



Sichere Kommunikation,
Kostensenkung und
ein breites Einsatzspektrum

**VIRTUELLE
PRIVATE
NETZWERKE**

Inhalt

Vernetzung über Standleitungen und Festverbindungen	3
Kostensenkung durch das Internet	3
Sicherer Transfer über VPN.	4
Hoher Datenumsatz durch XSR	5
Gezielter Zugriff über das Extranet.	5
Standardisierte VPNs	6
Security Router von Enterasys.	6
Erprobter Schutz mit IPSec.	6
Transport- oder Tunnelmodus	7
Gesicherte Verbindungen.	7

EIN PLUS AN SICHERHEIT: STANDLEITUNGEN UND FESTVERBINDUNGEN

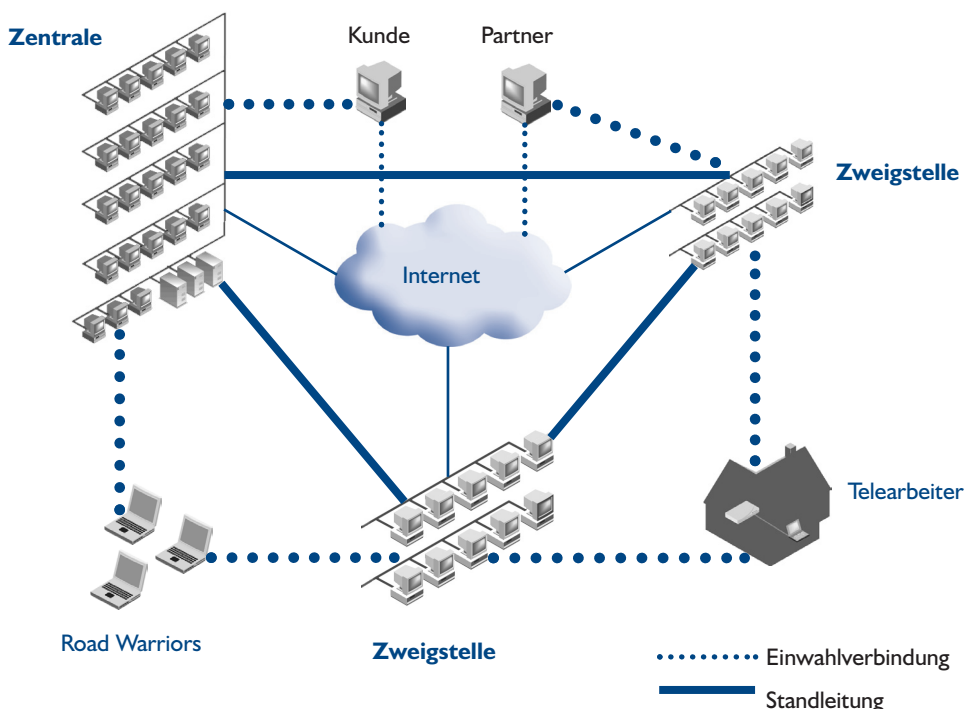
Bereits lange vor der flächendeckenden Verbreitung des Internets wurden zur Vernetzung von Zweigstellen und Partnern Standleitungen und Festverbindungen für die transkontinentale digitale Kommunikation genutzt. Diese Art der Anbindung bietet entscheidende Vorteile: Sie ist zuverlässig und garantiert Datenintegrität und Schutz der Kommunikation vor Dritten. Doch diese Sicherheit hat auch ihren Preis. Standleitungen, vor allem internationale, sind mit hohen laufenden Kosten verbunden. Außendienst- und Telearbeitsplätze erfordern spezielle DV-Strukturen, die einen Datenfernzugriff erlauben. Wählverbindungen, kostspielige Router und große Einwahlpools sowie ein unverhältnismäßiger Administrationsaufwand und Schutzmechanismen z. B. gegen Hacker treiben die Kosten für Kommunikation weiter in die Höhe.

