Vue d'ensemble et pratiques recommandées des affaires VPN de Cisco

Objectif

L'objectif de ce document est de donner une vue d'ensemble des pratiques recommandées du réseau privé virtuel (VPN) à n'importe qui nouveau à l'entreprise de Cisco.

Table des matières

Introduction

Il semble tellement il y a bien longtemps que le seul endroit que vous pourriez travailler était au bureau. Vous pouvez se souvenir, soutenir pendant le jour, devant se diriger dans le bureau la fin de semaine pour obtenir une question de travail réglée. Il n'y avait aucune autre manière d'obtenir des données des ressources en société à moins que vous ayez été physiquement dans votre bureau. Ces jours sont terminés. En périodes d'aujourd'hui, vous pouvez être sur l'aller ; entreprise de conduite d'une maison, d'un bureau différent, d'un café, ou même d'un pays différent. Le du côté incliné est que les pirates informatiques regardent toujours pour saisir vos données sensibles. Juste utilisant l'Internet public n'est pas sûr. Que pouvez-vous faire pour obtenir la flexibilité aussi bien que la Sécurité ? Installez un VPN !

Une connexion VPN permet à des utilisateurs pour accéder à, envoyer, et recevoir des données à et d'un réseau privé au moyen d'aller par un public ou du réseau partagé tel que l'Internet mais au moyen de assurer toujours une connexion sécurisée à une infrastructure réseau sous-jacente pour protéger le réseau privé et ses ressources.

Un tunnel VPN établit un réseau privé qui peut envoyer des données sécurisé utilisant le cryptage pour encoder les données, et l'authentification pour assurer l'identité du client. Les entreprises utilisent souvent une connexion VPN puisqu'il est utile et nécessaire de permettre à leurs employés d'avoir accès à leur réseau privé même si ils sont en dehors du bureau.

Normalement, le site à site VPN connectent des tout le réseau entre eux. Ils étendent un réseau et permettent à des ressources informatiques d'un emplacement pour être disponibles à d'autres emplacements. Par l'utilisation d'un routeur capable VPN, une société peut connecter les sites réparés par multiple au-dessus d'un réseau public tel que l'Internet.

L'installation de client-à-site pour un VPN permet à un serveur distant, ou au client, pour agir comme si ils se sont trouvés sur le même réseau local. Une connexion VPN peut être installée entre le routeur et un point final après que le routeur ait été configuré pour la connexion Internet. Le client vpn dépend des configurations du routeur VPN en plus de la condition requise des configurations appariées afin d'établir une connexion. En outre, certaines des applications de client vpn sont particularité de plate-forme, elles dépendent de la version du système d'exploitation (de SYSTÈME D'EXPLOITATION) aussi bien. Les configurations doivent être exactement identiques ou elles ne peuvent pas communiquer.

Un VPN peut être installé avec suivre l'un des :

- Secure Socket Layer (SSL)
- IPSec (IPSec)
- Perçage d'un tunnel point par point Protocol (PPTP) - pas aussi sécurisé que le SSL ou l'IPSec
- Encapsulation de routage générique (GRE)
- Layer 2 Tunneling Protocol (L2TP)

Si vous n'avez jamais installé un VPN avant, vous recevrez beaucoup de nouvelles informations dans tout cet article. Ce n'est pas un guide pas à pas, mais plus d'une vue d'ensemble pour la référence. Par conséquent, il serait salutaire de lire cet article en sa totalité avant de passer et tenter d'installer un VPN sur votre réseau. Des liens pour les étapes spécifiques sont fournis dans tout cet article.

La tierce partie, des Produits de non-Cisco, y compris TheGreenBow, OpenVPN, musaraigne molle, et EZ VPN ne sont pas prises en charge par Cisco. Ils sont inclus strictement pour des conseils. Si vous avez besoin du support sur ces derniers au delà de l'article, vous devriez contacter la tierce partie pour le support.

