Hoe Virtual Private Networks werken

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Conventies](#)
[Achtergrondinformatie](#)
[Wat maakt een VPN?](#)
[Analogie: Elk LAN is een ISLANd](#)
[VPN-technologieën](#)
[VPN-producten](#)
[Gerelateerde informatie](#)

Inleiding

Dit document behandelt de fundamentele waarden van VPN's, zoals basiscomponenten van VPN, technologieën, tunneling en VPN-beveiliging.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

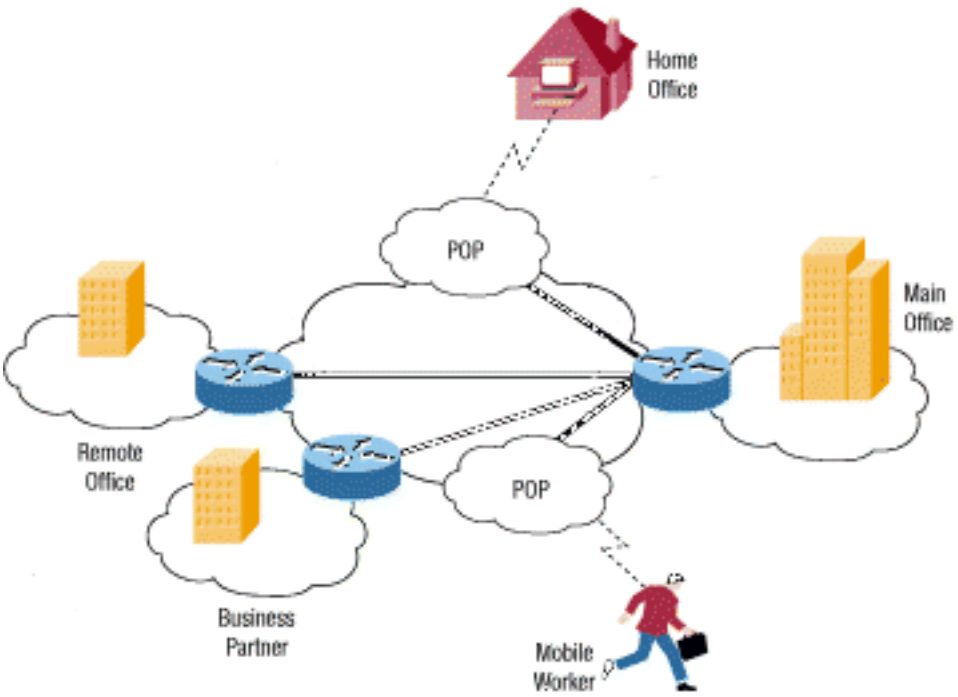
Achtergrondinformatie

De wereld is de afgelopen paar decennia veel veranderd. In plaats van louter te reageren op lokale of regionale zorgen, moeten veel bedrijven nu nadenken over mondiale markten en logistiek. Veel bedrijven hebben faciliteiten die zich over het hele land, of zelfs over de hele wereld, verspreiden. Maar er is één ding dat alle bedrijven nodig hebben: een manier om snelle,

veilige en betrouwbare communicatie te onderhouden waar hun kantoren ook zijn.

Tot voor kort betekende betrouwbare communicatie het gebruik van huurlijnen om een breed netwerk (WAN) te onderhouden. Geleasede lijnen, variërend van ISDN (Integrated Services Digital Network), dat 144 Kbps bedraagt, tot Optical Carrier-3 (OC3, dat 155 Mbps draait) vezel, bieden een bedrijf een manier om hun privénetwerk uit te breiden buiten hun onmiddellijke geografische gebied. Een WAN heeft duidelijke voordelen ten opzichte van een openbaar netwerk als het internet als het op betrouwbaarheid, prestaties en veiligheid aankomt; maar het behouden van een WAN, vooral bij gebruik van huurlijnen, kan vrij duur worden (het verhoogt vaak de kosten naarmate de afstand tussen de kantoren toeneemt). Daarnaast zijn huurlijnen geen levensvatbare oplossing voor organisaties waar een deel van de beroepsbevolking zeer mobiel is (zoals het geval is met het marketingpersoneel) en vaak op afstand en toegang tot gevoelige gegevens nodig kan zijn.

