

# Eine sichere Verbindung

Von Ken Araujo

Secure Sockets Layer (SSL) VPNs haben in jüngster Vergangenheit einen Popularitätsschub im Remote-Access-Markt erfahren. Einige Analysten gehen sogar davon aus, dass die **SSL-VPN-Technologie** IPSec-basierende VPN-Lösungen zunehmend verdrängen: SSL VPNs sollen nicht nur günstiger in der Anschaffung, sondern auch leichter zu skalieren sein.

**B**is vor kurzem wurden VPNs, die auf dem IPSec-Protokoll (Internet Protocol Security) basieren, als die einzig logische Wahl für sichere Netzwerkverbindungen über die Firewall hinaus angesehen. IPSec-VPNs verhalten der Datenübertragung über das Internet zu großer Resonanz, insbesondere durch massive Kostensenkung gegenüber den klassischen Datenübertragungstechniken wie Mietleitungen, Asynchronous Transfer Mode (ATM) oder Frame Relay. Auch für Punkt-

Ken Araujo ist Chief Technology Officer und Senior Vice President of Engineering bei Netilla Networks, einem Hersteller von SSL-VPN-Lösungen.

zu-Punkt-förmige On-Demand-Verbindungen stellen sie eine weniger kostspielige Alternative mit hohem Sicherheitsniveau dar.

Dennoch ermöglichen Remote-Zugänge via IPSec-VPNs Sicherheit nur zu einem relativ hohen Preis. IPSec setzt die Installation und Konfiguration entsprechender Softwareclients auf den Rechnersystemen der Remote-Nutzer voraus. Weil sie auf der Netzebene funktionieren, gewähren IPSec-VPNs weiterhin dem Remote-PC die vollständige Sicht auf das Netzwerk, so als ob es sich um Computer aus dem lokalen Netzwerk (LAN) handeln würde. Die Umsetzung von IT-Sicherheitsrichtlinien (Policy Enforcement) ist mit einem solchen Lösungsansatz nur schwierig realisierbar. Aus diesen Gründen schneiden Remote-Zugänge mittels IPSec-VPNs durch ihre hohen Gesamtkosten (TCO) im Vergleich zu SSL-VPNs schlechter ab.

Während die Zahl webbasierter Intranetanwendungen innerhalb der Unternehmen wächst, bilden nicht netzwerkfähige Legacy-Anwendungen auf zentralen Windows-, UNIX/Linux-, Mainframe oder AS/400-Hosts gegenwärtig noch immer den lebenswichtigen Kern vieler Unternehmensanwendungen. Für IT-Manager stellen diese Anwendungen die größte Herausforderung bei Auswahl und Design eines sicheren Fernzugriffs dar, sollen die gleichen On-Demand-Zugangsverfahren für alle Anwendungen eingesetzt werden.

## SSL VPNs: Application Gateways für Unternehmen

Hersteller von SSL-VPN-Appliances lösen dieses Dilemma, indem sie Client-losen Fernzugriff auf Legacy-Applikationen durch direkte Implementierung von Web-enabling-Technologien auf der System-



Bild: Symantec, funkschau

plattform realisieren. Dieser integrierte Ansatz beseitigt die Notwendigkeit für die Unternehmen, Server-basierte Middleware und die zugehörigen Remote-Access-Clients installieren und betreiben zu müssen. In einem solchen Modell werden sowohl die Client- als auch Serverelemente einer Anwendung weiterhin zentral im Rechenzentrum des Unternehmens gehostet. Der Vorteil dieses Ansatzes ist, dass die Endbenutzer lediglich einen gewöhnlichen Browser benötigen, um auf die entfernten Anwendungen zugreifen zu können und keine zusätzliche Software oder Konfiguration des zugreifenden Rechnersystems erforderlich ist.

Ein SSL-VPN-Appliance macht Client-/Serveranwendungen für Remote-Benutzer durch das Netz zugänglich, erlaubt Firmen, ihre vorhandenen Legacy-Applicationen weiterhin einzusetzen ohne diese teuer neu programmieren zu müssen. Nahezu jedes Programm auf jeder heute üblichen Plattform – sei es Windows, Unix und Linux, oder 3270 Mainframe beziehungsweise 5250 AS/400 – kann folglich für Remote-Anwender leicht zur Verfügung gestellt werden.

