So funktionieren virtuelle private Netzwerke

Inhalt

Einführung

In diesem Dokument werden die Grundlagen von VPNs beschrieben, z. B. grundlegende VPN-Komponenten, Technologien, Tunneling und VPN-Sicherheit.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

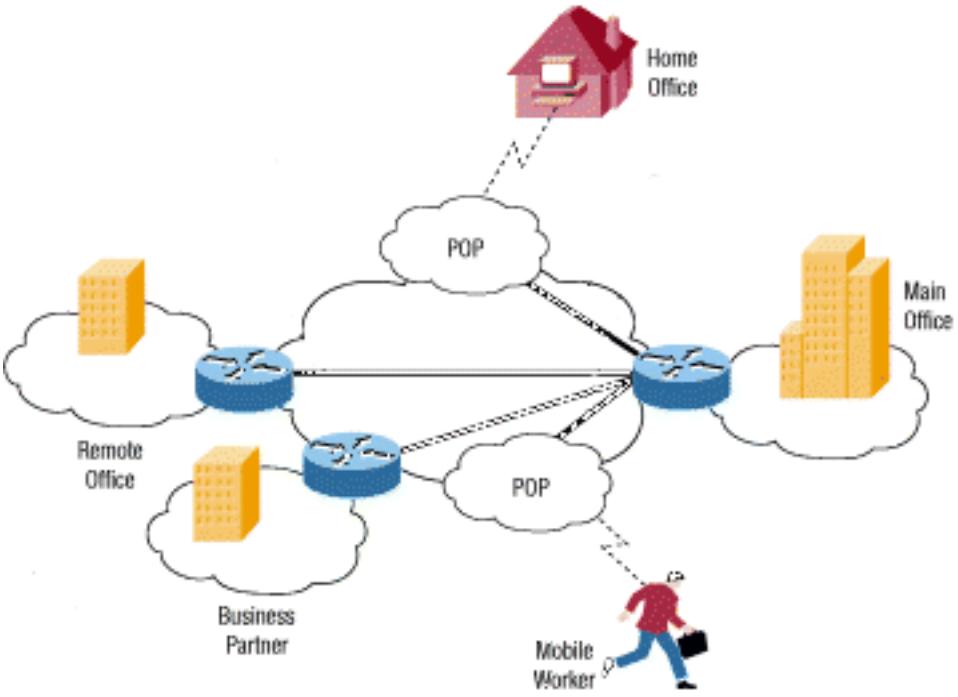
Hintergrundinformationen

Die Welt hat sich in den letzten Jahrzehnten stark verändert. Statt sich einfach mit lokalen oder regionalen Belangen auseinanderzusetzen, müssen viele Unternehmen jetzt über globale Märkte und Logistik nachdenken. Viele Unternehmen verfügen über Einrichtungen, die sich über das ganze Land oder sogar auf der ganzen Welt verteilen. Es gibt aber eines, das alle Unternehmen

brauchen: eine Möglichkeit, eine schnelle, sichere und zuverlässige Kommunikation an allen Standorten zu gewährleisten.

Bis vor Kurzem war für eine zuverlässige Kommunikation die Nutzung von Mietleitungen erforderlich, um ein WAN (Wide Area Network) zu unterhalten. Mietleitungen reichen von Integrated Services Digital Network (ISDN mit 144 Kbit/s) bis hin zu Glasfaserkabeln des Optical Carrier-3 (OC3 mit 155 Mbit/s) und bieten dem Unternehmen die Möglichkeit, sein privates Netzwerk über die unmittelbare geografische Region hinaus zu erweitern. Ein WAN bietet gegenüber einem öffentlichen Netzwerk wie dem Internet deutliche Vorteile in Bezug auf Zuverlässigkeit, Leistung und Sicherheit. Die Wartung eines WAN, insbesondere bei der Nutzung von Mietleitungen, kann jedoch sehr teuer werden (häufig steigen die Kosten, wenn die Entfernung zwischen den Niederlassungen zunimmt). Darüber hinaus stellen Mietleitungen keine praktikable Lösung für Unternehmen dar, in denen ein Teil der Belegschaft (wie bei den Marketingmitarbeitern) sehr mobil ist und häufig eine Verbindung zum Unternehmensnetzwerk herstellen und auf vertrauliche Daten zugreifen müssen.

