Présentation et bonnes pratiques des routeurs VPN Cisco RV

Objectif

L'objectif de ce document est de présenter les meilleures pratiques en matière de réseau privé virtuel (VPN) à toute personne qui découvre les routeurs de la gamme Cisco RV.

Table des matières

Introduction

Il semble qu'il y a si longtemps que le seul endroit où vous pouviez travailler était au bureau. Vous vous souvenez peut-être, à l'époque, d'avoir dû vous rendre au bureau le week-end pour régler une affaire de travail. Il n'y avait pas d'autre moyen d'obtenir des données auprès des ressources de l'entreprise, sauf si vous étiez physiquement dans votre bureau. Cette époque est révolue. Aujourd'hui, vous pouvez vous déplacer, travailler de chez vous, dans un autre bureau, dans un café ou même dans un autre pays. L'inconvénient est que les pirates cherchent toujours à récupérer vos données sensibles. Le simple fait d'utiliser Internet n'est pas sûr. Que pouvez-vous faire pour bénéficier de la flexibilité et de la sécurité ? Configurez un VPN !

Une connexion VPN permet aux utilisateurs d'accéder à un réseau privé, d'envoyer et de recevoir des données vers et depuis un réseau privé en passant par un réseau public ou partagé tel qu'Internet, tout en assurant une connexion sécurisée à une infrastructure réseau sous-jacente

afin de protéger le réseau privé et ses ressources.

Un tunnel VPN établit un réseau privé qui peut envoyer des données en toute sécurité en utilisant le chiffrement pour coder les données et l'authentification pour garantir l'identité du client. Les bureaux d'entreprise utilisent souvent une connexion VPN, car il est à la fois utile et nécessaire de permettre à leurs employés d'accéder à leur réseau privé, même s'ils sont à l'extérieur du bureau.

Normalement, les VPN de site à site connectent des réseaux entiers entre eux. Ils étendent un réseau et permettent aux ressources informatiques d'un emplacement d'être disponibles à d'autres emplacements. Grâce à l'utilisation d'un routeur compatible VPN, une entreprise peut connecter plusieurs sites fixes sur un réseau public tel qu'Internet.

La configuration client-à-site pour un VPN permet à un hôte distant, ou client, d'agir comme s'ils se trouvaient sur le même réseau local. Une connexion VPN peut être établie entre le routeur et un point d'extrémité une fois que le routeur a été configuré pour la connexion Internet. Le client VPN dépend des paramètres du routeur VPN, en plus de l'exigence des paramètres correspondants afin d'établir une connexion. En outre, certaines des applications clientes VPN sont spécifiques à la plate-forme, elles dépendent également de la version du système d'exploitation. Les paramètres doivent être exactement les mêmes ou ils ne peuvent pas communiquer.

Un VPN peut être configuré avec l'un des éléments suivants :

- Secure Socket Layer (SSL)
- Sécurité du protocole Internet (IPSec)
- Protocole PPTP (Point to Point Tunneling Protocol) : pas aussi sécurisé que SSL ou IPSec
- Encapsulation de routage générique (GRE)
- Protocole L2TP (Layer 2 Tunneling Protocol)

Si vous n'avez jamais configuré de VPN auparavant, vous recevrez beaucoup de nouvelles informations tout au long de cet article. Il ne s'agit pas d'un guide étape par étape, mais plutôt d'une présentation à titre de référence. Par conséquent, il serait utile de lire cet article dans son intégralité avant de passer à l'étape suivante et d'essayer de configurer un VPN sur votre réseau. Des liens vers des étapes spécifiques sont fournis tout au long de cet article.

Les produits tiers non Cisco, notamment TheGreenBow, OpenVPN, Shrew Soft et EZ VPN ne sont pas pris en charge par Cisco. Ils sont inclus uniquement à titre indicatif. Si vous avez besoin d'aide sur ces éléments au-delà de l'article, vous devez contacter le tiers pour obtenir de l'aide.

Avantages de l'utilisation d'une connexion VPN

- L'utilisation d'une connexion VPN permet de protéger les données et les ressources réseau confidentielles.

