Austausch großer Datenmengen konzipiert, sondern für den Zugriff auf einzelne Dateien zur Bearbeitung, Präsentation oder ähnliches. Unterstützt werden Windows- und Samba-Freigaben.

Ob auf einem Server der Zugriff auf Freigaben und Dateien möglich ist, richtet sich danach, ob die Anmeldung mit den im Dateisystem hinterlegten Benutzerrechten übereinstimmt. Der Administrator kann diesbezüglich festlegen, ob die RD VPN-Anmeldedaten verwendet werden sollen, was bei einer LDAP-Anbindung an ein Active Directory wohl das Beste sein dürfte. Alternativ fragt der Client Anmeldedaten ab oder der Administrator hinterlegt Benutzer und Passwort, was aber den Nachteil hat, dass bei der Nutzung des Profils durch mehrere Anwender alle die gleichen Anmeldedaten verwenden.

Mit dem Feature "Web Server Gate" kann der Administrator den Remote-Zugriff auf firmeninterne Webserver, also das Intranet, ermöglichen. Zur Nutzung muss nur die Funktion "Web Server Gate" aktiv sein. Auf den Webseiten enthaltene Links werden beim Zugriff automatisch umgemappt, so dass sich der Anwender transparent bewegen kann. Ein Target-Filter gibt dem Administrator zusätzlich die Möglichkeit, die Zugriffe auf bestimmte Bereiche zu beschränken.

Tunnel ins Firmen-Netz

Der so genannte PPP-Tunnel von RD VPN ersetzt den klassischen IPSec-Client. Dieser ist momentan mit Clients unter Vista und Windows 7 nutzbar, geplant ist noch die Unterstützung von Linux/Unix und Mac

Systemvoraussetzungen

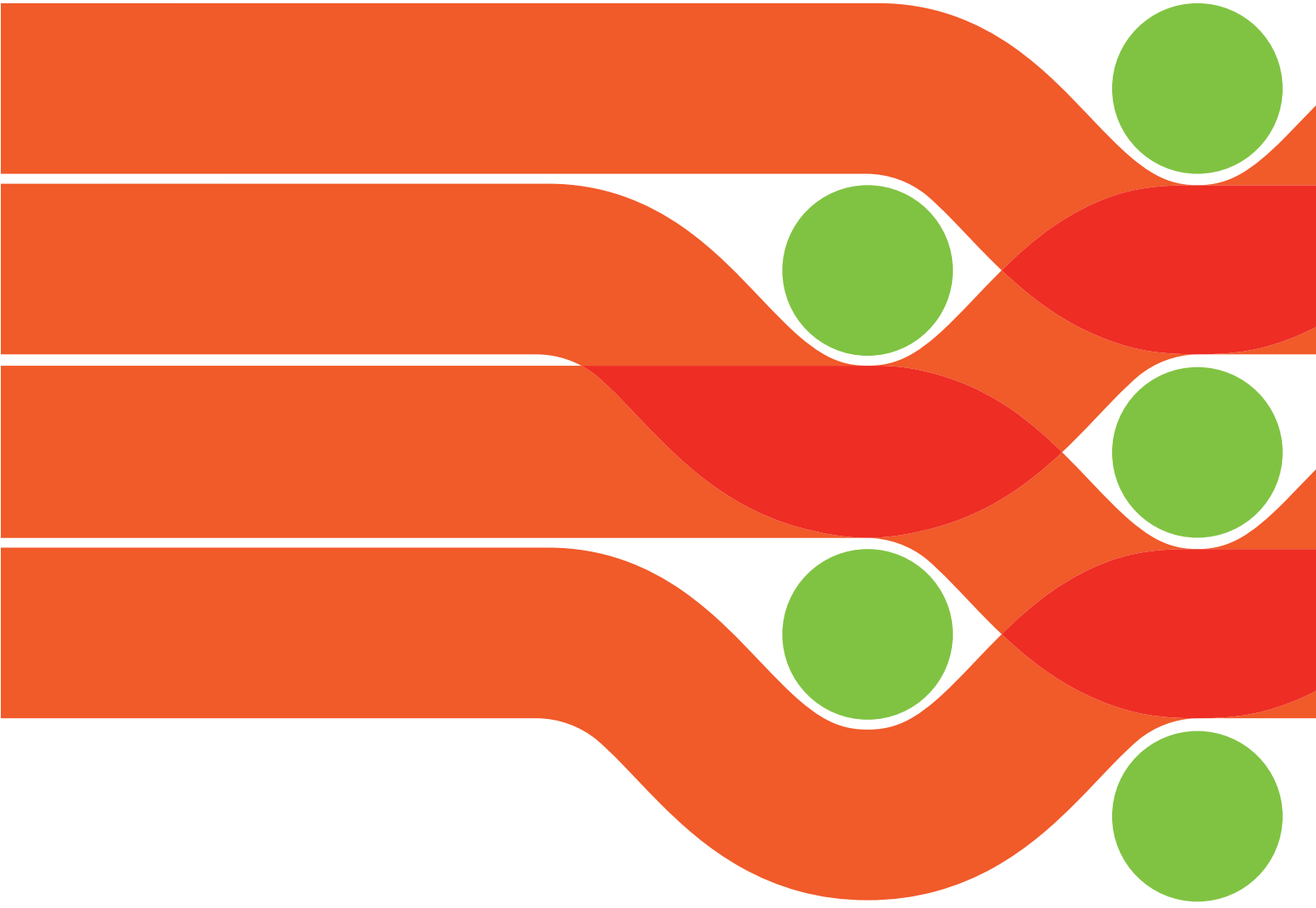
WebSecureProxy ist verfügbar für Windows (x86, EM64T, Itanium), Sun Solaris (Sparc, x86, EM64T), IBM AIX, HP-UX (PA-Risc, Itanium), Linux (x86, EM64T, Itanium), auf Clientseite reicht ein beliebiger Browser mit Java-Unterstützung (1.4.2 oder höher)

Intelligente Technologien für einen smarten Planeten

Wie man Flexibilität ins Unternehmen einbaut.

Bis heute wenden Unternehmen Milliarden auf, um automatische Systeme zu entwickeln, die vertikale Prozesse im Unternehmen steuern – wie ERP, CRM, SCM. Das Manko dabei: Diese Systeme waren nie dafür geschaffen, um miteinander zu kommunizieren. Kein Wunder also, wenn jeder Mitarbeiter durchschnittlich über 5 Stunden pro Woche vergeudet, weil er mit ineffizienten Insellösungen arbeiten muss. Die umfassenden Business Process Management-Lösungen von IBM dagegen verbinden all diese isolierten Prozesse und ermöglichen so reibungslose Abläufe. Schon über 5.000 Unternehmen hat IBM geholfen, die nötigen Einblicke in alle Bereiche zu erlangen und Prozesse zu automatisieren – um schneller auf eine wechselnde Nachfrage zu reagieren und intelligenter zu arbeiten: von einem Logistik-Unternehmen, das seine Entwicklungskosten um 30 % senkte, bis hin zu einem Energie-Unternehmen, das seine Ölfelder in Echtzeit überwacht und so seine durchschnittliche Ausbeute verdoppelt.

Smarte Unternehmen brauchen intelligente Software, Systeme und Services.
Also: Machen wir den Planeten ein bisschen smarter. Wie, erfahren Sie unter ibm.com/bpm/de



O&M IBM IT 4/10

OS X. Für die Realisierung des PPP-Tunnels ist im Firmennetz zusätzlich ein L2TP-Gateway einzurichten. RDVPN baut dann einen SSL-verschlüsselten PPP-Tunnel zwischen dem Client und dem L2TP-Gateway auf. Anschließend ist der Anwender transparent mit dem Firmennetz verbunden.

Für eine individuelle Konfiguration für spezielle Applikationen steht dem Administrator der "Universal Client" zur Verfügung. Er dient zum Durchschalten einzelner Ports etwa für SAP oder einen Datenbankzugriff. Bei einer Client-Server-Applikation ist dann das Frontend auf der Anwenderseite installiert, das über einen bestimmten Port auf die Applikation oder Datenbank auf einem Server remote zugreift. Dass hier nur der benötigte Kommunikationsport über SSL verschlüsselt durchgereicht werden muss, ist unter Sicherheitsaspekten sehr vorteilhaft.

Drucken ohne Treiber auf dem Server

Für die oft lästige und vor allem beim Einsatz vieler unterschiedlicher Drucker nicht immer reibungslose Druckerverwaltung in Verbindung mit Terminalservern besitzt RDVPN die Funktion "Easy Print". Hierbei wird der zum Drucker gehörige Druckertreiber nur auf dem Client installiert, während auf dem Terminalserver selbst lediglich ein Standardtreiber ausgewählt wird. Dies soll vermeiden, dass der Terminalserver durch zu viele Treiber instabil wird. Der Standardtreiber sendet Druckaufträge im HP PCL-Format an den Client, der den Datenstrom dann aufnimmt und an den tatsächlichen Druckertreiber weiterleitet. Für den Schwarz-Weiß-Druck handelt es sich um einen HP LaserJet Series II-Treiber, für den Farbdruck um einen HP DeskJet 500 C-Treiber. Übliche Druckaufträge lassen sich damit problemlos erledigen, spezielle Schachtansteuerungen und ähnliches sind allerdings nicht möglich.

Sollte bei RDVPN einmal die Verbindung abbrechen, sorgen der Client und der WSP dafür, dass die aktiven Sitzungen nicht sofort geschlossen werden. Vielmehr wird der Anwender wieder mit der alten Sitzung verbunden und kann weiterarbeiten. So sind die Chancen gut, dass der Anwender seinen Arbeitsfortschritt nicht verliert. Auch in einer Umgebung mit Load Balancing prüft der WSP bei einer Clientanmeldung zuerst, ob für diesen noch eine offene Sitzung vorhanden ist und verbindet diese wieder. Dies hat natürlich Vorrang gegenüber einer gleichmäßigen Lastverteilung.

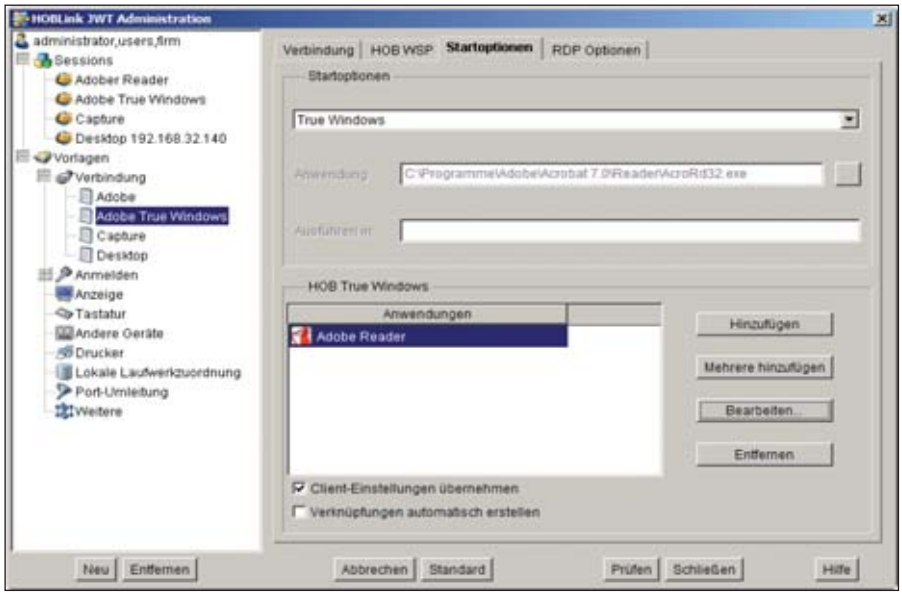


Bild 3: Die Freigabe einer Applikation im True Windows-Modus erfordert mehrere Konfigurationsschritte und ist vergleichsweise komplex

Mehr Komfort durch zusätzliche Optionen

Mit den "Enhanced Terminal Services" bietet HOB einen Zusatz an, der bei intensiver Terminalserver-Nutzung die Funktionalität in den Punkten "True Windows", "Erweitertes Load Balancing" (ELB) und "Erweitertes Local Drive Mapping" verbessert: Wenn Anwender ständig eine oder gar mehrere über Terminalsitzungen bereitgestellte Applikationen nutzen, ist es meist störend, dass jede Applikation in einem eigenen RDP-Fenster läuft. Die True Windows-Funktion löst dies, indem die Remote-Applikation in den lokalen Desktop integriert wird. Dies beinhaltet auch ein Session-Sharing, indem dann mehrere Anwendungen eines Servers in einer Sitzung laufen.

Für die Nutzung von True Windows ist auf jedem beteiligten Terminalserver eine Erweiterung zu installieren, mit der eine zusätzliche Konsole, die ETS Management-Konsole, eingerichtet wird. Im Vergleich zur normalen Applikationsveröffentlichung ist True Windows deutlich komplizierter zu konfigurieren. So ist für True Windows ein Load Balancing Voraussetzung, wozu in der neuen Konsole eine Farm zu definieren ist. Dann muss dort für jede zu veröffentlichende Applikation ein Objekt angelegt werden. Weiterhin ist in der der EA-Administration untergeordneten JWT-Administration eine Session einzurichten, die mit dem besagten Objekt verknüpft wird. Im Test klappte dies nicht auf Anhieb und erforderte eine zusätzliche Unterstützung durch den Support. Hier zeigte sich, dass es bei komplexeren Konfigurationswünschen durchaus sinnvoll ist, sich der Hilfe von HOB oder eines kompetenten Partners zu bedienen. Bei der eigenen Suche nach einer Problemlösung fiel übrigens auch auf, dass im Handbuch zwar grundsätzlich alles beschrieben ist, aber häufig die Zusammenhänge fehlen. Sinnvoll wären entweder mehr Assistenten oder mehr schrittweise Beschreibungen der erforderlichen Arbeitsabläufe für die Realisierung typischer Funktionen.

Das ELB hilft dem Administrator, die Terminalserver optimal zu nutzen, indem die

Last innerhalb einer Farm gleichmäßig verteilt wird. Dazu misst ein Agent auf jedem Server wichtige Kenndaten wie CPU- und Netzwerkauslastung, Swap-Aktivität, die Speichernutzung sowie die Anzahl der Aktivitäten, berechnet daraus einen Lastwert und entscheidet anhand dessen, welchem Server neue Sitzungen zugewiesen werden. Über das erweiterte Local Drive Mapping ist es möglich, dass die Anwendungen des Terminalservers auf die Laufwerke des Clients zugreifen können. Hierbei lässt sich der Zugriff gezielt steuern, indem auf vorgegebene Pfade oder auch Dateitypen beispielsweise nur Leserechte oder aber Vollzugriff vergeben werden. Auch kann der Administrator über einen hexadezimalen Mustervergleich die Ausführung bestimmter Dateien sperren, beispielsweise Spiele, die lokal installiert sind.

Obwohl für die meisten Aufgaben der beschriebene Zugriff auf eine Terminalsitzung ausreichen dürfte, bietet RD VPN noch zwei weitere Zugriffsoptionen an. Desktop-on-Demand ermöglicht einem Anwender den Zugriff auf seinen Arbeitsplatz-PC. Das hat den Vorteil, dass der Anwender auch aus der Ferne oder von daheim mit seinem gewohnten Arbeitsplatzrechner arbeiten kann. Voraussetzung ist, dass er dort Windows XP, Vista oder Windows 7 einsetzt. Die zweite Variante ist die Unterstützung von VMware VDI. Hier bekommt ein Anwender auf Anforderung einen kompletten PC aus einer VDI-Farm zugewiesen, was vor allen beim Einsatz von sehr leistungshungrigen Applikationen, die eine Terminalsitzung überfordern, sinnvoll ist. Hier ist es Aufgabe von RD VPN, das nächste freie System zu finden und bereitzustellen.

Fazit

HOB RD VPN erwies sich im Test als überaus flexibel einsetzbarer SSL-VPN-Client, der auch für die Nutzung mit vielen gleichzeitigen Verbindungen geeignet ist. Hervorzuheben sind die Einsatzbandbreite für verschiedene Aufgaben sowie die umfassende Betriebssystemunterstützung. Hinsichtlich der Funktionalität dürften kaum Wünsche offen bleiben, was eine besondere Stärke im Vergleich zu üblichen SSL-VPN-Gateways als Hardware-Appliance darstellt. Aus der Funktionsvielfalt ergibt sich aber auch, dass sich die Grundfunktionen zwar noch recht einfach konfigurieren lassen, dass aber gerade in Verbindung mit erweiterten Optionen eine umfassende Einarbeitung erforderlich ist. Wir können hier nur empfehlen, die Inbetriebnahme mit einem HOB-Partner zusammen durchzuführen und sich dann sukzessive einzuarbeiten. *(dr)*

Produkt
Remote Access-Lösung per SSL-VPN.

Hersteller
www.hob.de

Preis
RD VPN kostet bis 49 Named User jeweils 250 Euro pro Lizenz, darüber hinaus gibt es Staffelpreise. Die beschriebenen Optionen werden extra berechnet.

Technische Daten
www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator *(max. 10 Punkte)*

Installation	9
Bedienung	7
VPN-Funktionalität	9
Betriebssystemunterstützung	9
Dokumentation	6

Dieses Produkt eignet sich

optimal für die Realisierung komplexer SSL-VPN-Zugänge, bei denen der umfassende Funktionsumfang des Produkts erforderlich ist.

bedingt für die Realisierung einfacher SSL-VPN-Zugänge mit Standardfunktionalität. Hier lohnt sich eine Abschätzung, ob nicht weniger flexible Lösungen preiswerter zum Ziel führen.

nicht, falls zwingend IPSec für einen Remote-Zugang gefordert ist.

HOB RD VPN 1.3

Im Test: Cyberoam CR50ia

Netzwerkverkehr unter Argusaugen

von Sandro Lucifora

Der beste Schutz vor externen Bedrohungen wäre es, das eigene Netzwerk nicht mit dem Internet zu verbinden – im heutigen Geschäftsumfeld eine undenkbare Variante. Andere Lösungen für den sicheren Aufenthalt im World Wide Web sind deshalb Pflicht. Cyberoam bietet mit dem Modell "CR50ia" eine UTM-Appliance an, die das Firmennetzwerk nicht nur gegen Gefahren aus dem Internet schützen soll, sondern auch das Einrichten von VPN-Tunneln und das Filtern des Datenverkehrs erlaubt. IT-Administrator hat für Sie ausführlich getestet, ob das Gerät all diese Funktionen zufriedenstellend erfüllen kann.

Um die Anforderungen verschiedener Netzwerke zu bedienen, hat Cyberoam seine UTM-Serie in verschiedene Leistungsmodelle gefasst. Die Dimensionierung für die eigene Absicherung ist dabei nicht nur von den im Netzwerk betriebenen Arbeitsplätzen abhängig, sondern muss vor allem den Anforderungen an den Datendurchsatz sowie den laufenden Datenverkehr gerecht werden. Unser Testgerät Cyberoam CR50ia siedelt sich im ersten Drittel der Leistungsklasse an und eignet sich als Torwächter von mittelgroßen Netzwerken.

Großzügige Ausstattung

Als Appliance zum Unified Threat Management (UTM) dient die CR50ia vorrangig als Inhalts-Filter im Datenaustausch und regelt durch die Firewall und den gesicherten VPN-Zugang den Zugriff von außen ins LAN. Zusätzlich will die Lösung die Auslastung der WAN-Verbindungen verbessern. Auf Basis von Fedora Linux, versehen mit einer Intel Celeron 1,6 GHz-CPU, 512 MByte Speicher und einer 80 GByte Festplatte, ist das Gerät für seine Aufgaben gut ausgestattet.

Auf den ersten Blick bietet die Appliance eine ganze Menge Funktionen. Dass das Gerät Routing und Firewall beherrscht, stellt keine Überraschung dar. Einen Mehrwert zu anderen Lösungen finden wir im Benutzer-basierten UTM: Dies bedeutet, dass der Administrator IP- und User-basiert Regeln aufstellen kann, die den Zugriff auf das Internet steuern. Vor der Internet-Nutzung muss sich jeder Anwender mit Benutzernamen und Kennwort autorisieren. Dabei ist es irrelevant, an welchem Computer und unter welchem Betriebssystem der User gerade arbeitet. Da ein Firmennetzwerk im Regelfall über ein zentrales Benutzermanagement verfügt und sich Mitarbeiter stets am PC anmelden müssen, kann diese Anmeldung auch mit dem Single Sign-On (SSO) gekoppelt werden. Dazu liefert der Hersteller eine entsprechende Software mit.

Ein weiteres Plus zu üblichen Firewalls und Routern zeigt sich im Content-Filter. Damit Nutzer auch wirklich nur auf die erlaubten Inhalte zugreifen, führt die CR50ia eine ständige Kontrolle des Datenverkehrs durch. So wird jeglicher Netzwerkverkehr entsprechend den eingestellten Firmen- oder Nutzerregeln geprüft und darauf reagiert. Außerdem rundet der Hersteller seine Appliance mit Load-Balancing- und Fail-Over-Gateway-Funktionen ab.

Inbetriebnahme mit leichten Hürden

Bis zur erfolgreichen Inbetriebnahme des Geräts war zu Beginn unseres Tests eine kleine Hürde zu überwinden: Da die Appliance über ein Webinterface administriert wird, galt es zunächst, dieses überhaupt aufzurufen. Leider holt sich das Gerät in der Grundkonfiguration seine IP-Adresse nicht über einen DHCP-Server, sondern lässt sich nur über eine statisch verankerte Zugriffsnummer aufrufen. Arbeitet das eigene Netzwerk nun in einem anderen IP-Bereich, bleibt nur die Möglichkeit, entweder mit einem Cross-Connect-Kabel und einem Standalone-Rechner oder dem mitgelieferten Konsolen-Kabel auf die Appliance zuzugreifen. Der zweite Weg setzt einen Computer mit serieller Schnittstelle vo-

raus und führte uns mit einem beliebigen SSH-Client schließlich auf die Konsole der CR50ia. Dort konnten wir dann die IP-Adresse ändern, um aus unserem regulären LAN heraus die Konfigurationsarbeiten aufzunehmen.

Bei der ersten Einrichtung hilft ein gut strukturierter Assistent. Im Test haben wir die Appliance im "Gateway Mode" eingerichtet. Das heißt, LAN und WAN sind über zwei separate Netzwerkports physisch getrennt. Dazu verbanden wir unser LAN mit Port A und den Router für das WAN mit Port B. An Port C schlossen wir einen separaten Server an, den wir in der DMZ einrichteten. Je nachdem, zu welchem Zweck die CR50ia genutzt wird, sollte auch die Policy gewählt werden. Wir entschieden uns für die General Internet Policy, die den Datenverkehr auf schädliche Informationen scannt und den HTTP-Traffic auf Viren prüft.

Als Alternativen existieren noch die Optionen "Monitor Only" – dabei wird der Datenverkehr unverändert durchgelassen – und "Strict Internet Policy", womit der Internetzugriff nur noch nach einer Autorisierung möglich ist. Nach einem Neustart greifen die eingestellten Schutzfunktionen. Nachdem wir die notwendigen Lizenzen für die Viren- und Spam-Signaturen aktiviert hatten, mussten wir uns der Firewall und dem Einrichten des Port Forwarding widmen. Wenn zum Beispiel der Exchange-Server im LAN und nicht der DMZ steht, lässt sich nur so weiterhin über Outlook Web Access auf die Daten zugreifen.

Dazu haben wir die Firewall-Regeln "WAN->LAN" erweitert. Im LAN benötigten wir daher zuerst einen virtuellen Host, den wir mit der Ziel-IP und den Ports definierten. Wichtig dabei ist, als externe IP-Adresse diejenige des Netzwerk-Anschlusses B der Appliance anzugeben und nicht die öffentliche IP-Adresse des Routers. Denn die Daten kommen ja über die Schnittstelle B. Im zweiten Schritt konfigurierten wir die Firewall so, dass über den WAN-Port und jede Client-IP (möglich wäre hier auch das Einschränken externer IP-Adressen) ins LAN an den zuvor eingetragenen virtuellen Host mit dem definierten Port zugegriffen werden darf. Diese Regel lässt sich noch zeitlich begrenzen und mit diversen Policies belegen.

Umfangreiche Inhaltsfilter

Wie bereits erwähnt bietet die CR50ia umfangreiche Möglichkeiten zum Content Filtering auf IP-, User- und Applikations-Ebene. Damit erlaubt der Hersteller eine Policy-basierte Blockade des Datenverkehrs. Die Regeln haben wir für verschiedene Benutzer und Gruppen erstellt. Die Definitionen trafen wir wahlweise IP- oder User-basiert. Darüber hinaus haben wir beim Content-Filter und dem Zugriff auf Internetseiten eine globale Regel erstellt, die unter anderem den Zugriff auf Spiele- und Pornoseiten blockiert.

Um den Inhaltsfilter zu überprüfen, installierten wir das Gerät für mehrere Wochen in einem realen Netzwerk. Hierbei konnten wir gute Leistung feststellen. Das System handelte nach den Richtlinien und war in der Lage, Benutzern den Zugriff auf bestimmte Websites zu blockieren. Zudem meldete es auf Wunsch Benutzer ab, wenn das zugeteilte Traffic- oder Zeit-Kontingent überschritten wurde. Neben Quota-Regelungen beim Surfen ließ sich über die Internet-Richtlinien einfach regeln, welche Benutzer überhaupt Zugriff auf die Websites oder Anwendungen haben.

Eine weitere Regel, die wir später nicht global, sondern userbasiert zuordneten, verhindert den Zugriff auf webbasierte E-Mail-Angebote und die klassischen Chat-Server. Die User-Level-Authentifizierung kann über die lokale Be-

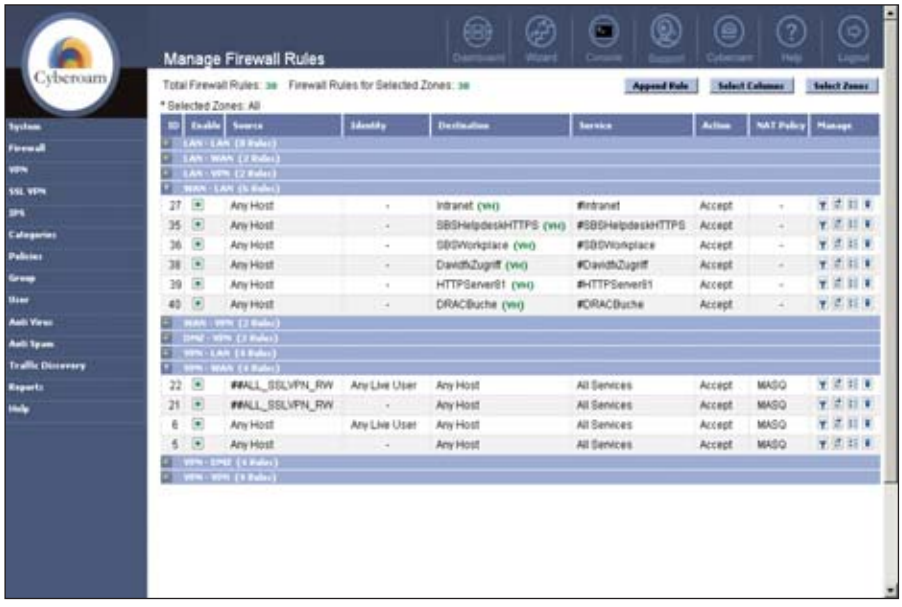


Bild 1: Die Firewall-Regeln steuern die Zugriffe vom WAN ins LAN und umgekehrt

Gateway versus Bridge

Um die volle Funktionsweise der Cyberoam CR50ia nutzen zu können, empfehlen wir die Einrichtung im Gateway-Modus. Dadurch wird das LAN und WAN physikalisch über zwei Netzwerkports der Appliance getrennt und geroutet. Der gesamte Datenverkehr vom und ins LAN läuft über die CR50ia.

Ist dagegen bereits eine Firewall im Einsatz, und Sie möchten die Konfiguration nicht ändern, bietet der Hersteller auch den Bridge-Modus an. Dabei ist die Appliance über einen Switch/Hub im Netzwerk, wie jedes andere Netzwerkgerät, eingebunden. In diesem Modus können die Routing-, Anti-Viren- und Anti-Spam-Funktionen nicht eingesetzt werden.

nutzer-Datenbank der Appliance oder einem mit Active Directory Service (ADS) und LDAP verbundenen User-Management erfolgen. Wir entschieden uns für das ADS und richteten auf den Arbeitsplätzen das Single Sign-On-Programm ein.

Verbesserungsfähiger Spam-Blocker

Wird die CR50ia wie in unserem Test im Gateway-Modus eingerichtet, fließt jeglicher Datenverkehr über das System. Mit einer gültigen Lizenz für Spam- und Viren-Schutz verwehrt die Appliance nicht nur den Zugriff auf ungewollte Internetseiten, sondern scannt zusätzlich den gesamten Datenstrom auf Spam-Nachrichten und Viren. Dabei beschränkt sich Letzteres nicht nur auf Anhänge von E-Mails, sondern auf jeglichen Code, der zum Beispiel durch einen regulären Download oder den Besuch einer Internetseite in das LAN übertragen wird. Ungebetenes wird so schon an der Eingangstüre zum Netzwerk abgelehnt.

Die Spam-Engine war im Test nicht so erfolgreich wie der Viren-Schutz. Während die CR50ia alle Viren entdeckt und in Quarantäne geschickt hat, machte die Spam-Engine einen etwas willkürlicheren Eindruck. Teilweise wurde Spam gar nicht erkannt, teilweise wurden ganz normale Nachrichten als Spam oder spamverdächtig deklariert. Die auf dem Exchange-Server im LAN betriebene alternative Anti-Spam-Lösung hatte weniger Probleme mit den Werbemails und hat die zuvor durch die Appliance durchgelassenen Nachrichten richtig klassifiziert und geblockt. Hier besteht also seitens des Herstellers noch Verbesserungsbedarf.

Guter Schutz vor DoS-Attacken

Mit dem Schutz vor Denial of Service (DoS)-Attacken verfügt die Appliance über ein besonderes Feature. Das Gerät lässt sich so konfigurieren, dass es Drop SYN Flood, UDP Flood und TCP-Traffic Flood-Attacken erkennt, wenn die Anzahl der Pakete die pro Minute definierte Quell-/Ziel-Paket-Rate übersteigt. Um die Firewall-Fähigkeiten zu testen, haben wir im Testumfeld über einen 1-GBit-Switch und das Tool "Nessus" DoS-Angriffe simuliert. Wir haben die Attacken über das LAN und den Switch simuliert, um Latenzen und Engpässen durch langsame ISP-Verbindungen vorzubeugen. Der so vorgetäuschte extreme Angriff wurde dennoch in Echtzeit erkannt und blockiert. Danach führten wir mit "Nmap Syn Stealth-Scan" und "TCP SYN" Ping-Attacken durch, die ebenfalls erfolgreich blockiert wurden.

