Cisco RV100 routers voor VPN - Overzicht en beste praktijken

Doel

Het doel van dit document is een overzicht van de best practices van Virtual Private Network (VPN) te geven aan iedereen die nieuw is in Cisco RV-routers.

Inhoud

Inleiding

Het lijkt zo lang geleden dat de enige plek waar je kon werken was op kantoor. Misschien herinner je je nog dat je 's nachts naar kantoor moet gaan om een werkkwestie af te handelen. Er was geen andere manier om gegevens te verkrijgen van bedrijfsmiddelen tenzij u fysiek in uw kantoor was. Die dagen zijn voorbij. Vandaag de dag kunt u onderweg zijn; zaken doen vanuit huis, een ander kantoor, een koffietentje of zelfs een ander land. Het nadeel is dat hackers altijd op zoek zijn om uw gevoelige gegevens te grijpen. Alleen het gebruik van het openbare internet is niet veilig. Wat kunt u doen om flexibiliteit en beveiliging te krijgen? Stel een VPN in!

Een VPN-verbinding stelt gebruikers in staat om toegang te krijgen tot, gegevens te verzenden en te ontvangen van en naar een privaat netwerk door middel van een openbaar of gedeeld netwerk zoals het internet, maar nog steeds om een veilige verbinding met een onderliggende netwerkinfrastructuur te garanderen om het privaat netwerk en zijn bronnen te beschermen.

Een VPN-tunnel maakt een privaat netwerk dat gegevens veilig kan verzenden met codering om de gegevens te coderen, en authenticatie om de identiteit van de client te garanderen. Bedrijfskantoren maken vaak gebruik van een VPN-verbinding omdat het zowel nuttig als noodzakelijk is om hun werknemers toegang te geven tot hun privénetwerk, zelfs als ze buiten het kantoor zijn.

Normaal verbinden site-to-site VPNâ€™s hele netwerken met elkaar. Ze breiden een netwerk uit en maken het mogelijk dat computerbronnen van de ene locatie beschikbaar zijn op andere locaties. Door het gebruik

van een VPN-geschikte router kan een bedrijf meerdere vaste sites verbinden via een openbaar netwerk zoals het internet.

De client-to-site configuratie voor een VPN stelt een externe host, of client, in staat te handelen alsof ze zich op hetzelfde lokale netwerk bevinden. Er kan een VPN-verbinding tussen de router en een eindpunt worden ingesteld nadat de router is geconfigureerd voor internetverbinding. De VPN-client is afhankelijk van de instellingen van de VPN-router, naast de vereiste aangepaste instellingen om een verbinding tot stand te brengen. Ook zijn sommige VPN-clienttoepassingen platformspecifiek, ze zijn ook afhankelijk van de versie van het besturingssysteem. De instellingen moeten precies hetzelfde zijn of ze kunnen niet communiceren.

Een VPN kan met een van de volgende opties worden ingesteld:

- Secure Socket Layer (SSL)
- Internet Protocol Security (IPSec)
- Point-to-Point Tunneling Protocol (PPTP) - niet zo veilig als SSL of IPSec
- Generic Routing Encapsulation (GRE)
- Layer 2 Tunneling Protocol (L2TP)

Als u nog nooit een VPN hebt ingesteld, ontvangt u veel nieuwe informatie in dit artikel. Dit is geen stap-voor-stap gids, maar meer een overzicht voor referentie. Het zou daarom goed zijn om dit artikel in zijn geheel te lezen voordat je verder gaat en probeert om een VPN op je netwerk te installeren. In dit artikel vindt u links voor specifieke stappen.

Producten van derden, niet-Cisco-producten, zoals The GreenBow, OpenVPN, Shrew Soft en EZ VPN, worden niet ondersteund door Cisco. Deze zijn uitsluitend bedoeld als leidraad. Als u ondersteuning nodig hebt op deze buiten het artikel, moet u contact opnemen met de derde partij voor ondersteuning.