Nu de populariteit van het internet is toegenomen, hebben bedrijven zich erop gericht hun eigen netwerken uit te breiden. Eerst werden intranets binnengebracht, die sites zijn die uitsluitend ontworpen zijn voor gebruik door werknemers van het bedrijf. Nu, veel bedrijven creëren hun eigen Virtual Private Networks (VPN's) om de behoeften van externe werknemers en kantoren in de verte te lenigen.



Een standaard VPN kan een hoofdnetwerk (LAN) hebben op het hoofdkantoor van een bedrijf, andere LAN's op afgelegen kantoren of faciliteiten en individuele gebruikers die vanuit het veld verbonden zijn.

Een VPN is een privaat netwerk dat een openbaar netwerk (meestal het internet) gebruikt om externe sites of gebruikers onderling aan te sluiten. In plaats van gebruik te maken van een speciale echte verbinding, zoals een huurlijn, gebruikt een VPN "virtuele" verbindingen die via het internet zijn verstuurd van het privénetwerk van het bedrijf naar de externe site of medewerker.

Wat maakt een VPN?

Er zijn twee gebruikelijke VPN's.

- **Remote-Access--ook** een Virtual Private Dial-up Network (VPDN) genoemd, dit is een user-to-LAN verbinding die wordt gebruikt door een bedrijf dat medewerkers heeft die verbinding moeten maken met het particuliere netwerk vanaf diverse externe locaties. Meestal biedt een bedrijf dat een groot VPN voor toegang op afstand wilt instellen, een of andere vorm van inbelaccount voor internet aan zijn gebruikers via een internetprovider (ISP). De telecombedrijven kunnen dan een 1-800 nummer bellen om het internet te bereiken en hun VPN clientsoftware gebruiken om toegang te krijgen tot het bedrijfsnetwerk. Een goed voorbeeld van een bedrijf dat een VPN op afstand heeft nodig, zou een groot bedrijf zijn met honderden verkopers in het veld. VPN's met externe toegang maken beveiligde, versleutelde verbindingen mogelijk tussen het particuliere netwerk van een bedrijf en externe gebruikers via een serviceprovider van een derde.
- **Site-to-Site**-Via het gebruik van speciale apparatuur en encryptie op grote schaal kan een bedrijf meerdere vaste sites aansluiten via een openbaar netwerk, zoals internet. Iedere site heeft alleen een lokale verbinding met hetzelfde openbare netwerk nodig, waardoor geld wordt bespaard op lange particuliere huurlijnen. Site-to-site VPN's kunnen verder worden gecategoriseerd in intranets of extranets. Een site-to-site VPN die tussen vestigingen van hetzelfde bedrijf is gemaakt, wordt aangeduid als een intranet VPN, terwijl een VPN dat is gebouwd om het bedrijf met zijn partner of klant te verbinden, wordt aangeduid als een extranet VPN.

Een goed ontworpen VPN kan een bedrijf enorm voordeel opleveren. Het kan bijvoorbeeld:

- Lijnt geografische connectiviteit uit
- Verminder operationele kosten tegenover traditionele WAN's
- Verminder de doorvoertijden en de reiskosten voor externe gebruikers
- Verbeteren van de productiviteit
- Vereenvoudig netwerktopologie
- Biedt wereldwijde netwerkmogelijkheden
- Ondersteuning voor telecommunicatie bieden
- Zorg voor een sneller rendement op investeringen (ROI) dan traditioneel WAN

Welke functies zijn nodig in een goed ontworpen VPN? Het dient deze punten te omvatten:

- Security
- Betrouwbaarheid
- schaalbaarheid
- Netwerkbeheer
- Beleidsbeheer

Analogie: Elk LAN is een ISLANd

Stel je voor dat je op een eiland in een grote oceaan woont. Er zijn duizenden andere eilanden om je heen, sommige heel dichtbij en andere verder weg. Normaal reizen is een veerboot nemen van je eiland naar elk eiland dat je wilt bezoeken. Reizen op een veerboot betekent dat je bijna geen privacy hebt. Alles wat je doet kan door iemand anders gezien worden.

