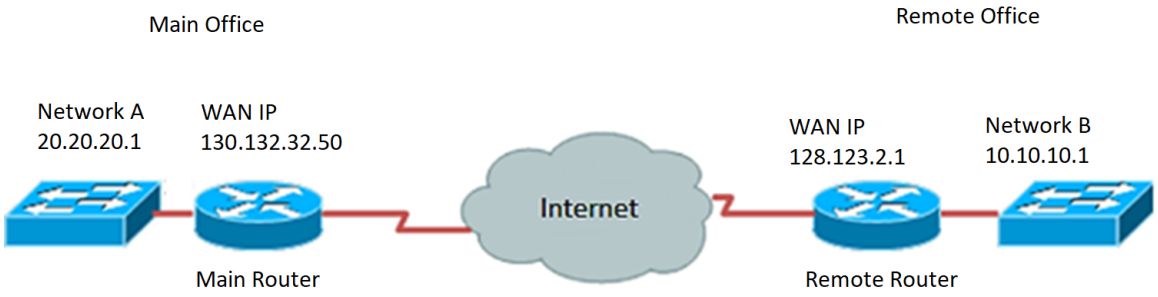
Configuration de la connexion VPN à l'aide de l'Assistant de configuration du routeur de la gamme RV34x

Objectif

Une connexion de réseau privé virtuel (VPN) permet aux utilisateurs d'accéder, d'envoyer et de recevoir des données à destination et en provenance d'un réseau privé en passant par un réseau public ou partagé tel qu'Internet, tout en assurant des connexions sécurisées 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 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.

Le VPN permet à un hôte distant d'agir comme s'il se trouvait sur le même réseau local. Le routeur prend en charge 50 tunnels. L'Assistant de configuration VPN permet de configurer une connexion sécurisée pour le tunnel IPSec site à site. Cette fonctionnalité simplifie la configuration et empêche les paramètres complexes et facultatifs. De cette manière, n'importe qui peut configurer le tunnel IPSec de manière rapide et efficace.



Avantages de l'utilisation d'une connexion VPN :

1. L'utilisation d'une connexion VPN permet de protéger les données et les ressources réseau confidentielles.
2. Fournit la commodité et l'accessibilité pour les travailleurs distants ou les employés d'entreprise, car ils pourront facilement accéder au bureau central sans avoir à être physiquement présents, tout en maintenant la sécurité du réseau privé et de ses ressources.
3. La communication via une connexion VPN offre un niveau de sécurité plus élevé que les autres méthodes de communication à distance. Un niveau de technologie avancé permet aujourd'hui de protéger le réseau privé contre tout accès non autorisé.
4. Les emplacements géographiques réels des utilisateurs sont protégés et ne sont pas exposés aux réseaux publics ou partagés comme Internet.
5. L'ajout de nouveaux utilisateurs ou de nouveaux groupes d'utilisateurs au réseau est facile car les VPN sont très réglables. Il est possible de développer le réseau sans avoir besoin de nouveaux composants supplémentaires ou de configurations

compliquées.

Risques d'utilisation d'une connexion VPN :

1. Risque de sécurité dû 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 hautement expérimenté afin de s'assurer que la sécurité du réseau privé ne sera pas compromise.
2. Fiabilité. Étant donné qu'une connexion VPN nécessite une connexion Internet, il est important de choisir un fournisseur qui a fait ses preuves et qui a été testé pour fournir un excellent service Internet et garantir un temps d'arrêt minimal, voire nul.
3. Évolutivité. S'il est nécessaire d'ajouter une nouvelle infrastructure ou de définir de nouvelles configurations, des problèmes techniques peuvent se poser en raison d'une incompatibilité, en particulier s'il s'agit de produits ou de fournisseurs différents, autres que ceux que vous utilisez déjà.
4. Problèmes de sécurité pour les appareils mobiles. Parfois, lors de l'utilisation d'appareils mobiles lors de l'ouverture de la connexion VPN, des problèmes de sécurité peuvent survenir, en particulier lors de l'utilisation d'une connexion sans fil. Certains fournisseurs non vérifiés se présentent comme “ fournisseurs VPN gratuits ” et peuvent même installer des programmes malveillants sur votre ordinateur. Il est donc possible d'ajouter des mesures de sécurité pour éviter de tels problèmes lors de l'utilisation d'appareils mobiles.
5. Vitesses de connexion lentes. Si vous utilisez un client VPN qui fournit un service VPN gratuit, il est probable que votre vitesse de connexion ralentira car ces fournisseurs ne donnent pas la priorité aux vitesses de connexion.

