

## Hintergrund

# SSL-VPN: Einfach und sicher

Die zunehmend beliebten SSL-VPNs bieten dank der Implementation im Applikations-Layer verschiedene Vorteile gegenüber den traditionellen, auf IPSec basierenden Lösungen.

Sichere Netzwerkverbindungen über die Firewall hinaus werden traditionell mit VPNs (virtuellen privaten Netzwerken) aufgebaut – und als einzig wahre Lösung stand diesbezüglich die VPN-Technologie per IPSec im Vordergrund. Die IPSec-VPNs boten gegenüber klassischen Datenübertragungstechniken wie Mietleitungen, ATM oder Frame Relay nicht nur eine hohe Sicherheit, sondern waren insbesondere wesentlich kostengünstiger zu implementieren.

In Zeiten der wachsenden Nutzung von Extranets durch externe Mitarbeiter und Partnerfirmen, flexibler Arbeitsformen und verschärfter Datenschutzgesetze genügen die Möglichkeiten der IPSec-VPNs den Anforderungen allerdings nicht mehr. Die Systeme verursachen beispielsweise durch Installation und Konfiguration von Clients auf den Rechnern der Remote-Anwender einen nicht zu unterschätzenden Wartungs- und Kostenaufwand. Ausserdem sind sie in bestehende Sicherheitsrichtlinien nur schwer einzufügen, und weil sie auf Netzwerkebene laufen, erlauben sie einen kompletten Einblick ins Gastnetzwerk, der in den meisten Fällen aus Sicherheitsgründen unerwünscht ist – das Policy Enforcement wird dadurch zusätzlich erschwert.

## Client-loser Zugriff auf Legacy-Anwendungen

Eine Lösung für einen grossen Teil dieser Probleme bilden die SSL-VPNs (Secure Socket Layer), die in jüngster Zeit einen grossen Popularitätsschub im Remote-Access-Markt erfahren haben. Die Technologie vereint in einem Application-Layer-Gateway den Client-losen, browserbasierten Zugriff auf Remote-Legacy-Anwendungen, den sicheren Zugriff auf webbasierte Anwendungen und Portale sowie den Desktop-Access über SSL-Tunnel. Damit lässt sich die historisch gewachsene Vielfalt von Anwendungen auf Terminalservern, Unix-

Systemen und Mainframes, wie sie heute in vielen Rechenzentren existiert, problemlos sowohl für Partner als auch für Zulieferer und eigene Angestellte öffnen, während gleichzeitig die Anforderungen der Sicherheitsrichtlinien adäquat umgesetzt werden können.

Für den Client-losen Fernzugriff auf Legacy-Anwendungen werden web-enabling-Technologien direkt auf der Systemplattform dieser Applikationen implementiert; serverseitige Middleware mitsamt den nötigen Remote-Access-Clients entfallen ebenso wie die aufwendige Wartung der Clients, da der Zugriff über einen normalen Browser sowie beim ersten Zugriff automatisch installierte Java- und ActiveX-Applets erfolgt. Übertragen wird dabei dank eines "Screen-Scraping-Protocol", das Emulation und Display Processing aufsplittet, nur die Darstellung der Anwendung, was auch eine hohe Performance der Remote-Anwendung garantiert.

Ähnlich erfolgt auch der Zugriff per Browser auf webbasierte Anwendungen und Portale. Die Intranet-Ressourcen werden über einen SSL-Tunnel mit Reverse-Proxy-Technologie ausschliesslich autorisierten Anwendern zur Verfügung gestellt. Die Lösung ist nicht nur skalierbar, sondern bietet auch eine hohe Sicherheit; der Webserver bleibt geschützt in der DMZ hinter der Firewall, und Sicherheitsrichtlinien lassen sich fein verästelt für Verzeichnisse, Server oder einzelnen Benutzer definieren.