Stel dat elk eiland een privé LAN vertegenwoordigt en de oceaan het internet is. Wanneer u per veerboot reist, is het vergelijkbaar met wanneer u verbinding maakt met een webserver of met een ander apparaat via het internet. Je hebt geen controle over de draden en routers die het internet vormen, net zoals je geen controle hebt over de andere mensen op de veerboot. Dit laat u vatbaar

voor veiligheidskwesties als u probeert te verbinden tussen twee particuliere netwerken die een openbare bron gebruiken.

Je eiland besluit een brug naar een ander eiland te bouwen zodat er een makkelijker, zekerder en directere manier is om tussen de twee te reizen. Het is duur om de brug te bouwen en onderhouden, ondanks dat het eiland waarmee je verbinding maakt zeer dicht is. Maar de behoefte aan een betrouwbaar, veilig pad is zo groot dat je het toch doet. Je eiland zou graag verbinding maken met een tweede eiland dat veel verder weg is, maar je besluit dat het te duur is.

Deze situatie lijkt erg op een huurlijn. De bruggen (huurlijnen) zijn gescheiden van de oceaan (internet), maar ze kunnen de eilanden (LAN's) verbinden. Veel bedrijven hebben deze route gekozen vanwege de noodzaak van beveiliging en betrouwbaarheid bij het aansluiten van hun verafgelegen kantoren. Maar als de kantoren zeer ver uit elkaar liggen kunnen de kosten buitensporig hoog zijn - net zoals bij het bouwen van een brug die veel afstand overbrugt.

Dus hoe past VPN in deze analogie? We kunnen elke bewoner van onze eilanden hun eigen kleine onderzeeër met deze eigenschappen geven.

- Het is snel.
- Het is makkelijk om met je mee te nemen waar je ook gaat.
- Het kan je volledig verstoppen tegen andere boten of onderzeeërs.
- Het is betrouwbaar.
- Het kost weinig om extra onderzeeërs aan uw vloot toe te voegen zodra de eerste is aangeschaft.

Hoewel ze samen met ander verkeer in de oceaan reizen, konden de bewoners van onze twee eilanden heen en weer reizen wanneer ze wilden met privacy en veiligheid. Dat is in essentie hoe een VPN werkt. Elk extern lid van uw netwerk kan op een veilige en betrouwbare manier communiceren met behulp van het internet als het medium voor de verbinding met het particuliere LAN. Een VPN kan groeien om meer gebruikers en verschillende locaties te bedienen en veel gemakkelijker dan een huurlijn. In feite is schaalbaarheid een groot voordeel dat VPN's hebben over typische huurlijnen. In tegenstelling tot huurlijnen waar de kosten in verhouding staan tot de afstanden in kwestie, zijn de geografische locaties van elk kantoor weinig belangrijk bij het maken van een VPN.

VPN-technologieën

Een goed ontworpen VPN gebruikt verschillende methoden om uw verbinding en gegevens veilig te stellen.

- **Vertrouwelijkheid van gegevens** - Dit is mogelijk de belangrijkste service die door een VPN-implementatie wordt geleverd. Aangezien uw privé-gegevens over een openbaar netwerk reizen, is de vertrouwelijkheid van gegevens essentieel en kan worden bereikt door de gegevens te versleutelen. Dit is het proces om alle gegevens in te voeren die een computer naar een ander stuurt en ze te coderen in een formulier dat alleen de andere computer kan decoderen.De meeste VPN's gebruiken één van deze protocollen om encryptie te verstrekken.**IPsec**-Internet Protocol Security Protocol (IPsec) biedt verbeterde beveiligingsfuncties zoals sterkere encryptie-algoritmen en meer uitgebreide verificatie. IPsec bevat twee coderingsmodi: tunnel en vervoer. De tunnelmodus versleutelt de kop en de lading van elk pakket terwijl de transportmodus alleen de lading versleutelt. Alleen systemen die IPsec-compatibel zijn kunnen gebruik maken van dit protocol. Alle hulpmiddelen moeten

