
SSL-VPNs: Nun auch in Preis und Funktionsumfang mit KMUs kompatibel

Einleitung

Informationen sind das A und O eines jeden Unternehmens. Ohne zuverlässige, praktikable und sichere Methoden zum Austausch dieser Informationen mit den Benutzern können Unternehmen jedoch nicht effektiv arbeiten. In der Vergangenheit war der elektronische Informationsaustausch für viele Unternehmen völlig irrelevant, denn ihre Bedürfnisse konnten intern abgedeckt werden. Wichtig war lediglich, dass die Mitarbeiter von ihrem Standort und über ihren Desktop im Unternehmen Zugriff auf eine begrenzte Anzahl an Anwendungen hatten.

Heutzutage können sich die meisten Unternehmen (ob groß oder klein) kaum noch vorstellen, wie es war, in einer derart unkomplizierten Welt Geschäfte zu machen. Völlig unterschiedliche Benutzer, z. B. Mitarbeiter in verschiedenen Positionen, Lieferanten, Geschäftspartner und sogar Kunden, rund um die Uhr weltweit greifen über Internetverbindungen und über Computer, die nicht immer unternehmenseigen sind und auch nicht unbedingt vom Unternehmen verwaltet werden, auf Datenbanken, Dateiserver und Geschäftsanwendungen zu.

In dieser ressourcenintensiven, jederzeit und überall erreichbaren Umgebung werden Unternehmen mit komplexen technischen, administrativen und sicherheitsrelevanten Anforderungen konfrontiert. Großunternehmen mit internem IT-Personal und hohen IT-Budgets können sich diesen Anforderungen wesentlich leichter stellen als kleine und mittlere Unternehmen, in denen für den IT-Bereich geringere Ressourcen vorhanden sind. Nichtsdestotrotz können es sich KMUs nicht leisten, größeren Unternehmen in Punkto Informationszugriff nachzustehen.

Und das ist auch gar nicht nötig, denn nun gibt es SSL-VPN, eine neue Methode mit granularen Sicherheitsebenen zum zuverlässigen, einfachen und sicheren Aufbau einer Onlineverbindung mit beliebigen Benutzern an beliebigen Orten. Die bisher erhältlichen SSL-VPN-Lösungen wurden ausschließlich für Großunternehmen entwickelt, sodass ihre Funktionen und ihr Preis den Bedarf und die Mittel von kleinen und mittleren Unternehmen weit überstiegen. Das Angebot an neuen, speziell für kleine und mittlere Unternehmen konzipierten SSL-VPN-Produkten, bietet nun ganz andere Möglichkeiten.

In der vorliegenden Studie werden die Probleme diskutiert, die sich bei der derzeit gängigen Methode zur Unterstützung des Remotezugriffs über ein VPN, nämlich IPSec-VPNs, stellen. Im Anschluss daran erfahren Sie, wie diese Probleme durch ein SSL-VPN bewältigt werden können und wie Unternehmen durch den Fernzugriff mittels SSL-VPN auch Geschäftsvorteile realisieren. Durch Kombination der SSL-VPN- mit der IPSec-VPN-Technologie werden ferner alle Anforderungen von kleinen und mittleren Unternehmen für sichere Netzwerke unterstützt (siehe Abb. 1). Am Ende dieser Studie werden die Merkmale der neuen SSL-VPN-Appliances von SonicWALL vorgestellt und erläutert.