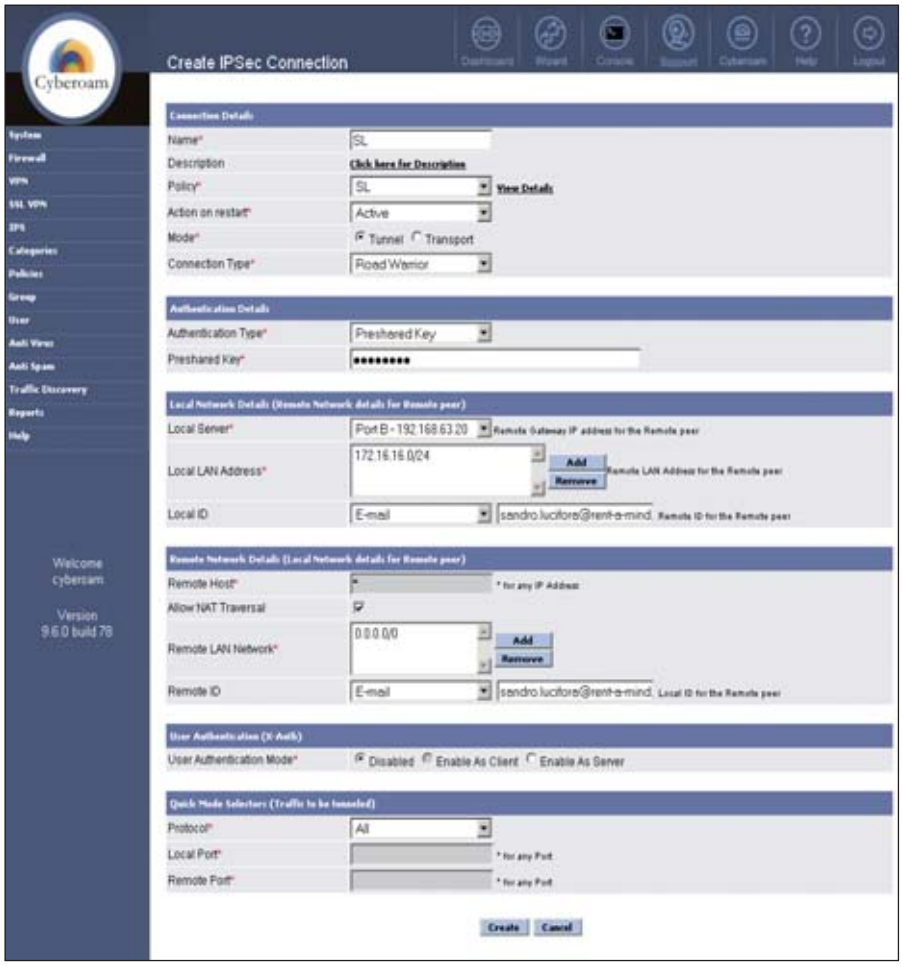


Bild 2: Die Einstellungen für die VPN-Regeln sind übersichtlich und einfach zu setzen

Remotezugriff per VPN

Mit dem VPN-Modul können mobile Benutzer und Telearbeiter über jedes Gerät einen sicheren Remote-Zugriff ins Netzwerk bekommen. Um Filialen, Home-Offices oder ein Notebook über feste oder dynamische Verbindung zu tunneln, ist ein VPN-Client nötig. Das Cyberoam-VPN unterstützt L2TP- und PPTP-Verbindungen sowie IPSec und kann so Net-to-Net- oder Host-to-Host-VPN-Verbindungen und Verbindungen für mobile Benutzer aufbauen. Der Client kann eine unter jedem Betriebssystem installierte VPN-Client-Software oder eine in einem Router integrierte VPN-Client-Lösung sein. Die VPNs von Cyberoam sind laut Hersteller von VPNC zertifiziert und sollten daher mit den meisten VPNs von Drittanbietern kommunizieren können.

Die wohl eleganteste Umsetzung für einen Remote-Client ist die in unserem Test eingesetzte Konfiguration mittels Preshared Key. Dazu haben wir die VPN-Policy unter dem entsprechenden

Menüpunkt erstellt. Danach wird eine IPSec-Verbindung auf Basis der VPN-Policy erstellt. Dabei wählten wir als Authentication Type "Preshared Key" aus. Nach der Erstellung dieses VPN-Zugangs muss dann der Schlüssel als TGB-Datei exportiert und im VPN-Client importiert werden. Als Client kam in unserem Test der Cyberoam-Client zum Einsatz.

Um sicherzustellen, dass auch durch einen VPN-Tunnel keine Malware oder Viren eingeschleust werden, sucht die Threat Free Tunneling (TFT)-Technologie im VPN-Datenverkehr nach unerwünschtem Code. Wer mehrere ISP-Gateways verbunden hat, nutzt den bei Cyberoam-VPN integrierten Failover der VPN-Konnektivität. Beim Ausfall einer ISP-Verbindung schaltet die Appliance auf die alternative VPN-Verbindung zum sekundären Gateway um.

Granulare Regeln erhöhen Komplexität

Die Appliance ermöglichte uns auch einen Echtzeiteinblick in die Verbindungen unseres Netzwerkes. Die Darstellung erfolgt wahlweise anwendungs- oder userbasiert. Auch nach IP-Adressen, der Datenübertragung oder der Bandbreiten-Nutzung werden Details der einzelnen Verbindung dargestellt. Voreingestellt generiert die CR50ia sieben ausführliche Berichte, die unter anderem Aufschluss geben über die Internet-Nutzung, die aufgerufenen Internetseiten, die Auslastung des Caches und den Mailzugriff. Die Berichte lassen sich ein Mal täglich per E-Mail an den Administrator senden. Im Laufe des Praxistests haben wir die Policies immer enger und genauer definiert. Dadurch steigerte sich die Leistung des Gerätes, was es aber auch immer schwieriger machte, mit der Appliance umzugehen. Denn schon kleine Änderungen und Anpassungen können große Wirkungen haben. Es zeigte sich, dass es sinnvoll ist, gerade zu Anfang eines der von Cyberoam vorkonfigurierten Regelwerke zum Bandbreiten-Management zu nutzen und darauf aufbauend individuelle Anpassungen vorzunehmen. Für fast jedes Szenario ist eine Policy verfügbar.

Fazit

Insgesamt ist der Funktionsumfang sehr gut und vielfältig. Und genau deshalb finden wir eine deutsche Benutzeroberfläche und Dokumentation unerlässlich. Die Konfiguration erschließt sich nicht sofort und die unstrukturierten Dokumentationen erleichtern das Vorhaben nicht wirklich. Der Hersteller hat jedoch für das nächste Update ein deutsches Interface angekündigt. Technisch gesehen ist die Appliance CR50ia ausgereift und hat auch im Härtetest gezeigt, dass sie die Anforderungen erfüllt. Die Konfiguration und Einrichtung sollte einem erfahrenen Administrator überlassen werden, da schnell das gesamte Netzwerk ohne Schutz dastehen kann oder, im Gegenteil, kein WAN-Zugriff mehr möglich ist. In Anbetracht der vielfältigen Management- und anderer Funktionen ist die CR50ia für mittelgroße Unternehmen sehr gut geeignet. *(ln)*

Produkt
UTM-Appliance mit VPN-Funktion und Bandbreitenmanagement.

Hersteller
Cyberoam – www.cyberoam.com/de/

Preis
Das Gerät selbst kostet rund 1.300 Euro. Das jährliche Abonnement für Webfilterung, Virenschutz und Spamabwehr schlägt mit etwa 1.200 Euro zu Buche.

Technische Daten
www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator *(max. 10 Punkte)*

Installation und Konfiguration	7
Content Filter-Funktionen	8
Schutz der Applikationen	10
Performance	8
VPN-Funktion	9

Dieses Produkt eignet sich

optimal für mittelgroße Netzwerke, die neben einem Content-Filter auch Remote-Anbindungen ans LAN benötigen.

bedingt für kleine Netzwerke, in denen IT-Verantwortlichen vor allem die Reglementierung des Internetzugriffs der Mitarbeiter und der Schutz des LAN wichtig ist.

nicht für den Schutz von kleinen Netzwerken mit wenigen Arbeitsplätzen, da dafür der administrative Aufwand zu groß ist.

Cyberoam CR50ia

Im Test: Clavister SG 4310

Vielzweckzugang zum Netzwerk

von Florian Thiessenhusen

Die UTM-Appliance 4310 der SG 4300-Serie von Clavister bündelt die klassischen Sicherheitsfunktionen Intrusion Detection/Prevention, Gateway Antivirus, Content Filtering und VPN in einer Hardware. Der Firewall-Hersteller mit Hauptsitz in Schweden schmückte sich noch bis vor kurzem mit dem Leitspruch "The platform techies will love". Und er könnte passender nicht sein, denn fast keine andere Firewall ist so administrationsfreundlich bei gleichzeitiger Erfüllung fast aller Sicherheitsanforderungen. Im IT-Administrator-Test zeigte sich anhand der Leistungsfähigkeit der untersuchten Sicherheitsfunktionen, dass sich Clavister keineswegs hinter den Großen verstecken muss.

Clavister unterteilt seine Produktreihen in die drei Hauptkategorien "Hardware Appliance", "Software Appliance" und "Virtual Appliance". Die einzelnen Produkte unterscheiden sich dabei nicht in den Funktionen. Ein Feature, das sich beispielsweise in der "Hardware Appliance" findet, ist genauso in den beiden anderen vorhanden und lässt sich über dieselbe Managementschnittstelle auf gleiche Weise konfigurieren. Dem Kunden wird jedoch die Wahl überlassen, auf welcher Plattform er sein Firewallprodukt implementieren will. So ist es nun auch endlich möglich, sinnvolle Netzwerksegmentierungen innerhalb einer virtuellen Umgebung durchzuführen.

Innerhalb dieses Produkttests jedoch liegt der Fokus auf einer klassischen UTM-Hardwareappliance der SG4300-Serie, der Clavister SG4310. Diese zeichnet sich durch folgende Spezifikationen aus:

- 1,5 GBit/s Firewalldurchsatz
- 600 MBit/s VPN Durchsatz
- 1.000.000 gleichzeitige Verbindungen
- 1.000 VPN-Tunnel

Eine Clavister-Firewall der SG-Serie besteht aus hauptsächlich drei Teilen: Der "Loader" ist eine abgespeckte Software, die nur dazu da ist, den Core zu starten. Dieser kommt auch dann zum Einsatz, wenn der "Core" aktualisiert wird. Der Core ist der Hauptbestandteil der Firewall. Auf diesem setzt die "Konfiguration" auf, die über eine reine Text-Datei zu bearbeiten ist.

Passgenaue Lizenzierung

Lizenziert wird bei Clavister nach einem denkbar einfachen Schema. Dabei sind Appliances fast jeder Größenordnung (von SMB/SOHO bis Enterprise) verfügbar und für jede Plattform existieren verschiedene "Hardwareprofile" (so basieren die SG4320, SG4330, SG4350 und SG4370 auf derselben Hardware), die abhängig von der Lizenz freigeschaltet werden und gleichzeitig folgende Eigenschaften verändern:

- Die maximale Anzahl gleichzeitiger Benutzer
- VPN-Durchsatz
- VPN-Tunnel
- Maximale Anzahl bedienbarer virtueller Netzwerke (VLANs)
- Die maximale Anzahl gleichzeitiger Verbindungen
- Maximale Anzahl der Firewallregeln

Dies hat den Vorteil, dass Kunden mit geringem Datendurchsatz, die dennoch viele Interfaces benötigen, nicht zu einem teuren Enterprise-Produkt wechseln müssen. Zudem kann die eigene Firewall mit den Anforderungen und Gegebenheiten des Unternehmens wachsen, ohne dass eine neue Appliance erworben werden muss. Dieses Modell macht Clavister einzigartig am Markt.

Integrierte Sicherheitsfunktionen

Wie es sich für eine UTM-Appliance gehört, sind nebst der Standardfunktion einer Stateful Firewall verschiedenste Sicherheitsfunktionen bereits integriert. Dazu gehören

- Intrusion Prevention,
- Intrusion Detection,
- Content Filtering und
- Gateway Antivirus.

Intrusion Prevention und Detection

Die Intrusion Prevention und Detection werden häufig miteinander verwechselt oder als eine Funktion angesehen. Dabei gibt es Unterschiede: Intrusion Detection erkennt Angriffe oder maliziöse Anfragen direkt am Gateway aufgrund von Patternmatching und leitet daraufhin Ak-

tionen ein (zum Beispiel Alerting, Drop, Blacklisting). Die richtige Erkennungsrate ist dabei sehr hoch. Intrusion Prevention wiederum bemerkt Angriffe aufgrund von heuristischer Erkennung. Die fälschliche Erkennungsrate kann unter Umständen groß sein, so dass der Einsatz dieser Komponente wohl überlegt sein sollte.

Im Gegensatz zu vielen anderen Wettbewerbsprodukten, in denen Intrusion Prevention/Detection lediglich generell ein- oder ausgeschaltet werden kann oder sich für nur ein Interface aktivieren lässt, bietet Clavister die Möglichkeit, eine Intrusion Prevention-/Detection-Regel für einen oder mehrere spezielle Datenstreams zu definieren. Desweiteren sind diese Regeln so modifizierbar, dass nur spezifische Angriffsmuster untersucht werden. So lässt sich zum Beispiel für einen in der DMZ platzierten Apache-Webserver, der auf Port 80 eine Webseite für externe (WAN) und interne (LAN) Benutzer ausliefert, eine IDP-Regel definieren, die zwischen WAN und DMZ Port80- und Apache-spezifische Angriffe filtert.

Content Filtering und Gateway-Antivirus

Ein wichtiges Thema auf der diesjährigen CeBIT war der Schutz von geistigem und informationellem Eigentum – kurz IPP (Intelligent Property Protection). Für Unternehmen heißt dies insbesondere, den unerwünschten Abfluss von Informationen zu verhindern. Im Normalfall fließen viele digitalen Informationen beispielsweise über E-Mail, mitunter mit sensiblen Dateianhängen. Bei Clavister lässt sich neben der Hauptfunktion des Content-Filteringdienstes (Kategorie- und Signatur-basiert Zugriff auf Webseiten unterbinden) auch der Transfer spezieller Dateitypen verhindern. Die Appliance zieht bei der Analyse einer Datei nicht nur die Dateiendung heran, sondern auch den tatsächlichen Inhalt.

Der klassische Content-Filteringdienst bietet überdies noch die Möglichkeit, dem Benutzer "overriding" zu ermöglichen. Ein Verbotshinweis beim Aufruf einer Webseite wird angezeigt, aber der Benutzer kann die Sperre für fünf Minuten aufheben und für sich den Content-Filter aussetzen. Dies hilft bei falsch klassifizierten Webseiten und verringert den Administrationsaufwand. Der Benutzer bestätigt mit einem Knopfdruck, dass seine Session in dem Fall aufgezeichnet und der IT-Abteilung zur Verfügung gestellt wird. Der Antivirus-Dienst der SG 4310 am Gateway lässt sich auf "Well known"-Ports (21, 25, 80 et cetera) aktivieren. Die Antivirus-Engine untersucht den aktuellen TCP-Stream (also ohne Caching und Verzögerungen) nach Schadcode jeder Art. Dies kann, im Gegensatz zu IDP, Dienste- und somit Regel-basiert definiert werden.

Drei Administrationsschnittstellen zur Wahl

Die Clavister-Appliance bietet gleich drei Administrationsschnittstellen. Der IT-Ver-

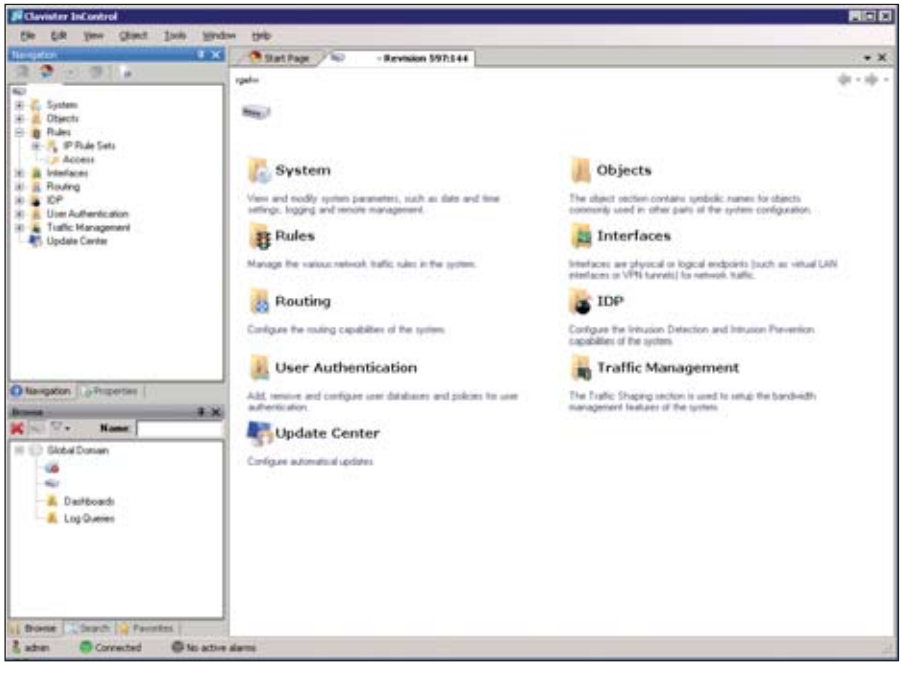


Bild 1: Die Administrationsoberfläche von InControl

UTM- versus dedizierte VPN-Appliance

Viele IT-Verantwortliche stehen bei der Wahl des VPN-Gateways vor der entscheidenden Frage, ob eine dedizierte VPN-Box (zum Beispiel "VPN Concentrator") im Rahmen der Funktionstrennung oder eine "Rundumsorglos"-Box (UTM) betrieben werden soll. Dabei zeigen sich folgende Vor- und Nachteile:

Dedizierte VPN-Appliance

Pro
- Strikte Trennung der Funktionen
- Fokus liegt technologisch auf VPN (viele Anforderungen werden erfüllt)
- Segmentierung des Perimeterübergangs leichter

Contra
- Lizenzkosten
- Erhöhter Administrationsaufwand

UTM-Appliance

Pro
- Kopplung und Adaptierung mehrerer Sicherheitsfunktionen auf einem Server: Einfache Administration
- Lizenzkosten

Contra
- Kopplung und Adaptierung mehrerer Sicherheitsfunktionen auf einem Server: Eine Schwachstelle gefährdet das gesamte System
- Single-Point-of-Failure

Aus sicherheitstechnischer Sicht ist eine dedizierte VPN-Lösung einer UTM vorzuziehen. Jedoch geht der Trend in eine ganz andere Richtung: IT-Verantwortliche wollen eine günstige Lösung, die alles kann. In größeren Umgebungen, wo spezielle Anforderungen an eine VPN-Lösung gestellt werden (Ausfallsicherheit, Performance, Verschlüsselungsdurchsatz), kann eine UTM-Appliance jedoch nicht mithalten.

antwortliche kann wählen zwischen einer Web-Oberfläche (die ohne Java/ActiveX auskommt), SSH oder einem zentralisierten Management mit "InControl". Jede dieser Schnittstellen ist vollumfänglich entwickelt. Das heißt, jede Konfiguration lässt sich an der Schnittstelle vornehmen, es gibt hier keine Limitierung. Das zentralisierte Managementtool "InControl" sollte bei einer verteilten Umgebung genutzt werden, in der mehrere Clavister-Produkte zum Einsatz kommen. Dabei können einmal getätigte Konfigurationen auf mehrere Firewalls übertragen werden.

Grundsätzlich nimmt der Administrator bei der SG 4310 zunächst seine Konfigurationen vor und muss diese in einem weiteren Schritt auf das Gerät übertragen. Das heißt, es gibt keine Änderungen, die direkt übernommen werden. Das minimiert Ausfallzeiten bei größeren Änderungen, da alle Änderungen gesammelt in einem Schritt übertragen werden. Wie schon erwähnt, besteht eine Clavister-Firewall aus Loader, Core und Konfiguration. Für ein Backup relevant sind lediglich die Konfigurationen. Diese befinden sich in einer Textdatei und sind, abhängig von der Installation, 10 bis 20 KByte groß und sollten bei jeder größeren Systemänderung manuell gesichert werden.

Aufbau eines VPNs

Für den Betrieb eines Client-VPN mit der UTM-Appliance ist auf einem Windows-basierten PC kein separater Client erforderlich. Dies wird mit dem integrierten L2TP über IPSec-Client erledigt (welchen übrigens auch das iPhone nutzt und somit 100 Prozent kompatibel ist). IPSec bietet hier die Verschlüsselung, welche das L2TP-Protokoll nicht mitbringt. Als Authentifizierungsverfahren kann eine interne Benutzerdatenbank, Radius oder auch LDAP eingesetzt werden. Kombinationen mit Token-basierten Lösungen (zum Beispiel RSA, Alladin) sind somit möglich.

Mit einem VPN wird das Hauptziel verfolgt, mobilen Benutzern und entfernten Standorten eine sichere Verbindung über öffentliche Netze in das Unternehmensnetzwerk zu ermöglichen. Es gibt zwei Hauptunterscheidungen bei dieser Art des Remote-Zugriffs, die Clavister unterstützt:

- Client-VPN (klassischer Remotezugang mit Client)
- Site-to-Site VPN (sichere Kopplung von ganzen Netzwerken über öffentliche Netze)

Die Öffnung des Unternehmensnetzwerkes per Client-VPN nach außen zu möglicherweise nicht vertrauenswürdigen Clients sollte wohl überlegt sein. Die im Unternehmensnetzwerk geltende Sicherheitsrichtlinie kann durch fehlende Kontrolle untergraben werden. Daher müssen am Gateway Lösungen gefunden werden, um die Gefahr einzudämmen.

Authentifizierung

Jeder VPN-Benutzer muss sich authentifizieren. IT-Verantwortlichen reicht dabei Username und Passwort möglicherweise nicht mehr aus, da diese an unauthorisierte Dritte weitergegeben werden können oder sich auf illegalem Weg (Sniffing oder dem "Post-it unter der Tatstatur") beschaffen lassen. Eine weitere mögliche Authentifizierungsschnittstelle ist die Token-basierte Authentifizierung. Diese lässt sich bei einer Clavister-VPN-Lösung in Kombination mit einer klassischen Authentifizierung nutzen (LDAP). Weitere mögliche Authentifizierungsquellen können sein:

- Zertifikate (Bedingen eine PKI)
- LDAP-Benutzerdatenbank (Microsoft Active Directory)
- Radius-Benutzerdatenbank
- Lokale Datenbank (Clavister)

Als sinnvoll erweist sich eine Schnittstelle mit LDAP. Geltende Passwort- und Authentifizierungsrichtlinien können so direkt adaptiert werden. Um einem Brute Force-Angriff entgegenzuwirken, sollte eine Anzahl maximaler Fehlversuche in den Gruppenrichtlinien auf den Domaincontrollern für den Remotebenutzer konfiguriert werden. Remotebenutzer können aufgrund ihrer Gruppenmitgliedschaften als auch ihrem Platz im Active Directory (OU) kategorisiert werden.

Freie Wahl bei VPN-Clients

Entgegen vielen anderen Lösungen bietet Clavister keinen eigenen VPN-Client. Somit hat sich der Hersteller selbst gezwungen, eine standardbasierte VPN-Lösung zu integrieren, zu der alle frei verfügbaren VPN-Clients verbinden können. Der in Microsoft Windows integrierte VPN-Client (der auf Basis eines über IPSec getunneltem L2TP arbeitet) ist kompatibel, genauso wie das iPhone, welches sich der gleichen Technologie bedient. Der Windows VPN-Client ist über Windows-Gruppenrichtlinien steuerbar, also erleichtert es die Administration gegenüber sogenannten "Fat Clients", die in den meisten Fällen den IP-Stack verändern und mehr Probleme bringen als sie lösen. Der in Windows integrierte Client kann sogar vor dem Anmelden am PC ausgeführt werden. Somit können Roaming User eine vollständige Domänenanmeldung erfahren.

Da die VPN-Clients im normalen Netzwerk integriert sind, werden (logischerweise) auch IP-Adressen benötigt. Deren Zuteilung geschieht zumeist per DHCP. Um die Administration zu vereinfachen, kann ein vorhandener interner Server genutzt werden, an den die Appliance diese Anfragen weiterleitet. Am elegantesten wäre es dann aber, für VPN-Clients ein eigenes Netzwerk zu bilden. Um die VPN-Clients trotzdem mit IP-Adressen aus einem differierenden Netz mit einem vorhandenen DHCP-Server versorgen zu können, muss dieser als DHCP-Relay konfiguriert werden. Diese Struktur vereinfacht das Routing und natürlich die Administration. Jedoch sollte bedacht werden, dass auch hier eine weitere Schnittstelle die Gefahr birgt, dass bei einem Ausfall des DHCP-Servers nicht einmal der VPN-Zugang funktioniert. Da Clavister in diesem Bereich

Online-Support: Die Maus zeigt mehr als tausend Worte

Mit Netviewer Online-Support sorgen Sie per Mausklick für einen besseren Kundenservice bei niedrigeren Kosten. Anfragen lösen Sie schnell und unkompliziert – und Ihre Kunden werden sich zu echten Fans mausern.

Weitere überraschende Anregungen erhalten Sie im kostenlosen Netviewer-Buch. Gleich bestellen und Gratis-Testversion anfordern unter **0721 35 44 99 400** oder:

www.netviewer.com/maus

Online-Meeting-Kultur jetzt leben!

netviewer

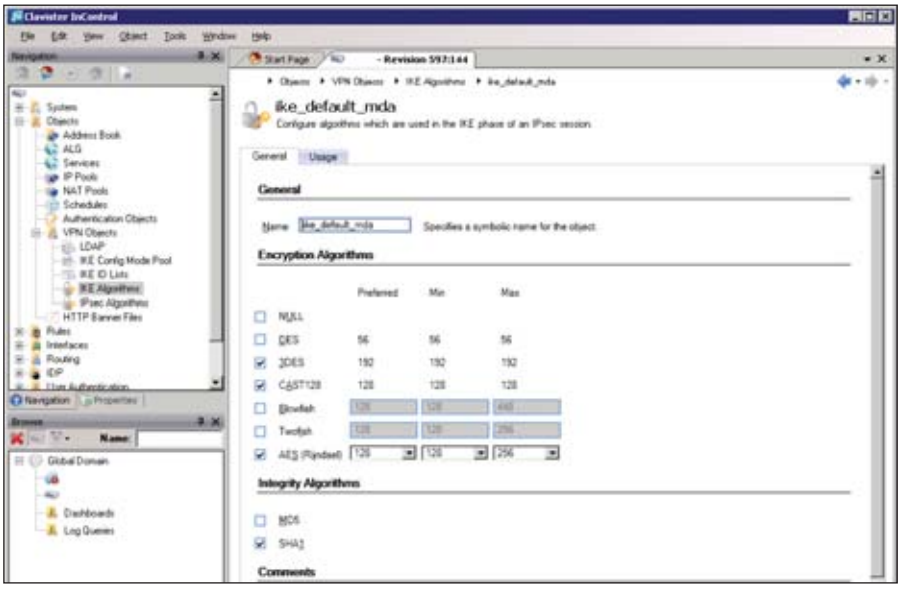


Bild 2: Die SG 4310 bietet umfassende Verschlüsselungsoptionen, die den Anforderungen der meisten VPN-Clients gerecht werden

jede erdenkliche Konfiguration unterstützt, hat der IT-Verantwortliche alle Möglichkeiten, die Anforderungen seines Unternehmens umzusetzen.

Der von den mobilen Benutzern ausgehende Datenverkehr sollte das Unternehmensnetzwerk nicht unkontrolliert passieren. Um das zu realisieren, stehen bei Clavister oben beschriebene Sicherheitsfunktionen bereit (IDP, Antivirus, ContentFilter), die auf den Datenverkehr der VPN-Benutzer angewendet werden können. Antivirus lässt sich auch auf die Windows-Dateifreigabe binden.

Umsetzung Client-VPN

Für unseren Test fokussierten wir uns im Weiteren auf den Aufbau und Betrieb eines VPN mit der Clavister-Lösung und wollen dies im Folgenden detailliert betrachten. Dafür richteten wir im Test eine über IPSec getunnelte L2TP-Verbindung ein, welche zu Windows-, Windows Mobile- und iPhone-Geräten kompatibel ist. Die Authentifizierung (Zwei Faktor: Preshared Key sowie Username/Passwort) und die Zuteilung von IP-Adressen übernimmt die Clavister-Firewall.

Innerhalb der Konfiguration benötigten wir dafür folgende Einzelkonfigurationen:

- Adressobjekte (Adressrange für die mobilen Benutzer und sonstige Objekte)
- Preshared Key
- IPSec Tunnel-Konfiguration
- L2TP Server-Konfiguration
- User Authentication-Konfiguration
- Firewallregel

Für die Konfiguration nutzten wir InControl. Das Werkzeug ist neben der Weboberfläche das komfortabelste und für Einsteiger besonders zu empfehlen, da diese Software sehr benutzerfreundlich ist. Zunächst wandten wir uns den Adressobjekten zu. Adressobjekte können Netze, IP-Adressen, MAC-Adressen oder auch Gruppen derer sein. Für unser Vorhaben definierten wir eine Range an IP-Adressen, die der interne DHCP-Server bei einem Client-Connect ausliefern soll. Unser Adressobjekt nannten wir "net_l2tp" und wiesen 40 nutzbare IP-Adressen aus einem neuen, im Netzwerk noch nicht genutzten Adresskreis zu.

Die Berechtigung eines Benutzers zur Authentifizierung legten wir in diesem Fall über den in der Clientverbindung fest konfigurierten Preshared Key fest. Stimmt dieser nicht, gelangt der Benutzer nicht zur eigentlichen Authentifizierung. Anschließend nahmen wir die IPSec-Tunnel-Konfiguration vor, die wir unter "Object / VPN Object / IKE Algorithm" erreichten. Hier definierten wir die einzelnen Protokolle. Die jeweiligen Anforderungen dafür erhalten Sie vom Hersteller des VPN-Clients. Als zugelassene Verschlüsselungsalgorithmen wählten wir 3DES, CAST128 und AES (ab 128 Bit) aus.

Der nächste Schritt bestand darin, die Entities in der IPSec-Tunnel-Konfiguration zusammenzuführen. Diese muss mit den entsprechenden Parametern erstellt werden, die davon abhängen, welche der Client bietet. Diese Parameter sind jeweils einzeln zu erfragen. Hohe und somit sichere Verschlüsselungen werden nicht immer unterstützt. Somit empfiehlt sich, für jeden Anwendungsfall eine separate Richtlinie zu erstellen. Die Verknüpfung des vorher angelegten Shared Key erfolgte unter dem Reiter "Authentication".

Über den Menüpunkt "L2TP Server Konfiguration" führten wir anschließend die angelegten Adressobjekte und die IPSec-Tunnel-Konfiguration zusammen. Nachdem Benutzer angelegt und den richtigen Gruppen zugeordnet worden waren, mussten wir nur noch eine Regel definieren, die steuert, welche Authentifizierungsquelle für das soeben eingerichtete VPN genutzt werden soll. Jedoch bringt auch die beste VPN-Konfiguration nichts, wenn der Zugriff der Clients in das Unternehmensnetzwerk nicht auch zugelassen wird. Hierfür legten wir eine Regel an. Die Clients konnten sich nun mit Angabe des Shared Keys und der Username/Passwort-Kombination am VPN anmelden. Dabei ist "net_inside" in diesem Fall das Adressobjekt für das gesamte interne Netz (angeschlossen an Interface GE1).

