

Configurer la connectivité du réseau privé virtuel (VPN, pour Private Virtual Network) d'AnyConnect sur le routeur de la gamme RV34x

Objectif

L'objectif de ce document est de décrire la marche à suivre pour configurer la connectivité VPN AnyConnect sur un routeur de la gamme RV34x.

Avantages de l'utilisation d'AnyConnect Secure Mobility Client :

1. Connectivité sécurisée et permanente
2. Sécurité permanente et application des stratégies
3. Déploiement à partir de l'appliance de sécurité adaptative (ASA) ou des systèmes de déploiement de logiciels d'entreprise
4. Personnalisable et traduisible
5. Configuration facile
6. Prise en charge des protocoles IPSec (Internet Protocol Security) et SSL (Secure Sockets Layer)
7. Prise en charge du protocole IKEv2.0 (Internet Key Exchange version 2.0)

Introduction

Une connexion de réseau privé virtuel (VPN) permet aux utilisateurs d'accéder à un réseau privé, d'envoyer et de recevoir des données vers et depuis 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.

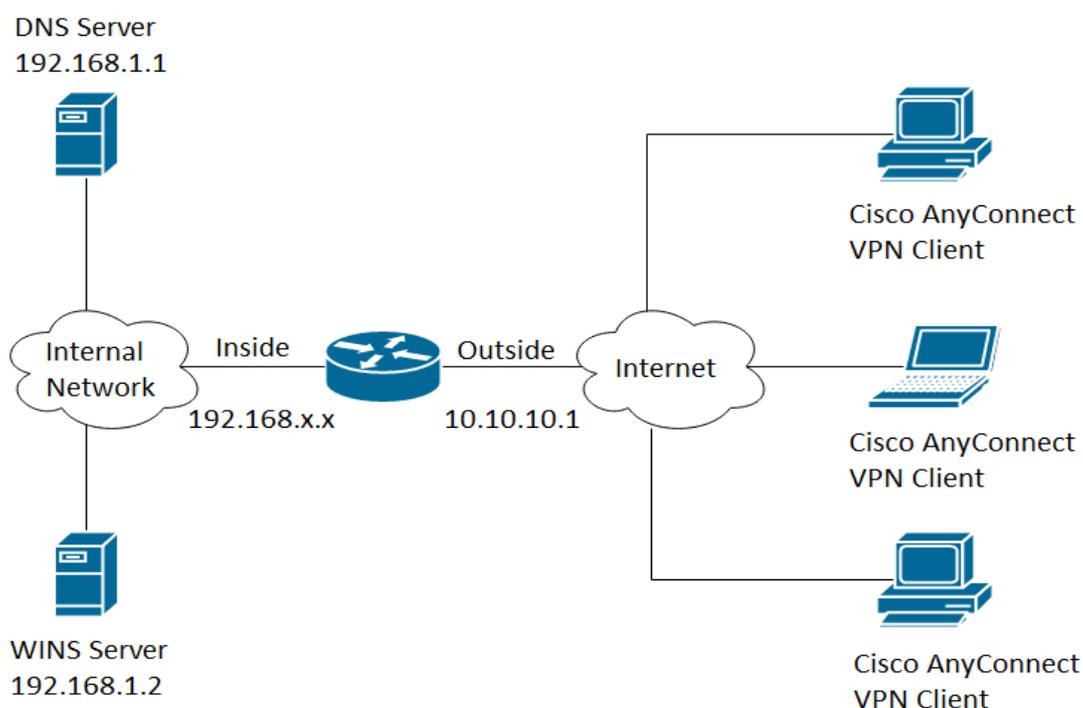
Un client VPN est un logiciel installé et exécuté sur un ordinateur qui souhaite se connecter au réseau distant. Ce logiciel client doit être configuré avec la même configuration que celle du serveur VPN, par exemple l'adresse IP et les informations d'authentification. Ces informations d'authentification incluent le nom d'utilisateur et la clé pré-partagée qui seront utilisés pour chiffrer les données. Selon l'emplacement physique des réseaux à connecter, un client VPN peut également être un périphérique matériel. Cela se produit généralement si la connexion VPN est utilisée pour connecter deux réseaux situés à des emplacements distincts.