In diesem Application-Layer-Zugangsmodell verwendet das SSL-VPN-Gateway ein so genanntes Screen-Scraping Protocol, das Emulation und Display Processing aufspaltet, sodass nur die Darstellung der Anwendung zum Webbrowser des Remote-Benutzers übertragen wird. Das Gateway unterstützt diese Fähigkeit durch ein Java-Applet, das beim ersten Benutzer-Login automatisch installiert wird. Im Ergebnis kann der Anwender die Applikation selbst über schmalbandige Verbindungen mit der

gewohnten Geschwindigkeit bedienen, etwa so, als ob die Anwendung auf der lokalen Maschine des Benutzers ausgeführt wird.

### Sicherer Intranet-Zugriff auf Web-basierte Applikationen und Portale

Auch wenn Unternehmen an ihren Legacy-Applikationen als Teil ihrer Anwendungsstrategie festhalten, kommen sie oft kaum umhin, browserbasierten Webzugriff auf Anwendungen zu ermöglichen. Natürlich lassen sich auch Legacy-Applikationen, wie zum Beispiel Microsoft Outlook oder proprietäre Intranet-Anwendungen webfähig machen. Die Bereitstellung solcher Informationen über das Web kann jedoch zu ernsthaften Sicherheitsrisiken führen, die sorgfältig geprüft werden müssen. In jedem Fall stellt die Bereitstellung von Webzugriff auf interne Anwendungen bei gleichzeitiger Erweiterung des Nutzerkreises IT-Abteilungen vor eine herausfordernde Aufgabe. Dies beginnt beispielsweise schon damit, dass viele Anwendungen im geschützten Intranet des Unternehmens gehostet werden und für die Hostname-Auflösung das interne Domain Name System (DNS) nutzen, welches aber nicht im öffentlichen Internet aufgelöst werden kann und soll.

Aktuell verfügbare SSL-VPN-Appliances überwinden ein solches Hindernis in der Regel, indem Intranetressourcen über SSL-Tunnel gesichert ausschließlich autorisierten Anwendern zur Verfügung gestellt werden. Dies wird erreicht durch Client-losen, browserbasierten Zugriff auf Web-basierte Ressourcen unter Verwendung der HTTP-Reverse-Proxy-Technologie (Hyper Text

## SSL VPNs sind die bessere Alternative

Tony Caine, Vice President EMEA bei Aventail Corporation: „SSL VPNs sind sicherer, einfacher zu managen und flexibler als IPSec-basierte VPNs. SSL hat sich als De-facto-Standard in der Welt des E-Commerce bewährt und erlaubt die Kommunikation über Breitband, Satellit, Wireless und Mobilfunk-Netze. Da SSL in jedem Standardbrowser enthalten ist, entfällt – im Unterschied zu IPSec VPNs – die Client Software auf dem Endgerät des Anwenders. Und damit entfällt auch der administrative Aufwand für Clients auf unzähligen Endgeräten, was sich äußerst positiv auf die Gesamtkosten einer SSL-VPN-Lösung auswirkt. Der Anwender hat bei SSL VPNs die Wahl, mit welchem Internetzugangsgeschäft er wann und von welchem Ort auf Firmenressourcen zugreifen will. Selbst der Zugang zu E-Mail, Client/Server-Anwendungen wie SAP, PeopleSoft oder Oracle oder auch komplexe Web-Anwendungen mit Java-Applets oder Active-X-Steuerungen, ist heute bei SSL VPNs kein Thema mehr. Für die Anforderungen der modernen Arbeitswelt und den sicheren, ortsunabhängigen Remote-Zugriff sind SSL VPNs klar die bessere Alternative.“ (SW)



Tony Caine ist Vice President EMEA bei Aventail Corporation

Transfer Protocol). Im Gegensatz zu einem Forwarding Proxy, der in der Regel als Mittler zwischen dem Nutzer im Corporate Intranet und einer Internet Website geschaltet wird, stellt ein Reverse Proxy das Bindeglied zwischen dem Remote-Anwender im Internet und der Enterprise-Webseite dar. Den so genannten Single Point of Entry über das Internet bildet dann das SSL-VPN-Gateway, über welches der Remote-Anwender sicher auf Webserver im Backend mit Hilfe seines Browsers zugreifen kann.

### SSL-Tunneling: Technologie und Nutzenaspekte

Eine solche Architektur ermöglicht schnellen, sicheren und bedarfsweisen Zugriff auf Web-basierte Informationen und ist zudem hochgradig skalierbar, falls die Zahl der zu autorisierenden Nutzer rasch ansteigen sollte. Die Corporate Web Server bleiben dabei im von der Firewall gesicherten privaten Netzbereich und es entstehen keine Zusatzkosten, etwa für aufwendiges Server-Hardening und Maintenance, weil Public Access von vornherein vermieden wird. Zusätzlich werden die Administratoren in die Lage versetzt, die Zugriffskontrolle auf Verzeichnisse, Server, Pfade und Benutzergruppen die Sicherheitsrichtlinien im Unternehmen wesentlich feingranularer umzusetzen.