- Il offre commodité et accessibilité aux travailleurs distants ou aux employés de l'entreprise, car ils pourront facilement accéder aux ressources du bureau central sans avoir à être physiquement présents et tout en préservant la sécurité du réseau privé et de ses ressources.
- La communication à l'aide d'une connexion VPN offre un niveau de sécurité plus élevé que les autres méthodes de communication à distance. Un algorithme de chiffrement avancé rend cela possible, protégeant le réseau privé contre les accès non autorisés.
- Les emplacements géographiques réels des utilisateurs sont protégés et ne sont pas exposés au public ou aux réseaux partagés comme Internet.
- Un réseau privé virtuel permet d'ajouter de nouveaux utilisateurs ou un groupe d'utilisateurs sans nécessiter de composants supplémentaires ou une configuration complexe.

Risques liés à l'utilisation d'une connexion VPN

- Il peut y avoir des risques de sécurité dus à une mauvaise configuration. Étant donné que la conception et la mise en oeuvre d'un VPN peuvent être compliquées, il est nécessaire de confier la tâche de configuration de la connexion à un professionnel expérimenté et expérimenté afin de s'assurer que la sécurité du réseau privé ne serait pas compromise.
- Il est peut-être moins fiable. Étant donné qu'une connexion VPN nécessite une connexion Internet, il est important d'avoir un fournisseur avec une réputation éprouvée et testée pour fournir un excellent service Internet et garantir un temps d'arrêt minimal ou nul.
- Si une situation se présente où il est nécessaire d'ajouter une nouvelle infrastructure ou un nouvel ensemble de configurations, des problèmes techniques peuvent survenir en raison d'une incompatibilité, en particulier si elle implique des produits ou des fournisseurs différents de ceux que vous utilisez déjà.
- Des vitesses de connexion lentes peuvent se produire. Si vous utilisez une connexion de FAI qui fournit un service VPN gratuit, il est probable que votre connexion soit également lente, car ces fournisseurs ne donnent pas la priorité aux vitesses de connexion. Il est important de noter que le débit VPN dépend des capacités matérielles du routeur.

Pour plus d'informations sur le fonctionnement des VPN, cliquez ici.

Conseils à utiliser lors de la configuration d'un VPN

1. Utilisez un sous-réseau IP LAN différent aux deux extrémités lors de la configuration du VPN entre différents sites. Par exemple, si le site auquel vous vous connectez utilise un système d’adressage 192.168.xx, vous pouvez utiliser un sous-réseau 10.xxx ou 172.16.xx - 172.31.xx. Une autre option consiste à utiliser des masques de sous-réseau différents. Lorsque vous modifiez l'adresse IP de votre routeur, les périphériques sur le protocole DHCP (Dynamic Host Configuration Protocol) récupèrent automatiquement une adresse IP dans ce sous-réseau.
2. Utilisez l'adresse IP publique statique sur l'interface WAN du routeur pour une connectivité VPN stable.
3. Assurez-vous que le niveau de cryptage et d'authentification sélectionné est le même que celui du routeur vers lequel vous souhaitez établir un tunnel VPN pour le VPN.

4. Assurez-vous que la clé PSK et la durée de vie de la clé saisies sont identiques à celles du routeur distant. Un PSK peut être ce que vous voulez qu'il soit, il doit simplement correspondre au site et avec le client quand ils configurent en tant que client sur leur ordinateur. Selon le périphérique, il peut y avoir des symboles interdits que vous ne pouvez pas utiliser. La durée de vie de la clé est la fréquence à laquelle le système change la clé. Un certificat est préférable car il est considéré comme plus sécurisé.
5. Pour la plupart des VPN, les clients n'ont pas besoin d'un certificat pour utiliser un VPN, c'est juste pour la vérification par le routeur. Par exemple, OpenVPN nécessite des certificats de client et de site.
6. Définissez la durée de vie de votre SA dans la phase I plus longue que la durée de vie de votre SA dans la phase II. Si vous raccourcissez la phase I par rapport à la phase II, vous devrez alors renégocier le tunnel en avant et en arrière fréquemment par opposition au tunnel de données. Un tunnel de données a besoin de plus de sécurité, il est donc préférable d'avoir une durée de vie plus courte dans la Phase II que dans la Phase I.
7. Remplacez tous les mots de passe par des mots plus complexes.

Types de VPN

SSL (Secure Sockets Layer)

Les routeurs de la gamme Cisco RV34x prennent en charge un VPN SSL, utilisant AnyConnect. Les routeurs RV160 et RV260 ont la possibilité d'utiliser OpenVPN, qui est un autre VPN SSL. Le serveur VPN SSL permet aux utilisateurs distants d'établir un tunnel VPN sécurisé à l'aide d'un navigateur Web. Cette fonctionnalité permet d'accéder facilement à un large éventail de ressources Web et d'applications Web à l'aide du support de navigateur HTTP (Hypertext Transfer Protocol) natif sur SSL HTTPS (Hypertext Transfer Protocol Secure).

