



MPLS- und IPSec-VPN

Die Optimierung der Sicherheit im
Unternehmens-WAN

CONTENTS

Einleitung	2
VPN-Technologie	3
Was ist MPLS?	4
Was ist IPSec?	6
Ein Vergleich	7
Vergleich: MPLS-VPN und IPSEC-VPN	7
Quality of Service (QoS)	8
Komplementäre Technologien	9
Die Integration von IPSec in ein MPLS-VPN	9
Die SonicWALL Lösung	10

Einleitung

Rasant expandierende Unternehmen, Firmenfusionen und -übernahmen sowie eine vermehrt auf Informationsaustausch beruhende Geschäftsumgebung haben den Bedarf an sicheren End-to-End-Verbindungen stark erhöht. Die Währung des modernen Handels ist die Information, und die unternehmensweite Bereitstellung und Nutzung dieser Informationen ist das Erfolgsgeheimnis der marktführenden Unternehmen. Veraltete Geschäftsmodelle basierten auf isolierter Informationsverwaltung – jede Abteilung und jeder Geschäftsbereich innerhalb eines Unternehmens verfügte über eigene Daten-Pools, die es zu schützen galt. Das ist heute anders. Im Laufe der Zeit hat sich das Unternehmens-WAN (Wide-Area-Network) immer weiter entwickelt und den individuellen Bedürfnissen und Anforderungen von Unternehmen angepasst; heute ermöglicht es die Hochgeschwindigkeits-Übertragung von Daten zwischen den unterschiedlichsten Standorten, unterstützt diverse Protokolle und bietet exzellenten Service. Nicht nur ein sich schnell vergrößernder Nutzerkreis und der Fernzugriff auf das Netzwerk durch Mitarbeiter in Home Offices auch der externe Zugriff durch Kunden und Partner über Extranets macht ein neues Kommunikationsmodell erforderlich.

Heutzutage werden die einzelnen Arbeitsbereiche miteinander verknüpft, damit sowohl die Mitarbeiter im Unternehmen als auch Partnerfirmen und wichtige Kunden auf die internen Informationen zugreifen können. Diese Servicequalität trägt entscheidend zu den Wettbewerbsvorteilen für ein modernes Unternehmen bei.

Um Informationen nicht wie bisher gegen die Einsicht von außen zu schützen, sondern vielmehr „freizugeben“, ist jedoch eine absolut sichere Netzwerkumgebung mit zuverlässigen Sicherheitstechnologien erforderlich. Mit Technologien wie ATM und Frame Relay konnten mehrere Standorte miteinander verbunden werden und die Grundlage für ein modernes, offenes Unternehmen geschaffen werden. Der Nachteil von ATM und Frame Relay jedoch waren und sind die hohen Kosten und der enorme Investitionsaufwand für Material und Installation/Wartung. Heutzutage ist ein WAN dank IPSec und IP weitaus erschwinglicher geworden, da Unternehmen zur Einrichtung eines eigenen VPN die Freigabe-Ressourcen der Service Provider bzw. auch das Internet nutzen können – und zwar zu einem Bruchteil der Kosten für eine Standleitung bzw. ein Netzwerk des Service Providers. So können Unternehmen kostengünstig viele Einzelstandorte weltweit miteinander verbinden.

VPN-Technologie

Das moderne, auf den Prinzipien Verbindung und Informationsfreigabe basierende Kommunikationsmodell bringt das Problem der Datensicherheit mit sich: Informationen sollen zwar für viele Benutzer zugänglich sein, gleichzeitig aber muss der Zugriff in einem sicheren Rahmen erfolgen. Das VPN (Virtuelles Privates Netzwerk) stellt eine Art logische Verknüpfung der einzelnen Benutzer innerhalb eines größeren Netzwerks dar. Bei VPN wird der Datenverkehr durch einen umfassend geschützten, separaten Tunnel innerhalb eines öffentlichen und gemeinsam genutzten Netzwerks geleitet. Bei dem öffentlichen Netzwerk kann es sich um das Internet oder – wie im Falle von MPLS (Multi Protocol Label Switching) – um das Netzwerk eines Service Providers handeln.

