

Configuration et utilisation du client VPN IPsec IPsec de TheGreenBow pour la connexion avec les routeurs RV160 et RV260

Objectif

L'objectif de ce document est de configurer et d'utiliser le client VPN IPsec TheGreenBow pour se connecter aux routeurs RV160 et RV260.

Introduction

Une connexion de réseau privé virtuel (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 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 souvent une connexion VPN car il est à la fois utile et nécessaire de permettre à leurs employés d'accéder à leur réseau privé même s'ils se trouvent en dehors du bureau.

Le VPN permet à un hôte distant, ou client, d'agir comme s'ils se trouvaient sur le même réseau local. Le routeur RV160 prend en charge jusqu'à 10 tunnels VPN et le routeur RV260 jusqu'à 20. Une connexion VPN peut être configurée entre le routeur et un point d'extrémité une fois que le routeur a été configuré pour la connexion Internet. Le client VPN dépend entièrement des paramètres du routeur VPN pour établir une connexion. Les paramètres doivent correspondre exactement ou ils ne peuvent pas communiquer.

Le client VPN GreenBow est une application cliente VPN tierce qui permet à un périphérique hôte de configurer une connexion sécurisée pour un tunnel IPsec client à site avec les routeurs des gammes RV160 et RV260.

Avantages de l'utilisation d'une connexion VPN

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

Elle offre commodité et accessibilité aux travailleurs distants ou aux employés d'entreprise, car ils pourront facilement accéder au bureau central sans avoir à être physiquement présents et, pourtant, maintenir la sécurité du réseau privé et de ses ressources.

La communication via une connexion VPN offre un niveau de sécurité plus élevé que les autres méthodes de communication à distance. Un algorithme de chiffrement avancé rend cela possible, protégeant le réseau privé contre les accès non autorisés.

Les emplacements géographiques réels des utilisateurs sont protégés et ne sont pas exposés aux réseaux publics ou partagés comme Internet.

Un VPN permet d'ajouter de nouveaux utilisateurs ou un groupe d'utilisateurs sans avoir à ajouter

de composants supplémentaires ou une configuration compliquée.

Risques d'utilisation d'une connexion VPN

Il peut y avoir des risques de sécurité en raison d'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 soit pas compromise.

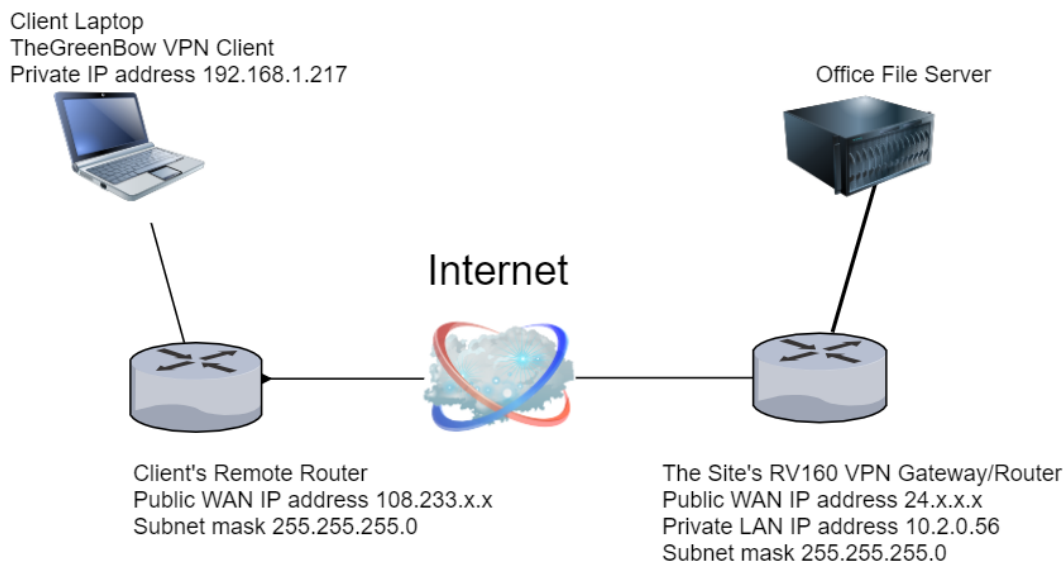
Il est peut-être moins fiable. Étant donné qu'une connexion VPN nécessite une connexion Internet, il est important d'avoir un fournisseur ayant une réputation éprouvée et testée pour fournir un excellent service Internet et garantir un temps d'arrêt minimal voire nul.

Si une situation se produit lorsqu'il est nécessaire d'ajouter une nouvelle infrastructure ou un nouvel ensemble de configurations, des problèmes techniques peuvent survenir en raison de l'incompatibilité, en particulier s'il s'agit de produits ou de fournisseurs différents autres que ceux que vous utilisez déjà.

Des vitesses de connexion lentes peuvent se produire. Si vous utilisez un client VPN qui fournit un service VPN gratuit, il est probable que votre connexion sera également lente car ces fournisseurs ne donnent pas la priorité aux vitesses de connexion. Dans cet article, nous utiliserons un tiers rémunéré qui devrait éliminer ce problème.

Topologie de base du réseau client-site

Il s'agit de la configuration de base du réseau pour la configuration. Les adresses IP WAN publiques ont été partiellement floues ou affichent un x au lieu de chiffres réels pour protéger ce réseau contre les attaques.



Cet article décrit les étapes nécessaires à la configuration du routeur RV160 ou RV260 sur le site pour les éléments suivants :

- Groupe d'utilisateurs — **Utilisateurs de réseau privé virtuel**
- Comptes d'utilisateurs (un ou plusieurs utilisateurs) auxquels l'accès sera autorisé en tant que client
- Un profil IPsec — **TheGreenBow**

- Un profil client-site — **client**
- Vous verrez également comment afficher l'état du VPN sur le site une fois le client connecté

Note: Vous pouvez utiliser n'importe quel nom pour le groupe d'utilisateurs, le profil IPsec et le profil client à site. Les noms listés ne sont que des exemples.

Cet article explique également les étapes que chaque client doit suivre pour configurer le VPN TheGreenBow sur son ordinateur :

- Télécharger et configurer le logiciel client VPN TheGreenBow
- Configurer les paramètres des phases 1 et 2 pour le client
- Démarrer et vérifier une connexion VPN en tant que client

Il est essentiel que chaque paramètre du routeur sur site corresponde aux paramètres du client. Si votre configuration n'aboutit pas à une connexion VPN réussie, vérifiez tous les paramètres pour vous assurer qu'ils correspondent. L'exemple présenté dans cet article n'est qu'une façon de configurer la connexion.

Table des matières

Configuration sur le routeur RV160 ou RV260 sur le site

[Créer un groupe d'utilisateurs](#)

[Créer un compte d'utilisateur](#)

[Configurer le profil IPsec](#)

[Configuration des paramètres des phases 1 et 2](#)

[Créer un profil client-site](#)

Configurer à l'emplacement du client

[Configuration des paramètres de phase 1](#)

[Configuration des paramètres de tunnel](#)

[Démarrer une connexion VPN en tant que client](#)

Vérification de la connectivité sur le RV160 ou le RV260

[Vérifier l'état du VPN sur le site](#)

Périphériques pertinents

- RV160
- RV260

Version du logiciel

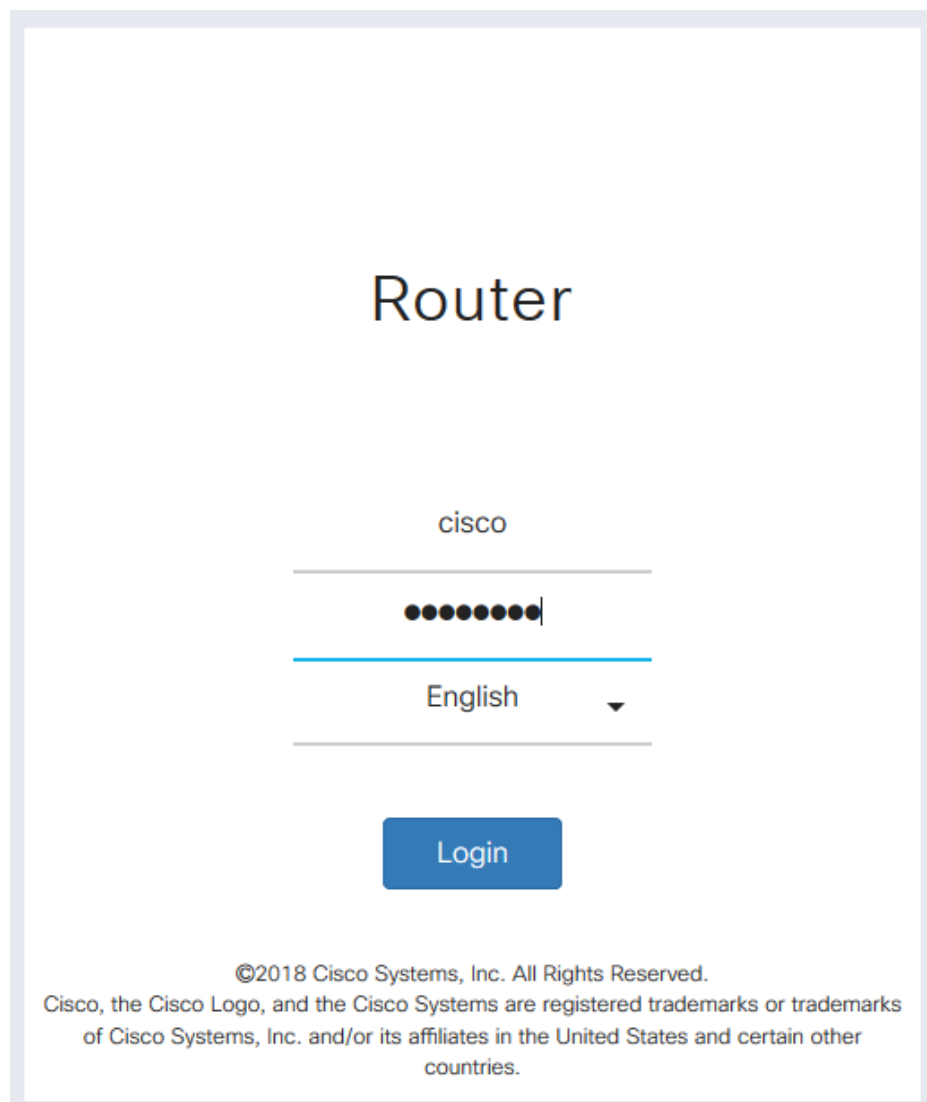
- 1.0.00.15

Configuration du client VPN sur le site sur le routeur RV160 ou RV260

Créer un groupe d'utilisateurs

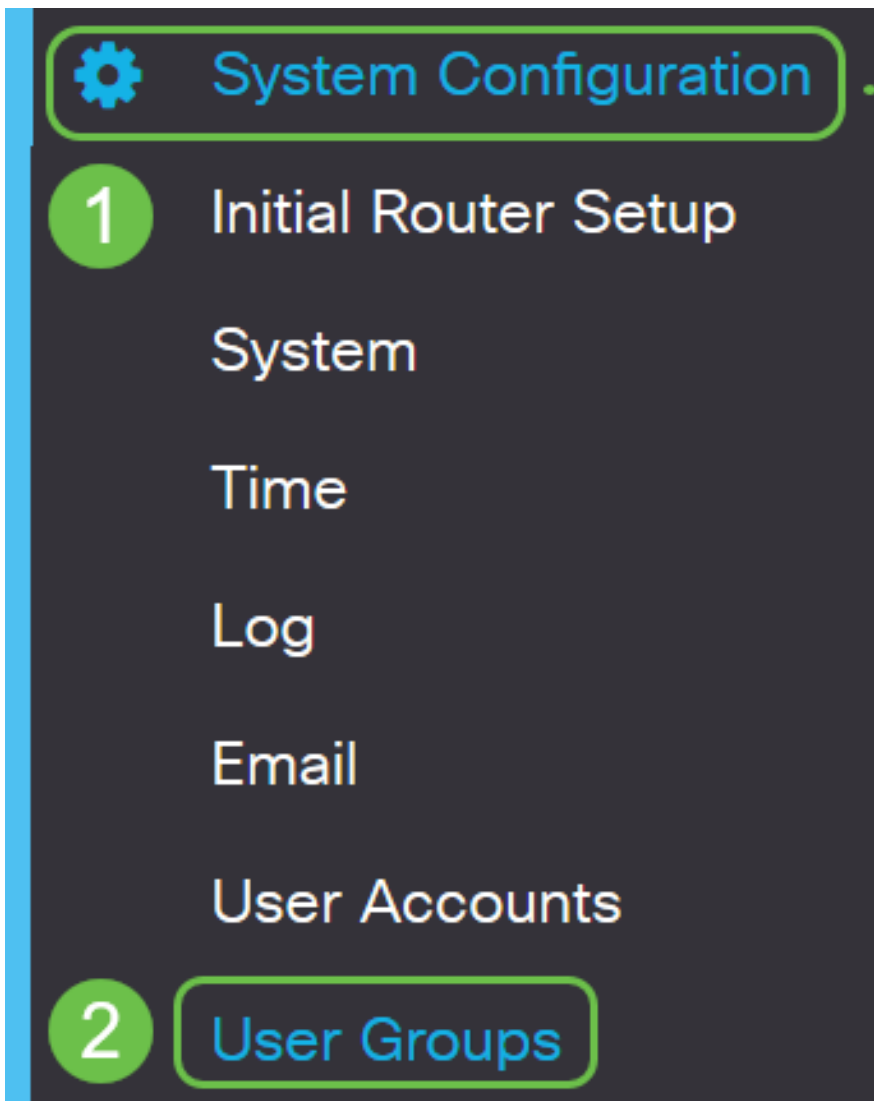
Remarque importante : Laissez le compte d'administrateur par défaut dans le groupe d'administrateurs et créez un nouveau compte d'utilisateur et un nouveau groupe d'utilisateurs pour TheGreenBow. Si vous déplacez votre compte d'administrateur vers un autre groupe, vous vous empêcherez de vous connecter au routeur.

