

## Sonderdruck für Netilla Networks

### SSL-VPN-GATEWAYS FÜR REMOTE ACCESS

# Alternative zu IPSec

Secure-Sockets-Layer-VPNs haben in jüngster Vergangenheit einen enormen Popularitätsschub im Remote-Access-Markt erfahren. Eine Reihe namhafter Analysten sagt voraus, dass Produkte auf Basis der SSL-VPN-Technologie zunehmend mit klassischen auf IPSec basierenden VPN-Lösungen konkurrieren und diese zunehmend verdrängen könnten. Dieser Beitrag geht auf die den SSL-Gateways zugrunde liegende Technologie ein.

Zurzeit ist eine steigende Nachfrage nach SSL-VPNs zu verzeichnen. Diese lässt sich vor allem auf drei wichtige Faktoren zurückführen: erstens die Verschärfung der Datenschutzgesetze. Der Schutz der Privatsphäre muss gewährleistet sein, insbesondere durch den Schutz von Vertraulichkeit, Integrität und Authentizität beim Übertragen und Speichern personenbezogener, sensibler Daten. Zweitens die wachsende Nutzung von Extranets. Der gesicherte Zugriff auf interne Netzwerke für externe Mitarbeiter und Partnerunternehmen hat sich zur Basisanforderung im Geschäftsalltag entwickelt. Und drittens der gestiegene Bedarf nach Flexibilisierung der Arbeit. Mitarbeiter wünschen sich oft flexible Arbeitszeiten und die Möglichkeit, von zu Hause aus arbeiten zu können – ein Trend, der zum Beispiel in Großbritannien sogar vom Gesetzgeber im so genannten "Flexible Working Act" begünstigt wird, um für arbeitende Eltern mit kleinen Kindern angemessene Rahmenbedingungen zu schaffen.

Es überrascht nicht, dass SSL-VPNs von diesen Entwicklungen profitieren. Sie vereinen unterschiedlichste Anforderungen an Remote-Zugänge und bieten verhältnismäßig niedrige Kosten bei hoher Flexibilität, angemessener Sicherheit und Benutzerfreundlichkeit.

**TRADITIONELLE LÖSUNGEN GREIFEN ZU KURZ** Bis vor kurzem wurden VPNs, die auf IPSec basieren, als die einzig Wahl für sichere Netzwerkverbindungen über öffentliche Netze angesehen. IPSec-VPNs verhalten vor allem der Datenübertragung über das Internet zu großer Popularität, insbesondere durch massive Kostensenkung gegenüber den klassischen Datenübertragungstechniken wie Mietleitungen, Asynchronous Transfer Mode (ATM) oder Frame Relay. Auch für Punkt-zu-Punkt-On-Demand-Verbindungen stellen sie eine weniger kostspielige Alternative mit hohem Sicherheitsniveau dar. Dennoch bringen Remote-Zugänge via IPSec-VPNs immer noch einen relativ hohen Preis mit sich.

IPSec setzt die Installation und Konfiguration entsprechender Software-Clients auf den Rechnersystemen der entfernten Nutzer voraus – eine kostspielige und schwierige Aufgabe insbesondere dann, wenn die Administratoren keinen direkten Zugang auf diese Systeme besitzen. Weil sie auf der Netzebene arbeiten, gewähren IPSec-VPNs den Remote-PCs eine vollständige Sicht auf das Unternehmensnetz, so, als ob es sich um Computer aus dem LAN handeln würde. Und auch die Umsetzung von IT-Sicherheitsrichtlinien (Policy Enforcement) lässt sich mit einem solchen Lösungsansatz nur schwer realisieren. Aus diesen Gründen schneiden Remote-Zugänge mittels IPSec-VPNs durch ihre hohen Gesamtkosten oftmals nur unbefriedigend ab.

**SSL-VPNS: APPLICATION GATEWAYS FÜR UNTERNEHMEN** Das moderne Unternehmensnetz unterliegt dynamischen Veränderungen. So ist es unvermeidlich, dass geschäftliche Kooperationen eine Vielzahl von Anwendungen für die Nutzergemeinschaft hervorbringen. Folglich findet sich heute in den Rechenzentren, die oft historisch gewachsen sind, eine stattliche Zahl von Anwendungen auf Windows Terminalserver-, Unix-/Linux-Systemen oder Mainframes aber auch Netzanwendungen auf Intranetservern.