ATM- und Frame Relay-Netzwerke ermöglichten höhere Datenübertragungsraten im WAN und vereinfachten die Verwaltung durch den Einsatz virtueller Leitungen im Frame Relay bzw. ATM-Netzwerk. Doch aufgrund ihrer begrenzten Übertragungsmöglichkeiten für verschiedene Arten von Datenverkehr machten diese beiden Netzwerktechnologien neueren, auf dem Internet-Protokoll basierenden VPN-Lösungen den Weg frei. Diese VPNs gewährleisteten eine höhere Flexibilität beim Versenden unterschiedlicher Arten von Informationen über das Netzwerk. Auf IPSec und MPLS basierende VPNs sind die neue Generation der WANs, die eine Vielzahl von Services anbieten und alle Arten der Datenübertragung unterstützen.

Das zugrunde liegende VPN-Konzept ist dasselbe, dennoch verfügen moderne VPNs über einen größeren Funktionsumfang, sind weitaus sicherer und können verschiedene Arten von Datenverkehr übertragen. Wie bei den meisten Technologien wurden auch hier die Kosten gesenkt, da neue Entwicklungen eine Verbesserung der Funktionalität zu günstigeren Preisen ermöglichen. Die großflächige Einrichtung mehrerer VPNs ist zwar über ein ATM-Netzwerk möglich, jedoch mit hohen Kosten und umfangreichen Upgrades der technischen Ausstattung verbunden, und dies bei einer Einschränkung der Reichweite auf das ATM-Netzwerk selbst. Mit IPSec-VPNs dagegen können sichere Remote-Verbindungen in einer bereits bestehenden, gemeinsam genutzten Infrastruktur über einen offenen Standard eingerichtet werden. Aus der Perspektive der Service Provider wird es allerdings immer schwieriger, Frame Relay- und ATM-Installationen zu unterstützen, da immer mehr Benutzer IP-basierte VPNs mit ihrem höheren Funktionsumfang und niedrigeren Kosten vorziehen.

Die Übertragung unternehmensinterner Daten über das öffentlich zugängliche Internet birgt natürlich eine Vielzahl von Sicherheitsproblemen in sich. Grundsätzlich gewährleisten alle VPNs aufgrund ihrer Fähigkeit, Datenströme zu isolieren und unterschiedliche Benutzergruppen logisch zu gruppieren, eine grundlegende Sicherheit: Benutzer können lediglich die in ihrem VPN vorhandenen Daten anzeigen. Für die meisten Unternehmensabläufe jedoch ist die Isolierung als alleinige Sicherheitsmaßnahme nicht ausreichend und zu stark einschränkend. Auf IPSec basierende VPNs gehen einen Schritt weiter: Sie verwenden Verschlüsselungs- und Authentifizierungstechnologien und schaffen so einen sicheren, privaten Tunnel in einem ansonsten ungeschützten IP-Netzwerk. Eine weitere unerlässliche Maßnahme zum Schutz des Netzwerks vor kombinierten Angriffen ist die Integration einer Sicherheits-Appliance in eine UTM- (Unified Threat Management) Architektur.

Eine Studie von Infonetics Research ergab, dass die kontinuierlichen technischen Neuerungen bei VPNs der Hauptgrund dafür sind, dass Firmen ihre VPN-Produkte aktualisieren. Die Studie besagt weiter, dass über ein Drittel der befragten Unternehmen Sicherheitsbedenken bei der Implementierung von VPNs angab. Sicherheit ist also das entscheidende Thema.

Was ist MPLS?

MPLS (Multi Protocol Label Switching), ein IETF-Standard zur Integration von Netzwerkschichtdaten in IP-basierte Systeme, ist ein IP-basiertes VPN-Modell, das als verwalteter Dienst innerhalb eines proprietären Netzwerks des Service Providers implementiert wird. MPLS wurde konzipiert, um die älteren Frame Relay- bzw. ATM-Technologien zu ersetzen. Im Gegensatz hierzu ist MPLS – wie auch IP – eine Technologie, die Datenverkehr verschiedener Protokolle über den gleichen Kanal übertragen kann.

Für die Service Provider war MPLS als Marketing-Tool äußerst nützlich, garantiert es ihnen doch auch weiterhin lukrative Managed-Service-Verträge. Viele Service Provider spüren deutlich die zurückgehenden Erträge aus dem traditionellen Voice-Geschäft und die Verluste im VPN-Bereich, da immer weniger Kunden Frame Relay- bzw. ATM-Netzwerke nutzen und vielmehr die kostengünstigeren IPSec-VPNs über das öffentliche Internet bevorzugen. Im Gegensatz zum IPSec-VPN wird MPLS als verwalteter Dienst über das Netzwerk des Service Providers ausgeführt und ist daher für diesen weitaus profitabler.