Étape 1. Connectez-vous à l'utilitaire Web du routeur.

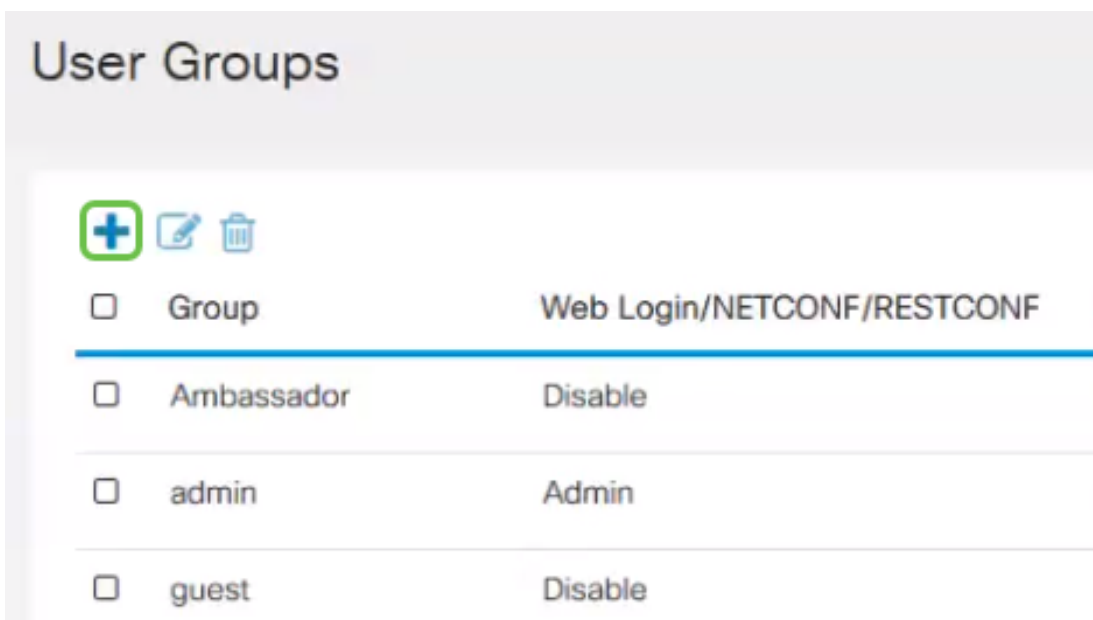


The screenshot shows the Cisco Router Web Utility login interface. At the top, the word "Router" is displayed in a large, dark font. Below it, the word "cisco" is centered. There are two input fields: the first contains the text "cisco" and the second contains a series of ten black dots representing a password. Below the password field is a language selection dropdown menu currently set to "English". A blue "Login" button is positioned below the language menu. At the bottom of the page, there is a copyright notice: "©2018 Cisco Systems, Inc. All Rights Reserved. Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries."

Étape 2. Sélectionnez **Configuration système > Groupes d'utilisateurs**.



Étape 3. Cliquez sur l'icône **plus** pour ajouter un groupe d'utilisateurs.



Étape 4. Dans la zone Vue d'ensemble, saisissez le nom du groupe dans le champ *Nom du groupe*.

User Groups

Group Name:

VPNUsers

Local User Membership List



Étape 5. Sous *Liste des membres des utilisateurs locaux*, cliquez sur l'icône **plus** et sélectionnez l'utilisateur dans la liste déroulante. Pour en ajouter d'autres, appuyez de nouveau sur l'icône **plus** et sélectionnez un autre membre à ajouter. Les membres ne peuvent faire partie que d'un groupe. Si tous les utilisateurs ne sont pas déjà entrés, vous pouvez en ajouter d'autres dans la section [Créer un compte d'utilisateur](#).

Local User Membership List

1



User

<input type="checkbox"/>	1	John <input type="text"/>
<input type="checkbox"/>	2	Kevin <input type="text"/>
<input type="checkbox"/>	3	Teri <input type="text"/>

2

Étape 6. Sous *Services*, choisissez une autorisation à accorder aux utilisateurs du groupe. Les options sont les suivantes :

- Disabled : cette option signifie que les membres du groupe ne sont pas autorisés à accéder à l'utilitaire Web via un navigateur.
- Lecture seule : cette option signifie que les membres du groupe ne peuvent lire l'état du système qu'après leur connexion. Ils ne peuvent modifier aucun des paramètres.
- Admin : cette option donne aux membres du groupe des privilèges de lecture et d'écriture et permet de configurer l'état du système.

Services

Web Login/NETCONF/RESTCONF: Disable Readonly Admin

Étape 7. Cliquez sur l'icône **plus** pour ajouter un VPN client à site existant. Si vous ne l'avez pas configuré, vous trouverez des informations dans cet article sous la section [Créer un profil client-site](#).

Client to Site VPN:



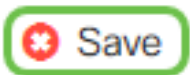
Group Name

1 Client

Étape 8. Cliquez sur Apply.



Étape 9. Click **Save**.



cisco(admin)

English



Étape 10. Cliquez à nouveau sur **Apply** pour enregistrer la configuration en cours dans la configuration initiale.

Configuration Management Apply

Configuration File Name

Last Change Time

Running Configuration: 2019-Jan-29, 17:51:56 UTC

Startup configuration: 2019-Jan-29, 17:52:43 UTC

Mirror Configuration: 2019-Jan-27, 23:00:07 UTC

Backup Configuration: --

Copy/Save Configuration

All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots.

To retain the configuration between reboots, make sure you copy the Running Configuration file to the Startup Configuration file after you have completed all your changes.

Source: Running Configuration

Destination: Startup Configuration

Étape 11. Lorsque vous recevez la confirmation, cliquez sur **OK**.

Information



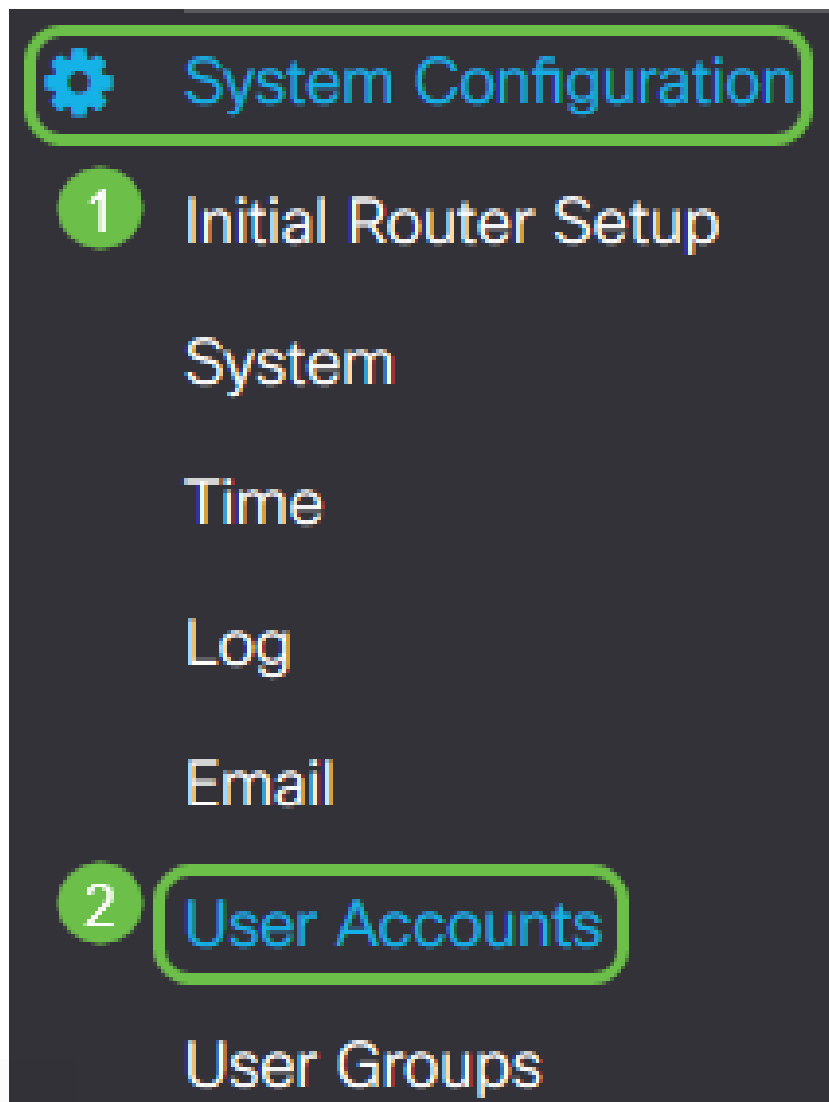
Running configuration saved to startup configuration

OK

Vous devez maintenant avoir créé un groupe d'utilisateurs sur les routeurs de la gamme RV160 ou RV260.

Créer un compte d'utilisateur

Étape 1. Connectez-vous à l'utilitaire Web du routeur et sélectionnez **Configuration système > Comptes d'utilisateurs**.



Étape 2. Dans la zone *Utilisateurs locaux*, cliquez sur l'icône **Ajouter**.

Local Users



Username

John


Kevin

Teri

cisco

Étape 3. Entrez un nom pour l'utilisateur dans le champ *Nom d'utilisateur*, le mot de passe et le groupe auquel vous voulez ajouter l'utilisateur dans le menu déroulant. Cliquez sur Apply.

Add user account

 The current minimum requirements are as follows

* Minimal Password Length: 8

* Minimal Number of Character Classes: 3

Username:

1

Dave

New Password:

2

●●●●●●●●

Confirm Password:

3

●●●●●●●●

Password Strength meter:



Group:

4

VPNUsers

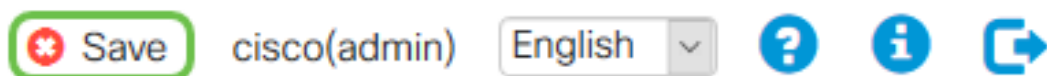
5

Apply

Cancel

Note: Lorsque le client configure TheGreenBow Client sur son ordinateur, il se connecte avec le même nom d'utilisateur et mot de passe.

Étape 4. Cliquez sur **Save**.



Étape 5. Cliquez à nouveau sur **Apply** pour enregistrer la configuration en cours dans la configuration initiale.

Configuration Management Apply

Configuration File Name

Last Change Time

Running Configuration: 2019-Jan-29, 17:51:56 UTC

Startup configuration: 2019-Jan-29, 17:52:43 UTC

Mirror Configuration: 2019-Jan-27, 23:00:07 UTC

Backup Configuration: --

Copy/Save Configuration

All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots.

To retain the configuration between reboots, make sure you copy the Running Configuration file to the Startup Configuration file after you have completed all your changes.

Source:

Destination:

Étape 6. Lorsque vous recevez la confirmation, cliquez sur **OK**.

Information ×

 Running configuration saved to startup configuration

OK

Vous devez maintenant avoir créé un compte d'utilisateur sur votre routeur RV160 ou RV260.

Configurer le profil IPsec

Étape 1. Connectez-vous à l'utilitaire Web du routeur RV160 ou RV260 et choisissez **VPN > IPsec VPN > Profils IPsec**.



Étape 2. Le tableau Profils IPsec affiche les profils existants. Cliquez sur l'icône **plus** pour créer un nouveau profil.

IPSec Profiles



Name

Default

Amazon_Web_Services

Microsoft_Azure

VPNTTest

Note: Amazon_Web_Services, Default et Microsoft_Azure sont des profils par défaut.

Étape 3. Créez un nom pour le profil dans le champ *Nom du profil*. Le nom du profil ne doit contenir que des caractères alphanumériques et un trait de soulignement (_) pour les caractères spéciaux.

Add/Edit a New IPSec Profile

Profile Name:

TheGreenBow

Keying Mode:

Auto Manual

IKE Version:

IKEv1 IKEv2

Étape 4. Cliquez sur une case d'option pour déterminer la méthode d'échange de clés que le profil utilisera pour s'authentifier. Les options sont les suivantes :

- Auto : les paramètres de stratégie sont définis automatiquement. Cette option utilise une stratégie IKE (Internet Key Exchange) pour l'intégrité des données et les échanges de

clés de chiffrement. Si cette option est sélectionnée, les paramètres de configuration de la zone Paramètres de stratégie automatique sont activés.

