Cisco RV Router VPN - Überblick und Best Practices

Ziel

Dieses Dokument bietet eine Übersicht über die Best Practices für Virtual Private Networks (VPN) für alle, die neu bei Routern der Cisco RV-Serie sind.

Inhalt

Einleitung

Es scheint so lange her zu sein, dass der einzige Ort, an dem man arbeiten konnte, im Büro war. Sie erinnern sich vielleicht, dass Sie am Wochenende ins Büro gehen mussten, um eine Arbeitsangelegenheit zu regeln. Es gab keine andere Möglichkeit, Daten aus Unternehmensressourcen zu erhalten, wenn Sie sich nicht physisch in Ihrem Büro befanden. Diese Tage sind vorbei. In der heutigen Zeit können Sie unterwegs sein und von zu Hause aus, in einem anderen Büro, einem Café oder sogar in einem anderen Land aus Geschäfte abwickeln. Der Nachteil ist, dass Hacker immer darauf bedacht sind, an Ihre vertraulichen Daten zu gelangen. Die Nutzung des öffentlichen Internets ist nicht sicher. Wie profitieren Sie von mehr Flexibilität und Sicherheit? Richten Sie ein VPN ein!

Eine VPN-Verbindung ermöglicht es Benutzern, auf ein privates Netzwerk zuzugreifen, Daten zu senden und von diesem zu empfangen. Dies geschieht über ein öffentliches oder gemeinsam genutztes Netzwerk wie das Internet, wobei jedoch eine sichere Verbindung zu einer zugrunde liegenden Netzwerkinfrastruktur gewährleistet wird, um das private Netzwerk und seine Ressourcen zu schützen.

Ein VPN-Tunnel stellt ein privates Netzwerk bereit, das Daten sicher verschlüsselt senden kann, um die Daten zu verschlüsseln, und das eine Authentifizierung durchführt, um die Identität des Clients sicherzustellen. Die Firmenbüros verwenden häufig eine VPN-Verbindung, da es sowohl nützlich als auch notwendig ist, ihren Mitarbeitern den Zugriff auf ihr privates Netzwerk zu ermöglichen, selbst wenn sie sich außerhalb des Büros befinden.

In der Regel verbinden Site-to-Site-VPNs ganze Netzwerke miteinander. Sie erweitern ein Netzwerk und ermöglichen, dass Computerressourcen von einem Standort aus an anderen Standorten verfügbar sind. Mithilfe eines VPN-fähigen Routers kann ein Unternehmen mehrere feste Standorte über ein öffentliches Netzwerk wie das Internet verbinden.

Die standortübergreifende Einrichtung eines VPN ermöglicht es einem Remote-Host oder -Client, so zu agieren, als befänden sie sich im selben lokalen Netzwerk. Nachdem der Router für die Internetverbindung konfiguriert wurde, kann eine VPN-Verbindung zwischen dem Router und einem Endpunkt hergestellt werden. Der VPN-Client ist für die Herstellung einer Verbindung nicht nur von den Einstellungen des VPN-Routers abhängig, sondern auch von den entsprechenden Einstellungen. Einige der VPN-Client-Anwendungen sind plattformspezifisch und zudem abhängig von der Betriebssystemversion. Die Einstellungen müssen identisch sein, da sie sonst nicht kommunizieren können.

Ein VPN kann wie folgt eingerichtet werden:

- Secure Sockets Layer (SSL)
- Internet-Protokollsicherheit (IPSec)
- Point-to-Point Tunneling Protocol (PPTP) - nicht so sicher wie SSL oder IPSec
- Generic Routing Encapsulation (GRE)
- Layer 2 Tunneling Protocol (L2TP)

Wenn Sie noch nie ein VPN eingerichtet haben, erhalten Sie viele neue Informationen in diesem Artikel. Hierbei handelt es sich nicht um eine schrittweise Anleitung, sondern eher um eine Übersicht. Daher wäre es vorteilhaft, diesen Artikel vollständig zu lesen, bevor Sie fortfahren und versuchen, ein VPN in Ihrem Netzwerk einzurichten. Links zu spezifischen Schritten finden Sie in diesem Artikel.

Produkte von Drittanbietern, die nicht von Cisco stammen, wie TheGreenBow, OpenVPN, Shrew Soft und EZ VPN, werden von Cisco nicht unterstützt. Sie werden ausschließlich zu Orientierungszwecken aufgeführt. Wenn Sie über diesen Artikel hinaus Unterstützung benötigen, wenden Sie sich an den Drittanbieter, um Unterstützung zu erhalten.

