SSL-VPN versus IPSec

Von Dominic Haussmann

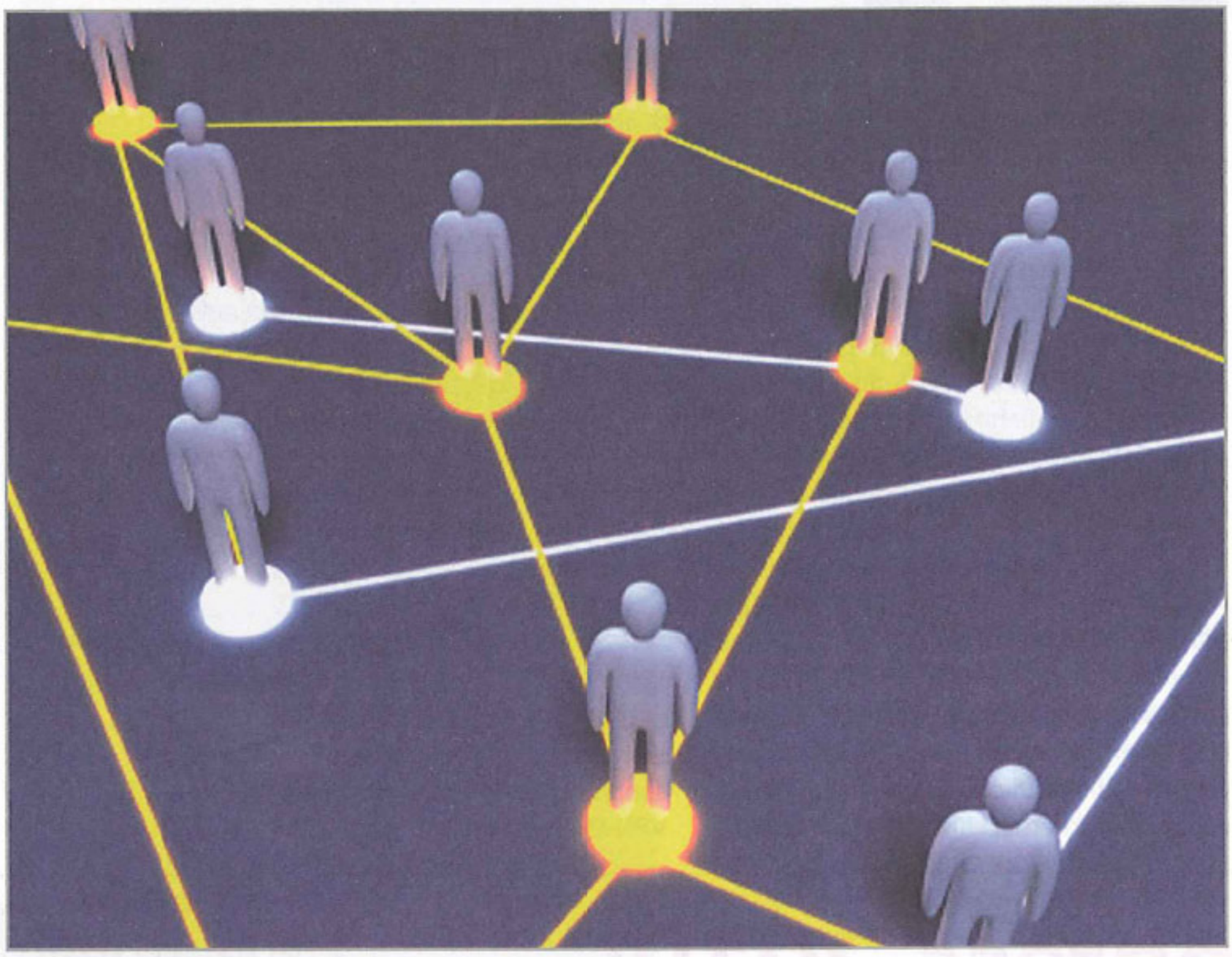

Bild: fotolia.com

Der Markt verlangt heute nach VPN-Lösungen, die es Außendienstmitarbeitern ermöglichen, einfach und sicher auf die Ressourcen im Unternehmensnetzwerk zuzugreifen. Zwei Technologien haben sich hierbei in den letzten Jahren etabliert: SSL-VPN und IPSec. Eine Diskussion der Vor- und Nachteile.