Le VPN SSL permet aux utilisateurs d'accéder à distance à des réseaux restreints, en utilisant un chemin sécurisé et authentifié en chiffrant le trafic réseau.

Il existe deux options pour configurer l'accès dans SSL :

1. Certificat auto-signé : certificat signé par son propre créateur. Ceci n'est pas recommandé et ne doit être utilisé que dans un environnement de test.
2. Certificat signé par l'autorité de certification : il est beaucoup plus sécurisé et fortement recommandé. Moyennant des frais, un tiers valide que le réseau est légitime et crée un certificat d'autorité de certification qui est ensuite joint au site. Pour plus d'informations sur les certificats CA, consultez la section Certificats de cet article.

Ce document contient des liens vers des articles sur AnyConnect. Pour une présentation d'AnyConnect, cliquez ici.

Profil IPsec

Easy VPN (EZVPN), TheGreenBow et Shrew Soft sont des VPN IPSec (Internet Protocol Security). Les VPN IPSec fournissent des tunnels sécurisés entre deux homologues ou entre un

client et un site. Les paquets considérés comme sensibles doivent être envoyés via ces tunnels sécurisés. Les paramètres tels que l'algorithme de hachage, l'algorithme de chiffrement, la durée de vie de la clé et le mode doivent être utilisés pour protéger ces paquets sensibles. Pour ce faire, il convient de définir les caractéristiques de ces tunnels. Ensuite, lorsque l'homologue IPsec voit un paquet aussi sensible, il configure le tunnel sécurisé approprié et envoie le paquet à travers ce tunnel à l'homologue distant.

Lorsqu'IPsec est mis en oeuvre dans un pare-feu ou un routeur, il offre une sécurité renforcée qui peut être appliquée à tout le trafic traversant le périmètre. Le trafic au sein d'une entreprise ou d'un groupe de travail n'engendre pas les frais de traitement liés à la sécurité.

Pour que les deux extrémités d'un tunnel VPN soient correctement chiffrées et établies, elles doivent toutes deux s'entendre sur les méthodes de chiffrement, de déchiffrement et d'authentification. Le profil IPsec est la configuration centrale d'IPsec qui définit les algorithmes tels que le chiffrement, l'authentification et le groupe Diffie-Hellman (DH) pour la négociation des phases I et II en mode automatique ainsi qu'en mode de saisie manuelle.

Les composants importants d'IPsec sont les phases 1 et 2 d'Internet Key Exchange (IKE).

L'objectif de base de la première phase IKE est d'authentifier les homologues IPSec et de configurer un canal sécurisé entre les homologues pour permettre les échanges IKE. La première phase IKE remplit les fonctions suivantes :

- Authentifie et protège les identités des homologues IPSec
- Négocie une stratégie d'associations de sécurité IKE correspondante entre des homologues pour protéger l'échange IKE
- Effectue un échange Diffie-Hellman authentifié avec le résultat final d'avoir des clés secrètes partagées correspondantes
- Configure un tunnel sécurisé pour négocier les paramètres de la phase 2 IKE
- Se produit dans deux modes, le mode principal et le mode agressif

La deuxième phase du protocole IKE a pour but de négocier des associations de sécurité IPSec pour configurer le tunnel IPSec. La deuxième phase IKE remplit les fonctions suivantes :

- Négocie les paramètres de SA IPSec protégés par une SA IKE existante
- Établit des associations de sécurité IPSec
- Renégocie régulièrement les SA IPSec pour garantir la sécurité
- Effectue éventuellement un échange Diffie-Hellman supplémentaire
- Un seul mode utilisé, le mode rapide

Si le protocole PFS (Perfect Forward Secrecy) est spécifié dans la stratégie IPSec, un nouvel échange DH est effectué avec chaque mode rapide, fournissant ainsi un matériel de chiffrement présentant une plus grande entropie (durée de vie du matériel clé) et donc une plus grande résistance aux attaques cryptographiques. Chaque échange DH nécessite de grandes exponentiations, ce qui augmente l'utilisation du CPU et impose un coût de performance.