SSL-VPN und IPSec VPN

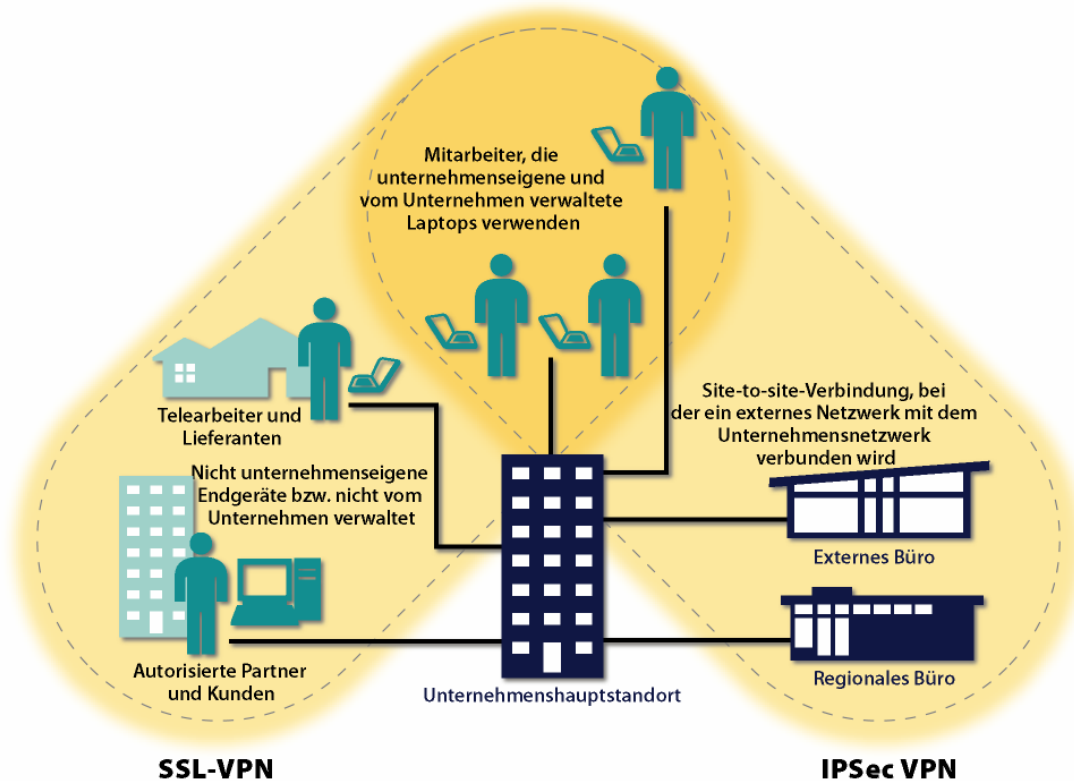


Abb. 1. Die Kombination aus SSL-VPN- und IPSec-VPN-Technologie unterstützt alle Anforderungen, die kleine und mittleren Unternehmen an sichere Netzwerke stellen

Ganz gleich, ob Ihr Unternehmen für den Remotezugriff bereits ein VPN nutzt (beispielsweise über ein IPSec-VPN) oder sich den wachsenden Anforderungen an den Remotezugriff (mehr Benutzer, Einhaltung von Auflagen) stellen muss: Sie können sich schon in kurzer Zeit die grundlegenden Informationen zum Verständnis von SSL-VPNs aneignen.

IPSec-VPNs: Eine gängige Methode mit uneinheitlichen Ergebnissen

Im Prinzip ist ein VPN (Virtual Private Network) ein Technologie-Set, das mithilfe eines verschlüsselten Tunnels eine private Verbindung über ein Kommunikationsnetzwerk zwischen zwei Parteien herstellen. In finanzieller Hinsicht können VPNs, die nicht über dedizierte oder private Netzwerke wie MPLS-, Frame Relay- oder ATM-Netzwerke für statische Verbindungen zwischen zwei oder mehreren Standorten, sondern über das öffentliche Internet bereitgestellt werden, zu beträchtlichen Kosteneinsparungen führen. Ein Teil des Kostenunterschiedes ist sicherlich auf die höheren Leistungsmerkmale dedizierter Netzwerke (z. B. Verfügbarkeit und Zuverlässigkeit) zurückzuführen.

Mit zunehmend besserer Internetleistung werden jedoch immer mehr internetbasierte VPNs für Site-to-Site-Verbindungen in Betrieb genommen. Dennoch werden internetbasierte VPNs weiterhin

hauptsächlich für den Remotezugriff, d. h. zum Aufbau einer Verbindung zwischen Offsite-Benutzern mit Onsite-Unternehmensressourcen genutzt. In diesem Fall profitieren die Remotebenutzer von der dynamischen Erstellung der VPN-Verbindung: Ihre Verbindungen sind meist nicht permanent (zB. müssen sie nicht ständig online sein) und ihr Ursprung ist nicht vorhersehbar. Da das Internet nahezu allgegenwärtig und von einem gemeinsamen Kommunikationsprotokoll abhängig ist, bietet es eine dauerhaft verfügbare Infrastruktur für Remoteverbindungen.

Heutzutage werden mehrere Arten von VPNs genutzt. IPSec- (Internet Protocol Security) VPNs (Internet Protocol Security) sind in Bezug auf unterstützte Verbindungen am weitesten verbreitet. Unabhängig davon, ob die Verbindungen zwischen entfernten Unternehmensstandorten oder mit Remotebenutzern hergestellt werden, funktioniert ein IPSec-VPN immer auf die gleiche Art und Weise: In jedem Fall wird in der Netzwerkschicht ein Tunnel über das Internet erstellt.

Diese Methode ist zwar effektiv, jedoch nur in dem Maße, wie der Anbieter des IPSec-VPN die administrative Kontrolle übernimmt. Und gerade letzteres ist nicht immer gewährleistet. Es gibt drei Bereiche, in denen die administrative Kontrolle notwendig ist, damit ein IPSec-VPN ordnungsgemäß funktioniert: (1) beim VPN-Gateway, (2) bei den Geräten der Remotebenutzer und (3) bei den Sicherheitsrichtlinien für die Appliances in der Netzwerkumgebung, die im Netzwerkverkehr zwischen dem Benutzergerät und dem VPN-Gateway integriert sind. Der Anbieter des IPSec-VPNs übernimmt die gesamte administrative Kontrolle des VPN-Gateways. Dies gilt jedoch nicht ohne Weiteres für jedes für den Remotezugriff genutzte Gerät bzw. für die im VPN-Netzwerkverkehr integrierten Sicherheits-Appliances der Netzwerkumgebung. Da die administrative Kontrolle also nicht für die gesamte Verbindung gilt, ist ein IPSec-VPN für den Remotezugriff nur begrenzt anwendbar und mögliche Geschäftsvorteile können nicht voll ausgeschöpft werden. In der nachstehenden Tabelle sind mögliche Auswirkungen für ein Unternehmen aufgeführt, wenn die administrative Kontrolle für Benutzergeräte und Sicherheits-Appliances in der Netzwerkumgebung fehlt.