Voordelen van het gebruik van een VPN-verbinding

- Het gebruik van een VPN-verbinding helpt vertrouwelijke netwerkgegevens en bronnen te beschermen.
- Het verstrekt gemak en toegankelijkheid voor verre arbeiders of collectieve werknemers aangezien zij tot de belangrijkste bureaumiddelen zullen kunnen gemakkelijk toegang hebben zonder het moeten fysiek aanwezig zijn en toch, de veiligheid van het privé netwerk en zijn middelen handhaven.
- Communicatie met een VPN-verbinding biedt een hoger beveiligingsniveau dan andere methoden voor communicatie op afstand. Een geavanceerd encryptie-algoritme maakt dit mogelijk, het beschermen van het privé netwerk tegen onbevoegde toegang.
- De daadwerkelijke geografische plaatsen van de gebruikers worden beschermd en niet blootgesteld aan het openbare of gedeelde netwerk zoals Internet.
- Met een VPN kunnen nieuwe gebruikers of een groep gebruikers worden toegevoegd zonder dat extra componenten of een gecompliceerde configuratie nodig zijn.

Risico's van het gebruik van een VPN-verbinding

- Er kunnen veiligheidsrisico's zijn toe te schrijven aan misconfiguratie. Aangezien het ontwerp en de implementatie van een VPN gecompliceerd kunnen zijn, is het noodzakelijk om de taak van het configureren van de verbinding toe te vertrouwen aan een deskundige en ervaren professional om ervoor te zorgen dat de beveiliging van het particuliere netwerk niet in gevaar wordt gebracht.
- Het kan minder betrouwbaar zijn. Aangezien een VPN-verbinding een internetverbinding vereist, is

het belangrijk dat er een provider is met een bewezen en geteste reputatie die uitstekende internetservice biedt en minimale tot geen downtime garandeert.
- Als er een situatie ontstaat waarin er behoefte is aan een nieuwe infrastructuur of een nieuwe set configuraties, kunnen er technische problemen ontstaan door incompatibiliteit, met name als er andere producten of leveranciers bij betrokken zijn dan die u al gebruikt.
- Er kunnen langzame verbindingssnelheden optreden. Als u een ISP-verbinding gebruikt die gratis VPN-service biedt, kan worden verwacht dat de verbinding ook traag is omdat deze providers geen prioriteit geven aan verbindingssnelheden. Het is belangrijk om op te merken dat de doorvoersnelheid van VPN afhangt van de hardwaremogelijkheden van de router.

Klik hier voor meer informatie over hoe VPN's werken.

Tips voor gebruik bij het configureren van een VPN

1. Gebruik aan beide uiteinden een ander LAN IP-subnet terwijl u VPN tussen verschillende sites configureert. Wanneer de locatie die u wilt verbinden bijvoorbeeld het adresseringsschema 192.168.x.x gebruikt, dan kunt u een subnet 10.x.x.x of 172.16.x.x - 172.31.x.x gebruiken. Een andere optie zou zijn verschillende subnetmaskers te hebben. Wanneer u uw router IP-adres wijzigt, zullen de apparaten in Dynamic Host Configuration Protocol (DHCP) automatisch een IP-adres in dat subnetnummer ophalen.
2. Gebruik het statische openbare IP op de WAN-interface van de router voor stabiele VPN-connectiviteit.
3. Zorg ervoor dat het geselecteerde versleutelings- en verificatieniveau hetzelfde is als de router waarvoor u een VPN-tunnel wilt instellen voor VPN.
4. Zorg ervoor dat de ingevoerde PSK en sleutellevensduur hetzelfde zijn als de externe router. Een PSK kan zijn wat je wilt dat het is, het hoeft alleen maar te matchen op de site en met de klant wanneer ze instellen als een klant op hun computer. Afhankelijk van het apparaat, kunnen er verboden symbolen zijn die u niet kunt gebruiken. Key Lifetime is hoe vaak het systeem de sleutel wijzigt. Een certificaat heeft de voorkeur omdat het als veiliger wordt beschouwd.
5. Voor de meeste VPN's hebben clients geen certificaat nodig om een VPN te gebruiken, het is alleen voor verificatie via de router. OpenVPN vereist bijvoorbeeld zowel client- als sitecertificaten.
6. Zet je SA Lifetime in fase I langer dan je fase II SA Lifetime. Als u uw fase I korter maakt dan fase II, dan zult u regelmatig opnieuw moeten onderhandelen over de tunnel in plaats van over de gegevenstunnel. Een gegevenstunnel heeft meer veiligheid nodig, dus is het beter om de levensduur in fase II te beperken tot fase I.
7. Verander alle wachtwoorden in iets complexers.

Typen VPN

Secure Sockets Layer (SSL)

Cisco RV340x Series-routers ondersteunen een SSL VPN met AnyConnect. De RV160 en RV260 hebben de optie om OpenVPN te gebruiken, wat een andere SSL VPN is. De SSL VPN server staat externe gebruikers toe om een beveiligde VPN-tunnel te maken met behulp van een webbrowser. Deze functie biedt eenvoudige toegang tot een breed scala aan webbronnen en web-enabled applicaties met behulp van native Hypertext Transfer Protocol (HTTP) via SSL Hypertext Transfer Protocol Secure (HTTPS) browser ondersteuning.