Vorteile einer VPN-Verbindung

- Mithilfe einer VPN-Verbindung können vertrauliche Netzwerkdaten und -ressourcen geschützt werden.
- Es bietet Komfort und Zugänglichkeit für Remote-Mitarbeiter oder Firmenmitarbeiter, da sie leicht auf die Ressourcen der Hauptniederlassung zugreifen können, ohne physisch anwesend zu sein, und dennoch die Sicherheit des privaten Netzwerks und seiner Ressourcen aufrecht erhalten.
- Die Kommunikation über eine VPN-Verbindung bietet ein höheres Maß an Sicherheit als andere Methoden der Fernkommunikation. Ein fortschrittlicher Verschlüsselungsalgorithmus macht dies möglich und schützt das private Netzwerk vor nicht autorisierten Zugriffen.
- Die tatsächlichen geografischen Standorte der Benutzer sind geschützt und nicht öffentlichen oder gemeinsam genutzten Netzwerken wie dem Internet ausgesetzt.
- Mit einem VPN können neue Benutzer oder eine Benutzergruppe hinzugefügt werden, ohne dass zusätzliche Komponenten oder eine komplizierte Konfiguration erforderlich sind.

Risiken bei der Verwendung einer VPN-Verbindung

- Eine Fehlkonfiguration kann zu Sicherheitsrisiken führen. Da der Entwurf und die Implementierung

eines VPNs kompliziert sein können, ist es notwendig, die Konfiguration der Verbindung einem erfahrenen Fachmann zu übertragen, um sicherzustellen, dass die Sicherheit des privaten Netzwerks nicht beeinträchtigt wird.
- Es könnte weniger zuverlässig sein. Da eine VPN-Verbindung eine Internetverbindung erfordert, ist es wichtig, dass ein Anbieter mit bewährter und getesteter Reputation einen ausgezeichneten Internetdienst bereitstellt und minimale bis gar keine Ausfallzeiten garantiert.
- Wenn eine Situation eintritt, in der neue Infrastruktur oder eine neue Gruppe von Konfigurationen hinzugefügt werden müssen, können technische Probleme aufgrund von Inkompatibilität auftreten, insbesondere wenn es sich um andere Produkte oder Anbieter als die von Ihnen bereits verwendeten handelt.
- Es kann zu langsamen Verbindungsgeschwindigkeiten kommen. Wenn Sie eine ISP-Verbindung verwenden, die einen kostenlosen VPN-Dienst bereitstellt, ist zu erwarten, dass Ihre Verbindung ebenfalls langsam ist, da diese Anbieter keine Priorität auf Verbindungsgeschwindigkeiten legen. Der VPN-Durchsatz hängt von den Hardwarefunktionen des Routers ab.

Weitere Informationen zur Funktionsweise von VPNs finden Sie hier.

Tipps zur Konfiguration eines VPNs

1. Verwenden Sie an beiden Enden ein anderes LAN-IP-Subnetz, während Sie das VPN zwischen verschiedenen Standorten konfigurieren. Wenn die Site, mit der Sie eine Verbindung herstellen, beispielsweise ein 192.168.x.x-Adressierungsschema verwendet, sollten Sie ein 10.x.x.x- oder 172.16.x.x - 172.31.x.x-Subnetz verwenden. Eine weitere Option wären andere Subnetzmasken. Wenn Sie die IP-Adresse Ihres Routers ändern, übernehmen die Geräte im Dynamic Host Configuration Protocol (DHCP) automatisch eine IP-Adresse in diesem Subnetz.
2. Verwenden Sie die statische öffentliche IP an der WAN-Schnittstelle des Routers, um eine stabile VPN-Verbindung zu gewährleisten.
3. Stellen Sie sicher, dass die ausgewählte Verschlüsselungs- und Authentifizierungsebene mit dem Router übereinstimmt, zu dem Sie einen VPN-Tunnel für das VPN einrichten möchten.
4. Vergewissern Sie sich, dass PSK und Key Lifetime (Schlüsselverwendungsdauer) mit den Angaben für den Remote-Router übereinstimmen. Ein PSK kann sein, was Sie wollen, es muss nur am Standort und mit dem Client übereinstimmen, wenn sie als Client auf ihrem Computer eingerichtet. Je nach Gerät kann es verbotene Symbole geben, die Sie nicht verwenden können. Die Schlüssel-Lebensdauer gibt an, wie oft das System den Schlüssel ändert. Ein Zertifikat wird bevorzugt, da es als sicherer gilt.
5. Für die meisten VPNs benötigen die Clients kein Zertifikat, um ein VPN zu verwenden. Es dient lediglich zur Verifizierung über den Router. Beispielsweise erfordert OpenVPN sowohl Client- als auch Standortzertifikate.
6. Stellen Sie die SA-Lebenszeit in Phase I länger ein als die SA-Lebenszeit in Phase II. Wenn Sie Phase I kürzer als Phase II machen, müssen Sie den Tunnel im Gegensatz zum Datentunnel häufig neu verhandeln. Ein Datentunnel benötigt mehr Sicherheit, daher ist es besser, die Lebensdauer in Phase II kürzer als in Phase I zu halten.
7. Ändern Sie alle Kennwörter in etwas Komplexeres.

VPN-Typen

Secure Sockets Layer (SSL)

Cisco Router der Serie RV34x unterstützen über AnyConnect ein SSL VPN. Der RV160 und der RV260 können OpenVPN verwenden, ein weiteres SSL VPN. Über den SSL VPN-Server können Remote-Benutzer einen sicheren VPN-Tunnel über einen Webbrowser einrichten. Diese Funktion ermöglicht den einfachen Zugriff auf eine Vielzahl von Webressourcen und webfähigen Anwendungen über die native HTTP-Browserunterstützung (Hypertext Transfer Protocol Secure) über SSL.