bovendien een gemeenschappelijke sleutel of een gemeenschappelijk certificaat gebruiken en moeten een vergelijkbaar beveiligingsbeleid hebben.Voor VPN-gebruikers die op afstand toegang hebben, biedt een of ander softwarepakket van derden de verbinding en encryptie op de pc van de gebruikers. IPsec ondersteunt 56-bits (single-DES) of 168-bits (triple-DES) encryptie.**PPTP/MPPE**-PPTP werd opgericht door het PPTP Forum, een consortium dat bestaat uit Amerikaanse robotica, Microsoft, 3COM, Ascend en ECI Telematica. PPTP ondersteunt multiprotocol VPN's, met 40-bits en 128-bits codering, met behulp van een protocol dat Microsoft Point-to-Point Encryption (MPPE) wordt genoemd. Het is belangrijk op te merken dat PPTP op zichzelf geen gegevensencryptie verstrekt.**L2TP/IPsec**-veel genoemd L2TP via IPsec, biedt dit de beveiliging van het IPsec-protocol via het tunneling van Layer 2 Tunneling Protocol (L2TP). L2TP is het product van een partnerschap tussen de leden van het PPTP-forum, Cisco, en de Internet Engineering Task Force (IETF). Primair gebruikt voor VPN's met toegang op afstand met Windows 2000-besturingssystemen, aangezien Windows 2000 een native IPsec- en L2TP-client biedt. Internet Service Providers kunnen ook L2TP-verbindingen aanbieden voor inbelgebruikers en dan het verkeer versleutelen met IPsec tussen hun access point en de externe Office-server.

- **Integriteit van gegevens**: terwijl het belangrijk is dat uw gegevens versleuteld zijn via een openbaar netwerk, is het net zo belangrijk om te controleren of ze tijdens het transport niet gewijzigd zijn. IPsec heeft bijvoorbeeld een mechanisme om er zeker van te zijn dat het gecodeerde gedeelte van het pakket, of het gehele header en gegevensgedeelte van het pakket, niet met geknoeid is. Als vervalsing wordt gedetecteerd, wordt het pakket verbroken. De gegevensintegriteit kan ook worden geauthentificeerd door de peer op afstand.
- **Verificatie van oorsprong van gegevens** - het is van belang om de identiteit van de bron van de gegevens te verifiëren die wordt verzonden. Dit is nodig om te beschermen tegen een aantal aanvallen die afhangen van het mijden van de identiteit van de zender.
- **Anti-Replay**-dit is de mogelijkheid om teruggespeeld pakketten te detecteren en af te wijzen en helpt spoofing te voorkomen.
- **Data Tunneling/Traffic Flow Confidentiality**-Tunneling is het proces van het insluiten van een volledig pakket binnen een ander pakket en het verzenden ervan via een netwerk. Het afstemmen van gegevens is nuttig in gevallen waarin het wenselijk is de identiteit van het apparaat dat van het verkeer afkomstig is te verbergen. Bijvoorbeeld, één apparaat dat IPsec gebruikt kapselt verkeer in dat aan een aantal hosts achter het toestel hoort en voegt zijn eigen header bovenop de bestaande pakketten toe. Door het oorspronkelijke pakket en de header te versleutelen (en het pakket te routeren op basis van de extra laag 3 die bovenop wordt toegevoegd), verbergt het tunnelapparaat effectief de werkelijke bron van het pakket. Alleen de vertrouwde peer kan de ware bron bepalen, nadat hij de extra header wegvalt en de oorspronkelijke header decrypteert. Zoals opgemerkt in RFC 2401 , "...ook de bekendmaking van de externe kenmerken van de communicatie kan in bepaalde omstandigheden aanleiding geven tot bezorgdheid . Verkeersstroomvertrouwelijkheid is de dienst die dit laatste probleem aanpakt door bron- en doeladressen, berichtlengte of -frequentie te verbergen. In de IPsec-context kan het gebruik van ESP in tunnelmodus, met name bij een beveiligingsgateway, enige mate van vertrouwelijkheid van verkeersstromen opleveren."Alle hier vermelde encryptieprotocollen gebruiken ook een tunneling als middel om de gecodeerde gegevens over het openbare netwerk over te brengen. Het is belangrijk om te realiseren dat tunneling op zichzelf geen gegevensbeveiliging biedt. Het oorspronkelijke pakket is slechts ingekapseld in een ander protocol en is, indien niet versleuteld, mogelijk nog zichtbaar met een pakketvastlegging. Het wordt hier echter genoemd, omdat het een integraal onderdeel is van de manier waarop VPN's functioneren.Tunneling vereist drie verschillende