Le client Cisco AnyConnect Secure Mobility est une application logicielle permettant de se

connecter à un VPN fonctionnant sur divers systèmes d'exploitation et configurations matérielles. Cette application logicielle permet aux ressources distantes d'un autre réseau d'être accessibles comme si l'utilisateur était directement connecté à son réseau, mais de manière sécurisée. Le client Cisco AnyConnect Secure Mobility offre une nouvelle façon innovante de protéger les utilisateurs mobiles sur des plates-formes informatiques ou de smartphones, offrant une expérience plus transparente et toujours protégée pour les utilisateurs finaux et une application complète des politiques pour l'administrateur informatique.

Sur le routeur RV34x, à partir de la version 1.0.3.15 du micrologiciel et plus tard, la licence AnyConnect n'est pas nécessaire. Des frais seront facturés uniquement pour les licences client.

Pour plus d'informations sur les licences AnyConnect sur les routeurs de la gamme RV340, consultez l'article sur : [Licences AnyConnect pour les routeurs de la gamme RV340](#).



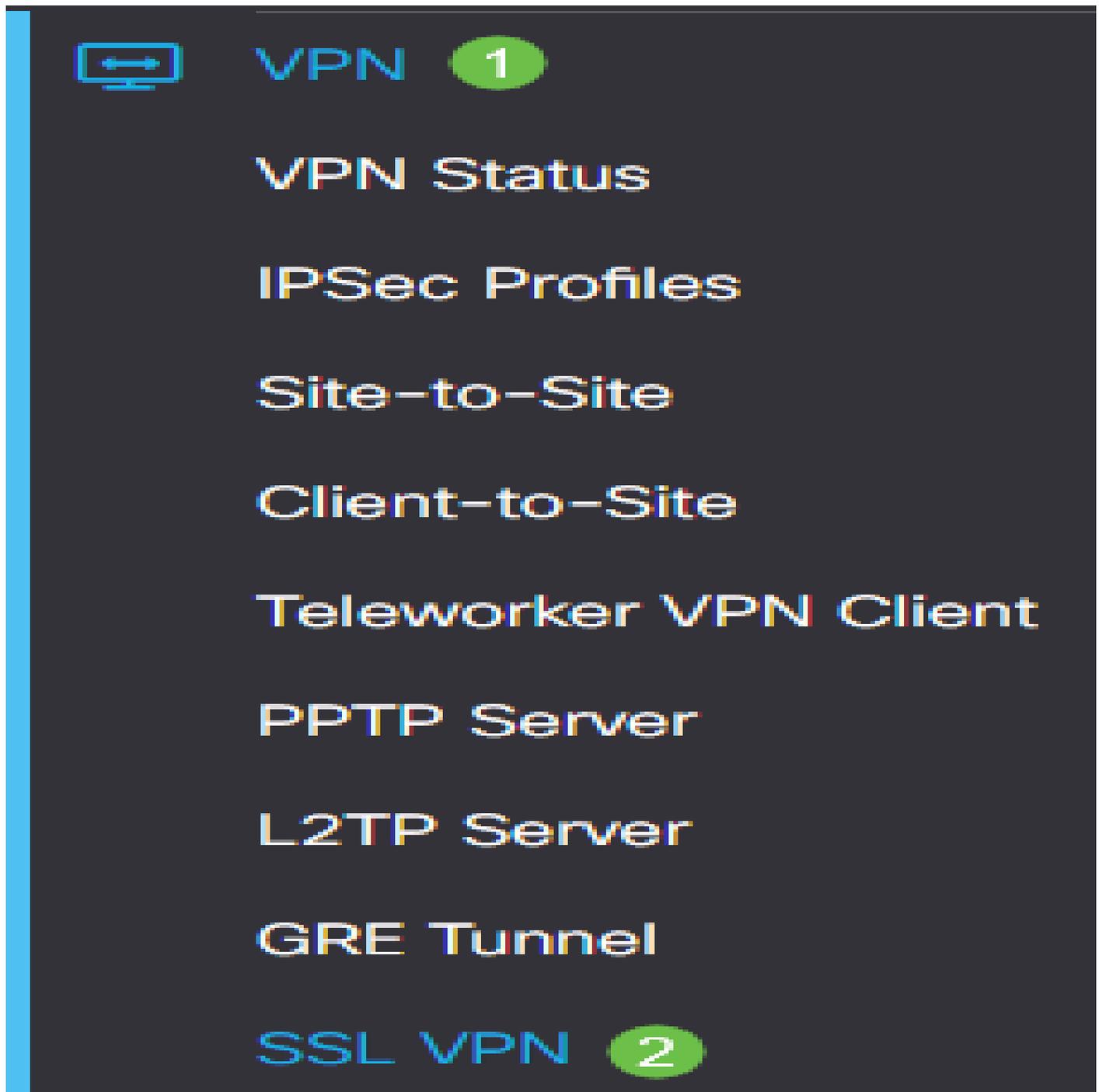
Périphériques pertinents | Version du micrologiciel

