

Die Zukunft der IP VPNs

VPN-Lösungen mit Tunneln waren bis vor kurzem die Methode der Wahl, um Firmenstandorte über öffentliche IP-Netze zu koppeln. Es gab zwar auch ein Konzept mit doppeltem NAT (Network Address Translation) und ohne Tunnel, das jedoch aufgrund schlechten Skalierungsverhaltens nur geringe praktische Bedeutung erlangte. Die wesentliche Konkurrenz wurde von VPNs mit Festverbindungen sowie von Layer-2-VPNs mit Frame Relay und ATM gebildet. Mit der Markteinführung von MPLS VPNs hat sich die Lage dramatisch geändert. Die meisten Neukunden fordern in der Ausschreibung ihres VPNs den Einsatz von MPLS durch den Provider, selbst wenn gar nicht klar ist, ob dies im Einzelfall die beste Technologie ist. Auch Bestandskunden werden nervös und möchten auf den fahrenden Zug aufspringen, um nicht den Megatrend der nächsten Jahre zu verpassen. Die Betreiber von Frame-Relay- und ATM-Netze sehen ihren Kundenstamm bröckeln und reagieren durch mehr oder weniger drastische Preissenkungen, um ihr Bestehen noch einige Jahre zu sichern. Welches Schicksal droht den herkömmlichen IP VPNs? Werden sie durch MPLS überflüssig und vom Markt verschwinden? Ein Blick in die Kristallkugel einer Wahrsagerin könnte vielleicht Antworten auf diese Fragen bieten. Sicherer ist jedoch eine Untersuchung aus technischer Sicht. Macht man sich die Eigenschaften klar, die herkömmliche IP VPNs sowie die dabei verwendeten Tunnelprotokolle haben und vergleicht diese mit den Eigenschaften von MPLS VPNs, kann man eine Prognose wagen. Dieser Artikel möchte genau dies tun.

1. Der Zweck von IP-Tunneln

Tunnelprotokolle existieren in verwirrender Vielfalt. Um sich dennoch einen Überblick zu verschaffen, ist es hilfreich, den Sinn und Zweck dieser Protokolle zu hinterfragen.

1.1 Layer-3-Tunnel

Layer-3-Tunnelprotokolle werden dazu verwendet, Pakete durch ein IP-Netz zu schleusen, die für sich alleine dort nicht routbar wären. Nicht-routbare Pakete haben entweder überhaupt keinen IP-Paketkopf (z. B. IPX- oder Apple-Talk-Pakete), oder sie tragen private IP-Adressen, die im öffentlichen IP-Netz unbekannt sind. Für IP VPNs ist dieser zweite Fall relevant: das Tunnelprotokoll sorgt dafür, dass mit privaten IP-Adressen versehene Pakete durch ein öffentliches Netz hindurch zugestellt werden können. Protokolle, die hierfür in Frage kommen, sind z. B. GRE (Generic Route Encapsulation) oder IPsec im Tunnel Mode.

Das Motiv für die Verwendung privater IP-Adressen ist die Bildung einer geschlossenen Benutzergruppe. Die Ausgangssituation für eine Station am öffentlichen IP-Netz ist eine allseitige Erreichbarkeit: man kann alle anderen Stationen erreichen, aber auch von diesen erreicht werden. Was zunächst wie eine Wohltat aussieht, wird jedoch leicht zur Plage. Eine Erreichbarkeit der eigenen Standorte für Angreifer wie z. B. Hacker ist zumeist unerwünscht. Private IP-Adressen schränken die Erreichbarkeit sofort radikal ein. Nun ist man für niemanden außerhalb des eigenen Standorts mehr erreichbar. Das ist natürlich auch nicht Sinn und Zweck der Vernetzung. Mit Hilfe von Tunneln wird nun manuell genau die gewünschte Erreichbarkeit wiederhergestellt.

Bild 1 zeigt die grundsätzliche Arbeitsweise eines Tunnels. Die Router zwischen den Tunnelendpunkten haben keinerlei Kenntnis von dem Tunnel. Sie transportieren die Pakete wie gewohnt anhand der IP-Adresse. Dass sich hinter dem äußeren IP Header ein weiterer befindet, wissen und interessiert sie nicht.

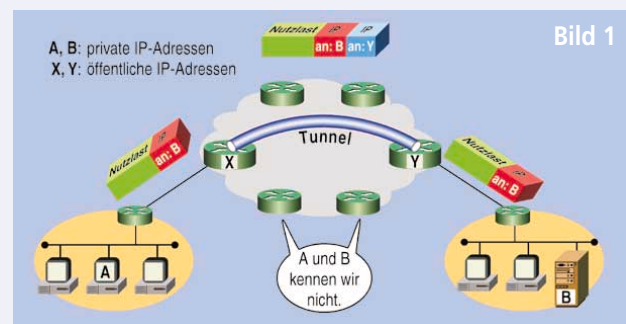
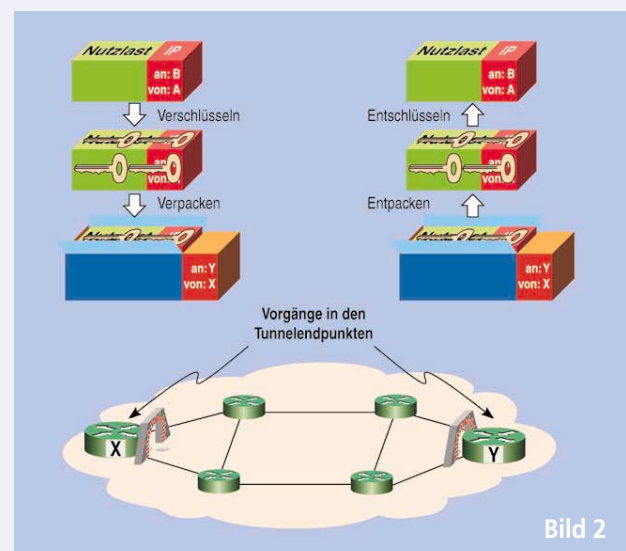


Bild 2 beleuchtet die Abläufe an den Tunnelendpunkten genauer. Auf jeden Fall muss das Originalpaket in ein neues Paket eingepackt werden. Je nach Tunnelprotokoll wird dabei noch Overhead zwischen dem neuen IP Header und das zu verpackende Paket eingefügt. Dieser Overhead ist im Bild allerdings nicht eingezeichnet.