Das SSL VPN ermöglicht Benutzern den Remote-Zugriff auf Netzwerke mit Zugangsbeschränkungen. Dabei wird ein sicherer und authentifizierter Pfad verwendet, indem der Netzwerkverkehr verschlüsselt wird.

Es gibt zwei Optionen für die Einrichtung des Zugriffs in SSL:

1. Selbstsigniertes Zertifikat: Ein Zertifikat, das von seinem eigenen Ersteller signiert wird. Dies wird nicht empfohlen und sollte nur in einer Testumgebung verwendet werden.
2. CA Signed Certificate: Dies ist viel sicherer und sehr zu empfehlen. Gegen eine Gebühr validiert ein Drittanbieter, dass das Netzwerk legitim ist, und erstellt ein Zertifizierungsstellenzertifikat, das dann mit dem Standort verbunden wird. Weitere Informationen zu Zertifizierungsstellenzertifikaten finden Sie im Abschnitt Zertifikate dieses Artikels.

Dieses Dokument enthält Links zu Artikeln auf AnyConnect. Klicken Sie hier, um einen Überblick über AnyConnect zu erhalten.

IPsec-Profil

Easy VPN (EZVPN), TheGreenBow und Shrew Soft sind Internet Protocol Security (IPSec) VPNs. IPSec-VPNs bieten sichere Tunnel zwischen zwei Peers oder von einem Client zum anderen. Pakete, die als sensibel gelten, sollten über diese sicheren Tunnel gesendet werden. Zum Schutz dieser sensitiven Pakete müssen Parameter wie Hash-Algorithmus, Verschlüsselungsalgorithmus, Schlüssellebensdauer und Modus verwendet werden. Hierzu müssen die Merkmale dieser Tunnel angegeben werden. Wenn der IPsec-Peer ein solches sensibles Paket erkennt, richtet er den entsprechenden sicheren Tunnel ein und sendet das Paket über diesen Tunnel an den Remote-Peer.

Wenn IPsec in einer Firewall oder einem Router implementiert wird, bietet es starke Sicherheit, die auf den gesamten Datenverkehr angewendet werden kann, der den Perimeter passiert. Der Datenverkehr innerhalb eines Unternehmens oder einer Arbeitsgruppe verursacht keine zusätzlichen Kosten für die sicherheitsrelevante Verarbeitung.

Damit die beiden Enden eines VPN-Tunnels erfolgreich verschlüsselt und eingerichtet werden können, müssen sie sich auf die Verfahren zur Verschlüsselung, Entschlüsselung und Authentifizierung einigen. IPsec-Profil ist die zentrale Konfiguration in IPsec, die die Algorithmen wie Verschlüsselung, Authentifizierung und DH-Gruppe (Diffie-Hellman) für Phase I und II-Aushandlung im Auto-Modus sowie im manuellen Schlüsselungsmodus definiert.

Wichtige Komponenten von IPsec sind Internet Key Exchange (IKE) Phase 1 und Phase 2.

Der grundlegende Zweck von IKE Phase 1 besteht darin, die IPSec-Peers zu authentifizieren und einen sicheren Kanal zwischen den Peers einzurichten, um IKE-Austauschvorgänge zu ermöglichen. In der ersten IKE-Phase werden folgende Funktionen ausgeführt:

- Authentifizierung und Schutz der Identität der IPSec-Peers
- Verhandelt eine passende IKE Security Associations (SA)-Richtlinie zwischen Peers, um den IKE-Austausch zu schützen
- Führt einen authentifizierten Diffie-Hellman-Austausch mit dem Endergebnis übereinstimmender gemeinsamer geheimer Schlüssel durch
- Richtet einen sicheren Tunnel für die Aushandlung der IKE-Parameter der zweiten Phase ein.
- Tritt in zwei Modi auf: im Hauptmodus und im aggressiven Modus.

Der Zweck von IKE Phase zwei besteht darin, IPSec-Sicherheitszuordnungen auszuhandeln, um den IPSec-Tunnel einzurichten. IKE Phase zwei führt die folgenden Funktionen aus:

- Verhandelt IPSec-SA-Parameter, die durch eine vorhandene IKE-SA geschützt sind

- Erstellt IPSec-Sicherheitszuordnungen
- Regelmäßige Neuverhandlung von IPSec-Sicherheitszuordnungen zur Gewährleistung der Sicherheit
- Optional einen zusätzlichen Diffie-Hellman-Austausch
- Nur ein Modus verwendet, Schnellmodus

Wenn Perfect Forward Secrecy (PFS) in der IPSec-Richtlinie angegeben ist, wird ein neuer DH-Austausch mit jedem Quick-Mode durchgeführt, der Schlüsselmaterial mit größerer Entropie (Key-Material-Life) und damit größerer Widerstandsfähigkeit gegen kryptographische Angriffe bereitstellt. Jeder DH-Austausch erfordert hohe Exponentiationen, wodurch sich die CPU-Nutzung erhöht und hohe Leistungskosten entstehen.