Das Erschließen einer so komplexen Umgebung für Partnerunternehmen, Zulieferer und Angestellte bei gleichzeitiger Erfüllung der Anforderungen der Sicherheitsrichtlinien, ist eine der großen Herausforderungen erfolgreicher Remote-Zugangslösungen.

Heutige SSL-VPNs lösen diese Anforderungen durch die Konsolidierung von drei

verschiedenen Zugangstechnologien in nur einem Application-Layer-Gateway:

- Client-loser, Browser-basierter Zugriff auf Remote Legacy Applications,
- Secure Intranet Access auf webbasierte Anwendungen und Portale und
- Desktop Access für Client-/Server-Anwendungen über SSL-Tunnel.

### CLIENT-LOSER ZUGRIFF AUF LEGACY APPLICATIONS

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 doch die gleichen On-Demand-Zugangsverfahren für alle Anwendungen zum Einsatz kommen.

Führende Hersteller von SSL-VPN-Appliances lösen dieses Dilemma, indem sie Client-losen Fernzugriff auf Legacy Applications durch eine direkte Implementierung von Web-enabling-Technologien auf der Systemplattform realisieren. Dieser integrierte Ansatz beseitigt die Notwendigkeit für die Unternehmen, serverbasierte Middleware und die zugehörigen Remote-Access-Clients installieren und betreiben zu müssen. In einem solchen Modell werden sowohl die Client- als auch die Serverelemente einer Anwendung zentral im Rechenzentrum des Unternehmens gehostet. Der Vorteil dieses Ansatzes liegt darin, 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-/Server-Anwendungen für Remote-Benutzer durch das Netz zugänglich und erlaubt Firmen, ihre vorhandenen Legacy-Applications weiterhin einzusetzen, ohne diese teuer neu programmieren zu müssen. Nahezu jedes Programm auf jeder heute üblichen Plattform – sei es Windows, Unix, Linux oder 3270-Mainframe beziehungsweise 5250-AS/400 – lässt sich folglich für Remote-Anwender leicht zur Verfügung stellen.

In diesem Application-Layer-Zugangsmodell verwendet das SSL-VPN-Gateway ein so genanntes "Screen-Scraping Protocol", das Emulation und Display-Processing aufspaltet, sodass lediglich eine Übertragung der Darstellung der Anwendung zum Webbrowser des Remote-Benutzers erfolgt. Das Gateway unterstützt diese Fähigkeit durch ein Java-Applet, welches beim ersten Benutzer-Login automatisch im Hintergrund heruntergeladen und installiert wird. Im Ergebnis kann der Anwender die Applikation selbst über etwas schmalbandigere Verbindungen mit der gewohnten Geschwindigkeit bedienen, im Idealfall so, als ob die Anwendung auf der lokalen Maschine des Benutzers ausgeführt würde.

### SICHERER INTRANET-ACCESS AUF WEBBASIERTE APPLIKATIONEN

Auch wenn Unternehmen an ihren Legacy-Applikationen als Teil ihrer Anwendungsstrategie festhalten, kommen sie oft kaum umhin, Browser-basierten Webzugriff auf Anwendungen zu ermöglichen. Natürlich lassen sich auch Applikationen wie beispielsweise Microsofts Exchange Server oder proprietäre Intranetanwendungen webfähig machen. Die Bereitstellung solcher Informationen über das Web kann jedoch zu ernsthaften Sicherheitsrisiken führen, die sorgfältig zu prüfen sind.

In jedem Fall stellt die Bereitstellung von Webzugriff auf interne Anwendungen bei gleichzeitiger Erweiterung des Nutzerkreises für IT-Abteilungen und sonstige Verantwortliche eine Herausforderung dar. Dies beginnt beispielsweise damit, dass viele Anwendungen im geschützten Intranet des Unternehmens gehostet werden und für die Host-Namenauflösung 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 durch das zur Verfügung stellen von Intranetressourcen über SSL-Tunnel nur für autorisierte Anwender. Dies läuft durch Client-losen, Browser-basierten Zugriff auf webbasierte Ressourcen unter Verwendung der HTTP-Reverse-Proxy-Technologie.

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-User im Internet und der Enterprise-Website dar. Den "Single Point of Entry" über das Internet bildet dann das SSL-VPN-Gateway, über welches der Remote-Anwender mithilfe seines Browsers gesichert auf Webserver im Backend zugreifen kann. Eine solche Architektur ermöglicht schnellen, sicheren und bedarfsweisen Zugriff auf webbasierte Informationen und ist zudem skalierbar, falls die Zahl der zu autorisierenden Nutzer rasch ansteigen sollte.