- **Manual** : cette option vous permet de configurer manuellement les clés pour le chiffrement des données et l'intégrité du tunnel VPN. Si cette option est sélectionnée, les paramètres de configuration de la zone Manual Policy Parameters sont activés. Cette méthode n'est pas très répandue.

Add/Edit a New IPSec Profile

Profile Name:

Keying Mode: Auto Manual

IKE Version: IKEv1 IKEv2

Note: Pour cet exemple, **Auto** a été choisi.

Étape 5. Sélectionnez la version IKE. Lorsque vous configurez TheGreenBow côté client, la même version est sélectionnée.

Add/Edit a New IPSec Profile

Profile Name:

Keying Mode: Auto Manual

IKE Version: IKEv1 IKEv2

Configuration des paramètres des phases 1 et 2

Étape 1. Dans la zone Options de phase 1, sélectionnez le groupe Diffie-Hellman (DH) approprié à utiliser avec la clé de phase 1 dans la liste déroulante *Groupe DH*. Diffie-Hellman est un protocole d'échange de clés cryptographiques utilisé dans la connexion pour échanger des ensembles de clés pré-partagés. La force de l'algorithme est déterminée par des bits. Les options sont les suivantes :

- **Group2-1024 bit** : cette option calcule la clé plus lentement, mais elle est plus sécurisée que le groupe 1.
- **Group5-1536 bit** : cette option calcule la clé la plus lente, mais la plus sécurisée.

Phase I Options

DH Group:

Group2 - 1024 bit

Encryption:

3DES

Authentication:

MD5

SA Lifetime:

28800

Étape 2. Dans la liste déroulante *Encryption*, choisissez une méthode de chiffrement pour chiffrer et déchiffrer les données utiles de sécurité encapsulante (ESP) et l'Association de sécurité Internet et le protocole ISAKMP (Key Management Protocol). Les options sont les suivantes :

- 3DES - Triple Data Encryption Standard. Non recommandé. Ne l'utilisez que si elle est nécessaire pour la compatibilité descendante car elle est vulnérable à certaines attaques " de collision " .
- AES-128 — Advanced Encryption Standard utilise une clé de 128 bits. La norme AES (Advanced Encryption Standard) est un algorithme cryptographique conçu pour être plus sécurisé que DES. AES utilise une taille de clé plus grande qui garantit que la seule approche connue pour déchiffrer un message est qu'un intrus tente toutes les clés possibles.
- AES-192 — Advanced Encryption Standard utilise une clé 192 bits.
- AES-256 — Advanced Encryption Standard utilise une clé de 256 bits. Il s'agit de l'option de cryptage la plus sécurisée.

Phase I Options

DH Group:

Group2 - 1024 bit

Encryption:

AES-128

Authentication:

MD5

SA Lifetime:

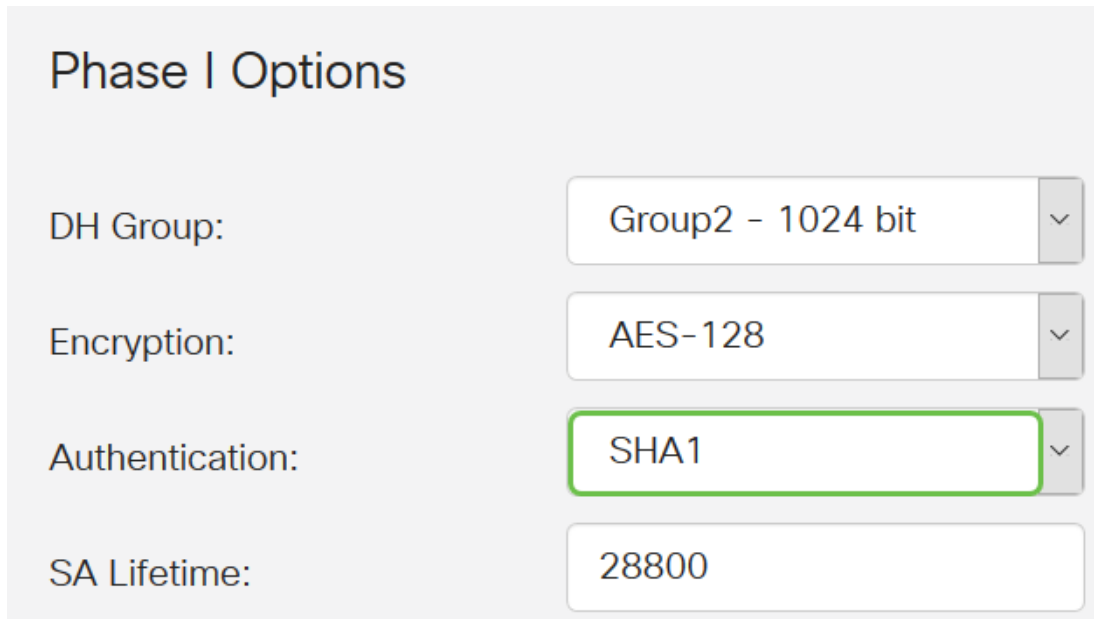
28800

Note: AES est la méthode standard de cryptage sur DES et 3DES pour ses performances et sa sécurité accrues. Le renforcement de la clé AES augmentera la sécurité en réduisant les performances.

Étape 3. Dans la liste déroulante *Authentification*, choisissez une méthode d'authentification qui déterminera comment ESP et ISAKMP sont authentifiés. Les options sont les suivantes :

- MD5 — L'algorithme Message-Digest a une valeur de hachage de 128 bits.
- SHA-1 — L'algorithme de hachage sécurisé a une valeur de hachage de 160 bits.
- SHA2-256 — Algorithme de hachage sécurisé avec une valeur de hachage de 256 bits.
Il s'agit de l'algorithme le plus sécurisé et recommandé.

Note: Assurez-vous que les deux extrémités du tunnel VPN utilisent la même méthode d'authentification.



Phase I Options

DH Group: Group2 - 1024 bit

Encryption: AES-128

Authentication: SHA1

SA Lifetime: 28800

Note: MD5 et SHA sont deux fonctions de hachage cryptographique. Ils prennent une donnée, la compactent et créent une sortie hexadécimale unique qui ne peut généralement pas être reproduite. Dans cet exemple, SHA1 est sélectionné.

Étape 4. Dans le champ *Durée de vie de la SA*, saisissez une valeur comprise entre 120 et 86 400. La valeur par défaut est 28800. Le *SA Lifetime (Sec)* vous indique la durée, en secondes, pendant laquelle une SA IKE est active dans cette phase. Une nouvelle association de sécurité (SA) est négociée avant l'expiration de la durée de vie afin de s'assurer qu'une nouvelle association de sécurité est prête à être utilisée lorsque l'ancienne expire. La valeur par défaut est 28800 et la plage est comprise entre 120 et 86400. Nous utiliserons 28800 secondes comme durée de vie SA pour la phase I.

Note: Il est recommandé que votre durée de vie de SA dans la phase I soit plus longue que votre durée de vie de SA de phase II. Si vous raccourcissez la phase I par rapport à la phase II, vous devrez renégocier le tunnel d'un point à l'autre fréquemment, par opposition au tunnel de données. Le tunnel de données est ce qui a besoin de plus de sécurité. Il est donc préférable que la durée de vie de la phase II soit plus courte que celle de la phase I.

Phase I Options

DH Group:

Group2 - 1024 bit

Encryption:

AES-128

Authentication:

SHA1

SA Lifetime:

28800

Étape 5. Dans la liste déroulante *Sélection de protocole* de la zone Options de phase II, sélectionnez un type de protocole à appliquer à la deuxième phase de la négociation. Les options sont les suivantes :

- ESP - Cette option est également appelée Encapsulating Security Payload. Cette option encapsule les données à protéger. Si cette option est sélectionnée, passez à l'étape 6 pour choisir une méthode de cryptage.
- AH : cette option est également appelée en-tête d'authentification (AH). Il s'agit d'un protocole de sécurité qui fournit une authentification des données et un service anti-relecture en option. AH est incorporé dans le datagramme IP à protéger. Si cette option est sélectionnée, passez à l'étape 7.

Phase II Options

Protocol Selection:

ESP

Encryption:

3DES

Authentication:

MD5

SA Lifetime:

3600

Perfect Forward Secrecy:

Enable

DH Group:

Group2 - 1024 bit

Étape 6. Si ESP a été sélectionné à l'étape 6, sélectionnez un *chiffrement*. Les options sont les suivantes :

- 3DES - Triple Data Encryption Standard
- AES-128 — Advanced Encryption Standard utilise une clé de 128 bits.
- AES-192 — Advanced Encryption Standard utilise une clé 192 bits.
- AES-256 — Advanced Encryption Standard utilise une clé de 256 bits.

Phase II Options

Protocol Selection:	ESP
Encryption:	AES-128
Authentication:	MD5
SA Lifetime:	3600
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable
DH Group:	Group2 - 1024 bit

Étape 7. Dans la liste déroulante *Authentication*, choisissez une méthode d'authentification qui déterminera comment ESP et ISAKMP sont authentifiés. Les options sont les suivantes :

- MD5 — L'algorithme Message-Digest a une valeur de hachage de 128 bits.
- SHA-1 — L'algorithme de hachage sécurisé a une valeur de hachage de 160 bits.
- SHA2-256 — Algorithme de hachage sécurisé avec une valeur de hachage de 256 bits.

Phase II Options

Protocol Selection:	ESP
Encryption:	AES-128
Authentication:	SHA1
SA Lifetime:	3600
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable
DH Group:	Group2 - 1024 bit

Étape 8. Dans le champ *Durée de vie de la SA*, saisissez une valeur comprise entre 120 et 28 800. Il s'agit de la durée pendant laquelle l'association de sécurité IKE restera active dans cette phase. La valeur par défaut est 3600.

Phase II Options

Protocol Selection:	ESP
Encryption:	AES-128
Authentication:	SHA1
SA Lifetime:	3600

Étape 9. (Facultatif) Cochez la case **Activer** Perfect Forward Secrecy pour générer une nouvelle clé pour le chiffrement et l'authentification du trafic IPsec. Perfect Forward Secrecy est utilisé pour améliorer la sécurité des communications transmises sur Internet à l'aide de la cryptographie à clé publique. Cochez cette case pour activer cette fonctionnalité ou décochez-la pour la désactiver. Cette fonction est recommandée.

Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable
DH Group:	Group2 - 1024 bit

Étape 10. Dans la liste déroulante *Groupe DH*, choisissez un groupe DH à utiliser avec la clé dans la phase 2. Les options sont les suivantes :

- Group2-1024 bit : cette option calcule la clé plus rapidement, mais elle est moins sécurisée.
- Group5-1536 bit : cette option calcule la clé la plus lente, mais la plus sécurisée.

Phase II Options

Protocol Selection: ESP

Encryption: AES-128

Authentication: SHA1

SA Lifetime: 3600

Perfect Forward Secrecy: Enable

DH Group: Group2 - 1024 bit


Étape 11. Cliquez sur Apply.

Apply Cancel

Étape 12. Cliquez sur **Enregistrer** pour enregistrer la configuration de manière permanente.

cisco(admin) English ? i

Étape 13. Cliquez à nouveau sur **Apply** pour enregistrer la configuration en cours dans la configuration initiale.

Configuration Management 

Configuration File Name

Last Change Time

Running Configuration: 2019-Jan-29, 17:51:56 UTC

Startup configuration: 2019-Jan-29, 17:52:43 UTC

Mirror Configuration: 2019-Jan-27, 23:00:07 UTC

Backup Configuration: --

Copy/Save Configuration


All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots.

To retain the configuration between reboots, make sure you copy the Running Configuration file to the Startup Configuration file after you have completed all your changes.

Source:

Destination:

Étape 14. Lorsque vous recevez la confirmation, cliquez sur **OK**.

Configuration Management 

Configuration File Name

Last Change Time

Running Configuration: 2019-Jan-29, 17:51:56 UTC

Startup configuration: 2019-Jan-29, 17:52:43 UTC

Mirror Configuration: 2019-Jan-27, 23:00:07 UTC

Backup Configuration: --

Copy/Save Configuration

All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots.

To retain the configuration between reboots, make sure you copy the Running Configuration file to the Startup Configuration file after you have completed all your changes.