- Konfiguration des IPSec-Profils (Internet Protocol Security) auf einem Router der Serie RV34x
- Konfigurieren von IPSec-Profilen (Auto-Keying-Modus) auf dem RV160 und RV260
- Konfigurieren des manuellen IPsec-Profilschlüsselungsmodus auf RV160- und RV260-Routern

Point-to-Point Tunneling Protocol (PPTP)

PPTP ist ein Netzwerkprotokoll zum Erstellen von VPN-Tunneln zwischen öffentlichen Netzwerken. PPTP-Server werden auch als VPDN-Server (Virtual Private Dialup Network) bezeichnet. PPTP wird manchmal im Vergleich zu anderen Protokollen verwendet, da es schneller ist und auf Mobilgeräten verwendet werden kann. Beachten Sie jedoch, dass die Sicherheit nicht so hoch ist wie bei anderen VPN-Typen. Es gibt mehrere Methoden, um eine Verbindung mit PPTP-Konten herzustellen. Klicken Sie auf die Links, um mehr zu erfahren:

- Konfigurieren eines Point-to-Point Tunneling Protocol (PPTP)-Servers auf dem Router der Serie Rv34x
- Konfiguration eines Point-to-Point Tunneling Protocol (PPTP)-Servers auf den RV320- und RV325-VPN-Routern unter Windows

Generic Routing Encapsulation

Generic Routing Encapsulation (GRE) ist ein Tunneling-Protokoll, das einen einfachen generischen Ansatz für den Transport von Paketen eines Protokolls über ein anderes Protokoll mittels Kapselung bietet.

GRE kapselt eine Nutzlast, d. h. ein inneres Paket, das an ein Zielnetzwerk innerhalb eines äußeren IP-Pakets übermittelt werden muss. Der GRE-Tunnel verhält sich wie eine virtuelle Point-to-Point-Verbindung mit zwei Endpunkten, die durch die Tunnelquelle und die Tunnelzieladresse identifiziert werden.

Die Tunnel-Endpunkte senden Payloads durch GRE-Tunnel, indem sie gekapselte Pakete über dazwischenliegende IP-Netzwerke weiterleiten. Andere IP-Router analysieren die Payload (das innere Paket) nicht. Sie analysieren nur das äußere IP-Paket, während sie es an den Endpunkt des GRE-Tunnels weiterleiten. Beim Erreichen des Tunnelendpunkts wird die GRE-Kapselung entfernt, und die Nutzlast wird an das endgültige Ziel des Pakets weitergeleitet.

Die Kapselung von Datagrammen in einem Netzwerk erfolgt aus mehreren Gründen, z. B. wenn ein Quellserver die Route beeinflussen möchte, die ein Paket zum Ziel-Host nimmt. Der Quellserver wird auch als Kapselungsserver bezeichnet.

Die IP-in-IP-Kapselung beinhaltet das Einfügen eines äußeren IP-Headers über den vorhandenen IP-Header. Die Quell- und Zieladresse im äußeren IP-Header verweist auf die Endpunkte des IP-in-IP-Tunnels. Der Stack aus IP-Headern leitet das Paket über einen vorbestimmten Pfad zum Ziel, vorausgesetzt, der Netzwerkadministrator kennt die Loopback-Adressen der Router, die das Paket transportieren.

Dieser Tunneling-Mechanismus kann zur Bestimmung der Verfügbarkeit und Latenz für die meisten

Netzwerkarchitekturen verwendet werden. Es ist zu beachten, dass der gesamte Pfad von der Quelle zum Ziel nicht in den Headern enthalten sein muss, sondern dass ein Netzwerksegment für die Weiterleitung der Pakete ausgewählt werden kann.

Layer-2-Tunneling-Protokoll

L2TP bietet keine Verschlüsselungsmechanismen für den Datenverkehr, den es tunnelt. Stattdessen setzt es auf andere Sicherheitsprotokolle, wie IPSec, um die Daten zu verschlüsseln.

Zwischen dem L2TP-Zugriffskonzentrator (LAC) und dem L2TP-Netzwerkserver (LNS) wird ein L2TP-Tunnel eingerichtet. Zwischen diesen Geräten wird ein IPSec-Tunnel eingerichtet, und der gesamte L2TP-Tunnelverkehr wird mit IPSec verschlüsselt.

Einige Schlüsselbegriffe von L2TP:

- **CHAP -** Challenge Handshake Authentication Protocol Ein Point-to-Point Authentication Protocol (PPP)
- **L2TP Access Concentrator (LAC) -** Ein LAC kann ein Cisco Network Access Server sein, der mit dem öffentlichen Telefonnetz (PSTN) verbunden ist. Die LAC muss nur Medien für den Betrieb über L2TP implementieren. Ein LAC kann eine Verbindung zum LNS über ein LAN oder ein WAN (z. B. ein öffentliches oder privates Frame Relay) herstellen. Die LAC initiiert eingehende Anrufe und empfängt ausgehende Anrufe.
- **L2TP Network Server (LNS) -** Fast jeder Cisco Router, der mit einem LAN- oder WAN-Netzwerk verbunden ist, z. B. ein öffentlicher oder privater Frame Relay, kann als LNS fungieren. Es ist die Serverseite des L2TP-Protokolls und muss auf jeder Plattform ausgeführt werden, die PPP-Sitzungen beendet. Das LNS initiiert ausgehende Anrufe und empfängt eingehende Anrufe. Abbildung 1 zeigt die Anrufroutine zwischen dem LAC und dem LNS.
- **Virtual Private Dial Network (VPDN) -** Ein Access-VPN, das PPP zur Bereitstellung des Services verwendet.