EIN BEITRAG ZUR KOSTEN-SENKUNG: DAS INTERNET

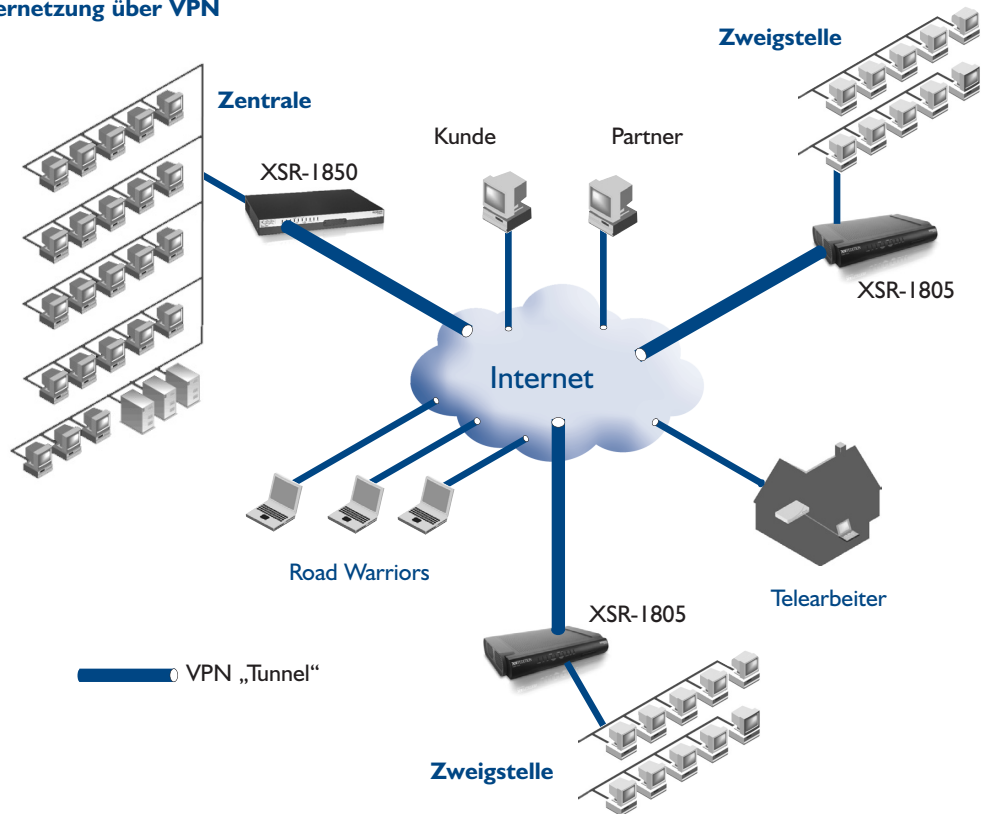
Die weite Verbreitung des Internets trug entscheidend zur Senkung der Kosten dieser neuen Technologie bei. Da sich das Internet jedoch nicht für den verschlüsselten Datentransfer eignete, ließ es sich nicht ohne weiteres in die Kommunikationsstruktur der Unternehmen einbinden. Das Internetprotokoll TCP/IP besitzt keine integrierten Sicherheitsmechanismen zum Schutz gegen unbefugten Fremdzugriff und birgt die Gefahr, dass sich ein Mitbewerber vertrauliche Informationen wie Produktinterna, Geschäftsabschlüsse, Angebote oder andere interne Mitteilungen ohne Schwierigkeiten beschafft. Identitäten können in der virtuellen Welt des Internets leicht verschleiert werden, wodurch sich z. B. die unbefugte Teilnahme an einer Datenkommunikation oder eine versteckte Veränderung von Daten leicht bewerkstelligen lassen. Um diesen Gefahren zu begegnen, wurden verschiedene Verschlüsselungs- und Signierungsverfahren für den TCP/IP-Verkehr entwickelt. Ein verschlüsselter „Tunnel“ ermöglicht die sichere Übermittlung von Daten über unsichere Netze, wie z. B. eine Festverbindung. Erste Produkte und Konzepte waren jedoch unausgereift oder durch Exportembargos nicht international einsetzbar. Fehlende Standardisierung verhinderte den Datenaustausch zwischen Produkten verschiedener Hersteller. Dennoch war das Konzept des virtuellen privaten Netzwerks (VPN) geboren.