| Administrative Anforderungen an ein IPSec-VPN | Auswirkungen bei Fehlen der administrativen Kontrolle |
|--|--|
| <p>Installation eines VPN-Softwareclients</p> <p>Für den Remotezugriff muss auf jedem hierfür genutzten Gerät ein mit dem VPN-Gateway kompatibler IPSec-VPN-Softwareclient installiert werden. Wie bei den meisten Softwareinstallationen kann diese Aufgabe nur von einem Benutzer mit Administratorenrechten ausgeführt werden.</p> | <p>Hiervon können zwei Gruppen von VPN-Benutzern betroffen sein:</p> <p>Lieferanten und Geschäftspartner: Hier liegt die administrative Kontrolle über die Benutzergeräte bei den jeweiligen IT-Abteilungen. Diese können verhindern, dass auf den Benutzergeräten zusätzliche Software installiert wird, ohne die der Zugriff auf das VPN-Hostnetzwerk nicht möglich ist. Diese möglichen Benutzer können daher nicht mit den unternehmenseigenen Geräten Teil des VPNs werden, so lange die jeweiligen IT-Abteilungen diese Einschränkung nicht aufheben. Je mehr Lieferanten und Geschäftspartnern auf diese Weise daran gehindert werden, Teil des VPNs zu werden, desto schwerer wiegt dieser Nachteil eines IPSec-VPN. Aber auch wenn diese Hürde überwunden wurde, besteht das Risiko, dass mehrere, auf dem gleichen Gerät installierte IPSec-VPN-Clients (beispielsweise wenn ein Lieferant mehreren VPNs angehört) miteinander in Konflikt treten.</p> <p>Mitarbeiter, die vom Home Office auf das Unternehmensnetzwerk zugreifen: Mitarbeiter haben in der Regel Administratorenrechte für den eigenen Computer und sind wahrscheinlich mit der Installation neuer Software einverstanden, die den Zugriff auf Unternehmensressourcen ermöglicht. In vielen Fällen sind es jedoch die IT-Abteilungen, die damit zögern, allen Mitarbeitern den VPN-Zugriff zu ermöglichen. Diese zögernde Haltung ist darauf zurückzuführen, dass die unterschiedlichen Computerumgebungen (d. h. die Betriebssysteme und ihre Versionen, die Hersteller und die auf den Computern ausgeführten Anwendungen) Kompatibilitätsprobleme mit dem VPN-Softwareclient mit sich bringen, eine Ausweitung des IT-Supports auf nicht unternehmenseigene Geräte erforderlich machen und eine erhöhte Anzahl von Anrufen beim Helpdesk auslösen. All dies führt beim Unternehmen zu höheren IT-Kosten.</p> |
| <p>Kontrolle der Firewallrichtlinie</p> <p>IPSec-VPNs erstellen zwischen den Kommunikationspartnern eine Verbindung über die Netzwerkschicht. Dies ist allerdings nur möglich, wenn die Konfiguration der Sicherheits-Appliances der Netzwerkumgebung eine vorübergehende Verbindung mit externen Netzwerken zulässt.</p> | <p>Remotezugriff: Um eine IPSec-VPN-Verbindung über ein Gastnetzwerk herzustellen (wenn ein Mitarbeiter beispielsweise remote eine Verbindung mit einem verfügbaren Netzwerkanschluss in einem Gastnetzwerk herstellt), muss ein Firewallport in der Umgebung des Gastnetzwerks geöffnet werden, damit der IPSec-VPN-Tunnel zum VPN-Hostnetzwerk erstellt werden kann. Auch das zeitweilige Öffnen von Firewallports legt einen Angriffspunkt bloß, über den Bedrohungen der Netzwerkschicht vom VPN-Hostnetzwerk in das Gastnetzwerk und umgekehrt gelangen können. Da Sicherheit heute groß geschrieben wird, sind die IT-Administratoren eines Gastnetzwerks nur ungern bereit, die Firewallrichtlinien für sporadische Verbindungen mit externen Netzwerken anzupassen. Daher ist nicht immer garantiert, dass Mitarbeiter remote über ein Gastnetzwerk auf ein IPSec-VPN zugreifen können. Ihnen wird somit die Nutzung eines Tools verweigert, mit dem sie ihre Produktivität steigern könnten.</p> |

Auf der vorhergehenden Seite wurde ausgeführt, dass IPSec-VPNs der administrativen Kontrolle unterliegen. Dadurch können Unternehmen daran gehindert werden, einer größeren Zahl von Benutzern bzw. verschiedenen Zugriffsmodi den Zugriff auf ihre Ressourcen zu ermöglichen. Neben der administrativen Kontrolle gibt es jedoch bei IPSec-VPNs noch weitere mögliche Schwierigkeiten, die sich aus der Verbindungsherstellung über die Netzwerkschicht ergeben. Dies ist z. B. die Zugriffssteuerung.