Wenn Sie weitere Informationen zu L2TP erhalten möchten, klicken Sie auf die folgenden Links:

- Konfigurieren der L2TP-WAN-Einstellungen auf dem RV34x-Router
- Konfigurationsleitfaden für WANs: Layer-2-Services, Cisco IOS XE Release 3S

Mit Cisco VPN-Routern der RV-Serie kompatible VPNs

	RV34X	RV32X	RV 160X/RV 260X
IPSec (IKEv1)			
ShrewSoft	Ja	Ja	Ja
Greenbow	Ja	Ja	Ja
Integrierter Mac-Client	Ja	Ja	Nein
iPhone/iPad	Ja	Ja	Nein
Android	Ja	Ja	Ja
L2TP/IPSec	Ja (PAP)	Nein	Nein
PPTP	Ja (PAP)	Ja*	Ja (PAP)
Andere			
AnyConnect	Ja	Nein	Nein
OpenVPN	Nein	Ja	Ja

IKEv2			
Windows	Ja*	Nein	Ja*
Mac	Ja	Nein	Ja
iPhone	Ja	Nein	Ja
Android	Ja	Nein	Ja

VPN-Technologie	Unterstützte Geräte	Unterstützte Clients*	Details und Hinweise
IPSec (IKEv1)	RV34X, RV32X, RV160X/RV260X	Systemeigen: Mac, iPhone, iPad, Android Sonstige: EasyVPN (Cisco VPN Client), ShrewSoft, Greenbow	Einfache Einrichtung, Fehlerbehebung und Unterstützung Es ist auf allen Routern verfügbar, lässt sich (größtenteils) einfach einrichten und bietet die beste Protokollierung zur Fehlerbehebung. Und schließt die meisten Geräte ein. Deshalb empfehlen wir in der Regel ShrewSoft (frei und funktioniert) und Greenbow (nicht frei, aber funktioniert). Für Windows haben wir ShrewSoft- und Greenbow-Clients als Optionen, da Windows nicht über einen reinen IPSec-nativen VPN-Client verfügt. Für ShrewSoft und Greenbow ist es etwas komplizierter, aber nicht schwer. Nach der Ersteinrichtung können die Clientprofile exportiert und dann auf andere Clients importiert werden. Da für RV160X-/RV260X-Router keine Easy VPN-Option zur Verfügung steht, muss die Client-Option eines Drittanbieters verwendet werden, die mit Mac, iPhone oder iPad nicht funktioniert. Wir können jedoch ShrewSoft-, Greenbow- und Android-Clients für die Verbindung einrichten. Für Mac, iPhone und iPad-Clients empfehle ich IKEv2 (siehe unten).
AnyConnect	RV34X	Windows, Mac, iPhone, iPad, Android	Einige Kunden fordern eine vollständige Lösung von Cisco. Es ist einfach einzurichten, verfügt über Protokollierung, kann jedoch schwierig sein, die Protokolle zu verstehen. Erfordert Client-Lizenzierungsanforderungen, die Kosten verursachen. Es handelt sich um eine vollständige Cisco Lösung, die aktualisiert wurde. Die Fehlerbehebung ist nicht so einfach wie bei IPSec, aber besser als bei den anderen VPN-Optionen.
L2TP/IPSec	RV34X	Systemeigen: Fenster	Dies empfehle ich Kunden, die den integrierten VPN-Client in Windows verwenden müssen. Hier zwei Vorbehalte: 1. PAP-Authentifizierung wird nur bei Verwendung der lokalen Authentifizierung unterstützt. Wir müssen in jeden Client gehen und optional oder keine