Darüber hinaus liegen die Sicherheitsvorteile auf Basis eines SSL-VPN-Gateway klar auf der Hand: Die Webserver des Unternehmens bleiben im von der Firewall gesicherten privaten Netzbereich, und es entstehen keine Zusatzkosten, etwa für aufwändiges Server-Hardening und Maintenance, weil öffentliche Zugriffe von vornherein vermieden werden. Zusätzlich setzen die Administratoren die Sicherheitsrichtlinien mittels Zugriffskontrolle auf Verzeichnisse, Server, Pfade und Benutzergruppen wesentlich feiner um.

### CLIENT-/SERVER-ANWENDUNGEN ÜBER SSL-TUNNEL

Die beiden oben beschriebenen Client-losen Remote-Access-Methoden erfüllen die Anforderungen der meisten Fernanwender. Zusätzlich besteht oft die Forderung, lokal ins-

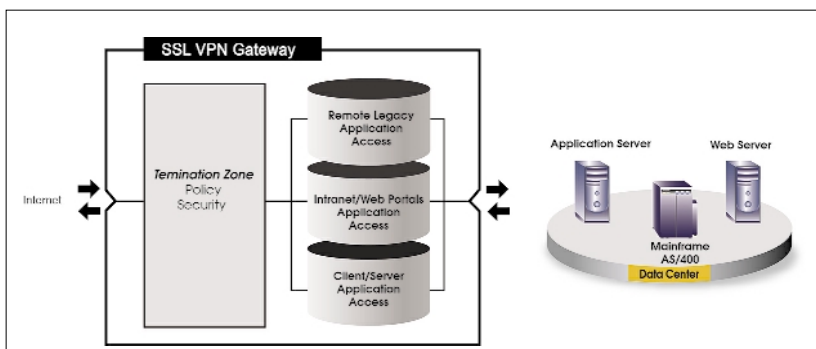


Bild 1. Funktion eines SSL-VPN-Gateways

Server-Anwendungen wie zum Beispiel E-Mail-Programme zu nutzen. Typischerweise erfolgt dann der Datenaustausch zwischen der lokal installierten Anwendung und dem Server im Backend, parallel zur Offlinenutzung (ein Beispiel dafür sind Microsofts Outlook Client und der Exchange Server für E-Mail). Auch solche Szenarien, in denen bisher in der Regel Network-Layer-VPNs à la IPSec zum Einsatz kamen, lassen sich mit SSL-Tunneling sicher realisieren, allerdings nur mit Anwendungen, die das jeweilige SSL-Gateway unterstützt.

Typischerweise verwirklichen die SSL-VPN-Gateways den Zugriff auf Desktop-Anwendungen via SSL-Tunnel mithilfe eines VPN-Plug-ins, das auf den lokalen Rechner heruntergeladen und installiert wird, wenn sich der Anwender zum ersten Mal erfolgreich am Remote-Access-System anmeldet. Der virtuelle Adapter baut danach einen sicheren SSL-Tunnel via Webbrowser auf. Anpassungen an den Client-/Server-Anwendungen selbst sind dabei nicht erforderlich. Sobald der Netzwerkadministrator einen Anwender für bestimmte Applikationen autorisiert hat, kann dieser Benutzer darauf über den SSL-Tunnel zugreifen, 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 klassischen IPSec-VPNs mit sich.

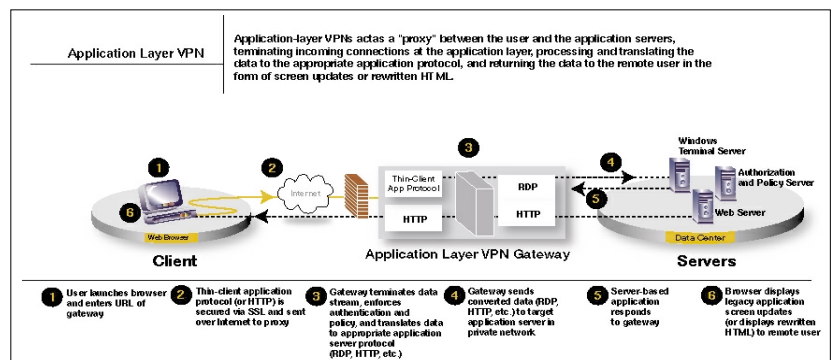
**POLICY UND NETWORK SECURITY: DER APPLICATION LAYER PROXY** Beim Bereitstellen Client-loser Zugriffe auf Legacy Applications und der Nutzung als HTTP-Reverse-Proxy für Webanwendungen werden die umfangreichen Zugriffsmöglichkeiten auf Applikationen deutlich. So gesehen sind SSL-VPN-Gateways gleichzusetzen mit einem echten Application-Layer-Proxy.