protocollen.**Passagiersprotocol**: de oorspronkelijke gegevens (IPX, NetBeui, IP) die worden vervoerd.**Inkapselend protocol**-het protocol (GRE, IPsec, L2F, PPTP, L2TP) dat rond de oorspronkelijke gegevens is gewikkeld.**Carrier Protocol**-Het protocol dat door het netwerk wordt gebruikt waarover de informatie reist.Het oorspronkelijke pakket (Passenger Protocol) is opgenomen in het omkapselende protocol en wordt vervolgens in de header van het protocol geplaatst voor transmissie via het openbare netwerk. Merk op dat het inkapselende protocol ook vrij vaak de encryptie van de gegevens uitvoert. Protocollen zoals IPX en NetBeui, die normaliter niet via het internet worden overgedragen, kunnen veilig en veilig worden verzonden.Voor site-to-site VPN's is het inkapselende protocol meestal IPsec of Generic Routing Encapsulation (GRE). GRE bevat informatie over welk type pakket u inkapselt en informatie over de verbinding tussen de client en de server.Voor VPN's met toegang op afstand wordt een tunneling normaal gesproken uitgevoerd via Point-to-Point Protocol (PPP). Een deel van de TCP/IP stapel, PPP is de drager voor andere IP protocollen bij het communiceren over het netwerk tussen de host computer en een extern systeem. PPP-tunneling gebruikt een van PPTP-, L2TP- of Cisco Layer 2-doorsturen (L2F).

- **AAA**-verificatie, autorisatie en accounting wordt gebruikt voor beveiligde toegang in een externe VPN-omgeving. Zonder gebruikersverificatie kan iedereen die op een laptop/PC zit met vooraf ingestelde VPN-clientsoftware een beveiligde verbinding naar het externe netwerk opzetten. Met gebruikersverificatie echter moet ook een geldige gebruikersnaam en wachtwoord worden ingevoerd voordat de verbinding wordt voltooid. Gebruikersnaam en wachtwoorden kunnen worden opgeslagen op het VPN-afgifteapparaat zelf of op een externe AAA-server, die verificatie kan leveren aan talloze andere databases zoals Windows NT, Novell, LDAP enzovoort.Wanneer een verzoek om een tunnel in te stellen van een wijzerplaat-op client komt, het apparaat van VPN voor een gebruikersnaam en een wachtwoord. Dit kan dan lokaal worden geauthentiseerd of naar de externe AAA server worden verzonden, die controleert:Wie u bent (Verificatie)Wat u mag doen (autorisatie)Wat u feitelijk doet (accounting)De boekhoudkundige informatie is met name nuttig voor het volgen van het gebruik van cliënten voor veiligheidscontrole, facturering of rapportage.
- **Niet** - In bepaalde gegevensoverdrachten, met name die welke verband houden met financiële transacties, is niet - reputatie een zeer wenselijk kenmerk. Dit is nuttig om situaties te voorkomen waarin een eindgebruiker ontkent dat hij aan een transactie heeft deelgenomen. Net zoals een bank je handtekening nodig heeft voordat je cheque wordt nagekomen, werkt deze niet-weigerachtigheid door een digitale handtekening aan het verstuurde bericht toe te voegen, waardoor de mogelijkheid wordt uitgesloten om deelname aan de transactie te weigeren.