			Verschlüsselung auswählen, MS-CHAP-Optionen deaktivieren und PAP aktivieren. Dies bedeutet, dass Benutzername/Kennwort unverschlüsselt gesendet werden. Es ist kein großes Geschäft, da alles mit IPSec verschlüsselt ist und auf jedem Client eingerichtet werden muss. Unter Windows ist dies konfigurierbar, jedoch nicht auf Mac-, iPhone-, iPad- oder Android-Geräten. Daher können Windows-Clients nur verwendet werden, wenn sie über einen externen Authentifizierungsserver wie Radius oder LDAP verfügen. 2. Wenn sich der Router hinter einem NAT-Gerät befindet, schlägt die Verbindung auf Windows-Computern fehl. Die Problemumgehung besteht darin, auf jedem Client einen Registrierungsschlüssel zu erstellen, um NAT sowohl auf dem Client als auch auf dem Router zuzulassen.
IPSec (IKEv2)	RV34X, RV160X/RV260X	Systemeigen: Windows, Mac, iPhone, iPad, Android	Der native Windows-Client für IKEv2 erfordert eine Zertifikatsauthentifizierung, die eine PKI-Infrastruktur erfordert, da sowohl der Router als auch alle Clients über Zertifikate von derselben Zertifizierungsstelle (oder einer anderen vertrauenswürdigen Zertifizierungsstelle) verfügen müssen. Für diejenigen, die IKEv2 verwenden möchten, richten wir dies für ihre Mac-, iPhone-, iPad- und Android-Geräte ein und richten IKEv1 für ihre Windows-Computer ein (ShrewSoft, Greenbow oder L2TP/IPSec).
Offenes VPN	RV32X, RV160X/RV260X	Offenes VPN ist der Client	schwieriger einzurichten, schwierige Fehlerbehebung und Supportleistungen Unterstützt auf RV160X/RV260X und RV320. Die Einrichtung ist komplizierter als IPSec oder AnyConnect, insbesondere wenn Zertifikate verwendet werden, was in den meisten Fällen der Fall ist. Die Fehlerbehebung ist schwieriger, da wir keine nützlichen Protokolle auf dem Router haben und uns auf die Client-Protokolle verlassen. Außerdem haben OpenVPN Client-Versionsaktualisierungen ohne Vorwarnung geändert, welche Zertifikate sie akzeptiert haben. Auch fanden wir, dass dies nicht funktioniert auf Chromebooks und musste zu einer IPSec-Lösung gehen.

* Wir testen so viele Kombinationen wie möglich, wenn es eine bestimmte Hardware/Software-Kombination gibt, wenden Sie sich bitte hier an. Ansonsten finden Sie Informationen zur zuletzt getesteten Version im zugehörigen Konfigurationsleitfaden für die einzelnen Geräte.

Zertifikate

Haben Sie schon einmal eine Website besucht, auf der Sie gewarnt wurden, dass sie nicht sicher ist? Es erfüllt Sie nicht mit der Gewissheit, dass Ihre privaten Daten sicher sind, und das ist es auch nicht! Wenn eine Website sicher ist, wird vor dem Namen der Website ein geschlossenes Schlosssymbol angezeigt. Dies ist ein Symbol dafür, dass die Website sicher überprüft wurde. Sie möchten sicherstellen, dass das Schlosssymbol geschlossen wird. Dasselbe gilt für Ihr VPN.

Wenn Sie ein VPN einrichten, sollten Sie ein Zertifikat von einer Zertifizierungsstelle (Certificate Authority, CA) erhalten. Zertifikate werden von Drittanbieter-Websites erworben und für die Authentifizierung verwendet. Es ist ein offizieller Weg zu beweisen, dass Ihre Website sicher ist. Im Wesentlichen handelt es sich bei der CA um eine vertrauenswürdige Quelle, die sicherstellt, dass Sie ein legitimes Unternehmen sind und vertrauenswürdig sind. Für ein VPN benötigen Sie nur ein Zertifikat der niedrigeren Stufe mit minimalen Kosten. Sie werden von der Zertifizierungsstelle ausgecheckt. Sobald diese Ihre Informationen überprüft hat, stellt sie Ihnen das Zertifikat aus. Dieses Zertifikat kann als Datei auf Ihren Computer heruntergeladen werden. Sie können dann in Ihren Router (oder VPN-Server) gehen und ihn dort hochladen.

CA verwendet die Public Key Infrastructure (PKI), wenn digitale Zertifikate ausgestellt werden, die zur Gewährleistung der Sicherheit eine Verschlüsselung mit öffentlichem Schlüssel oder privatem Schlüssel verwenden. CAs sind für die Verwaltung von Zertifikatsanforderungen und die Ausstellung digitaler Zertifikate zuständig. Zu den CAs von Drittanbietern gehören IdenTrust, Comodo, GoDaddy, GlobalSign, GeoTrust und Verisign.

Es ist wichtig, dass alle Gateways in einem VPN denselben Algorithmus verwenden, da sie sonst nicht kommunizieren können. Um die Dinge einfach zu halten, wird empfohlen, alle Zertifikate von demselben vertrauenswürdigen Drittanbieter zu erwerben. So können mehrere Zertifikate einfacher verwaltet werden, da sie manuell erneuert werden müssen.

Hinweis: Clients benötigen normalerweise kein Zertifikat, um ein VPN zu verwenden. Das Zertifikat dient lediglich zur Verifizierung über den Router. Eine Ausnahme hiervon ist OpenVPN, für das ein Client-Zertifikat erforderlich ist.

Einige kleine Unternehmen verwenden aus Gründen der Einfachheit anstelle eines Zertifikats ein Passwort oder einen vorinstallierten Schlüssel. Dies ist weniger sicher, kann aber kostenlos eingerichtet werden.

Weitere Informationen zu Zertifikaten finden Sie unter den folgenden Links:

- Zertifikat (Import/Export/Generate CSR) für Router der Serien RV160 und RV260
- Ersetzen Sie das standardmäßige selbstsignierte Zertifikat auf dem Router der Serie RV34x durch ein SSL-Zertifikat eines Drittanbieters.