- Configuration du profil IPSec (Internet Protocol Security) sur un routeur de la gamme RV34x
- Configuration des profils IPSec (mode de frappe automatique) sur les modèles RV160 et

RV260
- Configuration du mode de frappe manuelle du profil IPsec sur les routeurs RV160 et RV260

Protocole de tunnellisation point à point (PPTP)

PPTP est un protocole réseau utilisé pour créer des tunnels VPN entre des réseaux publics. Les serveurs PPTP sont également appelés serveurs VPDN (Virtual Private Dialup Network). Le protocole PPTP est parfois utilisé sur d'autres protocoles, car il est plus rapide et peut fonctionner sur des périphériques mobiles. Cependant, il est important de noter qu'il n'est pas aussi sécurisé que les autres types de VPN. Il existe plusieurs méthodes pour se connecter à des comptes de type PPTP. Cliquez sur les liens pour en savoir plus :

- Configurer un serveur PPTP (Point-to-Point Tunneling Protocol) sur le routeur de la gamme Rv34x
- Configurer le serveur PPTP (Point to Point Tunneling Protocol) sur les routeurs VPN RV320 et RV325 sous Windows

Encapsulation de routage générique

Le protocole GRE (Generic Routing Encapsulation) est un protocole de tunnellisation qui fournit une approche générique simple pour transporter des paquets d'un protocole sur un autre protocole au moyen de l'encapsulation.

GRE encapsule une charge utile, c'est-à-dire un paquet interne qui doit être livré à un réseau de destination à l'intérieur d'un paquet IP externe. Le tunnel GRE se comporte comme une liaison point à point virtuelle qui a deux points d'extrémité identifiés par la source du tunnel et l'adresse de destination du tunnel.

Les points d'extrémité du tunnel envoient des données utiles via des tunnels GRE en acheminant des paquets encapsulés via des réseaux IP intermédiaires. D'autres routeurs IP n'analysent pas la charge utile (le paquet interne) ; ils analysent uniquement le paquet IP externe lorsqu'ils le transfèrent vers le point d'extrémité du tunnel GRE. Une fois le point d'extrémité du tunnel atteint, l'encapsulation GRE est supprimée et la charge utile est transmise à la destination finale du paquet.

L’encapsulation de datagrammes dans un réseau est effectuée pour plusieurs raisons, par exemple lorsqu’un serveur source souhaite influencer la route empruntée par un paquet pour atteindre l’hôte de destination. Le serveur source est également appelé serveur d’encapsulation.

L’encapsulation IP-in-IP implique l’insertion d’un en-tête IP externe sur l’en-tête IP existant. Les adresses source et de destination dans l'en-tête IP externe pointent vers les points d'extrémité du tunnel IP-in-IP. La pile d’en-têtes IP est utilisée pour diriger le paquet sur un chemin prédéterminé vers la destination, à condition que l’administrateur réseau connaisse les adresses de bouclage des routeurs transportant le paquet.

Ce mécanisme de tunnellisation peut être utilisé pour déterminer la disponibilité et la latence de la plupart des architectures réseau. Il est à noter que le chemin complet de la source à la destination

n'a pas à être inclus dans les en-têtes, mais un segment du réseau peut être choisi pour diriger les paquets.

Protocole de tunnellisation de couche 2

L2TP ne fournit pas de mécanismes de cryptage pour le trafic qu'il tunnalise. Au lieu de cela, il s'appuie sur d'autres protocoles de sécurité, tels qu'IPSec, pour chiffrer les données.

Un tunnel L2TP est établi entre le concentrateur d'accès L2TP (LAC) et le serveur réseau L2TP (LNS). Un tunnel IPSec est également établi entre ces périphériques et tout le trafic du tunnel L2TP est chiffré à l'aide d'IPSec.

Quelques termes clés avec L2TP :

- CHAP - Challenge Handshake Authentication Protocol. Protocole d'authentification point à point (PPP).
- Concentrateur d'accès L2TP (LAC) : un LAC peut être un serveur d'accès réseau Cisco connecté au réseau téléphonique public commuté (RTPC). Le LAC n'a besoin d'implémenter que des supports pour fonctionner sur L2TP. Un LAC peut se connecter au LNS à l'aide d'un réseau local ou d'un réseau étendu, tel qu'un relais de trames public ou privé. La LAC est l'initiateur des appels entrants et le destinataire des appels sortants.
- Serveur réseau L2TP (LNS) : presque tous les routeurs Cisco connectés à un réseau local ou étendu, tel que Frame Relay public ou privé, peuvent servir de LNS. Il s'agit du côté serveur du protocole L2TP et doit fonctionner sur n'importe quelle plate-forme qui met fin aux sessions PPP. Le LNS est l'initiateur des appels sortants et le destinataire des appels entrants. La Figure 1 illustre la routine d'appel entre le LAC et le LNS.
- Virtual Private Dial Network (VPDN) : type de VPN d'accès qui utilise le protocole PPP pour fournir le service.