## Jede Sicherheitstechnologie hat ihren Einsatzbereich

Dr. Christoph Skornia, Technical Manager Central Europe bei Check Point: „Der Trend, das Internet für den Remote-Zugriff auf Server und Netzwerke zu nutzen, ist in den letzten Jahren rapide angestiegen. Für immer mehr Firmen steigt der Bedarf, Mitarbeitern von außerhalb den Zugriff auf das Firmennetzwerk zu ermöglichen. Parallel wächst natürlich die Bedeutung von Datensicherheit in Form von Verschlüsselungsmechanismen und VPNs.“

Die Klassifizierung der Sicherheitsmechanismen SSL und IPSec in 'besser' oder 'weniger gut' ist nicht sinnvoll. Beide Technologien dienen dazu, Kommunikation zu schützen und beide haben ihren eigenen Einsatzbereich, in dem die immanenten Stärken zum Tragen kommen. Um ganzheitlichen Schutz und Sicherheit zu bieten, sollte eine Firewall beziehungsweise jedes Security-Tool beide Sprachen sprechen. Die Check Point Firewall-1 tut dies.

Grundsätzlich kann man sagen, dass eine Firma tendenziell dazu neigen wird, die internen Abläufe durch eine IPSec-Verbindung abzusichern. In dem Moment, in dem es aber darum geht, dass anonyme Personen, beziehungsweise einzelne Nutzer über das Web Zugriff auf einen der Firmen-Server zugreifen, ist sicherlich SSL die sinnvollere – weil einfachere – Methode.



Dr. Christoph Skornia ist Technical Manager Central Europe bei Check Point

Typischerweise wird der Zugriff auf Desktopanwendungen via SSL-Tunnel mit Hilfe eines VPN-Adapters realisiert, der heruntergeladen und installiert wird, wenn sich der Anwender zum ersten Mal am Remote-Access-System anmeldet. Der virtuelle Adapter baut danach einen sicheren SSL-Tunnel per Webbrowser auf. Anpassungen bei den Client- und Serveranwendungen sind dabei nicht erforderlich. Sobald der Netzwerkadministrator einen Anwender für bestimmte Applikationen autorisiert hat, kann auf diese über den SSL-Tunnel zugegriffen werden, und zwar ohne weitere Konfigurationsänderungen. Die meisten aktuell verfügbaren SSL-VPN-Gateways sind für derartige Client-/ Server Arrangements bestens geeignet und bringen eine Reihe signifikanter Vorteile gegenüber

### SSL VPN und IPSec VPN im Vergleich

	SSL	IPSec
Datensicherheit	Sehr hoch	Extrem Hoch
Starke Authentifizierung	Ja	Ja
Transparentes IP-Tunneling	Nein	Ja
Remote Access VPN	Ja	Ja
Branch Office VPN	Nein	Ja
Aufwand für Client Roll-Out	Keiner (Clientless)	Keiner

Quelle: Nortel Networks

klassischen IPSec-VPNs mit sich: Bei der Bereitstellung client-losem Zugriffs auf Legacy-Applikationen und der Nutzung als HTTP Reverse Proxy für Webanwendungen werden die umfangreichen Zugriffsmöglichkeiten auf Applikationen deutlich. So gesehen sind SSL-VPN-Gateways gleichzusetzen mit einem echten Application-Layer Proxy.

SSL-VPNs werden insbesondere deshalb so genannt, weil sie auf der Schicht fünf des OSI-Layer-Modells, also der Anwendungsschicht arbeiten. Im Vergleich dazu arbeiten IPSec-VPNs auf Netzwerkebene. Aus dieser Tatsache entspringt für den Administrator der große Vorteil, dass SSL-VPN-Gateways Anwendungsdaten interpretieren können und somit die Umsetzung von Sicherheitsrichtlinien auf Anwendungsebene erzwungen werden kann. Damit wird es möglich, an zentraler Stelle

### Zeitgleicher Einsatz von IPSec und SSL VPN verursacht die geringsten Gesamt-Kosten

*funkschau: Worin liegen die grundsätzlichen Unterschiede zwischen IPSec VPNs und SSL VPNs?*

Heinz Behrens: Nicht nur für den Netzzugang über das Internet und die Verbindung von Zweigstellen miteinander wird heute der Aufbau eines VPNs empfohlen, sondern auch für den Netzzugang über ein WLAN.