In IPSec VPNs werden authentifizierte Remotebenutzer (d. h. Benutzer, die ihre Identität erfolgreich bewiesen haben) zu einem virtuellen Punkt (Node) im Unternehmensnetzwerk. Als solcher kann ein Benutzer zunächst auf alle vernetzten Ressourcen zugreifen, sofern seine Zugriffsrechte nicht eingeschränkt wurden. Es gibt zwei Methoden zum Einschränken der Netzwerkressourcen, auf die Remotebenutzer, die über einen IPSec-VPN-Gateway Zugang zum Unternehmensnetzwerk erhalten, zugreifen können: Zugriffssteuerungslisten (Access Control Lists, ACLs) und die Einteilung des Netzwerks in physische Segmente. Diese Methoden sind zwar wirksam, gehen jedoch zu Lasten des Verwaltungsaufwands und der Flexibilität, und zwar in dem Maße, wie die Zahl an VPN-Benutzern und Netzwerkressourcen mit unterschiedlichen Bedürfnissen zunimmt.

Eine weiterer wichtiger Punkt, wenn Remotebenutzer über ein IPSec-VPN auf die Netzwerkressourcen zugreifen, besteht darin, dass die Benutzer und ihre Geräte direkt mit der Infrastruktur des Backends interagieren (d. h. mit File-Shares, Anwendungs- und E-Mail-Servern usw.). Auch dies legt einen Angriffspunkt für Bedrohungen offen, die speziell Sicherheitslücken dieser Backend-Ressourcen ausnutzen. Aus diesem Grund empfiehlt sich die Installation zusätzlicher Sicherheits-Appliances wie Firewalls, Intrusion-Detection-Systeme und Virenschutzfilter zwischen dem VPN-Gateway und den Backend-Ressourcen. Das VPN muss also in die vorhandene Sicherheitsumgebung des Unternehmens integriert werden.

SSL-VPN bietet kleinen und mittleren Unternehmen den Remotezugriff, den sie benötigen

Wie in der Einleitung erwähnt, sind SSL-VPNs genau das, worauf Unternehmen, die für den Remotezugriff eine Alternative zu IPSec-VPNs suchen, gewartet haben.¹ SSL-VPNs haben den Vorteil, dass sie die im vorherigen Abschnitt erläuterten Einschränkungen und Probleme von IPSec-VPNs umgehen. Denn SSL-VPNs werden auf der Anwendungsschicht implementiert, und nicht wie IPSec-VPNs auf der Netzwerkschicht. In der folgenden Tabelle werden die unmittelbaren Geschäftsvorteile beschrieben, die sich für Unternehmen aufgrund der besonderen Merkmale von SSL-VPNs erzielen lassen.

¹ SSL (Secure Sockets Layer) bietet Sicherheit und Datenschutz für Nachrichten, die über das Internet übertragen werden. SSL wird von den meisten e-Commerce-Websites als Sicherheitstechnologie verwendet und von den meisten Webbrowser unterstützt.

| Merkmale von SSL-VPN | Geschäftsvorteile |
|------------------------------------|---|
| Ohne Client | <p>Der verschlüsselte Tunnel zwischen dem Computer des Benutzers und dem SSL-VPN-Gateway wird mithilfe des Webbrowsers auf dem Benutzercomputer realisiert. Über einen Webbrowser können Benutzer auf verschiedene Anwendungen und Ressourcen zugreifen, darunter folgende:</p> <ul style="list-style-type: none"> • HTTP- und HTTPS-basierte Anwendungen und Intranets • Dateien und Dateisysteme, die FTP und Windows Network File Sharing unterstützen <p>Um weitere Ressourcen über ein SSL-VPN zu nutzen, werden dynamisch kleine Adapter und Tunnelingsoftware auf den Computer des Benutzers heruntergeladen. Über ein ActiveX-Steuerelement oder ein Java-Applet heruntergeladene Adapter erweitern die Reichweite der Anwendung so, dass auch weit verbreitete Client-Server-Anwendungen wie Microsoft Outlook und Lotus Notes, Terminal Services, VNC und SSH unterstützt werden können. Dynamisch heruntergeladene und aktivierte Tunnelingsoftware verkapselt den gesamten Datenverkehr zwischen Benutzer und Gateway in einem SSL-Tunnel. Somit können Benutzer auf eine ähnliche Bandbreite an Ressourcen zugreifen, wie sie normalerweise nur über IPSec-VPNs möglich ist. Diese Zugriffsmodi können jedoch nur verwendet werden, wenn die Benutzer weiterhin über grundlegende administrative Kontrolle verfügen (z. B. zur Aktivierung von ActiveX-Steuerelementen oder zur Unterstützung von JAVA).</p> <p>Der Verzicht auf einen Softwareclient hat einen wichtigen Vorteil: Je nach Zugriffsanforderung des Benutzers muss keine VPN-Software installiert werden bzw. erfordert die Installation von Adaptern und Tunnelingsoftware wesentlich weniger IT-Aufwand als bei einem IPSec-VPN-Softwareclient. Somit können auch bei Benutzergeräten, die einer strengen administrativen Kontrolle unterliegen, alle Benutzer – Lieferanten, Geschäftspartner, Kunden und Mitarbeiter – nahezu unmittelbar Teil des VPNs werden.</p> |
| Firewall-freundlich | <p>SSL-VPNs stellen die Verbindung zwischen Benutzer und VPN-Gateway nicht über die Netzwerkschicht her, sondern vielmehr über die darüber liegende Transportschicht. Daher drohen keine Probleme mit Sicherheitslücken, die beim Öffnen neuer Ports in Netzwerkfirewalls entstehen. Im Prinzip wird der SSL-VPN-Datenverkehr durch die Firewallports geleitet, die Unternehmen für Web- und sicheren Webdatenverkehr (Port 80 bzw. 443) geöffnet haben.</p> <p>Daher werden Remotebenutzer über ein Gastnetzwerk nicht mit Firewallsperrern konfrontiert wie bei IPSec-VPNs.</p> |
| Granulare Zugriffssteuerung | <p>Während IPSec-VPNs zunächst allen vernetzten Ressourcen Zugriff gewähren und diesen dann nach Bedarf einschränken, verfahren SSL-VPNs genau umgekehrt. Bei SSL-VPNs werden Netzwerkressourcen individuell als Objekte angesehen. Darüber hinaus sind die Zugriffsrechte der Benutzer objektbasiert, sodass ihnen nur Zugriff auf die Ressourcen gewährt wird, die ihnen ausdrücklich zugewiesen wurden (d. h., Benutzer A kann nur auf eine definierte Gruppe von Ressourcen zugreifen). Zugriffsrechte werden also von unten nach oben (auf Ressourcenebene) und nicht von oben nach unten (zunächst globaler Zugriff, dann Einschränkung) gewährt.</p> <p>Zudem können viele SSL-VPN-Lösungen weitere Merkmale in die granulare</p> |