L'objectif de ce document est de vous montrer comment configurer la connexion VPN sur le routeur de la gamme RV34x à l'aide de l'Assistant de configuration.

Périphériques pertinents

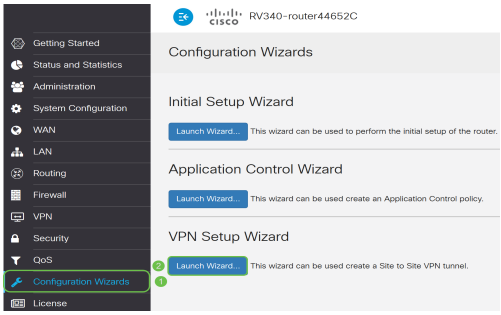
- Gamme RV34x

Version du logiciel

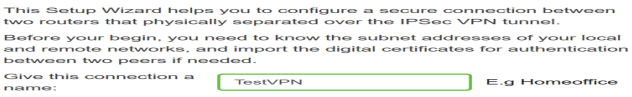
- 1.0.01.16

Configuration de la connexion VPN à l'aide de l'Assistant de configuration

Étape 1. Connectez-vous à l'utilitaire Web du routeur et choisissez **Configuration Wizard**. Cliquez ensuite sur **Launch Wizard** sous *VPN Setup Wizard* section.



Étape 2. Dans le champ fourni, saisissez un nom pour identifier cette connexion.



Note: Dans cet exemple, TestVPN est utilisé.

Étape 3. Dans la zone Interface, cliquez sur le menu déroulant et choisissez l'interface à activer pour cette connexion. Les options sont les suivantes :

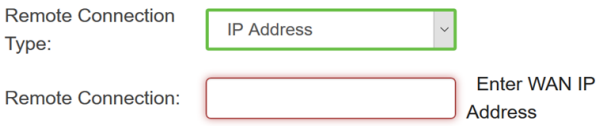
- WAN1
- WAN2
- USB1
- USB2

Note: Dans cet exemple, WAN1 est utilisé.

Étape 4. Cliquez sur **Next** (Suivant).

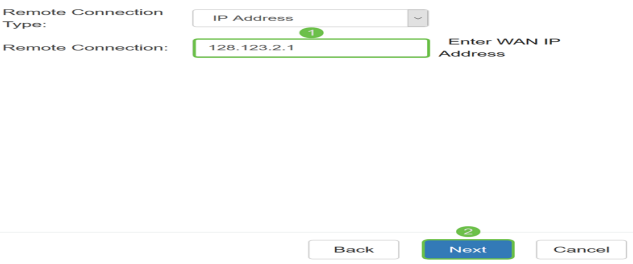
Étape 5. Sélectionnez le type de connexion distante en cliquant sur la flèche de la liste déroulante. Les options sont les suivantes :

- IP Address : sélectionnez cette option si vous souhaitez utiliser l'adresse IP du routeur distant à l'autre extrémité du tunnel VPN.
- FQDN : (Fully Qualified Domain Name) sélectionnez cette option si vous souhaitez utiliser le nom de domaine du routeur distant à l'autre extrémité du tunnel VPN.



Note: Dans cet exemple, l'adresse IP est choisie.