Wird besondere Sicherheit im Sinne von Vertraulichkeit oder Datenintegrität gewünscht, können Tunnel optional verschlüsseln, Prüfsummen mitschicken oder eine Authentisierung des Absenders leisten. Dies ist die Domäne von IPSec.

1.2 Layer-2-Tunnel

Für den Transport von Ebene-2-Frames können Layer-2-Tunnel verwendet werden. In der Regel wird man das über ein WAN wegen des damit verbundenen Overheads nur ungern tun. Im Zusammenhang mit VPNs spielen Layer-2-Tunnel dennoch eine wichtige Rolle. Der Grund sind die Prozeduren des PPP (Point-to-Point Protocol) zur Authentisierung, die bei einer Einwahl mobiler Benutzer in ein VPN sehr nützlich sein können. In diesem Fall wird ein Layer-2-Tunnelprotokoll wie L2TP verwendet, um die PPP-Sitzung vom Einwahl-User bis zu dem Punkt zu verlängern, an dem eine Authentisierung mit Hilfe eines RADIUS Servers durchgeführt werden soll.

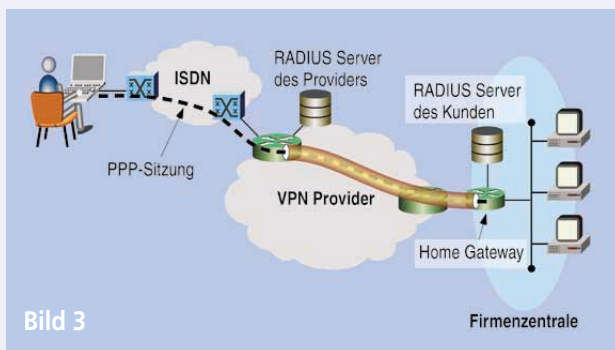


Bild 3

Bild 3 zeigt die Einwahl eines Mitarbeiters über ISDN in die Firmenzentrale. Die PPP-Sitzung, die zu Beginn nur zwischen dem Laptop des Benutzers und dem Einwahlrouter besteht, wird durch den Tunnel bis zum Home Gateway geführt. Der RADIUS Server des VPN Providers musste hierzu dem Einwahlrouter des Providers die IP-Adresse des Home Gateways mitteilen.

2. Das klassische IP VPN

Klassische IP VPNs binden eine Vielzahl von Filialen an eine Firmenzentrale mit Hilfe einer sternförmigen Topologie an. Andere Topologien sind ebenfalls möglich, verursachen aber in der Regel einen höheren Konfigurationsaufwand in Form von Tunneln. Die Tunnelendpunkte können entweder beim PE Router (Provider Edge Router) oder beim CE Router (Customer Edge Router) angesiedelt sein. Auf jeden Fall benötigen die Tunnelendpunkte eine öffentliche IP-Adresse, denn sie werden für den Datentransport durch das öffentliche Netz direkt adressiert.

2.1 Tunnelendpunkte bei den PE Routern

Liegt der Tunnelendpunkt beim Provider, so hat dies den Vorteil, dass der CE Router bereits aufgrund seiner privaten IP-Adresse nicht mehr angreifbar ist – auch nicht durch Denial-of-Service-Angriffe. So kann die Anschlussleitung des angebundenen Standortes nicht ohne weiteres von Hackern außer Betrieb genommen werden. Der einzige verwundbare Punkt ist dann der PE Router, der vom Provider entsprechend gut geschützt werden muss. Als Nachteil kann der Umstand gesehen werden, dass der Provider für die Einrichtung des VPNs tätig werden muss, was natürlich für jeden einzelnen Tunnel mit Kosten verbunden ist.

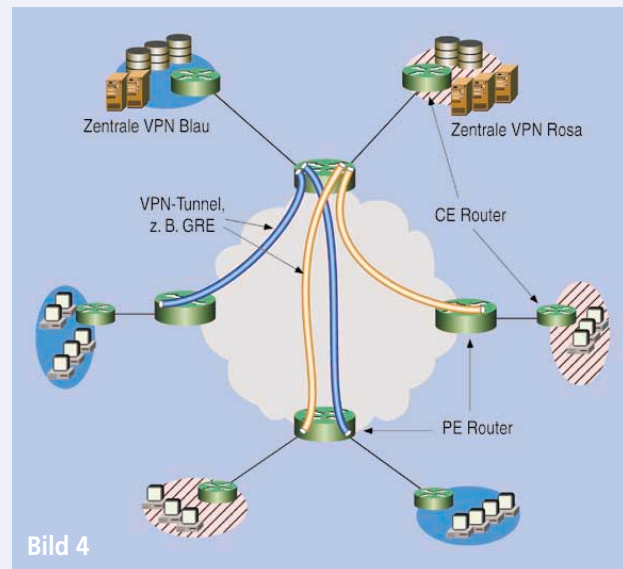
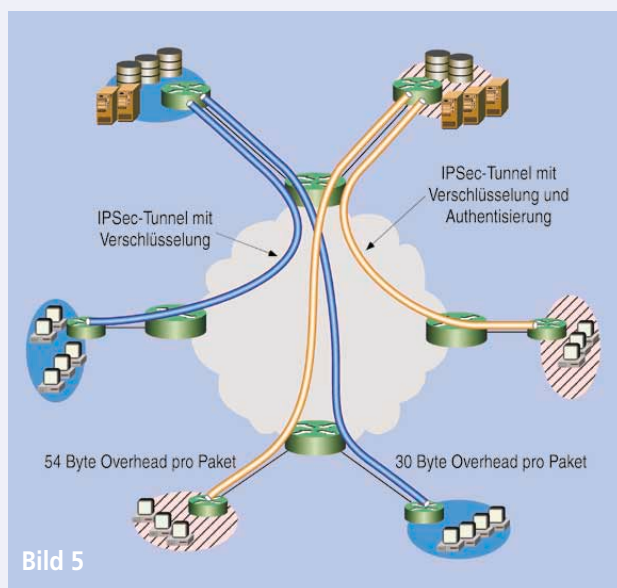