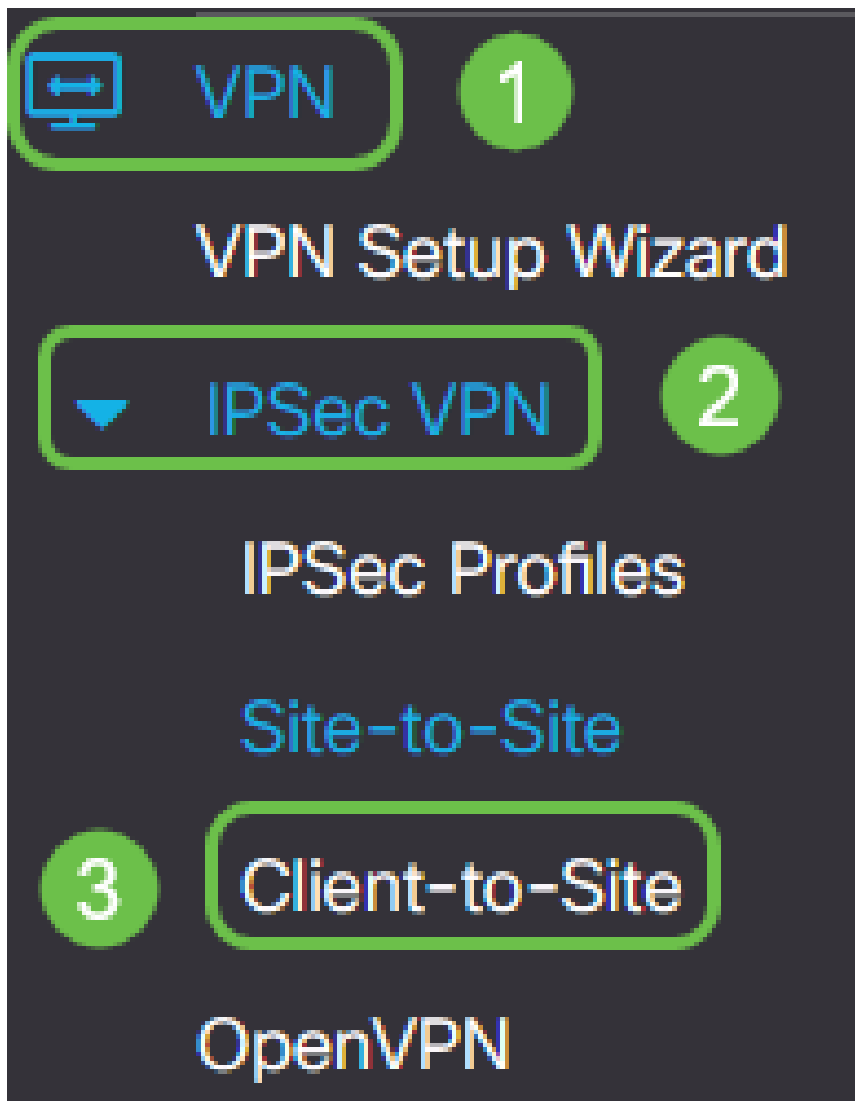
Source:

Destination:

Vous devez maintenant avoir correctement configuré un profil IPsec sur votre routeur RV160 ou RV260.

Créer un profil client-site

Étape 1. Choisissez **VPN > IPSec VPN > Client-to-Site** .



Étape 2. Cliquez sur l'icône plus.

IPSec Profiles		
<input type="checkbox"/> Name	Policy	IKE Version
<input type="checkbox"/> Default	Auto	IKEv1
<input type="checkbox"/> Amazon_Web_Services	Auto	IKEv1
<input type="checkbox"/> Microsoft_Azure	Auto	IKEv1

Étape 3. Sous l'onglet Basic Settings (Paramètres de base), cochez la case **Enable (Activer)** pour vous assurer que le profil VPN est actif.

Add/Edit a New Tunnel

Basic Settings

Advanced Settings

Enable:



Tunnel Name:

Étape 4. Entrez un nom pour la connexion VPN dans le champ *Tunnel Name*.

Basic Settings

Advanced Settings

Enable:



Tunnel Name:

IPSec Profile:

(Auto Profile (IKEv1) is chosen.)

⚠ Configure higher lifetimes if this profile is used for Windows Clients.

Interface:

Étape 5. Sélectionnez le profil IPsec à utiliser dans la liste déroulante *IPsec*.

Basic Settings

Advanced Settings

Enable:



Tunnel Name:

IPSec Profile:

(Auto Profile (IKEv1) is chosen.)

⚠ Configure higher lifetimes if this profile is used for Windows Clients.

Interface:

Étape 6. Choisissez Interface dans la liste déroulante *Interface*.

Basic Settings

Advanced Settings

Enable:



Tunnel Name:

IPSec Profile:

(Auto Profile (IKEv1) is chosen.)

⚠ Configure higher lifetimes if this profile is used for Windows Clients.

Interface:

Note: Les options dépendent du modèle de routeur que vous utilisez. Dans cet exemple, le WAN est choisi.

Étape 7. Sélectionnez une méthode d'authentification IKE. Les options sont les suivantes :

- Pre-shared Key : cette option nous permet d'utiliser un mot de passe partagé pour la

connexion VPN.

- **Certificate** : cette option utilise un certificat numérique qui contient des informations telles que le nom, ou l'adresse IP, le numéro de série, la date d'expiration du certificat et une copie de la clé publique du titulaire du certificat.

IKE Authentication Method

Pre-shared Key:

Please enter a valid Preshared Key.

Show Pre-shared Key: Enable

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Certificate:

Note: Une clé pré-partagée peut être ce que vous voulez qu'elle soit, elle doit juste correspondre sur le site et avec le client lorsqu'ils configurent le client TheGreenBow sur leur ordinateur.

Étape 8. Entrez le mot de passe de connexion dans le champ *Clé prépartagée*.

IKE Authentication Method

Pre-shared Key:

Show Pre-shared Key: Enable

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Certificate:

Étape 9. (Facultatif) Décochez la case *Complexité minimale de clé prépartagée Activer* pour pouvoir utiliser un mot de passe simple.

IKE Authentication Method

Pre-shared Key:

Show Pre-shared Key: Enable

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Certificate:

Note: Dans cet exemple, la Complexité de clé prépartagée minimale reste activée.

Étape 10. (Facultatif) Cochez la case *Afficher la clé prépartagée Activer* pour afficher le mot de passe en texte clair.

si vous rencontrez des problèmes de connexion après une configuration réussie, il peut s'agir d'une zone à vérifier et à modifier à la fois sur le client et sur le site.

Local Identifier:

Remote Identifier: **1** **2**

Étape 13. (Facultatif) Cochez la case **Authentification étendue** pour activer la fonction. Lorsqu'elle est activée, cette option fournit un niveau d'authentification supplémentaire qui nécessite que les utilisateurs distants saisissent leurs informations d'identification avant d'obtenir l'accès au VPN.

Extended Authentication +

Group Name

Étape 14. (Facultatif) Choisissez le groupe qui utilisera l'authentification étendue en cliquant sur l'icône **plus** et sélectionnez l'utilisateur dans la liste déroulante.

Extended Authentication **1** +

Group Name

CiscoTest123

KevGroupTest

VPNUsers **2**

Note: Dans cet exemple, **VPNUsers** est sélectionné.

Étape 15. Sous *Pool Range for Client LAN*, saisissez la première adresse IP et l'adresse IP de fin pouvant être attribuées à un client VPN. Il doit s'agir d'un pool d'adresses qui ne se chevauchent pas avec les adresses de site. Ces interfaces peuvent être appelées interfaces virtuelles. Si vous recevez un message indiquant qu'une interface virtuelle doit être modifiée, c'est là que vous corrigerez cette situation.

Pool Range for Client LAN:

Start IP: **1**

End IP: **2**

Étape 16. Sélectionnez l'onglet **Paramètres avancés**.

Basic Settings

Advanced Settings

Étape 17. (Facultatif) Faites défiler la page vers le bas et sélectionnez **Mode agressif**. La fonctionnalité Mode agressif vous permet de spécifier des attributs de tunnel RADIUS pour un homologue de sécurité IP (IPsec) et d'initier une négociation de mode agressif IKE (Internet Key Exchange) avec le tunnel. Pour plus d'informations sur le mode agressif par rapport au mode principal, cliquez [ici](#).

Additional Settings

Aggressive Mode

Compress (Support IP Payload Compression Protocol (IPComp))

Note: La case à cocher Compresser permet au routeur de proposer la compression lorsqu'il démarre une connexion. Ce protocole réduit la taille des datagrammes IP. Si le répondeur rejette cette proposition, le routeur n'implémente pas la compression. Lorsque le routeur est le répondeur, il accepte la compression, même si la compression n'est pas activée. Si vous activez cette fonctionnalité pour ce routeur, vous devez l'activer sur le routeur distant (l'autre extrémité du tunnel). Dans cet exemple, *Compress* n'a pas été coché.

Étape 18. Cliquez sur Apply.

Apply

Cancel

Étape 19. Cliquez sur **Save**.

 Save

cisco(admin)

English



Étape 20. Cliquez à nouveau sur **Apply** pour enregistrer la configuration en cours dans la configuration initiale.

Configuration Management 

Configuration File Name

Last Change Time

Running Configuration: 2019-Jan-29, 17:51:56 UTC

Startup configuration: 2019-Jan-29, 17:52:43 UTC

Mirror Configuration: 2019-Jan-27, 23:00:07 UTC

Backup Configuration: --

Copy/Save Configuration

All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots.

To retain the configuration between reboots, make sure you copy the Running Configuration file to the Startup Configuration file after you have completed all your changes.

Source:

Destination:

Étape 21. Lorsque vous recevez la confirmation, cliquez sur **OK**.

Information

 Running configuration saved to startup configuration



Vous devez maintenant avoir configuré le tunnel client-à-site sur le routeur pour le client VPN TheGreenBow.

Configurer le client VPN GreenBow sur l'ordinateur du télétravailleur

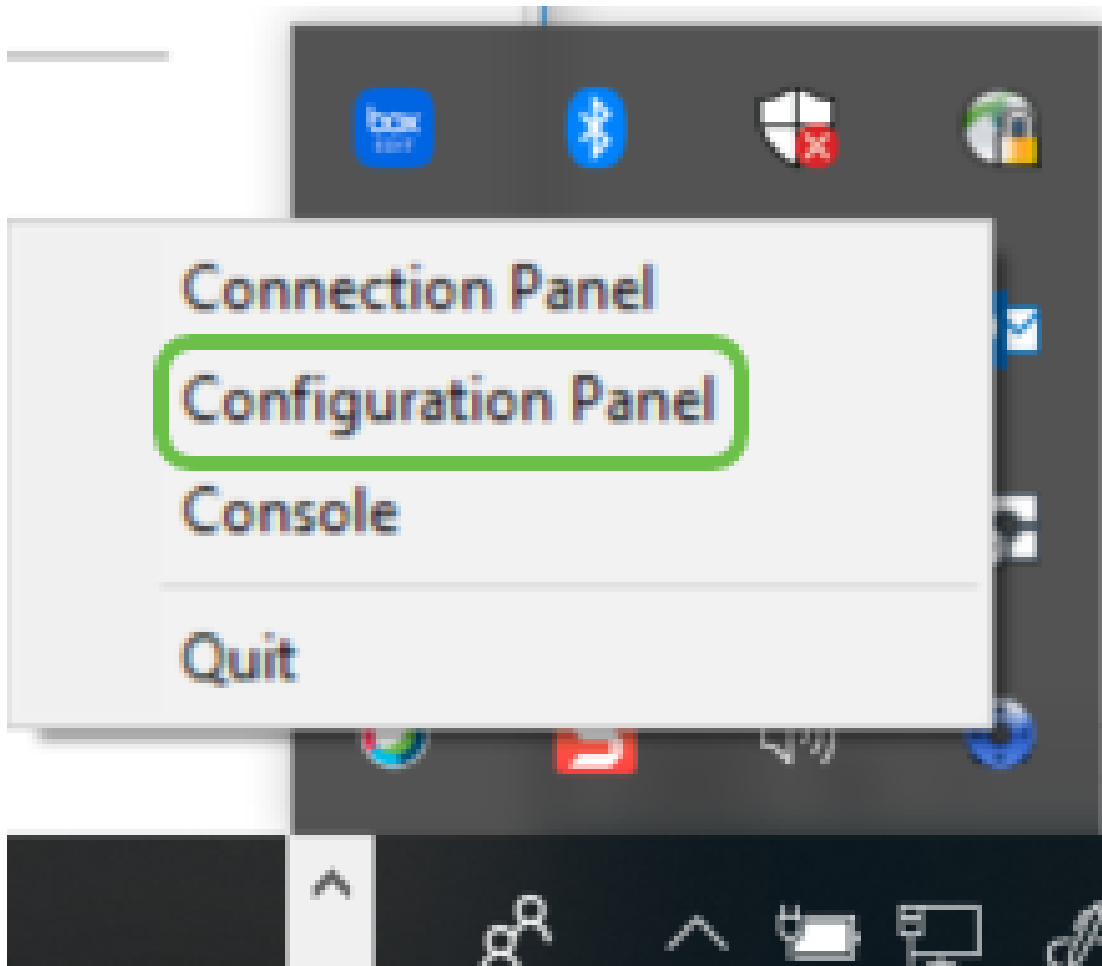
Configuration des paramètres de phase 1

Pour télécharger la dernière version du logiciel client VPN IPsec de TheGreenBow, cliquez [ici](#).

Étape 1. Cliquez avec le bouton droit sur l'icône Client VPN TheGreenBow. Elle se trouve dans le coin inférieur droit de la barre des tâches.



Étape 2. Sélectionnez **Panneau de configuration**.



Note: Ceci est un exemple sur un ordinateur Windows. Cela peut varier en fonction du logiciel que vous utilisez.

Étape 3. Sélectionnez **Assistant de création de tunnel IPsec IKE V1**.



Note: Dans cet exemple, IKE Version 1 est en cours de configuration. Si vous souhaitez configurer IKE Version 2, suivez les mêmes étapes, mais cliquez avec le bouton droit sur le dossier IKE V2. Vous devez également sélectionner IKEv2 pour le profil IPsec sur le routeur du site.