Avantages d'utiliser une connexion VPN

- Utilisant une connexion VPN aide à protéger des données et des ressources confidentielles de réseau.
- Il fournit la commodité et l'accessibilité pour des travailleurs distants ou des employés entreprise puisqu'elles pourront accéder à facilement les ressources en bureau central sans devoir être physiquement présentes mais, mettent à jour la Sécurité du réseau privé et de ses ressources.
- La transmission utilisant une connexion VPN fournit un niveau supérieur de Sécurité comparé à d'autres méthodes de transmission distante. Un algorithme de chiffrement avancé fait ce possible, protégeant le réseau privé contre l'accès non autorisé.
- Les situations géographiques réelles des utilisateurs sont protégées et pas exposées au public ou aux réseaux partagés comme l'Internet.
- Un VPN permet de nouveaux utilisateurs ou un groupe d'utilisateurs à ajouter sans besoin de composants supplémentaires ou de configuration compliquée.

Risques d'utiliser une connexion VPN

- Il peut y avoir des risques de sécurité dus à la mauvaise configuration. Puisque la conception et réalisation d'un VPN peut être compliquée, il est nécessaire de confier à la tâche de configurer la connexion à un professionnel bien informé et expérimenté afin de s'assurer que

la Sécurité du réseau privé ne serait pas compromise.
- Il peut être moins fiable. Puisqu'une connexion VPN exige une connexion Internet, il est important d'avoir un fournisseur avec une réputation avérée et testée fournir l'excellent service Internet et garantir minimal à aucun temps d'arrêt.
- Si une situation se produit où il y a un besoin d'ajouter la nouvelle infrastructure ou un nouvel ensemble de configurations, les problèmes techniques peuvent surgir en raison de l'incompatibilité particulièrement si elle implique différents Produits ou des constructeurs autres que ceux que vous utilisez déjà.
- Les vitesses de connexion lentes peuvent se produire. Si vous utilisez une connexion ISP qui fournit le service libre VPN, il peut prévoir que votre connexion serait également lente puisque ces fournisseurs ne donnent pas la priorité à des vitesses de connexion. Il est important de noter que le débit du VPN dépend des capacités matérielles du routeur.

Pour plus d'informations sur la façon dont les VPN fonctionnent, a cliquez ici.

Conseils aux utiliser en configurant un VPN

1. Utilisez un différent IP de sous-réseau de RÉSEAU LOCAL aux deux extrémités tout en configurant le VPN entre différents sites. Par exemple, si le site que vous connectez à utilise un système d'adressage 192.168.x.x, vous voudrait utiliser un 10.x.x.x ou un 172.16.x.x - le sous-réseau 172.31.x.x. Une autre option serait d'avoir des masques de différent sous-réseau. Quand vous changez votre adresse IP du routeur, les périphériques sur le protocole DHCP (DHCP) prendraient automatiquement une adresse IP dans ce sous-réseau.
2. Utilisez l'IP statique de public sur l'interface WAN du routeur pour la connectivité VPN stable.
3. Soyez sûr que le niveau de cryptage et d'authentification sélectionné est identique que le routeur vous souhaitent établir un tunnel VPN à pour le VPN.
4. Soyez sûr que les PSK et la vie principale écrits sont identiques que le routeur distant. Un PSK peut être celui qui vous vouliez qu'il soit, il juste doit apparier au site et avec le client quand ils installent en tant que client sur leur ordinateur. Selon le périphérique, il peut y avoir des symboles interdits que vous ne pouvez pas utiliser. La vie principale est combien de fois les évolutions des systèmes la clé. Un certificat est préféré puisqu'il est considéré plus sécurisés.
5. Pour la plupart des VPN, les clients n'ont pas besoin d'un certificat pour utiliser un VPN, il est juste pour la vérification par le routeur. Par exemple, OpenVPN a besoin des Certificats de client et de site.
6. Placez votre vie SA dans la phase I plus longue que votre vie SA de la phase II. Si vous rendez votre phase I plus courte que la phase II, alors vous devrez renégocier le tunnel dans les deux sens fréquemment par opposition au tunnel de données. Des données percent un tunnel les besoins plus de Sécurité, ainsi il vaut mieux d'avoir la vie dans la phase II à être plus court que la phase I.
7. Changez tous les mots de passe à quelque chose plus complexe.

Types de VPN

Secure Sockets Layer (SSL)

Les Routeurs de gamme RV34x d'affaires de Cisco prennent en charge un VPN SSL, utilisant

AnyConnect. Les RV160 et les RV260 ont l'option d'utiliser OpenVPN, qui est un autre VPN SSL. Le serveur de VPN SSL permet à des utilisateurs distants pour établir un tunnel VPN sécurisé utilisant un navigateur Web. Cette caractéristique permet l'accès facile à un large éventail de ressources web et les applications Web-activées utilisant le Protocole HTTP (Hypertext Transfer Protocol) indigène au-dessus de l'hypertexte Transfer Protocol SSL sécurisent la prise en charge du navigateur (HTTPS).