Mit MPLS können zwei oder mehr feste Endpunkte innerhalb des Netzwerks des Service Providers miteinander verbunden werden. Allerdings wird bei MPLS keine zusätzliche Installation auf Benutzerseite durchgeführt und alle Endpunkte müssen sich im Netzwerk des Service Providers befinden. Daher eignet es sich weniger für die Verbindung mit mobilen Remote-Geräten und wird selten eingesetzt, wenn weit entfernte Standorte miteinander verbunden werden sollen. MPLS wird dagegen häufiger verwendet, wenn viele Abteilungen oder Zweigniederlassungen mit zahlreichen Benutzern innerhalb eines räumlich begrenzten Bereichs verbunden werden müssen.

MPLS kennzeichnet jedes IP-Paket mit einem Label, damit alle Pakete aus einer Sitzung in denselben Datenstrom gelangen. Im MPLS-Netzwerk erhält jedes Paket ein Label vom LER (Label Edge Router). Anschließend leitet der LSR (Label Switch Router) die Pakete abhängig von ihrem Label über einen LSP (Label Switch Path) weiter. Bei jeder Etappe entfernt der dortige LSR das aktuelle Label und erstellt ein neues, das dem nächsten LSR mitteilt, wohin er das Paket weiterleiten soll.

Der LSP ist gut geeignet, um Überlastungen im Netzwerk und Verbindungsausfälle zu umgehen und eine gleich bleibende Verfügbarkeit zu gewährleisten. Die Technologie kann effektiv zur Datenweiterleitung zwischen Standorten in einem verwalteten Netz verwendet werden und erfordert kein Eingreifen des Endbenutzers. Der LSP ist vergleichbar mit den Circuit-Switched-Pfaden im ATM-Netzwerk. Daneben kann MPLS, wie ATM auch, eine Bandbreite für unterschiedliche Arten von Datenverkehr garantieren – ein großer Vorteil bei der Übertragung von Daten, die keine Latenzzeit gestatten.

Der LSP ermöglicht Providern zu entscheiden, ob der Datenverkehr nach Datentyp oder Kundenkategorie weitergeleitet werden soll. Dank der Label kann das Netzwerk die Datenübertragung mit hoher Priorität wie

Audio- oder Videodaten in eigene Datenströme aufteilen. MPLS ist zwar ideal zur Einrichtung von Verbindungen zwischen zwei Standorten geeignet, ist aber nicht hinreichend effizient für Verbindungen zwischen einem Benutzer und einem Standort oder für Remote-Zugriffe. Die einzelnen Standorte können nur dann miteinander verbunden werden, wenn der Service Provider die jeweilige Infrastruktur bereits eingerichtet hat – die Verbindung ist also immer abhängig vom Netzwerk des Service Providers. Das Konzept von MPLS sah keine Verbindungen zwischen mobilen Mitarbeitern und der Unternehmenszentrale vor. Für diese Verbindungsart bieten sich IPSec- oder SSL-VPNs an. MPLS ist zwar bei der Einrichtung eines Mehrprotokollkanals von Nutzen, bietet jedoch keine Sicherungsmechanismen bei der Datenübertragung selbst. Ein MPLS-VPN bietet ebenso wie ATM oder Frame Relay die Möglichkeit der Datenisolierung, benötigt aber IPSec, um Daten zu verschlüsseln. Theoretisch ist es also vorstellbar, dass ein VPN von einem anderen VPN „angegriffen“ wird, wobei dieses Risiko durch die entsprechende Konfiguration minimiert werden kann. Dennoch gibt es viele Möglichkeiten zur Fehlkonfiguration, die von Angreifern schamlos ausgenutzt werden können.

Der Hauptgedanke bei MPLS war nicht die Konzipierung einer sicheren Protokolls; vielmehr sollte mit Hilfe von Paket-Labels die Datenübertragung beschleunigt werden, was auch gut gelungen ist. Da MPLS die Pakete jedoch nicht verschlüsselt, macht sie dies anfällig für Angriffe, Abhörversuche und andere gefährliche Hacker-Aktionen. Außerdem kann die Adresse des Absenders bzw. das MPLS-Label selbst gespoofed werden. Das bedeutet nicht, dass die MPLS-Technologie unzulänglich ist; es sollte lediglich darauf geachtet werden, dass eine MPLS-Installation stets eine zusätzliche Sicherheitsfunktion benötigt. Eine solche Sicherheitsfunktion kann beispielsweise auf Unternehmensseite in Form einer separaten Firewall im IPSec-VPN erfolgen.