Pour plus d'informations sur L2TP, cliquez sur les liens suivants :

- Configuration des paramètres WAN L2TP sur le routeur RV34x
- Guide de configuration du réseau étendu : services de couche 2, Cisco IOS XE version 3S

VPN compatibles avec les routeurs VPN de la gamme Cisco RV

	RV34X	RV32X	RV160X/RV260X
IPSec (IKEv1)			
ShrewSoft	Oui	Oui	Oui
Arc Vert	Oui	Oui	Oui
Client intégré Mac	Oui	Oui	Non
iPhone/iPad	Oui	Oui	Non
Android	Oui	Oui	Oui
L2TP/IPSec	Oui (PAP)	Non	Non

PPTP	Oui (PAP)	Oui*	Oui (PAP)
Other (autre)			
AnyConnect	Oui	Non	Non
Openvpn	Non	Oui	Oui
IKEv2			
Fenêtres	Oui*	Non	Oui*
Mac	Oui	Non	Oui
iPhone	Oui	Non	Oui
Android	Oui	Non	Oui

Technologie VPN	Périphériques pris en charge	Clients pris en charge*	Détails et mises en garde
IPSec (IKEv1)	RV34X, RV32X, RV160X/RV260X	Native : Mac, iPhone, iPad, Android Autres : EasyVPN (client VPN Cisco), ShrewSoft, Greenbow	Facilité de configuration, de dépannage et d'assistance. Il est disponible sur tous les routeurs, est simple à configurer (pour la plupart), a la meilleure journalisation pour dépanner. Et inclut le plus grand nombre de périphériques. C'est pourquoi nous recommandons typiquement ShrewSoft (libre et fonctionne) et Greenbow (pas libre, mais fonctionne). Pour Windows, nous avons des clients ShrewSoft et Greenbow en option, puisque Windows n'a pas de client VPN natif IPSec pur. Pour ShrewSoft et Greenbow, c'est un peu plus compliqué, mais pas difficile. Une fois configurés la première fois, les profils client peuvent être exportés, puis importés sur d'autres clients. Pour les routeurs RV160X/RV260X, comme nous n'avons pas l'option Easy VPN, nous devons utiliser l'option Client tiers, qui ne fonctionne pas avec Mac, iPhone ou iPad. Nous pouvons configurer ShrewSoft, Greenbow et les clients Android pour se connecter, cependant. Pour les clients Mac, iPhone et iPad, je recommande IKEv2 (voir ci-dessous).
AnyConnect	RV34X	Windows, Mac, iPhone, iPad, Android	Certains clients demandent une solution Cisco complète, et c'est tout. Il est simple à configurer, il comporte une journalisation, mais

			il peut être difficile de comprendre les journaux. Nécessite une licence client pour un coût élevé. Il s'agit d'une solution Cisco complète mise à jour. Le dépannage n'est pas aussi simple qu'IPSec, mais il est préférable aux autres options VPN. C'est ce que je recommanderai aux clients qui ont besoin d'utiliser le client VPN intégré dans Windows. Voici deux avertissements à ce sujet : 1. Nous ne prenons en charge l'authentification PAP que lorsque vous utilisez l'authentification locale. Nous devons accéder à chaque client et sélectionner le chiffrement facultatif ou non, désactiver les options MS-CHAP et activer PAP. Cela signifie que le nom d'utilisateur/mot de passe est envoyé en clair. Ce n'est pas énorme, car tout est chiffré avec IPSec et doit être configuré sur chaque client. Sous Windows, cette option est configurable, mais pas sur les appareils Mac, iPhone, iPad ou Android. Elle ne peut donc être utilisée que par les clients Windows, à moins qu'ils ne disposent d'un serveur d'authentification externe tel que Radius ou LDAP. 2. Si le routeur se trouve derrière un périphérique NAT, la connexion échouera sur les ordinateurs Windows. La solution de contournement consiste à créer une clé de registre sur chaque client pour permettre la NAT sur le client et le routeur.
L2TP/IPSec	RV34X	Native : Windows	
IPSec (IKEv2)	RV34X, RV160X/RV260X	Native : Windows, Mac, iPhone, iPad, Android	Le client natif Windows pour IKEv2 nécessite une authentification de certificat, ce qui nécessite une infrastructure PKI car le routeur et tous les clients doivent avoir des certificats de la même autorité de certification (ou d'une autre autorité de certification approuvée). Pour ceux qui veulent utiliser IKEv2, nous configurons cela pour leurs appareils Mac, iPhone, iPad et Android et nous configurons