Mit der zunehmenden Beliebtheit des Internets haben Unternehmen das Internet als Mittel zur Erweiterung ihrer eigenen Netzwerke genutzt. Als Erstes kamen Intranets auf den Markt, die ausschließlich für die Verwendung durch Mitarbeiter des Unternehmens vorgesehen sind. Viele Unternehmen erstellen jetzt ihre eigenen Virtual Private Networks (VPNs), um die Anforderungen von Mitarbeitern an entfernten Standorten und von entfernten Standorten zu erfüllen.



Ein typisches VPN kann ein lokales Hauptnetzwerk (LAN) in der Firmenzentrale, andere LANs in Außenstellen oder Einrichtungen und einzelne Benutzer haben, die eine Verbindung von außerhalb herstellen.

Ein VPN ist ein privates Netzwerk, das ein öffentliches Netzwerk (in der Regel das Internet) verwendet, um Remote-Standorte oder Benutzer miteinander zu verbinden. Anstatt eine dedizierte, reale Verbindung wie eine Mietleitung zu verwenden, verwendet ein VPN "virtuelle" Verbindungen, die über das Internet vom privaten Netzwerk des Unternehmens zum Remote-Standort oder Mitarbeiter geroutet werden.

Was macht ein VPN?

Es gibt zwei gängige VPN-Typen.

- **Remote-Zugriff** - Dies wird auch als Virtual Private Dial-up Network (VPDN) bezeichnet und ist eine Benutzer-zu-LAN-Verbindung, die von einem Unternehmen verwendet wird, dessen Mitarbeiter von verschiedenen Remote-Standorten aus eine Verbindung zum privaten Netzwerk herstellen müssen. In der Regel stellt ein Unternehmen, das ein großes Remote-Access-VPN einrichten möchte, seinen Benutzern über einen Internet-Service-Provider (ISP) eine Art Internet-Einwahlkonto zur Verfügung. Die Telearbeiter können dann eine 1-800-Nummer wählen, um ins Internet zu gelangen, und ihre VPN-Client-Software für den Zugriff auf das Unternehmensnetzwerk verwenden. Ein gutes Beispiel für ein Unternehmen, das ein Remote-Access-VPN benötigt, wäre ein großes Unternehmen mit Hunderten von Vertriebsmitarbeitern vor Ort. VPNs mit Remote-Zugriff ermöglichen sichere, verschlüsselte Verbindungen zwischen dem privaten Netzwerk eines Unternehmens und Remote-Benutzern über einen Drittanbieter.
- **Site-to-Site** - Durch die Verwendung dedizierter Geräte und eine umfangreiche Verschlüsselung kann ein Unternehmen mehrere feste Standorte über ein öffentliches Netzwerk wie das Internet verbinden. Jeder Standort benötigt nur eine lokale Verbindung mit demselben öffentlichen Netzwerk, wodurch Kosten für lange private Mietleitungen eingespart werden. Site-to-Site-VPNs können weiter in Intranets oder Extranets kategorisiert werden. Ein Site-to-Site-VPN, das zwischen Standorten desselben Unternehmens aufgebaut ist, gilt als Intranet-VPN, während ein VPN, das für die Verbindung des Unternehmens mit seinem Partner oder Kunden erstellt wurde, als Extranet-VPN bezeichnet wird.