Er bestaat een aantal protocollen die kunnen worden gebruikt om een VPN-oplossing te maken. Al deze protocollen bieden een subset van de services die in dit document worden opgesomd. De keuze van een protocol is afhankelijk van de gewenste serviceset. Een organisatie zou bijvoorbeeld wel eens comfortabel kunnen zijn met de overdracht van de gegevens in duidelijke tekst, maar zeer bezorgd over het behoud van haar integriteit, terwijl een andere organisatie het bewaren van de vertrouwelijkheid van gegevens absoluut noodzakelijk zou kunnen vinden. Hun keuze aan protocollen kan dus anders zijn. Raadpleeg voor meer informatie over de beschikbare protocollen en hun relatieve sterke punten op Welke VPN-oplossing is geschikt voor U?

VPN-producten

Gebaseerd op het type van VPN (ver-toegang of site-to-site) moet u bepaalde componenten installeren om uw VPN te bouwen. Deze zouden kunnen omvatten:

- Desktopsoftwareclient voor elke externe gebruiker
- Speciale hardware zoals een Cisco VPN-Concentrator of een Cisco Secure PIX-firewall
- Speciale VPN-server voor inbelservices
- Network Access Server (NAS) gebruikt door serviceprovider voor VPN-toegang voor externe gebruikers
- Particuliere netwerken en beleidsbeheercentra

Omdat er geen breed geaccepteerde standaard is voor het implementeren van een VPN hebben veel bedrijven op zichzelf kant-en-klare oplossingen ontwikkeld. Bijvoorbeeld, biedt Cisco verschillende oplossingen van VPN die omvatten:

- VPN Concentrator - Met de meest geavanceerde encryptie en authenticatietechnieken beschikbaar, worden Cisco VPN Concentrators speciaal gebouwd voor het maken van een externe toegang of site-to-site VPN en worden idealiter ingezet op plaatsen waar de vereisten voor één apparaat zijn om een zeer groot aantal VPN-tunnels aan te kunnen. De VPN Concentrator werd specifiek ontwikkeld om aan de eis te voldoen voor een speciaal gebouwd, extern toegang VPN-apparaat. De concentrators bieden hoge beschikbaarheid, hoge prestaties en schaalbaarheid en omvatten componenten, genaamd Scalable Encryption Processing (SEP)-modules, die gebruikers in staat stellen de capaciteit en de doorvoersnelheid gemakkelijk te verhogen. De concentrators worden aangeboden in modellen die geschikt zijn voor kleine bedrijven met 100 of minder gebruikers die toegang op afstand hebben tot grote bedrijven met maximaal 10.000 gebruikers op afstand. 
- VPN-enabled router/VPN-geoptimaliseerde router-Alle Cisco routers die Cisco IOS® software gebruiken ondersteunen IPsec VPN's. Het enige vereiste is dat de router een Cisco IOS beeld met de juiste functieset moet lopen. De Cisco IOS VPN-oplossing ondersteunt volledig de vereisten voor toegang op afstand, intranet en extranet. Dit betekent dat Cisco-routers even goed kunnen werken wanneer ze worden aangesloten op een externe host die VPN-clientsoftware draait, of wanneer ze worden aangesloten op een ander VPN-apparaat, zoals een router, PIX-firewall of VPN-centrator. VPN-enabled routers zijn geschikt voor VPN's met matige encryptie- en tunnelvereisten en bieden VPN-services volledig aan via Cisco IOS-softwarefuncties. Voorbeelden van VPN-enabled routers zijn de Cisco 1000, Cisco 1600, Cisco 2500, Cisco 4000, Cisco 4500 en Cisco 4700 Series.De VPN-geoptimaliseerde routers van Cisco bieden schaalbaarheid, routing, beveiliging en Quality of Service (QoS). De routers zijn gebaseerd op de Cisco IOS-software en er is een apparaat dat geschikt is voor elke situatie, van de toegang tot klein kantoor/thuiskantoor (SOHO) via centrale VPN-aggregatie naar grootschalige ondernemingsbehoeften. VPN-geoptimaliseerde routers worden ontworpen om te voldoen aan hoge eisen voor encryptie en tunneling en maken vaak gebruik van extra hardware zoals encryptiekaarten om hoge prestaties te bereiken. Voorbeelden van VPN-geoptimaliseerde routers zijn Cisco 800, Cisco 1700, Cisco 2600, Cisco 3600, Cisco