Le VPN SSL permet à des utilisateurs pour accéder à distance les réseaux restreints, utilisant une voie sécurisée et authentifiée en chiffrant le trafic réseau.

Il y a deux options d'installer l'accès dans le SSL :

1. Certificat Auto-signé : Un certificat qui est signé par son propre créateur. Ceci n'est pas recommandé et devrait seulement être utilisé dans un environnement de test.
2. Certificat signé CA : C'est beaucoup plus sécurisé et fortement recommandé. Pour des frais, une tierce partie valide que le réseau est légitime et crée un certificat de CA qui est alors reliée au site. Pour plus d'informations sur des Certificats CA, contrôle la section de Certificats de cet article.

Il y a des liens aux articles sur AnyConnect dans ce document. Pour une vue d'ensemble d'AnyConnect, a cliquez ici.

Profil IPSec

L'Easy VPN (EZVPN), le TheGreenBow, et le doux de musaraigne sont IPSec (IPSec) VPN. IPSec VPN fournissent sécurisent des tunnels entre deux pairs ou d'un client-à-site. Des paquets qui sont considérés sensibles devraient être envoyés par des ces sécurisent des tunnels. Des paramètres comprenant l'algorithme de hachage, l'algorithme de chiffrement, la vie principale, et le mode doivent être utilisés pour protéger ces paquets sensibles devraient être définis en spécifiant les caractéristiques de ces tunnels. Puis, quand le pair d'IPsec voit un paquet si sensible, il a installé l'approprié sécurisent le tunnel et envoient le paquet par ce tunnel au pair distant.

Quand IPsec est mis en application dans un Pare-feu ou un routeur, il fournit la forte sécurité qui peut être appliquée à tout le trafic croisant le périmètre. Le trafic dans une société ou un groupe de travail n'encourt pas le temps système du traitement lié à la sécurité.

Afin des deux extrémités d'un tunnel VPN avec succès à chiffrer et être établi, ils chacun des deux doivent convenir sur les méthodes de cryptage, de déchiffrement, et d'authentification. Le profil IPSec est la configuration centrale dans IPsec qui définit les algorithmes tels que le cryptage, l'authentification, et le groupe de Protocole DH (Diffie-Hellman) pour la phase I et II négociation en mode automatique aussi bien que mode de introduction manuel.

Les importants composants d'IPsec incluent le Phase 1 et le Phase 2 d'Échange de clés Internet (IKE).

Le but de base de la phase une d'IKE est d'authentifier les pairs d'IPSec et d'installer un canal de sécuriser entre les pairs pour activer des échanges d'IKE. La phase une d'IKE remplit les fonctions suivantes :

- Authentifie et protège les identités des pairs d'IPSec
- Négocie une stratégie assortie des associations de sécurité d'IKE (SA) entre les pairs pour

protéger l'échange d'IKE
- Exécute un échange authentifié de Diffie-Hellman avec le résultat final de avoir des clés secrètes partagées assorties
- Installent un tunnel sécurisé pour négocier des paramètres de la phase deux d'IKE
- Se produit en deux modes, mode principal et mode agressif

Le but de la phase deux d'IKE est de négocier IPSec SAS pour installer le tunnel d'IPSec. La phase deux d'IKE remplit les fonctions suivantes :

- Négocie des paramètres d'IPSec SA protégés par IKE existant SA
- Établit des associations de sécurité d'IPSec
- Renégocie périodiquement IPSec SAS pour assurer la Sécurité
- Exécute sur option un échange supplémentaire de Diffie-Hellman
- Seulement un mode utilisé, mode rapide

Si le perfect forward secrecy (PFS) est spécifié dans la stratégie IPSec, un nouvel échange CAD est exécuté avec chaque mode rapide, fournissant le matériel de base qui a une plus grande entropie (vie d'élément de clé) et une résistance de ce fait plus grande aux attaques cryptographiques. Chaque échange CAD exige de grandes exponentiations, augmentant de ce fait utiliser-et CPU exigeant un coût de représentation.