MPLS kann alle Knoten eines Netzwerks kreuz und quer miteinander verbinden (Full-Mesh-Verbindung). Dies scheint ein Vorteil zu sein, doch angesichts von Hochgeschwindigkeits-Datenübertragung und der entsprechenden Bandbreite relativiert sich dieser Vorteil. Technologien wie Frame Relay, die vor MPLS konzipiert wurden, verwendeten eine Sternstruktur (Hub-and-Spoke). Dieser Ansatz hat gegenüber MPLS einen klaren Vorteil: Sicherheitsmaßnahmen können weitaus leichter zentral verteilt werden, das Netzwerk bleibt vor Viren, Würmern, Spyware und anderen Bedrohungen geschützt.

Ein Beispiel: Angenommen, die Niederlassung eines Unternehmens in Düsseldorf verfügt über eine DS3-Verbindung zu einem MPLS-Netzwerk, während die Niederlassung in Berlin eine Fractional-DS3-Verbindung besitzt. Hat sich nun das Düsseldorfer Büro mit einer kombinierten Bedrohung infiziert, könnte sich die Infektion auf die MPLS-Verbindungen ausweiten, die Verbindung zum Berliner Büro überlasten und einen DoS- (Denial-of-Service) Angriff auslösen. Ein weiteres Beispiel: Angenommen, die Computer einer Bank sind über ein ATM-Netzwerk verbunden. Auf diesen Computern wird häufig eine ältere Windows-Version ausgeführt, die bekanntermaßen anfällig für kombinierte Angriffe ist. Gehen wir weiter davon aus, dass ein technischer Mitarbeiter nun ein (unwissentlich) Wurm-infiziertes Laptop an das Netzwerk anschließt. Die Folge ist, dass alle ATM-Computer im Netzwerk gleichzeitig infiziert werden, der Datenverkehr drastisch zunimmt und das Datencenter und mit ihm das gesamte Netzwerk unter der Überlastung zusammenbricht.

Angesichts dieser potenziellen Bedrohungen können MPLS-Netzwerke nur geschützt werden, indem der Datenverkehr vor seiner Einleitung in das WAN isoliert wird. Dazu müssen komplexe Sicherheits-Appliances an jedem Verbindungspunkt im MPLS-Netzwerk eingesetzt werden.

Der erforderliche Schutz kann durch den Einsatz einer Sicherheits-Appliance mit UTM (Unified Threat Management) realisiert werden. Hierbei werden verschiedene Sicherheitsfunktionen wie Firewall, Virenschutz, Intrusion Detection und Intrusion Prevention in einer einzigen Hardware-Plattform integriert.

Was ist IPSec?

Die allgegenwärtige Breitband-Verfügbarkeit hat für Aufwind in der Netzwerkbranche gesorgt, da immer mehr Unternehmen die Vorteile immer kostengünstigerer Verbindungsmöglichkeiten zwischen einzelnen Standorten, mobilen Mitarbeitern, Partnerfirmen und wichtigen Kunden mit dem Firmenhauptsitz nutzen. Eine Breitband-Verbindung allein macht jedoch noch kein VPN; hierfür ist die Installation einer weiteren Technologie, wie z.B. IPSec (IP Security), erforderlich. IPSec wurde als Authentifizierungs- und Verschlüsselungsstandard für die Daten innerhalb eines IP-Netzwerks sowie für den Datenschutz von Netzwerkressourcen entwickelt.

Ein entscheidender Faktor bei der Implementierung von IPSec sind die Gesamtbetriebskosten (TCO). Mit IPSec können Benutzer eine günstige Internet-Verbindung nutzen und gleichzeitig ein sicheres, vollverknüpftes WAN mit der neuesten Technologie einrichten. Als verbindungsunabhängige Technologie ermöglichen IPSec-VPNs, insbesondere mit Remote-SSL-Funktionalität für einzelne mobile Benutzer, vollfunktionale Verbindungen zwischen zwei oder mehr beliebigen Punkten in der ganzen Welt.

Während IP-VPNs (z.B. MPLS-Netze) nur wenig Sicherheit bieten, war IPSec von Anfang an als sicheres Protokoll konzipiert. Ein IPSec-VPN gewährleistet Datensicherheit und -integrität, auch bei Remote-Access-Lösungen an mehreren Standorten. Als Teil des Ipv6-IETF-Protokolls umfasst IPSec neben Verschlüsselungs- und Authentifizierungsfunktionen auch die Schlüsselverwaltung und deckt somit diese drei, für die Sicherheit entscheidenden, Bereiche ab, die z.B. bei TCP/IP fehlen.

