Nouveautés de Cisco Business : Glossaire des équipements et des réseaux de base

Objectif

L'objectif de ce document est de familiariser les débutants avec l'équipement Cisco Business (Small Business) et certains termes généraux que vous devez connaître. Les sujets abordés incluent le matériel disponible, les termes commerciaux Cisco, les termes généraux relatifs aux réseaux, les outils Cisco, les notions de base sur l'échange de données, les notions de base sur une connexion Internet, les réseaux et leur adéquation.

Introduction

Commencez-vous tout juste à configurer votre réseau avec l'équipement Cisco ? Il peut être accablant d'entrer dans le nouveau monde de la configuration et de la maintenance d'un réseau. Cet article vous aidera à vous familiariser avec certains des éléments de base. Plus vous en saurez, moins ce sera intimidant !

Matériel disponible auprès de Cisco Business

Routeur

Les routeurs relient plusieurs réseaux ainsi que les données de route à l'endroit où elles doivent se trouver. Ils connectent également les ordinateurs de ces réseaux à Internet. Les routeurs permettent à tous les ordinateurs en réseau de partager une seule connexion Internet, ce qui permet d'économiser de l'argent.

Un routeur agit en tant que répartiteur. Il analyse les données envoyées sur un réseau, choisit la meilleure route pour les données à acheminer et les envoie sur son chemin.

Les routeurs connectent votre entreprise au monde entier, protègent les informations contre les menaces de sécurité et peuvent même décider quels ordinateurs sont prioritaires par rapport aux autres.

Au-delà de ces fonctions réseau de base, les routeurs disposent de fonctionnalités supplémentaires pour faciliter ou sécuriser le réseau. En fonction de vos besoins, par exemple, vous pouvez choisir un routeur avec un pare-feu, un réseau privé virtuel (VPN) ou un système de communication IP (Internet Protocol).

Les routeurs Cisco Business les plus récents incluent les gammes RV160, RV260, RV340 et RV345.

Commutateur

Les commutateurs constituent la base de la plupart des réseaux d'entreprise. Un commutateur fait office de contrôleur, connectant des ordinateurs, des imprimantes et des serveurs à un réseau dans un bâtiment ou un campus.

Les commutateurs permettent aux périphériques de votre réseau de communiquer entre eux, ainsi qu'avec d'autres réseaux, créant ainsi un réseau de ressources partagées. Grâce au partage des informations et à l'allocation des ressources, les commutateurs permettent d'économiser de l'argent et d'augmenter la productivité.

Il existe deux types de commutateurs de base parmi lesquels choisir parmi les éléments de base de votre réseau : gérés et non gérés.

> Un commutateur non géré est prêt à l'emploi mais ne peut pas être configuré. Les équipements de réseau domestique offrent généralement des commutateurs non gérés. Un commutateur géré peut être configuré. Vous pouvez surveiller et ajuster un commutateur géré localement ou à distance, ce qui vous permet de mieux contrôler le trafic et l'accès réseau.

Pour plus d'informations sur les commutateurs, consultez le Glossaire des termes relatifs aux commutateurs.

Les derniers commutateurs développés incluent les gammes Cisco Business Switch CBS110, CBS220, CBS250 et CBS350.

Si vous souhaitez connaître les différences entre les commutateurs CBS, extrayez

Point d'accès sans fil

Un point d'accès sans fil permet aux périphériques de se connecter au réseau sans fil sans câbles. Un réseau sans fil facilite la mise en ligne de nouveaux périphériques et offre une prise en charge flexible aux travailleurs mobiles.

Un point d'accès sert d'amplificateur pour votre réseau. Alors qu'un routeur fournit la bande passante, un point d'accès étend cette bande passante de sorte que le réseau

puisse prendre en charge de nombreux périphériques et que ces périphériques puissent accéder au réseau de plus loin.

Mais un point d'accès ne se contente pas d'étendre le Wi-Fi. Il peut également fournir des données utiles sur les périphériques du réseau, fournir une sécurité proactive et remplir de nombreuses autres fonctions pratiques.

Les points d'accès sans fil les plus récents, Cisco Business Wireless, incluent l'AC140, l'AC145 et l'AC240 qui permettent un réseau maillé sans fil. Si vous n'êtes pas familier avec les réseaux maillés sans fil, vous pouvez en savoir plus dans la section Bienvenue dans Cisco Business Wireless Mesh Networking ou Forum Aux Questions (FAQ) pour un réseau sans fil professionnel Cisco.

Si vous souhaitez connaître certains termes communs aux points d'accès sans fil, consultez le Glossaire WAP.

Téléphone multiplateforme

Les téléphones MPP fournissent des communications VoIP (Voice over IP) à l'aide du protocole SIP (Session Initiation Protocol). Cela élimine le besoin de lignes téléphoniques traditionnelles, rendant les téléphones plus portables au sein de l'entreprise. Avec la VoIP, un téléphone utilise une infrastructure réseau existante et une connexion Internet au lieu de lignes T1 coûteuses. Cela permet de gérer plus d'appels avec moins de 'lignes'. D'autres options avantageuses incluent la mise en attente d'appels, le parcage d'appels, le transfert d'appels, etc. Certains modèles permettent la communication vidéo en plus de la VoIP.

Les téléphones MPP sont conçus pour ressembler à un téléphone classique et ne sont utilisés qu'à cette fin, mais essentiellement, ils sont un ordinateur et font partie de votre réseau. Les téléphones MPP nécessitent un service d'un fournisseur de services de téléphonie Internet (ITSP) ou d'un serveur de contrôle d'appel IP Private Branch Exchange (PBX). WebEx Calling, Ring Central et Verizon sont des exemples d'ITSP. Les plates-formes Asterisk, Centile et Metaswitch sont quelques exemples de services PBX IP qui fonctionnent avec les téléphones MPP Cisco. De nombreuses fonctionnalités de ces téléphones sont programmées spécifiquement par des fournisseurs tiers (tels que FreePBX), de sorte que les processus (parking, accès à la messagerie vocale, etc.) peuvent varier.

Les téléphones Cisco Business MPP les plus récents incluent les gammes 6800, 7800 et 8800.

Couramment référencé dans Cisco Business

Guide d'administration et Guide de démarrage rapide

Voici deux ressources différentes à rechercher pour obtenir des informations très détaillées sur votre produit et ses fonctionnalités. Lorsque vous effectuez une recherche sur un site ou un site Web avec votre numéro de modèle, vous pouvez

ajouter l'un ou l'autre pour afficher ces guides plus longs.

Paramètres par défaut

Les périphériques sont fournis avec des paramètres présélectionnés par défaut. Il s'agit souvent des paramètres les plus courants qu'un administrateur choisirait. Vous pouvez modifier les paramètres en fonction de vos besoins.