SSL VPN staat gebruikers toe om ver tot beperkte netwerken toegang te hebben, die een veilige en voor authentiek verklaarde weg gebruiken door het netwerkverkeer te versleutelen.

Er zijn twee opties voor het instellen van toegang in SSL:

1. Zelfondertekend Certificaat: Een Certificaat dat wordt ondertekend door zijn eigen ontwerper. Dit wordt niet aanbevolen en dient alleen in een testomgeving te worden gebruikt.
2. CA Signed Certificaat: Dit is veel veiliger en sterk aanbevolen. Een derde partij valideert tegen betaling dat het netwerk legitiem is en maakt een CA-certificaat aan dat vervolgens aan de site wordt gekoppeld. Kijk voor meer informatie over CA-certificaten in de sectie Certificaten van dit artikel.

Er zijn links naar artikelen op AnyConnect binnen dit document. Klik hier voor een overzicht van AnyConnect.

IPsec-profiel

Easy VPN (EZVPN), The GreenBow en Shrew Soft zijn Internet Protocol Security (IPSec) VPNâ€™s. IPsec VPNâ€™s bieden beveiligde tunnels tussen twee peers of van een client-naar-site. Pakketten die als gevoelig worden beschouwd, moeten via deze beveiligde tunnels worden verzonden. De parameters met inbegrip van hashalgoritme, encryptiealgoritme, zeer belangrijke levensduur, en wijze moeten worden gebruikt om deze gevoelige pakketten te beschermen zouden moeten worden bepaald door de kenmerken van deze tunnels te specificeren. Wanneer de IPsec-peer een dergelijk gevoelig pakket ziet, wordt vervolgens de juiste beveiligde tunnel ingesteld en wordt het pakket door deze tunnel naar de externe peer verzonden.

Wanneer IPsec in een firewall of router wordt geïmplementeerd, biedt het een sterke beveiliging die op al het verkeer dat de perimeter oversteekt kan worden toegepast. Het verkeer binnen een bedrijf of een werkgroep heeft geen overheadkosten van security-related verwerking.

Om de twee uiteinden van een VPN-tunnel succesvol te kunnen versleutelen en tot stand te brengen, moeten ze het eens worden over de methoden van versleuteling, decryptie en verificatie. IPsec-profiel is de centrale configuratie in IPsec die de algoritmen definieert zoals codering, verificatie en Diffie-Hellman (DH) groep voor fase I en II onderhandeling in automatische modus, evenals handmatige toetsmodus.

Belangrijke componenten van IPsec zijn Internet Key Exchange (IKE), fase 1 en fase 2.

Het basisdoel van fase één van IKE is de peers van IPSec voor authentiek te verklaren en een veilig kanaal tussen de peers op te zetten om uitwisselingen IKE toe te laten. IKE fase één voert de volgende functies uit:

- Verificeert en beschermt de identiteiten van de IPSec-peers
- Onderhandelt een overeenkomend beleid van IKE Security Associations (SA) tussen peers om de IKE-uitwisseling te beschermen
- Voert een geauthenticeerde Diffie-Hellman uitwisseling uit met het eindresultaat van het hebben van bijpassende gedeelde geheime sleutels
- Stelt een beveiligde tunnel in om IKE fase twee parameters te onderhandelen
- Komt in twee wijzen voor, hoofd en agressieve wijze

Het doel van fase twee IKE is om IPSec SAs te onderhandelen om de IPSec-tunnel op te zetten. IKE fase twee voert de volgende functies uit:

- Onderhandelt IPSec SA-parameters die door een bestaande IKE SA worden beschermd
- Vestigt IPsec-beveiligingsassociaties
- Onderhandelt IPSec SAâ€™s periodiek opnieuw om de beveiliging te waarborgen
- Voert optioneel een extra Diffie-Hellman uitwisseling uit
- Er wordt slechts één modus gebruikt, de snelmodus

Als Perfect Forward Secrecy (PFS) is gespecificeerd in het IPSec-beleid, wordt een nieuwe DH-uitwisseling uitgevoerd met elke snelle modus, waardoor sleutelmateriaal wordt geleverd met een grotere entropie (key material life) en daardoor een grotere weerstand tegen cryptografische aanvallen. Elke DH-uitwisseling vereist grote uitbreidingen, waardoor het CPU-gebruik toeneemt en de prestatiekosten oplopen.