| Merkmale von SSL-VPN | Geschäftsvorteile |
|----------------------|--|
| | <p>Zugriffssteuerung integrieren. Zu diesen Merkmalen zählen z. B. der Ort, von dem der Benutzer die Verbindung herstellt (von zuhause oder einem öffentlichen Hotspot), die Benutzerrolle, das Authentifizierungsschema (z. B. Benutzername und Kennwort oder nur ein einmaliges Kennwort) und der Sicherheitsstatus des Computers (z. B. die neuesten Virenschutzsignaturen).</p> <p>Durch die granulare Zugriffssteuerung von SSL-VPNs können die Unternehmen bei den Zugriffsrechten das von den Umständen abhängige gewünschte Maß an Einschränkung und Großzügigkeit walten lassen; diese Steuerung wird zentral über den SSL-VPN-Gateway verwaltet. Des Weiteren muss das Netzwerk nicht in physische Segmente unterteilt sein, da die granulare Zugriffssteuerung ähnliche Ergebnisse erzielt.</p> <p>Die granulare Zugriffssteuerung macht es leichter, der ständig zunehmenden Anzahl von Auflagen seitens der Behörden und der Industriebranche zu entsprechen; diese Auflagen fordern eine eingehendere Prüfung und Steuerung der Interaktionen zwischen Benutzern und Ressourcen.</p> |
| Proxybasiert | <p>Bei webbasierten bzw. Client/Server-Anwendungen fungieren SSL-VPNs als Proxy zwischen den Benutzeranfragen und den Antworten der Backend-Ressourcen. Das SSL-VPN stellt auf der WAN-Seite des Unternehmensnetzwerks im Prinzip den ersten Server einer aus zwei Phasen bestehenden Client/Server-Konfiguration. In der ersten Phase sind die Remotebenutzer die Clients, und der SSL-VPN-Gateway ist ein Server, der die Einrichtung des Tunnels mit den Remoteclients, die Ver- und Entschlüsselung des Datenverkehrs und die Durchsetzung der Richtlinien für die Zugriffssteuerung unterstützt. Auf der LAN-Seite des Netzwerks wird der SSL-VPN-Gateway zu einem Client der Ressourcen- und Authentifizierungsserver. In dieser Phase organisiert er die WAN-seitigen Clientanfragen und überträgt sie erneut an die Backend-Server. Bei dieser aus zwei Phasen bestehenden Client/Server-Konfiguration entsteht eine virtuelle Barriere zwischen dem Benutzer und der Ressourceninfrastruktur. So lange der SSL-VPN-Gateway effektiv Angriffe von außen abwehrt, ist auch die Netzwerkschicht der Ressourceninfrastruktur im Unternehmen vor einer Reihe von Angriffen geschützt, die auf Remotebenutzer oder ihre Geräte zurückzuführen sind.</p> <p>Wenn der gesamte Datenverkehr zwischen den Benutzern und dem VPN-Gateway mithilfe eines SSL-Tunnels eingekapselt wird, bestehen Sicherheitsrisiken für die Verbindung auf der Netzwerkschicht. Diesen kann mit herkömmlichen Sicherheitstechnologien zum Schutz der Netzwerkumgebung, wie einer Firewall oder Intrusion-Prevention-Systemen, begegnet werden werden.</p> <p>Des Weiteren muss beachtet werden, dass ein SSL-VPN nicht für den Schutz gegen Würmer, Viren und Spyware konzipiert wurde, deren Schadteile im Datenverkehr versteckt sein können. Dies gilt unabhängig vom Zugriffsmodus (ohne Client, über Adapter oder per Tunnelingsoftware). Aus diesem Grund sollten weitere Sicherheitstechnologien wie Virenschutz, URL-Filter und Anti-Spyware mit dem SSL-VPN kombiniert werden.</p> |