IPSec: Komplexer Alleskönner

IPSec (Internet Protocol Security) arbeitet auf der Netzebene des OSI-Modells und sichert dabei alle Daten, die zwischen den zwei Endpunkten – ohne Zuordnung zu einer bestimmten Anwendung – übertragen werden. Wenn ein Client-Computer mit einem IPSec-VPN verbunden ist, ist er quasi ein Vollmitglied des Firmennetzes. Das bedeutet, dass der Client-Rechner das gesamte Netzwerk sehen und auf den Inhalt direkt zugreifen kann. Für Unternehmen ist dies eine unkomplizierte Variante – weshalb IPSec am Markt als Standard etabliert ist und in verschiedenen Varianten angeboten wird.

Um auf ein IPSec-VPN zuzugreifen, muss auf dem betreffenden Gerät eine Client-Software-Anwendung installiert sein. Das ist sowohl ein Vorteil als auch ein Nachteil. Der Vorteil ist, dass durch eine zusätzliche Software ausschließlich Client-Rechner zugreifen können, die über die richtige Software sowie Konfiguration verfügen.

Dies spiegelt aber zugleich den größten Nachteil von IPSec-VPNs wider: Nur durch eine komplexe Installation, die meist Administrationsrechte benötigt, ist ein Zugriff auf das Unternehmensnetzwerk möglich. Ein weiterer Nachteil ist, dass eine IPSec-Kommunikation über Router oder Firewall geschützte Netzwerke oft nicht gegeben ist, da in diesem Fall eine spezielle Konfiguration notwendig ist.

SSL-VPN: Simpel und schrankenlos

Es ist dieser Nachteil des IPSec-VPN, der im Allgemeinen als einer der größten Vorteile für konkurrierende SSL-VPN-Lösungen (Secure Socket Layer) gewertet wird.

SSL ist ein weit verbreitetes Protokoll, das heute in allen Web-Browsern integriert ist. Dadurch ist fast jeder Rechner bereits mit der notwendigen Client-Software versorgt, um eine Verbindung mittels SSL-VPN aufzubauen. Grundsätzlich unterscheidet man hier zwischen zwei verschiedenen Kommunikationswegen – dem Clientless-Zugriff und den Zugriff mittels eines Clients.

Der Clientless-Zugriff bezieht sich in erster Linie auf Web-Applikationen, die über HTTPS im internen, gesicherten Netzwerk bereitgestellt werden. Der Zugriff von extern erfolgt – gesichert mit SSL-VPN – direkt über den Browser. Hierbei muss der Benutzer keinerlei zusätzliche Software installieren. Die Verbindung wird wieder beendet, sobald der Browser geschlossen wird.

Beim Client-basierten Zugriff lädt der externe Benutzer meist eine Java oder ActiveX-basierte Applikation herunter, die sich grundsätzlich ohne Administrationsrechte ausführen lässt. Diese Applikation stellt dann die netzwerkseitige Verbindung in das Firmennetz her. Neben den nicht benötigten Rechten auf dem Client, kommt hier ein weiterer Vorteil von SSL-VPN zum Tragen. Der Client baut die Verbindung über den Standard-Port für SSL her – Port 443. Dadurch ergeben sich – anders als bei IPsec – keine Probleme bei Verbindungen über Firewalls oder Router, da SSL- und HTTPS-Kommunikation immer freigegeben sein sollte. Somit ist ein flexibler Zugriff von so gut wie jedem Standort mit dem Client möglich. Ebenfalls gelöst ist das Problem der Client-Installation. Da er in der Regel mittels ActiveX oder Java vom Browser bereitgestellt wird, sind mühsamer Rollout und Konfiguration eines IPSec-Clients nicht mehr notwendig.

