Le réseau privé virtuel rapide (VPN) a installé sur RV220W et RV120W

Objectifs

Un réseau privé virtuel (VPN) est un réseau qui utilise une infrastructure de télécommunication publique et leur technologie telle que l'Internet, pour fournir aux bureaux distants ou aux utilisateurs individuels l'accès sécurisé au réseau de leur organisation. La plupart des réalisations VPN emploient l'Internet en tant que l'infrastructure publique et un grand choix de protocoles spécialisés pour prendre en charge des communications privées par l'Internet. Le VPN suit une approche de client et serveur. Les clients vpn authentifient des utilisateurs, chiffrent des données, et gèrent des sessions avec des serveurs VPN utilisant une technique appelée le Tunnellisation.

Ce document explique comment installer le VPN rapide sur le RV220W et le RV120W.

Remarque: Téléchargez le dernier micrologiciel de www.cisco.com et sauvegardez-le dans votre ordinateur.

Périphériques applicables

- RV120W
- RV220W

URL de téléchargement logiciel

https://www.cisco.com/cisco/software/release.html?mdfid=283118607&flowid=24581&softwareid=282465795&release=1.4.2.1&relind=AVAILABLE&rellifecycle=&reltype=latest

Version de logiciel

- v1.0.4.17

Procédure pas à pas pour installer le réseau privé virtuel rapide

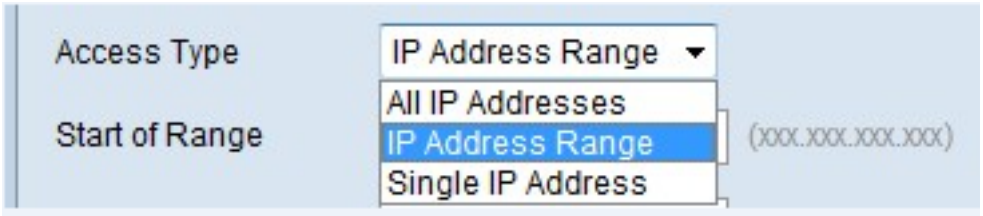
Gestion à distance d'enable

La gestion à distance te permet pour accéder à et contrôler le périphérique sans n'importe quelle connexion physique à l'unité réelle. L'activation de la gestion à distance te permet pour accéder au périphérique d'un réseau BLÊME distant. Le gestionnaire de périphériques est accédé à partir d'un ordinateur sur le RÉSEAU LOCAL à l'aide de l'adresse IP et du HTTP du RÉSEAU LOCAL du périphérique.

Étape 1. Ouvrez une session à l'utilitaire de configuration Web et choisissez la **gestion > la gestion à distance**. La page de *gestion à distance* s'ouvre :

Étape 2. Cochez la case de **gestion à distance** pour activer la gestion à distance.

Remarque: Si cette caractéristique n'est pas activée, Cisco QuickVPN et l'accès de VPN SSL ne fonctionneront pas.



Étape 3. Choisissez le type d'accès pour accorder dans le menu déroulant de type d'Access :

• Tous les IP address — Permet à n'importe quel IP address pour accéder au périphérique. L'utilisateur devra changer le mot de passe par défaut avant que vous choisissiez cette option.

• Chaîne d'IP address — Permet à n'importe quel IP address dans la plage configurée pour accéder au périphérique. Écrivez l'adresse IP commençante pour la plage permise dans le début du champ de plage. Écrivez l'adresse IP de fin pour la plage permise à la fin de champ de plage.

• Adresse IP simple — Limite l'accès à un périphérique avec une adresse IP simple (par exemple, l'ordinateur que vous utilisez pour accéder au gestionnaire de périphériques). Dans le champ IP Address, écrivez l'adresse IP du PC pour donner des autorisations de gestion à distance.

Étape 4. Introduisez le numéro de port utilisé pour la connexion distante dans le domaine de numéro de port. Le numéro de port 443 est placé par défaut.

Remarque: Si n'importe quel autre numéro de port excepté 443 ou 60443 est configuré, Cisco QuickVPN ne fonctionnera pas.

Étape 5. Cochez la case **SNMP de distant** pour activer le Protocole SNMP (Simple Network Management Protocol) et pour être utilisé à distance pour gérer le périphérique.