SonicWALLs zielbewusster Eintritt in den SSL-VPN-Markt

SonicWALL hat mit seiner Suite an Sicherheits-Applicances, bei denen die für kleine und mittlere Unternehmen wichtigen Faktoren (geringer Wartungsaufwand und Erschwinglichkeit) berücksichtigt werden, ohne bei den notwendigen Funktionen Kompromisse einzugehen, langjährige Erfahrung in diesem Marktsegment. Für die zweite Hälfte von 2005 hat SonicWALL die Einführung von zwei SSL-VPN-Applicances als Antwort auf den wachsenden Bedarf an Sicherheit beim Remotezugriff in kleinen und mittleren Unternehmen geplant: SonicWALL SSL-VPN 200 und 2000. Der Erfahrungsreichtum des Unternehmens gewährleistet, dass der Funktionsumfang und die Konzeption dieser SSL-VPN-Applicances genau auf die Anforderungen von kleinen und mittleren Unternehmen abgestimmt sind. Sie zeichnen sich unter anderem durch folgende Funktionen aus:

Nur zwei Zugriffsmodi und eine einzige URL

Die SSL-VPN-Applicances von SonicWALL verfügen standardmäßig über zwei Zugriffsmechanismen:

1. Ein Proxymechanismus für HTTP- und HTTPS-Anwendungen und Intranets sowie Dateien und Dateisysteme, einschließlich FTP und Windows Network Files Sharing. Diese Mechanismen werden vollständig vom Webbrowser des Benutzers unterstützt. Über den dynamischen Download eines ActiveX-Steuerelements bzw. eines JAVA-Clients lässt sich die Reichweite der Anwendungen und der Ressourcen vergrößern, um auch Terminal Services, VNC, Telnet und SSH-Ressourcen sowie Fernzugriffsfunktionen vollständig zu unterstützen.
2. Der ActiveX-Thin-Client NetExtender lässt sich aus dem Internet herunterladen. Mit diesem Client können die Benutzer eine Verbindung zu allen (kommerziell erhältlichen oder privat entwickelten) TCP/IP-basierten Anwendungen herstellen. In der Realität bedeutet dies, dass NetExtender den vollständigen, über IPSec möglichen Netzwerkzugriff für die Benutzer repliziert.

Der Benutzer kann beide Zugriffsmodi verwenden, indem er eine dem SSL-VPN-Gateway zugewiesene URL in die Adresszeile des Webbrowsers eingibt, dem vom Unternehmen definierten Authentifizierungsschema folgt (z. B. Benutzername und Kennwort) und dann die gewünschte Ressource aus einer Liste auswählt. Die Ressourcen werden für jeden Benutzer individuell anhand der ihm gewährten Zugriffsrechte auf einer Webportalseite aufgeführt. Für NetExtender wird ein separates Symbol angezeigt, sofern die vom Administrator festgelegten Richtlinien dies zulassen. Nach einem Klick auf dieses Symbol wird, falls noch nicht vorhanden, ein ActiveX-Thin-Client auf den Computer des Benutzers heruntergeladen, der die Benutzeroberfläche seines Desktops simuliert.

Interoperabilität mit den in kleinen und mittleren Unternehmen bereits vorhandenen Sicherheitslösungen und Authentifizierungsverzeichnissen

Sicherheitslösungen

Die meisten KMUs haben längst erkannt, dass die Verbindung mit dem Internet gewisse Risiken birgt. Aus diesem Grund werden Firewalls, Intrusion-Detection- und Intrusion-Prevention-Systeme, Virenschutz und Antispam-Software und -Appliances verwendet. Wie bereits weiter oben erwähnt, sind SSL-VPNs kein Ersatz für diese Technologien. Um die neue Investition in eine SSL-VPN-Appliance und bereits getätigte Investitionen in die Netzwerksicherheit zu optimieren, ist eine transparente Zusammenarbeit dieser Module unerlässlich.

Beide SonicWALL SSL-VPN-Appliances lassen sich einfach installieren und mit den bereits vorhandenen Sicherheits-Appliances kombinieren. Zusammen mit den von SonicWALL angebotenen Internetsicherheits-Appliances der Reihe TZ und PRO (Firewall, IDS, Virenschutz, Anti-Spyware, Antispam, Content-Filter) sind die SonicWALL SSL-VPNs eine logische Ergänzung, mit denen kleine und mittlere Unternehmen den Remotezugriff ohne Kompromittierung der Sicherheit ausweiten können. Bei der einfachen Installation empfängt die SonicWALL Internetsicherheits-Appliance die Zugriffsanforderungen des Benutzers und leitet sie zur Benutzerauthentifizierung, Verschlüsselung und Anzeige des für den Benutzer personalisierten Webportals an die SSL-VPN-Anwendung weiter. Ist die Authentifizierung erfolgreich, wird der Benutzerdatenverkehr von der SSL-VPN-Appliance an die SonicWALL Internetsicherheits-Appliance umgeleitet, wo sie auf Viren, Würmer, Trojaner, Spyware und andere Bedrohungen untersucht wird. Bei dieser Art der Bereitstellung werden die Vorteile der granularen Zugriffssteuerung und des mit SSL-VPN überall möglichen Zugriffs mit verlässlichen Sicherheitstechnologien für Internetbedrohungen kombiniert.