			généralement IKEv1 pour leurs machines Windows (ShrewSoft, Greenbow ou L2TP/IPSec).
VPN ouvert	RV32X, RV160X/RV260X	Open VPN est le client	Plus difficile à configurer, à dépanner et à prendre en charge. Pris en charge sur les modèles RV160X/RV260X et RV320. La configuration est plus complexe qu'IPSec ou AnyConnect, en particulier s'ils utilisent des certificats, ce qui est le cas de la plupart. Le dépannage est plus difficile, car nous ne disposons pas de journaux utiles sur le routeur et nous nous appuyons sur les journaux du client. En outre, les mises à jour de version du client OpenVPN ont modifié sans avertissement les certificats qu'ils ont acceptés. De plus, nous avons constaté que cela ne fonctionnait pas sur les Chromebooks et que nous devions opter pour une solution IPSec.

* Nous testons autant de combinaisons que possible. S'il existe une combinaison matérielle/logicielle spécifique, veuillez nous contacter ici. Sinon, reportez-vous au guide de configuration associé par périphérique pour connaître la version la plus récente testée.

Certificats

Avez-vous déjà visité un site Web et avez-vous été averti qu'il n'était pas sécurisé ? Cela ne vous donne pas l'assurance que vos informations privées sont sécurisées, et ce n'est pas le cas ! Si un site est sécurisé, une icône de verrou fermé s'affiche avant le nom du site. C'est un symbole que le site a été vérifié sûr. Vous voulez être sûr de voir cette icône de verrou fermée. Il en va de même pour votre VPN.

Lorsque vous configurez un VPN, vous devez obtenir un certificat auprès d'une autorité de certification (CA). Les certificats sont achetés sur des sites tiers et utilisés pour l'authentification. C'est un moyen officiel de prouver que votre site est sécurisé. Essentiellement, l'autorité de certification est une source fiable qui vérifie que vous êtes une entreprise légitime et que vous pouvez être fiable. Pour un VPN, vous avez seulement besoin d'un certificat de niveau inférieur à un coût minimal. Vous êtes retiré par l'autorité de certification et une fois qu'elle a vérifié vos informations, elle vous délivre le certificat. Ce certificat peut être téléchargé en tant que fichier sur votre ordinateur. Vous pouvez ensuite accéder à votre routeur (ou à votre serveur VPN) et l'y télécharger.

L'autorité de certification utilise l'infrastructure à clé publique (PKI) lors de l'émission de certificats numériques, qui utilise le chiffrement à clé publique ou à clé privée pour assurer la sécurité. Les

autorités de certification sont chargées de gérer les demandes de certificats et d'émettre des certificats numériques. Parmi les autorités de certification tierces, citons IdenTrust, Comodo, GoDaddy, GlobalSign, GeoTrust et Verisign.

Il est important que toutes les passerelles d'un VPN utilisent le même algorithme, sinon elles ne pourront pas communiquer. Pour simplifier les choses, il est recommandé que tous les certificats soient achetés auprès du même tiers de confiance. Cela facilite la gestion de plusieurs certificats, car ils doivent être renouvelés manuellement.

Remarque : les clients n'ont généralement pas besoin d'un certificat pour utiliser un VPN ; il s'agit simplement d'une vérification via le routeur. Une exception à cela est OpenVPN, qui nécessite un certificat client.

Certaines petites entreprises choisissent d'utiliser un mot de passe ou une clé prépartagée au lieu d'un certificat pour plus de simplicité. Cette option est moins sécurisée, mais peut être configurée gratuitement.