Bild 4

Die in Bild 4 skizzierte Konfiguration birgt noch unerwartete Tücken. Wenn nämlich Standorte mehrerer verschiedener VPNs an einem PE Router angebunden werden sollen, stellt sich die Frage nach dem korrekten Funktionieren des IP-Routings. So könnten z. B. die Adressräume der Kundenstandorte überlappen. Ein Ausweg wird durch Policy-based Routing geschaffen, was aber unangenehmen Konfigurationsaufwand bedeutet. Die Alternative wäre eine Beschaffung zusätzlicher PE Router.

2.2 Tunnelendpunkte bei den CE Routern

Sollen die Tunnelendpunkte in den CE Routern liegen, so kann ein VPN auch ohne Mithilfe des Providers aufgebaut werden. Dem gegenüber steht der Nachteil, dass der CE Router dann eine öffentliche Adresse benötigt und daher Angriffe – z. B. vom Typ Denial-of-Service – auf sich ziehen kann.



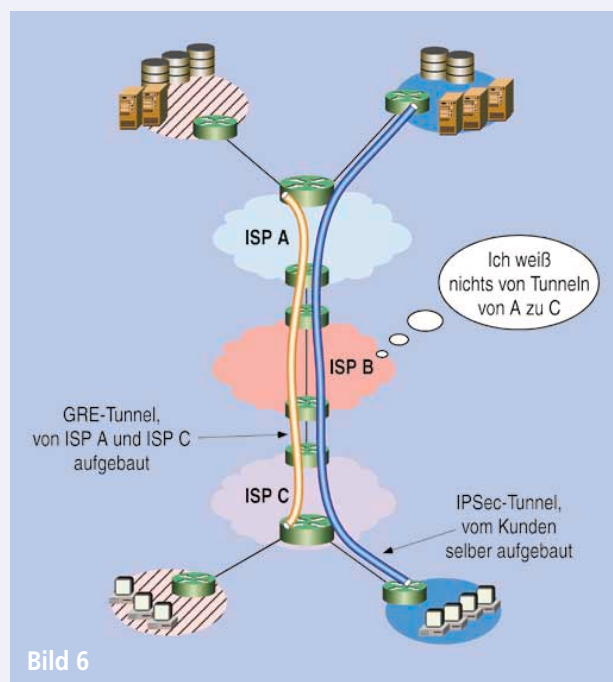
Ein weiterer und durchaus gravierender Nachteil ist der Overhead des Tunnelprotokolls auf der Anschlussleitung. In der Regel ist die Anschlussleitung ein Flaschenhals, der möglichst effizient genutzt werden soll. Durch ein Tunnelprotokoll kommen zwischen vier (GRE ohne Optionen) und 34 Byte (IPSec mit ESP und AH) sowie 20 Byte IP Header an Overhead zusammen, also insgesamt zwischen 24 und 54 Byte pro Paket.

Für kleine Pakete (z. B. TCP-Quittungen oder VoIP-Pakete mit einer Größe zwischen 40 und 80 Byte) verschlechtert sich so die Effizienz durch das Tunnelprotokoll dramatisch.

Bei vielen Firmennetzen wird der CE Router im Rahmen eines Managed Router Service vom Provider geliefert, konfiguriert und überwacht. In diesem Fall ist natürlich der Provider für die Konfiguration der Tunnel verantwortlich und wird diese in der Regel am PE Router einrichten.

2.3 Providerübergreifende VPNs

Providerübergreifend können VPNs mit Tunneln ganz problemlos aufgespannt werden. Für den Fall, dass die Tunnelendpunkte in den PE Routern liegen, ist nur erforderlich, dass diese Router das gleiche Tunnelprotokoll beherrschen und die beiden Provider auch gewillt sind, solche Tunnel bereitzustellen.



Noch einfacher wird die Lage für den Fall, dass die Tunnelendpunkte am CE Router definiert werden. Hier müssen die Provider nicht einmal kooperieren. Sie müssen einfach nur das tun, was sie immer tun: IP-Pakete transportieren.

2.4 Skalierbarkeit

Mangelnde Skalierbarkeit wird als Hauptkritikpunkt am VPN-Konzept mit Tunneln ins Feld geführt. Aber was bedeutet dieser Begriff eigentlich im Zusammenhang mit VPNs?

Grundsätzlich geht es bei der Skalierbarkeit um das Wachstum des Netzwerks. Die Anzahl der VPNs kann zunehmen, oder auch die Zahl der Standorte innerhalb eines VPNs. Die Frage ist nun, welche Konsequenzen ein solches Wachstum für Performance, Konfigurations-, Dokumentations- oder Wartungsaufwand hat.

Ein schönes Beispiel für mangelnde Skalierbarkeit sind mit Switches aufgebaute LANs. Mit der Anzahl der angeschlossenen Endgeräte nimmt die Last auf jeden LAN Switch durch Broadcasts (Rundsendenachrichten) in Form von ARP Requests linear (doppelte Anzahl Endgeräte führt auch zu doppelter Last) zu. Das heißt, dass ab einer bestimmten Anzahl Endgeräte alle LAN Switches voll mit Broadcasts ausgelastet sind. Ein weiteres Wachstum des LANs ist dann nur noch durch einen Technologiewechsel – die Segmentierung des LANs mit Hilfe von Routern – möglich. Zusätzliche LAN Switches würden dagegen nichts nutzen, da diese ebenfalls durch die Broadcasts außer Gefecht gesetzt würden.