- Configuratie van Internet Protocol Security (IPSec) profiel op een RV34x Series router
- IPsec-profielen configureren (automatische afsluitmodus) op de RV160 en RV260
- IPsec-profielmodus met handmatige toetsmodus configureren op RV160- en RV260-routers

Point-to-Point Tunneling Protocol (PPTP)

PPTP is een netwerkprotocol dat wordt gebruikt om VPN-tunnels tussen openbare netwerken te maken. PPTP-servers zijn ook bekend als Virtual Private Dialup Network (VPDN)-servers. PPTP wordt soms gebruikt over andere protocollen omdat het sneller is en capaciteit heeft om aan mobiele apparaten te werken. Het is echter belangrijk om op te merken dat het niet zo veilig is als andere typen VPN's. Er zijn meerdere methoden om verbinding te maken met PPTP-type accounts. Klik op de links voor meer informatie:

- Een Point-to-Point Tunneling Protocol (PPTP)-server op de RV34x Series-router configureren
- Point-to-Point Tunneling Protocol (PPTP)-server op RV320 en RV325 VPN-routerserie op Windows configureren

Generic Routing Encapsulation

Generic Routing Encapsulation (GRE) is een tunnelprotocol dat een eenvoudige generieke benadering biedt van transportpakketten van een protocol via een ander protocol door middel van inkapseling.

GRE kapselt een payload in, dat wil zeggen, een binnenpakket dat moet worden geleverd aan een doelnetwerk binnen een extern IP-pakket. De GRE-tunnel gedraagt zich als een virtuele point-to-point link die twee eindpunten heeft die worden geïdentificeerd door de tunnelbron en het doeladres van de tunnel.

De tunnelendpoints verzenden payloads via GRE-tunnels door ingekapselde pakketten te routeren via tussenliggende IP-netwerken. Andere IP routers langs de weg ontleden niet de payload (het binnenpakket); zij ontleden slechts het buitenste IP pakket aangezien zij het naar het GRE tunneleindpunt door:sturen. Bij het bereiken van het tunneleindpunt wordt GRE-inkapseling verwijderd en wordt de payload doorgestuurd naar de uiteindelijke bestemming van het pakket.

De insluiting van datagrammen in een netwerk gebeurt om meerdere redenen, zoals wanneer een bronserver de route wil beïnvloeden die een pakket neemt om de doelhost te bereiken. De bronserver is ook bekend als de inkapselingsserver.

IP-in-IP-insluiting impliceert de invoeging van een externe IP-header via de bestaande IP-header. Het bron- en doeladres in het externe IP-headerpunt naar de eindpunten van de IP-in-IP tunnel. De stapel IP-headers wordt gebruikt om het pakket via een vooraf bepaald pad naar de bestemming te leiden, mits de netwerkbeheerder de loopback-adressen kent van de routers die het pakket verzenden.

Dit tunnelmechanisme kan worden gebruikt voor het bepalen van de beschikbaarheid en latentie voor de meeste netwerkarchitecturen. Opgemerkt moet worden dat het gehele pad van de bron naar de bestemming niet hoeft te worden opgenomen in de kopregels, maar dat een segment van het netwerk kan worden gekozen voor het sturen van de pakketten.

Layer 2-tunnelprotocol

L2TP verstrekt geen encryptiemechanismen voor het verkeer het tunnels. In plaats daarvan maakt het gebruik van andere beveiligingsprotocollen, zoals IPSec, om de gegevens te versleutelen.

Er wordt een L2TP-tunnel tot stand gebracht tussen de L2TP-toegangsconcentrator (LAC) en de L2TP-netwerkserver (LNS). Er is ook een IPSec-tunnel tot stand gebracht tussen deze apparaten en al het L2TP-tunnelverkeer is versleuteld met IPSec.