Firmenstandorte verbinden

Um Firmenstandorte miteinander zu verbinden, wird das Site-to-Site-VPN genutzt. Hiermit lassen sich sowohl einfache als auch beliebig komplexe Strukturen aufbauen. Die Hauptprobleme bestehen bei solchen verteilten Netzwerken hauptsächlich in den Bandbreiten, mit denen die Standorte angeschlossen sind. In Zeiten von VoIP wird die Problematik nicht

kleiner und es bedarf dafür technischer Lösungen. Eine davon ist QoS, mit Hilfe derer der gesamte Datenverkehr einer komplexen VPN-Infrastruktur durchpriorisiert werden kann.

Standorte können unter Umständen mehrere Netzwerke betreiben, welche ebenfalls über das bestehende VPN konnektiert werden müssen, aber andere Sicherheitsstandards haben (zum Beispiel VoIP-Netze, welche sich mitunter nur am VLAN-Tag unterscheiden). Clavister-Firewalls arbeiten dort standardkonform und können mehrere Netze basierend auf deren Sicherheitsanforderungen in die entsprechenden VPN-Tunnel "verpacken" und am Ziel wieder logisch aufteilen.

IT-Verantwortliche sind in der Lage, jeden Standort zu verbinden, so lange ein mit der Clavister-Firewall kompatibles VPN-Protokoll zum Einsatz kommt. Empfehlenswert dafür ist ein reines, auf Shared Key basiertes IPSec. Damit sind dann viele der namhaften Firewalls koppelbar (Cisco, SonicWall, Netscreen et cetera).

Monitoring eingebaut

Clavister-Firewalls überwachen ihre Interfaces und auch bestehende VPN-Tunnel selbst. So lässt sich ein Mechanismus aufbauen, der eine nahezu ausfallsichere und für den Benutzer völlig transparente VPN-Konnektivität zur Unternehmenszentrale gewährleistet. Als Ereignis nach einem Interface- oder Leitungsausfall können ganze Routingtabellen auf Wege umgestellt werden, die verfügbar sind. Alternativ lassen sich auch externe Monitoringwerkzeuge wie Cacti oder Nagios mittels SNMP anbinden.

Fazit

Um VPN-Zugänge für Mitarbeiter bereitzustellen, muss weder eine professionelle VPN-Lösung beschafft noch tiefgreifende Änderungen innerhalb der bestehenden Netzwerkinfrastruktur durchgeführt werden. Mit dem Verständnis der Technologie und der nötigen Vorbereitungen ist jeder Administrator in der Lage, eine VPN-Infrastruktur aufzubauen und zu warten. Das Security-Gateway der Firma Clavister zeichnet sich durch eine leichte Bedienung bei gleichzeitiger Erfüllung sämtlicher Anforderungen aus. Und auch die Herstellerunterstützung kann sich sehen lassen (sie erfolgt aus Schweden) und brilliert durch Erfahrung und Kundenorientierung. *(jp)*

Florian Thiessenhusen ist IT-Security Consultant bei der adMERITia GmbH. Seinen Blog finden Sie unter blog.port389.de

Produkt
Kombinierte VPN/UTM-Appliance.

Hersteller
Clavister
www.clavister.de

Preis
Die Clavister SG 4310 kostet mit 1,2 GBit/s Durchsatz, 400 MBit/s AES/VPN-Durchsatz und 500 VPN-Tunneln 8.995 Euro.

Technische Daten
www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator *(max. 10 Punkte)*

UTM-Firewall	8
VPN-Gateway	8
Management und Administration	9
Einbindung VPN-Clients	8
Skalierbarkeit	10

Dieses Produkt eignet sich

optimal für mittlere bis große Netzwerke mit hohen Anforderungen an Performance, Verfügbarkeit und Skalierbarkeit.

bedingt für kleine Büros oder Homeoffices.

nicht, wenn Unternehmen eine Firewall suchen, die schnell implementiert ist und nahezu wartungsarm ist, dafür ist das Produkt zu komplex.

Clavister SG 4310

Im Kurztest: TELEJET Webresetter

Langer Arm zum Server

von Sandro Lucifora

Bild 1: Der Hub ist die zentrale Schaltstelle des Webresetters

Ist ein Server remote nicht mehr erreichbar, ist selten ein Hardwaredefekt dafür verantwortlich: Das System könnte nach einem automatischen Neustart bei einer BIOS-Fehlermeldung stehen, die lediglich das Drücken einer Taste erfordert – oder der Druck auf die Reset-Taste ist notwendig. Regulär muss für diese simple Aktion dann der Administrator vor Ort sein.

Mit dem TELEJET Webresetter sollen sich bis zu 3.000 Server über das Web steuern und auf diesen Wegen über die Tastatur ansprechen und neu booten lassen. IT-Administrator hat für Sie getestet, ob dieses Versprechen auch eingehalten wird. Die Funktionsweise des Webresetters liegt in einer Kombination aus Hard- und Software, die im Zusammenspiel ihre vollen Möglichkeiten entfalten.

Durchdachte Hardwarekomponenten

Das zentrale Gerät ist der "Keyboard Simulator Hub", an den die Keyboard-Simulatoren angeschlossen werden. Die Keyboard-Simulatoren gibt es in den Ausführungen PS2 und USB – je nachdem, welche Anschlussart der Server zur Verfügung stellt. Die Verbindung von Hub und Simulator erfolgt über 4-polige Flachbandkabel mit RJ 11-Stecker. Den Hub schlossen wir mittels RS232-Kabel an den Server an, über den die Webresetter gesteuert werden und auf dem die benötigte Software läuft – dazu später mehr. Hierfür verfügt der Hub über vier Ports. Die Simulatoren selber konnektierten wir dann in Reihe – also von Simulator zu Simulator. Neben einem hilfreichen Kabeltester hat der Hub einen Uplink-Port für die Verbindung zu weiteren Hubs – so lassen sich laut Hersteller bis zu 30 Hubs in Reihe schalten und ansteuern.

Der Keyboard-Simulator, eine Art Dongle am Server, wird wahlweise an den PS2- oder einen USB-Anschluss des Rechners angeschlossen. Er simuliert am Computer eine Tastatur. Bei der PS2-Variante ist dann jedoch kein Platz mehr für eine Tastatur vorhanden. Ein unscheinbares, zweiadriges Kabel mit Pfostenstecker verbindet den Keyboard-Simulator mit dem Mainboard parallel an dem Punkt, wo das Kabel für den Reset-Taster vom Gehäuse eingesteckt ist.

Für Switches, Hubs, Router, Printserver, et cetera – also alle Geräte, die keinen Tastaturanschluss haben – ist die TELEJET 220V-Schaltbox die optionale Lösung. Hierbei handelt es sich um ein Gerät, das zwischen Netzstecker und Steckdose eingebunden wird. Über ein Adapterkabel wird diese Box mit einem regulären PS2-Keyboard-Simulator verbunden. Bei der Ansteuerung trennt die Schaltbox dann kurzzeitig die Stromzufuhr zum Gerät und startet dieses so neu.

Softwarekomponente mit Schwachstellen

Nachdem die Hardware angeschlossen war, widmeten wir uns der Software-Komponente des Paketes. Diese läuft auf dem Server, an dem der erste Keyboard-Simulator-Hub über RS232 angeschlossen ist. Die Softwaresuite besteht aus einigen Perl-Skripten und Konfigurationsdateien, die die Keyboard-Simulatoren fernsteuern. Hierzu ist der Betrieb eines funktionierenden Apache-Webservers mit Perl-Unterstützung (als Modul oder CGI) notwendig.

Im Test richteten wir diesen unter Windows 2003 x64 über die Suite XAMPP

Bild 2: Die Keybord-Simulatoren für USB und PS/2

Bestellen Sie jetzt

das IT-Administrator

Sonderheft I/2010!

180 Seiten Praxis-Know-how

rund um das Thema

Windows Server 2008 R2 und Windows 7 + Tools-CD

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

**IT-Administrator Abonnenten erhalten das Sonderheft I/2010 für € 24,90. Nichtabonnenten zahlen € 29,90.*

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

www.it-administrator.de/kiosk/sonderhefte/

administrator
Das Magazin für professionelle System- und Netzwerkadministration

Einfach kopieren und per Fax an den Leserservice IT-Administrator senden: 06123/9238-252

☐ **Ja**, ich bin IT-Administrator Abonnent mit der Abonummer (falls zur Hand) _____
und bestelle das IT-Administrator Sonderheft I/2010 zum **Abonnenten-Vorzugspreis** von nur **€ 24,90** inkl. Versand und 7% MwSt.

☐ **Ja**, ich bestelle das IT-Administrator Sonderheft I/2010 zum Preis von **€ 29,90** inkl. Versand und 7% MwSt.

Der Verlag gewährt mir ein Widerrufsrecht. Ich kann meine Bestellung innerhalb von 14 Tagen nach Bestelldatum ohne Angaben von Gründen widerrufen.*

Ich zahle ☐ per Bankeinzug

Geldinstitut: _____

Kto.: _____ BLZ: _____

oder ☐ per Rechnung

Datum: _____

Unterschrift: _____

Firma: _____

Name, Vorname: _____

Straße: _____

Land, PLZ, Ort: _____

Tel: _____

E-Mail: _____

* Zur Fristwahrung genügt die rechtzeitige Absendung einer E-Mail an leserservice@it-administrator.de oder einer kurzen postalischen Mitteilung an Leserservice IT-Administrator, 65341 Eltville.

ITA 0510

So erreichen Sie unseren Vertrieb, Abo- und Leserservice:

Leserservice IT-Administrator
vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville
Tel: 06123/9238-251
Fax: 06123/9238-252
leserservice@it-administrator.de

Diese und weitere Aboangebote finden Sie auch im Internet unter www.it-administrator.de

E-BOOK SYSTEMS
Abos und Einzelhefte gibt es auch als E-Paper

Heinemann Verlag
Leopoldstraße 85
D-80802 München
Tel: 089-4445408-0
Fax: 089-4445408-99
Geschäftsführung:
Anne Kathrin Heinemann
Matthias Heinemann
Amtsgericht München HRB 151585

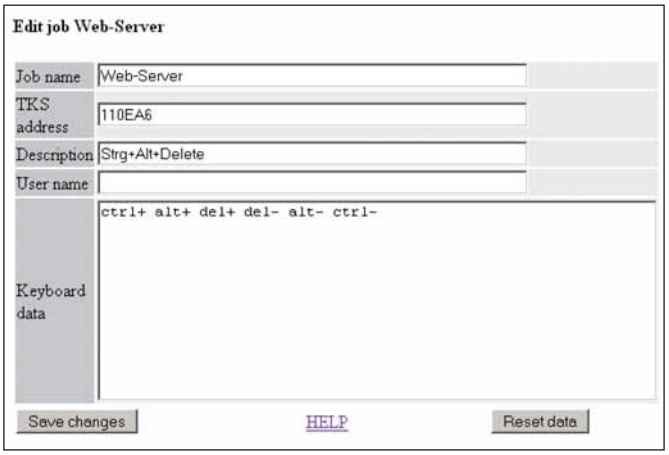


Bild 3: Die Konfiguration eines Simulators benötigt nur wenige Angaben

1.7.3 mit Apache 2.2.14 und Perl 5.10.1 ein. Zuvor mussten wir feststellen, dass der Betrieb der Lösung auf einem ISS 6 und 7 nicht möglich war. Der Hersteller gibt an, dass dieser Einsatz möglicherweise Änderungen am Programmcode erfordert, konnte jedoch dazu keine direkte Lösung liefern.

Die Web-Software selbst stellte sich als eine sehr einfache und wenig durchdachte Lösung dar, die lediglich als Basis für eigene Anpassungen dienen kann. Die Funktionsweise ist schnell erklärt: Jeder Keyboard-Simulator verfügt über eine einmalige Hardwareadresse (TKS-ID). An diese wird eine Folge von Tastaturkommandos oder der Reset-Befehl gesendet und entsprechend ausgeführt.

Im Test schlossen wir zwei Keyboard-Simulatoren, jeweils für PS2 und USB, an. Um diese anzusteuern, mussten wir neben der TKS-ID auch die zu sendenden Tastatur-Befehle eintragen. In der Übersichtstabelle wählten wir nun den anzusteuernden Simulator aus und sendeten dann wahlweise die hinterlegten Tastaturkommandos oder einen Hardwarereset. Leider ist es nicht möglich, für ein und dieselbe TKS-ID mehrere Einträge mit verschiedenen Tastaturkommandos zu hinterlegen. Änderungen der Tastaturkommandos müssen bei Bedarf jeweils vor dem Absenden erfolgen. Grundlegend leistet die Webapplikation ihre Dienste. Wer jedoch mehrere Dutzend oder 100 Simulatoren betreiben will, wird nicht darum herumkommen, seine eigene Applikation auf Basis dieser Skripte umzusetzen.

Reset des Resetters

Für den Fall, dass der Webresetter-Server nicht mehr erreichbar ist und selbst einen Reset benötigt, hat der Hersteller den Keyboard-Simulator mit einem verzögerten Reset ausgestattet. Erhält der Simulator das entsprechende Kommando, wird nach fünf Minuten ein Hardwarereset durchgeführt – es sei denn, das Kommando wird zwischenzeitlich noch mal gesendet und startet so den Timer neu.

Über diese Funktion realisierten wir eine Art "Totmann-Schalter": Geholfen hat uns das verfügbare Perl-Skript *cron-reset.pl*. Nach der Einrichtung richteten wir über den Windows-Scheduler – mithilfe des Tools "wget" – einen Job ein, der das Perl-Skript alle 290 Sekunden aufruft und somit die Verzögerung am Simulator neu setzt. Fällt der Server einmal aus und kann daher das Skript nicht mehr aufgerufen werden, startet der Keyboard-Simulator den Computer nach spätestens fünf Minuten neu.

Fazit

Die Funktion des Webresetters ist sinnvoll und gut umgesetzt. Die Ausführung der Hardware ist sehr gut gelungen und durchdacht. Die zwangsläufig benötigte Software entspricht jedoch in keiner Form dem sonst guten Eindruck der Lösung und wertet unser Testergebnis ab. Zwar kommen wir zum Ziel, doch schränkt die Anwenderführung als auch die äußerst puristische Umsetzung der Software den Nutzerkreis sehr ein. Wer jedoch plant, die Funktionen des Webresetters in eine eigene Web- oder Windows-Anwendung einzubinden, der ist mit dem Paket gut beraten. *(jp)*

Produkt
IP-basierter KVM-Hub.

Hersteller
Telejet Kommunikations GmbH,
Bezug über ICO Innovative Computer GmbH
www.webresetter.de

Preis
TELEJET Webresetter Starterkit (je zwei PS2- oder USB-Anschlüsse): 94 Euro
Keyboard Simulator: 46 Euro
220V-Schaltbox: 51 Euro

Technische Daten
www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator *(max. 10 Punkte)*

Umsetzung	6
Handhabung	7
Aufwand der Konfiguration	10
Zuverlässigkeit	10
Kosten/Nutzen	8

TELEJET Webresetter

BranchCache unter Windows 7 und Server 2008 R2 konfigurieren

Vorratsschrank für die Filiale

von Ulf B. Simon-Weidner

Bereits in älteren Windows-Versionen hatte Microsoft in die Unterstützung verteilter Infrastrukturen investiert. Allerdings lässt sich erst mit der Kombination von Windows 7 und Server 2008 R2 und der Option BranchCache eine nennenswerte Verringerung des WAN-Verkehrs erreichen. In diesem Workshop setzen wir uns mit den unterschiedlichen Modi der neuen Funktion auseinander und zeigen Ihnen Schritt für Schritt, wie Sie BranchCache für eine Filiale einrichten.

Wie bereits der Name erahnen lässt, ermöglicht BranchCache Unternehmen, eine Caching-Funktion in einer Zweigstelle zu implementieren. Diese Caching-Funktion steht sowohl den Dateidiensten zur Verfügung sowie für HTTP(S)und BITS, dem Background Intelligent Transfer Service, der vor allem beim Windows-Update und System Center Configuration Manager (SCCM) zum Einsatz kommt. Richten Sie die Clients einer Zweigstelle für BranchCache ein, wird eine vom zentralen Server angefragte Datei in der Filiale nur einmal über das WAN geladen, und zwar dann, wenn der erste Anwender darauf zugreifen möchte. Fordern nun weitere Clients der gleichen Zweigstelle die Daten an, erhalten diese die beim letzten Zugriff bereits im Cache abgelegte Version. Um zu verstehen, wie dieses Zwischenspeichern genau funktioniert, sehen wir uns zunächst die zwei Modi von BranchCache an.

So funktioniert BranchCache

Für jede Zweigstelle können Sie einzeln festlegen, ob diese im verteilten oder im gehosteten Modus operieren soll. Bild 1 und 2 verdeutlichen die generelle Funktionsweise von BranchCache im verteilten Modus.

Wenn der erste Client aus der Zweigstelle eine Datei anfragt, geschieht folgendes (siehe Bild 1):

1. Der Client fragt den Server nach der Datei.
2. Der Server gibt dem Client, wenn dieser das Recht hat die Datei einzusehen, einen Hash-Wert der Datei zurück.
3. Der Client fragt per Multicast in seinem Subnetz, ob bereits ein anderer Rechner eine Datei mit demselben Hash-Wert abgelegt hat.
4. Ist dies nicht der Fall und der Client erhält keine Antwort, bittet er den Server um die Dateiinhalte.
5. Der Client erhält vom Server die Datei und speichert sie zwischen.

Fragt nun ein zweiter Client aus der Zweigstelle die gleiche Datei an, ist der Ablauf, wie in Bild 2 ersichtlich, wie folgt:

1. Der Client fragt den Server nach der Datei.
2. Der Server überprüft wiederum die Berechtigung und liefert dem Client den Hash-Wert.
3. Der Client fragt per Multicast in seinem Subnetz nach der Datei.
4. Da der erste Client die Datei bereits hat, gibt er diese an Client zwei weiter. Die Daten müssen somit nicht über das WAN transportiert werden.

Schreibzugriffe geschehen immer auf dem Server, außerdem ist durch den Hash-Wert sichergestellt, dass der Client immer die aktuelle Version erhält. Denn ändert sich die Datei, wandelt sich auch deren Hash-Wert, und die Datei muss erneut in die Zweigstelle übermittelt werden. Damit stellt Microsoft sicher, dass Versionskontrolle und Zugriffsberechtigung immer vom Server in der Zentrale abgewickelt werden. Der Cache in der Zweigstelle bedient lediglich die Inhalte der Dateien. Allerdings hat der verteilte Modus auch Nachteile: Wenn derjenige Client, der die Kopie der Datei bereithält, gerade offline ist und sich nicht im Netzwerk befindet, muss die Datei erneut geladen werden. Außerdem werden durch den Multicast nur Cache-Inhalte aus dem gleichen Subnetz gefunden, da bei mehreren Subnetzen in einer Filiale die Dateien mehrfach angefragt und zwischengespeichert würden.

Deshalb gibt es neben dem verteilten Modus des BranchCache noch den gehosteten Modus. Hierbei wird der Cache in der Zweigstelle auf einem Server abgelegt. Der

Ablauf über das WAN bleibt der gleiche wie beim Distributed Mode, allerdings würde der erste Client, nachdem er die Datei des zentralen Servers erhalten hat, diese dem lokalen BranchCache-Server zur Zwischenspeicherung übergeben. Zudem führen Clients in dieser Konfiguration bei der Suche nach einer Datei keinen Multicast im Subnetz durch. Vielmehr kontaktiert der Client direkt den BranchCache-Server. Diesen nennt Microsoft den "Hosted Cache Server". Damit sind die Daten auch dezentral nur auf einem System vorgehalten und es ist unerheblich, ob Clients häufiger offline sind. Außerdem können so auch Zweigstellen, die über mehrere Subnetze verfügen, BranchCache einsetzen.

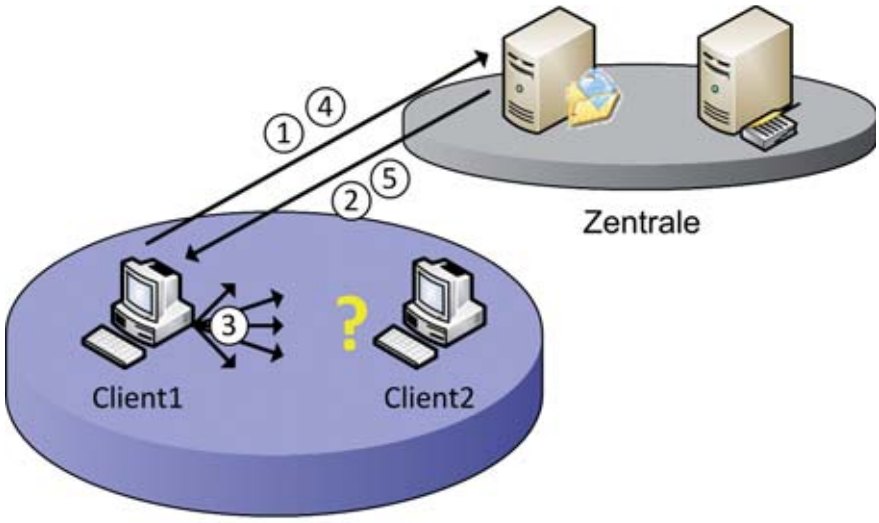


Bild 1: Beim ersten Zugriff erhält der Client die Daten vom zentralen Server und speichert diese zwischen

Verteilter versus gehosteter Cache

Sie müssen sich also pro Zweigstelle entscheiden, ob sie BranchCache verteilt über die Clients eines Subnetzes implementieren oder gehostet mit einem Cache-Server betreiben. Als generelle Richtlinie gilt: Wenn es in der Zweigstelle nur ein Subnetz gibt, die Stationen in der Regel zu Betriebszeiten innerhalb der Zweigstelle eingeschaltet sind und die Anzahl der Clients nicht zu groß ist (Microsoft schlägt hier einen Richtwert von 50 Clients vor), sollten Sie der Einfachheit halber den verteilten Modus wählen. Bei mehreren Subnetzen und/oder einer höheren Anzahl von Clients und wenn ein Server in der Zweigstelle existiert, bietet sich der gehostete Modus an.

Je nach Aufbau müssen Sie verschiedene Voraussetzungen beachten. Clientseitig benötigt BranchCache generell Windows 7 in der Enterprise- oder Ultimate-Version. Serverseitig ist zu unterscheiden zwischen Servern, welche die Inhalte in der Zentrale anbieten (wie Webserver, Update-Server oder Dateiserver) und Cache-Servern, die in der Zweigstelle den BranchCache im gehosteten Modus anbieten. Die Inhaltsserver können auf jeder Version von Windows Server 2008 R2 laufen, außer in der Kombination Servercore mit Hyper-V. Als Cache-Server für die Zweigstelle kommt entweder die Enterprise- oder die Datacenter-Version in Frage, wobei hier sowohl Servercore wie auch Hyper-V möglich ist. Damit lässt sich ein Zweigstellen-Server einrichten, der zum Beispiel einen Read-Only-Domänencontroller anbietet, für die Filiale den BranchCache verwaltet und zudem weitere Systeme über Hyper-V anbietet.

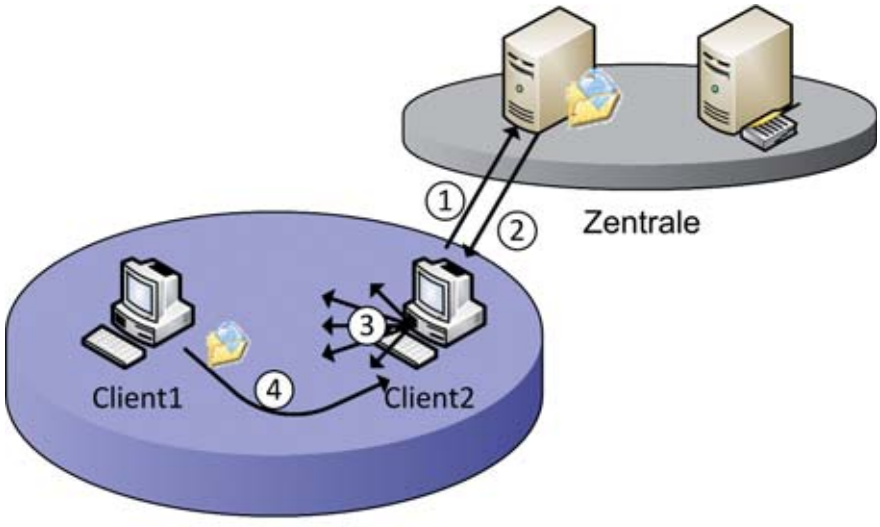


Bild 2: Weitere Clients der Zweigstelle erhalten die von ihren Kollegen im Cache vorgehaltenen Daten

Einrichten von BranchCache

Sie richten BranchCache in zwei beziehungsweise drei Schritten ein: Erst konfigurieren Sie die Clients, dann die Inhaltsserver in der Zentrale, und, wenn Sie den gehosteten Modus verwenden, abschließend den Cache-Server in der Zweigstelle.

Vorbereiten der Clients

Die Clients werden in Unternehmensnetzwerken meistens per Gruppenrichtlinien konfiguriert. Hierbei ist es am einfachsten, wenn im Active Directory bereits Organisationseinheiten für den Standort bestehen. Sie erstellen dann eine neue Gruppenrichtlinie, die Sie auf die OU des Standortes verknüpfen. Innerhalb dieser Richtlinie konfigurieren Sie im Abschnitt "Compu-

terkonfiguration / Richtlinien / Administrative Vorlagen / Netzwerk / BranchCache" die folgenden Einstellungen:

- "BranchCache aktivieren" auf "Aktiviert" setzen.
- "BranchCache-Modus 'Verteilter Cache'" auf "Aktiviert" setzen, wenn der Cache verteilt sein soll.
- "BranchCache-Modus 'Gehosteter Cache' festlegen" auf "Aktiviert" setzen, wenn Sie einen BranchCache-Server in der Zweigstelle einsetzen wollen. In diesem Fall müssen Sie den Namen des Servers über diese Einstellung konfigurieren.
- Mittels der Einstellung "BranchCache für Netzwerkdateien konfigurieren" können Sie festlegen, wie lange die Latenzzeit zwischen Client und Server sein soll, damit ein Inhalt zwischengespeichert wird. Tragen Sie hier den Wert "0" ein, kommt es immer zu einer Zwischenspeicherung der Inhalte. Der Standardwert beträgt 80 ms.
- Ist die Funktion "Prozentuale Speicherplatzbelegung durch Clientcomputercache festlegen" aktiv, können Sie im verteilten Modus festlegen, wie viel Prozent des Plattenplatzes von Clients Sie für das Zwischenspeichern verwenden wollen. Standardmäßig sind es fünf Prozent.

Da beim verteilten Modus keine standortspezifischen Einstellungen notwendig sind, reicht oftmals eine Richtlinie im Unternehmen für alle Standorte, die den verteilten Modus nutzen, aus.

Zusätzlich müssen Sie die Firewall auf den Clients anpassen, damit Anfragen nach den BranchCache-Daten von anderen Clients angenommen werden. Dies erledigen Sie am besten in der gleichen Richtlinie, unter dem Knoten "Computerkonfiguration / Richtlinien / Windows-Einstellungen / Sicherheitseinstellungen / Windows-Firewall mit erweiterter Sicherheit / Windows-Firewall mit erweiterter Sicherheit – LDAP". An dieser Stelle erstellen Sie die folgenden Richtlinien. Legen Sie hierbei jeweils neue Regeln an, wählen Sie vordefinierte Regeln aus und bestätigen Sie die Standardwerte. Für einen verteilten Cache sieht die Konfiguration folgendermaßen aus:

Eingehende Regeln:

- BranchCache – Inhaltsabruf (HTTP eingehend)
- BranchCache – Peerermittlung (WSD eingehend)

Ausgehende Regeln:

- BranchCache – Inhaltsabruf (HTTP ausgehend):Verbindung zulassen wählen.
- BranchCache – Peerermittlung (WSD ausgehend):Verbindung zulassen wählen.

Beim gehosteten Mode müssen Sie die Clients wie folgt einrichten:

Eingehende Regeln:

- BranchCache – Inhaltsabruf (HTTP eingehend)

Ausgehende Regeln:

- BranchCache – Inhaltsabruf (HTTP ausgehend):Verbindung zulassen wählen.
- BranchCache – Gehosteter Cache-Client (verwendet HTTPS)

Ob BranchCache bei den Clients eingeschaltet ist, können Sie mit dem folgenden Befehl überprüfen:

```
Netsh branchcache show status
```

Konfiguration der Inhaltsserver

Gehen wir zunächst davon aus, dass wir den verteilten Modus gewählt haben, müssen wir nun noch den Inhaltsserver entsprechend einrichten. Der Inhaltsserver bezeichnet bei BranchCache denjenigen Server in der Zentrale, dessen Ressourcen mittels BranchCache in der Zweigstelle zwischengespeichert werden dürfen.

Vorbereiten der Dienste

Dient der zentrale Server als Dateiserver, müssen Sie zusätzlich zur Dateiserverrolle noch der Rollendienst "BranchCache für Netzwerkdateien" einrichten. Dies geschieht einfach im Servermanager, entweder beim erstmaligen Einrichten der Dateiserverrolle oder indem Sie unterhalb der Rolle noch den Rollendienst nachinstallieren. Ein Tipp: Ist auf Dateiservern unter Windows Server 2008 oder höher noch der Rollendienst "Windows Search" installiert, können Clients ab Windows Vista die Inhalte von verbundenen Netzwerklaufwerken in die lokale Suche mit einbeziehen, wobei die Suchanfrage parallel an den Server geschickt wird und das Ergebnis in den Suchergebnissen integriert wird.

Erstellen von Hash-Werten

Danach müssen Sie den Fileserver noch anweisen, Hash-Werte für die Dateien zu generieren. Hierfür erstellen Sie für die Dateiserver eine eigene Gruppenrichtlinie und aktivieren die Einstellung "Hashveröffentlichung für Branchcache" unter "Computerkonfiguration / Richtlinien / Administrative Vorlagen / Netzwerk / LanMan-Server". Dabei wählen Sie aus, ob die Hashwerte nie generiert werden (und BranchCache damit auf diesem Server nicht funktioniert), ob die Werte immer generiert werden oder nur, wenn die jeweilige Freigabe per BranchCache zwischengespeichert werden darf.

Die Hashwerte werden erstellt, sobald sich Clients mit aktiviertem BranchCache verbinden. Sie können das Erstellen der Hashes aber auch erzwingen, indem Sie den folgenden Befehl auf dem Server eingeben:

```
Hashgen -f {freigegebener Ordner}
```

Dann müssen Sie noch das Zwischenspeichern auf der Freigabe für BranchCache erlauben. Dies können Sie entweder beim Erstellen einer Freigabe oder im Nachhinein einrichten.