- Client de mobilité sécurisée Cisco AnyConnect | 4.4 ([Télécharger la dernière version](#))
- Gamme RV34x | 1.0.03.15 ([Télécharger la dernière version](#))

Configuration de la connectivité VPN AnyConnect sur le routeur RV34x

Configuration du VPN SSL sur le RV34x

Étape 1. Accédez à l'utilitaire Web du routeur et choisissez VPN > SSL VPN.



Étape 2. Cliquez sur la case d'option On pour activer le serveur VPN SSL Cisco.



Paramètres de passerelle obligatoires

Les paramètres de configuration suivants sont obligatoires :

Étape 3. Sélectionnez l'interface de passerelle dans la liste déroulante. Il s'agit du port qui sera utilisé pour acheminer le trafic via les tunnels VPN SSL. Les options sont les suivantes :

- WAN1
- WAN2
- USB1
- USB2

Mandatory Gateway Settings

Gateway Interface:

WAN1 ▼

Remarque : dans cet exemple, WAN1 est choisi.

Étape 4. Entrez le numéro de port utilisé pour la passerelle VPN SSL dans le champ Gateway Port compris entre 1 et 65535.

Gateway Interface:

Gateway Port: (Range: 1-65535)

Remarque : dans cet exemple, 8443 est utilisé comme numéro de port.

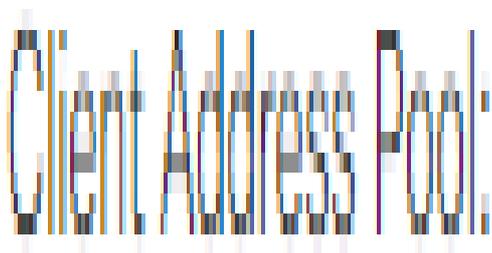
Étape 5. Sélectionnez le fichier de certificat dans la liste déroulante. Ce certificat authentifie les utilisateurs qui tentent d'accéder à la ressource réseau via les tunnels VPN SSL. La liste déroulante contient un certificat par défaut et les certificats importés.

Certificate File:

Remarque : dans cet exemple, Default est sélectionné.

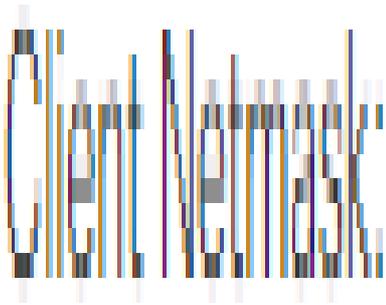
Étape 6. Saisissez l'adresse IP du pool d'adresses client dans le champ Client Address Pool. Ce pool correspond à la plage d'adresses IP qui sera allouée aux clients VPN distants.

Remarque : assurez-vous que la plage d'adresses IP ne chevauche aucune des adresses IP du réseau local.



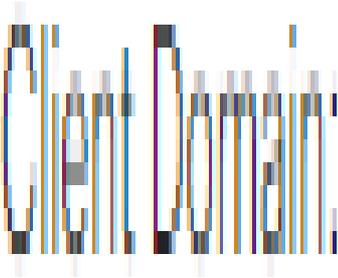
Remarque : dans cet exemple, 192.168.0.0 est utilisé.

Étape 7. Sélectionnez le masque de réseau du client dans la liste déroulante.



Remarque : dans cet exemple, 255.255.255.128 est sélectionné.

Étape 8. Entrez le nom de domaine du client dans le champ Client Domain. Il s'agit du nom de domaine qui doit être envoyé aux clients VPN SSL.



Remarque : dans cet exemple, WideDomain.com est utilisé comme nom de domaine client.

Étape 9. Saisissez le texte qui apparaîtra comme bannière de connexion dans le champ Bannière de connexion. Il s'agit de la bannière qui s'affiche chaque fois qu'un client se connecte.