In der Vergangenheit mussten meist nur die multinationalen Großkonzerne Lösungen für eine weltweite Vernetzung ihrer Zweigstellen und Außendienstmitarbeiter zur Ermöglichung der Kommunikation finden. Heute setzen sich auch viele mittelständische Betriebe mit diesem Bereich auseinander.

Vernetzung über Standleitung



Vernetzung über VPN



VPNs: SICHERER TRANSFER ÜBER UNSICHERE VERBINDUNGEN

Die beim VPN eingesetzte Technologie ermöglicht durch eine Kombination von Tunneling, Verschlüsselung, Authentifizierung und Zugriffskontrolle die sichere (geschützte) Datenübermittlung über ein unsicheres (ungeschütztes) Netzwerk wie das Internet. Dazu ist kein Eingriff in die bestehende Software erforderlich. Auch die Anwender müssen sich nicht umstellen oder umgeschult werden. Alle Sicherheitsfunktionen eines VPN arbeiten für den Benutzer transparent. Die Standardisierung von VPN-Technologien wie IPSec und L2TP führte in der jüngsten Vergangenheit zur weiten Verbreitung von VPNs, die inzwischen von allen aktuellen Betriebssystemen unterstützt werden.

Es stehen Verschlüsselungsverfahren in verschiedenen hohem Grad zur Verfügung. Die einfache Integration des VPN in bestehende Netzwerke erfolgt über einen Router (wobei aus einer Vielzahl ausgewählt werden kann) oder andere externe Hardware-Lösungen, die das VPN-Protokoll beherrschen.

KOSTENERSPARNIS INBEGRIFFEN

Bei der Kommunikation mit Zweigstellen, Partnern und Kunden können VPNs die Datenfestverbindungen vollständig ersetzen, d. h. die Kommunikation kann nun über die ohnehin vorhandene Internetanbindung ablaufen, was mit einer beträchtlichen Kostenersparnis verbunden ist. Manche Firmen beziffern ihre Internetgebühren auf monatlich 40 bis 100 Euro pro Verbindung, wohingegen die Kosten für eine vergleichbare Festverbindung ohne weiteres über 1000 Euro pro Monat steigen können.

Auch Außendienstmitarbeiter, die Zugriff auf Firmendaten benötigen, profitieren rundum vom Einsatz eines VPNs. Dies bedeutet, dass Einwahlrouter und -leitungen durch ein VPN ersetzt werden, wodurch auch die Flexibilität der Kommunikationsteilnehmer zugleich gesteigert wird. Der Road Warrior unter den Außendienstmitarbeitern, also derjenige Mitarbeiter, der ständig seinen Standort wechselt, kann nun eine beliebige Internetverbindung zur Kommunikation nutzen, da die Verbindung immer sicher und geschützt ist. Auf einer Messe verwendet er das vorhandene Funknetz, im Hotel sein Modem und beim Kunden ISDN oder einen dort zur Verfügung stehenden Internetzugang. Es kann dabei immer auf den regional günstigsten Internetprovider zugegriffen werden, was vor allem im Ausland wichtig ist.

Auch der Telearbeiter, der über einen längeren Zeitraum hinweg von einem gleichbleibenden Standort aus arbeitet, kann von kostspieligen ISDN-Verbindungen auf wesentlich schnellere Breitbandinternet-Verfahren umsteigen und spart durch Wahl eines Flatrate-Tarifs auch noch viel Geld dabei.