Welche Skalierungsprobleme treten im Zusammenhang mit IP VPNs auf? Tunnel müssen konfiguriert und dokumentiert werden. Dabei sind stets Konfigurationsarbeiten an beiden Tunnelendpunkten erforderlich. Bei großen Providern wird hier schnell eine Anzahl von mehreren zehntausend Tunneln erreicht. Dazu kommen gegebenenfalls noch Access-Listen, die im Sinne eines Policy-based Routing Daten in bestimmte Tunnel einsortieren. All dies muss sorgfältig dokumentiert werden, um spätere Wartungsarbeiten bei sinnvollem Aufwand möglich zu machen. Will man hingegen ein Policy-based Routing vermeiden, um dynamisches IP Routing innerhalb des VPNs zu ermöglichen, kann ein PE Router nicht mehrere verschiedene VPNs bedienen, was zu enormem Hardware-Aufwand führt.

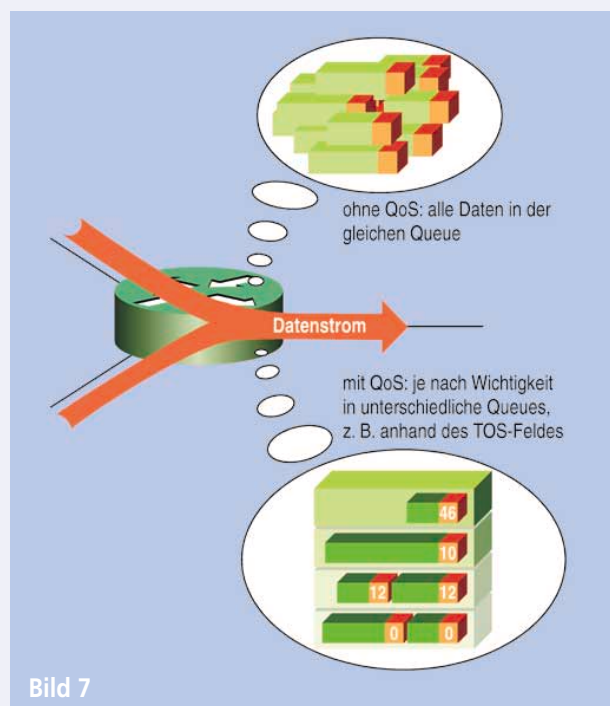
Solange keine nennenswerte Kommunikation zwischen den Filial-Standorten zu erwarten ist, genügt eine sternförmige Topologie. Dabei steigt der Aufwand für die Tunnel linear mit der Anzahl der Standorte in einem VPN. Bei herkömmlichen Client-Server-Anwendungen ist dies durchaus realistisch.

Mit der Einführung von VoIP in einem VPN fällt jedoch zunehmend Verkehr zwischen den Filialstandorten an, der auch noch zeitkritisch ist. Ein Transport aller Telefonate durch ein sternförmiges VPN und damit durch den Zentralstandort kommt nicht wirklich in Frage. Dann bleibt nur die Vollvermaschung der Standorte, was ein quadratisches Wachstum des Aufwands zur Folge hat. Bei einem vollvermaschten VPN mit 100 Standorten wären z. B. 4.950 Tunnel erforderlich, was kein akzeptabler Aufwand mehr ist. Dies ist ein typisches Skalierungsproblem.

2.5 Tunnel und QoS

Eine QoS (Quality of Service) wurde beim klassischen IP VPN nicht garantiert. Da heutige QoS-Lösungen in der Regel zusammen mit MPLS vermarktet werden, ist zudem der irriige Eindruck entstanden, QoS sei nur mit MPLS möglich. Dies wird durch falsche Argumente begründet – es seien beispielsweise feste Wege für die Daten erforderlich (also verbindungsorientierte Arbeitsweise), um QoS bereitstellen zu können. Tatsächlich wird beim derzeit dominierenden DiffServ-Konzept keinerlei fester Weg für die Daten benötigt – weder mit noch ohne MPLS. Im übrigen folgen die LSPs (Label Switched Paths) bei MPLS genau den vom IP Routing vorgegebenen Wegen. Ändern sich diese, werden die LSPs nachgezogen.

Im Router findet QoS stets an den Outgoing Interfaces statt. So lange der Router keine Überlast hat, bildet sich dort kein Stau, und die Daten werden auch nicht willkürlich verzögert. Strömen mehr Pakete in den Router, als abfließen können, bauen sich jedoch an den Outgoing Interfaces Warteschlangen – auch Queues genannt – auf.



Bei QoS-Lösungen wird für manche Datenströme garantiert, dass sie selbst bei Überlast eine bestimmte Bandbreite erhalten oder eine vorgegebene maximale Laufzeit nicht überschreiten, oder dass ihre Verlustwahrscheinlichkeit einen bestimmten Wert nicht übersteigt. Dies wird grob gesagt dadurch realisiert, dass diese Datenströme in gesonderte Queues einsortiert werden, die mit Vorrang abgearbeitet werden. So bleiben die Auswirkungen des Staus auf diese Daten begrenzt.

MPLS kann am Queueing überhaupt nichts verändern. MPLS ist gegenüber herkömmlichem IP einfach nur ein anderer Mechanismus, während des Datentransfers innerhalb des Routers das richtige Outgoing Interface zu bestimmen. Anstatt anhand der IP-Adresse in der Routing-Tabelle nach dem passenden Zielnetz zu suchen wird nun in der Switching-Tabelle anhand des Labels nachgeschlagen. Das Queueing kommt erst danach an die Reihe. Das heißt: MPLS hat mit QoS nicht das Geringste zu tun.

IP VPNs mit Tunneln und QoS sind daher möglich und werden in naher Zukunft sicherlich auch angeboten werden. Es ist allerdings ungewiss, ob sie ein Erfolg am Markt werden können. Provider-übergreifend wird QoS auch in der näheren Zukunft leider kaum angeboten werden. Dazu fehlt ein einheitlicher Umgang mit Verkehrsklassen (Classes of Service) zwischen den Providern, und auch die Tarifierungsmodelle im Internet sind der flächendeckenden Einführung von QoS eher hinderlich.