Mittlerweile hat sich IPSec zu einem Standard in der Implementierung von VPNs entwickelt – nicht allein wegen der inhärenten Sicherheit, sondern auch, weil keine zusätzlichen Hardware-Komponenten oder Umrüstungsmaßnahmen für die einzelnen Client-Arbeitsplätze erforderlich sind.

Neben der Verbindung zur Unternehmenszentrale ist es den meisten Firmen wichtig, dass jeder Endpunkt im Netzwerk mit dem Internet verbunden werden kann. Da ein IPSec-VPN das öffentlich zugängliche Internet nutzt, kann es problemlos ohne weitere technische Maßnahmen installiert werden. Optional kann auch ein MPLS-VPN mit dem Internet verbunden werden, dazu ist in der Regel jedoch eine dezidierte Internet-Leitung erforderlich.

Viele Service Provider bieten nun auch dort IPSec-VPN-Dienste an, wo sie bereits das IPSec-Gateway verwalten, obwohl die Installation normalerweise direkt auf der Kundenseite erfolgt. Dieses Managed-Service-Paket enthält meist eine Leistungsgarantie des Service Providers.

Ein Vergleich

Entgegen der Darstellung einiger Hersteller sind MPLS und IPSec keine miteinander konkurrierenden Produkte, sondern decken jeweils einen ganz bestimmten Funktionsbereich ab. So eignet sich MPLS (IP-VPN) vor allem zur Einrichtung fester Site-to-Site-Verbindungen und weniger für Client-to-Site-, Remote-Site- oder mobile Umgebungen. Darüber hinaus ist das IP-VPN in Sicherheitsfragen bei der Datenübertragung weniger zuverlässig. IPSec dagegen wurde als maximal sicheres Verbindungsmodell konzipiert. In einem auf dem IPSec-Protokoll basierenden VPN sind Daten sowohl durch Verschlüsselung als auch Authentifizierung geschützt.

Vergleich: MPLS-VPN und IPSEC-VPN

Funktion	MPLS-VPN (IP-VPN)	IPSec-VPN
Site-to-Site-Verbindung	Ja	Ja
Full-Mesh-Verbindung	Ja	Ja
QoS und Bandbreiten-Management	Ja (CoS)	Ja (granulare QoS)
Client-to-Site-Verbindung	Nein	Ja
AES-256-Bit-Verschlüsselung	Nein	Ja
PKI-basierte Authentifizierung	Nein	Ja
weltweite Verfügbarkeit	Nein	Ja
Interoperabilität mit verschiedenen Service Providern	Nein	Ja
Vertrag mit dem Service Provider erforderlich	Ja	Nein
Implementierungskosten	€€€€	€€
Monatliche Bandbreitenkosten	€€	€

Sei es im Internet oder im Netzwerk des Service Providers: Das Weiterleiten von Daten über den optimalen Pfad ist von höchster Wichtigkeit. Bezüglich der erneuten Weiterleitung hält MPLS stets einen zweiten, alternativen Pfad durch das Netzwerk bereit: Ist der Hauptpfad nicht durchlässig, kann MPLS den Datenverkehr über einen Sicherungspfad weiterleiten. Kann auf diesen allerdings auch nicht zugegriffen werden, muss ein dritter Pfad manuell erstellt werden. IPSec dagegen verwendet dynamische Routing-Protokolle: Pfadauslastungen werden automatisch entdeckt, der Datenverkehr wird entsprechend umgeleitet.

IPSec ist ein ausgereiftes und sicheres Modell, das aufgrund von End-to-End-Authentifizierung und -Verschlüsselung die optimale Sicherheitsumgebung darstellt. Auf der anderen Seite ist MPLS ein neueres Modell, das herkömmliche ATM- oder Frame Relay-Konzepte bei der Verbindung weitläufiger, fester

Standorte ersetzen kann. IPSec kann quasi überall implementiert werden, da es über das Internet ausgeführt wird, während sich die Verfügbarkeit von MPLS auf das Netz des Service Providers beschränkt.

Die Verwendung von Labels bei MPLS gewährleistet eine effiziente Datenübertragung im Service-Provider-Netzwerk. Zudem werden Garantien für die Bandbreitenverfügbarkeit und das Service-Level gegeben. Auch IPSec-VPNs werden mit einer Funktion für Bandbreiten-Management angeboten, und die drastisch fallenden Kosten für zusätzliche Bandbreite machen IPSec-VPNs zu einer kostengünstigeren und mindestens ebenso leistungsstarken Alternative wie MPLS-VPNs.