XSR: HOHER DATENUMSATZ IN KURZER ZEIT

Viele in Router und Firewalls integrierte VPNs sind mit den großen Datenströmen, die sie bewältigen sollen, überfordert und bleiben oftmals weit unter der technisch möglichen Geschwindigkeit. Der Grund dafür liegt darin, dass die Prozessoren dieser Geräte für das Weiterleiten von Daten ausgelegt sind, nicht aber für deren Verschlüsselung. Erst die neuen VPN-Accelerator-CPU's sind in der Lage, das heute übliche Datenvolumen zu sichern. Die XSR Security Router-Serie von Enterasys, die bis zu 100 Mbps verschlüsselt übertragen kann, wird selbst mit dem Datenaufkommen multinationaler Konzerne spielend fertig.

GEZIELTER ZUGRIFF: DAS EXTRANET

Das Extranet ist eine sehr aktuelle Anwendung von VPNs. Mit einem Extranet bieten Firmen ihren Partnern und Kunden den gezielten, über eine ausgefeilte Zugriffskontrolle geregelten Zugriff auf bestimmte Informationen und Dienste im internen Netzwerk. Wie bei der Standortvernetzung beschert das VPN als Extranet dem Unternehmen eine deutliche Kostensenkung.

Es bieten sich jedoch auch völlig neue Geschäftsmodelle und -prozesse, die ohne ein VPN nicht möglich wären. Eine besondere Dienstleistung wie der direkte Zugriff bindet nicht nur die Kunden stärker an das Unternehmen, sie bietet auch große Geschäftsvorteile.

Wenn jedoch zum Unternehmens-VPN noch das Extranet-VPN hinzutritt, erhöhen sich auch die Ansprüche an Zugriffskontrolle und VPN-Performance. Ein Security Router, der bis zu 200 gleichzeitige breitbandige VPN-Verbindungen unterstützt und noch eine Erweiterungskarte für die weitere Beschleunigung der Sicherheitsrechenprozesse aufnehmen kann, ist da mehr als eine gute Investition in die Zukunft: Die XSR Security Router-Serie bietet ein integriertes Intrusion Detection System (IDS), mit dem sich Einbruchsversuche in ein Netzwerk frühzeitig erkennen lassen.

STANDARDISIERTE VPNs

Drei der zurzeit verwendeten VPN-Verfahren sind standardisiert worden und haben eine große Verbreitung erlangt. IPSec (IP Security) befindet sich am häufigsten im Einsatz und wird auch von allen namhaften Herstellern unterstützt. L2TP (Layer 2 Tunneling Protocol) und PPTP (Peer to Peer Tunneling Protocol) werden ebenfalls von vielen VPNs gesprochen. Die drei genannten VPN-Verfahren setzen in der Transportschicht des Betriebssystems an und machen somit eine Veränderung der Anwendungssoftware unnötig – die Verschlüsselung erfolgt transparent.

IPSec entstand aus den Sicherheitsfunktionen, die in der neuen Version des Internetprotokolls IPv6 enthalten waren. Es wurde in einem langen Reifungsprozess seit den 80er Jahren von verschiedenen Gremien in einem offenen Verfahren entwickelt und bietet heute eine Vielzahl an hochwertigen Verschlüsselungsalgorithmen für ein breites Anwendungsspektrum, unter anderem auch Triple DES (Data Encryption Standard), AES (Advanced Encryption Standard), RC4 und Blowfish mit langen Schlüssellängen. IPSec lässt sich auf beliebig viele Teilnehmer ausdehnen und besitzt zur Vereinfachung der Verteilung und Verwaltung der kryptographischen Schlüssel eine integrierte Schlüsseldistribution. In vielen aktuellen Betriebssystemen ist IPSec zu finden, unter anderem in Windows 2000 und XP, Solaris, Linux und vielen anderen Unix-Systemen. Zahlreiche Firewall- und Router-Lösungen unterstützen ebenfalls IPSec.

L2TP und PPTP sind Protokolle, die die Nutzdaten in einen verschlüsselten PPP-Datenstrom einbetten. Sie lassen sich leichter konfigurieren als IPSec, eignen sich aber eher für eine Punkt-zu-Punkt-Kommunikation, besitzen also ein eingeschränkteres Einsatzgebiet. Auch diese beiden Protokolle werden von vielen aktuellen Betriebssystemen und Routern unterstützt.

