SSL-VPN versus IPsec

Sicherer Fernzugriff

Der Markt verlangt heute nach VPN-Lösungen, mit denen Außendienstmitarbeiter einfach und vor allem sicher auf Ressourcen im Firmennetzwerk zugreifen können. Zwei Technologien haben sich hierbei in den letzten Jahren etabliert: SSL-VPN und IPsec (Internet Protocol Security). Eine Diskussion der jeweiligen Vor- und Nachteile.

IPsec arbeitet auf der Netzebene des OSI (Open Systems Interconnection)-Modells und sichert dabei alle Daten, die zwischen den zwei Endpunkten ohne eine Zuordnung zu einer bestimmten Anwendung übertragen werden. Wenn ein Client-Computer mit einem IPsec-VPN verbunden ist, ist er praktisch ein Vollmitglied des Firmennetzes. Der Client-Rechner kann das gesamte Netzwerk sehen und auf den Inhalt direkt zugreifen. Für Unternehmen ist dies eine unkomplizierte Variante und daher ist IPsec am Markt als Standard etabliert und wird in verschiedenen Varianten angeboten.

Um auf ein IPsec-VPN zuzugreifen, muss auf dem betreffenden Arbeitsplatzrechner oder auf dem Gerät eine IPsec-Client-Software installiert sein. Dies ist sowohl ein Vorteil als auch ein Nachteil. Der Vorteil ist, dass durch eine zusätzliche Software nur Client-Rechner zugreifen können, die über eine richtige Software sowie Konfiguration verfügen. Dies spiegelt aber zugleich auf 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 Kommunikation über IPsec über Router oder Firewall-geschützte Netzwerke oft nicht möglich ist, da hier eine spezielle Konfiguration notwendig ist. Es ist dieser Nachteil des IPsec-VPN, der im Allgemeinen als einer der größten Vorteile für konkurrierende SSL-VPN-Lösungen gewertet wird.

SSL – Secure Socket Layer

SSL ist ein weit verbreitetes Protokoll, welches 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. Im OSI-Modell ist SSL in Schicht 6 (der Darstellungsschicht) angeordnet. Im TCP/IP-Modell ist SSL oberhalb der Transportschicht (zum Beispiel TCP) und unterhalb von Anwendungsprotokollen wie HTTP oder SMTP angesiedelt. In den Spezifikationen wird dies dann zum Beispiel als „HTTP over SSL" bezeichnet. Sollen jedoch beide Protokolle zusammengefasst betrachtet werden, wird üblicherweise ein „S" für Secure dem Protokoll der Anwendungsschicht angehängt (zum Beispiel HTTPS). Seit Version 3.0 wird das SSL-Protokoll unter dem neuen Namen TLS weiterentwickelt und standardisiert, wobei Version 1.0 von TLS der Version 3.1 von SSL entspricht. Bei SSL-VPN unterscheidet man grundsätzlich zwischen zwei verschiedenen Kommunikationswegen: dem „ClientLess"-Zugriff und dem 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 hier – 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 zu tragen. Der Client baut die Verbindung über den StandardPort für SSL auf – Port 443. Dadurch ergeben sich, anders als bei IPsec, keine Probleme bei Verbindungen über Firewalls oder Router, da SSL beziehungsweise die HTTPS-Kommunikation immer freigegeben sein sollten. Somit ist ein flexibler Zugriff von nahezu jedem Standort mit dem Client möglich. Ebenfalls gelöst ist das Problem der Client-Installation. Da der Client in der Regel mittels ActiveX oder Java vom Browser bereitgestellt wird, sind ein mühsamer Rollout und die 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. 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 nämlich bei IPsec nur die Firewall und damit der allgemeine Netzwerk-Traffic konfiguriert werden kann, 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

Die WatchGuard SSL 100 ist eine dieser sogenannten ‚all-in-one'-Lösungen. Bis zu 100 parallele Verbindungen werden unterstützt. Die einfache Technik zur Authentifizierung macht den Einsatz von Dritt-Systemen wie LDAP, Active Directory oder RADIUS überflüssig. Alle Funktionen der SSL 100 sind ohne kostenpflichtige Erweiterungen oder Service-Verträge verfügbar." Foto: WatchGuard

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. Allzu oft spielen Nachlässigkeit und Bequemlichkeit eine wesentliche Rolle – auf Kosten der IT-Sicherheit.

Neben der Authentifizierung steht vor allem das Endgerät selbst im Fokus. Manche SSL-VPN-Lösungen können einen sogenannten „Endpoint Security Check" durchführen, der den Client auf Viren-Scanner, Desktop Firewall sowie Antispyware hin untersucht. Hierbei wird zum einen geprüft, ob zum Beispiel ein definierter Viren-Scanner vorhanden und 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?

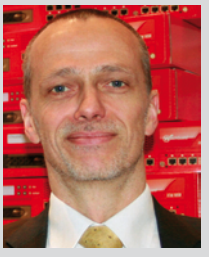
Es gilt, die oft geführte Sicherheitsdebatte rund um IPsec und SSL-VPN differenzierter zu betrachten. Denn im Grunde verwenden beide die gleichen Algorithmen, bieten Authentifizierung und eine Verschlüsselung beim Datenaustausch. Damit ist jedoch unter Security-Aspekten nur ein Basisschutz gegeben. Wird 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. Diese erhalten Lösungen, die unmittelbar auf ihre Anforderungen zugeschnitten und beispielsweise auch in Bezug auf das Management einfach zu handhaben sind. Ein anderer bekannter Hersteller ist Juniper. Die Produkte dieses Anbieters sind eher für größere Installationen vorgesehen und entsprechend umfangreich ist auch die Palette der Funktionen.

Neben dem Funktionsumfang spielt selbstverständlich der Preis eine entscheidende Rolle. Um beispielsweise die teils hochkomplexen Möglichkeiten einer High-End-Lösung auszuschöpfen, ist oft die Anschaffung weiterer Hard- und Software unumgänglich – etwa von Servern oder Lizenzen. Diese zusätzlichen Investitionen können sich leicht noch einmal auf dieselbe Summe belaufen, die bereits das eigentliche SSL-VPN-Produkt gekostet hat. Anbieter wie WatchGuard folgen dem Grundsatz, Lösungen „out of the box" bereitzustellen. Funktionen wie etwa Endpoint Security oder erweiterte Sicherheit durch Einmal-Passwörter, die per SMS zugeschickt werden, sind hier in der Regel bereits integriert.

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 oft bereits vorhandene Zertifikate weiter nutzen oder auch die bestehende Authentifizierungs-Software integrieren. ■

Anne Zozo,
Journalistin aus Ulm



Michael Haas,
Regional Sales Manager D-A-CH EE bei WatchGuard Technologies

Für Abonnenten ist dieser Artikel auch digital auf www.datakontext.com verfügbar

Weitere Artikel/News zum Schwerpunkt unter www.datakontext.com/mobile