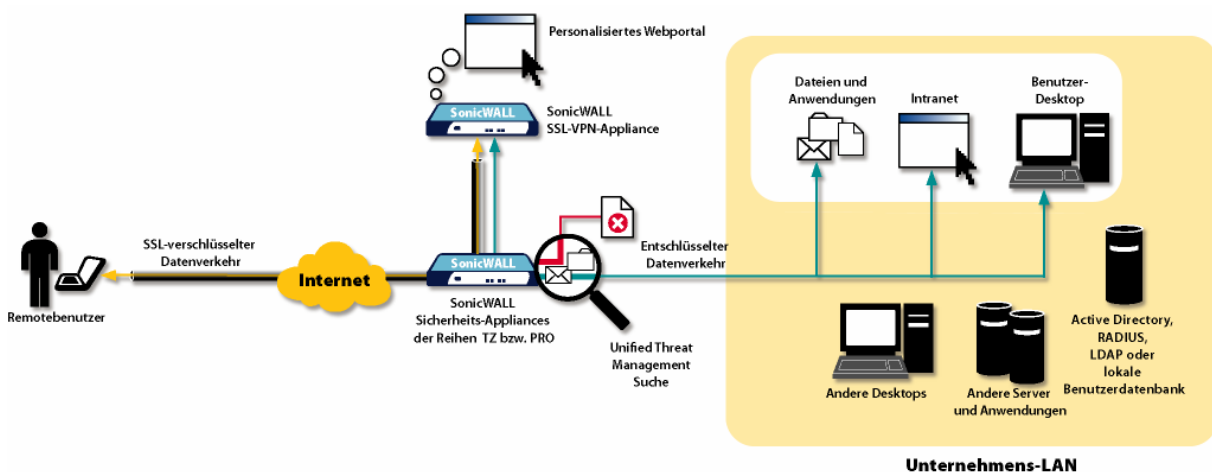


Abb. 2: Kombination einer SonicWALL SSL-VPN-Appliance mit einer SonicWALL Sicherheits-Appliance zum Schutz vor Internetbedrohungen

Da sich Unternehmen den Angeboten mehrerer Anbieter von Internet-Sicherheitstechnologien gegenübersehen, war SonicWALL bei der Entwicklung seiner SSL-VPN-Appliances darauf bedacht, dass deren Installation auch mit Firewalls und UTM-Appliances (Unified Threat Management) von Drittherstellern kompatibel ist.

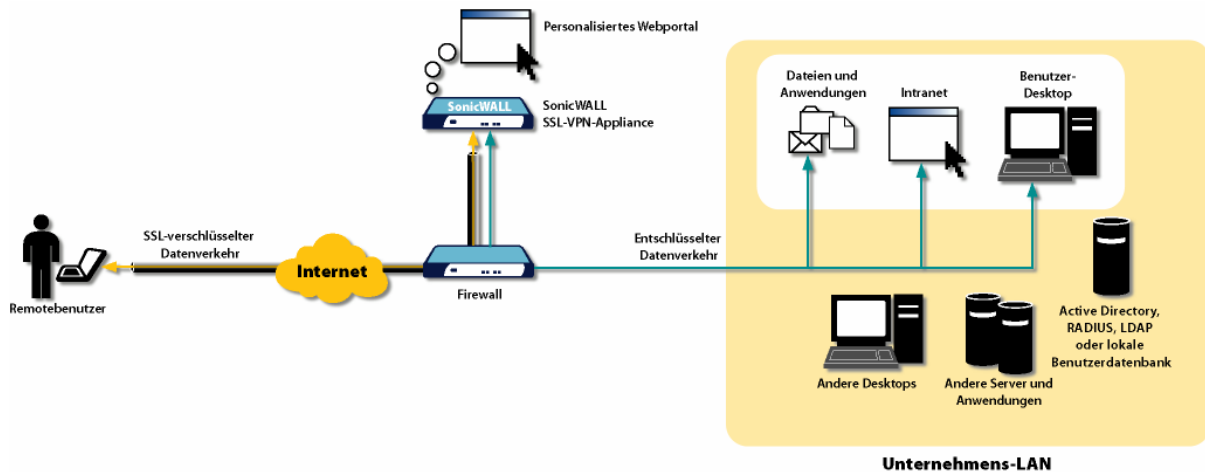


Abb. 3: Installation der SonicWALL SSL-VPN-Appliance in Kombination mit der Firewall eines Drittherstellers

Authentifizierungsverzeichnisse

Der erste Schritt der Zugriffssteuerung ist die Validierung der Benutzeridentität. Daher sind die SonicWALL SSL-VPN-Appliances so flexibel gestaltet, dass sie entweder als Host für ein Verzeichnis in der Appliance dienen oder mit bereits bestehenden Benutzerauthentifizierungsdatenbanken oder -schemen kombiniert werden können. SonicWALL SSL-VPN unterstützt die folgenden Authentifizierungsprozesse: RADIUS, LDAP, Active Directory und Windows NT-Domäne. Eine einzelne SSL-VPN-Appliance kann verschiedene Authentifizierungsprozesse unterstützen. Dies ist z. B. dann von Vorteil, wenn die Mitarbeiter eines Unternehmens bereits in einem Active Directory gespeichert wurden und nun ein Verzeichnis für Berater erstellt und in der SSL-VPN-Appliance selbst gespeichert wird.