3. Die Sonderlösung: Doppel-NAT

IP VPNs müssen nicht grundsätzlich mit Tunneln arbeiten. Ein Konzept mit Doppel-NAT stellt jede beliebige Topologie zur Verfügung und vermeidet Angriffe von außerhalb des VPNs – auch Denial-of-Service-Angriffe.

Das Konzept beruht auf der Idee, Access-Listen dafür zu verwenden, sowohl Absender- als auch Zieladresse der VPN-Standorte auf einen innerhalb des Netzwerks bekannten Adressraum aus dem Bereich 10.0.0.0/8 abzubilden. Die Access-Listen regeln dabei, welche Standorte mit welchen anderen kommunizieren dürfen.

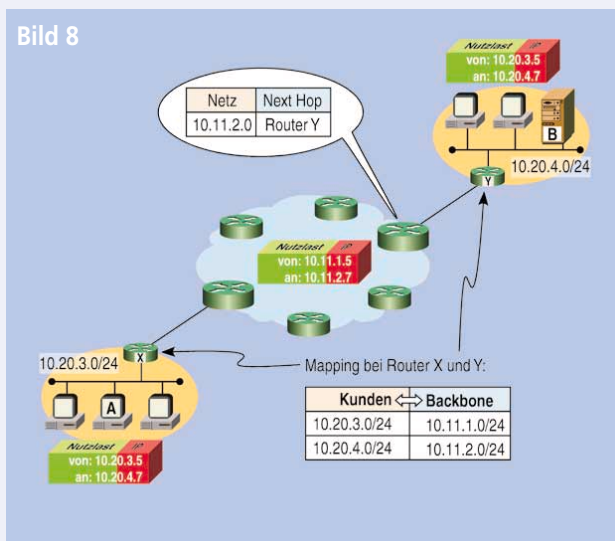


Bild 8 zeigt einen Fall mit zwei Standorten. Sendet die Station A mit der Absender-Adresse 10.20.3.5 an Station B mit der Ziel-Adresse 10.20.4.7, so tauscht der CE Router beide Adressen aus. Das neue Ziel lautet z. B. 10.11.2.7, da dem Netz 10.20.4.0/24 innerhalb des Providernetzes der Bereich 10.11.2.0/24 zugeordnet ist. Innerhalb des Providernetzes sind die Adressräume der Kundenstandorte unbekannt.

Ein Nachteil dieser Methode ist die mangelnde Skalierbarkeit. Einerseits ufern die Access-Listen bei großen VPNs aus, was die Performance der betroffenen Router beeinträchtigt. Andererseits wird bei wachsender Anzahl oder Größe der VPN-Standorte der für das Mapping auf Adressen im Backbone zur Verfügung stehende Adressraum knapp. Zudem bleibt die Anwendbarkeit auf ein Providernetz beschränkt. Providerübergreifende VPNs sind so nicht möglich.

Vor allem die mangelnde Skalierbarkeit spricht gegen eine Zukunft von VPNs mit doppeltem NAT. Ein Provider kann kein Interesse an einer VPN-Lösung haben, die nur begrenztes Wachstum der Kunden mitmachen kann.

4. Das MPLS VPN

MPLS VPNs wurden mit dem Anspruch guter Skalierbarkeit entwickelt. Diesem Anspruch werden sie auch gerecht. Bei geringem Konfigurationsaufwand bieten sie Any-to-Any-Topologie bei guter Sicherheit. Andere Topologien sind mit entsprechendem Konfigurationsaufwand möglich.

4.1 VRF-Tabellen, Route Targets und Topologie

Die Grundidee besteht darin, dass die PE Router für jedes VPN, in das sie einen Anschluss haben, eine separate Routing-Tabelle anlegen (VPN-Routing-and-Forwarding-Tabelle, kurz VRF). In dieser VRF-Tabelle speichern sie ausschließlich Erreichbarkeitsinformation für das zugeordnete VPN. Jede VRF-Tabelle an einem PE Router bekommt einen lokal eindeutigen Namen.

Bei der Configuration eines VPN-Anschlusses wird der Name der für diesen Anschluss zu verwendenden VRF-Tabelle angegeben. Informationen über die Erreichbarkeit der direkt benachbarten VPN-Standorte verbreitet der PE Router mit Hilfe des iBGP-4-Protokolls an alle anderen PE Router.

Dabei werden sogenannte Route Targets an die Erreichbarkeitsinformation angehängt. Dies sind Kennzahlen, die bei der Configuration der VPN-Anschlüsse eingetragen werden und dem Filtern von gelernten Routen dienen. Nur Ziele, die passende Route Targets tragen, werden in die VRF-Tabelle übernommen.

Im einfachsten Fall haben alle Standorte innerhalb eines VPNs dasselbe Route Target, und es werden keine weiteren Filterregeln definiert. Dann wird die Information über jeden Standort an jeden anderen weitergegeben, und eine Any-to-Any-Topologie entsteht.

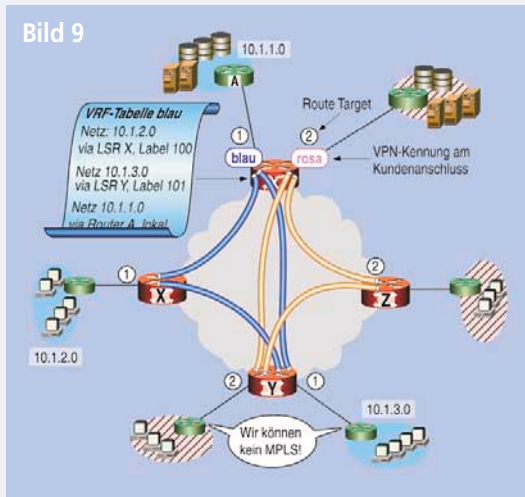


Bild 9 zeigt zwei VPNs an einem MPLS-Netz. Für den PE Router der Zentrale ist eine der beiden VRF-Tabellen angegeben, und zwar die für das VPN Blau. Informationen über das VPN Rosa sind in ihr nicht enthalten.