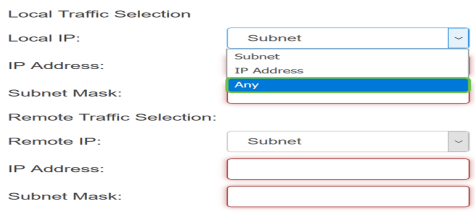
Étape 6. Saisissez l'adresse IP WAN de la connexion distante dans le champ prévu à cet effet, puis cliquez sur **Suivant**.



Note: Dans cet exemple, 128.123.2.1 est utilisé.

Étape 7. Dans la zone Sélection du trafic local, cliquez sur la liste déroulante pour choisir l'adresse IP locale. Les options sont les suivantes :

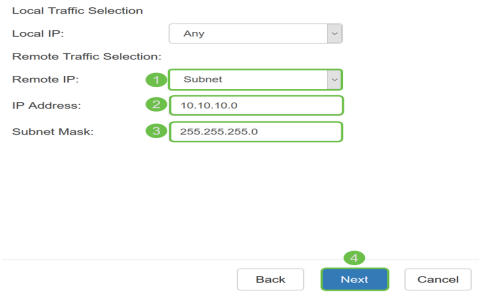
- Subnet : sélectionnez cette option si vous souhaitez saisir l'adresse IP et le masque de sous-réseau du réseau local.
- IP Address : sélectionnez cette option si vous souhaitez saisir uniquement l'adresse IP du réseau local.
- Any : sélectionnez cette option si vous voulez l'un des deux.



Note: Dans cet exemple, Any est sélectionné.

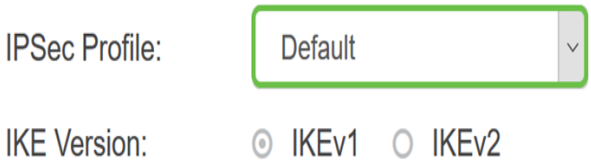
Étape 8. Sous Remote Traffic Selection, cliquez sur la flèche de la liste déroulante pour sélectionner Remote IP. Entrez l'adresse IP distante et le masque de sous-réseau dans le champ fourni, puis cliquez sur **Suivant**. Les options sont les suivantes :

- Subnet : sélectionnez cette option si vous souhaitez saisir l'adresse IP et le masque de sous-réseau du réseau distant.
- IP Address : sélectionnez cette option si vous souhaitez saisir uniquement l'adresse IP du réseau distant.



Note: Dans cet exemple, Subnet est sélectionné. 10.10.10.0 a été entré comme adresse IP et 255.255.255.0 comme masque de sous-réseau.

Étape 9. Cliquez sur la flèche de la liste déroulante de la zone Profil IPSec pour choisir le profil à utiliser.



Note: Dans cet exemple, Default est sélectionné.

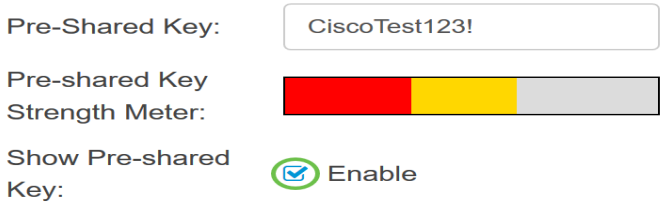
Étape 10. Dans la zone Options de phase 1, saisissez la clé pré-partagée pour cette connexion dans le champ prévu à cet effet. Il s'agit de la clé pré-partagée à utiliser pour authentifier l'homologue IKE (Internet Key Exchange) distant. Les deux extrémités du tunnel VPN doivent utiliser la même clé pré-partagée. Cette clé peut contenir jusqu'à 30 caractères ou valeurs hexadécimales.

Note: Il est vivement conseillé de changer régulièrement la clé pré-partagée pour maintenir la sécurité de votre connexion VPN.