Der Nachteil von MPLS gegenüber IPSec ist die fehlende zuverlässige Verschlüsselung und Authentifizierung, was nicht bedeutet, dass MPLS-Netzwerke überhaupt keine Sicherheit gewährleisten: Dank der MPLS-Strategie zur Isolierung von VPN-Datenströmen, welche einen gewissen Schutz für die Daten bietet, sind Angreifer kaum in der Lage, über eine separate VPN-Öffnung auf Bereiche des Netzwerks zuzugreifen. Doch trotz Isolierung werden Pakete in MPLS-VPNs weder verschlüsselt noch durch Authentifizierung geschützt. Wenn strenge Sicherheitsrichtlinien erforderlich sind, kann der Datenverkehr über IPSec verschlüsselt werden, ehe er in MPLS verkapselt wird.

Diese Erwägungen machen deutlich, dass MPLS wohl kaum einen Ersatz für IPSec-VPN darstellen kann. Bei der Einrichtung großflächiger Site-to-Site-Verbindungen können ATM oder Frame Relay effektiv durch MPLS ersetzt werden – optimale Sicherheit und Reichweite liefert erst die zusätzliche Verwendung von IPSec-VPNs.

Quality of Service (QoS)

Schon früh galt in ATM-Netzwerken das QoS-Konzept, mit dem Latenzzeiten, Paketverluste und Jitter reduziert werden konnten. Trotz der hohen Kosten wurden diese QoS-Eigenschaften für einige Unternehmen so bedeutend, dass sie die damit verbundenen Investitionen in Kauf nahmen. Bei der Übertragung von Standarddaten spielt QoS eine weniger wichtige Rolle, bei der Übertragung verschiedener Protokolle (sowohl Daten als auch Voice) über dieselbe Leitung wird QoS dagegen immer wichtiger. Besonders durch die Einführung, Entwicklung und weite Verbreitung von VoIP ist der Bedarf an QoS im Unternehmensnetzwerk deutlich gestiegen, da gerade bei diesen Anwendungen Unregelmäßigkeiten in der Übertragung (z.B. Latenzzeiten) vermieden werden sollen.

Hinsichtlich des Quality of Service (QoS) bietet MPLS eine Bandbreitengarantie zwischen dem Unternehmensstandort und dem Netzwerk des Service Providers. MPLS bietet Site-to-Site-Routing und grundlegende Management-Funktionalität ohne Eingreifen des Endbenutzers. QoS gilt jedoch nur für die komplette Verbindung. Das MPLS-Netzwerk hingegen erkennt nur den Inhalt des Paket-Headers. Diese Unterscheidung ist heute besonders wichtig geworden, vor allem für Service Provider, die "Dreifach-Pakete" anbieten, bei denen Voice, Video und Internet über denselben Kanal übertragen werden.

Wichtig hierbei ist die Unterscheidung zwischen Quality of Service (QoS) und Class of Service (CoS). "Class of Service" bezeichnet die Differenzierung des Netzwerkverkehrs; die Label-Funktion von MPLS dient genau diesem Zweck. "Quality of Service" dagegen bezieht sich auf die Leistungsstärke des Netzwerks und den Umgang mit Problemen, wie z.B. Latenzzeiten und Jitter. MPLS wurde entwickelt, um CoS-Funktionalität anzubieten und die Möglichkeit, unterschiedliche Datenströme effektiv zu verwalten und weiterzuleiten.

Während CoS durch Aufteilen der Datenströme in Daten, Video oder VoIP den gesamten Datenstrom formt, so dass die Routing-Funktion des Netzwerks den unterschiedlichen Datenströmen individuelle Prioritäten zuweisen kann, agiert QoS eher auf der Ebene der einzelnen Datenpakete und in der Schicht über den CoS-Parametern.

Auch wenn CoS für den gesamten Datenverkehr, der durch ein MPLS- (bzw. ATM- oder Frame Relay-) Netzwerk geleitet wird, gilt, muss doch erwähnt werden, dass die Klassifizierung erfolgen muss, noch bevor die übertragenen Daten den Router am Netzwerkrand erreichen. Neben Klassifizierungsfunktionen verfügen optimale Netzwerkumgebungen zusätzlich über Bandbreiten-Management und QoS-Funktionen.