Ein gut durchdachtes VPN kann einem Unternehmen enorme Vorteile bringen. Sie kann beispielsweise:

- Erweiterung der geografischen Anbindung
- Senkung der Betriebskosten im Vergleich zu herkömmlichen WANs
- Reduzierung von Transit- und Reisekosten für Remote-Benutzer
- Produktivitätssteigerung
- Vereinfachung der Netzwerktopologie
- Bereitstellung globaler Netzwerkchancen
- Unterstützung von Telearbeitern
- Schnellerer Return on Investment (ROI) als bei herkömmlichem WAN

Welche Funktionen sind für ein gut entwickeltes VPN erforderlich? Sie sollte folgende Punkte enthalten:

- Sicherheit
- Zuverlässigkeit
- Skalierbarkeit
- Netzwerkmanagement
- Richtlinienmanagement

Analogie: Jedes LAN ist ein IsLANd

Stellen Sie sich vor, Sie leben auf einer Insel in einem riesigen Ozean. Es gibt Tausende von anderen Inseln um Sie herum, einige sehr nah und andere weiter entfernt. Normalerweise fahren Sie mit einer Fähre von Ihrer Insel zu der Insel, die Sie besuchen möchten. Mit der Fähre zu fahren, bedeutet, dass man fast keine Privatsphäre hat. Alles, was Sie tun, können Sie von einem

anderen sehen.

Angenommen, jede Insel repräsentiert ein privates LAN und der Ozean ist das Internet. Wenn Sie mit der Fähre fahren, ist es ähnlich, wenn Sie über das Internet eine Verbindung zu einem Webserver oder einem anderen Gerät herstellen. Sie haben keine Kontrolle über die Drähte und Router, aus denen das Internet besteht, genau wie Sie keine Kontrolle über die anderen Personen auf der Fähre haben. Dadurch sind Sie anfällig für Sicherheitsprobleme, wenn Sie versuchen, eine Verbindung zwischen zwei privaten Netzwerken über eine öffentliche Ressource herzustellen.

Ihre Insel beschließt, eine Brücke zu einer anderen Insel zu bauen, damit es eine einfachere, sicherere und direktere Möglichkeit für die Menschen gibt, zwischen den beiden zu reisen. Es ist teuer, die Brücke zu bauen und zu warten, obwohl die Insel, mit der Sie verbunden sind, sehr nah ist. Aber der Bedarf an einem zuverlässigen, sicheren Pfad ist so groß, dass man es trotzdem macht. Ihre Insel möchte eine zweite Insel anschließen, die viel weiter entfernt ist, aber Sie entscheiden, dass sie zu teuer ist.

Diese Situation ist sehr ähnlich wie eine Mietleitung. Die Brücken (Mietleitungen) sind vom Ozean getrennt (Internet), aber sie können die Inseln (LANs) miteinander verbinden. Viele Unternehmen haben sich für diesen Weg entschieden, weil sie ihre Außenstellen sicher und zuverlässig miteinander verbinden müssen. Wenn die Büros jedoch sehr weit auseinander liegen, können die Kosten hoch sein - genau wie der Versuch, eine Brücke zu bauen, die sich über große Entfernungen erstreckt.

Wie passt VPN in diese Analogie? Wir könnten jedem Bewohner unserer Inseln ein eigenes kleines U-Boot mit diesen Eigenschaften geben.

- Es ist schnell.
- Es ist leicht, mit Ihnen zu nehmen, wohin Sie gehen.
- Sie kann Sie komplett vor allen anderen Booten oder U-Booten verstecken.
- Sie ist zuverlässig.
- Es kostet wenig, zusätzliche U-Boote zu Ihrer Flotte hinzuzufügen, sobald die erste gekauft wurde.