SSL-VPNs arbeiten auf Schicht 7 des OSI-Layer-Modells, also der Anwendungsschicht. Im Vergleich dazu arbeiten IPSec-VPNs auf Netzwerkebene, also Schicht 3. Aus dieser Tatsache ergibt sich für den Administrator der Vorteil, dass SSL-VPN-Gateways Anwendungsdaten interpretieren können und sich somit die Umsetzung von Sicherheitsrichtlinien auf Anwendungsebene erzwingen lässt. Damit wird

es möglich, an zentraler Stelle dynamische Zugriffsregeln auf Anwendungen im Kontext des jeweiligen Benutzers festzulegen.

In Bild 2 ist dargestellt, wie das SSL-VPN-Gateway interne Ressourcen effizient schützt, indem es in den Datenstrom von Remote-Client und serverbasierter Anwendung geschaltet wird und eingehende Verbindungen des Remote-Users auf Anwendungsebene terminiert. Sobald die eingehende Verbindung terminiert ist, baut die Appliance – für den Nutzer völlig transparent – eine interne Verbindung zum Backend-Server auf

direkt an den Anwendungsserver im privaten Netz gesendet werden. Stattdessen erfolgt immer eine Terminierung am SSL-VPN-Gateway mit anschließender Auswertung durch das Gateway anhand der Policy und einer Weiterleitung im jeweiligen Format zum entsprechenden Anwendungsserver über eine zweite interne Verbindung. Folglich erzwingt das Gateway die Nutzerauthentisierung und prüft die Policy vor der Weiterleitung des Datenstroms an den Anwendungsserver. Dieses Vorgehen schützt die Ressourcen im privaten Netz



**Bild 2. Das SSL-Gateway schützt interne Ressourcen durch das Terminieren eingehender Verbindungen auf Anwendungsebene**

und übersetzt die Anfrage in das entsprechende Format wie etwa:

- Remote Desktop Protocol (RDP) für Windows-Anwendungen auf einem Windows Terminal Server (TES),
- X.11 über SSH für Unix- und Linux-Applikationen,
- 3270-Emulation über Telnet für Mainframe- und AS/400-Anwendungen und
- HTTP/HTTPS für Webserver.

**TERMINIERUNGSVORTEIL POLICY ENFORCEMENT** Wie bei jedem Application-Proxy ermöglicht die "Terminierungslücke", also die Lücke zwischen Terminierung der eingehenden Verbindung und Weiterleitung der Anfrage im angepassten Format auch bei einem SSL-VPN-Gateway das Abfragen externer Authentisierungs- und Policy-Server. So lassen sich auf einfache Weise bestehende Active-Directory- oder Lightweight-Directory-Access-Protocol-Server (LDAP), auf denen Benutzerkennungen und Credentials bereits angelegt sind, auch für die Autorisierung der Zugriffe auf Anwendungen nutzen.

Ein Application-Layer-VPN funktioniert also so, dass die Nutzermeldungen niemals

auf deutlich effektivere Art als herkömmliche Remote-Access-Lösungen.

**FAZIT** Sicherheit stellt einen Eckpfeiler jeder Remote-Access-Implementierung dar, und eine gute Sicherheitslösung sollte dabei gleichzeitig auch eine einfach zu betriebsunterbrechungen der existierenden Anwendungsserver und Sicherheitsmechanismen.

Die aktuell verfügbaren SSL-VPN-Gateways führender Hersteller vereinigen alle wesentlichen Sicherheitsfunktionen in einer integrierten, gehärteten Appliance, das heißt, Authentisierung, Policy Enforcement und Verschlüsselung werden in einer Systemplattform gebündelt, was eine schnelle Integration ermöglicht. Damit erhält der Kunde eine einfach zu betriebsunterbrechungen und wartungsarme VPN-Lösung.

(Ken Araujo/gg)

Ken Araujo ist Chief Technology Officer und Senior Vice President of Engineering bei Netilla Networks.