Eine Frage der Sicherheit

Sowohl für IPSec als auch für SSL wird die Sicherheit der VPN-Verbindung wesentlich durch die erste Authentifizierung bestimmt. Zur Basisinstallation sollte generell

ein System zur Abwehr von DoS- und DDos (Denial of Service/ Distributed Denial of Service)-Attacken auf dem zentralen Zugangssystem gehören. Daneben gilt: Egal ob über einen Client oder über einen Browser – ein guter Nutzername und ein starkes Passwort sind entscheidend.

„Brute Force"-Angriffe, auch „Dictionary-Attacken" genannt, können andernfalls diese erste, wesentliche Hürde leicht überbrücken. Anders als IPSec tragen viele SSL-VPN-Systeme zu einer starken Authentifizierung bei. Sie bieten eine One-Time-Passwort (OTP)- oder Token-Lösung, ohne die der Zugriff auf das jeweilige Unternehmensnetzwerk nicht möglich ist. Die Authentifizierung und Autorisierung muss hier mit in die Security Policy einfließen. Das OTP kann sich der Benutzer mittels Software-Token oder SMS erstellen lassen.

Tunnelbau

Nach der ersten Phase der Vertrauensherstellung folgt der Aufbau eines Tunnels zum Unternehmensnetzwerk. Hier lassen sich die Zugriffsrechte bei SSL-VPN sehr viel feiner definieren, so dass der Zugriff auf Informationen besser an die Security Policy des Unternehmens angepasst werden kann, als es bei IPSec der Fall ist. Während bei IPSec nur die Firewall und damit der allgemeine Netzwerk-Traffic konfiguriert werden, bieten SSL-VPN-Lösungen den Administratoren eine dedizierte, rollenbasierte Zugriffskontrolle.

Auch IPSec kann anwendungsbezogen installiert werden, so dass der Tunnel nicht bei jeder Verbindung mit dem Client vollständig geöffnet ist. Mit anderen Worten lassen sich die Anwendungen, die über die Remote-Verbindung zugängig sind, je nach Bedarf beschränken. Jedoch ist hier die Sensibilisierung und Schulung der Außendienstmitarbeiter gefragt, welche diese Einstellungen selbst bestimmen.

Neben der Authentifizierung steht vor allem das Endgerät selbst im Fokus. Manche SSL-VPN-Lösungen können einen so genannten „Endpoint Security Check" durchführen, der den Client auf Viren-Scanner, Desktop-Firewall sowie Antispyware hin untersuchen. Hierbei wird zum einen geprüft, ob ein definierter Viren-Scanner aktiv ist und ob dieser aktuelle Definitionen enthält. Auch weitere Überprüfungen des Clients sind möglich – wie Rechnername, Betriebssystem und vieles mehr.

Welche Lösung für wen?

Es gilt, die oft geführte Sicherheitsdebatte rund um IPSec und SSL-VPN differenzierter zu betrachten. Denn im Grunde verwenden beide die gleichen Algorithmen, bieten Authentifizierung und eine Verschlüsselung beim Datenaustausch. Damit ist jedoch unter Security-Aspekten nur ein Basisschutz gegeben. Wird hingegen eine vielschichtige Sicherheitsarchitektur benötigt, so stoßen Firmen mit IPSec rasch an ihre Grenzen.

In der heutigen Zeit nehmen Sicherheitsbedrohungen rasant zu und ein einziger, mit Malware infizierter Computer kann in einem Netzwerk im Handumdrehen einen enormen Schaden anrichten. SSL-VPN ist hier das Mittel der Wahl. Administratoren können mit diesen Lösungen den Zugriff auf Unternehmensnetze sehr viel feiner steuern und regeln. Des Weiteren lässt sich eine SSL-VPN-Lösung besser an End-User verteilen als es bei IPSec der Fall wäre.