Obwohl sie zusammen mit anderem Verkehr im Ozean unterwegs sind, konnten die Einwohner unserer beiden Inseln immer wieder in Ruhe und Sicherheit reisen. So funktioniert ein VPN. Jedes Remote-Mitglied Ihres Netzwerks kann sicher und zuverlässig kommunizieren, indem es das Internet als Medium für die Verbindung mit dem privaten LAN nutzt. Ein VPN kann erweitert werden, um mehr Benutzer und verschiedene Standorte besser aufnehmen zu können als eine Mietleitung. Die Skalierbarkeit ist ein großer Vorteil von VPNs gegenüber herkömmlichen Mietleitungen. Im Gegensatz zu Mietleitungen, bei denen die Kosten im Verhältnis zu den Entfernungen steigen, sind die geografischen Standorte der einzelnen Niederlassungen bei der Erstellung eines VPNs wenig wichtig.

VPN-Technologien

Ein gut entwickeltes VPN verwendet verschiedene Methoden, um Ihre Verbindung und Daten sicher zu halten.

- **Datenvertraulichkeit**: Dies ist möglicherweise der wichtigste Service, der von einer VPN-Implementierung bereitgestellt wird. Da Ihre privaten Daten über ein öffentliches Netzwerk übertragen werden, ist die Vertraulichkeit der Daten unerlässlich und kann durch die Verschlüsselung der Daten erreicht werden. Dabei werden alle Daten, die ein Computer an

einen anderen sendet, in eine Form codiert, die nur der andere Computer decodieren kann.Die meisten VPNs verwenden eines dieser Protokolle, um Verschlüsselung bereitzustellen.**IPsec** - Internet Protocol Security Protocol (IPsec) bietet erweiterte Sicherheitsfunktionen wie stärkere Verschlüsselungsalgorithmen und eine umfassendere Authentifizierung. IPsec verfügt über zwei Verschlüsselungsmodi: Tunnel und Transport. Der Tunnelmodus verschlüsselt den Header und die Nutzlast jedes Pakets, während der Transportmodus nur die Nutzlast verschlüsselt. Nur IPsec-konforme Systeme können dieses Protokoll nutzen. Alle Geräte müssen außerdem einen gemeinsamen Schlüssel oder ein gemeinsames Zertifikat verwenden und über sehr ähnliche Sicherheitsrichtlinien verfügen.Für Remote-Access-VPN-Benutzer stellt ein Softwarepaket eines Drittanbieters die Verbindung und Verschlüsselung auf dem Benutzer-PC bereit. IPsec unterstützt entweder 56-Bit-Verschlüsselung (eine DES-Verschlüsselung) oder 168-Bit-Verschlüsselung (Triple-DES-Verschlüsselung).**PPTP/MPPE** - PPTP wurde vom PPTP Forum erstellt, einem Konsortium, das US Robotics, Microsoft, 3COM, Ascend und ECI Telematics umfasst. PPTP unterstützt Multi-Protocol-VPNs mit 40-Bit- und 128-Bit-Verschlüsselung unter Verwendung des Protokolls Microsoft Point-to-Point Encryption (MPPE). Es ist zu beachten, dass PPTP selbst keine Datenverschlüsselung bereitstellt.**L2TP/IPsec** - Wird häufig als L2TP über IPsec bezeichnet und sorgt so für die Sicherheit des IPsec-Protokolls über das Tunneling des Layer 2 Tunneling Protocol (L2TP). L2TP ist das Produkt einer Partnerschaft zwischen den Mitgliedern des PPTP-Forums, Cisco und der Internet Engineering Task Force (IETF). Hauptsächlich für Remotezugriff-VPNs mit Windows 2000-Betriebssystemen, da Windows 2000 einen nativen IPsec- und L2TP-Client bereitstellt. Internetdienstanbieter können auch L2TP-Verbindungen für Einwahlbenutzer bereitstellen und diesen Datenverkehr anschließend mit IPsec zwischen ihrem Access Point und dem Netzwerkserver der Außenstelle verschlüsseln.