Die Kriterien, von denen die Anwendung von IPSec oder SSL VPN (oder beidem) abhängt, gliedern sich in verschiedene Bereiche: Dazu gehört unter anderem der Security-Aspekt. Beide Verfahren bieten gleichwertige Sicherheit, lediglich der Schlüsselaustausch ist bei IPSec etwas aufwendiger gestaltet. Ebenso unterstützen beide Methoden starke Authentifizierung mit der Nutzung von digitalen Zertifikaten.

IPSec als Netzwerk-Layer-Protokoll sichert transparent den gesamten Datenverkehr zwischen den Tunnel-Endpunkten, unabhängig von der jeweiligen Applikation. SSL VPN ist ein Application-Layer-Protokoll und damit abhängig von der Unterstützung der jeweiligen Applikation. Nicht-Webbasierte Applikationen lassen sich mittels Java-Applets und Active-X-Controls ebenfalls mit SSL VPN verschlüsseln.

Mittels IPSec werden transparente Tunnel aufgebaut, sodass der Zugriff auf sämtliche Netzwerk-Ressourcen erlaubt wird. SSL VPN erlaubt Zugriffsregelungen auf Applikations-Ebene, sodass der User nur auf die Inhalte zugreifen darf, die für ihn erlaubt sind. Während für IPSec separate Clients verwendet werden müssen, findet man heute eine SSL-Implementierung in

allen gängigen Browsern (zum Beispiel Internet Explorer und Netscape) vor. Im Vergleich dazu gestaltet sich die Implementierung eines IPSec-Clients etwas schwieriger. Die Administration kann hierbei aber auch zentral für alle Clients erfolgen, wie es Nortel Networks bezüglich seiner Contivity IPSec-VPN Client-Software implementiert hat.

IPSec VPN skaliert bestens in Bezug auf neue Applikationen. Durch transparentes Tunneling werden neue Applikationen automatisch verfügbar. SSL VPN muss für jede neue Applikation angepasst werden. Für die Skalierbarkeit der User skaliert jedoch SSL VPN besser, da keine zusätzliche Software für einen neuen User installiert werden muss.

*funkschau: Welche Sicherheitstechnik eignet sich für welche Anwendung?*

Heinz Behrens: IPSec VPN eignet sich für Branch-Office VPN und Remote Access VPN für Teleworker. SSL VPN eignet sich für Remote Access VPN für Reisende und „Roadwarrior“ sowie für Extranet-VPN zur Anbindung von Partnern.

*funkschau: Auf wie hoch belaufen sich die Kosten im Schnitt im Unternehmenseinsatz pro User?*

Heinz Behrens: Der zeitgleiche Einsatz von IPSec und SSL VPN verursacht die geringsten Gesamt-Kosten, da für das jeweilige Anwendungsgebiet die optimale Technologie verwendet wird. Hier bietet das Nortel Networks VPN Gateway 3050 die optimale Kombination für den Remote-Zugang mit IPSec- und SSL VPN. (SW)



Herr Behrens ist Senior Network Consultant bei Nortel Networks Germany

dynamische Zugriffsregeln auf Anwendungen im Kontext des jeweiligen Benutzers festzulegen.

### Fazit

Sicherheit ist der Eckpfeiler jeder Remote-Access-Implementierung und eine gute Sicherheitslösung sollte dabei gleichzeitig auch eine einfach zu betreibende Lösung sein. SSL-VPN-Appliances können schnell ins Netzwerk integriert werden und erfordern weder Modifikationen noch Unterbrechungen der existierenden Anwendungs-Server und Sicherheitsmechanismen.

Die aktuell verfügbaren SSL-VPN-Gateways führender Hersteller vereinigen alle wesentlichen Sicherheitsfunktionen in ei-

ner integrierten Appliance, das heißt Authentisierung, Policy Enforcement und Verschlüsselung werden in einer Systemplattform gebündelt und somit eine schnelle und zuverlässige funktionierende Integration ermöglicht. Damit erhält der Kunde eine einfach zu betreibende und wartungsarme VPN-Lösung mit einem reichhaltigen Featureset, bei dem Network-Layer-VPNs nicht mithalten können.

Mit einer Vielzahl unterschiedlicher Zugriffsverfahren, dynamischen Policies zum Schutz der Netzressourcen und einer leichten intuitiven Konfiguration verhelfen aktuelle SSL-VPN-Gateways Unternehmen zu Produktivitätssteigerung, Ergebnisoptimierung und mehr Kundenorientierung. (SW)