Soll eine vollvermaschte Topologie vermieden werden, müssen mehrere Route Targets innerhalb eines VPNs verwendet werden. Ein sternförmiges VPN kann z. B. einfach dadurch konfiguriert werden, dass für die Filialen ein anderes Route Target als für die Zentrale definiert wird. Der Zentral-Standort verwendet dann zwei Regeln: Er exportiert Information über seinen eigenen Standort mit seinem Route Target und importiert Informationen über die Filialen mit deren Route Target. Umgekehrt sind die Regeln an den Filial-Standorten: Sie exportieren eigene Informationen mit ihrem Route Target, importieren aber nur Informationen mit dem Route Target der Zentrale. Der letzte Punkt ist entscheidend, da so vermieden wird, dass eine Filiale Informationen über die direkte Erreichbarkeit einer anderen erhält.

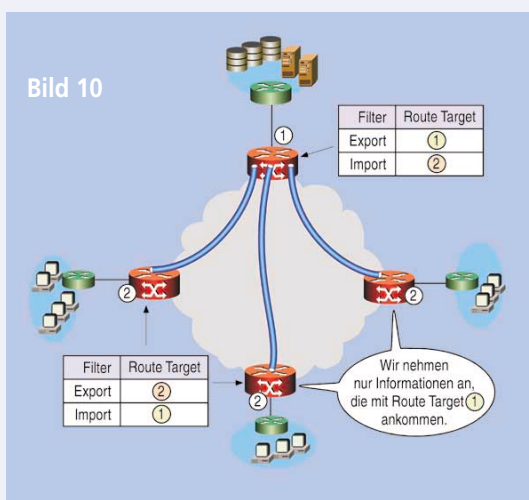
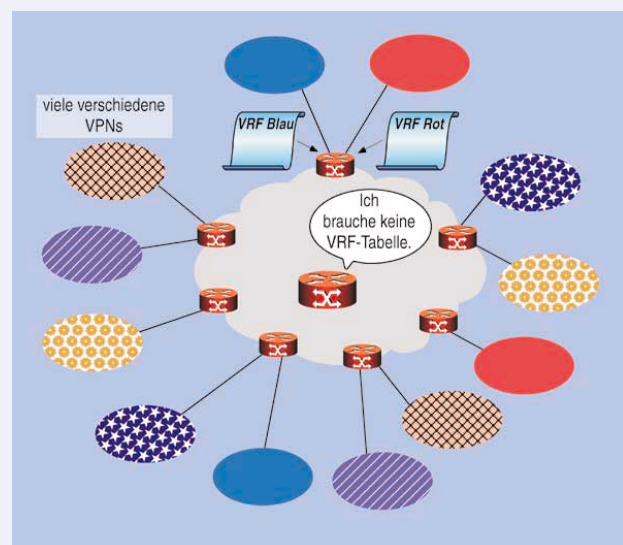


Bild 10 zeigt, wie ein sternförmiges VPN mit drei Filialstandorten nach der oben beschriebenen Methode konfiguriert werden kann.

4.2 Skalierbarkeit

Der Aufwand bei der Konfiguration wächst sehr moderat mit der Größe eines VPNs. Pro neuem Standort ist beim einfachsten Fall der vollvermaschten Topologie nur das Eintragen zweier Kennzahlen (VPN-Kennung sowie Route Target) sowie einer statischen Route auf die Ziele im angeschlossenen Standort am PE Router erforderlich.

Auch wenn die Anzahl der VPNs wächst, steigt der Aufwand dadurch nicht merklich. Es müssen lediglich eindeutige Route Targets vergeben werden.



Da nicht jeder PE Router alle Informationen über alle VPN-Ziele vorhalten muss, sondern nur VRF-Tabellen zu eigenen VPN-Standorten benötigt, wächst auch die Last auf das Netzwerk nur langsam. Backbone-Router müssen überhaupt keine VRF-Tabellen pflegen und kennen daher keine Ziele aus den VPN-Standorten. Sie sind nur dafür zuständig, Daten von einem PE Router zum anderen weiterzuleiten.

Wenn in der Folge des Netzwerkwachstums neue PE Router installiert werden müssen, fällt hierfür Konfigurationsaufwand für das BGP-4-Protokoll an, welches für die MPLS VPNs benötigt wird. Wenn hier Optimierungen wie z. B. Route-Reflektoren (das sind Verteilstationen für BGP-Informationen) zum Einsatz kommen, nimmt der Aufwand jedoch nur linear mit der Anzahl der PE Router zu.

4.3 Overhead

MPLS VPNs benötigen während des Datentransfers zwei MPLS Header (sogenannte Shim Header) zu je vier Byte pro Paket. Der innere Header trägt die Information, zu welchem VPN das Paket gehört; der äußere enthält das Label, welches den Weg zum entfernten PE Router finden hilft.



Dieser Overhead wird jedoch erst vom PE Router angehängt – der CE Router ist an den MPLS-Abläufen unbeteiligt. Das heißt, dass die Anschlussleitung nicht zusätzlich durch MPLS belastet wird.

4.4 Sicherheit

Die Sicherheit von MPLS VPNs ist hoch. Stationen innerhalb eines VPNs können nicht von außerhalb adressiert werden. Hacker haben damit weder von einem fremden VPN noch von einem Nicht-VPN-Anschluss aus die Möglichkeit, VPN-Standorte zu attackieren. Der verbleibende Unsicherheitsfaktor sind die LSRs (Label Switch Router) des Providers. Da sie neben ihrem Beruf als LSR stets auch als normaler Router funktionieren müssen, sind sie angreifbar, sofern sie adressierbar sind. Es liegt in der Verantwortung des Providers, dies möglichst wirksam zu unterbinden. Ein MPLS VPN auf einem MPLS-Netz, an dem ausschließlich VPN-Standorte konfiguriert wurden, kann mit gutem Gewissen als ebenso sicher bezeichnet werden wie ein Ebene-2-VPN mit Frame Relay oder ATM. Denn in diesem Fall sind die einzigen adressierbaren Stationen solche innerhalb der VPNs, und die LSRs können nicht angegriffen werden.