- **Datenintegrität** - Auch wenn es wichtig ist, dass Ihre Daten über ein öffentliches Netzwerk verschlüsselt werden, ist es ebenso wichtig, zu überprüfen, ob sie während der Übertragung nicht geändert wurden. Beispielsweise verfügt IPsec über einen Mechanismus, um sicherzustellen, dass der verschlüsselte Teil des Pakets oder der gesamte Header und Datenanteil des Pakets nicht manipuliert wurde. Wenn Manipulationen erkannt werden, wird das Paket verworfen. Datenintegrität kann auch die Authentifizierung des Remote-Peers beinhalten.
- **Authentifizierung von Datenquellen** - Es ist äußerst wichtig, die Identität der Quelle der gesendeten Daten zu überprüfen. Dies ist erforderlich, um eine Reihe von Angriffen zu verhindern, die vom Spoofing der Identität des Absenders abhängen.
- **Anti Replay** (**Anti-Wiedergabe**) - Hierbei handelt es sich um die Fähigkeit, wiedergegebene Pakete zu erkennen und abzulehnen und Spoofing zu verhindern.
- **Data Tunneling/Vertraulichkeit des Datenverkehrsflusses** - Beim Tunneling wird ein gesamtes Paket in ein anderes Paket eingekapselt und über ein Netzwerk gesendet. Das Daten-Tunneling ist hilfreich, wenn die Identität des Geräts, von dem der Datenverkehr stammt, verborgen werden soll. Beispielsweise kapselt ein einzelnes Gerät, das IPsec verwendet, Datenverkehr, der zu einer Reihe von Hosts dahinter gehört, und fügt einen eigenen Header zu den vorhandenen Paketen hinzu. Durch die Verschlüsselung des ursprünglichen Pakets und Headers (und das Routing des Pakets basierend auf dem zusätzlichen Layer-3-Header, der oben hinzugefügt wird) verbirgt das Tunneling-Gerät effektiv die tatsächliche Quelle des Pakets. Nur der vertrauenswürdige Peer kann die tatsächliche Quelle bestimmen, nachdem er den zusätzlichen Header entfernt und den ursprünglichen Header entschlüsselt hat. Wie in RFC 2401 erwähnt, "..Die Offenlegung der externen Merkmale der Kommunikation kann unter

bestimmten Umständen ebenfalls Besorgnis erregend sein. Die Vertraulichkeit des Datenverkehrs ist der Service, der diese Bedenken ausräumt, indem Quell- und Zieladressen, die Länge der Nachrichten oder die Häufigkeit der Kommunikation verdeckt werden. Im IPsec-Kontext kann die Verwendung von ESP im Tunnelmodus, insbesondere an einem Sicherheits-Gateway, eine gewisse Vertraulichkeit des Datenverkehrs gewährleisten."Alle hier aufgelisteten Verschlüsselungsprotokolle verwenden außerdem Tunneling, um die verschlüsselten Daten über das öffentliche Netzwerk zu übertragen. Es ist wichtig zu erkennen, dass das Tunneling an sich keine Datensicherheit bietet. Das ursprüngliche Paket wird lediglich in ein anderes Protokoll gekapselt und kann bei fehlender Verschlüsselung auch mit einem Paketerfassungsgerät sichtbar sein. Es wird hier jedoch erwähnt, da es ein integraler Bestandteil der VPN-Funktion ist.Tunneling erfordert drei verschiedene Protokolle.**Passenger-Protokoll** - Die ursprünglichen Daten (IPX, NetBeui, IP), die übertragen werden.**Kapselungsprotokoll** - Das Protokoll (GRE, IPsec, L2F, PPTP, L2TP), das um die ursprünglichen Daten umschlossen wird.**Carrier Protocol** (**Carrierprotokoll**): Das Protokoll, das vom Netzwerk verwendet wird, über das die Informationen übertragen werden.Das ursprüngliche Paket (Passenger-Protokoll) wird in das Kapselungsprotokoll eingekapselt, das dann in den Header des Carrier-Protokolls (in der Regel IP) zur Übertragung über das öffentliche Netzwerk eingefügt wird. Beachten Sie, dass das Kapselungsprotokoll auch oft die Verschlüsselung der Daten durchführt. Protokolle wie IPX und NetBeui, die normalerweise nicht über das Internet übertragen werden, können sicher und sicher übertragen werden.Bei Site-to-Site-VPNs ist das Kapselungsprotokoll normalerweise IPsec oder Generic Routing Encapsulation (GRE). GRE enthält Informationen darüber, welche Paketart Sie kapseln, und Informationen über die Verbindung zwischen Client und Server.Bei VPNs mit Remote-Zugriff erfolgt das Tunneling normalerweise über das Point-to-Point Protocol (PPP). PPP ist Teil des TCP/IP-Stacks und fungiert als Carrier für andere IP-Protokolle bei der Kommunikation über das Netzwerk zwischen dem Host-Computer und einem Remote-System. PPP-Tunneling verwendet eines von PPTP, L2TP oder L2F (Layer 2 Forwarding) von Cisco.