Vous trouverez plus d'informations sur les certificats dans les liens ci-dessous :

- Certificat (Import/Export/Generate CSR) sur les routeurs des gammes RV160 et RV260
- Remplacez le certificat auto-signé par défaut par un certificat SSL tiers sur le routeur de la gamme RV34x

VPN de site à site sur un routeur

Pour les routeurs local et distant, il est important de s'assurer que la clé prépartagée (PSK)/le mot de passe/certificat utilisé pour la connexion VPN et les paramètres de sécurité correspondent tous. Si un ou plusieurs routeurs utilisent la traduction d'adresses de réseau (NAT), que la plupart des routeurs de la gamme Cisco RV utilisent, vous devrez appliquer des exemptions de pare-feu pour la connexion VPN sur les routeurs local et distant.

Consultez ces articles de site à site pour plus d'informations :

- Configuration d'un VPN site à site sur le RV34x
- Configurer un VPN site à site sur un routeur RV340 ou RV345
- Cisco TechTalk : configuration d'un VPN site à site sur les routeurs de la gamme RV340 (vidéo)
- Configuration d'un VPN site à site sur un routeur RV160 et RV260 (paramètres de base)
- VPN de site à site sur les routeurs RV160 et RV260 (paramètres avancés et basculement)

VPN client-à-site sur un routeur

Avant de pouvoir configurer un VPN côté client, un administrateur doit le configurer sur le routeur.

Cliquez pour afficher les articles suivants sur la configuration des routeurs :

- Assistant de configuration VPN sur les routeurs RV160 et RV260
- Configuration du client VPN logiciel Shrew avec les routeurs RV160 et RV260
- Cisco Tech Talk : Configuration de Shrew Soft VPN sur les modèles RV160 et RV260 (vidéo)
- Configuration et utilisation du client VPN IPsec GreenBow pour la connexion aux routeurs RV160 et RV260

Créer un profil de client à site

Dans une connexion VPN client-à-site, les clients d'Internet peuvent se connecter au serveur pour accéder au réseau d'entreprise ou au réseau local derrière le serveur, tout en préservant la sécurité du réseau et de ses ressources. Cette fonctionnalité est très utile car elle crée un nouveau tunnel VPN qui permettrait aux télétravailleurs et aux voyageurs d'affaires d'accéder à votre réseau à l'aide d'un logiciel client VPN sans compromettre la confidentialité et la sécurité. Les articles suivants sont spécifiques aux routeurs de la gamme RV34x :

- Configuration de la connexion de réseau privé virtuel (VPN) client-site sur le routeur de la gamme RV34x
- Configurer la connectivité du réseau privé virtuel (VPN, pour Private Virtual Network) d'AnyConnect sur le routeur de la gamme RV34x

Le VPN client-à-site ne fonctionnera pas si le transfert de port est défini pour le trafic source tout et le trafic de destination tout.

Groupes d'utilisateurs

Les groupes d'utilisateurs sont créés sur le routeur pour un ensemble d'utilisateurs qui partagent le même ensemble de services. Ces groupes d'utilisateurs incluent des options pour le groupe, comme une liste d'autorisations sur la façon dont ils peuvent accéder au VPN. Selon le périphérique, PPTP, VPN IPSec site à site et VPN IPSec client à site peuvent être autorisés. Par exemple, le RV260 dispose d'options qui incluent OpenVPN, mais L2TP n'est pas pris en charge. La gamme RV340 est équipée d'AnyConnect pour un VPN SSL, ainsi que d'un portail captif ou d'un VPN EZ.

Ces paramètres permettent aux administrateurs de contrôler et de filtrer de sorte que seuls les utilisateurs autorisés puissent accéder au réseau. Shrew Soft et TheGreenBow sont deux des clients VPN les plus courants disponibles en téléchargement. Ils doivent être configurés en fonction des paramètres VPN du routeur pour pouvoir établir un tunnel VPN avec succès. L'article suivant traite spécifiquement de la création d'un groupe d'utilisateurs :

- Créer un groupe d'utilisateurs pour la configuration VPN sur le routeur RV34x

Lorsque vous configurez des groupes d'utilisateurs pour un VPN, veillez à conserver le compte d'administrateur par défaut dans le groupe d'administrateurs et à créer un nouveau compte d'utilisateur et un nouveau groupe d'utilisateurs pour le VPN. Si vous déplacez votre compte d'administrateur vers un autre groupe, vous vous empêcherez de vous connecter au routeur. Par conséquent, vous devez effectuer une réinitialisation d'usine et reconfigurer pour ce routeur, en

laissant le compte d'administrateur par défaut dans le groupe d'administrateurs.