UNIVERSELL EINSETZBAR: SECURITY ROUTER VON ENTERASYS

Eine flexible Kommunikation zwischen verschiedenen Gruppen wie Partnern, Kunden und Zweigstellen, teilweise über Landesgrenzen hinweg, erfordert flexible VPN-Lösungen. Zeitgemäße VPN-Hardware sollte sowohl größte Performance-Ansprüche erfüllen als auch mit allen VPN-Standards kommunizieren können und darüber hinaus ein möglichst einfaches und standardisiertes Konfigurationsverfahren bieten. Die Security Router von Enterasys unterstützen nicht nur alle aktuellen VPN-Protokolle, sondern erlauben auch eine Konfiguration sowohl über ein Cisco IOS-kompatibles Textinterface als auch über eine grafische Konfigurationssoftware, die ein Höchstmaß an Komfort bietet und einfach zu handhaben ist.

ERPROBTER SCHUTZ MIT IPSec

Während der langen Entwicklungszeit von IPSec ergab sich ein vielschichtiger Aufbau, der Schutz vor allen bekannten Angriffen auf Verschlüsselungstechnologien bietet. Grundsätzlich wird das IP-Datenpaket mit einem zusätzlichen Kopf („Header“) versehen, wobei hier zwischen zwei Arten von Headern unterschieden werden muss: Der Authentication Header (AH) sichert Authentizität und Integrität der Daten, verschlüsselt sie jedoch nicht. Aus Geschwindigkeitsgründen wurde in breitbandigen Netzwerken früher oft auf dieses nichtverschlüsselnde AH-Verfahren zurückgegriffen. Mit der Verfügbarkeit aktueller VPN-Accelerator-CPU's wie die der XSR Security Router-Serie gehört diese Beschränkung jedoch der Vergangenheit an. Das Encapsulating Security Payload (ESP) genannte Verfahren verschlüsselt dagegen die Daten auch. Beide Header schließen sich gegenseitig aus. Dies bedeutet, dass in den allermeisten Fällen die Anwendung eines der beiden Verfahren ausreichend ist.

ÜBERTRAGUNG IM TRANSPORT- ODER TUNNELMODUS?

VPNs auf IPSec-Basis unterstützen zwei verschiedene Übertragungsmodi. Im Transportmodus werden nur die Nutzdaten der IP-Pakete verschlüsselt, während der Kopf des Pakets, in dem unter anderem auch Absender- und Empfängeradressen stehen, unverschlüsselt bleibt.

Ein Angreifer könnte jedoch durch Paketanalyse ebenfalls den Weg der Daten erkennen, wenn auch nicht den Inhalt. Dieses Problem lässt sich mit dem Tunnelmodus umgehen. Die Nutzdaten werden dabei mitsamt der Kopfdaten komplett verschlüsselt. Ein Angreifer, der ein derartiges Datenpaket einsehen kann, sieht nur die Endpunkte der Tunnel, nicht aber die der eigentlichen Daten. Dieser Modus hat auch den Vorteil, dass dabei für jedes Netzwerk nur ein Router, der das Tunneling vornimmt, benötigt wird. Für die Hosts auf dem Netzwerk geschieht dies transparent. Der Tunnelmodus ist die typische Anwendung eines IPSec-VPNs.