- **AAA**: Authentifizierung, Autorisierung und Abrechnung werden für einen sichereren Zugriff in einer VPN-Umgebung mit Remote-Zugriff verwendet. Ohne Benutzerauthentifizierung kann jeder, der auf einem Laptop/PC mit vorkonfigurierter VPN-Client-Software sitzt, eine sichere Verbindung zum Remote-Netzwerk herstellen. Bei der Benutzerauthentifizierung müssen jedoch auch ein gültiger Benutzername und ein gültiges Kennwort eingegeben werden, bevor die Verbindung hergestellt wird. Benutzernamen und Kennwörter können auf dem VPN-Terminierungsgerät selbst oder auf einem externen AAA-Server gespeichert werden, der eine Authentifizierung für zahlreiche andere Datenbanken wie Windows NT, Novell, LDAP usw. ermöglicht.Wenn eine Anfrage zur Einrichtung eines Tunnels von einem DFÜ-Client eingeht, fordert das VPN-Gerät einen Benutzernamen und ein Kennwort an. Diese kann dann lokal authentifiziert oder an den externen AAA-Server gesendet werden, der Folgendes überprüft:Wer Sie sind (Authentifizierung)Ihre Berechtigung (Autorisierung)Was Sie tatsächlich tun (Buchhaltung)Die Rechnungslegungsinformationen sind besonders nützlich für die Verfolgung der Client-Verwendung zu Zwecken der Sicherheitsprüfung, der Rechnungsstellung oder der Berichterstattung.
- **Nichtabstreitbarkeit**: Bei bestimmten Datenübertragungen, insbesondere im Zusammenhang mit Finanztransaktionen, ist Nichtabstreitbarkeit eine höchst wünschenswerte Funktion. Dies ist hilfreich, um Situationen zu verhindern, in denen ein Ende die Teilnahme an einer Transaktion verweigert. Ähnlich wie bei einer Bank müssen Sie Ihre Unterschrift vor der Einhaltung des Schecks unterschreiben. Die Nichtabstreitbarkeit funktioniert, indem der gesendeten Nachricht eine digitale Unterschrift hinzugefügt wird, wodurch die Möglichkeit

ausgeschlossen wird, dass der Absender die Teilnahme an der Transaktion verweigert.

Es gibt eine Reihe von Protokollen, die zum Erstellen einer VPN-Lösung verwendet werden können. Alle diese Protokolle stellen eine Teilmenge der in diesem Dokument aufgeführten Dienste bereit. Die Wahl eines Protokolls hängt von der gewünschten Servicesammlung ab. So kann es beispielsweise vorkommen, dass ein Unternehmen mit der Übertragung von Daten in unverschlüsselten Texten vertraut ist, sich jedoch um die Wahrung der Integrität der Daten sorgt, während andere Unternehmen die Wahrung der Vertraulichkeit von Daten für absolut unerlässlich halten. Ihre Wahl der Protokolle könnte daher anders ausfallen. Weitere Informationen zu den verfügbaren Protokollen und ihren jeweiligen Stärken finden Sie unter Welche VPN-Lösung ist für Sie geeignet?