## Zahlreiche Vorteile

Der Zugriff auf Anwendungen über wartungsarme Java- oder ActiveX-Applets, die bei der ersten Anmeldung automatisch heruntergeladen und installiert werden und darauf den sicheren SSL-Tunnel via Webbrowser aufbauen, bietet verschiedene Vorteile gegenüber klassischen IPSec-Lösungen: Die Authentifizierung und Autorisierung sind wesentlich weniger aufwendig, und da der gesamte Verkehr

über einen einzigen Port (554 für SSL) läuft, der im allgemeinen eh geöffnet ist, sind Änderungen an der Firewall unnötig, was die Komplexität reduziert. Dank bei der Anmeldung automatisch erzeugter Security Tokens entfällt auch die Installation und Wartung von Schlüsseln und Zertifikaten. Die Sicherheit bleibt dennoch hoch, da die meisten aktuellen Browser mit 128-Bit-Verschlüsselung umgehen können, die zum heutigen Stand der Technik als ausreichend sicher gilt.

Zudem profitiert ein SSL-VPN von der Trennung zwischen dem Datenstrom vom Remote Client und der serverbasierten Anwendung, die durch die Implementierung der Technologie auf Anwendungs- statt auf Netzwerk-Ebene ermöglicht wird. Erst wenn die eingehende Verbindung terminiert ist, baut die Appliance die Verbindung zum Server auf und übersetzt die Anfrage ins passende Format. Durch die so entstehende "Terminierungslücke" ist es möglich, die Authentifizierung und die Durchsetzung von Sicherheits-Policies zu erzwingen: erst nach erfolgreicher Prüfung wird die Anfrage weitergeleitet. Dadurch lassen sich die Ressourcen im privaten Netz effektiver schützen als bei herkömmlichen Lösungen.

## Gute Prognosen

Nachdem in jüngster Zeit auch grosse Hersteller wie Cisco, Nokia

und Nortel auf den SSL-VPN-Zug aufgesprungen sind, stellen die Analysten der Technologie hervorragende Prognosen; so ist etwa die MetaGroup der Meinung, dass bereits 2004 ein Drittel der Unternehmen SSL-basierte Remote-Access-Technologien in Kombination mit IPSec-VPNs nutzen werden, und 2006 sollen über 80 Prozent aller Anwender die SSL-Technologie bevorzugen. Ähnliche Voraussagen wagt auch die Tolly Group: Laut einer aktuellen Umfrage der Marktforscher gehen über 75 Prozent der Befragten davon aus, dass SSL-VPNs die traditionellen IPSec-VPNs zumindest im Bereich Remote Access bereits in den kommenden zwei Jahren vollständig verdrängen werden.

Ob diese komplette Verdrängung der klassischen IPSec-Lösungen durch die SSL-VPNs stattfinden wird, ist allerdings nicht so sicher. Die althergebrachten IPSec-VPNs haben bei Site-to-Site-Verbindungen noch immer die Nase vorn und bieten maximale Sicherheit auf Netzwerk-Ebene; die flexiblen und einfach zu implementierenden SSL-VPNs, die einen geringen Wartungsaufwand verursachen und simpel zu bedienen sind, bilden dagegen eine optimale Ergänzung. In Enterprise-Architekturen werden die beiden Access-Technologien deshalb auf absehbare Zeit koexistieren. (mva)

## Ausgewählte Anbieter von SSL-VPN-Gateways

Anbieter	URL	SSL	IPSec
Aspelle	www.aspelle.com	■	□
Aventail	www.aventail.com	■	□
Checkpoint	www.checkpoint.com	■	■
Cisco	www.cisco.com	■	■
Citrix	www.citrix.com	■	□
Netilla	www.netilla.com	■	□
Netscreen	www.netscreen.com	■	■
Nokia	www.nokia.com	■	■
Nortel	www.nortel.com	■	■
Rainbow	www.rainbow.com	■	■
uRoam	www.uroam.com	■	□
Whale Communications	www.whale.com	■	□

■ = ja, □ = nein