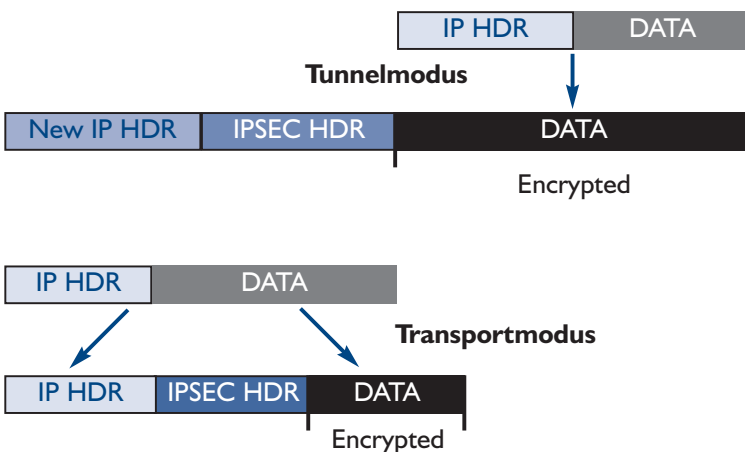
AUFBAU EINER GESICHERTEN VERBINDUNG

Vor dem Aufbau einer gesicherten Verbindung mit einem anderen IPSec-Host wird zunächst dessen Authentizität sichergestellt, dann werden die Schlüssel ausgetauscht. Diese Funktionalität ist nicht Teil von IPSec. Sie wird an einen Dienst namens Internet Key Exchange (IKE) ausgelagert, der jedem IPSec-VPN beiliegt. Hierbei müssen

sich die beiden Kommunikationspartner zuerst per IKE einander vorstellen. Es gibt drei Verfahren der gegenseitigen Vorstellung: Das einfachste davon verwendet so genannte „pre-shared secrets“, ist aber nur bei wenigen und im Wesentlichen konstant bleibenden VPN-Teilnehmern sinnvoll. Vor dem Datenaustausch wird bei diesem Verfahren allen Kommunikationspartnern auf sicherem Wege ein Schlüssel von Hand mitgeteilt.

Meistens ist es allerdings sinnvoller, die Authentifizierung automatisch durch IKE vollziehen zu lassen. Dafür besonders geeignet sind digitale Signaturen. Die zur Identifizierung des Kommunikationspartners nötigen Informationen werden entweder im IKE selbst gespeichert oder von externen Datenquellen bezogen.

Nachdem beide Partner sich gegenseitig anerkannt haben, einigen sie sich auf das zu verwendende Verschlüsselungsverfahren sowie auf einen Sitzungsschlüssel für die IPSec-Verbindung. Dies geschieht mit dem Diffie-Hellman-Protokoll, um gegen „Man in the middle“-Attacken resistent zu sein. Nun können Daten verschlüsselt und sicher durch den IPSec-Tunnel übertragen werden.



Enterasys Networks Germany GmbH

Solmsstr. 83
60486 Frankfurt/Main
Tel.: +49 (0) 69/4 78 60-0
Fax: +49 (0) 69/4 78 60-109

„Ludwigsforum“
Ludwigstraße 45
85399 Hallbergmoos
Tel.: +49 (0) 8 11/5 55 28-0
Fax: +49 (0) 8 11/5 55 28-11

Wittestraße 30, Haus J
13509 Berlin
Tel.: +49 (0) 30/3 99 79-5
Fax: +49 (0) 30/3 99 79-698

Neumarkt-Galerie
Richmodstr. 6
50667 Köln
Tel.: +49 (0) 221/9 20 42-742
Fax: +49 (0) 221/9 20 42-377

Große Bleichen 35
20354 Hamburg
Tel.: +49 (0) 40/34 99 99-0
Fax: +49 (0) 40/34 99 99-29

Walter-Köhn-Straße 1 d
04356 Leipzig
Tel.: +49 (0) 3 41/5 28-53 50
Fax: +49 (0) 3 41/5 28-53 69

Enterasys Networks Handelsgesellschaft m.b.H.

Twin Tower
Wienerbergstr. 11/14a
A-1100 Wien
Tel.: +43 (0) 1/994 60 66 05
Fax: +43 (0) 1/99 460 55 04

Enterasys Networks Switzerland AG

Industriestr. 19
CH-8304 Wallisellen-Zürich
Tel.: +41 (0) 1/839 54-54
Fax: +41 (0) 1/839 54-99

enterasys.com/de