Étape 4. Indiquez l'adresse IP WAN publique du routeur sur le site (bureau) où se trouve le serveur de fichiers, la clé pré-partagée et l'adresse interne privée du réseau distant sur le site. Cliquez sur **Next** (Suivant). Dans cet exemple, le site est 24.x.x.x. Les trois derniers octets (ensembles de nombres dans cette adresse IP) ont été remplacés par un x pour protéger ce réseau. Saisissez l'adresse IP complète.

VPN Configuration Wizard ×

VPN tunnel parameters 2/3

Enter the following parameters for the VPN tunnel:

IP or DNS public (external) address: 1

Preshared key: 2

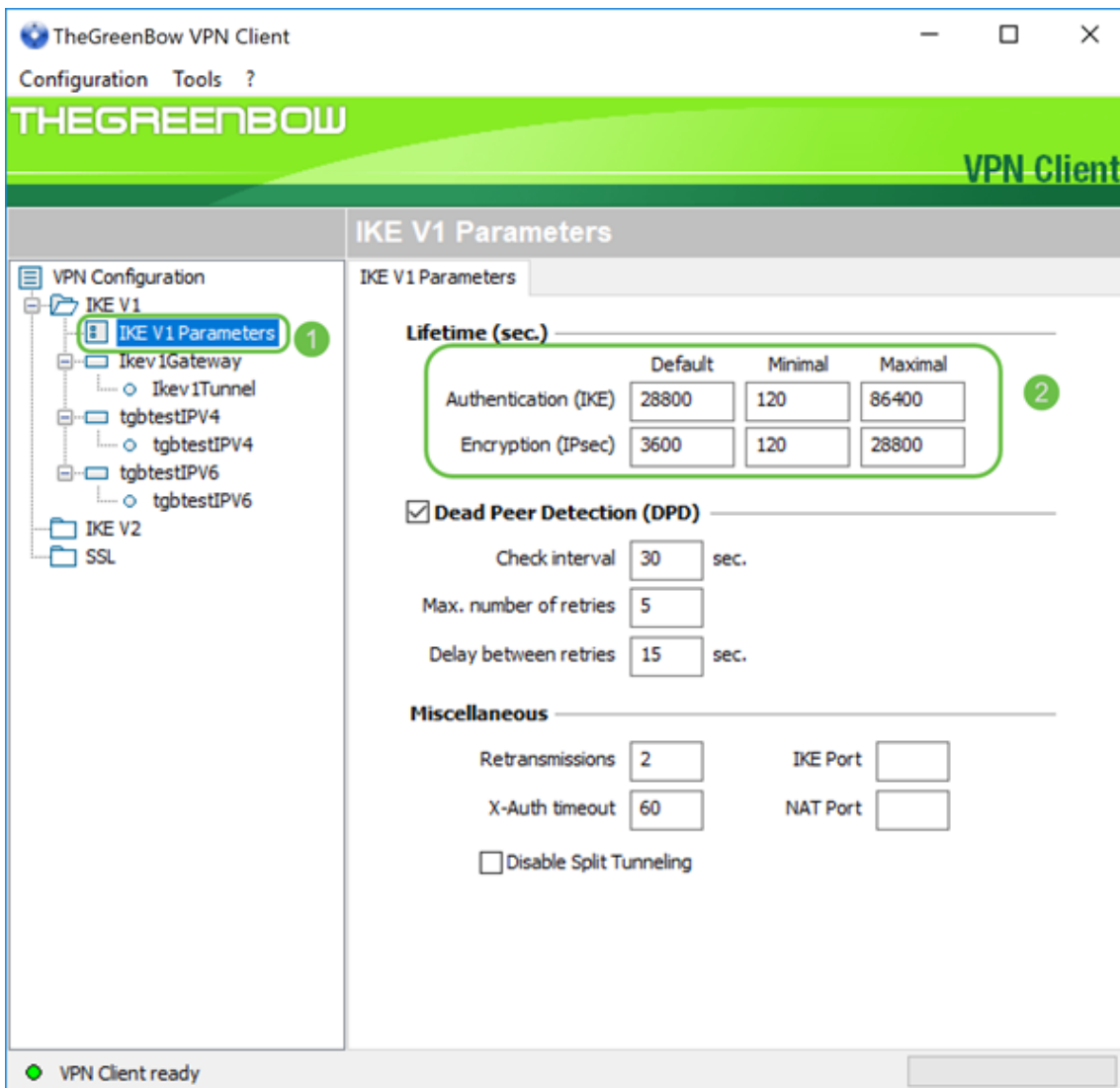
IP private (internal) address: 3

4

Étape 5. Cliquez sur **Finish**.

You may change these parameters anytime directly with the main interface.

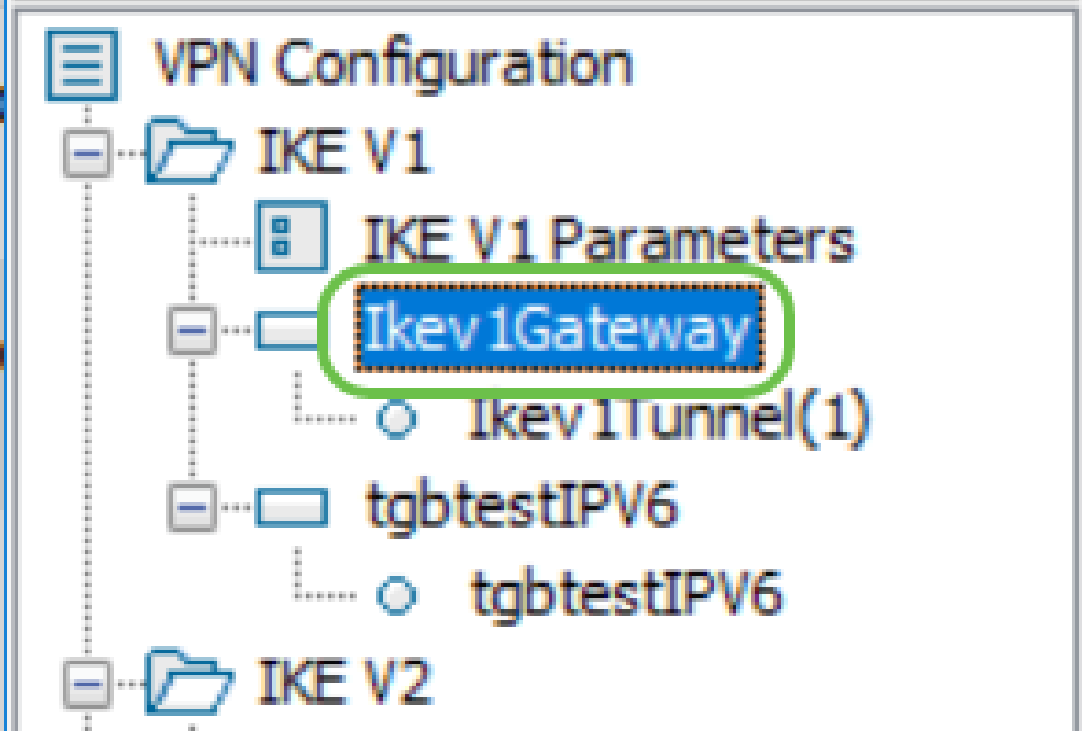
Étape 6 (Facultatif) Vous pouvez modifier les paramètres IKE V1. La durée de vie par défaut, minimale et maximale de GreenBow peut être ajustée. À cet emplacement, vous pouvez entrer la plage de la durée de vie que le routeur accepte.



Étape 7. Cliquez sur la passerelle que vous avez créée.

Configuration Tools ?

THEGREENBOW



Étape 8. Dans l'onglet *Authentication* sous *Adresses*, une liste déroulante d'adresses locales s'affiche. Vous pouvez en choisir un ou sélectionner **Any**, comme indiqué ci-dessous.

Configuration Tools ?

THEGREENBOW

VPN

Ikev1Gateway: Authentication

Authentication | Advanced | Certificate

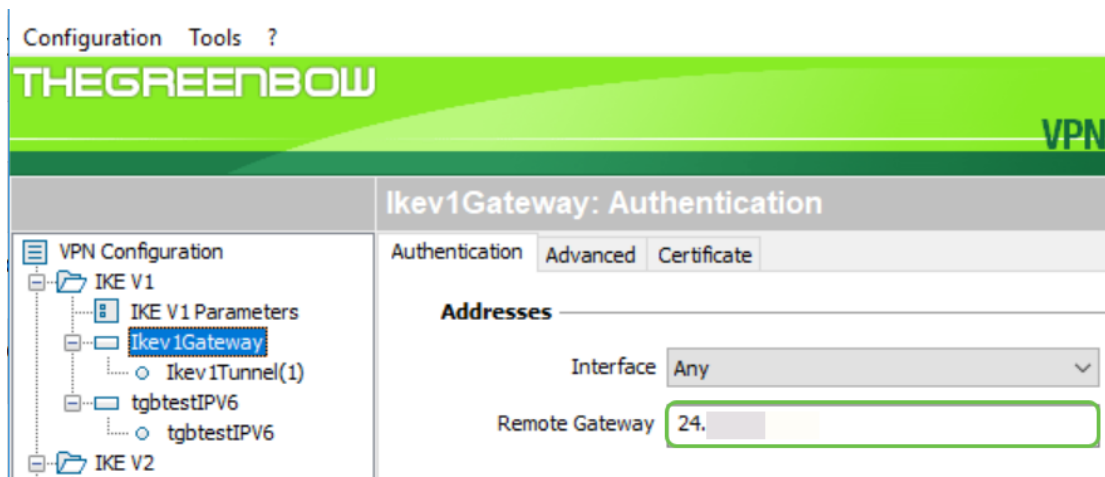
Addresses

Interface: Any

Remote Gateway:

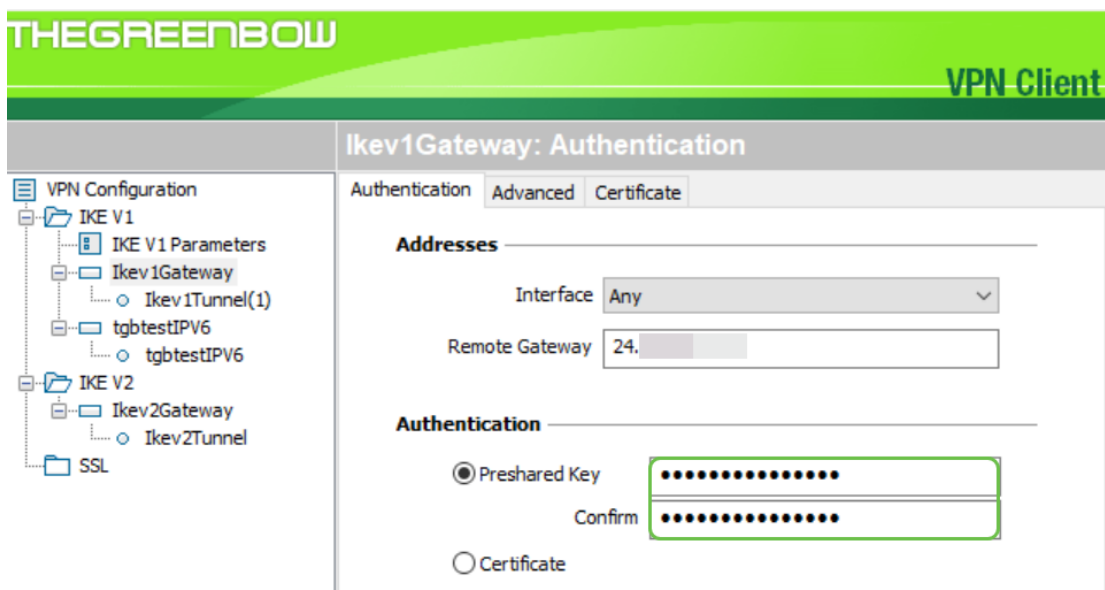
Étape 9. Entrez l'adresse de la passerelle distante dans le champ *Remote Gateway*. Il peut s'agir d'une adresse IP ou d'un nom DNS. Il s'agit de l'adresse IP publique du routeur sur le site

(bureau).



Étape 10. Sous *Authentication*, sélectionnez le type d'authentification. Les options sont les suivantes :

- Preshared Key : cette option permet à l'utilisateur d'utiliser un mot de passe configuré sur la passerelle VPN. Le mot de passe doit correspondre à celui de l'utilisateur pour pouvoir établir un tunnel VPN.
- Certificate : cette option utilise un certificat pour terminer la connexion entre le client VPN et la passerelle VPN.



Note: Dans cet exemple, la clé pré-partagée configurée sur le routeur a été entrée et confirmée.

Étape 11. Sous *IKE*, définissez les paramètres Encryption, Authentication et Key Group pour qu'ils correspondent à la configuration du routeur.

IKE

Encryption	AES 128	▼
Authentication	SHA-1	▼
Key Group	DH2 (1024)	▼

Étape 12. Cliquez sur l'onglet **Advanced**.

ikev1Gateway: Authentication

Authentication **Advanced** Certificate

Étape 13. Sous Fonctionnalités avancées, cochez les cases **Mode Config** et **Mode agressif**. Le mode agressif a été sélectionné sur le RV160 dans le profil Client-à-Site de cet exemple. Laissez le paramètre NAT-T sur Automatique.