Nach diesen Vorbereitungen können Sie mit den ersten Testläufen beginnen. Unter Umständen kann es etwas dauern, bis die Hashes berechnet werden, so dass in Testumgebungen nicht immer sofort etwas zu sehen ist. Über den folgenden Befehl können Sie die aktuell genutzte Größe für den lokalen Cache auf dem Client abfragen:

```
NetSh branchcache show localcache
```

In der Ereignisanzeige können Sie unter "Anwendungs- und Dienstprotokolle / Microsoft / Windows / BranchCache-SMB" die Ereignisse einsehen. Das Event 3005 bietet in der Detailansicht eine Übersicht, wie viel aus dem Cache geladen werden konnte. Im Internet ist mittlerweile ein Powershell-Skript [1] verfügbar, um über diese Events zu errechnen, wie viel WAN-Verkehr Sie durch die Verwendung von BranchCache gespart haben.

Einrichten eines gehosteten Caches

Betreiben Sie BranchCache im gehosteten Modus, müssen Sie noch den dazugehörigen Server konfigurieren. Hierzu müssen Sie zunächst das BranchCache-Feature – genauso wie beim Inhaltsserver – über den Servermanager installieren und sicherstellen, dass der dazugehörige Dienst gestartet ist. Dann müssen Sie den Server anweisen, dass er im gehosteten Servermodus laufen soll. Dies erledigen Sie in der Kommandozeile des Servers mit dem folgenden Befehl:

```
netsh branchcache set service
  mode=HOSTEDSERVER
```

Hierbei wird die Windows Firewall gleich korrekt konfiguriert. Wollen Sie die Firewall aber über Gruppenrichtlinien steuern, müssen Sie darauf achten, dass die BranchCache-Serverregeln nicht überschrieben beziehungsweise erlaubt werden.

Da im gehosteten Modus die Kommunikation per HTTPS läuft, muss der Server ein Zertifikat erhalten. Es ist empfehlenswert, dies mittels einer Windows-CA zu erledigen, da die Zertifikate durch ein AutoEnrollment automatisch an den oder die Server vergeben und verwaltet werden. Es ist wichtig, dass der Server ein SSL-Zertifikat vom Typ "Web Server" erhält, das den vollqualifizierten Namen des Servers enthält. Zusätzlich müssen sowohl der Server wie auch die Clients der Zertifikatsautorität vertrauen: Dies wird zumeist ebenso per Gruppenrichtlinien gesteuert. Die Schritte hierzu sind identisch zu anderen internen HTTPS-Servern. Wenn der Server sein Zertifikat erhalten hat, müssen Sie noch das Zertifikat für die Verwendung von BranchCache einrichten. Hierfür navigieren Sie in der Zertifikats-Managementkonsole zu dem Zertifikat des lokalen Computers, das Sie eben erstellt haben, navigieren in die Details des Zertifikates und kopieren den Thumbprint. Diesen kopieren Sie am besten vorübergehend in einen Texteditor, da Sie die Leerzeichen in der Zeichenfolge entfernen müssen. Den so bereinigten Thumbprint setzen Sie dann in den folgenden Befehl ein, damit BranchCache dieses Zertifikat verwendet:

```
netsh http add sslcert ip-
  port=0.0.0.0:433
  certhash={Thumbprint ohne Leerzei-
  chen} appid={d673f5ee-a714-454d-
  8de2-492e4c1bd8f8}
```

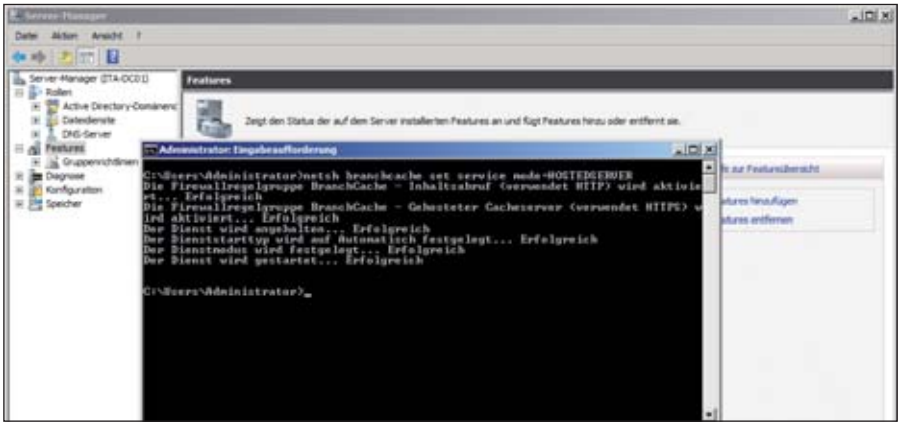


Bild 3: Mittels *netsh* weisen Sie den Server an, den Hosted Cache zur Verfügung zu stellen

Stellen Sie abschließend noch einmal sicher, dass der vollqualifizierte Name des Servers über die Gruppenrichtlinie korrekt bei den Clients eingetragen ist. Damit ist der Hosted-Cache funktionsfähig und wird von den Clients des Standortes verwendet.

Fazit

Zunächst mag das Einrichten von BranchCache etwas aufwändig erscheinen. Der Vorgang ist aber überwiegend durch Gruppenrichtlinien zu bewerkstelligen und insgesamt einfacher als gedacht. Zahlreiche NetSh-Befehle unterstützen die Konfiguration und das Überprüfen des Status. Wenn BranchCache einmal eingerichtet ist, sollten Sie sich in der Regel nicht mehr damit beschäftigen müssen. *(ln)*

Ulf B. Simon-Weidner ist MVP für Windows Server-Directory Services und arbeitet als Consultant und Trainer. Sein Weblog finden Sie unter http://msmvps.com/ulfbsimonweidner/

Links und Ressourcen

[1] PowerShell-Skript, um die Ersparnis der Bandbreite zu berechnen
http://code.msdn.microsoft.com/GetBandwidthSaving/

Microsoft TechCenter zu BranchCache
http://technet.microsoft.com/de-de/library/dd996634(WS.10).aspx

NetSh-Kommandos für BranchCache
http://technet.microsoft.com/de-de/library/dd979561(WS.10).aspx

BranchCache-Kommandos per Powershell auf zahlreichen Computern ausführen
http://blogs.msdn.com/powershell/archive/2009/10/31/quick-dirty-super-useful-scripting.aspx

BranchCache Migration
http://technet.microsoft.com/de-de/library/dd548365(WS.10).aspx

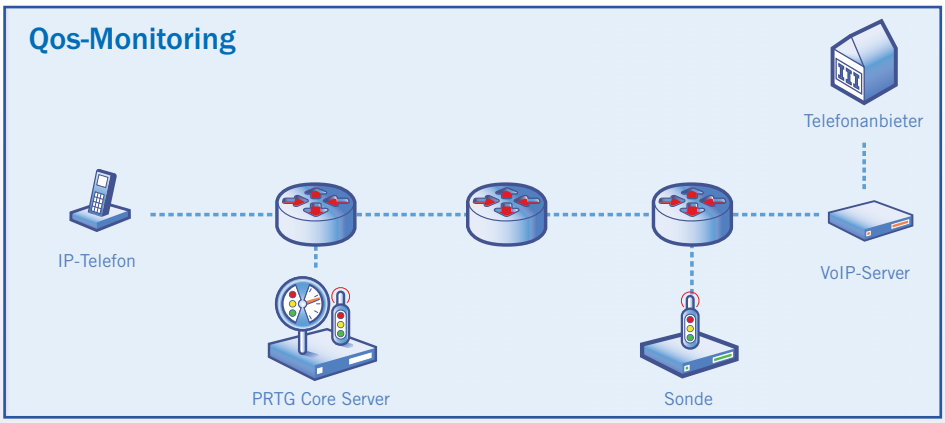
SCCM2007 für BranchCache einrichten
www.mssccmfaq.de/2010/02/02/configmgr-2007-sp2-branch-cache/

VoIP-Problemen frühzeitig entgegensteuern

Gesicherte Übertragungsqualität durch QoS-Monitoring

Immer mehr Unternehmen ersetzen ihre klassische Telefonie durch Voice-over-IP-Lösungen. Dabei ermöglichen High Density (HD) Audio Codecs heute eine sehr gute Sprachqualität. In der Praxis haben User jedoch immer noch mit Verbindungsfehlern, Sprachverzögerungen, Echos etc. zu kämpfen. Daher ist es für den Administrator von essenzieller Bedeutung, die Qualität der VoIP-Dienste auf Basis eines geeigneten Monitorings sicherzustellen.

Um „Voice over IP" (VoIP) als zuverlässige Telefonielösung nutzen zu können, ist die Übertragungsqualität entscheidend. Das gilt im selben Maße auch für die Datenpakete von Video- und anderen Streams. Oft ist eine unzureichende Quality-of-Service (QoS) im Netzwerk für Störungen und Ausfälle verantwortlich – sei es auf Seiten des Senders oder des Empfängers. Mit Hilfe eines professionellen Netzwerk-Managements sollte die QoS permanent überwacht werden.



Engpässe im Netzwerk entdecken und beseitigen

Dazu wird eine Monitoring-Lösung wie beispielweise PRTG Network Monitor der Paessler AG benötigt, die entsprechende Optionen wie IP SLA- oder QoS-Sensoren bietet. Beide Sensoren messen Parameter wie Jitter*) und Paket-Verzögerung**). Darüber hinaus protokolliert PRTG verlorene, neu angeforderte und duplizierte Pakete.

Die Parametermessungen erfolgen durch das Senden verschiedener UDP(User-Datagram-Protocol)-Pakete zwischen zwei Sonden. Die Übertragungsqualität von UDP-Paketen beeinflusst maßgeblich Ton und Bild der einzelnen Applikationen. Fehler, die Verbindungsfehler oder Sprachverzögerungen etc. zur Folge haben, können so auf einfache Weise ausfindig gemacht werden. Im laufenden Betrieb alarmiert PRTG den Administrator bei auftretenden Problemen oder überschrittenen Grenzwerten unverzüglich via E-Mail, SMS, SNMP Trap etc.

VoIP-Monitoring auch für Cisco IP SLA

Das Cisco IOS-Betriebssystem bietet mit IP SLA ein spezielles Feature, das QoS-Leistungsdaten zur Verfügung stellt. Es basiert auf einer Technologie zur aktiven Überwachung des Datenverkehrs und bietet so eine verlässliche Methode zur Messung der Performance. Als Cisco Technology Developer Partner hat die Paessler AG einen speziellen Sensor für die Überwachung der IP Service Levels entwickelt. Mit PRTG Network Monitor haben Administratoren, die mit entsprechenden Cisco-Routern und Switches arbeiten, so die Möglichkeit, Service Levels einfach in ihr Netzwerk-Monitoring zu integrieren.

Sowohl der QoS- als auch der IP SLA-Sensor sind ohne Aufpreis bereits in der Basis-Lizenz von PRTG enthalten. Detaillierte Informationen zu PRTG Network Monitor stehen unter folgendem Link zur Verfügung: http://www.de.paessler.com.

*) in Millisekunden übereinstimmend mit dem RFC 3550-Transportprotokoll

**) in Millisekunden übereinstimmend mit dem RFC 3393-Protokoll

PAESSLER®

Paessler AG
Burgschmietstraße 10
D-90419 Nürnberg
Tel.: +49 (911) 7 39 90 30,
Fax: +49 (911) 7 39 90 31

E-Mail: info@paessler.com
URL: www.de.paessler.com

Ansprechpartner:
Christian Twardawa

VPNs mit SSTP einrichten

Alternativer Datentunnel

von Oliver Ebel

VPNs sind praktisch für den sicheren Remote-Zugriff. Doch in vielen Umgebungen bereiten sie auch Probleme, etwa im Zusammenspiel mit NAT-Routern und Firewalls. Mit dem SSTP-Protokoll hat Microsoft diese Einschränkungen erheblich entschärft. Das Protokoll routet den Datenverkehr über den HTTPS-Port 443 und rutscht damit ohne Schwierigkeiten von außen ins lokale Netzwerk. IT-Administrator zeigt Ihnen, wie Sie SSTP auf einem Windows Server 2008 R2 einrichten und wo im Netzwerk Stolperfallen lauern.

Das Microsoft-Protokoll SSTP (Secure Socket Tunneling Protocol) basiert auf SSL und nutzt HTTPS-Verbindungen über Port 443. Dies ermöglicht den VPN-Verbindungsaufbau in das Firmennetz über Firewalls, nicht authentifizierende Proxys und NAT-Router hinweg, da dieser Port typischerweise nicht blockiert wird. Per Definition ist SSTP dabei ein Protokoll auf Applikationsebene und primär für Einwahl-Verbindungen (RAS) vorgesehen. SSTP bietet wie LTP/IPSec Datenvertraulichkeit, Datenintegrität und -Authentifizierung und erfordert ebenfalls eine Public Key Infrastruktur (PKI); unterstützt wird das VPN-Protokoll ab Windows Vista (SP1) und Windows Server 2008. Eine Übersicht und weiterführende Informationen zu den genannten VPN-Protokollen finden Sie bei Microsoft im Technet-Artikel "VPN-Tunneling-Protokolle" [1].

Ablauf eines SSTP-Verbindungsaufbaus

Beim Herstellen einer SSTP-basierten VPN-Verbindung finden folgende Ablaufschritte statt:

1. Der SSTP-VPN-Client initiiert eine TCP-Verbindung mit dem SSTP-Gateway-Server mit einem clientseitig dynamisch zugewiesenen TCP-Port und dem serverseitigen TCP-Port 443.
2. Daraufhin sendet der SSTP-VPN-Client eine SSL "Client-Hello"-Nachricht, die dem SSTP-Gateway-Server den Wunsch nach einem Verbindungsaufbau signalisiert.
3. Als Antwort auf diese Verbindungsanfrage sendet der SSTP-Gateway-Server sein Computerzertifikat an den SSTP-VPN-Client.
4. Das erhaltene Computerzertifikat validiert der SSTP-VPN-Client mit Hilfe seines lokalen Zertifikatspeichers. Das Zertifikat der Zertifizierungsstelle, mit dem das Computerzertifikat signiert wurde, muss sich in den vertrauenswürdigen Stammzertifizierungsstellen befinden. Anschließend handelt der SSTP-VPN-Client die Verschlüsselungsmethode aus, erzeugt einen SSL-Sitzungsschlüssel, verschlüsselt diesen mit dem öffentlichen Schlüssel des SSTP-Gateway-Servers und sendet zuletzt den so verschlüsselten SSL-Sitzungsschlüssel an den SSTP-Gateway-Server zurück.
5. Der SSTP-Gateway-Server entschlüsselt den SSL-Sitzungsschlüssel mit dem privaten Schlüssel seines Computerzertifikats; der nachfolgende verschlüsselte Datenaustausch erfolgt unter Verwendung der ausgehandelten Verschlüsselungsmethode und des SSL-Sitzungsschlüssels.
6. Der SSTP-VPN-Client schickt eine HTTPS-Anforderung an den SSTP-Gateway-Server.
7. Ein SSTP-Tunnel wird von Clientseite aus zum SSTP-Gateway-Server initiiert.

Bild 1: Der Verbindungsaufbau einer SSTP-VPN-Verbindung

8. Der SSTP-VPN-Client initiiert eine PPP-Verbindung mit dem SSTP-Gateway-Server; dies beinhaltet die Authentifizierung der Benutzer-Anmeldeinformationen mittels einer PPP-Authentifizierungsmethode und die Konfiguration von TCP/IP (IPv4 oder IPv6).
9. Der eigentliche TCP/IP-Datenverkehr findet nun über die PPP-Verbindung statt.

Aufbau einer SSTP-Umgebung

Anhand einer Beispielumgebung für den SSTP-VPN-Remotezugriff gehen wir nun auf die beteiligten Komponenten näher ein und betrachten deren Konfiguration im Detail. Der Domain Controller (Windows 2008 R2) beinhaltet neben DNS und DHCP auch Zertifikatsdienste; Letztere sollten in Produktivumgebungen auf einen dedizierten Server (nicht Domain Controller) verlagert werden. Alle Rechner sind Mitglied einer Active Directory-Domäne und mit aktuellen Microsoft-Updates versehen. Die Firewall (Windows 2008 R2) besitzt zwei Netzwerkkarten für die Verbindung ins interne Netz und für die öffentliche Internetanbindung; hier kommt Microsofts TMG 2010 (Threat Management Gateway – Nachfolger des ISA Server 2006) in der Standard-Version unter Windows 2008 R2 zum Einsatz. Das Betriebssystem des SSTP-VPN-Clients ist Windows 7.

Automatische Zertifikatsanforderung

Die Einstellungen für die automatische Zertifikatsanforderung befinden sich innerhalb einer Gruppenrichtlinie unter dem Punkt "Computerkonfiguration / Richtlinien / Windows-Einstellungen / Sicherheitseinstellungen / Richtlinien für öffentliche Schlüssel / Einstellungen der automatischen Zertifikatanforderung"; ein Assistent führt hier durch die weitere Konfiguration.

Die Zertifikatsdienste auf dem Domain Controller sind in Form einer im Active Directory integrierten Unternehmens-Stammzertifizierungsstelle konfiguriert. Durch eine entsprechende Gruppenrichtlinienkonfiguration fordern alle Clients, die Domänenmitglied sind, automatisch Zertifikate bei der Zertifizierungsstelle an. Diese stellt daraufhin diese Zertifikate aus – der Windows 7 Client in der Testumgebung besitzt also bereits ein Computerzertifikat. Weiterhin befindet sich auch das Zertifikat der Zertifizierungsstelle im lokalen Speicher des Clients im Segment der vertrauenswürdigen Stammzertifizierungsstellen. Detaillierte technische Information zu Zertifikatdiensten sind bei Microsoft im Technet-Artikel "Active Directory-Zertifikatsdienste" [2] verfügbar.

Erstellen und Installieren des Firewall-Zertifikats

TMG 2010 nutzt – wie auch der ISA Server 2006 – sogenannte Weblistener zum Empfang und zur Authentifizierung eingehender Webanforderungen. Dabei ist ein Zertifikat erforderlich, das an diesen Weblistener gebunden wird. Grundsätzlich gibt es zwei Möglichkeiten, an ein Zertifikat zu gelangen: Entweder Sie erwerben ein kommerzielles oder Sie bedienen sich eines privaten Zertifikats, das von einer internen vertrauten Zertifizierungsstelle ausgestellt wurde. Eine finale Entscheidung hierüber muss für eine Produktivumgebung neben den reinen Kostenfaktoren auch den gesamten Implementierungs- und Wartungsaufwand der notwendigen Komponenten berücksichtigen. Für unsere Workshop-Umgebung wollen wir ein Zertifikat der internen Active Directory-Zertifizierungsstelle verwenden. Dazu rufen Sie auf dem Firewall-Server die MMC-Konsole auf und fügen das Snap-In für die Zertifikate hinzu (dabei "Computerkonto / lokaler Computer" auswählen). Der nächste Schritt besteht dann in der eigentlichen Erstellung der Zertifikatsanforderung:

1. Rechter Mausklick auf "Eigene Zertifikate", dann "Alle Aufgaben / Neues Zertifikat anfordern …".
2. Wir entscheiden uns für die Webserver-Vorlage und definieren in den not-

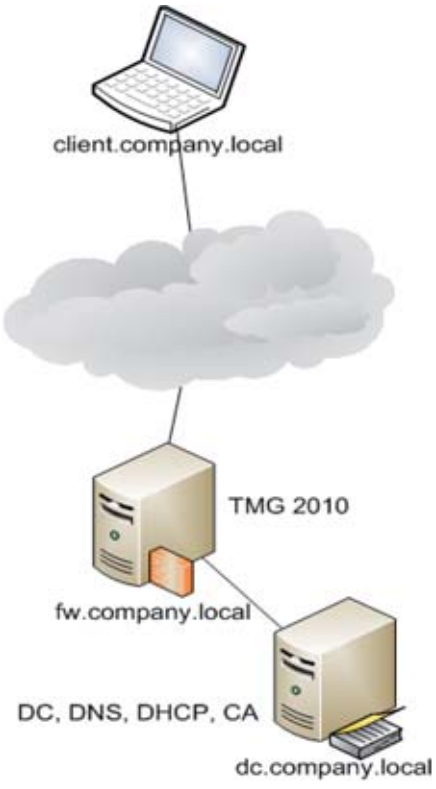


Bild 2: Unsere Beispielumgebung für die SSTP-VPN-Konfiguration

wendigen zusätzlichen Informationen als allgemeinen Namen (common name) den Wert "fw.company.local".
3. Bei erfolgreicher Anforderung wird das Zertifikat automatisch installiert und ist danach im MMC-Zertifikate-Snap-In unter "Zertifikate (Lokaler Computer)/ Eigene Zertifikate" zu finden.

Nebenbei sollten Sie auch sicherstellen, dass sich das Zertifikat der Zertifizierungsstelle unter "Zertifikate (Lokaler Computer) / Vertrauenswürdige Stammzertifizierungsstellen" befindet. Bei Problemen mit der Anforderung des Zertifikats überprüfen Sie zudem die folgenden Punkte:
- Lässt die TMG-Firewall den Netzwerkverkehr zur Zertifizierungsstelle bei der Zertifikatsanforderung überhaupt zu? Ist dies nicht der Fall (Blick in die TMG-Protokollierung bezüglich verweigerter Verbindungen), muss eine entsprechende Zugriffsregel erstellt werden.
- Hat die TMG-Firewall das Recht, Zertifikate zu beantragen? Hierfür sind auf der Zertifizierungsstelle in den Zertifikatvorlagen (rechter Mausklick / Verwalten) die Berechtigungen auf der Webserver-Vorlage zu prüfen; das Active Directory-Computerkonto der TMG-Firewall muss über die Berechtigungen "Lesen" und "Registrieren" verfügen.

Veröffentlichung der Zertifikatssperrliste

Eine Zertifikatssperrliste (Certificate Revocation List, CRL) beinhaltet eine Liste von Zertifikaten, die vor Ablauf ihrer Gültigkeitsdauer aus verschiedenen Gründen zurückgezogen wurden. Diese Liste besitzt dabei eine fest definierte Laufzeit, nach deren Ende eine neue erzeugt wird. Der Sperrlisten-Verteilungspunkt (CRL Distribution Point, CDP) bezeichnet die Orte, die die aktuelle Zertifikatssperrliste bereitstellen; einsehbar ist die Konfiguration dieser Verteilungsorte in den Eigenschaften der Zertifizierungsstelle im Reiter "Erweiterungen". Dabei besteht neben der Bereitstellung im Dateisystem und per LDAP auch die Möglichkeit zur Webveröffentlichung; die Orte des Verteilungspunkts der Zertifikatssperrliste finden sich übrigens auch in jedem ausgestellten Zertifikat wieder (in den Zertifikatseigenschaften unter "Details / Sperrlisten-Verteilungspunkte").

Die Zertifikatssperrliste muss im Übrigen auch aus dem Internet für die Clients abrufbar sein. Falls ein kommerzielles Zertifikat für den Firewall-Server zum Einsatz kommt, entfällt die Notwendigkeit zur Veröffentlichung der Zertifikatssperrliste der internen Zertifizierungsstelle. Die folgenden Arbeitsschritte sind für die Webveröffentlichung auf der TMG-Firewall auszuführen:
1. Zunächst starten Sie in der TMG-Verwaltungskonsole den Assistenten für die Veröffentlichung von Websites (im Aufgabenfeld für die Firewall-Richtlinien) und vergeben einen eindeutigen Namen für die Webveröffentlichungsregel.
2. Die Regelbedingung setzen Sie auf "Zulassen" und als Veröffentlichungstyp wählen Sie "Einzelne Website oder Lastenausgleich veröffentlichen". SSL können Sie nicht verwenden (die Zertifikatssperrliste in Form einer Datei muss ohne vorherige Authentifizierung abrufbar sein).
3. Als internen Sitenamen benutzen Sie den normalen FQDN des Domain Controllers (dc.company.local). Der zu konfigurierende Pfad (Standard: "/CertEnroll/dc+.crl") enthält die Datei mit einem eingefügten "+" vor der Endung.
4. Der öffentliche Sitename ist in unserer Umgebung identisch mit dem internen; im produktiven Umfeld würde hier der öffentlich registrierte DNS-Name zum Einsatz kommen.
5. Für die eingehenden Webanfragen benötigen Sie nun noch einen Weblistener. Hierfür definieren Sie einen dem Zweck entsprechenden Namen, verwenden keine SSL-Verschlüsselung und aktivieren das externe Netzwerk für eintreffenden HTTP-Verkehr. Eine Authentifizierung darf nicht konfiguriert sein.
6. Die Konfiguration der Webveröffentlichungsregel schließen Sie mit der Einstellung für die Authentifizierungsdelegierung ab ("Keine Delegierung, keine direkte Authentifizierung des Clients").

Um den Zugriff auf die Zertifikatssperrliste zu prüfen, öffnen Sie auf dem Windows 7-Client per Internet Explorer die Adresse *http://dc.company.local/CertEnroll/dc.crl*. Daraufhin öffnet sich der bekannte Dialog zum Öffnen beziehungsweise Speichern der Datei, womit der Zugriff von außen verifiziert ist. In diesem Zusammenhang sei noch erwähnt, dass sich die Überprüfung der Zertifikatssperrliste clientseitig per Registry-Eintrag ausschalten lässt.

Dazu müssen Sie mit dem Registry-Editor unter "HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ Sstpsvc \ Parameters" den DWORD-Wert "NoCertRevocationCheck" auf "1" setzen. Aus Sicherheitsaspekten ist dies in einer Produktivumgebung aber nicht zu empfehlen und sollte lediglich im Rahmen der Problembehandlung eingesetzt werden. Legen Sie stattdessen den Ort für den Sperrlisten-Verteilungspunkt auf einen Webserver in der (in unserer Testumgebung nicht existierenden) DMZ. Dieser Ort muss dann zusätzlich in den Eigenschaften des Sperrlisten-Verteilungspunkts auf der Zertifizierungsstelle definiert werden. Weiterführende Angaben zum Sperren von Zertifikaten und Zertifikatssperrlisten (CRLs) finden Sie unter "How Certificate Revocation Works" [3].

VPN-Konfiguration der Firewall

Nun steht noch die eigentliche VPN-Konfiguration der TMG-Firewall aus. Hierfür bedienen wir uns wiederum der TMG-Verwaltungskonsole und konfigurieren den VPN-Zugriff per Aufgabenfeld in der Remotezugriffsrichtlinie:
1. Um die VPN-Clients mit IP-Adressen zu versorgen, ist zunächst die Art der Adresszuweisung zu konfigurieren ("Allgemeine VPN-Konfiguration / Adresszuweisung konfigurieren"). Hier verwenden Sie entweder statisch konfigurierte Adressbereiche auf der Firewall

selbst oder dynamische IP-Adressen vom internen DHCP-Server (auf dem Domain Controller).

2. Anschließend lässt sich im Aufgabenfeld unter "VPN-Clientaufgaben" der VPN-Zugriff durch Klick auf "VPN-Clientzugriff aktivieren" einschalten.
3. Im selben Aufgabenfeld ist jetzt die Konfiguration mit Hilfe des Punkts "VPN-Clientzugriff konfigurieren" anzupassen: im Reiter "Protokolle" ist hierfür die Option "SSTP aktivieren" auszuwählen. Zur Erstellung des benötigten Weblisteners dient der rechts daneben befindliche Button "Listener auswählen …".
4. Erstellen Sie einen neuen Weblistener, vergeben für diesen einen aussagekräftigen Namen und binden ihn an das externe Netzwerk an. Weiterhin ordnen Sie für diesen das zuvor ausgestellte und bereits installierte Zertifikat zu.

Ein Blick in die Systemrichtlinien ("Systemrichtlinienregeln einblenden" in der Aufgabenbox der "Firewall Richtlinie") zur Verifizierung der oben vorgenommenen Konfigurationseinstellungen zeigt Ihnen nun die aktivierte Richtlinie "SSTP-Veröffentlichung".

Client-seitige SSTP-VPN-Verbindung einrichten

Für einen abschließenden Test ist nun noch eine VPN-Verbindung auf dem Windows7-Client einzurichten. Im Netzwerk- und Freigabecenter wählen Sie den Punkt "Neue Verbindung oder neues Netzwerk einrichten" und als Verbindungsoption "Verbindung mit dem Arbeitsplatz herstellen".

Nach Festlegung der Verbindungsart (Einstellung: "Die Internetverbindung (VPN) verwenden") und ohne Einrichtung einer gesonderten Internetverbindung (wir sind in unserer Beispielumgebung per LAN verbunden) muss noch die Internetadresse (hier der DNS-Name, unter dem die TMG-Firewall auf der öffentlichen Seite erreichbar ist) und ein Namen für diese VPN-Verbindung eingegeben werden.

Die Angabe von Benutzername und Kennwort schließen die Verbindungskonfiguration ab. Unter dem Punkt "Adaptereinstellungen ändern" findet sich nun die soeben konfigurierte SSTP-VPN-Verbindung. Es empfiehlt sich, in den Eigenschaften der Verbindung den VPN-Typ von "Automatisch" auf "SSTP" zu ändern (Bild 3).

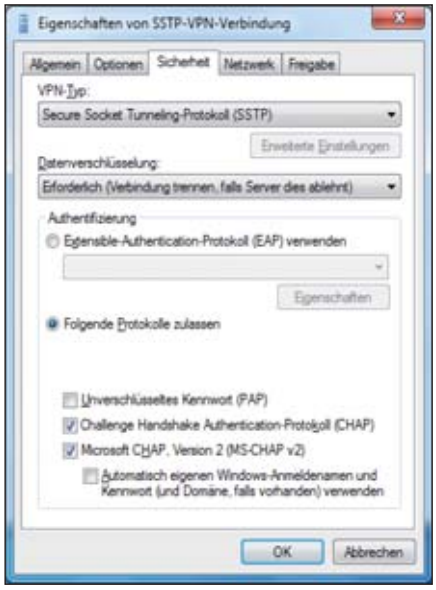


Bild 3: Eigenschaften der SSTP-VPN-Verbindung mit den möglichen Protokollen

Fazit

SSTP stellt eine sinnvolle und sichere Alternative für die Nutzung von VPN-Verbindungen dar. Insbesondere die weitgehende Unabhängigkeit von Port-Beschränkungen am Einsatzort und damit die Fähigkeit zum Verbindungsaufbau über Firewalls, nicht authentifizierende Proxys und NAT-Router hinweg in das interne Firmennetz stellt für Endanwender eine erhebliche technische Vereinfachung dar.

Weiterhin muss keine zusätzliche Software auf Clientseite installiert werden, da SSTP ab Windows Vista (SP1) bereits im Betriebssystem integriert ist; Microsoft stellt aber aktuell leider keinen separaten SSTP-VPN-Client für Windows XP zur Verfügung. Außerdem darf der erforderliche technische Implementierungsaufwand sowohl im Bereich der Firewall als auch der Zertifikatsdienste nicht unterschätzt werden. *(dr)*

Oliver Ebel ist Senior Consultant bei der CenterTools Software GmbH.

Links

[1] VPN-Tunneling-Protokolle
http://technet.microsoft.com/de-de/library/cc771298(WS.10).aspx

[2] Active Directory-Zertifikatsdienste
http://technet.microsoft.com/de-de/library/cc732625.aspx

[3] How Certificate Revocation works
http://technet.microsoft.com/en-us/library/ee619754(WS.10).aspx

Virtuelle Maschinen mit dem Citrix Provisioning Server warten (2)

Updates am laufenden Band

von Christian Knermann

Der erste Teil dieses Workshops führte Sie in die Arbeitsweise des Provisioning Server ein. Nachdem wir das Werkzeug erfolgreich installiert haben, wenden wir uns im zweiten Teil der Workshopserie zunächst der Konfiguration zu. Anschließend zeigen wir auf, wie virtuelle Maschinen Updates erhalten.