Durch die Gruppierung verschiedener Kategorien von Datenverkehr kann MPLS verschiedene CoS differenzieren. Aus Sicht des Service Providers ist dies ein Vorteil, der sich indirekt als QoS für den Kunden darstellt: Die von ihm versendeten Daten haben ihre eigene Kategoriengruppierung. Auf diese Weise garantiert MPLS die Bandbreite zwischen dem Unternehmensstandort und dem ISP sowie zwischen dem ISP und dem Remote-Standort. Diese Garantie gilt jedoch nur für die komplette Verbindung. Abgesehen von der Label-Funktion kann MPLS nicht zwischen verschiedenen Arten von Datenverkehr (wie z.B. Voice oder Daten) unterscheiden und daher auch keine wirkliche QoS-Umgebung bereitstellen.

Komplementäre Technologien

Zwar wird diskutiert, welches der Protokolle sich als tatsächlicher Standard für VPN-Verbindungen erweisen kann, doch gehen derartige Diskussionen am Ziel vorbei: Bei der Einrichtung einer zuverlässigen und optimal geschützten Umgebung können Unternehmen wie auch Service Provider sowohl MPLS als auch IPSec einsetzen und die Vorteile beider Protokolle nutzen. Service Provider können ihre Angebotspalette erweitern und als Wettbewerbsvorteil nutzen. Unternehmen, die eine integrierte IPSec-/MPLS-Umgebung implementieren, erhalten so ein vollständiges und umfassend geschütztes Intranet/Extranet mit sicheren Remote-VPN-Funktionen.

Das Ziel einer VPN-Lösung ist es, die Firmenzentrale mit den Mitarbeitern, Kunden, Zweigniederlassungen und jedem Benutzer, der jenseits der Firewall auf interne Inhalte zugreifen möchte, nahtlos zu verbinden. Ein MPLS-Netzwerk ist bei der Einrichtung großflächiger Site-to-Site-Verbindungen von Vorteil. Da es jedoch eine verbindungsorientierte Technik ist, können Standorte außerhalb der MPLS-Reichweite nicht auf das Netz zugreifen. IPSec dagegen ist eine verbindungslose Technologie, die Standorte auf der ganzen Welt einbeziehen kann, da sie das öffentlich zugängliche Internet als Backbone nutzt. Mit zunehmender Größe des Extranets eines Unternehmens durch die Integration weiterer Teilnehmer wird die Implementierung eines MPLS-Netzes immer schwieriger. Durch die Nutzung von IPSec kann die Reichweite von MPLS ausgebaut und eine Verbindungsqualität erreicht werden, die den Anforderungen moderner Unternehmen gerecht wird.

Die Integration von IPSec in ein MPLS-VPN

Mit IPSec können erhebliche Kosten eingespart werden – ganz gleich, ob das Internet, ein privates IP- oder ein MPLS-Netzwerk als Backbone genutzt wird. Ein Service Provider kann IPSec-VPNs zu seinem MPLS-Netzwerk hinzufügen und mit dem zugrunde liegenden VPN-Netz verbinden. Er profitiert dann von verbesserter Skalierbarkeit, Sicherheit und QoS-Funktionalität. MPLS wird üblicherweise als verwalteter

Dienst angeboten, wobei das VPN im IP-Netz des Service Providers beginnt und endet. Ein IPSec-VPN dagegen beginnt und endet im CPE (Customer Premises Equipment) und wird häufig vom Kunden selbst verwaltet (einige Service Provider bieten auch IPSec-basierte VPNs als verwalteten Dienst an). Eine kombinierte Lösung stellt also eine echte Alternative dar.

Neben dem Ausbau der Reichweite des MPLS-Netzwerks kann durch die Kombination der beiden Technologien Redundanz erzielt werden. Hierbei dient das IPSec-VPN aus Kostengründen als redundante Verbindung. Die beiden Technologien lassen sich einfach integrieren: Die MPLS-Arbeitsgruppe verfügt über eine Spezifikation zur Verkapselung von MPLS in das Internet-Protokoll, so dass MPLS-Pakete mit Hilfe von IPSec sicher auch in einem Nicht-MPLS-Netzwerk versendet werden können und die Daten durch Verschlüsselung und Authentifizierung geschützt sind.

Einige Service Provider bieten bereits kombinierte Lösungen an, bei denen flexible VPN-Umgebungen ganz den individuellen Bedürfnissen des Kunden angepasst werden können.