Comptes utilisateurs

Les comptes d'utilisateurs sont créés sur le routeur afin de permettre l'authentification des utilisateurs locaux à l'aide de la base de données locale pour divers services tels que PPTP, le client VPN, la connexion à l'interface graphique utilisateur (GUI) Web et le réseau privé virtuel Secure Sockets Layer (SSLVPN). Les administrateurs peuvent ainsi contrôler et filtrer les utilisateurs autorisés uniquement pour accéder au réseau. L'article suivant traite spécifiquement de la création d'un compte d'utilisateur :

- Créer un compte d'utilisateur pour la configuration du client VPN sur le routeur RV34x

Client à site sur le site du client

Dans une connexion VPN client-à-site, les clients d'Internet peuvent se connecter au serveur pour accéder au réseau d'entreprise ou au réseau local derrière le serveur, tout en préservant la sécurité du réseau et de ses ressources. Cette fonctionnalité est très utile car elle crée un nouveau tunnel VPN qui permet aux télétravailleurs et aux voyageurs d'affaires d'accéder à votre réseau à l'aide d'un logiciel client VPN sans compromettre la confidentialité et la sécurité. Le VPN est configuré pour chiffrer et déchiffrer les données lors de leur envoi et de leur réception.

L'application AnyConnect fonctionne avec le VPN SSL et est utilisée spécifiquement avec les routeurs RV34x. Il n'est pas disponible avec les autres routeurs de la gamme RV. À partir de la version 1.0.3.15, une licence de routeur n'est plus nécessaire, mais des licences doivent être achetées pour le côté client du VPN. Pour plus d'informations sur le client Cisco AnyConnect Secure Mobility, cliquez ici. Pour les instructions d'installation, sélectionnez l'un des articles suivants :

- Installer Cisco AnyConnect Secure Mobility Client sur un ordinateur Macintosh
- Installer Cisco AnyConnect Secure Mobility Client sur un ordinateur Windows

Certaines applications tierces peuvent être utilisées pour le VPN client-à-site avec tous les routeurs de la gamme RV. Comme indiqué précédemment, Cisco ne prend pas en charge ces applications ; ces informations sont fournies à titre indicatif.

Le client VPN GreenBow est une application cliente VPN tierce qui permet à un périphérique hôte de configurer une connexion sécurisée pour le tunnel IPsec client-à-site ou SSL. Il s'agit d'une application payante qui inclut une assistance.

- Configuration et utilisation du client VPN IPsec GreenBow pour la connexion aux routeurs RV160 et RV260

OpenVPN est une application libre et open source qui peut être configurée et utilisée pour un VPN SSL. Il utilise une connexion client-serveur pour assurer des communications sécurisées entre un serveur et un emplacement client distant sur Internet.

- OpenVPN sur les routeurs RV160 et RV260

Shrew Soft est une application libre et open source qui peut être configurée et utilisée pour un VPN IPsec. Il utilise une connexion client-serveur pour assurer des communications sécurisées entre un serveur et un emplacement client distant sur Internet.

- Configuration du client VPN logiciel Shrew avec les routeurs RV160 et RV260

Easy VPN était couramment utilisé sur les routeurs RV32x. Voici quelques informations à titre de référence :

- Configuration d'un client facile pour un réseau privé virtuel (VPN) de passerelle sur les routeurs VPN RV320 et RV325
- FAQ – Cisco Easy VPN
- Easy VPN sur les routeurs basés sur le logiciel Cisco IOS

Assistant de configuration

Les derniers routeurs de la gamme Cisco RV sont livrés avec un assistant de configuration VPN qui vous guide tout au long des étapes de configuration. L'Assistant de configuration VPN vous permet de configurer les connexions VPN de base entre réseaux locaux et d'accès à distance et d'attribuer des clés pré-partagées ou des certificats numériques pour l'authentification. Consultez ces articles pour plus d'informations :

- Assistant de configuration VPN sur les routeurs RV160 et RV260
- Configuration de la connexion VPN (Virtual Private Network) à l'aide de l'Assistant de configuration sur le routeur de la gamme RV34x

Conclusion

Cet article vous a permis de mieux comprendre les réseaux privés virtuels et vous a donné des conseils pour vous aider. Vous devez maintenant être prêt à configurer le vôtre ! Prenez le temps de consulter les liens et de choisir la meilleure façon de configurer un VPN sur votre routeur Cisco série RV.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.