- Configuration de profil d'IPSec (IPSec) sur un routeur de gamme RV34x
- Profils de configuration d'IPSec (mode de introduction automatique) sur le RV160 et le RV260
- Mode de introduction manuel de profil de configuration d'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 les réseaux publics. Des serveurs PPTP sont également connus comme serveurs de Réseau privé virtuel à accès commuté (VPDN). PPTP est parfois utilisé au-dessus d'autres protocoles parce qu'il est plus rapide et a la capacité de travailler aux périphériques mobiles. Cependant, il est important de noter qu'il n'est pas aussi sécurisé que d'autres types de VPN. Il y a de plusieurs méthodes à connecter aux comptes de type PPTP. Cliquez sur les liens pour apprendre plus :

- Configurez un serveur de Protocole PPTP (Point-to-Point Tunneling Protocol) sur le routeur de gamme Rv34x
- Configurez le serveur de perçage d'un tunnel point par point de Protocol (PPTP) sur la gamme du routeur VPN RV320 et RV325 sur Windows

Encapsulation de routage générique

L'Encapsulation de routage générique (GRE) est un protocole de Tunnellisation qui fournit une approche générique simple pour transporter des paquets d'un protocole au-dessus d'un autre protocole au moyen d'encapsulation.

GRE encapsule une charge utile, c.-à-d., 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 en tant que lien point par point virtuel qui a deux points finaux identifiés par la source du tunnel et l'adresse de destination de tunnel.

Les périphériques du tunnel envoient des charges utiles par des tunnels GRE en conduisant des paquets encapsulés par les réseaux IP intervenants. D'autres routeurs IP le long de la route

n'analysent pas la charge utile (le paquet interne) ; ils analysent seulement le paquet IP externe comme ils l'expédient vers le périphérique du tunnel GRE. Lors d'atteindre le périphérique du tunnel, l'encapsulation GRE est enlevée, et la charge utile est expédiée à la destination finale du paquet.

L'encapsulation des datagrammes dans un réseau est faite pour de plusieurs raisons, comme quand un serveur source veut influencer l'artère qu'un paquet prend pour atteindre la destination host. Le serveur source est également connu en tant que serveur d'encapsulation.

L'encapsulation d'IP-in-IP comporte la mise en place d'une en-tête IP externe au-dessus de l'en-tête IP existante. L'adresse source et de destination au point externe d'en-tête IP aux points d'extrémité du tunnel d'IP-in-IP. La pile d'en-têtes IP est utilisée pour diriger le paquet au-dessus d'un chemin prédéterminé vers la destination, si l'administrateur réseau connaît les adresses de bouclage des Routeurs transportant le paquet.

Ce mécanisme de Tunnellisation peut être utilisé pour déterminer la Disponibilité et la latence pour la plupart des architectures de réseau. Il doit être noté que le chemin entier de la source à la destination ne doive pas être inclus dans les en-têtes, mais un segment du réseau peut être choisi pour diriger les paquets.

Layer 2 Tunneling Protocol

L2TP ne fournit pas des mécanismes de chiffrement pour le trafic qu'il perce un tunnel. Au lieu de cela il se fonde sur d'autres protocoles de Sécurité, tels qu'IPSec, pour chiffrer les données.

Un tunnel L2TP est établi entre le concentrateur L2TP Access (LAC) et le serveur de réseau L2TP (LNS). Un tunnel d'IPSec est également établi entre ces périphériques et tout le trafic de tunnel L2TP est chiffré utilisant IPSec.

Quelques termes principaux avec L2TP :

- **CHAP -** Authentification Protocol à échanges confirmés. Une authentification Protocol point par point (PPP).
- **Concentrateur L2TP Access (LAC) -** UN LAC peut être un serveur d'accès à distance de Cisco connecté au réseau téléphonique public commuté (PSTN). Les medias de mise en place du besoin de LAC seulement pour l'exécution au-dessus de L2TP. Un LAC peut se connecter au LNS utilisant un réseau de réseau local ou d'étendu tel que le public ou le relais de trame privé. Le LAC est le demandeur des appels entrant et le récepteur des appels sortants.
- **Serveur de réseau L2TP (LNS) -** Presque n'importe quel routeur connecté de Cisco à un réseau de réseau local ou d'étendu, tel que le public ou le relais de trame privé, peut agir en tant que LNS. C'est le côté serveur du protocole L2TP et doit traiter n'importe quelle plate-forme qui termine des sessions PPP. Le LNS est le demandeur des appels sortants et le récepteur des appels entrant. La figure 1 dépeint la routine d'appel entre le LAC et le LNS.
- **Réseau commuté privé virtuel (VPDN) - un** type d'accès VPN qui emploie le PPP pour fournir le service.