Nom d'utilisateur et mot de passe par défaut

Dans les équipements Cisco Business plus anciens, la valeur par défaut était *admin* pour le nom d'utilisateur et le mot de passe. Maintenant, la plupart ont une valeur par défaut *cisco* pour le nom d'utilisateur et le mot de passe. Sur les téléphones VoIP (Voice over IP), vous devez vous connecter en tant qu'*administrateur* pour modifier de nombreuses configurations. Il est fortement recommandé de modifier le mot de passe pour le rendre plus complexe à des fins de sécurité.

Adresses IP par défaut

La plupart des équipements Cisco sont fournis avec des adresses IP par défaut pour les routeurs, les commutateurs et les points d'accès sans fil. Si vous ne vous souvenez pas de l'adresse IP et que vous n'avez pas de configuration spéciale, vous pouvez utiliser un trombone ouvert pour appuyer sur le bouton de réinitialisation de votre périphérique pendant au moins 10 secondes. Les paramètres par défaut seront rétablis. Si votre commutateur ou WAP n'est pas connecté à un routeur avec DHCP activé et que vous êtes connecté directement au commutateur ou au WAP avec votre ordinateur, il s'agit des adresses IP par défaut.

L'adresse IP par défaut d'un routeur Cisco Business est 192.168.1.1.
L'adresse IP par défaut d'un commutateur Cisco Business est 192.168.1.254.
L'adresse IP par défaut d'un point d'accès sans fil Small Business est 192.168.1.245. Il n'existe aucune adresse IP par défaut pour les nouveaux points d'accès sans fil maillés.

Rétablir les paramètres d'usine par défaut

Il se peut que vous souhaitiez rétablir les paramètres d'usine par défaut de votre routeur, commutateur ou point d'accès sans fil d'entreprise Cisco et repartir de zéro. Cela est pratique lorsque vous déplacez l'équipement d'un réseau à un autre, ou en dernier recours lorsque vous ne pouvez pas résoudre un problème de configuration. Lorsque vous réinitialisez les paramètres d'usine par défaut, vous perdez toutes les configurations.

Vous pouvez sauvegarder les configurations afin de pouvoir les restaurer après une réinitialisation en usine. Pour plus d'informations, cliquez sur les liens suivants :

- Redémarrer ou restaurer les paramètres d'usine par défaut du routeur de la gamme RV34x via l'utilitaire Web
- Sauvegarde et restauration ou remplacement du micrologiciel sur un commutateur

- Télécharger, sauvegarder, copier et supprimer des fichiers de configuration sur un point d'accès sans fil
- Gestion des fichiers de configuration sur le point d'accès WAP125 ou WAP581

Si vous ne sauvegardez pas la configuration, vous devrez reconfigurer le périphérique à partir de zéro afin de vous assurer d'avoir les détails de la connexion. La plupart des modèles ont un article détaillant les étapes à suivre pour une réinitialisation, mais la façon la plus simple d'y parvenir est d'utiliser un trombone ouvert et d'appuyer sur le bouton de réinitialisation de votre périphérique pendant au moins 10 secondes. Cela ne s'applique pas aux téléphones MPP. Consultez donc Réinitialiser un téléphone IP Cisco pour plus d'informations.

Interface utilisateur Web

Chaque équipement Cisco Business est fourni avec une interface utilisateur Web, à l'exception des commutateurs non gérés de la gamme 100.

Ce type d'interface, ce que vous voyez à l'écran, affiche les options de sélection. Vous n'avez pas besoin de connaître de commandes pour naviguer dans ces écrans. L'interface utilisateur Web est parfois appelée interface graphique utilisateur (GUI), interface Web, guide Web, utilitaire Web ou utilitaire de configuration Web.

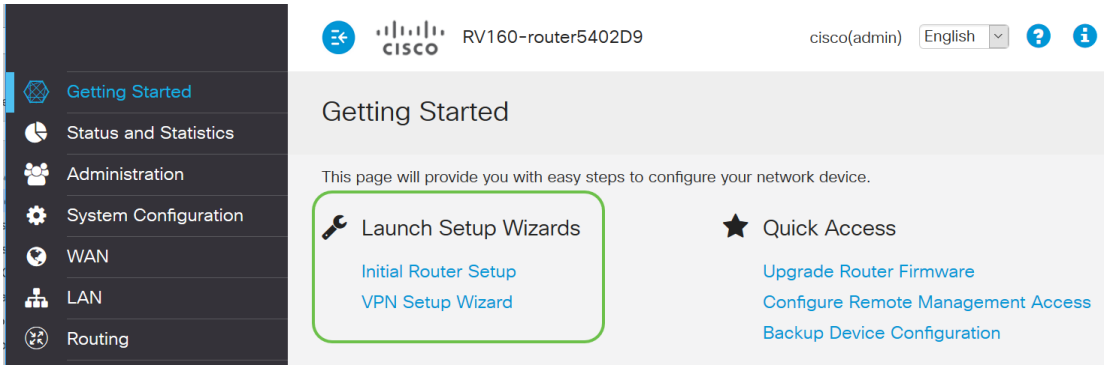
L'interface utilisateur Web est l'un des moyens les plus simples de modifier la configuration d'un périphérique. L'interface utilisateur Web fournit à l'administrateur un outil qui contient toutes les fonctionnalités possibles qui peuvent être modifiées pour modifier les performances d'un périphérique.

Après vous être connecté à un périphérique Cisco, un écran d'interface utilisateur Web s'affiche et comprend un volet de navigation situé sur le côté gauche. Il contient une liste des fonctions de niveau supérieur du périphérique. Le volet de navigation est parfois appelé arborescence de navigation, barre de navigation ou carte de navigation.

Les couleurs de cette page peuvent varier, ainsi que les fonctions de niveau supérieur, selon l'équipement et la version du micrologiciel.

Assistant de configuration

Il s'agit d'un écran interactif que vous naviguerez lorsque vous vous connecterez à un périphérique Cisco Small Business pour la première fois, et éventuellement après. Il peut s'avérer un excellent moyen de vous mettre en service sur votre réseau. Plusieurs paramètres par défaut présélectionnés peuvent être modifiés. Certains périphériques sont fournis avec plusieurs assistants de configuration. Cet exemple montre deux Assistants de configuration, *Configuration initiale du routeur* et *Assistant Configuration VPN*.



Appartient à Cisco

Spécifiquement développé et détenu par Cisco. Par exemple, le protocole CDP (Cisco Discovery Protocol) est propriétaire de Cisco. En règle générale, les protocoles propriétaires Cisco ne peuvent être utilisés que sur les périphériques Cisco.