Enkele sleuteltermen met L2TP:

- **CHAP -** Challenge Handshake-verificatieprotocol. Een Point-to-Point-verificatieprotocol (PPP).
- **L2TP Access Concentrator (LAC) -** Een LAC kan een Cisco-netwerktoegangsserver zijn die is aangesloten op het openbare telefoonnetwerk (PSTN). De LAC hoeft alleen media te implementeren voor gebruik via L2TP. Een LAC kan met LAN verbinden via een lokaal netwerk of een groot netwerk zoals een openbaar of privé Frame Relay. De LAC is de initiator van inkomende oproepen en de ontvanger van uitgaande oproepen.
- **L2TP Network Server (LNS) -** Bijna elke Cisco-router die is aangesloten op een lokaal netwerk of een breedbandnetwerk, zoals openbaar of privaat Frame Relay, kan fungeren als een LNS. Het is de serverkant van het L2TP protocol en moet werken op elk platform dat PPP-sessies beëindigt. LNS is de initiator van uitgaande vraag en de ontvanger van inkomende vraag. Figuur 1 schildert de vraagroutine tussen LAC en LNS af.
- **Virtual Private Dial Network (VPDN) -** een type VPN-toegang dat PPP gebruikt om de service te leveren.

Als u meer informatie over L2TP wilt, klikt u op de volgende links:

- L2TP WAN-instellingen op de RV34x router configureren
- Wide Area Networking Configuration Guide: Layer 2 services, Cisco IOS XE release 3S

VPNâ€™s die compatibel zijn met Cisco RV Series VPN-routers

	RV340X	RV320X	RV160X/RV260X
IPsec (IKEv1)			
ShrewSoft	Ja	Ja	Ja
groenboog	Ja	Ja	Ja
Geïntegreerde Mac-client	Ja	Ja	Nee
iPhone/iPad	Ja	Ja	Nee
Android	Ja	Ja	Ja
L2TP/IPSec	Ja (PAP)	Nee	Nee
PPTP	Ja (PAP)	Ja*	Ja (PAP)
Other (Overig)			
AnyConnect	Ja	Nee	Nee
OpenVPN	Nee	Ja	Ja
IKEv2			
Windows	Ja*	Nee	Ja*
Mac	Ja	Nee	Ja
iPhone	Ja	Nee	Ja
Android	Ja	Nee	Ja

VPN-technologie	Ondersteunde apparaten	Ondersteunde clients*	Details en voorbehouden
IPsec (IKEv1)	RV340X, RV32X, RV160X/RV260X	Native: Mac, iPhone, iPad,	Eenvoudig te installeren, probleemoplossing en ondersteuning. Het is beschikbaar op alle routers, is

		Android Overige: EasyVPN (Cisco VPN-client), ShrewSoft, Greenbow	eenvoudig aan opstelling (voor het grootste deel), heeft het beste registreren om problemen op te lossen. En bevat de meeste apparaten. Dit is de reden waarom we meestal aanraden ShrewSoft (gratis en werkt) en Greenbow (niet gratis, maar werkt). Voor Windows hebben we ShrewSoft en Greenbow-clients als opties, omdat Windows geen pure IPSec native VPN-client heeft. Voor ShrewSoft en Greenbow is het iets meer betrokken, maar niet moeilijk. Na de eerste installatie kunnen clientprofielen worden geëxporteerd en vervolgens op andere clients worden geïmporteerd. Voor RV160X/RV260X routers, omdat we niet de Easy VPN optie hebben, moeten we de 3rd Party Client optie gebruiken, die niet werkt met Mac, iPhone of iPad. We kunnen wel ShrewSoft, Greenbow en Android-clients instellen om verbinding te maken. Voor Mac-, iPhone- en iPad-clients raad ik IKEv2 aan (zie hieronder).
AnyConnect	RV340X	Windows, Mac, iPhone, iPad, Android	Sommige klanten vragen een volledige Cisco-oplossing en dit is de oplossing. Het is eenvoudig te installeren, heeft vastlegging, maar kan uitdagend zijn om de logbestanden te begrijpen. Vereist clientlicentievereisten tegen hoge kosten. Het is een volledige Cisco-oplossing die wordt bijgewerkt. Probleemoplossing is niet zo eenvoudig als IPSec, maar beter dan de andere VPN-opties.
L2TP/IPSec	RV340X	Standaard: Windows	Dit is wat ik zal aanraden voor klanten die de ingebouwde VPN-client in Windows moeten gebruiken. Twee voorbehouden hierbij zijn: 1. We ondersteunen alleen de PAP-verificatie bij gebruik van lokale verificatie. We moeten naar elke client gaan en optionele of geen encryptie selecteren, MS-CHAP opties uitschakelen en PAP inschakelen. Dit betekent dat de gebruikersnaam/het wachtwoord in het duidelijke wordt verzonden. Het is geen grote deal omdat alles is versleuteld met IPSec, en moet worden ingesteld op elke client. Op Windows, is dit configureerbaar, maar niet op Mac, iPhone, iPad of Android-apparaten, dus echt kan alleen worden gebruikt door Windows-clients, tenzij ze een externe verificatieserver zoals Radius of LDAP hebben. 2. Als de router zich achter een NAT-apparaat bevindt, kan de verbinding niet worden gemaakt op Windows-machines. De tijdelijke oplossing is om een registratiesleutel op elke client te maken om