Si vous voudriez que plus d'informations sur L2TP cliquent sur en fonction les liens suivants :

- Configurez les configurations BLÊMES L2TP sur le routeur RV34x
- Guide de configuration de réseau d'étendu : Services de la couche 2, release 3S de Cisco

IOS XE

VPN qui sont compatibles avec des routeurs VPN d'affaires de Cisco

	RV34X	RV32X	RV160X/RV260X
IPSec (IKEv1)			
ShrewSoft	Oui	Oui	Oui
Greenbow	Oui	Oui	Oui
Client de fonction intégrée de MAC	Oui	Oui	Non
iPhone/iPad	Oui	Oui	Non
Android	Oui	Oui	Oui

Technologie VPN	Périphériques pris en charge	Clients Supported*	Détails et mises en garde
IPSec (IKEv1)	RV34X, RV32X, RV160X/RV260X	Indigène : MAC, iPhone, iPad, Android Autre : EasyVPN (Client VPN Cisco), ShrewSoft, Greenbow	Le plus facile à installer, dépannez et le prenez en charge. Il est disponible sur tous les Routeurs, est simple d'installer (pour la plupart), a meilleur se connecter à dépanner. Et inclut les la plupart des périphériques. C'est pourquoi nous recommandons typiquement ShrewSoft (libérez et des travaux) et Greenbow (non libre, mais des travaux). Pour Windows, nous avons des clients de ShrewSoft et de Greenbow comme options, puisque Windows n'a pas un client vpn pur d'indigène d'IPSec. Pour ShrewSoft et Greenbow, il est un peu plus impliqué, mais non difficile. Installez une fois la première fois, des profils de client peuvent être exportés et puis importés sur d'autres clients. Pour des Routeurs RV160X/RV260X, puisque nous n'avons pas l'option d'Easy VPN, nous devons utiliser l'option Client de tiers, qui ne fonctionne pas avec le MAC, l'iPhone, ou l'iPad. Nous pouvons installer des clients de ShrewSoft, de Greeenbow, et d'Android pour nous connecter, cependant. Pour le MAC, l'iPhone, et les clients d'iPad, je recommande IKEv2 (voir ci-dessous).
AnyConnect	RV34X	Windows, MAC, iPhone, iPad, Android	Quelques clients demandent une pleine solution de Cisco et c'est lui. Il est simple d'installer, a se connecter, mais peut être provocant pour comprendre les logs. Exige le coût incuring de condition d'autorisation de client. C'est une pleine solution de Cisco et est mis à jour. Le dépannage n'est pas aussi facile qu'IPSec, mais mieux que les autres options VPN. Est ce ce que je recommanderai pour les clients qui doivent utiliser le client vpn intégré dans Windows. Deux mises en garde avec ceci sont :
L2TP/IPSec	RV34X	Indigène : Fenêtres	1. Nous prenons en charge seulement l'authentification PAP en utilisant l'authentification locale. Nous devons entrer dans chaque client et facultatif choisi ou aucun cryptage, désactiver des options MS-CHAP, et activer le PAP. Ceci signifie que le nom