Note: La valeur de la clé prépartagée indique la puissance de la clé que vous avez entrée en fonction des éléments suivants :

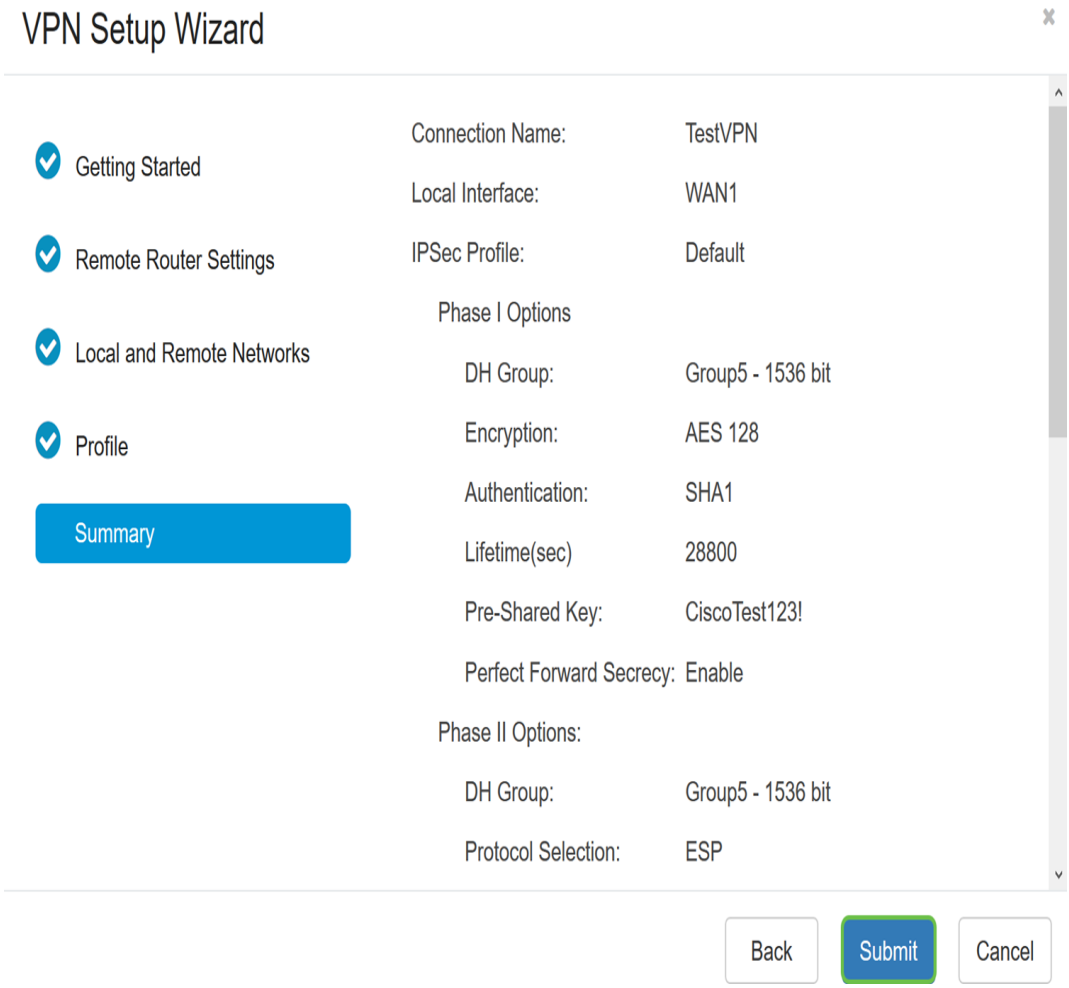
- Rouge : le mot de passe est faible.
- Orange : le mot de passe est assez fort.
- Vert : le mot de passe est fort.

Étape 11. (Facultatif) Vous pouvez également cocher la case **Activer** dans Afficher le texte brut lors de la modification pour afficher le mot de passe en texte brut.



Étape 12. Cliquez sur **Suivant**.  .

Étape 13. La page affiche ensuite tous les détails de configuration de votre connexion VPN. Cliquez sur Submit.



Vous devez maintenant avoir correctement configuré la connexion VPN sur le routeur de la gamme RV34x à l'aide de l'Assistant de configuration. Pour connecter correctement un VPN site à site, vous devez configurer l'Assistant de configuration sur le routeur distant.