4.5 Internationale Verfügbarkeit

Providerübergreifende MPLS VPNs sind heute nicht verfügbar. Das wird sich allerdings bald ändern. Voraussetzung hierfür ist, dass nicht nur innerhalb der Providernetze, sondern auch zwischen diesen MPLS gesprochen wird.

Solange dies noch nicht der Fall ist, können MPLS VPNs nur innerhalb eines zusammenhängenden Providernetzes realisiert werden. Für internationale Kunden hat dies die Folge, dass gegebenenfalls ein Tier-1-Provider genutzt werden muss. Das kann – je nach Lage der Kundenstandorte – den Nachteil langer Wege bis zum nächsten PoP und damit entsprechend hoher Kosten für Anschlussleitungen haben, denn aufgrund ihrer weltweiten Präsenz haben Tier-1-Provider in der Regel kein sehr engmaschiges Netz, und die PoPs sind in vielen Ländern nur in den wichtigsten Ballungsräumen zu finden.

5. Künftige Einsatzzwecke für IP Tunnel

Nachdem in den vorangehenden Kapiteln wichtige Eigenschaften von IP VPNs sowie von MPLS VPNs zusammengetragen wurden, kann nun die Frage angegangen werden, inwieweit IP VPNs mit Tunneln heute noch eine Existenzberechtigung haben bzw. in Zukunft haben werden.

5.1 Vom Kunden selbst aufgespannte VPNs

Will ein Kunde eines Providers sein VPN an einem öffentlichen IP- oder MPLS-Netz selber aufspannen, so bietet sich eine Lösung mit IPSec im Tunnel Mode an. Der Vorteil für den Kunden ist, dass er vom Provider nur eine Transport-Dienstleistung für seine IP-Pakete benötigt, was im Regelfall preiswerter als eine VPN-Lösung ist. Ein Nachteil ist natürlich die Konfigurationsarbeit, die mit den IPSec-

Tunneln verbunden ist. Problematisch ist auch der Overhead von IPSec, der pro Paket je nach Betriebsart zwischen 30 Byte (nur verschlüsselt, nicht authentisiert) und 54 Byte beträgt.

Die Sicherheit eines so gebildeten VPNs kann sehr hoch sein, was Vertraulichkeit und Datenintegrität anbetrifft. Lediglich die Tunnelendpunkte sind angreifbar und müssen entsprechend geschützt werden. Denial-of-Service-Angriffe auf die Tunnelendpunkte bleiben allerdings ein Problem.

Auf jeden Fall muss darauf geachtet werden, dass die CE Router die erforderliche Performance für die Verschlüsselung und Authentisierung durch IPSec besitzen – am besten mit speziell hierfür konstruierter Hardware.

Ein typisches Szenario ist die Verwendung von VPN-Boxen an den Filialstandorten, die ihre IPSec-Tunnel zu einem Security Gateway (einer Firewall) am Standort der Zentrale aufbauen. Moderne Firewall-Produkte bieten hierbei die Möglichkeit eines zentralisierten Managements der verteilten VPN-Boxen.

QoS kann in einem solchen VPN nur dann implementiert werden, wenn die Provider bereit ist, DiffServ oder ein ähnliches Konzept auch ohne VPN-Lösung zu verkaufen. Der Sinn oder Unsinn einer so gearteten Implementierung hängt sicherlich von den Anwendungen ab, die über das VPN dann genutzt werden. Eine wesentliche Triebfeder für den Einsatz von QoS ist VoIP, aber der mit IPSec verbundene Overhead führt VoIP direkt ad absurdum. Wieso sollte man mit Sprachkompression und Header Compression auf Kosten von Laufzeiteigenschaften Bandbreite sparen, nur um diese anschließend wieder durch Tunnelprotokolle zu verpulvern?

5.2 Providerübergreifende VPNs

Solange zwischen den Providernetzen noch kein MPLS implementiert ist, sind MPLS VPNs für internationale Kunden nicht in jedem Fall optimal. Hier ist zumindest für eine Übergangszeit noch eine ökologische Nische für VPNs mit Tunneln. Diese wird jedoch bald sehr eng werden, da MPLS für die Provider eine so nützliche Technologie ist, dass eine vollständige Durchdringung des Internets mit MPLS nur eine Frage der Zeit ist.

5.3 Remote Access

Einwahl-Prozeduren für mobile Mitarbeiter können je nach VPN-Technologie sehr unterschiedlich ausfallen.

Bei der Verwendung von Layer-2-Tunneln wie z. B. L2TP wird vom NAS (Network Access Server) ein Tunnel zum Home Gateway des VPNs aufgebaut. Der RADIUS Server des Providers muss hierbei als wesentliche Information die IP-Adresse des Home Gateways an den NAS übermitteln. Am Home Gateway kann der Einwahl-User dann noch einmal gründlich authentisiert und autorisiert werden. So können z. B. Access-Listen durch den RADIUS des Kunden im Home Gateway dynamisch installiert werden, welche die Zugriffsmöglich-



keiten einschränken können. So kann beispielsweise der Zugang zur Firmendatenbank freigegeben, der zu den File Servern jedoch blockiert werden.

Für eine Einwahl über einen fremden Provider wird die beschriebene Methode in der Regel nicht funktionieren, da der RADIUS des Einwahl-Providers keine Informationen über VPNs in fremden Netzen hat.