Modèles d'une série

Cisco propose aux propriétaires de petites entreprises de nombreux modèles différents répondant aux besoins de leur entreprise. Souvent, un modèle est proposé avec différentes fonctionnalités, un nombre de ports, une technologie Power over Ethernet ou même un réseau sans fil. S'il existe plusieurs modèles dans une série, Cisco placera un x au lieu du numéro ou de la lettre qui varie d'un modèle à l'autre, mais les informations s'appliquent à tous les modèles de cette série. Par exemple, les routeurs RV340 et RV345 sont référencés à la gamme RV34x. Si un périphérique a un point d'accès à l'extrémité, il offre la technologie Power over Ethernet. Si un nom de périphérique se termine en W, il offre des fonctionnalités sans fil. En général, plus le nombre de modèles est élevé, plus les capacités du périphérique sont élevées. Pour en savoir plus, consultez les articles suivants :

- Sonnerie de décodeur de produits - Routeur
- Décodeur d'ID de produit - Commutateur
- Sonnerie de décodage de produit - WAP
- Cisco Business Wireless Model Decoder (sans fil maillé)

Micrologiciel

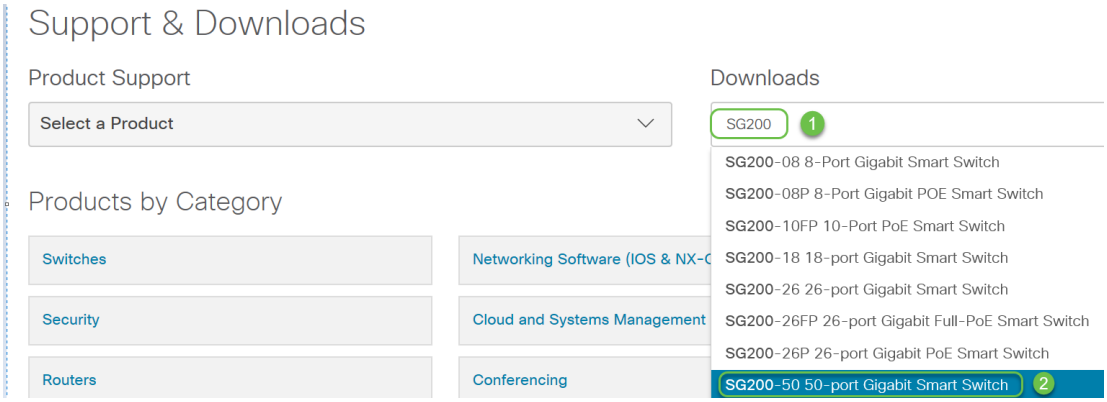
Également appelée image. Programme qui contrôle les opérations et les fonctionnalités du périphérique.

Mettre à niveau le micrologiciel

La mise à niveau du micrologiciel est essentielle pour des performances optimales sur chaque périphérique. Il est très important d'installer les mises à niveau lorsqu'elles sont publiées. Lorsque Cisco lance une mise à niveau du micrologiciel, elle contient souvent des améliorations telles que de nouvelles fonctionnalités ou corrige un bogue qui peut provoquer une vulnérabilité de sécurité ou un problème de performances.

Accédez à Assistance Cisco, puis saisissez le nom du périphérique qui nécessite une mise à niveau sous *Téléchargements*. Un menu déroulant doit apparaître. Faites

défiler la liste vers le bas et choisissez le modèle que vous possédez.



Conseil : lorsque vous recherchez différentes versions du micrologiciel Cisco, chacune d'elles suit un format x.x.x.x. qui sont considérés comme quatre octets. En cas de mise à jour mineure, le quatrième octet change. Le troisième octet change lorsqu'il s'agit d'un changement plus important. Le deuxième octet implique un changement majeur. Le premier octet change s'il s'agit d'une révision complète.

Si vous souhaitez obtenir des conseils, cliquez sur ce lien pour télécharger et mettre à niveau le micrologiciel sur n'importe quel périphérique.

Cet article présente quelques idées de dépannage au cas où vous rencontreriez des problèmes avec une mise à niveau de commutateur : mettre à niveau le micrologiciel sur un commutateur de la gamme 200/300.

Conditions générales relatives aux réseaux

Une fois que vous avez votre équipement, vous devez vous familiariser avec certains termes courants relatifs aux réseaux.

Interface

Une interface est généralement cet espace entre un système et un autre. Tout ce qui peut communiquer avec votre ordinateur, y compris les ports. Une adresse IP locale est généralement attribuée à une interface réseau. Une interface utilisateur permet à l'utilisateur d'interagir avec le système d'exploitation.

Noeud

Terme général désignant tout périphérique qui établit une connexion ou une interaction au sein d'un réseau, ou qui peut envoyer, recevoir et stocker des informations, communiquer avec Internet et avoir une adresse IP.

Hôte

Un hôte est un périphérique qui est un point d'extrémité pour les communications sur un réseau, l'hôte peut fournir des données ou un service (comme DNS) à d'autres

noeuds. Selon la topologie, un commutateur ou un routeur peut être un hôte. Tous les hôtes sont également des noeuds. Par exemple, un ordinateur, un serveur ou une imprimante.

Programme informatique

Un programme informatique contient des instructions qui peuvent être exécutées sur un ordinateur.

Application

Le logiciel d'application est un programme qui vous aide à effectuer des tâches. Ils sont souvent appelés interchangeables car ils sont semblables, mais tous les programmes ne sont pas des applications.

Meilleure pratique

Méthode recommandée pour configurer un élément et exécuter votre réseau.

Topologie

La manière physique dont votre équipement est connecté. Carte du réseau.

Configuration

Il s'agit de la façon dont les choses sont configurées. Vous pouvez laisser les paramètres par défaut, ceux qui sont préconfigurés lors de l'achat d'équipement, ou vous pouvez configurer pour vos besoins spécifiques. Les paramètres par défaut sont les configurations de base, souvent recommandées. Lorsque vous vous connectez à votre périphérique, il se peut qu'un Assistant de configuration vous guide tout au long de ce que vous devez faire.

Adresse MAC :

Identificateur unique pour chaque périphérique. Se trouve sur le périphérique physique et peut être détecté avec Bonjour, LLDP ou CDP. Un commutateur suit les adresses MAC sur les périphériques lorsqu’il interagit avec eux et crée une table d’adresses MAC. Cela aide le commutateur à savoir où acheminer les paquets d’informations.