Site-to-Site-VPN auf einem Router

Für den lokalen und den Remote-Router muss sichergestellt werden, dass der vorinstallierte Schlüssel (PSK), das Passwort und das Zertifikat für die VPN-Verbindung sowie die Sicherheitseinstellungen übereinstimmen. Wenn ein oder mehrere Router Network Address Translation (NAT) verwenden, was bei den meisten Routern der Cisco RV-Serie der Fall ist, müssen Sie für die VPN-Verbindung auf dem lokalen und dem Remote-Router Firewallausnahmen vornehmen.

Weitere Informationen finden Sie in den folgenden Artikeln:

- Konfigurieren des Site-to-Site-VPNs auf dem RV34x
- Konfigurieren eines standortübergreifenden VPNs auf einem RV340- oder RV345-Router

- Cisco Tech Talk: Konfigurieren eines standortübergreifenden VPNs auf Routern der Serie RV340 (Video)
- Konfigurieren eines Site-to-Site-VPNs auf einem RV160- und RV260-Router (Grundeinstellungen)
- Site-to-Site-VPN auf dem RV160- und RV260-Router (erweiterte Einstellungen und Failover)

Client-to-Site-VPN auf einem Router

Bevor ein VPN auf der Client-Seite eingerichtet werden kann, muss es vom Administrator auf dem Router konfiguriert werden.

Klicken Sie hier, um folgende Artikel zur Routerkonfiguration anzuzeigen:

- Konfigurieren des VPN-Einrichtungsassistenten auf den Routern RV160 und RV260
- Konfigurieren des Shrew Soft VPN Client für den RV160 und den RV260
- Cisco Tech Talk: Konfigurieren von Shrew Soft VPN auf RV160 und RV260 (Video)
- Richten Sie den GreenBow IPsec VPN Client für die Verbindung mit RV160- und RV260-Routern ein, und verwenden Sie ihn.

Erstellen eines Client-to-Site-Profils

Bei einer Client-to-Site-VPN-Verbindung können sich Clients aus dem Internet mit dem Server verbinden, um auf das Unternehmensnetzwerk oder LAN hinter dem Server zuzugreifen, ohne die Sicherheit des Netzwerks und seiner Ressourcen zu beeinträchtigen. Diese Funktion ist sehr nützlich, da sie einen neuen VPN-Tunnel erstellt, über den Telearbeiter und Geschäftsreisende mithilfe einer VPN-Client-Software auf Ihr Netzwerk zugreifen können, ohne dass Datenschutz und Sicherheit beeinträchtigt werden. Die folgenden Artikel gelten speziell für die Router der RV34x-Serie:

- Konfigurieren der VPN-Verbindung (Virtual Private Network) zwischen Clients auf dem Router der Serie RV34x
- Konfigurieren von AnyConnect Virtual Private Network (VPN)-Konnektivität auf dem Router der RV34x-Serie

Das standortübergreifende Client-VPN funktioniert nicht, wenn Port Forwarding für den *gesamten Quelldatenverkehr* und den *gesamten Zieldatenverkehr* festgelegt ist.

Benutzergruppen

Benutzergruppen werden auf dem Router für eine Reihe von Benutzern erstellt, die den gleichen Satz von Services nutzen. Diese Benutzergruppen enthalten Optionen für die Gruppe, z. B. eine Liste der Berechtigungen für den Zugriff auf das VPN. Je nach Gerät können PPTP, Site-to-Site-IPSec-VPN und Client-to-Site-IPSec-VPN zugelassen werden. Der RV260 verfügt beispielsweise über Optionen wie OpenVPN, L2TP wird jedoch nicht unterstützt. Die RV340-Serie ist mit AnyConnect für ein SSL VPN sowie mit Captive Portal oder EZ VPN ausgestattet.

Mithilfe dieser Einstellungen können Administratoren festlegen und filtern, dass nur autorisierte Benutzer auf das Netzwerk zugreifen können. Shrew Soft und TheGreenBow sind zwei der gängigsten VPN Clients, die zum Download zur Verfügung stehen. Sie müssen auf Basis der VPN-Einstellungen des Routers konfiguriert werden, damit ein VPN-Tunnel erfolgreich eingerichtet werden kann. Der folgende Artikel behandelt speziell die Erstellung einer Benutzergruppe:

- Erstellen einer Benutzergruppe für die VPN-Einrichtung auf dem RV34x-Router

Achten Sie beim Einrichten von Benutzergruppen für ein VPN darauf, dass Sie das Standard-Admin-Konto in der Admin-Gruppe belassen und ein neues Benutzerkonto und eine neue Benutzergruppe für VPN

erstellen. Wenn Sie Ihr Administratorkonto in eine andere Gruppe verschieben, können Sie sich nicht mehr beim Router anmelden. Daher müssten Sie den Router auf die Werkseinstellungen zurücksetzen und erneut konfigurieren, wobei das standardmäßige Admin-Konto in der Admin-Gruppe erhalten bleibt.