Zuletzt hatten wir in unserem Workshopszenario den Citrix Provisioning Server (CPS) auf zwei Hosts installiert. Jetzt wenden wir uns der Konfiguration der vDisk und Target Devices zu.

Konfiguration

Öffnen Sie die Provisioning Services Console (PSC) und legen Sie zunächst einen ersten Store zur Aufnahme unserer vDisks an. Dazu rufen Sie per Rechtsklick auf den Knoten "Stores" die Aktion "Create Store…" auf und erzeugen einen Speicherort namens "PVS-Store", den Sie Ihrer ersten und einzigen Site "Oberhausen" zuordnen. Auf der Registerkarte "Servers" stellen Sie sicher, dass der Store beiden Servern zugeordnet ist. Diese Einstellung ist wichtig für die HA-Konfiguration. Als Voraussetzung ist natürlich zu beachten, dass der Pfad zum Store von beiden Servern gleichermaßen erreichbar ist.

Erzeugen Sie entsprechend auf Ihrem Filer eine CIFS-Freigabe, auf der Sie dem User "ctx_provisioning" und den Domänen-Administratoren Vollzugriff einräumen. Innerhalb dieser Freigabe legen Sie einen Ordner für die vDisks und einen weiteren für den Write Cache an. In dieser Konfiguration sollen sich 25 bis 50 Target Devices betreiben lassen, wobei es sich dabei natürlich um eine recht grobe Abschätzung handelt. Die tatsächliche Zahl wird nicht zuletzt von der Nutzungsart der Maschinen und ihrer Auslastung abhängen. Sollte es zu Engpässen kommen, ließe sich die Performance durch Bereitstellung des Stores via iSCSI oder gar FibreChannel verbessern. Eine weitere Möglichkeit der Optimierung besteht darin, den Cache vom Shared Storage auf die lokale Festplatte oder in den Hauptspeicher der Target Devices zu verlagern. Der Sinn und Zweck des Caches erschließt sich mit einem kleinen Exkurs zu den unterschiedlichen vDisk-Typen:

- Im Modus "Private Image" erlaubt eine vDisk Lese- und Schreibzugriffe, verhält sich also analog zu einer lokalen Partition. Alle Operationen eines Target Devices werden persistent gespeichert, womit die vDisk über die Zeit wächst. Nachteilig daran ist, dass in diesem Modus jede vDisk nur exklusiv von einem Target Device genutzt werden kann. 100 gleichzeitig laufende Targets würden entsprechend 100 Images auf vergleichsweise teurem Speicher im NAS/SAN erfordern.
- Diesen Umstand adressiert das "Standard Image", das zahlreichen Target Devices gleichzeitig lesenden Zugriff erlaubt. Möglich macht dies wiederum der Festplatten-Treiber des CPS, welcher sämtliche Schreibzugriffe in den Cache umleitet. Das jeweilige Target Device kann transparent zugreifen und merkt nichts davon, dass es das Image im Hintergrund tatsächlich nicht beschreiben kann. Wird ein Target Device neu gestartet, so wird der Cache verworfen und der unveränderte Ursprungszustand der vDisk wird erneut geladen. Damit eignet sich dieser Modus insbesondere zur Bereitstellung vieler standardisierter Maschinen wie Desktops oder Terminalserver.
- Einen Mittelweg bietet das "Difference Disk Image", bei dem der Cache zwischen Reboots erhalten bleibt und erst verworfen wird, sobald der Administrator eine neue Version der vDisk bereitstellt. Auswählbar war dieser Punkt bereits seit längerem, doch erst mit Service Pack 1 für den Provisioning Server 5.1 wird die Funktionalität tatsächlich unterstützt.

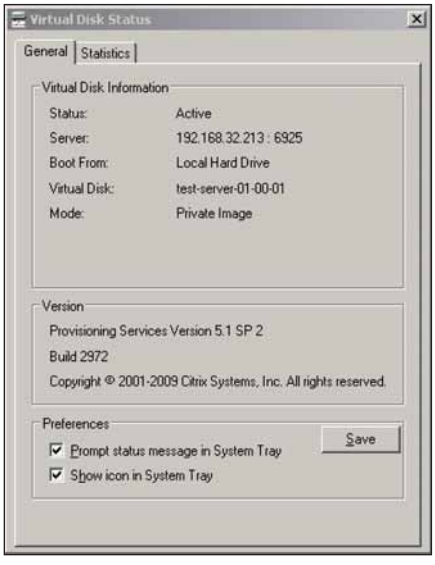


Bild 1: Der "Virtual Disk Status" zeigt, welche vDisk verbunden ist

Dies wirft weitere Fragen auf, die wir im Weiteren beantworten: Wie lassen sich Updates an vDisks im Modus "Standard Image" durchführen? Und wie gelangen viele Maschinen, die aus einem Image booten, an eine eindeutige Identität, insbesondere wenn sie ins Active Directory eingebunden werden sollen?

Betrieb des Provisioning Server

Sehen wir uns zunächst die grundlegende Funktionalität genauer an. Hierzu verwenden Sie eine Gruppe von virtuellen Test-Servern, die von einer gemeinsamen vDisk den Windows Server 2003 R2 starten sollen. Dazu rufen Sie in der PSC per Rechtsklick auf den Ordner "vDisk Pool" die Aufgabe "Create vDisk…" auf. Die vDisk erhält den Namen "test-server-01-00-01" – später mehr zu diesem Namensschema. Die vDisk wird 15 GByte groß und soll dynamisch bis zu dieser Grenze wachsen. In den Eigenschaften der vDisk aktivieren Sie die Option "Use the load balancing algorithm", um startende Target Devices auf beide Provisioning Server zu verteilen und die Ausfallsicherheit zu gewährleisten.

Weiter geht es über die Schaltfläche "Edit File Properties…": Im nachfolgenden Dialog tragen Sie auf der Registerkarte "General" in den Feldern "Class" und "Type" jeweils den String "test-server" ein. Wir kommen später im Rahmen der Updates auf diese Werte zurück. Da die vDisk anfänglich leer ist und noch mit Inhalt befüllt werden will, wählen Sie auf der Registerkarte "Mode" den Modus "Private Image". Unter "Options" aktivieren Sie zudem die "High availability (HA)".

Die vDisk befüllen

Als Quelle für den Inhalt der vDisk kann nun eine beliebige physische oder virtuelle Maschine dienen. Für unser Beispiel installieren wir auf einem der XenServer eine virtuelle Maschine namens "test-server" mit dem Windows Server 2003 R2. Auf Ihrem DHCP-Server erzeugen Sie eine statische Zuordnung für diese Maschine. Anschließend booten Sie die VM und starten die "Target Device Installation" aus dem Umfang des Citrix Provisioning Services 5.1 SP2 Archivs, welche wiederum zunächst die Installation des Tools "XenConvert 2.0.3" initiiert und anschließend das eigentliche Target Device mit dem Festplatten Treiber zum Verbinden von vDisks hinzufügt. Nach der Installation ist ein Neustart erforderlich. Anschließend findet sich im Systemtray ein neues Icon, das den "Virtual Disk Status" anzeigt. Dieser ist aber zunächst noch "Inactive", da auf dem Provisioning Server noch keine vDisk zugeordnet ist.

Sofern es sich bei einem Target Device um die Enterprise Edition des Windows Server handelt, muss Automount manuell aktiviert werden. Das Verbinden von vDisks wird ansonsten fehlschlagen. Um die Option zu aktivieren, starten Sie von der Kommandozeile das Tool "diskpart", welches in den gleichnamigen Prompt wechselt. Die Eingabe von *automount* gibt den aktuellen Status aus. Mit *automount enable* lässt sich die Funktion aktivieren.

Zurück auf dem Provisioning Server rufen Sie in der PSC per Rechtsklick auf die Device Collection "Test-Server" die Aktion "Create Device…" auf und legen ein Objekt für unsere VM an. Die Zuordnung erfolgt an Hand der MAC-Adresse. In den Eigenschaften des Devices ändern Sie auf der Registerkarte "General" die Boot-Quelle zunächst auf "Hard Disk" und ordnen auf der Registerkarte "vDisks" unser zuvor erstelltes Image "test-server-01-00-01" zu. Im XenCenter fahren Sie anschließend die VM herunter, ändern die Boot-Reihenfolge derart, dass sie ausschließlich via Netzwerk bootet, und starten die Maschine anschließend neu.

Die virtuelle Maschine in Betrieb nehmen

Die Maschine bootet nun via Netzwerk und meldet sich per Broadcast mit ihrer MAC-Adresse. Vom DHCP-Server erhält sie wie zuvor ihre IP-Adresse. Da auch dem PXE-Dienst des Provisioning Servers die MAC-Adresse bekannt ist, erhält die Maschine zusätzlich die Anweisung, das Bootstrap-Image *ARDPB32.BIN* über den TFTP-Dienst des Provisioning Servers zu laden. Dieses nimmt wiederum Kontakt zum Streaming Service auf und erfährt, dass die Maschine zum einen den Startvorgang von der lokalen Platte fortsetzen und zum anderen zusätzlich die vDisk verbinden soll. Nach der Anmeldung verkündet entsprechend ein Tooltip im System Tray, dass neue Hardware gefunden wurde und der "Virtual Disk Status" wechselt auf "Active". Der Dialog zeigt zudem, welche vDisk von welchem Provisioning Server verbunden ist. Nun rufen Sie im Startmenü das Tool "XenConvert 2.0" auf. Die gewünschte Aktion, das Klonen der lokalen Maschine in die vDisk, ist bereits per Default ausgewählt. Es können bis zu vier Partitionen transferiert werden. Unsere VM besitzt nur eine, die im Folgenden zu konvertieren ist. Bevor Sie aber damit beginnen, klicken Sie auf die Schaltfläche "Optimize". Der folgende Dialog bietet an, Einstellungen des Betriebssystems auf für den Betrieb als Standard-Image sinnvolle Werte zu ändern. So werden beispielsweise automatische Updates und Memory Dumps deaktiviert, da diese beim Neustart eines Standard-Images ohnehin mitsamt Cache entsorgt würden.

Eine letzte Sicherheitsabfrage weist darauf hin, dass der Inhalt der vDisk überschrieben wird. Bestätigen Sie dies mit "Ja", wird das lokale System übertragen, was je nach Plattenbelegung und Storage-Anbindung eine Weile dauern kann. Weiter geht es anschließend wiederum in der PSC, wo Sie in den Eigenschaften unserer vDisk den Modus auf "Standard Image" ändern und die Option "Enable automatic updates for this vDisk" aktivieren. In den Eigenschaften des Target Devices setzen Sie die Boot-Quelle zurück auf "vDisk".

Starten Sie nun die VM neu, wiederholt sich der zuvor beschriebene Boot-Prozess. Das System wird nun aber vom Streaming Service angewiesen, direkt von der vDisk zu starten. Eine lokale Platte ist dazu nicht

mehr erforderlich. Der Provisioning Server kümmert sich nun auch um die Identität des Target Devices. Melden Sie sich an der VM an, so sehen Sie, dass der Computername automatisch mit "test-server" überschrieben wurde, obwohl Sie dies zuvor nicht manuell eingetragen hatten. Entsprechend können Sie nun beliebig weitere VM ohne eigene Festplatte auf dem XenServer anlegen, im DHCP eintragen und passende Target-Devices dazu erzeugen. Weisen Sie diesen Targets ebenfalls unsere vDisk zu, so booten alle Systeme von ein und demselben Image. Alle Änderungen, die Sie an einer der laufenden VM vornehmen, gehen mit dem nächsten Neustart verloren, da es sich um ein Standard-Image handelt. Dies führt uns zurück zur ursprünglichen Frage: Wie lassen sich gewollte Änderungen, wie die Installation weiterer Updates oder Applikationen, vornehmen und persistent speichern?

vDisk Updates

Wir wollen nun ein Update durchführen, ohne dabei den laufenden Betrieb der aus der vDisk erzeugten Systeme zu unterbrechen. Dazu verbinden Sie sich als Benutzer "ctx_provisioning" von einem beliebigen Client aus mit dem vDisk Store. Dort erstellen Sie Kopien der Dateien *test-server-01-00-01.pvp* und *test-server-01-00-01.vhd*. Die Kopien benennen Sie dabei "test-server-01-01-01.*". Weiter geht es wiederum in der PSC, wo Sie mit einem Rechtsklick auf den vDisk Store die Aufgabe "Add Existing vDisks…" aufrufen. Im entsprechenden Dialog fördert die Schaltfläche "Search" sämtliche noch nicht bekannten vDisks zu Tage. Über die Schaltfläche "Add" fügen Sie die neue vDisk dem Store hinzu. Sie ändern anschließend in den Eigenschaften den Modus dieser vDisk auf "Private Image". Nach dem bereits bekannten Prozedere erstellen Sie dann eine weitere festplattenlose VM und ein passendes Target Device namens "update-server", dem Sie die neue vDisk zuordnen.

Jetzt können Sie den Update-Server booten und beliebige Änderungen an dem System vornehmen, weitere Dienste und Applikationen installieren oder einfach Hintergrundbild und Desktop-Theme des Administrators ändern. Dann fahren Sie den Update-Server wieder herunter und setzen den Modus der vDisk zurück auf "Standard Image". Die Änderungen sind damit dauerhaft in der vDisk gespeichert. Nun kommt der Update-Mechanismus des Provisioning Servers ins Spiel. Bereits beim Erstellen der vDisk hatten Sie in deren Eigenschaften die Felder "Class" und "Type" belegt. Über Letzteres werden vDisks einander zugeordnet. Dies bedeutet konkret, dass im Kontext des Provisioning Servers mehrere vDisks mit identischen Type-Einträgen logisch verknüpft werden und zwar unabhängig vom Dateinamen. Über das Feld "Class" werden die vDisks dann mit Target Devices verknüpft. Entsprechend setzen Sie in den Eigenschaften unserer Targets das Class-Attribut ebenfalls auf "test-server".

Alle Target Devices mit diesem Eintrag sind nunmehr logisch mit allen vDisks mit identischem Eintrag im Class-Feld verbunden. Nun öffnen Sie die Eigenschaften der vDisk "test-server-01-01-01" und erhöhen auf der Registerkarte "Identification" die Minor-Nummer von "0" auf "1". Damit erklärt sich das anfänglich gewählte Schema der Datei-Namen, die in unserem Beispiel die Major-, Minor- und Build-Nummern widerspiegeln. Es handelt sich hierbei lediglich um eine Empfehlung, damit die Übersicht im Dateisystem nicht verloren geht. Selbst wenn mehrere vDisks vollkommen unterschiedliche Namen tragen, funktioniert die Zuordnung, solange die Type-Attribute übereinstimmen. Zu guter Letzt bleibt nur noch, auf allen Provisioning Servern per Rechtsklick die Aktion "Check for Updates\Automatic…" auszuführen, um die neue vDisks-Version bekannt zu geben. Sobald die Target Devices neu gestartet werden, wechseln sie automatisch zur vDisk mit der höchsten Versionsnummer und starten von dieser. Im dritten Teil unseres Workshops wenden wir uns der Integration ins Active Directory zu und betrachten ausführlich die Bereitstellung von Terminal Servern. *(jp)*

Christian Knermann ist stellvertretender Leiter des IT-Managements am Fraunhofer Institut für Umwelt-, Sicherheits- und Energietechnik UMSICHT in Oberhausen. Zugleich leitet er das Projekt "Competence Center Application Service Providing" der Fraunhofer Gesellschaft.

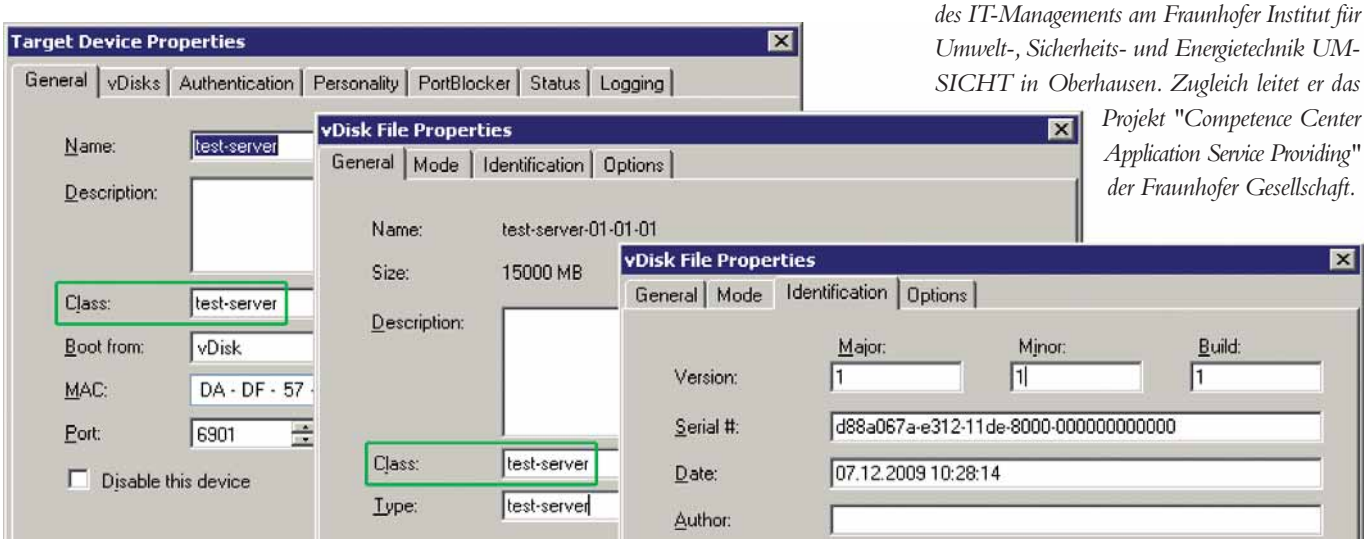


Bild 2: Das Class-Attribut verbindet Target Devices und vDisks. Von mehreren vDisks eines Typs wird die höchste Versionsnummer geladen

Unter Exchange E-Mails mit unbekanntem Empfänger verwalten

Postfach für Mr. Nobody

von Thomas Joos

Sobald eine E-Mail bei einem Exchange-Server eingeht und deren Empfänger im Active Directory nicht bekannt ist, blockiert der Empfängerfilter diese E-Mail. Es ist jedoch möglich mit dem kleinen Zusatztool "CatchAll Agent" den Empfängerfilter so zu konfigurieren, dass bestimmte E-Mails entweder an ein spezifisches Postfach oder an einen öffentlichen Ordner zugestellt werden. In diesem Workshop erklären wir Ihnen, wie Exchange normalerweise mit unbekannten Adressaten verfährt und erläutern die Verwendung des CatchAll Agent.

Quelle: Georgios Kollidas - Fotolia.com

Der CatchAll Agent ist ein so genannter Transport-Agent, der E-Mails überprüft und Aktionen durchführt. Auch die Antispam-Agenten sind solche Transport-Agenten, weswegen wir zuerst darauf eingehen, wie sich ein derartiger Antispam-Agent integriert. Üblicherweise installieren Sie den Spamschutz auf einem Edge-Transport-Server und verwalten dort dessen Einstellungen. Sie finden die Spam-Agenten auf der Registerkarte "Antispam", wenn Sie auf dem Edge-Transport-Server in der Exchange-Verwaltungskonsole auf "Edge-Transport" klicken. Microsoft empfiehlt ausdrücklich den Einsatz eines Edge-Transport-Servers für die Verbindung einer Exchange-Organisation zum Internet. Setzen Sie keinen Edge-Transport-Server ein, können Sie die Antispam-Filter auch auf einem Hub-Transport-Server einrichten. Starten Sie dazu die Exchange-Verwaltungsshell und wechseln Sie in das Unterverzeichnis "Scripts" der Exchange Server 2007-Installation auf Ihrem Server. Dieses Verzeichnis befindet sich im Exchange-Installationsverzeichnis. Geben Sie hier den Befehl *Install-AntispamAgents* ein. Im Anschluss bestätigen Sie die erfolgreiche Installation der Agenten. Danach starten Sie den System-Dienst "Microsoft Exchange-Transport" neu. Nach der Einrichtung der Spam-Agenten finden Sie die neue Registerkarte "Antispam", wenn Sie in der Exchange-Verwaltungskonsole auf "Organisationskonfiguration / Hub-Transport" klicken.

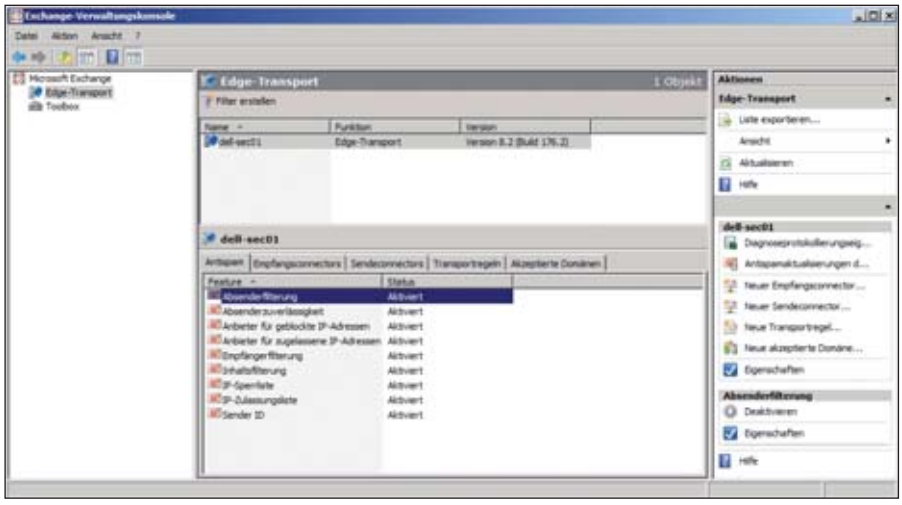


Bild 1: Über die Exchange-Verwaltungskonsole lassen sich auf einem Edge-Transport-Server die Antispam-Einstellungen verwalten

Empfängerfilterung verhindert Zustellung

Viele Spam-Versender verschicken E-Mails, bei denen die Empfänger-Adressen nicht existieren, die E-Mail-Domäne jedoch schon. Dies bewirkt, dass Administratoren im Unternehmen zahlreiche E-Mails erhalten, die nicht zugestellt werden können, aber dennoch gesichtet werden müssen, um normale E-Mails, bei denen ein Schreibfehler vorliegt, von Spam-E-Mails zu unterscheiden. Eine Option zur Bekämpfung von Spam ist daher die Empfängerfilterung. Mit Hilfe dieses Filters lassen sich E-Mails, die an bestimmte Empfänger innerhalb des Unternehmens geschickt werden, blockieren. Hauptsächlich kommt der Filter aber dann zum Einsatz, wenn es um das Blo-

cken von E-Mails geht, für die es im Unternehmen gar keinen Empfänger gibt. Unter Exchange Server 2007 ist daher in den Eigenschaften des Filters auf der Registerkarte "Geblockte Empfänger" die Option "Nachrichten, die an Empfänger gesendet werden, die nicht in der globalen Adressliste stehen, blocken" im Regelfall aktiviert. So sind Sie vor Spam-E-Mails verschont, die ungezielt ins Blaue gerichtet sind. Absender, die versehentlich die falsche Adresse verwendet haben, erhalten einen Bericht über die Nichtzustellbarkeit (NDR) und können die E-Mail erneut versenden.

CatchAll Agent leitet unklare Mails weiter

Alternativ können Sie einen Exchange-Server so konfigurieren, dass dieser E-Mails an unbekannte Empfänger entgegennimmt und weiterleitet. Gehen Sie dazu folgendermaßen vor:

1. Laden Sie sich CatchAll Agent [1] herunter. Sie benötigen nicht die Quelldateien, sondern nur den Agenten selbst. Dies sind die Dateien *CatchAll Agent.dll* und *config.xml*.
2. Kopieren Sie die Dateien in ein Verzeichnis auf dem Edge- oder Hub-Transport-Server, zum Beispiel "C:\Programme\CatchAll Agent".
3. Öffnen Sie anschließend die Datei *config.xml* mit einem Editor.
4. Die Datei enthält eine Beispielkonfiguration für Ihre Domäne nach der Art:
```
<config>
<domain name="domain1.com"
address="catchall@domain1.com" />
<domain name="domain2.com"
address="admin@domain2.com" />
</config>
```
5. Der Wert bei "domain name=" legt fest, welche DNS-Domäne der Agent behandeln soll, also Ihre E-Mail-Domäne, zum Beispiel *contoso.com*. Der Wert bei "address" bestimmt, wie der Agent den Empfänger von unbekannten E-Mails umändern soll. Hier tragen Sie dann die Adresse ein, zu der unbekannte Mails gesendet werden sollen, zum Beispiel "spam@contoso.com". Haben Sie den Agenten einmal eingerichtet, können Sie in dieser XML-Datei beliebig weitere Eintragungen vornehmen. Die Einstellungen sind sofort aktiv, ohne dass Sie Dienste neu starten müssen. Fehler in der XML-Datei ignoriert Exchange einfach. Bearbeiten Sie die Datei mit der Domäne und dem Empfänger. Alle anderen E-Mail-Domänen, die Sie nicht in der Konfigurationsdatei hinterlegen, blockiert der Empfängerfilter weiterhin.
6. Anschließend öffnen Sie auf dem Edge- oder Hub-Transport-Server eine Exchange-Verwaltungsshell. Sie müssen den Agenten nach dem Download in Exchange integrieren und starten. Zum Installieren geben Sie in der Verwaltungsshell den Befehl
```
install-transportagent -Name
 "CatchAll Agent" -Transport
 AgentFactory:CatchAll.CatchAll
 Factory -AssemblyPath:"C:\
 Program Files (x86)\CatchAll
 Agent\CatchAllAgent.dll"
```
ein. Achten Sie auf den korrekten Pfad zur Datei.
7. Mit dem Befehl *get-transportagent* lassen Sie sich alle installierten Transport-Agenten anzeigen. Dies sind die installierten Spamagenten von Exchange Server 2007 und der neu installierte CatchAll Agent. Dieser wird allerdings noch als "nicht gestartet" angezeigt und ist die Priorität betreffend ganz zuletzt angeordnet, wird also als letzter Agent und Filter ausgeführt.
8. Der Empfängerfilter (Recipient Filter Agent) hat die Priorität 7, wird also vorher verwendet. Damit Exchange den CatchAll Agent verwendet, müssen Sie diesen von der Priorität her vor den Empfängerfilter setzen. Dazu verwenden Sie den Befehl *set-transportagent "CatchAll Agent" -Priority:7*. Überprüfen Sie nun wieder mit *get-transportagent*, dass der Agent ordnungsgemäß vor dem Empfängerfilter angesetzt ist.
9. Im nächsten Schritt aktivieren Sie den Agenten mit dem Befehl *enable-transportagent "CatchAll Agent"*. Auch diesen Vorgang kontrollieren Sie wieder mit *get-transportagent*.
10. Anschließend müssen Sie noch den Systemdienst "MSExchangeTransport" neu starten, verwenden Sie dazu die beiden Befehle:
```
net stop MSExchangeTransport
net start MSExchangeTransport
```

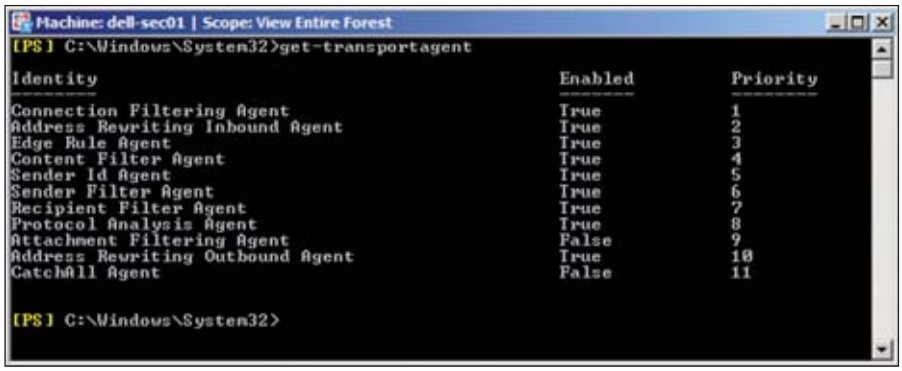


Bild 2: Mit dem Kommando *get-transportagent* zeigen Sie die installierten Transport-Agenten von Exchange und deren Priorität an

Benachrichtigungen an öffentliche Ordner

Neben der Möglichkeit, Nachrichten an Administratoren zu senden, können Sie diese auch an öffentliche Ordner übermitteln. Dazu legen Sie einen entsprechenden öffentlichen Ordner an und aktivieren diesen für den E-Mail-Empfang. Über den Befehl *enable-mailpublicfolder* können Sie einen öffentlichen Ordner mit E-Mail aktivieren, mit dem Befehl *disable-mailpublicfolder* heben Sie die

E-Mail-Erreichbarkeit wieder auf. Dem öffentlichen Ordner wird, genau wie Ihren Benutzern, eine E-Mail-Adresse durch die E-Mail-Adressenrichtlinien zugeteilt. Sie können die E-Mail-Aktivierung eines öffentlichen Ordners widerrufen. Die E-Mail-Adresse des öffentlichen Ordners wird gelöscht und sein Eintrag aus den Adresslisten entfernt. Benutzer können weiterhin Nachrichten im öffentlichen Ordner mit Outlook oder einem anderen Client bereitstellen, der Ordner ist aber nicht mehr per E-Mail direkt erreichbar. Daten gehen bei der E-Mail-Deaktivierung nicht verloren.

Standardmäßig darf jeder Benutzer E-Mails an diesen öffentlichen Ordner senden. Wollen Sie, dass ein öffentlicher Ordner E-Mails aus dem Internet erhalten soll, müssen Sie ihn zunächst für E-Mails aktivieren und Benutzern anonymen Zugriff gestatten. Entziehen Sie einem öffentlichen Ordner die Berechtigung, von anonymen Benutzern E-Mails zu empfangen, ist dieser Ordner nicht per E-Mail über das Internet erreichbar. E-Mail-Absender, die über das Internet E-Mails an Ihre Exchange-Organisation schicken, sind immer anonym. Die Syntax des Befehls lautet:

```
enable-MailPublicFolder -Identity {PublicFolderIdParame-
  ter} [-Confirm [{SwitchParameter}]] [-DomainController
  {FFQDN}] [-HiddenFromAddressListsEnabled {$true |
  $false}] [-Server {ServerIdParameter}] [-WhatIf
  [{SwitchParameter}]]
```

Verwenden Sie den Parameter "HiddenFromAddressListsEnabled", wenn Sie den Ordner in der Adressliste ausblenden wollen. Alternativ können Sie auch die neue Öffentliche Ordner-Verwaltungskonsole im Bereich "Toolbox" der Exchange-Verwaltungskonsole verwenden. Klicken Sie dazu im linken Bereich auf "Öffentliche Standardordner" und im Ergebnisbereich auf den Ordner, für den Sie E-Mail aktivieren wollen. Wählen Sie im Aktionsbereich "E-Mail aktivieren". Über den gleichen Weg deaktivieren Sie die E-Mail-Adresse auch wieder.