			d'utilisateur/mot de passe sont envoyés en clair. Ce n'est pas une affaire énorme puisque tout est chiffré avec IPSec, et doit installer sur chaque client. Sur Windows, c'est configurable, mais pas sur le MAC, l'iPhone, l'iPad, ou les périphériques d'Android, tellement vraiment peuvent seulement être utilisés par des clients Windows à moins qu'ils aient un serveur d'authentification externe comme Radius ou le LDAP. 2. Si le routeur est derrière un périphérique NAT, la connexion échouera sur des ordinateurs Windows. Le contournement est de créer une clé de registre sur chaque client pour permettre NAT sur le client et le routeur.
IPSec (IKEv2)	RV34X, RV160X/RV260X	Indigène : Windows, MAC, iPhone, iPad, Android	Le client indigène de Windows pour IKEv2 a besoin de l'authentification de certificat, qui exige une infrastructure de PKI puisque le routeur et tous besoin des clients d'avoir des Certificats du même CA (ou des autres CA de confiance). Pour ceux qui veulent utiliser IKEv2, nous avons établi cela pour leur MAC, iPhone, iPad, et les périphériques et nous d'Android avons habituellement installé IKEv1 pour leurs ordinateurs Windows (ShrewSoft, Greenbow, ou L2TP/IPSec). Installer plus dur, difficile à dépanner et prendre en charge. Pris en charge sur RV160X/RV260X et RV320.
Ouvrez le VPN	RV32X, RV160X/RV260X	Le VPN ouvert est le client	L'établissement est plus complexe qu'IPSec ou AnyConnect, particulièrement s'ils utilisent les Certificats, que les la plupart font. Le dépannage est plus dur puisque nous n'avons aucun utile ouvre une session le routeur et compte sur les logs de client. En outre, les mises à jour de version du client d'OpenVPN ont sans avertissement changé que les Certificats ils ont reçu. En outre, nous fondons ceci ne travaille pas à Chromebooks et a dû aller à une solution d'IPSec.

* Nous testons autant de combinaisons comme nous pouvons, s'il veuillez y a une combinaison spécifique de matériel/logiciel atteignez ici. Autrement, voyez le guide de configuration relatif par

le périphérique pour la plupart de version récente testée.

Certificats

Avez-vous jamais visité un site Web et avez-vous été donné un avertissement qu'il n'est pas sécurisé ? Il ne vous remplit pas avec confiance que vos informations personnelles sont sécurisées, et elles ne sont pas ! Si un site est sécurisé vous verrez une icône fermée de verrouillage avant le nom du site. C'est un symbole que le site a été coffre-fort vérifié. Vous voulez être sûr de voir que l'icône de verrouillage s'est fermée. Le même est vrai pour votre VPN.

Quand vous installez un VPN, vous devriez obtenir un certificat d'un Autorité de certification (CA). Des Certificats sont achetés des sites tiers et utilisés pour l'authentification. C'est une manière officielle de montrer que votre site est sécurisé. Essentiellement, le CA est une source sûre qui vérifie que vous êtes une entreprise légitime et pouvez êtes de confiance. Pour un VPN vous avez besoin seulement d'un certificat plus élémentaire à un coût minimal. Vous obtenez vérifié par le CA, et une fois qu'ils vérifient vos informations, ils fourniront le certificat à vous. Ce certificat peut être téléchargé comme fichier sur votre ordinateur. Vous pouvez alors entrer dans votre routeur (ou serveur VPN) et le télécharger là.

Le CA utilise l'Infrastructure à clés publiques (PKI) en délivrant des Certificats numériques, qui emploie la clé publique ou le chiffrement à clé privé pour assurer la Sécurité. Les CAs sont responsables de gérer des demandes de certificat et de délivrer des Certificats numériques. Quelque la tierce partie CAs incluent IdenTrust, Comodo, GoDaddy, GlobalSign, GeoTrust, et Verisign.

Il est important que toutes les passerelles dans un VPN utilisent le même algorithme, autrement elles ne pourront pas communiquer. Pour maintenir des choses simples, l'il est recommandé que tous les Certificats sont achetés de la même chose tierce partie de confiance. Ceci maintient de plusieurs Certificats plus faciles à gérer pendant qu'ils doivent être manuellement renouvelés.

Remarque: Les clients habituellement n'ont pas besoin d'un certificat pour utiliser un VPN ; il est juste pour la vérification par le routeur. Une exception à ceci est OpenVPN, qui exige un certificat client.

Quelques petites entreprises choisissent d'utiliser un mot de passe ou une clé pré-partagée au lieu d'un certificat pour la simplicité. C'est moins sécurisé mais peut être installé gratis.