Benutzerkonten

Benutzerkonten werden auf dem Router erstellt, um die Authentifizierung lokaler Benutzer mithilfe der lokalen Datenbank für verschiedene Dienste wie PPTP, VPN-Client, GUI-Anmeldung (Web Graphical User Interface) und SSL VPN (Secure Sockets Layer Virtual Private Network) zu ermöglichen. So können Administratoren autorisierte Benutzer nur kontrollieren und filtern, um auf das Netzwerk zuzugreifen. Der folgende Artikel behandelt speziell die Erstellung eines Benutzerkontos:

- Erstellen eines Benutzerkontos für die VPN-Client-Einrichtung auf dem RV34x-Router

Client-to-Site am Client-Standort

Bei einer Client-to-Site-VPN-Verbindung können sich Clients aus dem Internet mit dem Server verbinden, um auf das Unternehmensnetzwerk oder LAN hinter dem Server zuzugreifen, ohne die Sicherheit des Netzwerks und seiner Ressourcen zu beeinträchtigen. Diese Funktion ist sehr nützlich, da sie einen neuen VPN-Tunnel erstellt, über den Telearbeiter und Geschäftsreisende mithilfe einer VPN-Client-Software auf Ihr Netzwerk zugreifen können, ohne dass Datenschutz und Sicherheit beeinträchtigt werden. Das VPN ist so eingerichtet, dass Daten beim Senden und Empfangen verschlüsselt und entschlüsselt werden.

Die AnyConnect-Anwendung arbeitet mit SSL VPN und wird speziell mit den RV34x-Routern verwendet. Es ist nicht mit anderen Routern der RV-Serie verfügbar. Ab Version 1.0.3.15 ist keine Router-Lizenz mehr erforderlich. Es müssen jedoch Lizenzen für die Client-Seite des VPN erworben werden. Weitere Informationen zum Cisco AnyConnect Secure Mobility Client finden Sie hier. Anweisungen zur Installation finden Sie in den folgenden Artikeln:

- Installieren des Cisco AnyConnect Secure Mobility Client auf einem Mac-Computer
- Installieren des Cisco AnyConnect Secure Mobility Client auf einem Windows-Computer

Es gibt einige Anwendungen von Drittanbietern, die für ein standortübergreifendes VPN mit allen Routern der RV-Serie verwendet werden können. Wie bereits erwähnt, unterstützt Cisco diese Anwendungen nicht. Diese Informationen werden lediglich als Orientierungshilfe bereitgestellt.

Der GreenBow VPN Client ist eine VPN Client-Anwendung eines Drittanbieters, mit der ein Hostgerät eine sichere Verbindung für einen Client-to-Site-IPsec-Tunnel oder SSL konfigurieren kann. Hierbei handelt es sich um eine kostenpflichtige Anwendung mit Support.

- Richten Sie den GreenBow IPsec VPN Client für die Verbindung mit RV160- und RV260-Routern ein, und verwenden Sie ihn.

OpenVPN ist eine kostenlose Open-Source-Anwendung, die für ein SSL VPN eingerichtet und verwendet werden kann. Es verwendet eine Client-Server-Verbindung, um über das Internet eine sichere Kommunikation zwischen einem Server und einem entfernten Client-Standort zu ermöglichen.

- OpenVPN auf Routern der Serien RV160 und RV260

Shrew Soft ist eine kostenlose Open-Source-Anwendung, die auch für ein IPsec-VPN eingerichtet und verwendet werden kann. Es verwendet eine Client-Server-Verbindung, um über das Internet eine sichere Kommunikation zwischen einem Server und einem entfernten Client-Standort zu ermöglichen.

- Konfigurieren des Shrew Soft VPN Client für den RV160 und den RV260

Easy VPN wurde in der Regel auf RV32x-Routern verwendet. Nachstehend finden Sie einige Referenzinformationen:

- Konfiguration eines Easy Client-Gateways für ein Virtual Private Network (VPN) auf den VPN-Routern RV320 und RV325
- Fragen und Antworten zu Cisco Easy VPN
- Easy VPN auf softwarebasierten Cisco IOS Routern

Setup-Assistent

Die neuesten Router der Cisco RV-Serie werden mit einem VPN Setup Wizard (VPN-Einrichtungsassistent) ausgeliefert, der Sie durch die Schritte zur Einrichtung führt. Mit dem VPN Setup Wizard (VPN-Einrichtungsassistent) können Sie grundlegende LAN-zu-LAN- und Remote Access-VPN-Verbindungen konfigurieren und entweder Pre-Shared Keys oder digitale Zertifikate für die Authentifizierung zuweisen. Weitere Informationen finden Sie in diesen Artikeln:

- Konfigurieren des VPN-Einrichtungsassistenten auf dem RV160 und RV260
- Konfigurieren der VPN-Verbindung mithilfe des Setup-Assistenten auf dem Router der Serie RV34x

Schlussfolgerung

Dieser Artikel hat Ihnen zu einem besseren Verständnis von VPNs geführt, zusammen mit Tipps, um Sie auf den Weg zu bringen. Jetzt sollten Sie bereit sein, Ihre eigenen zu konfigurieren! Nehmen Sie sich etwas Zeit, um sich die Links anzusehen und zu entscheiden, wie Sie am besten ein VPN auf Ihrem Router der Cisco RV-Serie einrichten.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.