Mandatory Gateway Settings

Gateway Interface:	<input type="text" value="WAN1"/>
Gateway Port:	<input type="text" value="8443"/>
Certificate File:	<input type="text" value="Default"/>
Client Address Pool:	<input type="text" value="192.168.0.0"/>
Client Netmask:	<input type="text" value="255.255.255.0"/>
Client Domain:	<input type="text" value="yourdomain.com"/>
Login Banner:	<input type="text" value="Welcome to WideDomain!"/>

Remarque : dans cet exemple, Welcome to Widedomain ! est utilisé comme bannière de connexion.

Paramètres de passerelle facultatifs

Les paramètres de configuration suivants sont facultatifs :

Étape 1. Entrez une valeur en secondes pour le délai d'inactivité compris entre 60 et 86400. Il s'agit de la durée pendant laquelle la session VPN SSL peut rester inactive.

Optional Gateway Settings

Idle Timeout: sec. (Range: 60-86400)

Remarque : Dans cet exemple, l'adresse IP 3000 est utilisée.

Étape 2. Entrez une valeur en secondes dans le champ Session Timeout. Il s'agit du temps nécessaire à la session TCP (Transmission Control Protocol) ou UDP (User Datagram Protocol) pour expirer après le temps d'inactivité spécifié. Elle est située entre 60 et 1209600.

Optional Gateway Settings

Idle Timeout:	<input type="text" value="3000"/>	sec. (Range: 60-86400)
Session Timeout:	<input type="text" value="60"/>	sec. (Range: 0,60-1209600)

Remarque : Dans cet exemple, l'adresse IP 60 est utilisée.

Étape 3. Entrez une valeur en secondes dans le champ ClientDPD Timeout comprise entre 0 et 3600. Cette valeur spécifie l'envoi périodique de messages HELLO/ACK pour vérifier l'état du tunnel VPN.

Remarque : cette fonctionnalité doit être activée aux deux extrémités du tunnel VPN.

Optional Gateway Settings

Idle Timeout:	<input type="text" value="3000"/>	sec. (Range: 60-86400)
Session Timeout:	<input type="text" value="60"/>	sec. (Range: 0,60-1209600)
Client DPD Timeout:	<input type="text" value="350"/>	sec. (Range: 0-3600)

Remarque : Dans cet exemple, l'adresse IP 350 est utilisée.

Étape 4. Entrez une valeur en secondes dans le champ GatewayDPD Timeout comprise entre 0 et 3600. Cette valeur spécifie l'envoi périodique de messages HELLO/ACK pour vérifier l'état du tunnel VPN.

Remarque : cette fonctionnalité doit être activée aux deux extrémités du tunnel VPN.

Optional Gateway Settings

Idle Timeout:	<input type="text" value="3000"/>	sec. (Range: 60-86400)
Session Timeout:	<input type="text" value="60"/>	sec. (Range: 0,60-1209600)
Client DPD Timeout:	<input type="text" value="350"/>	sec. (Range: 0-3600)
Gateway DPD Timeout:	<input type="text" value="360"/>	sec. (Range: 0-3600)

Remarque : Dans cet exemple, l'adresse IP 360 est utilisée.

Étape 5. Entrez une valeur en secondes dans le champ Keep Alive comprise entre 0 et 600. Cette fonction garantit que votre routeur est toujours connecté à Internet. Il tentera de rétablir la connexion VPN si elle est abandonnée.

Optional Gateway Settings

Idle Timeout:	<input type="text" value="3000"/>	sec. (Range: 60-86400)
Session Timeout:	<input type="text" value="60"/>	sec. (Range: 0,60-1209600)
Client DPD Timeout:	<input type="text" value="350"/>	sec. (Range: 0-3600)
Gateway DPD Timeout:	<input type="text" value="360"/>	sec. (Range: 0-3600)
Keep Alive:	<input type="text" value="40"/>	sec. (Range: 0-600)

Remarque : Dans cet exemple, l'adresse IP 40 est utilisée.

Étape 6. Entrez une valeur en secondes pour la durée du tunnel à connecter dans le champ Lease Duration. Elle est située entre 600 et 1209600.

Optional Gateway Settings

Idle Timeout:	<input type="text" value="3000"/>	sec. (Range: 60-86400)
Session Timeout:	<input type="text" value="60"/>	sec. (Range: 0,60-1209600)
Client DPD Timeout:	<input type="text" value="350"/>	sec. (Range: 0-3600)
Gateway DPD Timeout:	<input type="text" value="360"/>	sec. (Range: 0-3600)
Keep Alive:	<input type="text" value="40"/>	sec. (Range: 0-600)
Lease Duration:	<input type="text" value="43500"/>	sec. (Range: 600-1209600)

Remarque : Dans cet exemple, l'adresse IP 43500 est utilisée.