7200 en Cisco 7500 Series.

- **Cisco Secure PIX-firewall** - De Private Internet eXchange (PIX)-firewall combineert dynamische netwerkadresomzetting, proxy-server, pakketfiltratie, firewall en VPN-functies in één stuk hardware. In plaats van Cisco IOS-software te gebruiken heeft dit apparaat een zeer gestroomlijnd besturingssysteem dat de mogelijkheid verhandelt om een verscheidenheid aan protocollen voor extreme robuustheid en prestaties aan te pakken door zich op IP te richten. Net als Cisco-routers ondersteunen alle PIX-firewallmodellen IPsec VPN. Alles wat vereist is, is dat aan de licentievereisten voor de VPN-functie moet worden

voldaan.

- **Cisco VPN Clients** - Cisco biedt zowel hardware- als software-VPN-clients aan. De Cisco VPN-client (software) wordt zonder extra kosten gebundeld met Cisco VPN 3000 Series Concentrator. Deze softwareclient kan op de host-machine worden geïnstalleerd en op een beveiligde manier worden gebruikt voor de verbinding met de centrale site-concentrator (of met een ander VPN-apparaat, zoals een router of firewall). De VPN 3002 Hardware Client is een alternatief voor het inzetten van de VPN-clientsoftware op elke machine en biedt VPN-connectiviteit op een aantal apparaten.

De keuze van apparaten die u zou gebruiken om uw VPN-oplossing te bouwen is uiteindelijk een ontwerpprobleem dat afhangt van een aantal factoren, waaronder de gewenste doorvoersnelheid en het aantal gebruikers. Op een externe site met een handvol gebruikers achter een PIX 501 kunt u bijvoorbeeld overwegen om de bestaande PIX te configureren als het IPsec VPN-eindpunt, op voorwaarde dat u de 3DES-doorvoersnelheid van 501 van ruwweg 3 Mbps en de limiet van maximaal 5 VPN-peers accepteert. Aan de andere kant zou het, op een centrale plaats die als eindpunt van VPN voor een groot aantal tunnels van VPN handelt, binnen voor een VPN-geoptimaliseerde router of een VPN concentrator waarschijnlijk een goed idee zijn. De keuze van de OCR-opties hangt nu af van het type (LAN-to-LAN of externe toegang) en het aantal VPN-tunnels dat wordt ingesteld. Het brede scala van Cisco apparaten die VPN ondersteunen biedt de netwerkontwerpers een hoge mate van flexibiliteit en een robuuste oplossing om aan elke ontwerpbehoefte te voldoen.

Gerelateerde informatie

- Inzicht VPDN
- Virtual Private Networks (VPN's)

- Ondersteuning van Cisco VPN 3000 Series Concentrators
- Cisco VPN 3000 clientondersteuningspagina
- Ondersteuning van IPsec-onderhandeling/IKE-protocol
- Ondersteuning van PIX 500 Series firewalls
- RFC 1661: Het Point-to-Point Protocol (PPP)
- RFC 2661: Layer 2 Tunneling Protocol "L2TP"
- Hoe Stuff werkt: Hoe Virtual Private Networks werken
- Overzicht van VPN's
- De VPN-pagina van Tom Dunigan
- Consortium voor Virtual Private Network
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning - Cisco-systemen