Open Source

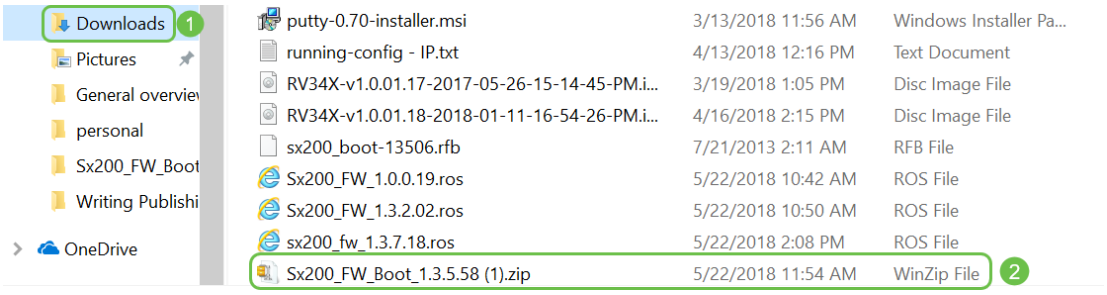
Un programme gratuit pour le public.

Fichier Zip

Groupe de fichiers compressés dans un fichier zip. Il est utilisé lorsque vous voulez transférer plusieurs fichiers en une seule étape. Le récepteur peut ouvrir le fichier zip

et accéder à chacun séparément. Un fichier zip se termine par *.zip*.

Si vous voyez un fichier au format se terminant par *.zip*, vous devez décompresser ce fichier. Si vous n'avez pas de programme de décompression, vous devrez en télécharger un. Il existe plusieurs options gratuites en ligne. Après avoir téléchargé un programme de décompression, cliquez sur **Téléchargements** et recherchez le fichier *.zip* dont vous avez besoin pour décompresser.



Cliquez avec le bouton droit de la souris sur le nom du fichier zip, un écran similaire à celui-ci apparaîtra. Passez le curseur sur le logiciel de décompression, puis sélectionnez **Extraire ici**. Dans cet exemple, 7-Zip est utilisé.

Interface de ligne de commande (CLI)

Interface de ligne de commande (CLI) : Parfois appelé terminal. Cette option est également utilisée pour choisir des configurations sur des périphériques tels que des routeurs et des commutateurs. Si vous avez de l'expérience, il peut s'agir d'une façon beaucoup plus simple d'installer les éléments, car vous n'aurez pas à naviguer dans les différents écrans de l'interface utilisateur Web. L'inconvénient est que vous devez connaître les commandes et les saisir parfaitement. Puisque vous lisez un article pour les débutants, l'interface de ligne de commande ne devrait probablement pas être votre premier choix.

Machine virtuelle

La plupart des machines ont des capacités supérieures à ce dont elles ont besoin. Un ordinateur peut être configuré pour contenir tout ce qui est nécessaire pour exécuter plusieurs machines. Le problème est que si une partie tombe en panne ou a besoin d'un redémarrage, ils suivent tous.

Si vous installez VMware ou Hyper-V, vous pouvez charger des logiciels, des serveurs Web, des serveurs de messagerie, FindIT, etc. sur un seul ordinateur. Une machine virtuelle peut même utiliser un système d'exploitation différent. Ils sont logiquement indépendants les uns des autres. Chacun remplit les fonctions d'un périphérique distinct sans en être un. Bien que le matériel soit partagé, chaque machine virtuelle

alloue une partie des recours physiques pour chaque système d'exploitation. Cela permet d'économiser de l'argent, de l'énergie et de l'espace.

Outils Cisco que vous pouvez utiliser

Tableau de bord Cisco Business (CBD)

Il s'agit d'un outil Cisco utilisé pour surveiller et gérer les réseaux. Le CBD peut vous aider à identifier les périphériques Cisco de votre réseau, ainsi que d'autres fonctions de gestion utiles.

Il s'agit d'un outil utile si vous exécutez des objets depuis votre domicile ou si vous surveillez plusieurs réseaux. CBD peut être exécuté sur une machine virtuelle. Pour plus d'informations sur CBD, consultez le site d'assistance Cisco Business Dashboard ou la présentation de Cisco Business Dashboard.

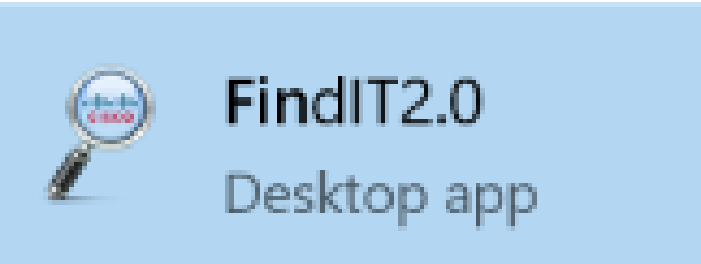
Utilitaire FindIT Network Discovery

Cet outil simple est très simple mais peut vous aider à découvrir rapidement les équipements Cisco sur votre réseau. Cisco FindIT détecte automatiquement tous les périphériques Cisco Small Business pris en charge dans le même segment de réseau local que votre ordinateur.

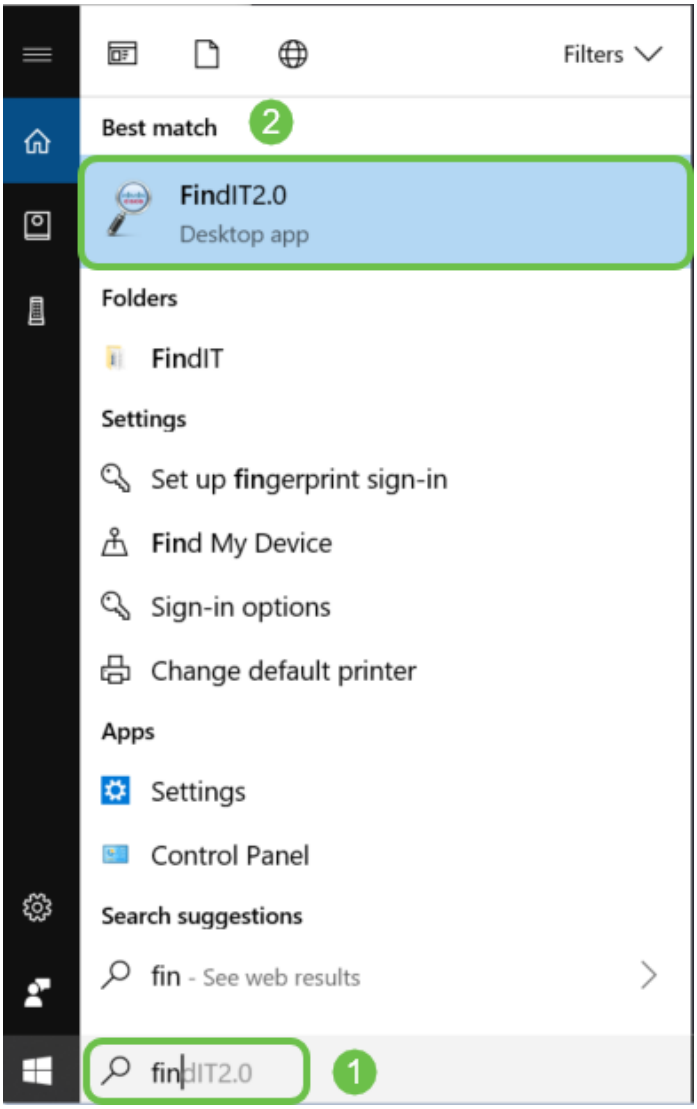
Cliquez pour en savoir plus et pour télécharger l'utilitaire Cisco Small Business FindIT Network Discovery.