			NAT op zowel de client als de router toe te staan.
IPsec (IKEv2)	RV340X, RV160X/RV260X	Native: Windows, Mac, iPhone, iPad, Android	Windows native client voor IKEv2 vereist certificaatverificatie, waarvoor een PKI-infrastructuur vereist is omdat zowel de router als alle clients certificaten van dezelfde CA (of een andere vertrouwde CA) moeten hebben. Voor degenen die IKEv2 willen gebruiken, hebben we dat ingesteld voor hun Mac, iPhone, iPad en Android-apparaten en meestal zetten we IKEv1 in voor hun Windows-machines (ShrewSoft, Greenbow of L2TP/IPSec).
VPN openen	RV320X, RV160X/RV260X	Open VPN is de client	Moeilijker te installeren, moeilijk op te lossen en ondersteuning. Ondersteund op RV160X/RV260X en RV320. Installatie is complexer dan IPSec of AnyConnect, met name als ze certificaten gebruiken, wat de meeste doen. Het oplossen van problemen is moeilijker aangezien wij geen nuttige logboeken op de router hebben en zich op de cliëntlogboeken baseren. Ook hebben de updates van de OpenVPN-clientversie zonder waarschuwing gewijzigd welke certificaten zij hebben geaccepteerd. Ook vonden we dat dit niet werkt op Chromebooks en moest naar een IPSec oplossing.

* We testen zoveel mogelijk combinaties als we kunnen, als er een specifieke hardware/software combinatie is, neem dan hier contact op. Anders, zie de verwante configuratiegids per apparaat voor meest recente geteste versie.

Certificaten

Heb je ooit een website bezocht en kreeg je de waarschuwing dat deze niet veilig is? Het vult u niet met vertrouwen dat uw privé-informatie veilig is, en het is niet! Als een site beveiligd is, ziet u een gesloten slotpictogram voor de naam van de site. Dit is een symbool dat de site veilig is bevonden. U wilt er zeker van zijn dat het slotpictogram gesloten is. Hetzelfde geldt voor je VPN.

Wanneer u een VPN instelt, moet u een certificaat verkrijgen bij een certificaatinstantie (CA). Certificaten worden aangeschaft op sites van derden en gebruikt voor verificatie. Het is een officiële manier om te bewijzen dat uw site veilig is. De CA is in wezen een betrouwbare bron die verifieert dat u een legitiem bedrijf bent en kan worden vertrouwd. Voor een VPN heb je alleen een certificaat op lager niveau nodig tegen minimale kosten. U wordt uitgecheckt door de CA, en zodra ze uw informatie verifiëren, zullen ze het Certificaat aan u afgeven. Dit certificaat kan als bestand op uw computer worden gedownload. U kunt dan naar uw router (of VPN-server) gaan en het daar uploaden.

CA maakt gebruik van Public Key Infrastructure (PKI) bij de uitgifte van digitale certificaten, waarbij gebruik wordt gemaakt van publieke sleutel- of private sleutelcodering om de beveiliging te waarborgen. CA's zijn verantwoordelijk voor het beheer van certificaataanvragen en de afgifte van digitale certificaten. Een paar derde partijen CA's zijn IdenTrust, Comodo, GoDaddy, GlobalSign, GeoTrust en Verisign.

Het is belangrijk dat alle gateways in een VPN hetzelfde algoritme gebruiken, anders zullen ze niet kunnen communiceren. Om de zaken eenvoudig te houden, is het aan te raden dat alle Certificaten worden aangeschaft bij dezelfde vertrouwde derde. Dit houdt meerdere Certificaten gemakkelijker te beheren als ze handmatig moeten worden vernieuwd.

Opmerking: Clients hebben meestal geen certificaat nodig om een VPN te gebruiken; het is alleen voor verificatie via de router. Een uitzondering hierop is OpenVPN, waarvoor een client-certificaat vereist is.

Sommige kleine bedrijven kiezen ervoor om een wachtwoord of een vooraf gedeelde sleutel te gebruiken in plaats van een Certificaat voor eenvoud. Dit is minder veilig maar kan kosteloos worden opgezet.