Normalerweise erhalten Öffentliche Ordner die E-Mail-Adresse {Name des Ordners}@{Ihre E-Mail-Domäne}. Sie können die Adresse in der Öffentliche Ordner-Verwaltungskonsole in der Exchange-Verwaltungskonsole überprüfen, die Sie in der Toolbox finden. Klicken Sie auf den Ordner und rufen Sie im Ergebnisbereich dessen Eigenschaften auf. Auf der Registerkarte "E-Mail-Adressen" sehen Sie die E-Mail-Adresse des Ordners. *(ln)*

Links

[1] CatchAll Agent
www.codeplex.com/catchallagent/Release/ProjectReleases.aspx?ReleaseId=8668

Microsoft Forefront Unified Access Gateway 2010

Festung Unternehmensnetz

von Marc Grote

Quelle: Pixelio.de

Microsoft schickt mit dem Forefront Unified Access Gateway 2010 (UAG) den Nachfolger des Intelligent Application Gateway (IAG) 2007 als sogenannte Unified Access Gateway-Lösung ins Rennen. Das Werkzeug stellt eine breite Palette von Remote-Zugriffslösungen zur Verfügung, mit deren Hilfe sowohl Firmenmitarbeiter als auch Partner und Lieferanten über eine Vielzahl von Endgeräten eine sichere Remote-Verbindung aufbauen. Die Endgeräte sind dabei nicht auf Windows-Rechner beschränkt, auch diverse Unix-Derivate und Apple Macintosh-Rechner können sicher angebunden werden, auch wenn diese Endgeräte nicht zentral durch die IT-Abteilung verwaltet werden. Dieser Beitrag erläutert, wie UAG über Trunks, Authentifizierung und DirectAccess den Fernzugriff auf veröffentlichte Applikationen absichert.

Forefront Unified Access Gateway 2010 (UAG) [1-3] erweitert die bereits mit dem Microsoft Intelligent Application Gateway 2007 zur Verfügung gestellten Remote Access-Möglichkeiten in Form von SSL-VPN und DirectAccess. Letzteres führte Microsoft mit Windows Server 2008 R2 ein und erlaubt einen transparenten Zugriff von Remote-Clients auf das interne Firmennetzwerk. Desweiteren stellt UAG eine Reihe von Konfigurationsmöglichkeiten zur Verfügung und steuert die Zugriffe mit Hilfe von Richtlinien zentral.

Die Schlüsselfunktionen von Microsoft Forefront UAG sind:

- Remote Zugriff (traditioneller und SSL-VPN)
- Anwendungsintelligenz
- Sicherheits- und Zugriffskontrolle
- Terminal Server-Veröffentlichung und Remote Apps-Zugriff
- Frontend- und Backend-Authentifizierung

Sichere Veröffentlichung von Applikationen

UAG integriert sich sehr stark in die veröffentlichten Anwendungen und ermöglicht es IT-Verantwortlichen mit seiner "Application Intelligence", eine Vielzahl von Anpassungen bei der Veröffentlichung vorzunehmen. Dies erhöht die Sicherheit und gibt dem Administrator mehr Flexibilität, Anwendungen für den Benutzer und auf die Firmenbedürfnisse anzupassen. Forefront UAG unterstützt eine Vielzahl von Authentifizierungsanbietern zur sicheren Authentifizierung von externen Benutzern und bietet eine granulare Zugriffssteuerung bis in tiefe Ebenen der Anwendung.

Forefront UAG agiert dabei als zentrales Sicherheitsgateway für eine Vielzahl von unterschiedlichen Endgeräten und Benutzern und stellt diesen über ein zentrales Portal alle notwendigen Informationen für Webanwendungen, Nicht-Webanwendungen und VPN-Zugangstechnologien zur Verfügung. UAG ist optimiert für die Veröffentlichung von Microsoft-Anwendungen wie zum Beispiel:

- Microsoft Sharepoint
- Microsoft Exchange Server
- Remote Desktop Services
- Microsoft Dynamics CRM

Für diese und weitere Produkte stellt Forefront UAG sogenannte "Application Optimizer" zur Verfügung. Diese Module enthalten die optimalen Sicherheits-, Performance- und Systemeinstellungen für die veröffentlichte Anwendung, aber auch notwendige Einstellungen, Prüfungen und Anforderungen von der Client-Seite.

Nutzer können folgende Anwendungen über Forefront UAG veröffentlichen:

- Webanwendungen mit Reverse Proxy
- Webfarmen mit Reverse Proxy
- Remote Desktop Service RemoteApps

Differenzierung zu Microsoft Forefront TMG

Microsoft Forefront TMG wird von UAG für die Standard-Firewallfunktionalitäten wie die Einhaltung des Firewallregelwerks, Malware-Inspection, Webfilterung, Intrusion Prevention System (IPS) und Network Inspection System (NIS) verwendet. Forefront UAG erweitert die Basis-Funktionalitäten der Firewall, speichert aber seine Konfiguration in dem standardmäßigen Konfigurationsspeicher. Die meisten Änderungen sollten Administratoren über die UAG-Verwaltungskonsole vornehmen.

durch ein Forefront UAG-Portal mit integriertem Remote Desktop Services Gateway
- Veröffentlichung von Nicht-Webanwendungen über eine Secure Socket-Verbindung
- VPN-Zugriff: VPN-Zugriffe lassen sich mit der in UAG integrierten Network Access Protection (NAP) durch einen lokalen Network Policy Server (NPS) oder durch einen zentralen NPS-Server schützen.

Authentifizierung und Hochverfügbarkeit

Benutzerzugriffe können durch eine Vielzahl von Verzeichnisdiensten in Forefront UAG authentifiziert werden. Dazu zählen unter anderem Active Directory, Netscape LDAP-Server, Notes Directory, Novell Directory, RADIUS, TACAS und RSA SecurID. Für eine Vielzahl der Veröffentlichungen wird auch ein Single Sign-On (SSO) unterstützt.

Forefront UAG stellt integrierte Netzwerklastenausgleichsfunktionen (Network Load Balancing, NLB) mit Hilfe des in Windows Server 2008 R2 integrierten NLB zur Verfügung, um ein UAG-Array hochverfügbar und skalierbar zu machen. Bis zu acht UAG-Server können in einem Array zusammengefasst werden. Die Konfiguration des Netzwerklastenausgleichs erfolgt in der UAG-Verwaltungskonsole. In der Konsole vorgenommene NLB-Einstellungen werden auf dem vom Windows-Betriebssystem zur Verfügung gestellten Netzwerklastenausgleich vorgenommen. Darüber hinaus stellt UAG eine Vielzahl von Protokollierungsmöglichkeiten zur Verfügung, welche von RADIUS, einer eingebauten Reporting-Funktion, Microsoft SQL-Server-Protokollierung bis hin zur Integration in den Microsoft System Center Operation Manager (SCOM) in Form von Management Packs reichen.

Installation erfordert Forefront TMG

Zum Beginn der Installation von UAG müssen als Erstes die Hardware- und Softwareanforderungen geprüft und die Deployment Checkliste [4] abgearbeitet werden. Zunächst installiert das System die notwendigen Voraussetzungen für Forefront UAG. Der anschließende Installationsprozess spielt Forefront TMG auf das System auf, welches die Basis-Firewallfunktionen zur Verfügung stellt und als Unterbau für das darauf zu installierende UAG dient. Wird Microsoft Forefront UAG deinstalliert, wird auch das darunterliegende Forefront TMG deinstalliert. Eine manuelle Installation/Deinstallation von Forefront TMG wird nicht unterstützt. Nachdem TMG installiert wurde, wird das eigentliche UAG aufgespielt. Der UAG-Installationsassistent stellt eine Reihe von Fragen und installiert dann die Software nach Vorgaben des Administrators.

Wie bei Forefront TMG startet nach der erfolgreichen Installation von UAG der "Getting Started Wizard", welcher die Konfiguration der Netzwerkeinstellungen, Server-Topologie und den Download von Microsoft Updates unterstützt. Die Konfiguration der Netzwerkeinstellungen fragt die verwendeten Netzwerkadapter ab und Administratoren müssen festlegen, welcher Netzwerkadapter für die interne und externe Verwendung eingerichtet werden soll.

Fehlersuche mit dem Activation Monitor

Forefront UAG stellt nun ein als "Activation Monitor" bezeichnetes Programm zur Verfügung, welches Administratoren bei der Überwachung der Konfigurations-Aktivitäten in einem UAG-Array hilft. Mit diesem Programm lässt sich zudem der Status der UAG-Server überwachen. Der Gateway Activation Monitor bietet einen reinen Lesezugriff und stellt Administratoren eine Informationsquelle zur Verfügung, um bei etwaigen Konfigurationsproblemen zu sehen, wo bei der Fehlersuche anzusetzen ist.

Kommt es beispielsweise bei der Veröffentlichung des Outlook Web Access Trunks zu Problemen, da der öffentliche Name nicht mit dem Common Name (CN) des auf dem UAG-Server liegenden Zertifikats übereinstimmt, zeigt der Activation Manager dieses in den Konfigurations-Aktivitäten an.

Trunks über die Verwaltungskonsole einrichten

Mit Hilfe der UAG-Verwaltungskonsole nehmen Sie allgemeine Einstellungen wie Authentifizierungsserver, Netzwerklastenausgleich (NLB), SSL-Protokolleinstellungen und eine Vielzahl weiterer Settings vor. Die Einrichtung von automatischen Datensicherungen ist an dieser Stelle ebenso möglich wie das erneute Ausführen des Getting Started Wizard und der Netzwerkkonfiguration.

Die Konsole erlaubt zudem die Einrichtung von sogenannten "Trunks" zur Veröffentlichung von HTTP- und HTTPS-Webportalen und -Applikationen für Windows- und Nicht-Windows-Endgeräte, wie Mac OS und Linux, sowie mobile Geräte über das Internet. Die UAG-Konsole ist in drei Knoten aufgeteilt: HTTP-Verbindung, HTTPS-Verbindung und DirectAccess.

Die Einrichtung der Trunks erfolgt mit Hilfe eines UAG-Assistenten, welcher die notwendigen Konfigurationsschritte abfragt und die Einstellungen durchführt. Eine nachträgliche Anpassung der erstellten Konfiguration ist möglich und in den meisten Fäl-

Bild 1: Zugriff auf wichtige Konfigurationsmöglichkeiten über die Verwaltungskonsole

len notwendig, da nur so die erweiterten Einstellungen konfiguriert werden können.

Als Beispiel für diesen Artikel erstellten wir ein Portal Trunk für die Veröffentlichung von Microsoft Exchange Server 2010 Outlook Web App (Outlook Web App ist der Nachfolger von Outlook Web Access in Exchange Server 2007). Der Assistent ermöglicht die einfache Erstellung der notwendigen Konfigurationsoptionen für die Portal-Veröffentlichung, welche weit über die Funktionen der Outlook Web App-Veröffentlichungen von Forefront TMG hinausgehen. Nach der Erstellung des neuen Trunks lassen sich die Einstellungen modifizieren und eine Vielzahl von zusätzlichen Einstellungen vornehmen.

Auf der Registerkarte "General" werden allgemeine Portal-Einstellungen, der Hostname, die IP-Adresse und der verwendete HTTPS-Port angezeigt. Durch einen Klick auf die Schaltfläche "Configure" in den Trunk-Konfigurationseinstellungen wird die wirkliche Leistungsfähigkeit von UAG ersichtlich. Die Einstellmöglichkeiten, welche sich dem Administrator hier bieten, gehen weit über die Möglichkeiten von Forefront TMG hinaus. Hier ist es beispielsweise möglich, die maximale Anzahl gleichzeitiger Verbindungen zu dem Outlook Web App-Server zu konfigurieren.

Links

[1] Microsoft Forefront UAG
www.microsoft.com/forefront/unified-access-gateway/en/us/

[2] Microsoft Forefront UAG supported configurations with TMG
http://technet.microsoft.com/en-us/library/ee522953.aspx#BKMK_SupportedConfig

[3] Support Boundaries
http://technet.microsoft.com/en-us/library/ee522953.aspx

[4] Microsoft Forefront UAG – FAQ
www.microsoft.com/forefront/prodinfo/roadmap/uag-faq.mspx

[5] Forefront UAG DirectAccess prerequisites
http://technet.microsoft.com/en-us/library/dd857262.aspx

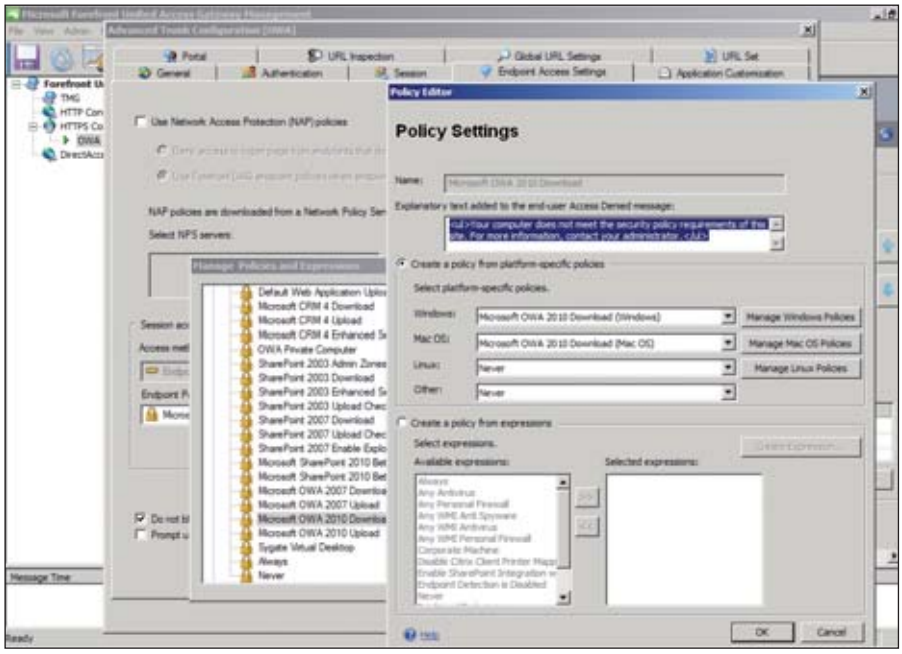


Bild 2: Erstellung einer Zugriffsregel inklusive einer Nachricht an User, denen der Zugriff verweigert wird

Forefront UAG stellt auch vielseitige Möglichkeiten zur URL-Überprüfung und URL-Satzkonfiguration zur Verfügung, mit deren Hilfe sich detailliert legen lässt, welche URLs erlaubt und welche für die Veröffentlichungsregel verweigert werden. Auf der Registerkarte "Endpoint Access Settings" kann die Verwendung von NPS (Network Policy Server) aktiviert und aus einer Vielzahl von Endpoint Policies die entsprechende Richtlinie für Outlook Web App ausgewählt werden. Eine Endpoint Policy beinhaltet tiefgreifende Möglichkeiten zur Filterung des Datenverkehrs der Anwendung. Microsoft spricht von der "Application Intelligence", mit deren Hilfe sich der Zugriff auf die veröffentlichte Anwendung im Detail steuern lässt.

Über der Registerkarte "Application Customization" konfigurieren Sie die Portalfunktionen und -Eigenschaften für die Endbenutzer. Mit dieser Funktion steuern Sie detailliert, welche Voraussetzung ein Client erfüllen muss, um über Forefront UAG eine Verbindung zu den veröffentlichten Servern herzustellen. Administratoren können aus einer Fülle von vordefinierten Richtlinien der Verbindungseinstellungen auswählen. Bei dem Verbindungsaufbau des Clients mit der veröffentlichten Anwendung prüft UAG die Client-Verbindung gegen die Richtlinien und erlaubt oder verweigert den Zugriff.

Auf der Registerkarte "Global URL Settings" kann eine erweiterte Link Adress Translation durchgeführt werden. Dabei handelt es sich um eine Funktion, mit deren Hilfe die intern verwendete URL für die veröffentlichte Applikation durch eine externe URL ersetzt wird, unter deren Namen die veröffentlichte Anwendung im Internet erreichbar ist. Mit Hilfe dieser Funktion ist es möglich, dass die internen Applikationen nicht angepasst werden müssen und beim Aufruf der Anwendung aus dem Internet keine Links auf interne Servernamen verweisen, welche nicht über das Internet erreichbar wären. Die Link Address Translation ist wesentlich umfangreicher und granularer konfigurierbar als über Forefront TMG, wo nur Basisfunktionalitäten zur Verfügung gestellt werden.

Nachdem die Einstellungen und Änderungen am Portal Trunk vorgenommen wurden, werden alle von UAG durchgeführten Änderungen in dem zentra-

len Konfigurationsspeicher gespeichert. Administratoren können die durchgeführten Änderungen im Activation Monitor nachvollziehen. Nach der Erstellung des neuen Portals durch UAG werden entsprechende Zugriffsregeln in Forefront TMG erstellt. Sie können die von UAG erstellten Zugriffsregeln mit Hilfe der Forefront TMG-Verwaltungskonsole einsehen. Von Forefront UAG erstellte Zugriffsregeln sollten nicht mit der Forefront TMG-Verwaltungskonsole geändert werden, sondern nur durch die Forefront UAG-Konsole.

DirectAccess und Web Monitor

Der DirectAccess-Knoten dient zur Erstellung von DirectAccess-Verbindungen von Windows Server 2008 R2. Forefront UAG erweitert die von Windows Server 2008 R2 zur Verfügung gestellten DirectAccess-Funktionen [5] um die Unterstützung von alten Anwendungen und den Zugriff auf Ressourcen in bestehenden Infrastrukturen. Zudem unterstützt es zusätzlich ältere Windows-Clients (Windows XP und Windows Vista), welche nicht DirectAccess-fähig sind, sowie Nicht-Windows-Clients durch integrierte SSL-VPN-Funktionalitäten.

Die Forefront UAG DirectAccess-Verwaltung ähnelt stark der DirectAccess-Verwaltungskonsole in Windows Server 2008 R2 und soll Administratoren die Einrichtung einer DirectAccess-Infrastruktur erleichtern. Administratoren, die bereits DirectAccess in Windows Server 2008 R2 eingerichtet haben, sollten mit der Grundkonfiguration von DirectAccess in UAG keine Probleme haben.

Der UAG Web Monitor erlaubt die Anzeige von UAG-spezifischen Ereignissen mit Hilfe eines Webbrowsers. Der Zugriff ist sowohl aus dem internen Netzwerk und mit etwas Konfiguration auch aus einem externen Netzwerk möglich und bietet Administratoren die Möglichkeit, Überwachung und Reporting-Informationen über die Verwendung von Forefront UAG von jedem beliebigen Ort einzusehen.

Fazit

Microsoft Forefront UAG stellt eine Reihe von sinnvollen Neuerungen gegenüber dem Micosoft Intelligent Application Gateway (IAG) zur Verfügung. Microsoft hat es verstanden, den vielen Kundenwünschen und Anforderungen gerecht zu werden und ist nun in der Lage, auch die aktuellen Microsoft-Serverprodukte sicher zu veröffentlichen. Eine der Stärken von UAG sind die vielseitigen Authentifizierungsmöglichkeiten und die Unterstützung des sicheren Zugriffs über UAG-Portale auch für Nicht-Microsoft-Betriebssysteme sowie die Integration und Erweiterungen der neuen DirectAccess Funktionen von Windows Server 2008 R2. *(jp)*

Marc Grote ist MVP für Forefront. Sie finden seinen Blog unter www.it-training-grote.de/blog.

Tipps zur PowerShell 2

Tuning mit dem Power-Paket

von Rolf Masuch

Das PowerShell Pack enthält zehn neue Module zur Erweiterung des Funktionsumfangs der PowerShell v2. Ob es sich um Skripte zur Erzeugung von Benutzeroberflächen oder zum automatisierten Erstellen von geplanten Aufgaben handelt – die nötige Einarbeitung entlohnt den Administrator mir einem nützlichen Werkzeug-Set.

Download und Installation

Das PowerShell Pack ist Bestandteil des Windows 7 Ressource Kits, aber auch als separater Download auf der MSDN-Seite unter [1] erhältlich. Zur Installation benötigen Sie keine administrativen Rechte. Die Module werden einfach in den Ordner "Dokumente" des installierenden Benutzers kopiert. Eine Pfadangabe lässt sich während der Installation nicht vornehmen. Sie finden die neuen Module im Ordner "…\ Users \ {Username} \ Documents \ WindowsPowerShell \ Modules". Wenn Sie die Elemente allen Benutzern des Rechners zur Verfügung stellen wollen, verschieben Sie die Unterordner in den Ordner "Modules" unterhalb des Windows-Pfades "…\Windows \ System32 \ WindowsPowerShell \ v1.0 \ Modules". Dazu sind dann allerdings wieder administrative Rechte vonnöten.

Die Module und drei erklärende Dokumente liegen in einzelnen Unterordnern des angegebenen Pfads. Sie laden das gesamte Paket mit dem Befehl *Import-Module PowerShellPack* in Ihre aktuelle PowerShell Sitzung. Eine Pfadangabe ist hierfür nicht erforderlich. Wenn Sie nur ein einzelnes der insgesamt zehn Module importieren möchten, geben Sie den Namen des jeweiligen Moduls direkt an. So importiert zum Beispiel der Befehl *Import-Module IsePack* die Erweiterung für die Integrierte Scripting Umgebung (ISE). Danach finden Sie die Erweiterungen im Menü "Add-ons" der ISE. Dies funktioniert auch, wenn die ISE bereits gestartet ist.

```
Import-Module PowerShellPack
Get-Module -ListAvailable | %{
Get-Module -Name $_
Get-Module -Name $_ | % {$_.exportedCommands} |
   %{$_.count}} |Out-Gridview
```

Listing 1: Auflistung der Modulnamen und ihrer Befehlsanzahl

Die Module im Einzelnen

Jedes der Module erweitert den Befehlssatz der PowerShell um eine unterschiedliche Anzahl von Befehlen. Dabei sticht das Modul WPK (Windows Presentation Foundation PowerShell Kit) mit 716 der insgesamt 813 neuen Befehle deutlich hervor. Die Befehle sind normalerweise als separate Skripte im PS1-Format implementiert. Somit können Sie diese gut als Vorlage für eigene Skripte nutzen. Unter [1] finden Sie eine Tabelle mit den zehn neuen Modulnamen, deren Beschreibung sowie die Anzahl der Befehle, die Ihnen damit zur Verfügung stehen.

Die Anzahl der Befehle, die über die einzelnen Module verfügbar sind, können Sie mit den Befehlen im Listing 1 ermitteln. Hilfe zu den einzelnen Befehlen erhalten Sie über das bewährte Cmdlet Get-Help. Das Cmdlet Out-Gridview setzt ein installiertes .Net Framework 3.51 voraus. Dies gilt auch für die Verwendung des Moduls WPK. Listing 2 soll die Verwendung dieses Moduls verdeutlichen. In VBS kommt häufig die Inputbox zum Einsatz, um Eingaben vom Benutzer abzuholen. Mit dem Skript wir diese Funktion nachgebildet. Der Zugriff auf die eingegebene Information erfolgt über die Variable "$dlgResult". Achten Sie bei der Nutzung des Skripts stets auf die Art des Aufrufs. Da es sich um eine Windows Presentation Foundation-Anwendung (WPF) handelt, müssen Sie entweder die PowerShell ISE verwenden oder die Datei *PowerShell.exe* mit dem Schalter "-sta" aufrufen.

Fazit

Das PowerShell Pack bietet entweder über das Windows 7 Ressource Kit oder als separater Download die Möglichkeit, eine vorhandene PowerShell v2.0-Installation um eine Vielzahl von Befehlen zu erweitern. Da Sie die Module nach Bedarf hinzuladen können, eröffnet sich eine größere Flexibilität in der Arbeit mit der PowerShell. *(ln)*

```
$dlgResult = New-Grid -Rows 2 -Columns
   'Auto','101' {
$TextChanged = {
$Input = Get-Resource Input | Select-Object
   -ExpandProperty Text
$this.Parent.Tag = "$Input"}
New-Label "Eingabe"
New-TextBox -Name Input -Column 1 -On_Loaded {
Set-Resource -Name Input -Value $this -Depth -1
} -On_TextChanged $TextChanged
New-Button "OK" -Name "btnOK" -IsDefault -Width
   '50' -Height '25' -Row 1 -column 1 -On_Click
   {$window.close()} -HorizontalAlignment 'left'
New-Button "cancel" -Name "btnCancel" -IsCancel
   -Width '50' -Height '25' -Row 2 -column 1
   -On_Click {$window.close()} -Horizontal-
   Alignment 'right'
} -show
```

Listing 2: Inputbox auf PowerShellPack-Art

Links

[1] Das PowerShell Pack auf MSDN
http://code.msdn.microsoft.com/PowerShellPack/

In jeder Ausgabe präsentiert Ihnen IT-Administrator Tipps, Tricks und Tools zu den aktuellen Betriebssystemen und Produkten, die in vielen Unternehmen im Einsatz sind. Wenn Sie einen tollen Tipp auf Lager haben, zögern Sie nicht und schicken Sie ihn per E-Mail an tipps@it-administrator.de. Für jeden Tipp, der veröffentlicht wird, bedanken wir uns mit einem Gutschein über 20 Euro für den Internetshop getDigital.de.

Tipps & Tricks ohne Gewähr

Microsoft Windows

Leider kommt es in unserem **Netzwerk** ab und an zu **Konflikten** durch **doppelt vergebene IPv4-Adressen**. Dies ist wohl darauf zurückzuführen, dass ein **DHCP-Server unter Windows Server 2008** nur die aktuell reservierten Leases überprüft, jedoch nicht im Netzwerk nachfragt, welche Adressen tatsächlich vergeben sind. Ein PC, der länger offline war und dann wieder ans Netz geht, sorgt so unter Umständen für Verwirrung. Kann ich dem DHCP-Server irgendwie beibringen, vor der Vergabe einer IPv4-Adresse nach deren Belegung im Netzwerk nachzufragen?

Windows Server verfügt mit der "IPv4 Address Conflict Detection" über eine Funktion, mit der sich die von Ihnen geschilderten Probleme aus der Welt schaffen lassen. Leider ist das Feature standardmäßig nicht aktiviert. Um dies zu ändern, navigieren Sie in der DHCP-Konsole auf den Server-Node, den Sie modifizieren wollen. Klicken Sie mit der rechten Maustaste auf "IPv4" und dann mit der linken Maustaste auf "Eigenschaften". Auf dem Reiter "Erweitert" ersetzen Sie nun bei "Conflict Detection Attempts" die Zahl "0" durch einen höheren Wert. Dieser Wert gibt an, wie oft der DHCP-Server einen PING-Request an das gesamte Netzwerk verschickt, bevor er eine IPv4-Adresse vergibt. Eine Erhöhung des Werts verlangsamt so zwar die Vergabe einer IP-Adresse, stellt aber durch den Rundruf im Netzwerk sicher, dass jede Zahlenfolge auch wirklich nur einmal vergeben ist. *(ln)*

Um bei **Windows Server 2008 R2** ein **Backup** des Systemzustands zu machen, nutze ich bisher das Backup-Snap-In der Microsoft Management Console. Nun habe ich gelesen, dass sich das Speichern des Systemzustands auch über die **Kommandozeile** durchführen lässt. Können Sie mir sagen, wie der Befehl dazu lautet und welche Parameter es gibt?

Außer dem von Ihnen genannten Snap-In der MMC eignet sich auch das Kommando *wbadmin* dazu, um ein Backup vom Ist-Zustand eines Systems zu erstellen. Geben Sie dazu in der Befehlszeile Folgendes ein:

```
wbadmin start systemstatebackup
  -backupTarget:{Speicherort der
  Backup-Datei}
```

Nach diesem Kommando erstellt das Tool eine VHD-Datei, die sich auch mit Hyper-V nutzen lässt. Beachten Sie, dass ein Backup ohne weiteres mehr als 50.000 Dateien und mehr als 4 GByte umfassen kann und das Speichern auf eine direkt angeschlossene Festplatte gut eine Stunde und mehr dauern kann.

Die Wiederherstellung eines gespeicherten Systemzustands funktioniert analog mit dem Kommando

```
wbadmin start systemstaterecovery
  -backupTarget:{Speicherort der
  Backup-Datei}
```

Mit dem Parameter "-machine" können Sie dem Backup einen Computernamen zuweisen, falls am Speicherort mehrere Sicherungen vorhanden sind. Mit dem Parameter "-recoveryTarget" lässt sich die Sicherung an einem alternativen Zielpfad wieder einspielen, während der Zusatz "-authSysvol" eine Wiederherstellung des SYSVOL-Verzeichnisses erzwingt. *(ln)*

Wenn ich unter **Windows 7** den **Windows Explorer** öffne, präsentiert mir dieser nach dem Start immer die Bibliotheken. Ich würde aber lieber mit einem **bestimmten Ordner starten** oder mir sogar direkt die Netzwerkumgebung anzeigen lassen. Kann ich den Windows Explorer so modifizieren, dass er mit einer anderen Ansicht startet?

Sie können die Start-Ansicht des Windows Explorers ganz einfach ändern. Rufen Sie dazu mit der rechten Maustaste das Eigenschaften-Menü des Explorers auf und gehen Sie auf den Reiter "Verknüpfung". Hier ist eine Modifikation der Zeile "Ziel" nötig. Wenn Sie den Explorer etwa mit einem bestimmten Ordner starten wollen, geben Sie ein-

fach folgende Zeichenfolge ein:

```
%windir%\explorer.exe c:\{Pfad und
  Name des Ordners}
```

Wollen Sie im Windows Explorer mit einer bestimmten Ansicht, etwa dem Arbeitsplatz, der Netzwerkumgebung oder den Eigenen Dokumenten starten, ist eine spezielle Syntax nötig. Verwenden Sie für die Arbeitsplatz-Ansicht die Zeichenfolge

```
%windir%\explorer.exe ::{20D04FE0-
  3AEA-1069-A2D8-08002B30309D}
```

Für die "Eigenen Dokumente" greifen Sie auf die Syntax

```
%windir%\explorer.exe ::{450D8FBA-
  AD25-11D0-98A8-0800361B1103}
```

zurück, während die Eingabe von

```
%windir%\explorer.exe ::{208D2C60-
  3AEA-1069-A2D7-08002B30309D}
```

den Explorer dazu veranlasst, direkt mit der Ansicht der Netzwerkumgebung zu starten. Die Standard-Ansicht, also der Start mit den Bibliotheken, können Sie mit dem Pfad "%SystemRoot%\explorer.exe" jederzeit wieder herstellen. *(ln)*

Wie anscheinend so viele tue ich mich im Umgang mit der neuen **Taskleiste** unter **Windows 7** recht schwer. Zwar nutze ich die Möglichkeit, dort gewisse Programme fest zu verankern, die alte Schnellstart-Leiste fand ich jedoch ebenfalls sehr nützlich, um ab und an genutzte Anwendungen nicht immer über das Start-Menü aufrufen zu müssen. Gibt es irgendeine Möglichkeit, die **Quick Launch-Leiste** auch unter Windows 7 zu reaktivieren?