Cliquez sur ce lien pour lire un article sur Comment installer et configurer Cisco FindIT Network Discovery Utility.

L'application ressemble à ceci pour Windows 10.



Une fois téléchargé, vous le trouverez ici dans Windows 10.



AnyConnect (routeurs/VPN de la gamme RV34x)

Ce VPN est spécifiquement utilisé avec les routeurs de la gamme RV34x (et les équipements d'entreprise/grande entreprise). Le client Cisco AnyConnect Secure Mobility fournit aux utilisateurs distants une connexion VPN sécurisée. Il fournit aux utilisateurs finaux distants les avantages d'un client VPN SSL (Secure Sockets Layer) de Cisco et prend également en charge les applications et fonctions non disponibles sur une connexion VPN SSL basée sur navigateur. Généralement utilisés par les télétravailleurs, AnyConnect leur permet de se connecter à l'infrastructure informatique de l'entreprise comme s'ils se trouvaient physiquement au bureau, même s'ils ne le sont pas. Cela ajoute à la flexibilité, à la mobilité et à la productivité des travailleurs. Des licences client sont nécessaires pour utiliser AnyConnect. Cisco AnyConnect est compatible avec les systèmes d'exploitation suivants : Windows 7, 8, 8.1 et 10, Mac OS X 10.8 et versions ultérieures et Linux Intel (x64).

Reportez-vous aux articles suivants pour plus d'informations :

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

Notions de base sur l'échange de données

Paquet

Dans le domaine des réseaux, les informations sont envoyées en blocs, appelés paquets. En cas de problème de connexion, les paquets peuvent être perdus.

Latence

Retards dans le transfert de paquets.

Redondance

Dans un réseau, la redondance est configurée de sorte que si une partie du réseau présente des problèmes, l'ensemble du réseau ne tombe pas en panne. Considérez-le comme un plan de sauvegarde si quelque chose arrive à la configuration principale.

Protocoles

Deux périphériques doivent avoir certains des mêmes paramètres pour communiquer. Pensez-y comme une langue. Si une personne ne parle que l'allemand et l'autre ne parle que l'espagnol, elle ne pourra pas communiquer. Différents protocoles fonctionnent ensemble et plusieurs protocoles peuvent être transmis entre eux. Les protocoles ont des objectifs différents ; certains exemples sont énumérés et brièvement décrits ci-dessous.

Protocoles d'adressage

- **Session Initiation Protocol (SIP) :** protocole principal pour la voix sur IP (VoIP), les téléphones qui communiquent via Internet. Les deux côtés du réseau doivent être configurés à l'aide du même protocole pour communiquer, afin qu'ils aient tous deux besoin du protocole SIP pour initier la communication sur VoIP.
- **Le protocole DHCP (Dynamic Host Configuration Protocol)** gère un pool d'adresses IP disponibles, en les attribuant aux hôtes lorsqu'ils rejoignent le réseau.
- **Protocole de résolution d'adresse** (ARP) : mappe une adresse IP dynamique à une adresse MAC physique permanente dans un réseau local.
- **IPv4 :** il s'agit de la version la plus courante d'IP utilisée aujourd'hui. Une adresse IP est écrite sous la forme de 4 ensembles de nombres (également appelés octets) séparés par un point entre chaque ensemble. Chaque jeu peut être un nombre compris entre 0 et 255. Un exemple d'adresse IPv4 est 8.8.8.8, qui est le serveur DNS public de Google. Il existe plus de périphériques que d'adresses IP uniques pour IPv4, il peut donc être coûteux d'acheter une adresse IP publique permanente.
- **IPv6 :** Cette dernière version utilise 8 ensembles de nombres avec deux-points entre chaque ensemble. Il utilise un système numérique hexadécimal, de sorte qu'il peut y avoir des lettres dans l'adresse IP. Une entreprise peut avoir des adresses IPv4 et IPv6 exécutées simultanément.

Puisque nous parlons d'IPv6, voici quelques détails importants à savoir sur ce protocole d'adressage :

Abréviations IPv6 : si tous les nombres de plusieurs ensembles sont nuls, deux points-virgules d'une ligne peuvent représenter ces ensembles, cette abréviation ne peut être utilisée qu'une seule fois. Par exemple, l'une des adresses IP IPv6 de Google est 2001:4860:4860::8888. Certains périphériques utilisent des champs distincts pour les huit parties des adresses IPv6 et ne peuvent pas accepter l'abréviation IPv6. Dans ce cas, saisissez 2001:4860:4860:0:0:0:0:0:8888.

Hexadécimal : Un système numérique qui utilise une base 16 au lieu de la base 10, ce que nous utilisons dans les maths de tous les jours. Les nombres 0 à 9 sont représentés de la même manière. 10-15 sont représentées par les lettres A-F.

Protocoles de transfert de données

- **TCP (Transmission Control Protocol) et UDP (User Datagram Protocol) :** il s'agit de deux modes de transport des données. Le protocole TCP nécessite une connexion, appelée échange en trois étapes, avant d'envoyer des données, ce qui entraîne parfois un retard. Si des données (paquets) sont perdues, elles sont à nouveau envoyées. Le protocole UDP est moins fiable, mais plus rapide. Souvent, la voix et la vidéo utilisent le protocole UDP.
- **FTP (File Transfer Protocol) :** ce protocole permet de transférer des fichiers d'un client vers un serveur.
- **Hypertext Transfer Protocol (HTTP) vs. Hypertext Transfer Protocol Secure (HTTPS) :** Base générale de la communication de données sur Internet. Vous les trouverez au début des sites Web, écrits en *http://* et *https://*. Les sites qui commencent par *https://* sont plus sûrs à utiliser.
- **RIP (Routing Information Protocol) :** ce protocole existe depuis longtemps. Il existe trois versions, chaque version ajoutant davantage de sécurité et de fonctionnalités. Les routeurs partagent des routes entre eux. Son objectif est d'empêcher les boucles en définissant un nombre maximal de sauts “ ” d'un routeur à l'autre. D'autres protocoles de routage plus efficaces incluent **EIGRP (Enhanced Interior Gateway Routing Protocol)**, **OSPF (Open Shortest Path First)** et **IS (Intermediate System to Intermediate System)**. Ces trois dernières sont plus évolutives que le protocole RIP, mais peuvent être plus compliquées à configurer.
- **Secure Shell (SSH) :** canal sécurisé qui fournit une route sécurisée pour le trafic de ligne de commande. Il s'agit d'un protocole chiffré utilisé pour communiquer avec un serveur distant. De nombreuses technologies supplémentaires sont développées autour de SSH.