Plus d'informations sur des Certificats peuvent être trouvées dans les liens ci-dessous :

- Délivrez un certificat (l'importation/exportation/génèrent le CSR) sur le routeur de gammes RV160 et RV260
- Remplacez le certificat Auto-signé par par défaut par un certificat SSL de tiers sur le routeur de gamme RV34x

Site à site VPN sur un routeur

Pour le routeur local et distant, il est important de s'assurer la clé pré-partagée (PSK) /password/Certificate utilisée pour la connexion VPN, et les paramètres de sécurité toute la correspondance. Si un ou plusieurs Routeurs utilisent le Traduction d'adresses de réseau (NAT), qui la majeure partie de l'utilisation de Routeurs d'affaires de Cisco, vous devrez faire des exemptions de Pare-feu pour la connexion VPN sur le routeur local et distant.

Contrôle ces pour en savoir plus d'articles de site à site :

- Configurer le site à site VPN sur le RV34x
- Configurez un site à site VPN sur un routeur RV340 ou RV345
- Entretien de tech de Cisco : Configuration du site à site VPN sur des Routeurs de gamme RV340 (vidéo)
- Configurant le site à site VPN sur un routeur RV160 et RV260 (paramètres de base)
- Site à site VPN sur le routeur RV160 et RV260 (paramètres avancés et Basculement)

Client-à-site VPN sur un routeur

Avant qu'un VPN puisse être installé sur le côté client, un administrateur doit le configurer sur le routeur.

Clic pour visualiser ces articles de configuration de routeur :

- Configurant l'assistant de configuration VPN sur les Routeurs RV160 et RV260
- Configurer le client vpn mou de musaraigne avec le RV160 et le RV260
- Entretien de tech de Cisco : Configurant la musaraigne VPN doux sur RV160 et RV260 (vidéo)
- Client vpn de TheGreenBow IPsec d'installation et d'utilisation à connecter aux Routeurs RV160 et RV260

Créez un profil de Client-à-site

Dans une connexion VPN de Client-à-site, les clients de l'Internet peuvent se connecter au serveur pour accéder au réseau d'entreprise ou le RÉSEAU LOCAL derrière le serveur mais pour mettre à jour toujours la Sécurité du réseau et de ses ressources. Cette caractéristique est très utile puisqu'elle crée un nouveau tunnel VPN qui permettrait à des télétravailleurs et à des voyageurs d'affaires pour accéder à votre réseau à l'aide d'un logiciel de client VPN sans compromettre la sécurité et confidentialité. Les articles suivants sont spécifiques aux Routeurs de gamme RV34x :

- Configurez la connexion du réseau privé virtuel de Client-à-site (VPN) sur le routeur de gamme RV34x
- Configurez la Connectivité du réseau privé virtuel d'AnyConnect (VPN) sur le routeur de gamme RV34x

Groupes d'utilisateurs

Des groupes d'utilisateurs sont créés sur le routeur pour une collection 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, on peut permettre PPTP, site à site IPSec VPN, et client-à-site IPSec VPN. Par exemple, le RV260 a les options qui incluent OpenVPN mais L2TP n'est pas pris en charge. La gamme RV340 est équipée d'AnyConnect pour un VPN SSL, aussi bien que portail captif ou EZ VPN.

Ces configurations permettent à des administrateurs de contrôler et filtrer de sorte que seulement les utilisateurs autorisés puissent accéder au réseau. Le doux et le TheGreenBow de musaraigne sont deux des clients vpn les plus communs disponibles pour le téléchargement. Ils doivent être configurés ont basé sur les configurations VPN du routeur pour qu'elles puissent établir avec

succès un tunnel VPN. L'article suivant adresse spécifiquement la création d'un groupe d'utilisateurs :

- Créez un groupe d'utilisateurs pour le VPN installé sur le routeur RV34x

En installant des groupes d'utilisateurs pour un VPN, soyez sûr de laisser le compte par défaut d'admin dans le groupe d'admin et de créer un nouveaux compte utilisateur et groupe d'utilisateurs pour le VPN. Si vous déplacez votre compte d'admin à un groupe différent, vous vous empêcherez de se connecter dans le routeur. En conséquence, vous devriez faire une réinitialisation aux paramètres d'usine et la configurer pour ce routeur de nouveau, laissant le compte par défaut d'admin dans le groupe d'admin seul.