Auch wenn Microsoft die Schnellstart-Leiste in Windows 7 für überflüssig erklärt hat, gibt es dennoch einen Weg, diese parallel zur neuen Taskleiste zu nutzen. Klicken Sie hierfür mit der rechten Maustaste auf die Taskleiste und wählen Sie "Toolbars / Neue Toolbar" aus. Daraufhin öffnet sich ein neues Fenster. In der Zeile am unteren Rand des Fensters tragen Sie bei "Verzeichnis" folgende Zeile ein:

```
%userprofile%\AppData\Roaming\
  Microsoft\Internet Explorer\
  Quick Launch
```

Klicken Sie nun auf "Verzeichnis auswählen". Damit erscheint das Schnellstart-Menü in der Taskleiste. Allerdings fallen die Ausmaße der Quick-Launch Leiste recht üppig aus, zudem ist sie standardmäßig ganz rechts angesiedelt, so dass die enthaltenen Icons nicht angezeigt werden. Um diese Position zu ändern, klicken Sie mit rechts auf die Taskleiste und entfernen das Häkchen bei "Taskleiste fixieren". Klicken Sie danach mit rechts auf das Quick Launch-Element und entfernen Sie dort die Haken bei "Text anzeigen" und "Titel anzeigen". Ziehen Sie das Schnellstart-Menü nun noch auf der Taskleiste nach links und fixieren Sie diese wieder. Somit haben Sie in Zukunft an dieser Stelle Zugriff auf die altbekannte Quick Launch-Leiste. *(ln)*

In unserem Unternehmen ist **Exchange 2007** im Einsatz. Vor allem beim **Öffnen eines Voicemail-Attachments** mit Outlook kommt es des Öfteren vor, dass der E-Mailclient den Vorgang mit der Meldung **"Can't create file"** abbricht. Was ist die Ursache für diesen Fehler und wie können wir diesen beheben?

Das bekannte Problem liegt daran, dass Outlook beim Öffnen einer Anlage diese in einem speziellen temporären Ordner ablegt und auch dort belässt. Öffnet der Anwender ein Attachment mit gleichem Dateinamen – wie es bei mehreren Voicemail-Meldungen standardmäßig der Fall ist – so hängt Outlook einfach eine Nummer an den Dateinamen an, also beispielsweise *VoiceMessage(2).wav*. Dies funktioniert auch sehr gut, allerdings nur so lange, bis die Anzahl der gleichlautenden und lediglich durchnummerierten Files 100 nicht übersteigt. Liegen mehr als 100 Dateien im temporären Ordner, kommt es zur Fehlermeldung "Can't create file". Sie sollten diesen Ordner deshalb regelmäßig löschen. Er ist jedoch aus Sicherheitsgründen gut im System versteckt und lässt sich am einfachsten über die Registry herausfinden. Öffnen Sie mit *regedit* die Registrierungsdatenbank und navigieren Sie zu dem Eintrag "HKEY_CURRENT_USER \ Software \ Microsoft \ Office \ 12.0 \ Outlook \ Security". Öffnen Sie dort mit einem Doppelklick den Schlüssel "Outlook SecureTempFolder". Unter dem Eintrag "Value Data:" können Sie nun den vollständigen Pfad zum temporären Ordner für die Anlagen auslesen. Gehen Sie nun im Windows Explorer zu diesem Verzeichnis und löschen Sie dessen Inhalt. Die Meldung "Can't create file" sollte Ihnen nun in der nächsten Zeit nicht mehr unterkommen. *(ln)*

Unsere Anwender verfügen teilweise über **unterschiedliche E-Mailclients**, neben dem hauptsächlich verbreiteten Outlook 2007 gibt es auch einige Fans von Mozilla Thunderbird. Von beiden Nutzergruppen erhalte ich manchmal die Anfrage, ob es nicht möglich sei, den Start des Programms mit einem **Passwort** zu sichern, so dass die E-Mails bei Abwesenheit vom Rechner auch ohne ein Abmelden vom System vor neugierigen Blicken geschützt sind. Gibt es hier Möglichkeiten?

Microsoft Outlook 2007 erlaubt es mit Bordmitteln, bei jedem Start nach einem Passwort zu fragen. Die nötige Einstellung ist allerdings etwas versteckt. Um ein Kennwort zu vergeben, muss der Nutzer in Outlook mit der rechten Maustaste auf "Persönliche Ordner" klicken und dort die Option "Eigenschaften für Persönlicher Ordner" auswählen.

Im sich daraufhin öffnenden Fenster ist dann auf dem Reiter "Allgemein" ein weiterer Klick auf die Schaltfläche "Erweitert" nötig, um im folgenden Fenster über den Knopf "Passwort ändern" ein Passwort zu vergeben, das bei jedem Start von Outlook eingegeben werden muss. Thunderbird verfügt ab Werk leider über keine Möglichkeit, automatisch mit einer Passwortabfrage zu starten. Abhilfe verschafft jedoch das Add-On "ProfilePassword", das genau den gleichen Effekt hat. Beachten Sie, dass der Passwortschutz bei beiden E-Mailclients nicht dafür sorgt, dass gespeicherte E-Mails verschlüsselt werden. Diese liegen in den entsprechenden Ordnern nach wie vor unverschlüsselt und können von Datendieben eingesehen werden. *(ln)*

Tools

Steht der Administrator vor der Aufgabe, eine **Exchange-Testumgebung mit Daten zu befüllen**, um das jeweilige Testziel vor einem realistischen Hintergrund zu erreichen, sieht er sich oft einem Dilemma gegenübergestellt: Die Nutzung echter, produktiver Daten verbietet sich in vielen Fällen, andererseits ist die manuelle Bestückung des Testsystems mit einer realistischen Datenmenge eine extrem zeitraubende Aufgabe. Hier ist ein freies Tool sehr hilfreich, das Benutzer, Kontakte, Gruppen sowie Kalenderdaten und Frei/Abwesend-Informationen automatisch in großer Stückzahl im Active Directory und in Exchange anlegt.

Das **Test Data Tool** erledigt diese Aufgabe im Handumdrehen. Dabei erstellt das Werkzeug automatisch User und Mailboxen anhand mitgelieferter Dateien, die Beispielnamen enthalten. Darüber hinaus ist das Test Data Tool in der Lage, Kontakte, Gruppen sowie Verteilerlisten automatisch anzulegen. Letztendlich befüllt der kleine Helfer dann sogar noch die Kalender der User mit zufälligen Terminen mit den anderen erstellten Usern und klassifiziert diese Termine Outlook-konform als "Abwesend", "Frei" und so weiter. Der Einsatz der Software setzt das .Net Framework 2.x oder höher voraus. Zudem muss der Rechner, auf dem das Test Data Werkzeug läuft, Mitglied der Domäne sein und benötigt Outlook 2003 oder 2007. Das Tool ist lauffähig unter Windows Server 2003 und 2008/R2 sowie Windows XP, Vista und Windows 7. Die Erzeugung von Testdaten funktioniert unter Exchange 2003, 2007 und 2010. Für den Download bedarf es einer Registrierung beim Hersteller. *(jp)*

Quelle: www.netsec.de/de/produkte/test-data-tool/

Windows-Clients an die eigenen Bedürfnisse **anzupassen**, nicht benötigte Dienste abzuschalten oder die Sicherheit zu optimieren, ist für den Anwender auch unter Windows 7 noch immer eine Angelegenheit, die viele zeitraubende Klicks erfordert. Zugleich bleibt auch stets eine gewisse Unsicherheit, nichts vergessen zu haben. Und viele User möchten es auch vermeiden in die Untiefen der Registry abzutauchen, um derartige Anpassungen vorzunehmen. Für all diese Ansprüche bietet sich der kostenlose **Ultimate Windows Tweaker** an.

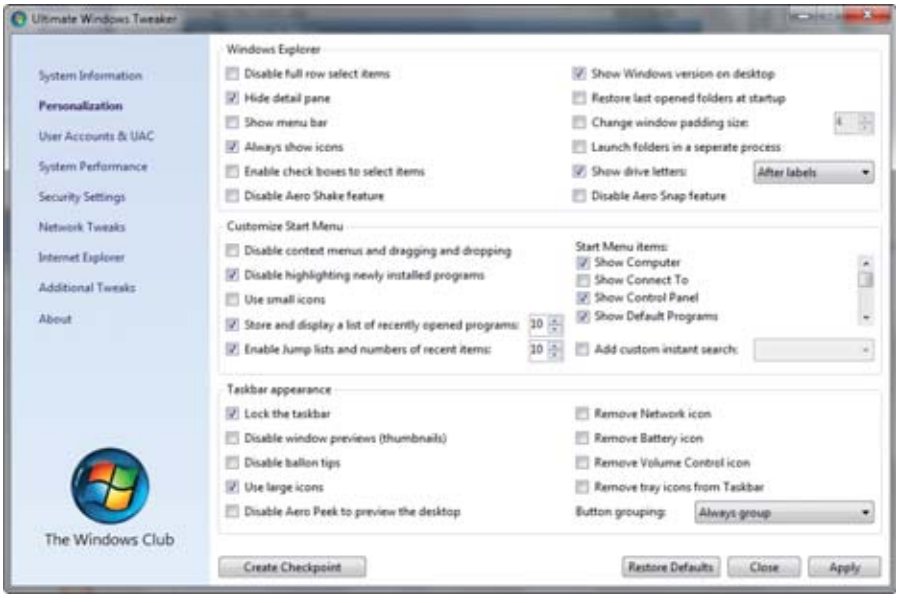
Die Freeware, die aktuell in der Version 2.1 vorliegt, bietet über 130 Einstellungsoptionen für Elemente wie **Internet Explorer, Sicherheit, Erscheinungsbild, Netzwerke, Nutzerkonten und System** unter einer Oberfläche. Nach dem Start greift der Anwender über die Programmoberfläche auf die thematisch gegliederten Menüpunkte zu. Als Rückversicherung bietet Ultimate Windows Tweaker das Anlegen eines Systemwiederherstellungspunkts an, bevor die Konfiguration von Windows 7 erfolgt. So ist sichergestellt, dass auch gravierende Fehlkonfigurationen ohne ebensolche Folgen bleiben. Ungewünschte Prozesse schalten Sie mit der Freeware per Mausklick ab. Nach dem Download muss lediglich das Archiv entpackt werden – eine Installation ist nicht notwendig. *(jp)*

Quelle: www.thewindowsclub.com

Auf der Homepage des IT-Administrator-Magazins stellen wir jede Woche für Sie ein praktisches Tool zum Download bereit. Neben einer Kurzbeschreibung finden Sie Systemvoraussetzungen und alle weiteren wichtigen Informationen auf einen Blick. Und können so gezielt Werkzeuge für Ihren täglichen Administrationsbedarf herunterladen.

www.it-administrator.de/downloads/software/

Download der Woche



Komplettes Windows 7-Tuning unter einer Oberfläche bietet der Ultimate Windows Tweaker

Trennung von Netzen durch Virtualisierung

Der Feind im Kinderzimmer

von Eckhart Traber

Mit dem Siegeszug von Remote Access und der damit verbundenen Möglichkeit, auch im Home Office wie in der Firma zu arbeiten, sehen sich die IT-Verantwortlichen mit ganz neuen Gefahrenquellen konfrontiert: Der Feind lauert nicht mehr in den Weiten des Internets, er befindet sich im Home Office hinter der nächsten Tür: Wenn die Familie, der Nachwuchs oder ein Mitbewohner beim unbedarften Surfen digitale Schädlinge ins heimische LAN einschleppen. In diesem Artikel stellen wir Methoden vor, diese Bedrohung durch Router-Virtualisierung in den Griff zu bekommen.

Eine Möglichkeit, dieser Gefahr vorbeugend zu begegnen, ist die Trennung von Heim-LAN und Teleworking-Umgebung in zwei virtuelle Netze (VLANs). Dabei wird ein einziges, physikalisches Netz durch Virtualisierung zur Grundlage einer Vielzahl von Anwendungen. Ähnlich wie im obigen Beispiel lassen sich auch Testnetz und operatives Netz trennen, Zugriffe steuern oder Gastzugänge realisieren. Sogar die gemeinsame Nutzung eines LANs durch mehrere Firmen – eine typische Situation in Technologiezentren – ist ohne Gefahr möglich.

Waren VLANs früher eine klassische Domäne der Switches, stellt sich heute die Frage, ob diese Funktionalität nicht besser im Router integriert ist. Schließlich funktioniert heute fast kein Netz mehr ohne Anbindung an das Internet – etwa bei dem eingangs erwähnten Teleworker zum Remote Access in das Firmennetz. Oder externe Partner sollen Zugriff auf einen Teil der Ressourcen erhalten. Letztlich muss der Virtualisierungsgedanke weiter gesponnen werden: Um unnötige Infrastruktur – also mehrere Router an einem Netz – zu vermeiden, wären Geräte sinnvoll, die ein Virtualisierungskonzept unterstützen.

Letztlich geht es darum, für unterschiedliche Anwendungen einen separaten IP-Kontext einzurichten. Jeder IP-Kontext wird wie ein eigenes Netzwerk beispielsweise mit DHCP- und DNS-Server konfiguriert und gegen alle anderen Netze abgeschirmt. Auf diese Art und Weise können mehrere externe Teilnehmer mit unterschiedlichen Anforderungen in das firmeninterne IP-Netzwerk eingebunden werden, ohne ihnen einen Zugang zum eigenen Intranet einzuräumen.

Trennung der Netzwerke

Wesentliche Voraussetzung für den sicheren Betrieb von unterschiedlichen IP-Netzen in einem Gerät ist die Möglichkeit, den Datenverkehr der einzelnen Netze voneinander abzuschirmen. Die Netzwerke sind über die physikalischen Schnittstellen mit dem Router verbunden. Diese physikalischen Interfaces werden aber nicht direkt für das Routing verwendet. Um eine möglichst hohe Flexibilität zu erreichen, werden die physikalischen Schnittstellen auf logische Interfaces gebunden.

Bei kabelgebundenen LAN-Anschlüssen findet die Zuordnung durch ein Ethernet-Port-Mapping statt: für jeden Ethernet-Port kann gezielt die gewünschte Verwendung als logisches LAN-Interface konfiguriert werden. Für WLAN-Schnittstellen entstehen durch den Aufbau von Point-to-Point-Strecken (PtP) beziehungsweise durch die Verwendung von Multi-SSID auf jedem physikalischen WLAN-Modul mehrere WLAN-Interfaces.

Geregeltes Routing mit Schnittstellen-Tags

Die Entscheidung über die Datenübertragung zwischen den einzelnen IP-Net-

zen ist also in den Router verlagert, in dem die Datenströme aus allen IP-Netzwerken zusammenlaufen. Grundsätzlich wird dabei das Routing zwischen den verschiedenen lokalen IP-Netzen erlaubt – ebenso ist aber auch das komplette Abschalten des Routings zwischen den IP-Netzen möglich. Über die Firewall kann der IT-Verantwortliche nun gezielt einstellen, welches IP-Netz über den Router auf welche Bereiche zugreifen darf. Bei einer größeren Anzahl von Netzen sind dazu aber unter Umständen viele Firewall-Regeln erforderlich. Um das Routing zwischen den logischen Interfaces zu vereinfachen, wird jedes IP-Netzwerk mit einem Schnittstellen-Tag versehen. Dieses Tag regelt auf sehr elegante Art und Weise, welche IP-Netze über den Router miteinander verbunden werden. Die Netzwerkgeräte in einem IP-Netzwerk können nur auf Ressourcen in Netzwerken mit dem gleichen Schnittstellen-Tag zugreifen. Das Schnittstellen-Tag "0" kennzeichnet ein Supervisor-Netzwerk: Geräte in diesem Netzwerk können auch auf Ressourcen in allen anderen Netzwerken zugreifen.

Das Schnittstellen-Tag steuert die Sichtbarkeit von IP-Netzen vom Typ "Intranet". Neben den Intranets lassen sich die Netzwerke auch als "DMZ" (demilitarisierte Zone) konfigurieren. Mit dem Netzwerk-Typ "DMZ" wird ein IP-Netzwerk definiert, auf dessen Ressourcen Teilnehmer aus allen anderen IP-Netzen zugreifen können – unabhängig von den verwendeten Schnittstellen-Tags. Dies könnte im Home Office etwa der Laser-Drucker sein, auf den alle Familienmitglieder Zugriff haben, während der im Unterhalt teure Fotodrucker in einem beschränkten IP-Netz installiert wird.

Virtuelle Router als flexible Schnittstelle ins WAN

Mit der Definition der IP-Netze und der Separierung des Datenverkehrs wird der parallele Betrieb mehrerer LANs an einem zentralen Router sichergestellt. Für die Verbindung zu anderen Netzen ist der IP-Router zuständig. Die in der Routing-Tabelle angelegten Routen sind grundsätzlich für alle an das Gerät angeschlossenen lokalen Netze gültig – anders als etwa die DHCP-Einstellungen, die für jedes IP-Netzwerk separat eingerichtet werden.

Der große Vorteil der virtuellen Router wird in folgendem Beispiel deutlich: Anhand der Quelle eines Datenpakets kann die Firewall ein Routing-Tag zuweisen, das im IP-Router zur Auswahl der geeigneten Route genutzt wird. Dieses Verfahren reicht aber dann nicht mehr, wenn der Router mehrere IP-Netze mit gleichem Adresskreis verwaltet: Eine Zuweisung des Tags anhand der Quell-Adresse wäre dann nicht mehr eindeutig möglich. Über das Schnittstellen-Tag ist jedoch die Zuordnung der Gegenstelle auch hier möglich. Das virtuelle Routing funktioniert nur durch die Auswertung der Schnittstellen-Tags, eine Konfiguration von zusätzlichen Firewall-Regeln ist nicht nötig. Für jedes lokale Netz kann so ein separater Provider-Zugang über eine getaggte Default-Route in der Routing-Tabelle angesteuert werden.

Die Firewall wird nur dann benötigt, wenn in den LANs mit gleichen IP-Adressen auch Server stehen, die aus dem Internet erreichbar sein sollen. In diesem Fall wird der Verbindungsaufbau von außen nach innen ausgelöst. Die beim Router-Modul aus dem Internet eintreffenden Datenpakete verfügen aber nicht über Schnittstellen-Tags, die für die weitere Verarbeitung verwendet werden könnten. In diesem Fall kann jedoch die externe Gegenstelle ausgewertet werden, über welche die Pakete empfangen werden. Mit einer speziellen Firewallregel können Verbindungen von dieser Gegenstelle über den entsprechenden Port (etwa Port 80 für Webserver) in das jeweilige Netzwerk erlaubt werden.

Fazit

Mit der Virtualisierung der Router lässt sich nicht nur der interne Datenverkehr im LAN lenken, sondern auch der Weg nach draußen und die Zugriffe von außen. Unternehmen erhalten damit ganz neue Möglichkeiten, ihre Infrastruktur externen Teilnehmern oder Teleworkern zu öffnen, ohne gleich den Zugriff auf das ganze LAN zu ermöglichen. Dabei wird sicher abgegrenzt: wer darf rein, worauf darf zugegriffen werden – und mit welcher Priorität. *(jp)*

Eckhart Traber ist Technical Consultant bei LANCOM.

SSL-VPNs sichern den Zugang ins Unternehmensnetz

Sichere Zugänge dank SSL-VPNs

Browser-basierte Sicherheit

von Hermann Klein

Sollen externe Mitarbeiter effizient in interne Prozesse eingebunden werden, stehen vor allem Unternehmen mit mehreren Standorten vor großen Herausforderungen: Alle Nutzer müssen gleichzeitig auf die jeweils benötigten Anwendungen zugreifen können. Zudem erfordern reibungslose Arbeitsabläufe eine stabile und sichere Verbindung, unabhängig von den verwendeten Endgeräten oder Authentifizierungsverfahren. Hier bieten web-basierte SSL-VPN-Portale eine unkomplizierte und sichere Alternative für den Netzwerkzugriff.

Ein dynamisches web-basiertes SSL-VPN-Portal erleichtert dem Administrator die Vergabe und das Management von Rechten über alle Nutzer hinweg und bietet gleichzeitig einen einheitlichen anwenderfreundlichen Zugriff auf alle Unternehmensanwendungen. Der besondere Vorteil des Portals: In einem einzigen System können IT-Verantwortliche unterschiedliche Authentifizierungs- und Autorisierungskriterien vergeben – je nach Bedarf beziehungsweise nach den Berechtigungen einzelner Anwender. Die zentrale Konfiguration über das web-basierte Portal erspart zudem eine aufwändige VPN-Installation auf jedem einzelnen Client. Dadurch lassen sich Partner und Lieferanten problemlos "remote" einbinden. Der Anwender kann sich dank der HTML-basierten Lösung direkt über die Eingabe einer URL in einem gängigen Internetbrowser im Unternehmensnetzwerk anmelden – unabhängig von Endgerät, Betriebssystem oder der IP-Adresse. Besonders attraktiv für den Administrator: In nur wenigen Schritten ist ein SSL-VPN-Portal einsatzbereit.

Sicher verbunden

Die Verbindung mit einem SSL-VPN-Portal wird über einen Browser initialisiert und dabei ein SSL-verschlüsselter Tunnel generiert. Dadurch ist von vornherein jeglicher Datenverkehr in und aus dem Unternehmensnetzwerk verschlüsselt. Darüber hinaus bietet das SSL-VPN-Portal zahlreiche zusätzliche Sicherheitsmechanismen, die sich individuell konfigurieren lassen. Beispielsweise können Administratoren die Lösung so einstellen, dass sie unmittelbar nach dem Aufbau der sicheren Verbindung das sich anmeldende Gerät auf die nötigen Sicherheitseinstellungen und auf vorhandene sicherheitsrelevante Softwarepakete überprüft. Diese so genannte Assessment-Funktion kontrolliert zum Beispiel, ob die richtige und aktuelle Firewall installiert, das Betriebssystem sowie die Antiviren-Software auf dem neuesten Stand und alle Patches aktuell sind. Sind eine oder mehrere dieser Kriterien nicht erfüllt, wird dem Endgerät automatisch der Zugriff eingeschränkt oder sogar verweigert. Bei Bedarf lassen sich solche Geräte direkt auf eine Website mit den nötigen Updates weiterleiten. Dadurch können IT-Verantwortliche sicherstellen, dass sich ausschließlich Geräte im Netzwerk anmelden, die den Sicherheitsrichtlinien des Unternehmens entsprechen und über alle aktuellen Einstellungen verfügen.

Besondere Beachtung sollten Administratoren dem mobilen Zugriff über PDAs widmen. Sie können ebenso Schadsoftware, Viren oder Würmer übertragen wie ein Notebook. Hier empfiehlt es sich, über die Grundkonfiguration des Portals den Zugriff dieser Geräte auf sehr wenige Anwendungen einzuschränken. Dadurch vermeidet man eine unnötige Gefährdung kritischer Unternehmensdaten und ermöglicht gleichzeitig dem mobilen Anwender den Zugriff auf die wichtigsten Basis-Applikationen. Ähnliches ist auch für Anfragen von Endgeräten aus unbekannten Netzwerken möglich.

Viele Wege zur Anmeldung

So spezifisch wie das Sicherheitsbedürfnis von Unternehmen sind auch die verschiedenen Methoden, mit denen sich Nutzer am SSL-VPN-Portal anmelden können. Je nach Bedarf der Anwender und dem Umfang der zu sichernden Da-

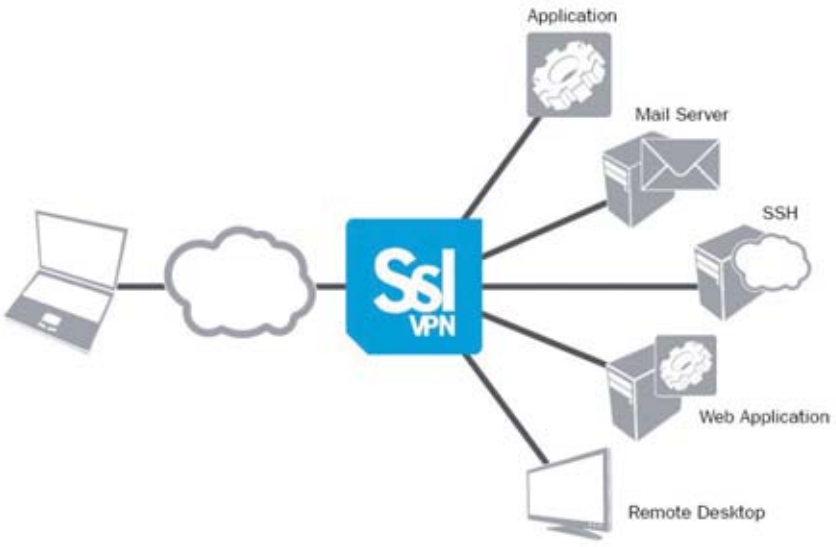


Bild 1: Ein SSL-VPN-Portal unterstützt unterschiedliche Authentifizierungstechnologien wie beispielsweise Single Sign-on

ten stehen dem Administrator mehrere Möglichkeiten zur Verfügung. Grundsätzlich unterstützt das Portal die gängigsten Verzeichnisdienste wie Microsoft Active Directory, LDAP (Lightweight Directory Access Protocol) oder Novell eDirectory. Meldet sich ein Nutzer am Portal an, gleicht ihn das System automatisch mit den Einträgen und Einstellungen in der Datenbank ab und vergibt einen entsprechenden Zugang. Diese Option ist besonders für Unternehmen interessant, die bereits einen solchen Verzeichnisdienst nutzen, denn alle Zugriffsrechte, Rollen und Berechtigungen werden in der Datenbank gepflegt. Das Portal kann diese Einstellungen übernehmen, so dass sie der Administrator nicht zweimal konfigurieren muss. Zusätzlich unterstützt das SSL-VPN-Portal auch Single Sign-on sowie andere Authentifizierungstechnologien wie Security Assertion Markup Language (SAML).

Sicher, auch unterwegs

Für Unternehmen mit vielen mobilen Mitarbeitern ist die SMS-Authentifizierung mit Einmal-Passwörtern ("one time password") eine interessante Alternative. Statt sich wie bisher über Tokens zu authentifizieren, können Mitarbeiter ihre Mobiltelefone verwenden. Damit lassen sich nicht nur Zusatzkosten für Hardware-Token sparen, die Methode ist auch zuverlässiger. Denn die meisten vergessen weitaus seltener ihr Handy als einen Hardware-Token. Für diese Form der Anmeldung muss zunächst eine Software auf dem Mobiltelefon installiert werden, kombiniert mit einem persönlichen Code. Wird ein Passwort zur Anmeldung am SSL-VPN-Portal benötigt, gibt der Nutzer seinen Code einfach ins Handy ein. Das Tool errechnet auf Basis eines zeitabhängigen Algorithmus ein Einmal-Passwort. Eine solche Zwei-Faktor-Authentifizierung ist besonders sicher, da sie das Passwort mit der Identifizierung über das Mobiltelefon kombiniert. Geht das Handy verloren oder wird es gestohlen, schützt der persönliche Code vor einem Missbrauch des Software-Tools. Eine solche Software lässt sich auch auf einem Notebook installieren. Ein beliebtes Mittel, um Passwörter auszuspionieren, ist das Mitprotokollieren der Tastatureingabe. Besonders öffentlich zugängliche Rechner können hier gefährlich sein. Aber auch dieser Gefahr lässt sich im SSL-VPN-Portal vorgreifen – mit der Integration einer Software, die automatisch mit der URL startet und die Eingabe der User-ID oder des Passworts über eine Bildschirmtastatur per Maus erfordert.

Zugriffsrechte nach Maß

Im SSL-VPN-Portal steht dem IT-Verantwortlichen eine große Auswahl an möglichen Anmeldefunktionen zur Verfügung, die bei Bedarf auch kombiniert werden können. Ebenfalls flexibel und variabel sind die Authentifizierungsmethoden, die ein SSL-VPN-Portal bietet. Beispielsweise kann eine Authentifizierung anhand von IP-Adressen erfolgen. Dabei lässt sich das Portal so einstellen, dass eine unbekannte oder öffentliche IP-Adresse automatisch eingeschränkten Zugang auf die Unternehmensapplikationen erhält. Zusätzlich erkennt die SSL-VPN-Lösung anhand von Parametern wie Uhrzeit, Ort oder Gerät, in welcher Ausgangssituation sich der Mitarbeiter befindet. Ist er im Büro oder Home Office, erhält er vollen Zugang auf alle Daten und Anwendungen. Hat er sich dagegen mit einem Notebook beispielsweise über einen Hot Spot am Flughafen eingeloggt, ist sein Zugriff auf das Unternehmensnetzwerk nach den Vorgaben des Administrators automatisch eingeschränkt. Selbst bei einem Diebstahl des Notebooks sind dadurch kritische Daten geschützt.

Die Anwender selbst lassen sich verschiedenen Authentifizierungs-Gruppen mit unterschiedlichen Zugriffsrechten zuordnen. Dadurch kann der Administrator für jede Applikation, die über SSL-VPN zur Verfügung steht, Gruppen mit spezifischen Zugriffsrechten und Rollen definieren. So muss er nicht für jeden Anwender einzeln die Konfigurationen erstellen, sondern kann ihn entsprechend seiner Funktion mit einem Klick den vordefinierten Gruppen zuordnen. Damit lassen sich alle Anwender – ob mobiler Mitarbeiter, Lieferant, Partner oder Kunde – in einem einzigen zentralen SSL-VPN-Portal verwalten. Die Freigabe auf das Unternehmensnetzwerk erfolgt dabei immer Anwendungs-orientiert, das heißt, zu jeder über das Portal verfügbaren Applikation sind unterschiedliche Rechte hinterlegt. Ändert sich die Rolle oder der Status eines Anwenders, lassen sich seine Zugriffsrechte entsprechend anpassen. Bei der nächsten Anmel-

dung am Portal erhält der betroffene Nutzer entweder eine Meldung über seine veränderten Rechte oder die Symbol-Ansicht der einzelnen Anwendungen ist einfach angepasst – je nach Konfiguration durch den IT-Verantwortlichen. Auf diese Weise stehen allen Nutzern gleichzeitig in einem einzigen Portal die jeweils für sie erforderlichen Anwendungen dynamisch zur Verfügung. Selbst bei einer komplexen Unternehmensstruktur mit vielen spezifischen Applikationen lassen sich so auch externe Dienstleister schnell und effizient in die Geschäftsprozesse einbinden.