Protocoles de détection

- **Cisco Discovery Protocol (CDP) :** détecte les informations relatives aux autres équipements Cisco directement connectés et enregistre ces informations. **Bonjour** et le **protocole LLDP (Link Layer Discovery Protocol)** remplissent les mêmes fonctions et peuvent également obtenir des informations sur les périphériques non-Cisco. La plupart des périphériques des petites entreprises utilisent le protocole LLDP.
- **Protocole LLDP (Layer Link Discovery Protocol) :** Permet à un périphérique d'annoncer son identification, sa configuration et ses fonctionnalités aux périphériques voisins qui stockent ensuite les données dans une base MIB (Management Information Base). Les

informations partagées entre les voisins permettent de réduire le temps nécessaire à l'ajout d'un nouveau périphérique au réseau local (LAN) et fournissent également les détails nécessaires au dépannage de nombreux problèmes de configuration. Le protocole LLDP peut être utilisé dans des scénarios où vous devez travailler entre des périphériques qui ne sont pas propriétaires de Cisco et des périphériques qui sont propriétaires de Cisco. Le commutateur fournit toutes les informations sur l'état LLDP actuel des ports et vous pouvez utiliser ces informations pour résoudre les problèmes de connectivité au sein du réseau. Il s'agit de l'un des protocoles utilisés par les applications de découverte de réseau telles que FindIT Network Management pour détecter les périphériques du réseau.

Identification des protocoles

- **Système de noms de domaine (DNS) :** une fois qu'un nom de domaine complet (FQDN) est attribué à une adresse IP, il est placé dans une base de données. Par exemple, lorsque vous effectuez une recherche sur *www.google.com* vous pouvez entrer le nom du site Web, et la base de données la recherche et peut vous y accéder via son adresse IP. Votre **fournisseur d'accès Internet (FAI)** utilise son serveur DNS par défaut et il a déjà été configuré. Cependant, vous pouvez modifier manuellement cette option si vous constatez des vitesses lentes lors de l'utilisation d'Internet.
- **DNS dynamique :** également appelé DDNS, met automatiquement à jour un serveur du DNS avec la configuration active de ses noms d'hôte, adresses ou toute autre information pertinente. En d'autres termes, DDNS attribue un nom de domaine fixe à une adresse IP WAN dynamique. Cela permet d'économiser le coût d'achat d'une adresse IP permanente.
- **Protocole Internet (IP) :** les adresses IP sont des identificateurs uniques qui permettent l'envoi et la réception de données entre les hôtes sur Internet. Cela se fait via des adresses Internet publiques, qui nécessitent un achat auprès d'un FAI.
- **Contrôle d'accès au support (adresse MAC) :** chaque périphérique est connecté à un identificateur unique. Cela ne change pas. Il est bon de connaître votre adresse MAC lors de la configuration d'un réseau et du dépannage. Il se trouve généralement sur le périphérique et contient des lettres et des chiffres. Les commutateurs assurent le suivi des adresses MAC des périphériques et créent une table d'adresses MAC.

Protocoles de dépannage

- **Ping :** une requête ping est une méthode de dépannage courante. Une requête ping envoie des messages d'écho ICMP à une adresse IP. Un message est reçu en retour. Une réponse réussie indique une connectivité physique bidirectionnelle. Il permet de voir si un paquet de données réseau peut être distribué à une adresse sans problème.
- **ICMP (Internet Control Message Protocol) :** messages relatifs aux erreurs et aux informations opérationnelles. Lorsque vous effectuez un test PING, un message d'écho ICMP est envoyé à la destination. Une connexion réussie obtient une réponse de ce périphérique.

Serveur

Un ordinateur ou un programme sur un ordinateur qui fournit des services à d'autres

ordinateurs. Un serveur peut être virtuel ou même une application. Il peut y avoir plusieurs serveurs sur un seul périphérique. Les serveurs peuvent partager entre eux. Ils peuvent être utilisés avec Windows, Mac ou Linux.

Serveurs Web : formatage et présentation des pages Web pour les navigateurs Web
Serveurs de fichiers - partagez des fichiers et des dossiers aux utilisateurs d'un réseau
Serveurs de messagerie - envoyer, recevoir et stocker des e-mails
Serveurs DNS - traduisez des noms conviviaux tels que www.cisco.com en adresse IP 173.37.145.84, par exemple
Serveurs de messagerie instantanée - contrôler le flux et gérer les messages instantanés (Jabber, Skype)

Quality of Service (QoS)

Ces paramètres sont configurés pour s'assurer que la priorité est donnée au trafic sur un réseau, généralement voix ou vidéo, car c'est souvent le plus visible en cas de retard de paquets (données).

Notions de base sur une connexion Internet

Fournisseur de services Internet (FAI)

Vous avez besoin d'un FAI pour accéder à Internet sur votre réseau. Il existe de nombreuses options pour les vitesses de connexion, ainsi qu'une variété de prix pour répondre aux besoins de votre entreprise. Outre l'accès à Internet, un FAI propose des e-mails, l'hébergement de pages Web, etc.

Navigateur Web

Application qui s'affiche sur votre périphérique. Il y en a d'autres que vous pouvez télécharger. Une fois téléchargé, vous pouvez ouvrir et saisir l'adresse IP ou le site Web auquel vous souhaitez accéder via Internet. Voici quelques exemples de navigateurs Web :

Microsoft Edge

 ,

Chrome

 ,

Firefox

 ,

et Safari.

 .

Si vous ne parvenez pas à ouvrir quelque chose ou si vous rencontrez d'autres problèmes de navigation, il est facile d'essayer d'ouvrir un autre navigateur Web et de réessayer.

Uniform Resource Locator (URL)

Dans un navigateur Web, vous tapez généralement le nom d'un site Web auquel vous voulez accéder, c'est-à-dire l'URL, son adresse Web. Chaque URL doit être unique. Un exemple d'URL est https://www.cisco.com.