VPN-Produkte

Je nach VPN-Typ (Remote-Zugriff oder Site-to-Site) müssen Sie bestimmte Komponenten zum Aufbau Ihres VPNs implementieren. Dazu gehören:

- Desktop-Software-Client für jeden Remote-Benutzer
- Dedizierte Hardware wie ein Cisco VPN Concentrator oder eine Cisco Secure PIX Firewall
- Dedizierter VPN-Server für Einwähldienste
- Network Access Server (NAS), der vom Service Provider für den VPN-Zugriff von Remote-Benutzern verwendet wird
- Privates Netzwerk- und Richtlinienmanagement-Center

Da es keinen allgemein akzeptierten Standard für die Implementierung eines VPN gibt, haben viele Unternehmen schlüsselfertige Lösungen eigenständig entwickelt. Cisco bietet beispielsweise mehrere VPN-Lösungen an, die Folgendes umfassen:

- **VPN Concentrator** - Cisco VPN Concentrator umfasst die modernsten verfügbaren Verschlüsselungs- und Authentifizierungsverfahren. Sie wurden speziell für die Erstellung eines Remote-Zugriffs oder Site-to-Site-VPNs entwickelt und werden im Idealfall bereitgestellt, wenn ein Gerät für die Verarbeitung einer sehr großen Anzahl von VPN-Tunneln erforderlich ist. Der VPN Concentrator wurde speziell für die Anforderungen eines speziell entwickelten VPN-Geräts mit Remote-Zugriff entwickelt. Die Konzentratoren bieten hohe Verfügbarkeit, hohe Leistung und Skalierbarkeit und umfassen Komponenten, die als Scalable Encryption Processing (SEP)-Module bezeichnet werden, mit denen Benutzer problemlos Kapazität und Durchsatz steigern können. Die Konzentratoren werden in Modellen angeboten, die für kleine Unternehmen mit 100 oder weniger Remote-Benutzern für große Unternehmen mit bis zu 10.000 gleichzeitigen Remote-Benutzern geeignet sind.

- **VPN-fähiger Router/VPN-optimierter Router**: Alle Cisco Router, auf denen die Cisco IOS®-Software ausgeführt wird, unterstützen IPsec-VPNs. Die einzige Anforderung besteht darin, dass der Router ein Cisco IOS-Image mit dem entsprechenden Feature-Set ausführen muss.

Die Cisco IOS VPN-Lösung unterstützt die VPN-Anforderungen für Remote-Zugriff, Intranet und Extranet vollständig. Dies bedeutet, dass Cisco Router genauso gut funktionieren können, wenn sie mit einem Remote-Host verbunden sind, auf dem VPN-Client-Software ausgeführt wird, oder wenn sie mit einem anderen VPN-Gerät wie einem Router, einer PIX-Firewall oder einem VPN-Konzentrator verbunden sind. VPN-fähige Router eignen sich für VPNs mit moderaten Verschlüsselungs- und Tunneling-Anforderungen und bieten VPN-Services ausschließlich über Cisco IOS-Softwarefunktionen. Beispiele für VPN-fähige Router sind Cisco 1000, Cisco 1600, Cisco 2500, Cisco 4000, Cisco 4500 und Cisco 4700.Die VPN-optimierten Router von Cisco bieten Skalierbarkeit, Routing, Sicherheit und Quality of Service (QoS). Die Router basieren auf der Cisco IOS-Software, und es gibt ein Gerät, das für jede Situation geeignet ist, vom Zugriff in kleinen Büros/Heimbüros (SOHO) über die VPN-Aggregation am zentralen Standort bis hin zu umfangreichen Unternehmensanforderungen. VPN-optimierte Router sind auf hohe Verschlüsselungs- und Tunneling-Anforderungen ausgelegt und nutzen häufig zusätzliche Hardware wie Verschlüsselungskarten, um eine hohe Leistung zu erzielen. Beispiele für VPN-optimierte Router sind die Cisco Serien 800, 1700,

2600, 3600, 7200 und 7500.