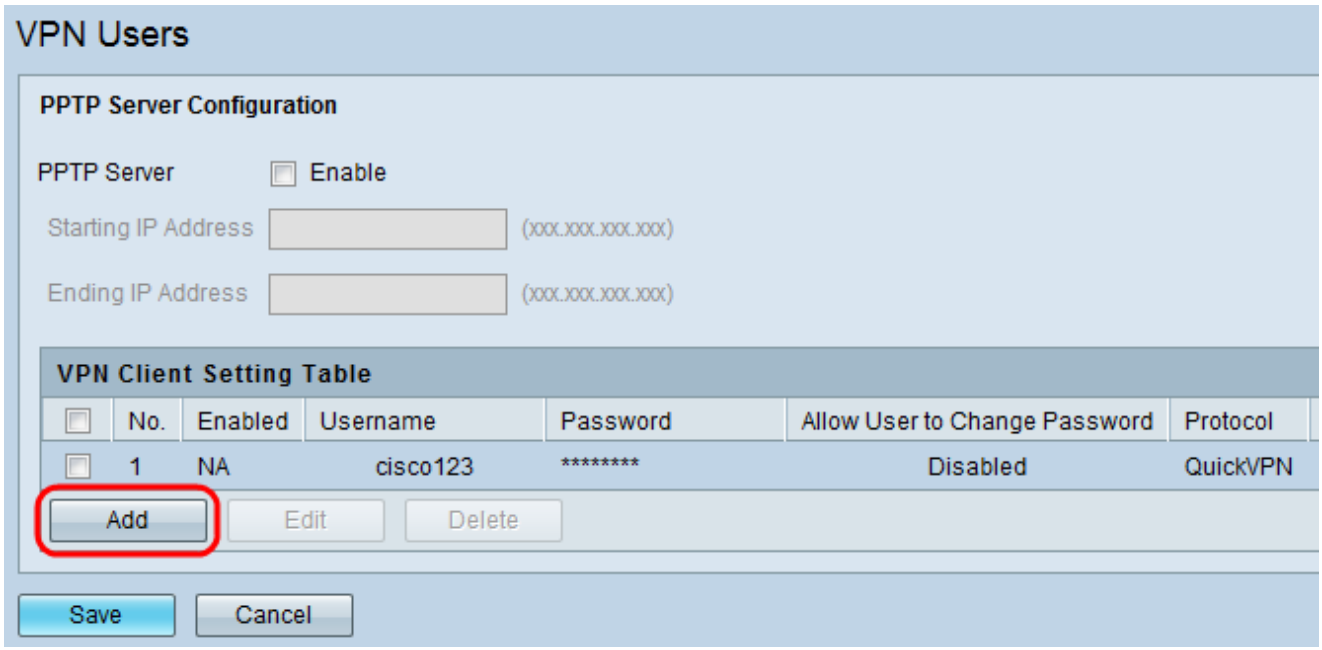
Étape 6. **Sauvegarde de** clic pour appliquer des configurations.

Note: Quand la gestion à distance est activée, le périphérique est accessible à n'importe qui qui connaît son adresse IP. Puisqu'un utilisateur de WAN malveillant peut modifier le périphérique et abuser de lui de plusieurs manières, changez l'administrateur et tous les mots de passe d'invité avant que la caractéristique soit activée.

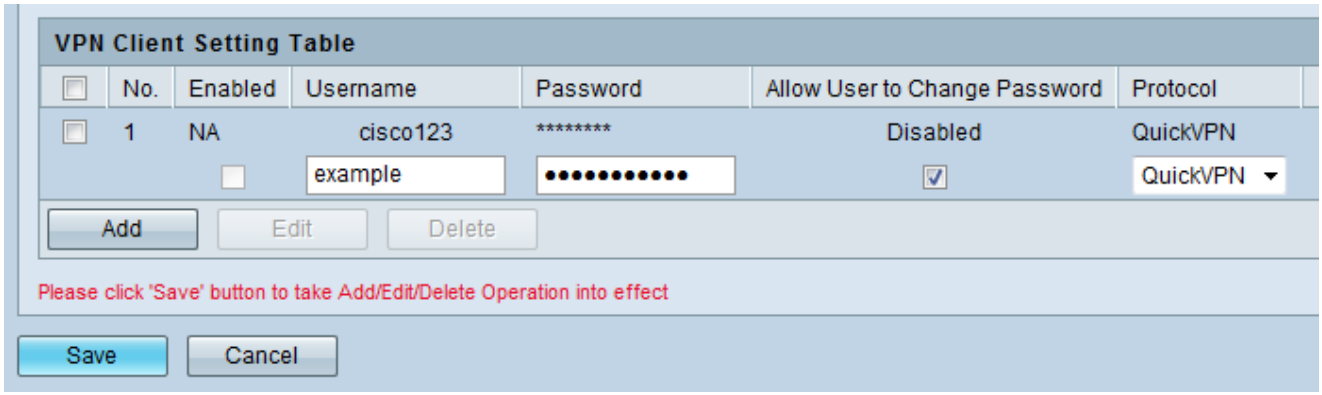
Configuration d'utilisateurs d'IPSec (IPsec)

L'IPSec (IPsec) est une suite de protocole pour sécuriser des Communications IP par l'authentification et le cryptage de chaque paquet IP d'une session de communication. IPsec inclut également des protocoles pour pour établir l'authentification mutuelle entre les agents au début de chaque session et la négociation des clés cryptographiques à utiliser pendant la session.

Étape 1. Ouvrez une session à l'utilitaire de configuration Web et choisissez **VPN > IPsec > utilisateurs VPN**. La page d'*utilisateurs VPN* s'ouvre :



Étape 2. Cliquez sur Add pour ajouter un client dans la table de configuration de client vpn.



Étape 3. Entrez dans le nom d'utilisateur ou l'identifiant unique pour l'utilisateur de XAUTH dans le domaine de nom d'utilisateur.

Étape 4. Entrez le mot de passe dans le domaine de mot de passe.

Étape 5. Cochez l'**utilisateur d'autoriser dans la** case de **Change Password** pour permettre à

l'utilisateur de QuickVPN pour changer ce mot de passe.

Étape 6. Choisissez le type de protocole du menu déroulant de Protocol :

- QuickVPN — Permet à un utilisateur distant pour accéder au périphérique de n'importe quelle autre connexion au réseau local connaissant l'IP address du périphérique.

- PPTP — Permet au Protocol de canalisation en tunnel point-à-point pour accéder au périphérique à distance.

- XAUTH — Permet l'authentification des utilisateurs avec des méthodes en plus de la méthode d'authentification mentionnée dans des paramètres d'IKE SA. Le XAUTH doit être configuré dans un les modes suivants :

  – Aucuns — Ce mode désactive le XAUTH.

  – Le routeur hôte d'IPsec est authentifié par une passerelle distante avec une combinaison de nom d'utilisateur et mot de passe. En ce mode particulier, le routeur agit en tant que client vpn de passerelle distante.

  – Base de données utilisateur — Ce compte utilisateur de mode créé dans le routeur sont utilisés pour authentifier les utilisateurs.