Meer informatie over Certificaten vindt u in de onderstaande links:

- Certificaat (Import/Export/Generate CSR) op de RV160 en RV260 Series router
- Vervang het standaard zelfondertekende certificaat door een SSL-certificaat van een derde partij op de RV34x Series router

Site-to-Site VPN op een router

Voor de lokale en externe router is het belangrijk dat de vooraf gedeelde sleutel (PSK)/het wachtwoord/certificaat dat wordt gebruikt voor de VPN-verbinding, en de beveiligingsinstellingen allemaal overeenkomen. Als een of meer routers gebruik maken van Network Address Translation (NAT), die door de meeste Cisco RV-routers wordt gebruikt, moet u firewallvrijstellingen uitvoeren voor de VPN-verbinding op de lokale en externe router.

Bekijk deze site-to-site artikelen voor meer informatie:

- Site-to-Site VPN configureren op de RV34x
- Een site-to-site VPN op een RV340 of RV345 router configureren
- Cisco Tech Talk: Site-to-Site VPN configureren op RV340 Series routers (video)
- Site-to-Site VPN configureren op een RV160 en RV260 router (basisinstellingen)
- Site-to-Site VPN op de RV160 en RV260 router (geavanceerde instellingen en failover)

Client-to-Site VPN op een router

Voordat een VPN kan worden ingesteld aan de clientzijde, moet een beheerder het op de router configureren.

Klik om deze artikelen van de routerconfiguratie te bekijken:

- De VPN Setup-wizard configureren voor de RV160- en RV260-routers
- Shrew zachte VPN-client configureren met de RV160 en RV260
- Cisco Tech Talk: Shrew Soft VPN configureren op RV160 en RV260 (video)
- De GreenBow IPsec VPN-client instellen en gebruiken om verbinding te maken met RV160- en RV260-routers

Een client-to-site profiel maken

In een client-to-site VPN-verbinding kunnen clients van het internet verbinding maken met de server om toegang te krijgen tot het bedrijfsnetwerk of LAN achter de server, maar de beveiliging van het netwerk en de bronnen blijft behouden. Deze eigenschap is zeer nuttig aangezien het tot een nieuwe tunnel leidt van VPN die telewerkers en zakenreizigers zou toestaan om tot uw netwerk toegang te hebben door een VPN cliëntsoftware te gebruiken zonder privacy en veiligheid te compromitteren. De volgende artikelen zijn

specifiek voor de routers uit de RV34x-serie:

- Configuratie van client-to-site Virtual Private Network (VPN)-verbinding op de RV34x Series router
- Connectiviteit van AnyConnect VPN (virtueel particulier netwerk) op de RV34x Series router configureren

De client-to-site VPN werkt niet als Port Forwarding is ingesteld voor *alle verkeer* en *alle verkeer* als bron.

Gebruikersgroepen

Gebruikersgroepen worden op de router aangemaakt voor een verzameling gebruikers die dezelfde reeks services delen. Deze gebruikersgroepen bevatten opties voor de groep, zoals een lijst met toegangsrechten voor de VPN. Afhankelijk van het apparaat kunnen PPTP, site-to-site IPSec VPN en client-to-site IPSec VPN worden toegestaan. De RV260 heeft bijvoorbeeld opties die OpenVPN omvatten, maar L2TP wordt niet ondersteund. De RV340-serie is uitgerust met AnyConnect voor een SSL VPN, evenals Captive Portal of EZ VPN.

Deze instellingen maken het voor beheerders mogelijk om te controleren en te filteren zodat alleen bevoegde gebruikers toegang kunnen krijgen tot het netwerk. Shrew Soft en TheGreenBow zijn twee van de meest voorkomende VPN-clients die beschikbaar zijn om te downloaden. Ze moeten geconfigureerd worden op basis van de VPN-instellingen van de router om met succes een VPN-tunnel te kunnen opzetten. Het volgende artikel richt zich specifiek op de vorming van een gebruikersgroep:

- Een gebruikersgroep voor VPN-instellingen op de RV34x router maken

Wanneer u Gebruikersgroepen voor een VPN instelt, dient u de standaardbeheerdersaccount in de beheergroep te laten staan en een nieuwe gebruikersaccount en gebruikersgroep voor VPN te maken. Als u uw admin-account naar een andere groep verplaatst, voorkomt u dat u bij de router inlogt. Dientengevolge, zou u een fabrieksterugstellen moeten doen en voor die router opnieuw vormen, verlatend de standaardadminrekening in de admingroep alleen.