- **Cisco Secure PIX Firewall** - Die Private Internet eXchange (PIX) Firewall kombiniert dynamische Netzwerkadressenumwandlung, Proxy-Server, Paketfiltration, Firewall- und VPN-Funktionen in einer einzigen Hardware. Anstatt die Cisco IOS-Software zu verwenden, verfügt dieses Gerät über ein hochgradig optimiertes Betriebssystem, das verschiedene Protokolle mit Schwerpunkt auf IP für extreme Robustheit und Leistung handhaben kann. Wie bei Cisco Routern unterstützen alle PIX-Firewall-Modelle IPsec-VPN. Es ist lediglich erforderlich, dass die Lizenzierungsanforderungen für die VPN-Funktion erfüllt

werden.

- **Cisco VPN Clients**: Cisco bietet sowohl Hardware- als auch Software-VPN-Clients. Der Cisco VPN Client (Software) ist ohne zusätzliche Kosten im Paket mit dem Cisco VPN Concentrator der Serie 3000 enthalten. Dieser Software-Client kann auf dem Host-Rechner installiert und verwendet werden, um eine sichere Verbindung mit dem zentralen Standort-Konzentrator (oder einem anderen VPN-Gerät wie einem Router oder einer Firewall) herzustellen. Der VPN 3002 Hardware Client ist eine Alternative zur Bereitstellung der VPN Client-Software auf allen Systemen und bietet VPN-Verbindungen zu einer Reihe von Geräten.

Die Auswahl der Geräte, die Sie für die VPN-Lösung verwenden würden, hängt letztendlich von einer Reihe von Faktoren ab, darunter dem gewünschten Durchsatz und der Anzahl der Benutzer.

Beispielsweise könnten Sie an einem Remote-Standort mit einer Handvoll von Benutzern hinter einem PIX 501 erwägen, das vorhandene PIX als IPsec-VPN-Endpunkt zu konfigurieren, vorausgesetzt, Sie akzeptieren den 3DES-Durchsatz des 501 von ungefähr 3 Mbit/s und die Obergrenze von maximal 5 VPN-Peers. Auf der anderen Seite wäre es wahrscheinlich eine gute Idee, einen zentralen Standort als VPN-Endpunkt für eine große Anzahl von VPN-Tunneln zu verwenden, der für einen VPN-optimierten Router oder einen VPN-Konzentrator verwendet wird. Die Auswahl hängt nun vom Typ (LAN-zu-LAN oder Remote-Zugriff) und der Anzahl der einzurichtenden VPN-Tunnel ab. Die breite Palette an Cisco Geräten, die VPN unterstützen, bietet Netzwerkdesignern ein hohes Maß an Flexibilität und eine robuste Lösung für alle Designanforderungen.

Zugehörige Informationen

- VPDN im Überblick
- Virtual Private Networks (VPNs)
- Support-Seite für Cisco VPN Concentrators der Serie 3000
- Cisco VPN 3000 Client Support-Seite
- Support-Seite für IPsec-Aushandlung/IKE-Protokoll
- Support-Seite für Firewalls der Serie PIX 500
- RFC 1661: Das Point-to-Point Protocol (PPP)
- RFC 2661: Layer-2-Tunneling-Protokoll "L2TP"
- So funktioniert Stuff: So funktionieren virtuelle private Netzwerke
- VPNs im Überblick
- VPN-Seite von Tom Dunigan
- Virtual Private Network Consortium
- Anforderungen für Kommentare (RFCs)
- Technischer Support – Cisco Systems