Étape 7. Saisissez la taille de paquet en octets qui peut être envoyée sur le réseau. Elle est située entre 576 et 1406.

Optional Gateway Settings

Idle Timeout:	<input type="text" value="3000"/>	sec. (Range: 60-86400)
Session Timeout:	<input type="text" value="60"/>	sec. (Range: 0,60-1209600)
Client DPD Timeout:	<input type="text" value="350"/>	sec. (Range: 0-3600)
Gateway DPD Timeout:	<input type="text" value="360"/>	sec. (Range: 0-3600)
Keep Alive:	<input type="text" value="40"/>	sec. (Range: 0-600)
Lease Duration:	<input type="text" value="43500"/>	sec. (Range: 600-1209600)
Max MTU:	<input type="text" value="1406"/>	bytes (Range: 576-1406)

Remarque : Dans cet exemple, l'adresse IP 1406 est utilisée.

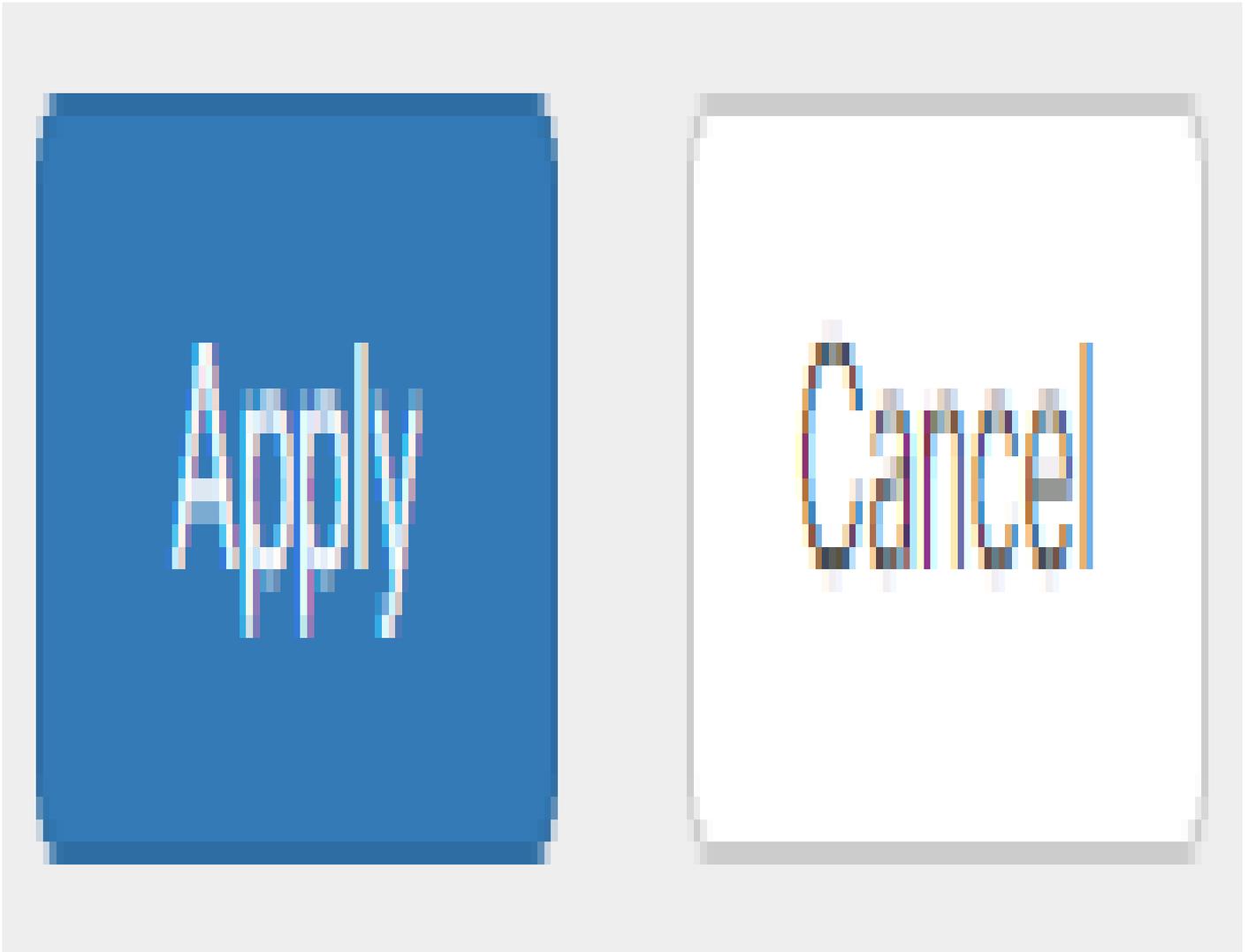
Étape 8. Saisissez la durée de l'intervalle de relais dans le champ Rekey Interval. La fonction Rekey permet aux clés SSL de renégocier une fois la session établie. Elle est située entre 0 et 43200.