Gebruikersaccounts

Gebruikersaccounts worden op de router gemaakt om verificatie van lokale gebruikers mogelijk te maken met behulp van de lokale database voor verschillende services zoals PPTP, VPN-client, GUI-aanmelding (web Graphical User Interface) en Secure Sockets Layer Virtual Private Network (SSLVPN). Hiermee kunnen beheerders geautoriseerde gebruikers alleen besturen en filteren om toegang te krijgen tot het netwerk. Het volgende artikel richt zich specifiek op het aanmaken van een gebruikersaccount:

- Een gebruikersaccount maken voor VPN-clientinstelling op de RV34x-router

Client-to-site op clientlocatie

In een client-to-site VPN-verbinding kunnen clients van het internet verbinding maken met de server om toegang te krijgen tot het bedrijfsnetwerk of LAN achter de server, maar de beveiliging van het netwerk en de bronnen blijft behouden. Deze eigenschap is zeer nuttig aangezien het tot een nieuwe VPN-tunnel leidt die telewerkers en zakenreizigers toestaat om tot uw netwerk toegang te hebben door een VPN clientsoftware te gebruiken zonder privacy en veiligheid te compromitteren. VPN is ingesteld om gegevens te versleutelen en te decrypteren zoals ze worden verzonden en ontvangen.

De AnyConnect-toepassing werkt met SSL VPN en wordt specifiek gebruikt met de RV34x-routers. Het is niet beschikbaar met andere routers uit de RV-serie. Beginnend met versie 1.0.3.15, is een routervergunning niet meer noodzakelijk, maar de vergunningen moeten voor de cliëntkant van VPN worden gekocht. Klik

hier voor meer informatie over Cisco AnyConnect Secure Mobility Client. Voor aanwijzingen over installatie, selecteer uit de volgende artikelen:

- Cisco AnyConnect Secure Mobility Client installeren op een Mac-computer
- Installeer Cisco AnyConnect Secure Mobility Client op een Windows-computer

Er zijn enkele toepassingen van derden die kunnen worden gebruikt voor client-to-site VPN met alle RV-routers. Zoals eerder vermeld, ondersteunt Cisco deze toepassingen niet. Deze informatie wordt voor geleidingsdoeleinden geleverd.

De GreenBow VPN-client is een externe VPN-clienttoepassing waarmee een hostapparaat een beveiligde verbinding voor client-to-site IPsec-tunnel of SSL kan configureren. Dit is een betaalde aanvraag die ondersteuning omvat.

- De GreenBow IPsec VPN-client instellen en gebruiken om verbinding te maken met RV160- en RV260-routers

OpenVPN is een gratis, open-source applicatie die kan worden ingesteld en gebruikt voor een SSL VPN. Het maakt gebruik van een client-server verbinding om veilige communicatie tussen een server en een externe client via het internet te bieden.

- OpenVPN op RV160- en RV260-routers

Shrew Soft is een gratis, opensourcetoepassing die ook voor een IPsec VPN kan worden ingesteld en gebruikt. Het maakt gebruik van een client-server verbinding om veilige communicatie tussen een server en een externe client via het internet te bieden.

- Shrew zachte VPN-client configureren met de RV160 en RV260

Easy VPN werd veel gebruikt voor RV32x routers. Hier is wat informatie voor referentie:

- Configureer Easy Client to Gateway Virtual Private Network (VPN) op RV320- en RV325 VPN-routerserie
- Cisco eenvoudige VPN Q&A
- Eenvoudig VPN op Cisco IOS-softwarereleases

Wizard Instellen

De nieuwste routers uit de Cisco RV-serie worden geleverd met een Wizard VPN Setup die u door de stappen voor de installatie leidt. Met de wizard VPN Setup kunt u basis-LAN-naar-LAN- en VPN-verbindingen met externe toegang configureren en vooraf gedeelde sleutels of digitale certificaten toewijzen voor verificatie. Bekijk deze artikelen voor meer informatie:

- VPN Setup-wizard configureren op de RV160 en RV260
- Virtual Private Network (VPN)-verbinding configureren met de installatiewizard op de RV34x Series-router

Conclusie

Dit artikel heeft je naar een beter begrip van VPNâ€™s geleid, samen met tips om je op weg te helpen. Nu zou u bereid moeten zijn om uw te vormen! Neem enige tijd om de koppelingen te bekijken en kies de beste manier om een VPN op uw Cisco RV Series-router in te stellen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.