VPN Client

thegreenbowvpn: Authentication

Authentication Advanced Certificate

Advanced features

1 Mode Config

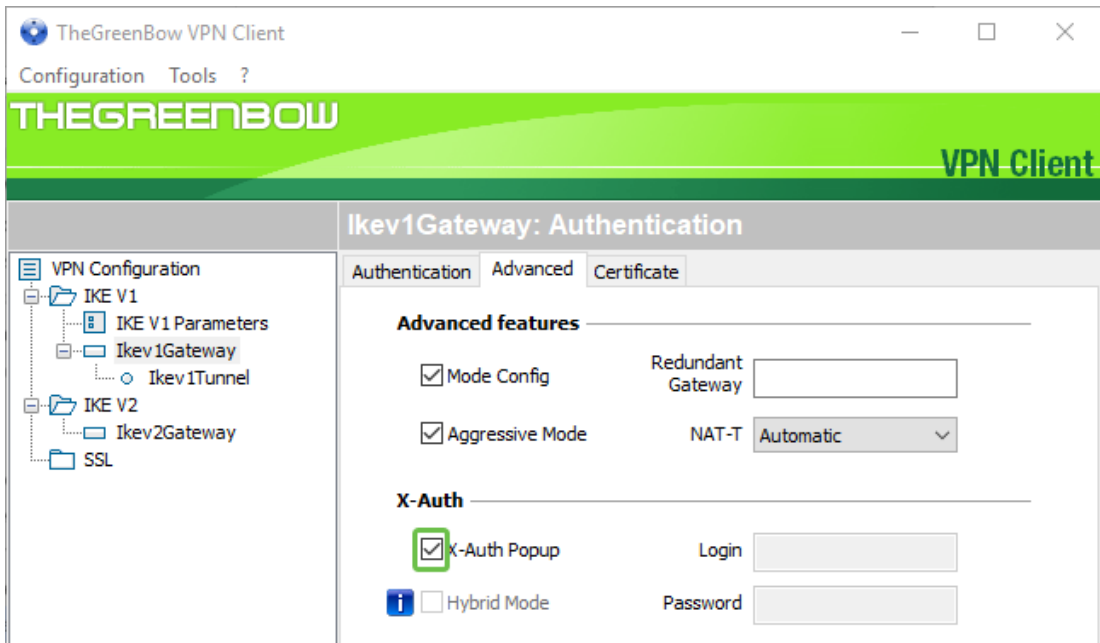
2 Aggressive Mode

Redundant Gateway

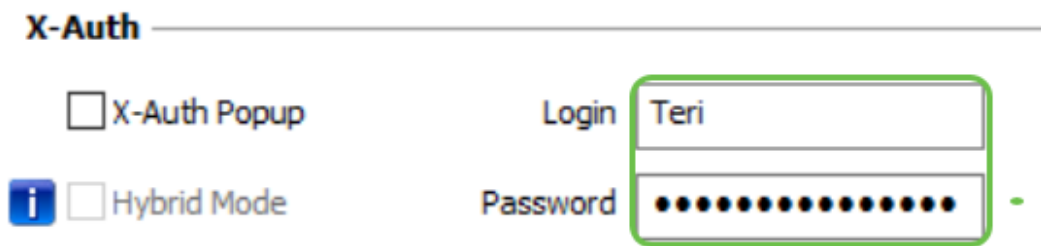
NAT-T Automatic ▼

Note: Lorsque la configuration du mode est activée, le client VPN TheGreenBow extrait les paramètres de la passerelle VPN pour tenter d'établir un tunnel. NAT-T accélère l'établissement d'une connexion.

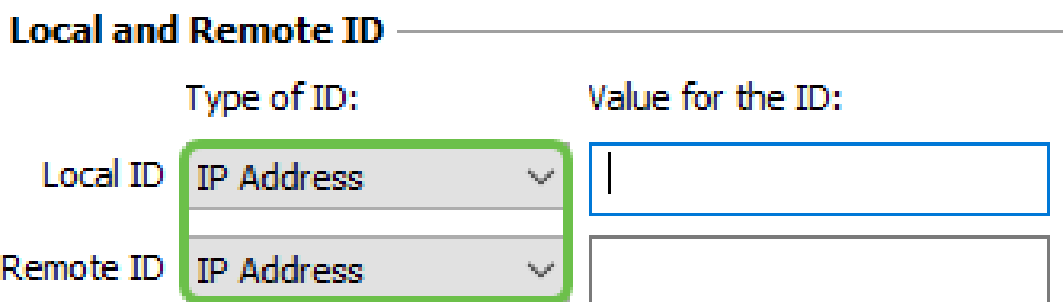
Étape 14. (Facultatif) Sous *X-Auth*, vous pouvez cocher la case **X-Auth Popup** pour afficher automatiquement la fenêtre de connexion lors du démarrage d'une connexion. La fenêtre de connexion permet à l'utilisateur de saisir ses informations d'identification pour pouvoir terminer le tunnel.



Étape 15. (Facultatif) Si vous ne sélectionnez pas *X-Auth Popup*, saisissez votre nom d'utilisateur dans le champ *Connexion*. Il s'agit du nom d'utilisateur entré lors de la création d'un compte d'utilisateur dans la passerelle VPN et le mot de passe du site.



Étape 16. Sous *Local and Remote ID*, définissez l'ID local et l'ID distant pour qu'ils correspondent aux paramètres de la passerelle VPN.



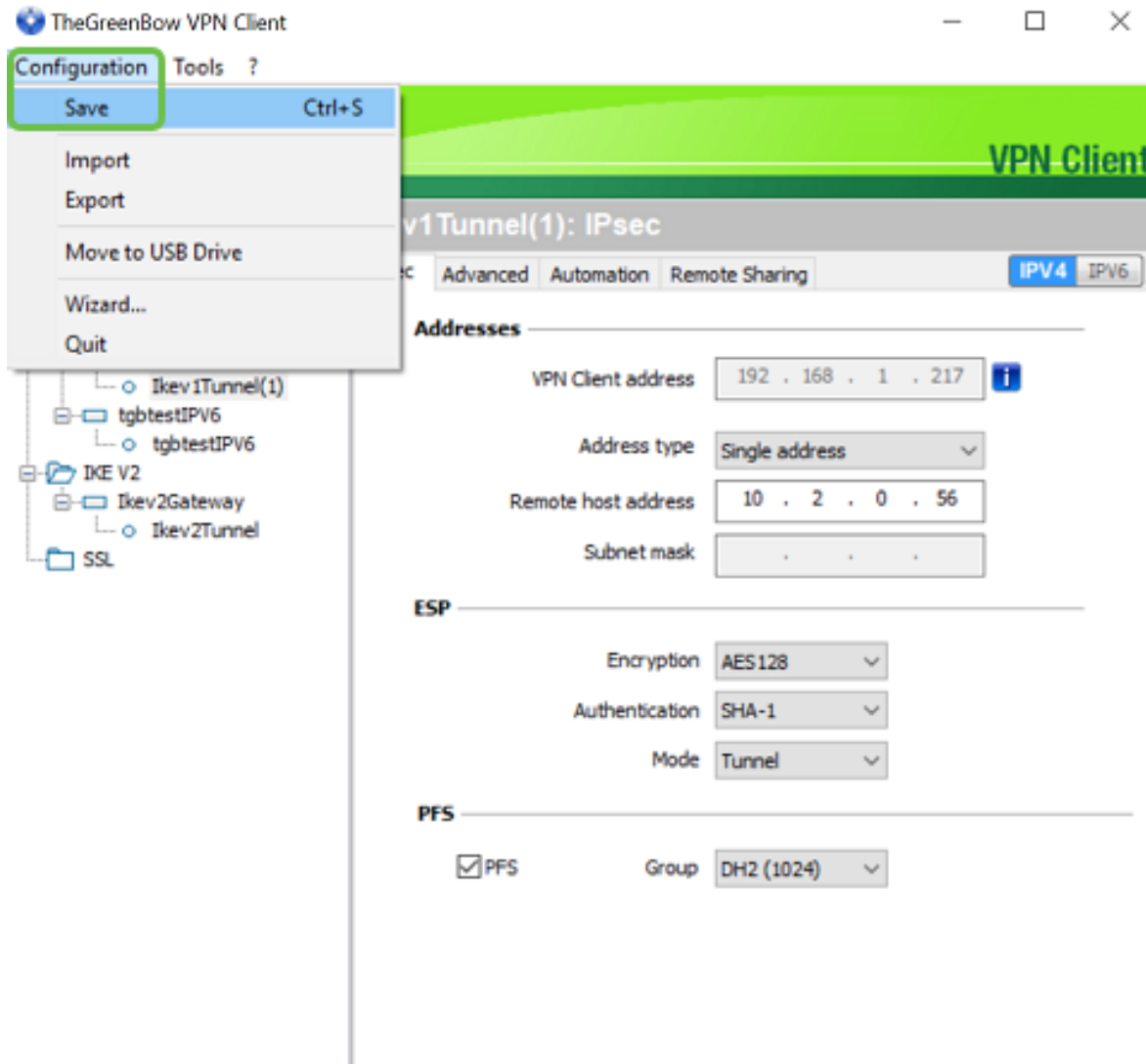
Note: Dans cet exemple, l'ID local et l'ID distant sont tous deux définis sur Adresse IP pour correspondre aux paramètres de la passerelle VPN RV160 ou RV260.

Étape 17. Sous *Valeur de l'ID*, saisissez l'ID local et l'ID distant dans leurs champs respectifs. L'ID local est l'adresse IP WAN du client. Vous pouvez le trouver en effectuant une recherche sur le Web "What's my IP". L'ID distant est l'adresse IP WAN du routeur sur le site.

Local and Remote ID

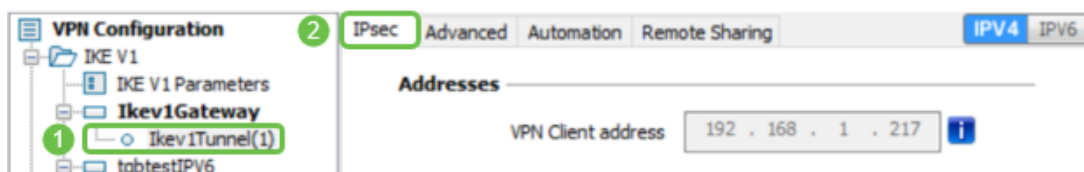
	Type of ID:	Value for the ID:
Local ID	IP Address	108.233.
Remote ID	IP Address	24.

Étape 18. Cliquez sur **Configuration** et choisissez **Enregistrer**.



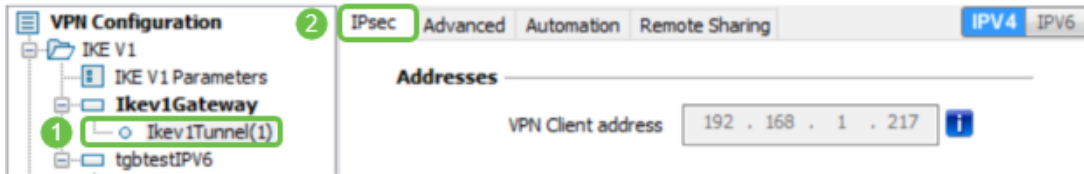
Configuration des paramètres de tunnel

Étape 1. Cliquez sur l'onglet **Ikev1Tunnel(1)** (votre nom peut être différent) et sur l'onglet **IPsec**. L'adresse du client VPN est automatiquement renseignée si vous avez sélectionné Mode Config dans les paramètres avancés de la passerelle Ikev1Gateway. Affiche l'adresse IP locale de l'ordinateur/ordinateur portable à l'emplacement distant.



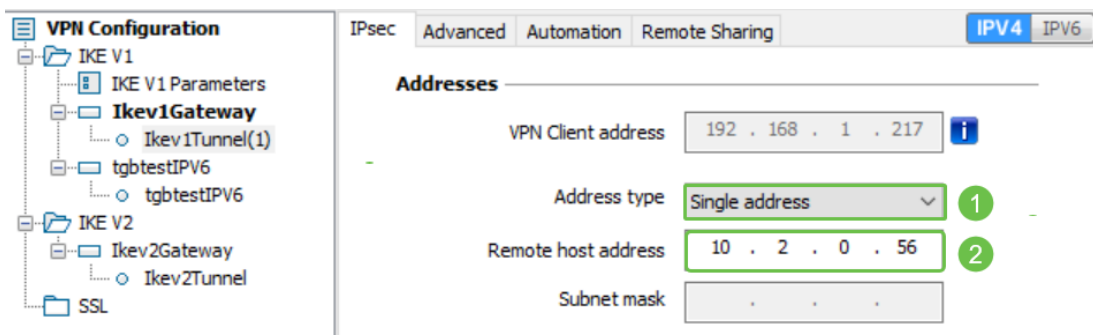
Étape 2. Choisissez le type d'adresse auquel le client VPN peut accéder dans la liste déroulante

Type d'adresse. Il peut s'agir d'une adresse unique, d'une plage d'adresses ou d'une adresse de sous-réseau. L'adresse de sous-réseau par défaut inclut automatiquement l'adresse du client VPN (l'adresse IP locale de l'ordinateur), l'adresse de réseau local distant et le masque de sous-réseau. Si l'option Adresse unique ou Plage d'adresses est sélectionnée, ces champs doivent être remplis manuellement. Entrez l'adresse réseau à laquelle le tunnel VPN doit accéder dans le champ *Adresse LAN distante* et le masque de sous-réseau du réseau distant dans le champ *Masque de sous-réseau*.