Passerelle par défaut

Il s'agit du routeur que le trafic du réseau local utilise en sortie vers le fournisseur d'accès Internet (FAI) et Internet. En d'autres termes, ce routeur vous connecte à d'autres périphériques en dehors de votre bâtiment et via Internet.

Pare-feu

Un pare-feu est un périphérique de sécurité réseau qui surveille le trafic réseau entrant et sortant et décide d'autoriser ou de bloquer un trafic spécifique en fonction d'un ensemble défini de règles de sécurité, appelé listes de contrôle d'accès (ACL).

Les pare-feu sont la première ligne de défense en matière de sécurité des réseaux depuis des décennies. Ils établissent une barrière entre les réseaux internes sécurisés et contrôlés qui peuvent être fiables et non fiables en dehors des réseaux, comme Internet.

Un pare-feu peut être matériel, logiciel ou les deux.

Pour plus d'informations, consultez Configurer les paramètres de base du pare-feu sur le routeur de la gamme RV34x.

Listes de contrôle d'accès (ACL)

Répertorie les listes qui bloquent ou autorisent l'envoi du trafic à destination et en provenance de certains utilisateurs. Les règles d'accès peuvent être configurées pour être en vigueur à tout moment ou en fonction d'un planning défini. Une règle d'accès

est configurée en fonction de différents critères afin d'autoriser ou de refuser l'accès au réseau. La règle d'accès est planifiée en fonction de l'heure à laquelle les règles d'accès doivent être appliquées au routeur. Celles-ci sont configurées sous les paramètres de sécurité ou de pare-feu. Par exemple, une entreprise peut vouloir empêcher les employés de diffuser des sports en direct ou de se connecter à Facebook pendant les heures d'ouverture.

Bande passante

Quantité de données pouvant être envoyées d'un point à un autre dans une certaine période. Si vous disposez d'une connexion Internet avec une bande passante plus large, le réseau peut déplacer les données beaucoup plus rapidement qu'une connexion Internet avec une bande passante inférieure. La diffusion vidéo en continu prend beaucoup plus de bande passante que l'envoi de fichiers. Si vous constatez un retard lors de l'accès à une page Web ou des retards dans la diffusion vidéo en continu, vous devrez peut-être augmenter la bande passante de votre réseau.

Câble Ethernet

La plupart des périphériques d'un réseau sont équipés de ports Ethernet. Les câbles Ethernet sont ce qui les relie à une connexion câblée. Les deux extrémités du câble RJ45 sont identiques et ressemblent aux prises de téléphone anciennes. Ils peuvent être utilisés pour connecter des périphériques et pour se connecter à Internet. Les câbles connectent les périphériques pour l'accès Internet et le partage de fichiers. Certains ordinateurs nécessitent une carte Ethernet, car ils ne fournissent pas forcément de port Ethernet.

Les réseaux et leur adéquation

Réseau local (LAN)

Un réseau qui peut être aussi grand que plusieurs bâtiments ou aussi petit qu'une maison. Toute personne connectée au réseau local se trouve au même emplacement physique et est connectée au même routeur.

Dans un réseau local, chaque périphérique se voit attribuer sa propre adresse IP interne unique. Ils suivent un modèle 10.x.x.x, 172.16.x.x - 172.31.x.x ou 192.168.x.x. Ces adresses ne sont visibles qu'à l'intérieur d'un réseau, entre des périphériques, et sont considérées comme privées. Des millions d'emplacements peuvent avoir le même pool d'adresses IP internes que votre entreprise. Peu importe, ils ne sont utilisés qu'au sein de leur propre réseau privé, donc il n'y a pas de conflit. Pour que les périphériques du réseau puissent communiquer entre eux, ils doivent tous suivre le même modèle que les autres périphériques, se trouver sur le même sous-réseau et être uniques. Vous ne devriez jamais voir aucune de ces adresses dans ce modèle comme une adresse IP publique, car elles sont réservées aux adresses LAN privées uniquement.

Tous ces périphériques envoient des données via une passerelle par défaut (un routeur) pour accéder à Internet. Lorsque la passerelle par défaut reçoit les

informations, elle doit effectuer la traduction d'adresses de réseau (NAT) et modifier l'adresse IP car tout ce qui se passe sur Internet nécessite une adresse IP unique.

Réseau étendu (WAN)

Un réseau étendu (WAN) est un réseau étendu, parfois au niveau mondial. De nombreux LAN peuvent se connecter à un seul WAN.

Seules les adresses WAN peuvent communiquer entre elles sur Internet. Chaque adresse WAN doit être unique. Pour que les périphériques d'un réseau puissent envoyer et recevoir des informations via Internet, vous devez disposer d'un routeur à la périphérie de votre réseau (une passerelle par défaut) capable de mener la NAT.

Cliquez pour lire Configurer les règles d'accès sur un routeur de la gamme RV34x.

Traduction d'adresses réseau (NAT)

Un routeur reçoit une adresse WAN par l'intermédiaire d'un fournisseur d'accès à Internet (FAI). Le routeur est doté de la fonction NAT qui prend le trafic sortant du réseau, traduit l'adresse privée en adresse WAN publique et l'envoie via Internet. Il fait l'inverse lors de la réception du trafic. Ceci a été configuré car il n'y a pas assez d'adresses IPv4 permanentes disponibles pour tous les périphériques dans le monde.

L'avantage de la fonction NAT est qu'elle fournit une sécurité supplémentaire en masquant efficacement l'ensemble du réseau interne derrière cette adresse IP publique unique. Les adresses IP internes restent souvent les mêmes, mais si elles sont débranchées pendant un certain temps, configurées d'une certaine manière ou réinitialisées à la valeur par défaut d'usine, elles peuvent ne pas l'être.

NAT statique

Vous pouvez configurer l'adresse IP interne pour qu'elle reste identique en configurant le protocole DHCP (Dynamic Host Configuration Protocol) statique sur le routeur. Les adresses IP publiques ne sont pas garanties non plus à moins que vous payiez pour avoir une adresse IP publique statique via votre FAI. De nombreuses entreprises paient ce service pour que leurs employés et leurs clients disposent d'une connexion plus fiable à leurs serveurs (Web, courrier, VPN, etc.) mais cela peut être coûteux.

La fonction NAT statique mappe une traduction un-à-un des adresses IP privées aux adresses IP publiques. Il crée une traduction fixe des adresses privées en adresses publiques. Cela signifie que vous auriez besoin d'une quantité égale d'adresses publiques en tant qu'adresses privées. Cela est utile lorsqu'un périphérique doit être accessible depuis l'extérieur du réseau.