Einfache Verwaltung

Arbeitsabläufe in Unternehmen können durch neue Technologien effizienter gestaltet werden. Sind die Technologien jedoch zu komplex oder nicht besonders benutzerfreundlich, führen sie wahrscheinlich eher zu Frustration. Wie bei den Internetsicherheits-Appliances von SonicWALL stehen auch für die SSL-VPN-Appliances Handbücher für die ersten Schritte zur Verfügung. Da die Anforderungen für den Remotezugriff von Unternehmen zu Unternehmen unterschiedlich sind, tragen die Handbücher drei unterschiedlichen Installationsszenarien Rechnung: (1) SSL-VPN in einer neuen DMZ (Demilitarized Zone), (2) SSL-VPN in einer vorhandenen DMZ und (3) SSL-VPN im LAN. Mithilfe dieser Handbücher lässt sich die SSL-VPN-Appliance in den meisten kleinen und mittleren Unternehmen in weniger als einer Stunde installieren. Künftige Änderungen und Verbesserungen können über das Verwaltungswebportal integriert werden.

Vollständige Unterstützung des Fernzugriffs

Für einen Teil der Benutzer ist der Desktop im Büro Dreh- und Angelpunkt ihrer Arbeit. Wenn sie nun extern auf diesen Desktop zugreifen können, erhöht dies die Flexibilität ihrer Arbeitsweise und ermöglicht ihnen, sich in dringenden Fällen mit Problemen auseinanderzusetzen, ohne ins Büro zurückkehren zu müssen. Aus diesem Grund bieten die SonicWALL SSL-VPN-Appliances sowohl in der Proxy- als auch in der NetExtender-Version standardmäßig eine vollständige Unterstützung des Fernzugriffs. Dies führt zu Kosteneinsparungen und vereinfacht die Administration, da diese Funktionen häufig noch über separate Produkte und Dienste realisiert werden.

Preisgestaltung ohne versteckte Kosten

Für jede SonicWALL SSL-VPN-Appliance gilt nur jeweils ein Preis – es fallen keine separaten Gebühren pro Lizenz an, und fast alle Funktionen sind im standardmäßigen Funktionsumfang enthalten. Die SSL-VPN 2000-Appliance kostet 2295 US-Dollar (Listenpreis November 2005). Der Preis für die SSL-VPN 200-Appliance wird Ende 2005 angekündigt, wird jedoch vermutlich wesentlich niedriger sein. Beide Appliances haben sehr ähnliche Funktionen; der Hauptunterschied besteht in der maximalen Anzahl der Benutzer, die gleichzeitig von der Anwendung unterstützt werden können. Expandierende Unternehmen müssen also keine Einbußen bei der Funktionalität hinnehmen, wenn sie VPN nur für eine kleine Benutzergruppe realisieren.

Ähnlich wie bei anderen SSL-VPN-Appliances hängt die zu einem bestimmten Zeitpunkt maximale Anzahl der gleichzeitig unterstützten Remotebenutzer davon ab, welche Anwendungen und Zugriffsmechanismen verwendet werden. Die SSL-VPN 2000-Appliance unterstützt den Fernzugriff für ca. 1000 Mitarbeiter. Genaue Leistungsmessdaten für SSL-VPN 200 sind noch nicht verfügbar, die Appliance wurde jedoch für Unternehmen mit 50 bis 100 Mitarbeitern entwickelt.

Dank der vereinfachten Preisgestaltung bei SonicWALL können kleine und mittlere Unternehmen bei den Kosten besser vorausplanen. Ändern sich die Bedingungen für den Fernzugriff (z. B. verfügbare Ressourcen, Benutzergruppen, Zugriffsmodi), fallen nur minimale zusätzliche Kosten an. Die angegebenen Preise für SonicWALLs SSL-VPN-Appliances liegen in der Preiskategorie der Investitionen, die KMUs für andere Sicherheitslösungen tätigen. Die Kombination aus vorhersehbaren Kosten und einer attraktiven Preisgestaltung bei SonicWALL ermöglichen es auch kleinen und mittleren Unternehmen, SSL-VPNs in Erwägung zu ziehen.

Zusammenfassung

Jedes Unternehmen muss unabhängig von seiner Größe ständig Möglichkeiten schaffen, den entsprechenden Personen zum richtigen Zeitpunkt Informationen zur Verfügung zu stellen. Um dieses Ziel zu erreichen, müssen zahlreiche technische, administrative und sicherheitsrelevante Hindernisse überwunden werden. Der Remotezugriff über SSL-VPN in Kombination mit anderen Technologien zum Schutz vor Sicherheitsbedrohungen ist hierbei ein wichtiges Element.

Der zweite Aspekt ist die Erschwinglichkeit. Die Preise von SSL-VPN-Produkten traditioneller Anbieter gehen derzeit weit über die Budgets vieler kleiner und mittlerer Unternehmen hinaus. Die Preisgestaltung der SSL-VPN-Appliances von SonicWALL ist auch für die meisten kleinen und mittleren Unternehmen tragbar. Wenn man darüber hinaus den Produktivitätszuwachs, der durch die Ausweitung des Remotezugriffs auf eine größere Benutzergruppe möglich wird, und die niedrigen Gesamtkosten der SonicWALL SSL-VPN-Appliances (Kaufpreis und Verwaltungsaufwand) berücksichtigt, ist die Investition schon in kürzester Zeit rentabel.

Michael Suby

Program Manager

Stratecast Partners (a Division of Frost & Sullivan)

msuby@stratecast.com