Bei der Auswahl einer geeigneten SSL-VPN-Lösung sind verschiedene Faktoren ausschlaggebend. Etablierte Anbieter am Markt sind beispielsweise Watchguard Technologies oder Sonicwall. Sie richten sich mit ihren Produkten überwiegend an kleine und mittelständische Unternehmen. Sie erhalten Lösungen, die unmittelbar auf ihre Anforderungen zugeschnitten und beispielsweise auch im Bezug auf das Management einfach zu handhaben sind. Ein anderer bekannter Hersteller ist Juniper. Die Produkte dieses Anbieters sind eher für größere Installationen vorgesehen – dementsprechend umfangreich ist auch die Palette der Funktionen.

Neben dem Funktionsumfang spielt selbstverständlich der Preis eine entscheidende Rolle. Um die teilweise hoch komplexen Möglichkeiten einer Juniper-Lösung auszuschöpfen, ist oft die Anschaffung weiterer Hard- und Software – wie beispielsweise Server oder Lizenzen – unumgänglich. Diese zusätzlichen Investitionen können sich leicht auf dieselbe Summe belaufen, die bereits das eigentliche SSL-VPN-Produkt gekostet hat.

Ein Anbieter wie Watchguard hingegen stellt eine Lösung „out of the box" bereit. Hier sind umfassende Funktionen schon integriert – wie etwa Endpoint Security oder erweiterte Sicherheit durch Einmal-Passwörter, die per SMS auf das Handy zugeschickt werden.

Ein solches Appliance-Produkt ist schnell in Betrieb genommen. Fällt die Wahl auf eine Stand-alone-Lösung, so sollte unbedingt darauf geachtet werden, dass sie mit den im Unternehmensnetz bereits vorhandenen Systemen kompatibel ist. So lassen sich bereits vorhandene Zertifikate weiter nutzen oder eine bestehende Authentifizierungs-Software integrieren. *(CR)*

funkschau Expertenkommentar

Bild: Watchguard

Michael Haas, Regional Sales Manager D-A-C-H bei Watchguard Technologies.

Sicher, flexibel, günstig

„Unser Ziel ist es, den Spagat zu schaffen zwischen höchstmöglicher Sicherheit und Flexibilität, einer einfachen Handhabung für maximale Produktivität sowie einem wettbewerbsfähigen Preis.

Die Watchguard SSL 100 ist eine dieser so genannten All-in-one-Lösungen. Bis zu 100 Verbindungen werden parallel unterstützt. Damit ist sie maßgeschneidert für die meisten KMUs, für die Mobilität der Schlüssel zum Erfolg ist. Die einfache Technik zur Authentifizierung macht den Einsatz von Dritt-Systemen wie LDAP *(Light Weight Directory Access Protocol, Anm.d.Red.)*, Active Directory oder Radius überflüssig. Durch Anwendungen wie SSH (Secure Shell) oder RDP (Remote Desktop) können mobile User aus aller Welt sicher auf Netzwerkapplikationen zugreifen. Darüber hinaus bietet die Watchguard SSL 100 einen Web-basierten Zugangsclient, der sich nach der erfolgreichen Authentifizierung selbst installiert. Dies ermöglicht einen raschen Zugriff auf Netzwerk-Ressourcen und die Vorinstallation von Clients auf den ‚Remote'-Geräten entfällt. Weiteren Schutz bietet die ausgefeilte Zwei-Wege-Authentifizierung, die Dritt-Software überflüssig macht.

Alle Funktionen der Watchguard SSL 100 sind ohne kostenpflichtige Erweiterungen oder Service-Verträge verfügbar." *(CR)*