Cliquez pour lire Configuration de NAT et de NAT statique sur les routeurs RV160 et RV260.

CGNAT

La NAT de niveau opérateur est un protocole similaire qui permet à plusieurs clients d'utiliser la même adresse IP.

VLAN

Un réseau local virtuel (VLAN) vous permet de segmenter logiquement un réseau local (LAN) en différents domaines de diffusion. Dans les scénarios où des données sensibles peuvent être diffusées sur un réseau, des VLAN peuvent être créés pour améliorer la sécurité en désignant une diffusion à un VLAN spécifique. Seuls les utilisateurs appartenant à un VLAN peuvent accéder aux données de ce VLAN et les manipuler. Les VLAN peuvent également être utilisés pour améliorer les performances en réduisant la nécessité d'envoyer des diffusions et des multidiffusions vers des destinations inutiles.

Un VLAN est principalement utilisé pour former des groupes entre les hôtes, quel que soit l'emplacement physique des hôtes. Ainsi, un VLAN améliore la sécurité à l'aide de la formation de groupes entre les hôtes. Lorsqu'un VLAN est créé, il n'a aucun effet tant que ce VLAN n'est pas connecté à au moins un port manuellement ou dynamiquement. Une des raisons les plus courantes de configurer un VLAN est de configurer un VLAN distinct pour la voix et un VLAN distinct pour les données. Ceci dirige les paquets pour les deux types de données, malgré l'utilisation du même réseau.

Pour plus d'informations, lisez Meilleures pratiques VLAN et conseils de sécurité pour les routeurs professionnels Cisco.

Sous-réseau

Souvent appelés sous-réseaux, les sous-réseaux sont des réseaux indépendants à l'intérieur d'un réseau IP.

SSID

Le SSID (Service Set Identifier) est un identificateur unique auquel les clients sans fil peuvent se connecter ou partager entre tous les périphériques d'un réseau sans fil. Il est sensible à la casse et ne doit pas dépasser 32 caractères alphanumériques. Il s'agit également du nom du réseau sans fil.

Réseau privé virtuel (VPNs)

La technologie a évolué et les activités sont souvent menées en dehors du bureau. Les périphériques sont plus mobiles et les employés travaillent souvent à domicile ou en déplacement. Cela peut provoquer certaines vulnérabilités de sécurité. Un réseau privé virtuel (VPN) est un excellent moyen de connecter les travailleurs distants sur un réseau de manière sécurisée. Un VPN permet à un hôte distant d'agir comme s'il se trouvait sur le même réseau local.

Un VPN est configuré pour assurer la transmission sécurisée des données. Il existe

différentes options pour configurer un VPN et la façon dont les données sont cryptées. Les VPN utilisent SSL (Secure Sockets Layer), PPTP (Point to Point Tunneling Protocol) et le protocole de tunnellisation de couche 2.

Une connexion VPN permet aux utilisateurs d'accéder, d'envoyer et de recevoir des données depuis et vers 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 pour protéger le réseau privé et ses ressources.

Un tunnel VPN établit un réseau privé qui peut envoyer des données en toute sécurité à l'aide du chiffrement et de l'authentification. Les bureaux d'entreprise utilisent principalement 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 se trouvent en dehors du bureau.

Une connexion VPN peut être configurée entre le routeur et un point d'extrémité une fois que le routeur a été configuré pour une connexion Internet. Le client VPN dépend entièrement des paramètres du routeur VPN pour établir une connexion.

Un VPN prend en charge un VPN de site à site pour un tunnel de passerelle à passerelle. Par exemple, un utilisateur peut configurer un tunnel VPN sur un site de filiale pour se connecter au routeur sur un site d'entreprise, afin que le site de filiale puisse accéder en toute sécurité au réseau d'entreprise. Dans une connexion VPN de site à site, n'importe qui peut lancer une communication. Cette configuration a une connexion cryptée constante.

Le VPN IPsec prend également en charge le VPN client-serveur pour un tunnel hôte-passerelle. Le VPN client-serveur est utile lors de la connexion de l'ordinateur portable/PC de la maison à un réseau d'entreprise via le serveur VPN. Dans ce cas, seul le client peut établir la connexion.

Cliquez ici pour lire Présentation et meilleures pratiques de Cisco Business VPN.

Certificats

Une étape sécurisée de la configuration d'un VPN consiste à obtenir un certificat auprès d'une autorité de certification (CA). Ceci est utilisé pour l'authentification. Les certificats sont achetés sur un certain nombre de sites tiers. C'est un moyen officiel de prouver que votre site est sécurisé. Essentiellement, l'AC est une source fiable qui vérifie que vous êtes une entreprise légitime et qu'elle peut être approuvée. Pour un VPN, vous n'avez besoin que d'un certificat de niveau inférieur à un coût minime. Vous êtes extrait par l'autorité de certification, et une fois qu'ils vérifient vos informations, ils vous délivrent le certificat. Ce certificat peut être téléchargé sous forme de fichier sur votre ordinateur. Vous pouvez ensuite accéder à votre routeur (ou à votre serveur VPN) et le télécharger ici.

Les clients n'ont généralement pas besoin d'un certificat pour utiliser un VPN ; il s'agit

uniquement d'une vérification via le routeur. Une exception à cette règle est OpenVPN, qui nécessite un certificat client.

De nombreuses petites entreprises choisissent d'utiliser un mot de passe ou une clé pré-partagée à la place d'un certificat pour plus de simplicité. Cette solution est moins sécurisée mais peut être mise en place gratuitement.

Certains articles sur ce sujet peuvent vous plaire :

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

Clé prépartagée (PSK)

Il s'agit d'un mot de passe partagé, décidé et partagé avant la configuration d'un VPN et peut être utilisé comme alternative pour utiliser un certificat. Une clé PSK peut être ce que vous voulez qu'elle soit, elle doit juste correspondre sur le site et avec le client lorsqu'ils sont configurés en tant que client sur leur ordinateur. N'oubliez pas que, selon le périphérique, il peut y avoir des symboles interdits que vous ne pouvez pas utiliser.

Durée de vie de la clé

Fréquence à laquelle le système modifie la clé. Ce paramètre doit également être identique au routeur distant.

Conclusion

Là vous avez, vous avez maintenant beaucoup de bases pour vous mettre en route.

Si vous voulez en savoir plus, consultez ces liens !

Méthodes Recommandées pour la définition des adresses IP statiques Présentation et meilleures pratiques de Cisco Business VPN Meilleures pratiques VLAN et conseils de sécurité pour les routeurs professionnels Cisco Sauvegarde Internet - Windows Sauvegarde Internet - Mac Comment se connecter à un commutateur