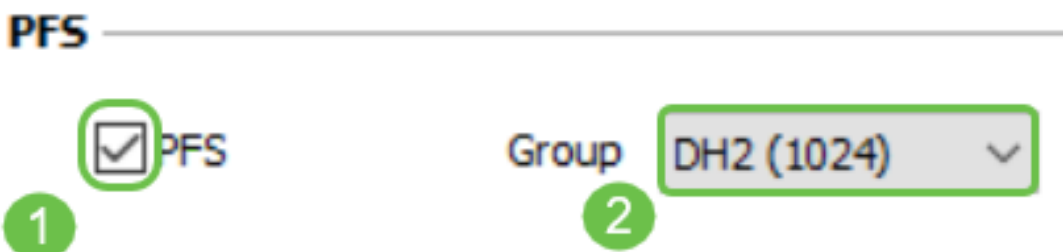


Note: Dans cet exemple, l'adresse unique a été choisie et l'adresse IP locale du routeur sur le site est entrée.

Étape 3. Sous *ESP*, définissez le chiffrement, l'authentification et le mode pour qu'ils correspondent aux paramètres de la passerelle VPN sur le site (bureau).



Étape 4. (Facultatif) Sous *PFS*, cochez la case **PFS** pour activer Perfect Forward Secrecy (PFS). PFS génère des clés aléatoires pour chiffrer la session. Sélectionnez un paramètre de groupe PFS dans la liste déroulante *Groupe*. Si elle a été activée sur le routeur, elle doit également l'être ici.









Étape 5. (Facultatif) Cliquez avec le bouton droit sur le nom de la passerelle Ikev1 et cliquez sur la section Renommer si vous souhaitez la renommer.

TheGreenBow VPN Client

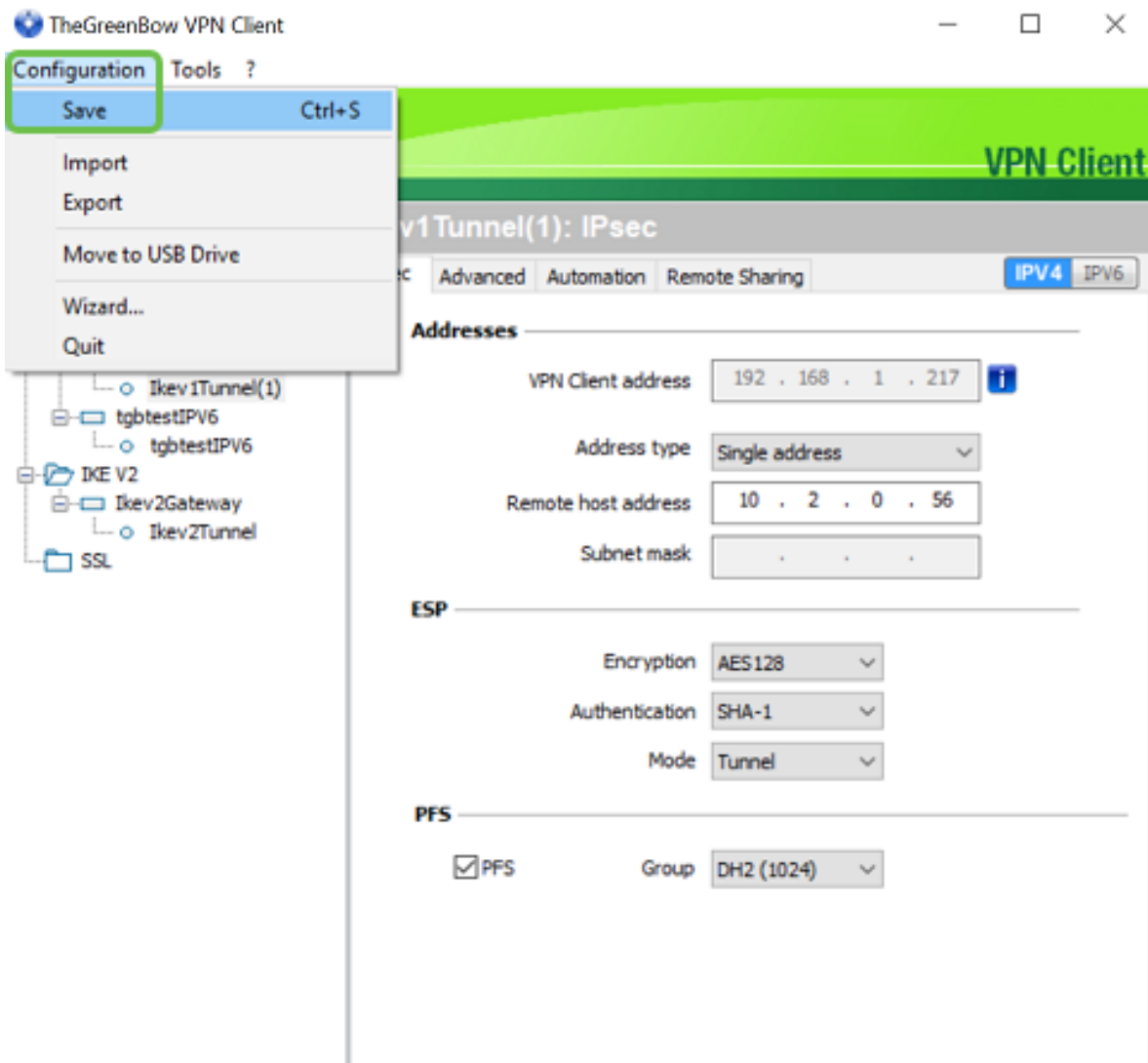
Configuration Tools ?

THEGREENBOW

VPN Configuration

-  IKE V1
 -  IKE V1 Parameters
 -  Ikev1Gateway
 -  Ikev1Tunnel
 -  **Connection_to_Office**
 -  Ikev1Gateway(2)

Étape 6. Cliquez sur Configuration et choisissez Enregistrer.



Vous devez maintenant avoir correctement configuré le client VPN TheGreenBow pour vous connecter au routeur RV160 ou RV260 via VPN.

Démarrer une connexion VPN en tant que client

Étape 1. Puisque TheGreenBow est ouvert, vous pouvez cliquer avec le bouton droit sur le tunnel et sélectionner **Ouvrir le tunnel pour commencer une connexion**.

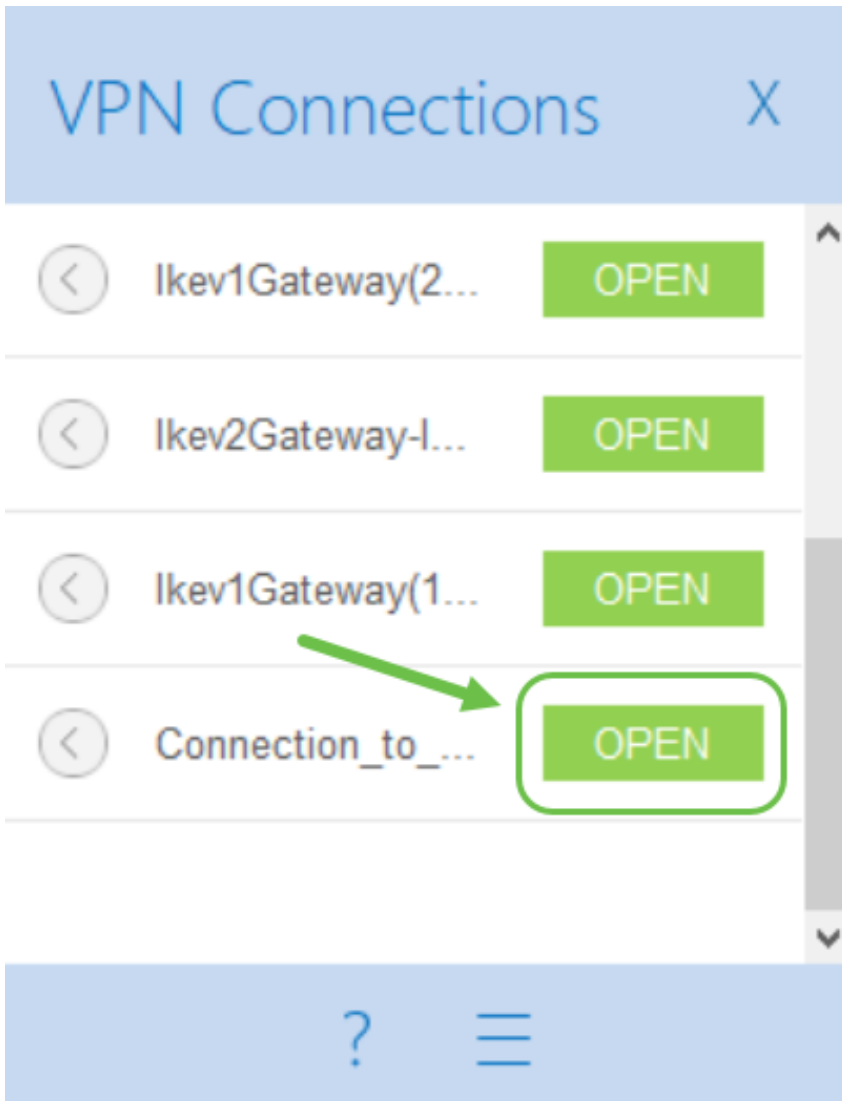
Open tunnel	Ctrl+O
Export	
Copy	Ctrl+C
Rename	F2
Delete	Del

Note: Vous pouvez également ouvrir un tunnel en double-cliquant sur le tunnel.

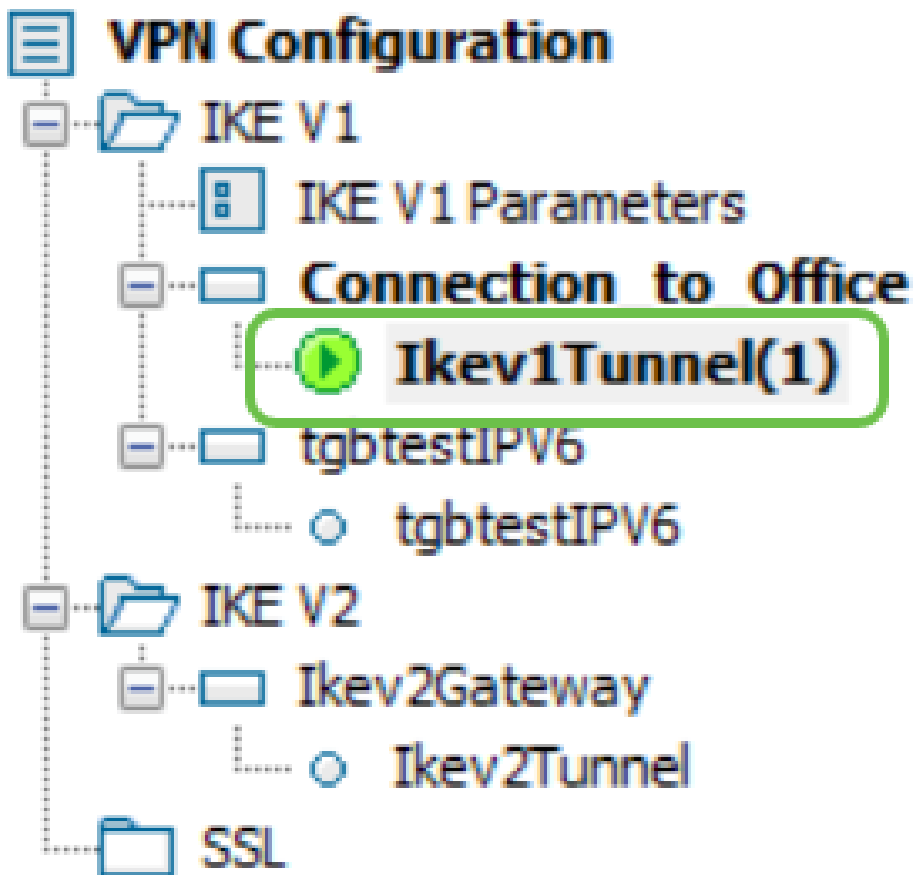
Étape 2. (Facultatif) Si vous commencez une nouvelle session et que vous avez fermé TheGreenBow, cliquez sur l'icône **Client VPN TheGreenBow** à droite de l'écran.