Comptes utilisateurs

Des comptes utilisateurs sont créés sur le routeur afin de permettre l'authentification des utilisateurs locaux utilisant la base de données locale pour de divers services comme PPTP, client vpn, procédure de connexion de l'interface utilisateur graphique de Web (GUI), et réseau privé virtuel de Secure Sockets Layer (SSLVPN). Ceci permet aux administrateurs de contrôler et filtrer les utilisateurs autorisés pour accéder à seulement le réseau. L'article suivant adresse spécifiquement la création d'un compte utilisateur :

- Créez un utilisateur expliquent le client vpn installé sur le routeur RV34x

Client-à-site à l'emplacement de client

Dans une connexion VPN de Client-à-site, les clients de l'Internet peuvent se connecter au serveur pour accéder au réseau d'entreprise ou le RÉSEAU LOCAL derrière le serveur mais mettent à jour toujours la Sécurité du réseau et de ses ressources. Cette caractéristique est très utile puisqu'elle crée un nouveau tunnel VPN qui permet à des télétravailleurs et à des voyageurs d'affaires pour accéder à votre réseau à l'aide d'un logiciel de client VPN sans compromettre la sécurité et confidentialité. Le VPN est installé pour chiffrer et déchiffrer des données pendant qu'il est envoyé et reçu.

L'application d'AnyConnect fonctionne avec le VPN SSL et est utilisée avec les Routeurs RV34x spécifiquement. Il n'est pas disponible avec l'autre gamme rv de Routeurs. Commençant par la version 1.0.3.15, un permis de routeur n'est plus nécessaire, mais des permis doivent être achetés pour le côté de client du VPN. Pour plus d'informations sur le Client à mobilité sécurisé Cisco AnyConnect, a cliquez ici. Pour des directions sur l'installation, choisissez parmi les articles suivants :

- Installez le Client à mobilité sécurisé Cisco AnyConnect sur un ordinateur de MAC
- Installez le Client à mobilité sécurisé Cisco AnyConnect sur un ordinateur Windows

Il y a quelques applications tierces qui peuvent être utilisées pour le client-à-site VPN avec tous les routeurs de la gamme rv. Comme indiqué précédemment, Cisco ne prend en charge pas ces applications ; ces informations sont données pour des conseils.

Le client vpn de TheGreenBow est une tiers application de client vpn qui permet à un périphérique hôte pour configurer une connexion sécurisée pour le tunnel d'IPsec de client-à-site ou le SSL. C'est une application payée qui inclut le support.

- Client vpn de TheGreenBow IPsec d'installation et d'utilisation à connecter aux Routeurs RV160 et RV260

OpenVPN est un libre, l'application open source qui peut être installée et utilisée pour un VPN SSL. Il emploie une connexion de client-serveur pour fournir des communications protégées entre un serveur et un emplacement de client distant au-dessus de l'Internet.

- OpenVPN sur les Routeurs RV160 et RV260

Le doux de musaraigne est un libre, l'application open source qui peut être aussi bien installée et utilisée pour un IPsec VPN. Il emploie une connexion de client-serveur pour fournir des communications protégées entre un serveur et un emplacement de client distant au-dessus de l'Internet.

- Configurer le client vpn mou de musaraigne avec le RV160 et le RV260

L'Easy VPN était utilisé généralement sur des Routeurs RV32x. Voici quelques informations pour la référence :

- Configurez le client facile au réseau privé virtuel de passerelle (VPN) sur la gamme du routeur VPN RV320 et RV325
- Solution Cisco Easy VPN Q&A
- Easy VPN sur les Routeurs articulés autour d'un logiciel de Cisco IOS

Assistant de configuration

Les plus défunts Routeurs d'affaires de Cisco été livré avec un assistant de configuration VPN qui vous guide par les étapes pour l'installation. L'assistant de configuration VPN vous permet de configurer les connexions VPN de base d'entre réseaux locaux et d'Accès à distance et d'assigner des clés pré-partagées ou des Certificats numériques pour l'authentification. Contrôle ces pour en savoir plus d'articles :

- Configurer l'assistant de configuration VPN sur le RV160 et le RV260
- Configurez la connexion du réseau privé virtuel (VPN) utilisant le magicien d'installation sur le routeur de gamme RV34x

Conclusion

Cet article vous a mené à une meilleure compréhension des VPN avec des conseils vous obtenir sur votre chemin. Maintenant vous devriez être prêt à configurer vos propres moyens ! Prenez un certain temps de visualiser les liens et de décider la meilleure manière d'installer un VPN sur votre routeur d'affaires de Cisco.