Ein Ausweg besteht darin, sich eben nicht über einen fremden Provider einzuwählen, sondern stets über einen NAS des eigenen Providers zu gehen. Hält sich der Einwahl-User jedoch im Ausland auf, kann dies unkontrollierbare Telefonkosten nach sich ziehen.

Die Alternative ist ein IPSec-Tunnel, der vom Client aufgebaut wird. In der ersten Stufe der Einwahl erhält der Client vom lokalen NAS eine öffentliche IP-Adresse. Damit ausgerüstet nimmt er Kontakt zum Home Gateway auf und etabliert zu diesem einen IPSec-Tunnel. Durch diesen Tunnel können dann Pakete mit privaten Adressen aus dem Adressraum des VPNs laufen. Der Vorzug dieser Methode ist die ausgezeichnete Sicherheit sowie die weitgehende Unabhängigkeit vom Provider. Solange der lokale Provider tatsächlich öffentliche Adressen verwendet und kein NAT durchführt, wird eine solche Einwahl immer funktionieren. Der offenkundige Nachteil ist der hohe Overhead, der um so schmerzlicher wird, je niedriger die zur Verfügung stehende Bitrate ist.

MPLS VPNs bieten eine sehr elegante Möglichkeit der Einwahl. Bereits bei der ersten Authentisierung durch den RADIUS des VPN Providers kann der Einwahlport temporär in das VPN aufgenommen werden. Hierzu muss der RADIUS die passende VPN-Kennung für den Einwahl-User kennen und dem NAS übermitteln. Damit weiß der NAS, welche VRF-Tabelle für den Einwahl-User gilt. So wird dieser zu einem vollwertigen Mitglied des VPNs, das – falls gewünscht – uneingeschränkte Any-to-Any-Konnektivität genießt. Diese Methode funktioniert aber derzeit nicht bei Einwahl über einen fremden Provider. Soll eine solche Einwahl jedoch auch möglich sein, empfiehlt sich die bereits beschriebene Methode, mit Hilfe eines IPSec-Tunnels Kontakt zum Home Gateway der Firmenzentrale herzustellen.

5.4 Altlasten

Trotz des Namens „Multiprotocol Label Switching“ ist MPLS derzeit nur zum Transport von IPv4-Paketen geeignet. In näherer Zukunft wird sicherlich noch IPv6-Transport über MPLS standardisiert werden, aber Protokolle wie Apple Talk, IPX oder Banyan Vines werden kaum noch Gegenstand zukünftiger MPLS-Standards werden. Existieren in einem VPN noch Altlasten dieser Art, so sind IP-Tunnel erforderlich. Diese können dann natürlich über ein MPLS VPN geführt werden. In einem solchen Anwendungsfall wird der Tunnel also nicht den Zweck haben, eine geschlossene Benutzergruppe zu definieren, sondern fremde Protokolle vor einem IP-Netz zu verstecken.

Ein anderer Ansatz für den Umgang mit fremden Protokollen wird AToM genannt – Any Transport over MPLS. Obwohl dies bislang nur

als Draft (also ein Standard im Entwurfsstadium) beschrieben ist, wird AToM von vielen Providern als zukunftsweisende Technologie betrachtet. AToM soll ermöglichen, Daten jeglichen Formats über ein MPLS-Netz zu transportieren. Mit AToM könnte MPLS eines Tages das werden, was ATM immer sein wollte: die universelle Netzplattform für alle Anwendungen.

5.5 Ausblick

Die weitere Verbreitung von MPLS scheint unaufhaltsam zu sein. Zu groß sind die Vorteile für die ISPs, als dass diese das von der Mode diktierte Bedürfnis der Kunden nach MPLS nicht allzu gerne aufgreifen würden. Und mit der Any-to-Any-Konnektivität sowie interessanten QoS-Angeboten, geringem Overhead und guter Sicherheit sind MPLS VPNs sicherlich nicht das Schlechteste, was den Kunden passieren kann.

Die Konkurrenzanbieter mit Frame-Relay-VPNs leiden unter dem Image einer angestaubten, wenig performanten und altbackenen Technologie. Das ist zwar schade, denn Frame Relay ist auch aus heutiger Sicht ein schlankes, effizientes und sehr sicheres Protokoll, das sich ausgezeichnet zum Transport von IP eignet. Dennoch wird die Bedeutung von Frame Relay VPNs stark abnehmen.

ATM wird zwar dem hausgemachten Anspruch an maximale QoS gerecht. Der Overhead, der einerseits durch die Zellköpfe und andererseits durch den AAL 5 beim Verpacken von IP in ATM entsteht, spricht jedoch gegen den Einsatz von ATM in Umgebungen, in denen ausschließlich IP-Anwendungen vorkommen. Dazu kommen noch gravierende Probleme mit Bursts, wenn die Endgeräte kein perfektes Traffic Shaping beherrschen. Geht auch nur eine ATM-Zelle am Netzeingang oder im Backbone verloren, wird dadurch ein ganzes IP-Paket aus bis zu 32 Zellen unbrauchbar – im ungünstigsten Fall sogar zwei. ATM wird seine Rolle jedoch auch zukünftig im Umfeld der Videoübertragung sowie im Access-Bereich der UMTS-Netze spielen. ATM VPNs werden sicherlich – genau wie auch Frame Relay VPNs – gegenüber MPLS stark an Boden verlieren.

IP-Tunnel behalten ihre Bedeutung in Fällen, bei denen Sicherheit durch IPSec erforderlich ist, oder für Einwahlszenarien. Für providerübergreifende VPNs werden sie hingegen nur noch für eine Übergangsphase die Methode der Wahl sein. Ansonsten sind die Weichen für MPLS gestellt.

© ExperTeach GmbH

ExperTeach Gesellschaft für Netzwerkkompetenz mbH
Waldstraße 94 • D-63128 Dietzenbach
Telefon 06074 4868-0 • Telefax 06074 4868-109
info@experteach.de • www.experteach.de

Druckfehler, Irrtümer und Änderungen vorbehalten.
Alle enthaltenen Angaben sind urheberrechtlich geschützt.