Die SonicWALL Lösung

Zur Verteilung und Installation von VPNs werden meist Firewalls eingesetzt. Infonetics zufolge spielen die Kosten bei der Einrichtung von VPN die wichtigste Rolle; besonders in den Bereichen Bildungswesen und Einzelhandel wird daher häufig auf VPN verzichtet. Aus diesem Grund setzen die meisten Unternehmen IPSec-VPNs ein, die auch in den Sicherheits-Appliances von SonicWALL verwendet werden. SonicWALL geht Klassifizierungsprobleme weitaus gezielter und umfassender als andere Lösungen an und bietet neben CoS- auch QoS-Funktionen und Bandbreiten-Management an, also genau die drei Elemente, die für Unternehmenskunden am wichtigsten sind.

Die SonicWALL Produktreihe von Internet-Sicherheits-Appliances bildet die vorderste Verteidigungslinie vor allen Sicherheitsbedrohungen aus dem Internet. Durch die Einrichtung einer UTM-Umgebung erweitert SonicWALL die allgemeine Sicherheit, da mehrere Sicherheitsfunktionen in dasselbe Gerät und denselben Verwaltungsbereich integriert werden. Zusätzlich verhindert UTM die Ausbreitung von Viren, Würmern und Spyware im WAN. Ohne UTM ist ein Unternehmen nicht in der Lage, potenziell gefährdete Standorte zu isolieren, so dass sich Infektionen im gesamten Intranet ausbreiten können. Gerade in einem MPLS-Netzwerk sollte UTM nicht fehlen – die Kombination von MPLS mit SonicWALL IPSec-VPN ist daher die ideale Lösung für Unternehmen jeder Größe.

Die SonicWALL UTM-Lösung schützt sowohl vor internen als auch externen Bedrohungen, einschließlich kombinierten Angriffsarten. Die Appliance überwacht diverse Zugangspunkte und durchsucht jede Netzwerkebene; die Deep-Packet-Inspection-Engine überprüft eine Vielzahl verschiedener Anwendungen und Protokolle und gleicht Dateien mit einer umfangreichen Signaturdatenbank ab. Die SonicWALL Deep-Packet-Inspection (DPI) geht dabei über Stateful-Packet-Inspection hinaus und gleicht alle heruntergeladenen, per E-Mail versendeten und komprimierten Dateien mit der Angriffssignatur-Datenbank ab.

In Ihre MPLS-Umgebung integriert, erweitert SonicWALL Ihre VoIP-Umgebung um Funktionen zur aktiven Anrufüberwachung, Protokollierung und Berichterstellung. Außerdem können Sie VoIP-Endpunkte vor DoS- (Denial-of-Service) Angriffen und anderem bösartigen Datenverkehr schützen. Zusätzlich erhalten Sie QoS

auch über VPN/WAN-Verbindungen und mithilfe des Bandbreiten-Managements kann WAN-Bandbreite für wichtigen Datenverkehr reserviert werden (QoS). Durch den Zugriff auf den WAN-Datenverkehr kann das SonicOS den Datenverkehr klassifizieren und mit einem Label versehen. Die SonicWALL Appliance verfügt über inhärente QoS-Funktionalität. Die Verwendung der standardmäßigen 802.1p- und der DSCP-(Differentiated Service Code Points) CoS-Bezeichner gewährleistet leistungsstarkes Bandbreiten-Management, das für VoIP- und andere IP-basierte Dienste unerlässlich ist.

Integriert in eine einzige, benutzerfreundliche Plattform verfügt SonicWALL über eine ICSA-zertifizierte Deep-Packet-Inspection Firewall, IPSec-VPN für den Remote-Zugriff, Funktionen zur IP-Adressverwaltung und unterstützt Virenschutz, Anti-Spyware, Intrusion-Prevention und Content-Filtering. Die SonicWALL-Sicherheits-Appliances ergänzen MPLS-Netzwerke um entscheidende Funktionen.

Das hohe Maß an Integration der SonicWALL Appliances beruht auf dem ausgereiften SonicOS Betriebssystem, das vor den weit verbreiteten Angriffen, die auf die Sicherheitslücken der handelsüblichen Betriebssysteme abzielen, schützt. SonicOS bietet neben WAN-Redundanz und Lastausgleich auch Sicherungsfunktionen beim Ausfall des Service Providers bzw. der Hardware; objektorientierte Verwaltungsfunktionen ermöglichen die einfache und konsistente Handhabung der Sicherheitsrichtlinien. Sämtliche SonicWALL Appliances verfügen über skalierbare VPN-Funktionen, die einzelne Home Offices, kleine und mittlere Unternehmen, und auch Unternehmensumgebungen mit Tausenden von VPNs unterstützen.