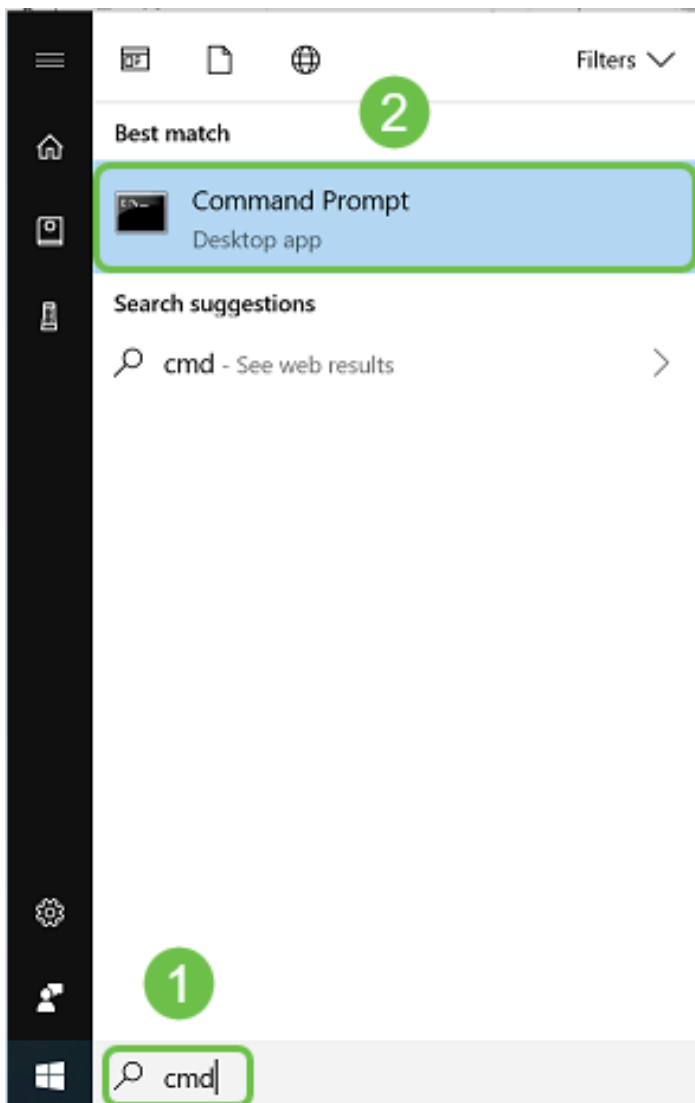
Étape 3. (Facultatif) Cette étape n'est nécessaire que si vous configurez une nouvelle session et que vous avez suivi l'étape 2. Choisissez la connexion VPN à utiliser, puis cliquez sur **OPEN**. La connexion VPN doit démarrer automatiquement.



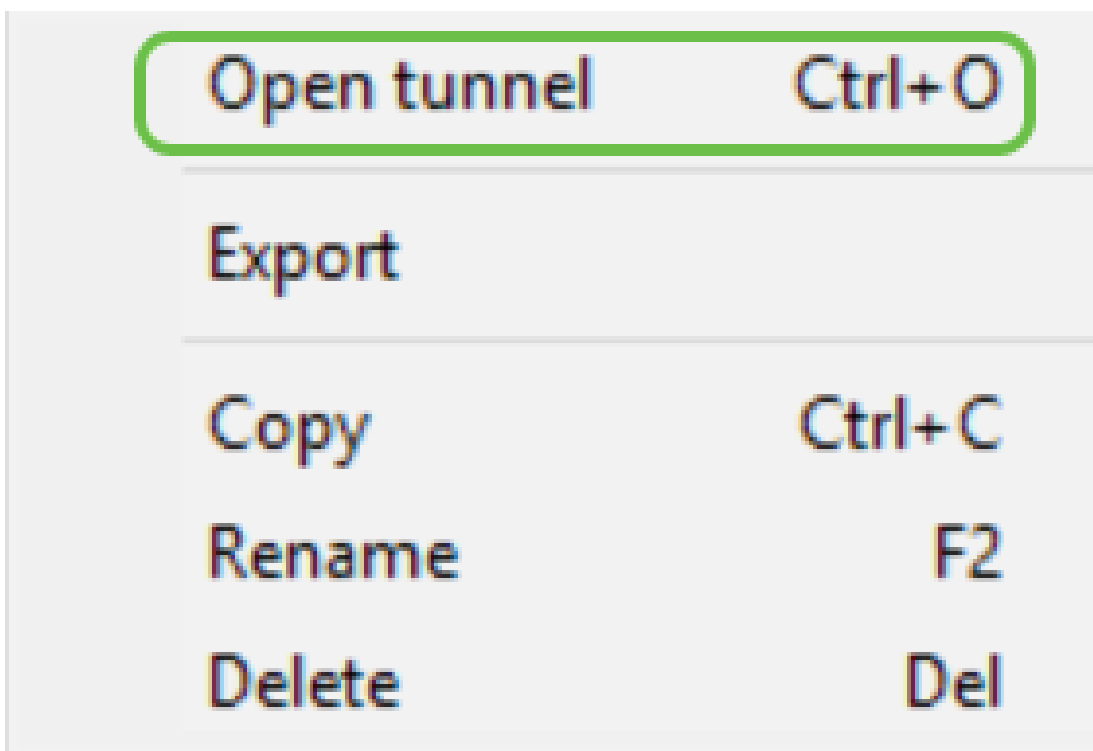
Étape 4. Lorsque le tunnel est connecté, un cercle vert apparaît à côté du tunnel. Si vous voyez un point d'exclamation, vous pouvez cliquer dessus pour trouver l'erreur.



Étape 5. (Facultatif) Pour vérifier que vous êtes connecté, accédez à l'invite de commande à partir de l'ordinateur client.



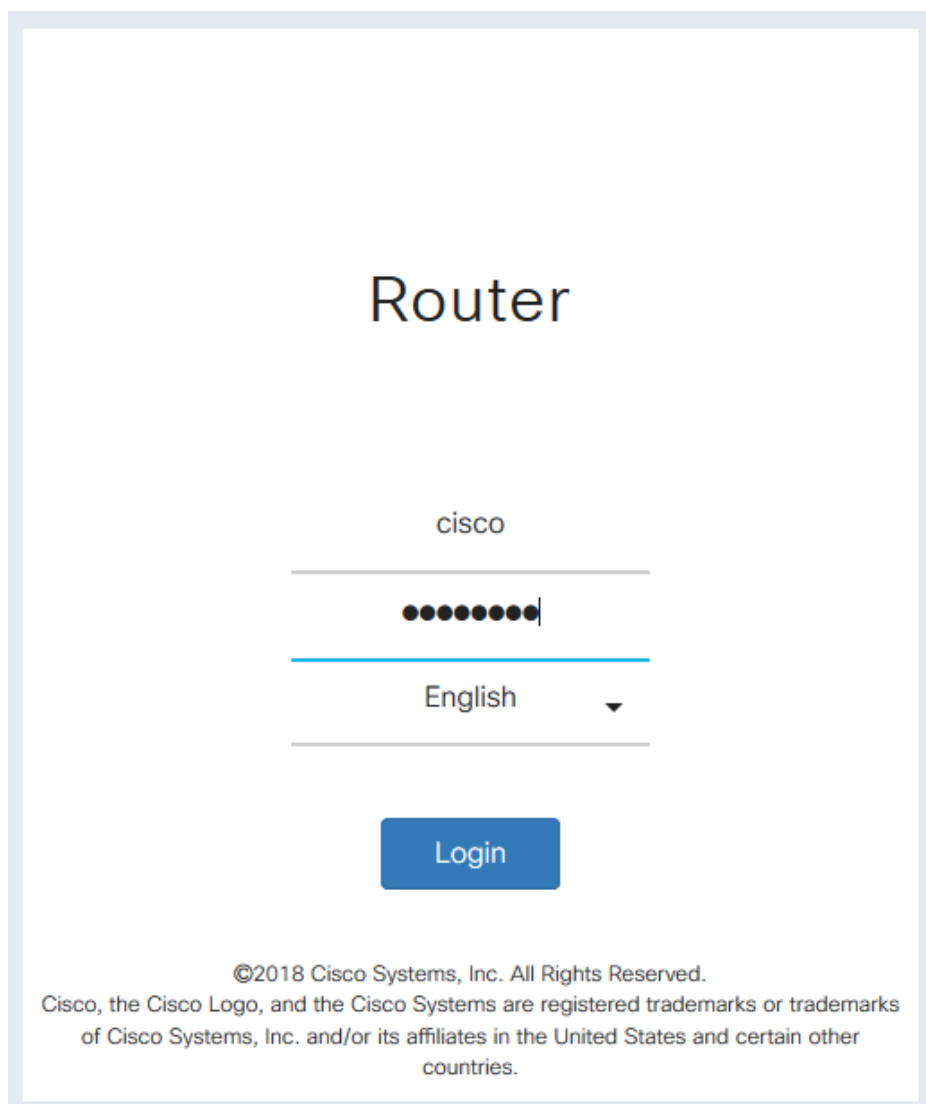
Étape 6. (Facultatif) Saisissez ping, puis l'adresse IP LAN privée du routeur sur le site. Si vous recevez des réponses, vous êtes connecté.



Vérifier l'état du VPN

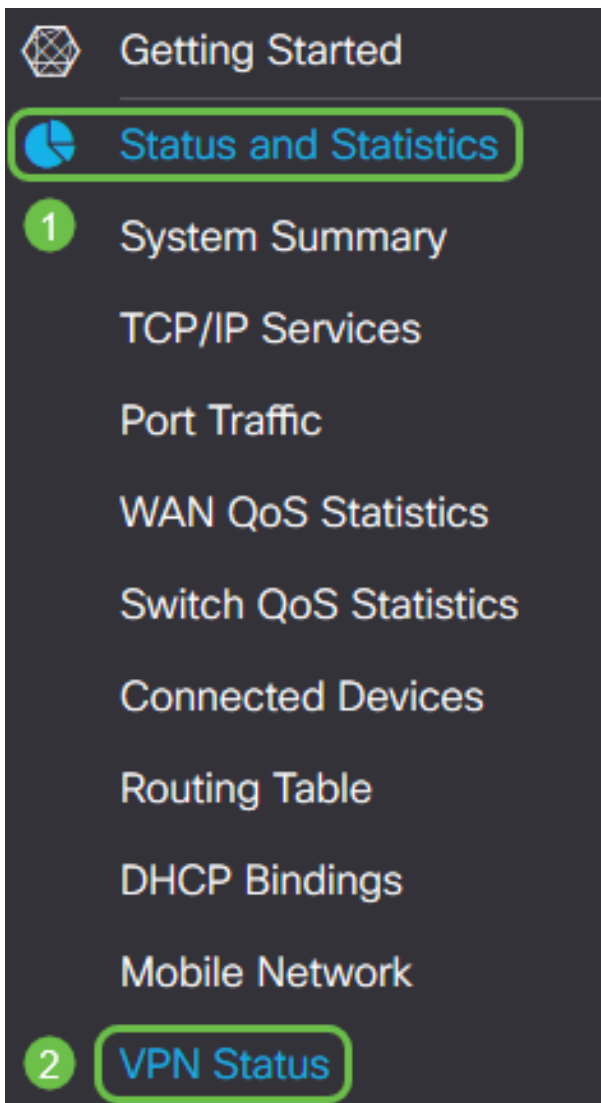
Vérifier l'état du VPN sur le site

Étape 1. Connectez-vous à l'utilitaire Web de la passerelle VPN du routeur RV160 ou RV260.



The screenshot shows the login page for a Cisco Router. At the top, the word "Router" is displayed in a large, black, sans-serif font. Below it, the text "cisco" is centered. A horizontal line separates the text from a password field, which contains ten black dots and a vertical cursor. Another horizontal line is below the password field. Below that, the word "English" is centered, followed by a small downward-pointing triangle indicating a dropdown menu. A blue rectangular button with the word "Login" in white text is centered below the language selection. At the bottom of the page, there is a copyright notice: "©2018 Cisco Systems, Inc. All Rights Reserved. Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries."

Étape 2. Choisissez **Status and Statistics > VPN Status**.



Étape 3. Sous *État du tunnel client à site*, cochez la colonne *Connexions* de la *table de connexion*. Vous devriez voir la connexion VPN confirmée.

Client to Site VPN Status

Connection Table

+ [edit] [delete]

<input type="checkbox"/>	Group/Tunnel Name	Connections	Phase2 Enc/Auth/Grp	Local Group	Action
<input type="checkbox"/>	Client	1	aes128-sha1-modp1024	0.0.0.0/0	

Étape 4. Cliquez sur l'icône **œil** pour voir plus de détails.

Client to Site VPN Status




Connection Table

+ [edit] [delete]

<input type="checkbox"/>	Group/Tunnel Name	Connections	Phase2 Enc/Auth/Grp	Local Group	Action
<input type="checkbox"/>	Client	1	aes128-sha1-modp1024	0.0.0.0/0	

Étape 5. Les détails de l'état du VPN client à site sont présentés ici. Vous remarquerez l'adresse IP WAN du client, l'adresse IP locale qui a été attribuée à partir du pool d'adresses configuré lors de la configuration. Il affiche également les octets et les paquets envoyés et reçus ainsi que le

temps de connexion. Si vous souhaitez déconnecter le client, cliquez sur l'icône bleue de **chaîne brisée** sous *Action*. Cliquez sur le **x** dans le coin supérieur droit pour fermer après inspection.

Client IP (Actual)	Client IP (VPN)	TX Bytes	RX Bytes	TX Packets	RX Packets	Connect Time	Action 
108.233. 	10.2.1.1	0	14273	0	181	5 mins.	

Conclusion

Vous devez maintenant avoir correctement configuré et vérifié la connexion VPN sur le routeur RV160 ou RV260, et avoir également configuré le client VPN TheGreenBow pour se connecter au routeur via VPN.