

Administrator

Das Magazin für professionelle System- und Netzwerkadministration

Im Test:
HOB RD VPN 1.3
Flexibles SSL-VPN

Sonderdruck für HOB

**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 RDVPN 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 Großrechnerterminalen oder das Durchreichen von Datenverkehr auf individuellen Ports. HOB RDVPN 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 RDVPN 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 RDVPN 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 RDVPN zusätzlich auf einem schon bestehenden Server mit installiert oder alleinstehend womöglich mit SCS betreibt.

Einfache Grundinstallation

Für unseren Test installierten wir RDVPN 1.3 auf einem Windows Server 2008. Neben RDVPN, das auch die Komponente "HOB Enterprise Access" enthält (hierzu später mehr), gibt es die etwas schlankere Lösung "RDVPN 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 Kopplung beispielsweise mit einem Active Directory. So kann der Administrator bei der großen Lösung für jeden Benutzer indivi-

duelle 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-

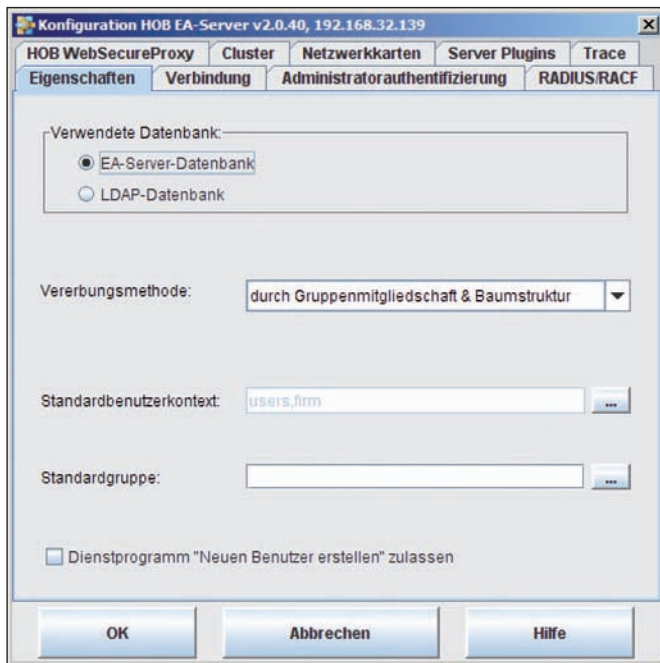


Bild 1: RD VPN lässt sich wahlweise mit einer eigenen Benutzerdatenbank oder einer LDAP-Anbindung, beispielsweise Active Directory, betreiben

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.

che 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

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

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 Auswahlménü 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

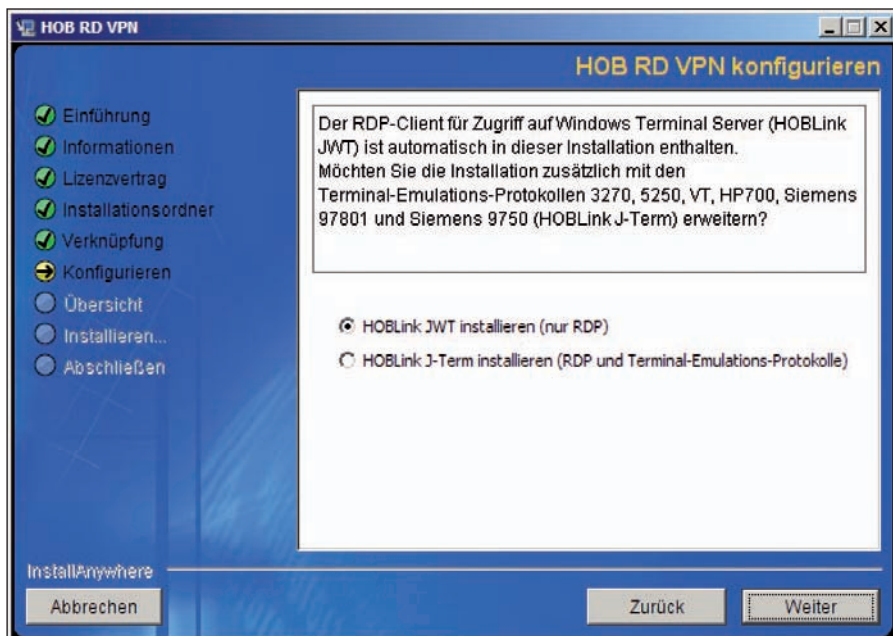


Bild 2: RD VPN unterstützt wahlweise nur RDP-Zugriffe oder auch die Nutzung spezieller Terminal-Emulations-Protokolle

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 RDVPN dürfte das WTS-Computing auf Basis des

Windows Terminalservers sein – neuerdings auch RDS-Computing (Remote Desktop Services) genannt. Bereits vor-konfiguriert 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 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.

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)

Systemvoraussetzungen





Tunnel ins Firmen-Netz

Der so genannte PPP-Tunnel von RDVPN 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 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.

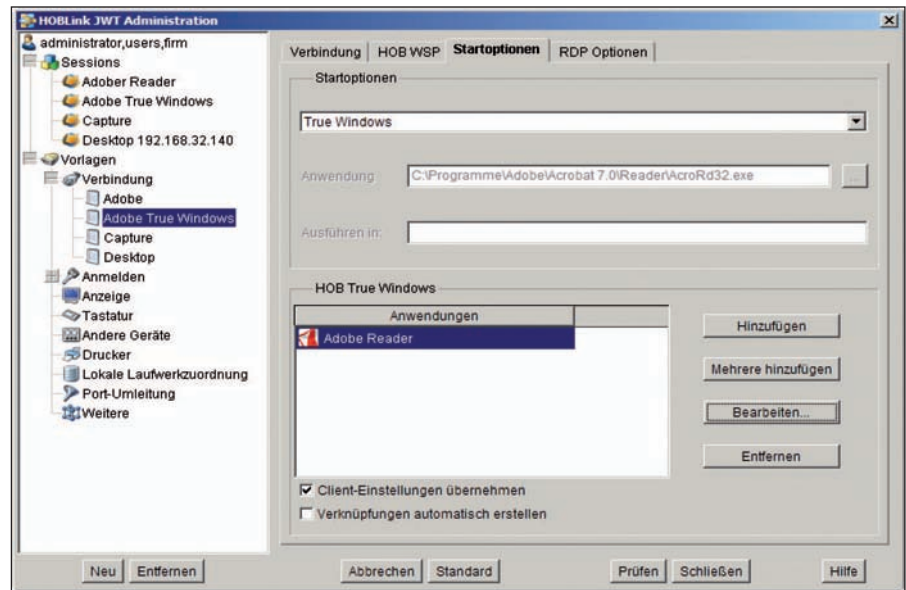


Bild 3: Die Freigabe einer Applikation im True Windows-Modus erfordert mehrere Konfigurationsschritte und ist vergleichsweise komplex

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.

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 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 be-



Produkt

Remote Access-Lösung per SSL-VPN.

Hersteller

www.hob.de

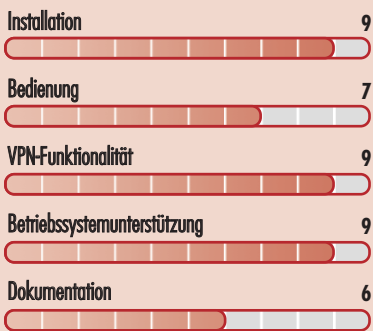
Preis

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)



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

schrieben 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 Vor-

teil, 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) 