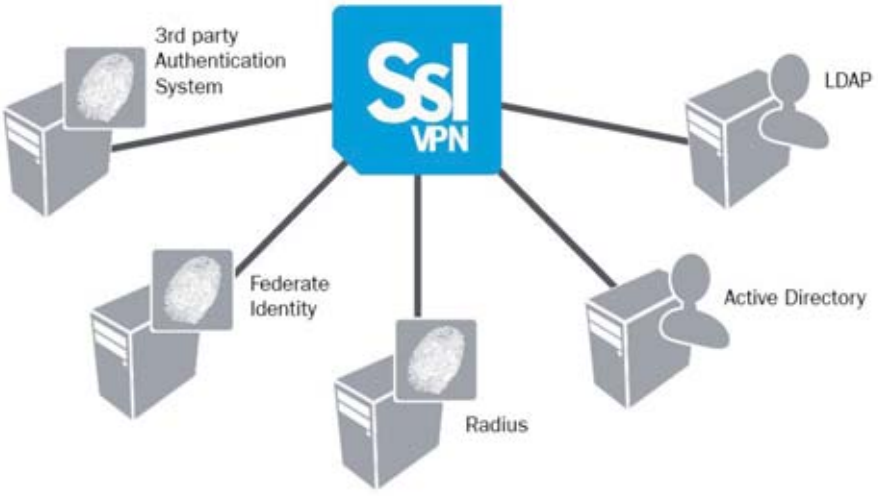


Bild 2: Ein dynamisches SSL-VPN-Portal integriert Verzeichnisdienste, verschiedene Authentifizierungssysteme und Zugriffskontrollen in einer Lösung

Die Oberfläche des Portals selbst stellt dem Anwender die verfügbaren Applikationen über verschiedene Icons dar. Je nach Nutzer und seinen Rechten variiert also die Ansicht der Symbole. Bei modernen Lösungen wie etwa StoneGate SSL-VPN von Stonesoft können Administratoren die Portalansicht auch an die Corporate Identity und die unternehmenseigene Schriftart anpassen. Eine weitere Komfortfunktion des SSL-VPN-Portals ist die Portweiterleitung (Port Forwarding). Damit können Anwender beispielsweise ihre E-Mail-Anwendung direkt starten und müssen nicht über einen möglicherweise eingeschränkten Web Access darauf zugreifen. Beendet der Anwender die Verbindung zum SSL-VPN-Portal, löscht das System dank Abolishment (Session Clean up) automatisch alle Cookies, den Cache, Download- sowie URL-Historien und schützt dadurch die Unternehmensdaten zusätzlich.

Zuverlässiger Vermittler

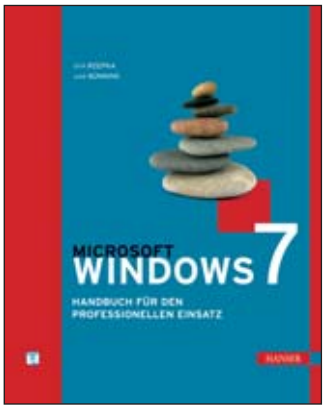
Das SSL-VPN-Portal agiert im Netzwerk als Stellvertreter (Proxy) für den Nutzer. Diese Proxy-Funktion sorgt dafür, dass sich kein Anwender jemals direkt an einer Backend-Anwendung anmelden und so auch keine Schadsoftware beispielsweise von einem mobilen Gerät übertragen kann. Dabei nimmt das Portal die Anfrage eines Geräts entgegen, baut anschließend eine neue Verbindung zum Server auf und gibt die Informationen vom Server über eine weitere neue Verbindung an das Endgerät weiter. Während dieses Prozesses entschlüsselt das Portal den SSL-Datenstrom für eine Inspektion durch die Firewall und verschlüsselt ihn wieder, bevor es die Daten an den endgültigen Bestimmungsort weiterleitet. Dadurch sind Workstations, interne Netze, Hosts und Server wirksam gegen versteckte Angriffe innerhalb von SSL-Tunneln geschützt. Für den Überblick im Netzwerk bietet das SSL-VPN-Portal auch verschiedene Reportingfunktionen. So lässt sich beispielsweise protokollieren, welche Nutzer auf welche Anwendungen zugegriffen haben. Dank eines frei konfigurierbaren Reportingtools können Administratoren zudem nahezu beliebig viele weitere Informationen abfragen.

Doppelt hält besser

Mithilfe eines dynamischen SSL-VPN-Portals können Administratoren die Herausforderungen heterogener Zugriffsrechte einfach in den Griff bekommen. Um das volle Potenzial des Systems optimal zu nutzen, sollte der Aufbau des Portals in folgenden Schritten erfolgen: Für hohe Zuverlässigkeit und Verfügbarkeit empfiehlt es sich, zwei gespiegelte SSL-VPN-Gateways parallel zu konfigurieren. Fällt eine der Appliances aus, kann aufgrund der automatischen Synchronisation die andere selbsttätig die bestehenden und neuen Verbindungen übernehmen. Der Remote-Nutzer selbst merkt davon nichts und kann unterbrechungsfrei auf seine Ressourcen zugreifen. In einem zweiten Schritt können IT-Verantwortliche alle Nutzer in Gruppen unterteilen und transparent an einen Verzeichnisdienst wie Microsoft Active Directory koppeln. Danach lässt sich für die Mitarbeiter außerhalb des Unternehmensnetzwerks eine SMS-Authentifizierung aktivieren. Als Nächstes werden Ressourcen und Webanwendungen sowie der Zugang zu älteren Client-Server-Anwendungen definiert. Hier kommt ein weiterer großer Vorteil eines SSL-VPN-Portals zum Tragen: Es ist wesentlich schneller und einfacher zu administrieren als ein reines SSL oder IPSec VPN-Gateway. Manche Lösungen unterstützen zudem das so genannte "Spike Licensing". Mit diesen temporären Lizenzen lässt sich in Ausnahmesituationen die Nutzerzahl kurzfristig erhöhen. Zum Beispiel, wenn – wie im Fall der Schweinegrippe – plötzlich viele Mitarbeiter von zu Hause aus arbeiten oder das Firmengebäude beispielsweise aufgrund eines Wasserschadens nicht genutzt werden kann. In solchen Fällen können IT-Verantwortliche die Anzahl der Remote-Nutzer innerhalb kurzer Zeit erhöhen und den Geschäftsbetrieb eines Unternehmens sichern. *(dr)*

Hermann Klein ist Country Manager DACH bei Stonesoft.

Microsoft Windows 7



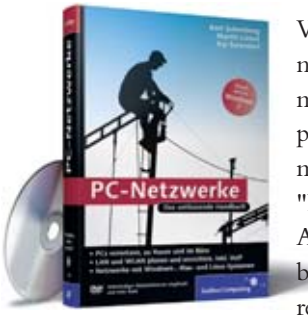
Neben Windows 7-Büchern mit starkem Fokus auf den Administrator haben natürlich auch Titel eine Daseinsberechtigung, die den Umgang mit Microsofts neuem Betriebssystem in seiner ganzen Bandbreite darstellen. "Microsoft Windows 7" von Dirk Rzepka und Uwe Bünning ist so ein Buch. Trotz der relativ umfangreichen Themenpalette hat es sich dennoch dem professionellen Leser verschrieben und behandelt nur Systemfragen, keine Anwendungen wie Paint oder den Media Player. Im Gegensatz zum erst kürzlich vorgestellten Windows 7-Buch aus dem Verlag Galileo Computing gehen Bünning und Rzepka auf alle Aspekte des Betriebssystems ein. Spezielle Themen wie das Deployment geraten dadurch sehr kurz, allerdings ist das Buch viel universeller und leistet auch Administratoren Hilfestellung, die sich vorher wenig oder gar nicht mit Vista oder Windows 7 befasst haben. Trotzdem finden die beiden Autoren Platz für interessante Randthemen. So ist beispielsweise die Parallelinstallation von Windows 7 in einer VHD-Datei sehr genau erläutert.

Generell sind die Kapitel ausreichend lang und gut erklärt. Nach der Installation geht es um Administrationswerkzeuge, Benutzer- und Rechteverwaltung, Massenspeicher und so weiter, bis hin zum Netzwerk. Fast immer folgt ein Kapitel mit Administrationsschwerpunkt auf einen Grundlagentext. So finden erfahrenere Admins den Einstieg in das Buch schneller, ohne sich durch bereits Bekanntes quälen zu müssen. Besonders bei den Admin-Kapiteln ist den Autoren die Schreibe allerdings reichlich hölzern geraten, viel Spaß stellt sich beim Lesen nicht ein. Dafür ist das Detaillevel genau richtig gewählt, um einen halbwegs erfahrenen Admin gut durch die diversen Aufgaben zu leiten. Und durch die knapp 1.000 Seiten Umfang bleibt auch genug Raum, damit grundlegende Dinge wie Gruppenrichtlinien oder Zugriffsrechte ausführlich erläutert werden können. Solche Basics kommen in einem Admin-spezifischen Buch notgedrungen zu knapp.

Fazit: "Microsoft Windows 7" ist ein gelungenes Universalbuch, mehr Nachschlagewerk als durchgehender Anleitungstext. Dank 1.000 Seiten bleibt genug Raum, um von den Basics bis zum Detail die meisten Aspekte von Windows 7 zu erklären. Themen wie Deployment kommen jedoch zu kurz. *Elmar Török*

Autoren:	Dirk Rzepka, Uwe Bünning
Verlag:	Hanser
Preis:	49,90 Euro
ISBN:	978-3-446-42093-3
Bewertung:	3,5 von 5 Sternen

PC-Netzwerke



Viele kleinere Unternehmen müssen selbst mit ihren Netzwerkproblemen klar kommen. Ein Buch wie "PC-Netzwerke" des Autorenteams Schemberg, Linten und Surendorf hilft dabei. Sicherlich muss kein Administrator mit ein wenig Praxiserfahrung einen Blick in das Buch werfen, doch für einen engagierten Einsteiger hält es alles bereit, was er zum Start braucht. Den Anfang machen Kapitel über die verschiedenen Arten von Netzwerken und deren physikalische Umsetzung. Sogar an explizite Kaufhilfen haben die Autoren gedacht, zum Beispiel für Netzwerkkarten oder Switches. Danach wird die Einrichtung eines Netzwerks unter Windows beschrieben, ganz aktuell mit Windows 7, aber auch Vista und XP sowie deren Besonderheiten bei gemischten Netzen sind erwähnt. Lobenswert: auch die Netzwerkinstallationen von Linux und Mac OS X haben eigene Kapitel bekommen.

Ein recht umfangreicher Abschnitt befasst sich mit dem Troubleshooting. Die Tipps gehen zwar nicht über die Bordmittel des Betriebssystems hinaus, mit einem Protokollanalyzer wäre der Nachwuchsadmin an dieser Stelle aber ohnehin überfordert. Wireshark wird allerdings im Anschluss dran erwähnt. Sehr praxisgerecht sind hingegen die Tipps um Netzwerk- und Massenspeicherperformance zu ermitteln. Die Autoren nutzen NetIO, iperf, FTP und das Intel NAS Performance Toolkit. Auch die Sicherheit wird angesprochen: SSH bekommt recht viel Aufmerksamkeit, Schwachstellen und Exploits werden nur gestreift. Dafür befasst sich ein eigenes Kapitel mit dem Thema Verschlüsselung und beschreibt den sicheren Mailversand per GnuPG und Enigmail sowie verschiedene Low-Level-VPNs. Einen großen Teil des Buchs machen Projekte aus, in denen der Leser selbst mit verschiedenen Programmen wichtige Infrastrukturkomponenten aufsetzt. So ist auf der Buch-CD ein Router (FlI4L) enthalten, im Kapitel 35 erfährt man alles über dessen Konfiguration. Ebenfalls mit dabei sind ein NAS-Server (OpenFiler), eine TK-Anlage (Trixbox) und ein universeller Backoffice-Server (siegfried3).

Fazit: Mit dem Buch lernen Einsteiger die Grundlagen der Administration eines kleinen Netzwerks kennen. Die Texte sind gut verständlich und praxisgerecht. Deutlich mehr lernt, wer auch die diversen Selbstbauprojekte umsetzt. *Elmar Török*

Autoren:	Axel Schemberg, Martin Linten, Kai Surendorf
Verlag:	Galileo Computing
Preis:	29,90 Euro
ISBN:	978-3-8362-1105-5
Bewertung:	4 von 5 Sternen

http://tweaks.com
Windows zurecht zwicken

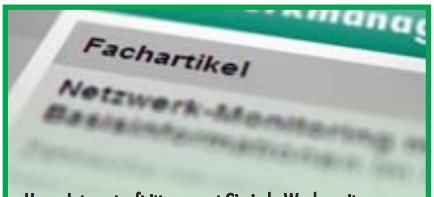
Windows-Clients ermöglichen dem Anwender einen hohen Grad an Individualisierung und Anpassung an die eigenen Arbeitsgewohnheiten. Zudem ist die Bedienung von Windows XP, Vista und 7 manchmal unnötig umständlich, so dass eine Vereinfachung Sinn macht – etwa wenn der Anwender alle geöffneten Applikationen mit einem Klick schließen möchte. Und letztendlich laufen unter den Client-Betriebssystemen oft unnötige oder gar potentiell gefährliche Dienste, die eigentlich gar nicht benötigt werden. Diesen Themenfeldern wendet sich *tweaks.com* zu und hilft Anwendern und Administratoren, ihre Systeme leistungsfähiger und bedienungsfreundlicher zu gestalten.

Wie sich aus der Einleitung schon erahnen lässt, gliedern die Betreiber ihre Site dann auch in die drei Kernbereiche Windows XP, Vista und 7. In jedem dieser Bereiche findet der Besucher die inhaltlichen Kategorien "Downloads", "How Tos" und eben "Tweaks" – letztere sind nochmals thematisch gegliedert in Bereiche wie Sicherheit, Netzwerk, Oberfläche und so weiter. Dabei bietet der Download-Bereich eine kompakte Sammlung von großen und kleinen Werkzeugen – vom Automated Installation Kit über Grafikkartentreiber bis hin zu Sicherheitstools. Die recht übersichtliche Auswahl zeigt aber schon, dass hier nicht der Schwerpunkt von tweaks.com liegt. Spannender sind da die How-Tos, die gut bebildert und mit großer Nachvollziehbarkeit Schritt für Schritt durch Aufgaben wie etwa die Installation von Windows 7 über einen USB-Stick oder das korrekte Abschalten von IPv6 führt.

Was folgt, sind die eigentlichen Tweaks – Optimierungs- und Tuningmaßnahmen für die drei Windows-Clients. Dabei erhält der Besucher der Website einerseits Kniffe, die das System mit Bordmitteln in die gewünschte Richtung manipulieren, etwa in Sachen Optimierung von Solid State-Laufwerken unter Windows 7. Die Bandbreite der Tipps reicht dabei von kleinen Verschönerungen der Oberfläche bis hin zu Virtualisierungstechnologien.

Neben den – identisch aufgebauten – Bereichen zu den Windows-Clients finden sich auf tweaks.com aber auch Tipps zu Windows- und Exchange-Servern. Allerdings nur eine Handvoll und zudem sind die Windows Server-Tricks oft identisch mit Beiträgen, die sich bereits für die Clients finden. Dennoch lohnt sich der Besuch der Seite aber unbedingt für jeden, der Optimierungsbedarf bei seinen Clients identifiziert hat. *(jp)*

Mit den richtigen Handgriffen läuft Windows besser. Tweaks.com verrät sie.



Unser Internetauftritt versorgt Sie jede Woche mit einem neuen interessanten Fachartikel. Dieser erklärt aktuelle Netzwerktechniken oder zeigt anhand eines Anwenderberichts ganz praktisch auf, mit welchen Lösungen Sie alltäglich anfallende Aufgaben leichter und effizienter erledigen können. Als Abonnent des IT-Administrator können Sie schon jetzt auf die Fachbeiträge zugreifen, noch bevor diese der Öffentlichkeit zur Verfügung stehen. **Diesen Monat erfahren Sie auf unserer Webseite mehr zu folgenden Themen:**

Monitoring für den Mittelstand

Viele Mittelständler betreiben ihr Netzwerk-Monitoring auf Open Source-Basis. So attraktiv dieser Ansatz auch ist – die Lösungen sind vergleichsweise wartungsintensiv, wenn es mehr als ein paar Basisparameter zu überwachen gilt. Kommerzielle Produkte großer Anbieter bringen hingegen oft hohe Startinvestitionen mit sich und eignen sich nicht immer für individuelle Anpassungen. In unserem Online-Fachartikel gehen wir darauf ein, wie mittelständische Firmen ihre häufig heterogene Infrastruktur effizient überwachen und die Verfügbarkeit so deutlich erhöhen können.

www.it-administrator.de/themen/netzwerkmanagement/fachartikel/80587.html

Reibungslose Umstellung auf IPv6

In den kommenden Jahren soll das bisherige Internetprotokoll IPv4 allmählich durch den neuen Standard IPv6 ersetzt werden. IT-Verantwortliche sollten sich bereits jetzt für die Umstellung wappnen. Der Fachbeitrag auf unserer Webseite beleuchtet, welche spezifischen Anwendungen das Protokoll bereits unterstützen und was Administratoren bei der Integration des neuen Protokolls auf Mail- und Web-Servern beachten sollten. Ferner machen wir klar, wo die Stolpersteine liegen und wie sich diese gekonnt umgehen lassen.

www.it-administrator.de/themen/netzwerkmanagement/fachartikel/80588.html

Anwenderbericht: Desktop-Virtualisierung

Parker SSD Drives ist einer der führenden Hersteller von Servoantrieben und -motoren und als industrieller Anbieter darum bestrebt, die produktive Zeit zu maximieren. Die für die Fertigungs-Steuerung eingesetzten PCs müssen rund um die Uhr betriebsbereit sein. Doch immer wieder kam es zu Störungen durch ungeplante Neustarts nach Updates oder bei Problemen mit den PCs. Lesen Sie in unserem Anwenderbericht, wie es durch Desktop-Virtualisierung gelang, dieser unbefriedigenden Situation wirkungsvoll zu begegnen.

www.it-administrator.de/themen/virtualisierung/fachartikel/80589.html

Besser informiert: Mehr Fachartikel auf der Website des IT-Administrator

»Es wird nie langweilig«

Roman Weber (39) sorgt in einem Team von Administratoren bei AutoScout24 dafür, dass die geschäftskritische IT-Infrastruktur und ihre Applikationen permanent verfügbar sind, damit die Online-Plattform rund um die Uhr läuft. Das bekannte Internet-Portal bietet Privatkunden, Autohändlern und anderen Nutzern eine umfassende Online-Plattform für den KFZ-Handel.

Welche Ausbildung haben Sie gemacht?

Nach meinem Schulabschluss machte ich zunächst eine Ausbildung zum Radio- und Fernsehtechniker. 1995 folgte dann die Weiterbildung zum IT Servicetechniker und Netzwerkadministrator. In den Folgejahren erwarb ich 2006 die Zertifizierung zum MCSE und 2008 dann die zum MCITP.

Warum sind Sie IT-Administrator geworden?

Während meiner Lehrzeit kam ich mit damaligen Bildschirmtext (BTX) in Berührung. Da hatte ich zum ersten Mal eine Computertastatur in den Händen und war wie elektrisiert. In einem Industriebetrieb arbeitete ich dann erstmals mit einem richtigen PC und merkte schnell, dass mir die Arbeit mit dem "Blechkollegen" viel Spaß macht.

Welche Position bekleiden Sie in Ihrem Unternehmen?

Bei AutoScout24 bin ich für die Administration von Oracle Hyperion und die Serverinfrastruktur verantwortlich. Zu meinem Aufgabengebiet gehört auch die Applikationsbetreuung sowie die Versorgung der Scout24-Holding mit einem Business-Performance-Management-System.

Welche IT-Umgebung betreuen Sie?

Unsere IT-Infrastruktur umfasst rund 800 Server. Davon entfallen auf meinen Bereich etwa 40 physikalische Server sowie zusätzlich rund 15 virtualisierte Windows Server-Systeme.

Welches Netzwerk- und Systemmanagement nutzen Sie?

Wir setzen in unserer Umgebung Nagios, Centron und Paessler PRTG ein.

Was sind im Hinblick auf die IT-Administration die größten Herausforderungen Ihres Arbeitsalltags?

Die Aufrechterhaltung des reibungslosen Serverbetriebs während der Servicezeiten ist meine wichtigste Aufgabe, denn ohne eine stabile Plattform läuft das Portal nicht. Hinzukommt die Vorgabe, Produktionsausfälle durch präventive Maßnahmen zu verhindern, damit die Prozesse reibungslos laufen.

Geburtstag: 04.08.1970
Familienstand: verheiratet
Hobbys: Modellbau, neue Medien

Roman Weber, IT-Administrator

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Eines der vordringlichsten Projekte ist die Einführung unseres System-Management-Tools in die Test- beziehungsweise Referenzumgebung von Oracle Hyperion. Dann steht auch noch die automatisierte Erstellung von Serverimages an.

Was macht Ihnen an Ihrem Job am meisten Spaß?

Der Beruf des Administrators ist in meinen Augen nie langweilig. Ständig neue Herausforderungen bewältigen zu dürfen, der Umgang mit meinen Kollegen und das Gefühl, am Ende des Tages etwas Sinnvolles gemacht zu haben, machen mir einfach viel Freude.

Was tun Sie für Ihre Fort- und Weiterbildung?

Das Lesen einschlägiger Fachliteratur sowie die regelmäßige Informationssuche auf diversen Internetseiten gehören zum Standard. Weitere Maßnahmen sind Besuche von Fortbildungsveranstaltungen sowie Classroom- und Onlinetrainings.

Was war der größte persönliche Flop oder Fehler, den Sie gemacht haben?

Bei einem früheren Arbeitgeber habe ich anstatt eines stillgelegten Servers einen aktiven Produktionsserver abgebaut. Das war ziemlich peinlich.

Was war Ihr größter Erfolg als IT-Administrator?

Auf den vollständigen Neuaufbau eines Disaster Recovery Server Centers mit Loadbalancing-Funktion zur Aufteilung der Serverlasten bin ich heute noch richtig stolz.

Was war der dümmste Anwender oder Anwenderfehler, der Ihnen untergekommen ist?

Eine ehemalige Kollegin bestellte fünf Tage in Folge immer 50 CD-Rohlinge, da sie ihre Dokumente archivieren wolle. Als sie kurz darauf nochmals eine stattliche Anzahl an Rohlingen bestellte, gingen wir Administratoren dem Grund für diesen überproportionalen Speicherbedarf nach: Sie verwendete pro Datei einen Rohling und staunte anschließend nicht schlecht, als wir ihr zeigten, dass ihre gesamte Korrespondenz locker auf einem Rohling Platz hat.

Was sehen Sie als die größte Herausforderung der IT in den nächsten drei Jahren?

Die weiter fortschreitende Virtualisierung von Servern und die ansteigende Datenflut werden uns weiterhin vor Herausforderungen stellen. Eines der wichtigsten Themen wird zudem die Einhaltung von Datenschutzrichtlinien und rechtskonformen Webinhalten sein.

Das Interview führte Petra Adamik.

Möchten Sie auch einmal das letzte Wort im IT-Administrator haben? Dann melden Sie sich einfach unter redaktion@it-administrator.de (Betreff: "Das letzte Wort"). Wir freuen uns auf Sie!

Was haben Sie zu sagen?

Die Ausgabe 6/10 erscheint am 4. Juni 2010

Schwerpunktthema:

Server-based Computing

Im Test: Thinstuff XP/VS Server 1.0390

Im Test: Immidio Flex Profiles

Workshopserie: Microsoft Desktop Optimization Pack

Know-how: Rechtsfragen beim Cloud-Computing

Das lesen Sie in den nächsten Ausgaben des IT-Administrator:

Unsere Ausgabe im **Juli** steht unter dem Schwerpunkt **SAN- und Datenmanagement**. In einem Vergleichstest nehmen wir Tools zur Dateikomprimierung unter die Lupe. In einem unserer Workshops lesen Sie außerdem, wie Sie mit vSphere 4.0 umfangreiche Storage-Umgebungen verwalten.

Als Schwerpunkt im **August** folgt dann das Thema **Management virtueller Infrastrukturen**.

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.

IMPRESSUM

Redaktion
John Pardey (jp), *Chefredakteur*
verantwortlich für den redaktionellen Inhalt
john.pardey@it-administrator.de

Daniel Richey (dr), *Stellv. Chefredakteur*
daniel.richey@it-administrator.de

Lars Nitsch (ln), *Redakteur*
lars.nitsch@it-administrator.de

Markus Heinemann, *Schlussredakteur*
markus.heinemann@email.de

Autoren dieser Ausgabe
Petra Adamik, Oliver Ebel, Marc Grote, Jürgen Heyer, Thomas Joos, Hermann Klein, Christian Knermann, Sandro Lucifora, Rolf Masuch, Ulf B. Simon-Weidner, Florian Thiessenhusen, Elmar Török, Eckhart Traber

Anzeigen
Anne Kathrin Heinemann, *Anzeigenleitung*
verantwortlich für den Anzeigenteil
kathrin@it-administrator.de
Tel.: 089/4445408-20

Es gilt die Anzeigenpreisliste Nr. 7 vom 01.11.2009

LAC/2008

Produktion / Anzeigendisposition
Lightrays: Andreas Skrzypnik
dispo@it-administrator.de
Tel.: 089/4445408-88
Fax: 089/4445408-99

Druck
Konrad Triltsch
Print und digitale Medien GmbH
Johannes-Gutenberg-Straße 1-3
97199 Ochsenfurt-Hohestadt

Vertrieb
Anne Kathrin Heinemann
Vertriebsleitung
kathrin@it-administrator.de
Tel.: 089/4445408-20

Abo- und Leserservice
Vertriebsunion Meynen GmbH & Co. KG
Stephan Orgel
Große Hub 10
65344 Eltville
leserservice@it-administrator.de
Tel.: 06123/9238-251
Fax: 06123/9238-252

Erscheinungsweise
monatlich

Bezugspreise
Einzelheftpreis: € 12,60
Jahresabonnement Inland: € 135,-
Studentenabonnement Inland: € 67,50
Jahresabonnement Ausland: € 150,-
Studentenabonnement Ausland: € 75,-
Jahresabonnement Inland mit Jahres-CD: € 144,84
Studentenabonnement Inland mit Jahres-CD: € 77,34
Jahresabonnement Ausland mit Jahres-CD: € 159,84
Studentenabonnement Ausland mit Jahres-CD: € 84,84
All-Inclusive Jahresabo
(mit Sonderheften + Jahres-CD) Inland: € 184,64
All-Inclusive Studentenabo Inland: € 117,14
All-Inclusive Jahresabo Ausland: € 199,64
All-Inclusive Studentenabo Ausland: € 124,64
E-Paper-Einzelheftpreis: € 9,45
E-Paper-Jahresabonnement: € 99,-
E-Paper-Studentenabonnement: € 49,50
Jahresabonnement-Kombi mit E-Paper: € 168,-
(Studentenabonnements nur gegen Vorlage einer gültigen Immatrikulationsbescheinigung)

Alle Preise verstehen sich inklusive der gesetzlichen Mehrwertsteuer sowie inklusive Versandkosten.

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
80802 München

Tel.: 089/4445408-0
Fax: 089/4445408-99

(zugleich Anschrift aller Verantwortlichen)

Web: www.heinemann-verlag.de
E-Mail: info@heinemann-verlag.de

Eingetragen im Handelsregister des Amtsgerichts München unter HRB 151585.

Geschäftsführung / Anteilsverhältnisse
Geschäftsführende Gesellschafter zu gleichen Teilen sind Anne Kathrin und Matthias Heinemann.

ISSN
1614-2888

Internet
www.it-administrator.de

So erreichen Sie den Leserservice
Leserservice IT-Administrator
Stephan Orgel
65341 Eltville
Tel.: 06123/9238-251
Fax: 06123/9238-252
E-Mail: leserservice@it-administrator.de

Bankverbindung für Abonnenten
Konto 174 966 462 bei der
Postbank Dortmund, BLZ 440 100 46
Kontoinhaber: Vertriebsunion Meynen

So erreichen Sie die Redaktion
Redaktion IT-Administrator
Heinemann Verlag GmbH
Leopoldstr. 85
80802 München
Tel.: 089/4445408-10
Fax: 089/4445408-99
E-Mail: redaktion@it-administrator.de

So erreichen Sie die Anzeigenabteilung
Anzeigenverkauf IT-Administrator
Anne Kathrin Heinemann
Heinemann Verlag GmbH
Leopoldstr. 85
80802 München

Tel.: 089/4445408-20
Fax: 089/4445408-99
E-Mail: kathrin@it-administrator.de

INSERENTENVERZEICHNIS

Die Ausgabe enthält zwischen Seite 34 und 35 einen Beihefter der Firma IAIT (Institut zur Analyse von IT-Komponenten) sowie ein Advertorial von itWatch.

Das IT-Administrator Komplettprogramm!!!

Sichern Sie sich jetzt das **IT-Administrator Jahresabo All-Inclusive** mit allen Monatsausgaben, Sonderheften und der Jahres-CD.

Statt Euro 29,90 zahlen Sie dabei für jedes Sonderheft nur Euro 19,90 – und müssen keine zusätzliche Bestellung mehr tätigen.

Automatisch bekommen Sie im März und Oktober jeden Jahres das jeweilige IT-Administrator Sonderheft und mit Ihrer Dezemberausgabe die jeweilige Jahres-CD mit allen Monatsausgaben des Jahres im PDF-Format zugestellt.

Als bestehender Jahresabonnent können Sie hier upgraden:

www.it-administrator.de/abonnements/aboupgrade/

Oder Sie sind Neukunde? Hier können Sie bestellen:

www.it-administrator.de/abonnements/jahresabo/

www.it-administrator.de

Heinemann Verlag
Im Dialog mit Spezialisten.

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
D-80802 München

Tel: 0049-89-4445408-0
Fax: 0049-89-4445408-99
info@heinemann-verlag.de

Vertrieb, Abo- und Leserservice IT-Administrator
vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville

Tel: 06123/9238-251
Fax: 06123/9238-252
leserservice@it-administrator.de

Drei aktuelle Angriffe - itWatch schützt

Angriffe über pdf Dateien - itWatch schützt:
Alle eingehenden pdf Dateien werden durch inhaltliche Patternprüfung auf schadhaften Code geprüft. Nicht nur Dateien, die über USB Sticks oder andere Datenträger (CD / DVD) eingelesen werden, sondern auch die, die von Anwendungen wie E-Mail-Client oder Browser auf den PC gebracht werden.

Schwachstelle im Internet Explorer – itWatch schützt:
Die Schwachstelle des IEs kann nur Schaden anrichten, weil der Angreifer die Rechte des angemeldeten Benutzers übernimmt. Mit der itWatch Applikationskontrolle kann der Rechteraum des IEs so eingeschränkt werden, dass er nur Konfigurationsdaten lesen darf, keine Schreibrechte auf anderen ausführbaren Dateien hat und solche auch nicht erstellen oder ausführen kann.

USB-Hardware-Verschlüsselung unsicher – itWatch schützt:
Der aktuell gemeldete Angriff auf selbst verschlüsselnde USB-Sticks lässt das Vertrauen in diese Technologie weiter sinken. Die Softwarelösung der itWatch schützt sowohl vor USB-Dumpern als auch vor Angriffen auf den Stick, da der Schlüssel nur im Kopf des Anwenders bekannt ist.

itWatch unterstützt WhiteIT:
WhiteIT will eine Strategie zur Bekämpfung von Kinderpornographie entwickeln und umsetzen. itWatch trägt neben der patentierten Inhaltsprüfung Echtzeitmonitoring und Forensik auf dem Endgerät bei. Dateiarchive und verschlüsselte Inhalte werden sicher auf frei definierbare schädliche Inhalte geprüft und im Trefferfall mit geeigneten Maßnahmen bekämpft.

itWatch GmbH

Endpoint Security, die mitdenkt

+49 (0) 89 620 30 100 - www.itWatch.de - Info@itWatch.de

Besuchen Sie uns: Basel, Berlin, Bonn, Sao Paulo, Karlsruhe, München, Nürnberg