Optional Gateway Settings

Idle Timeout:	<input type="text" value="3000"/>	sec. (Range: 60-86400)
Session Timeout:	<input type="text" value="60"/>	sec. (Range: 0,60-1209600)
Client DPD Timeout:	<input type="text" value="350"/>	sec. (Range: 0-3600)
Gateway DPD Timeout:	<input type="text" value="360"/>	sec. (Range: 0-3600)
Keep Alive:	<input type="text" value="40"/>	sec. (Range: 0-600)
Lease Duration:	<input type="text" value="43500"/>	sec. (Range: 600-1209600)
Max MTU:	<input type="text" value="1406"/>	bytes (Range: 576-1406)
Rekey Interval:	<input type="text" value="3600"/>	sec. (Range: 0-43200)

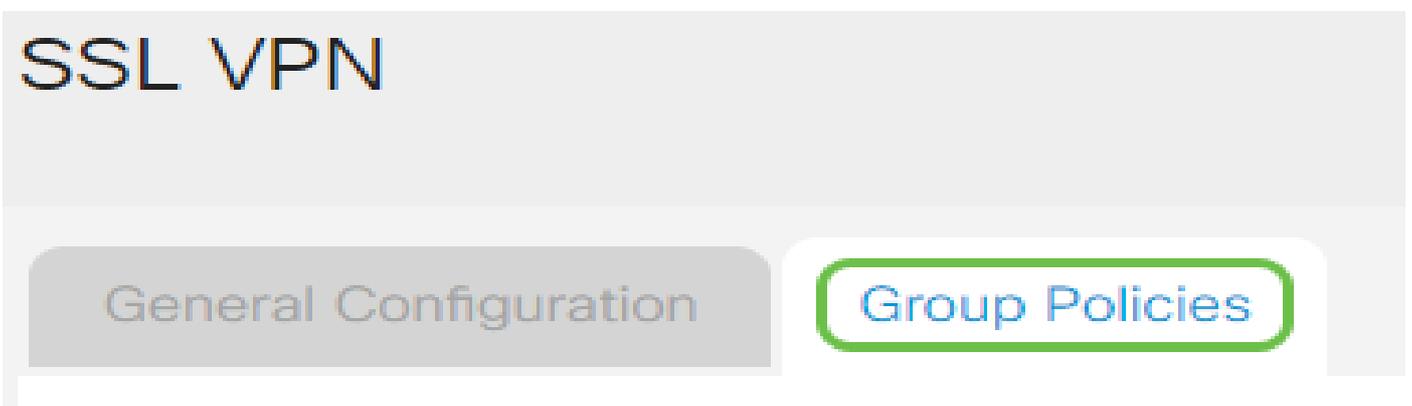
Remarque : Dans cet exemple, l'adresse IP 3600 est utilisée.

Étape 9. Cliquez sur Apply.



Configurer les stratégies de groupe

Étape 1. Cliquez sur l'onglet Stratégies de groupe.



Étape 2. Cliquez sur le bouton Add sous la table de groupe VPN SSL pour ajouter une stratégie de groupe.

SSL VPN

General Configuration

Group Policies

SSL VPN Group Table



Policy Name ↕

SSLVPNDefaultPolicy

Remarque : la table Groupe VPN SSL affiche la liste des stratégies de groupe sur le périphérique. Vous pouvez également modifier la première stratégie de groupe de la liste, nommée SSLVPNDefaultPolicy. Il s'agit de la stratégie par défaut fournie par le périphérique.

Étape 3. Saisissez votre nom de stratégie préféré dans le champ Nom de la stratégie.

SSLVPN Group Policy - Add/Edit

Basic Settings

Policy Name:

Group1Policy

Primary DNS:

192.168.1.1

Remarque : dans cet exemple, la stratégie de groupe 1 est utilisée.

Étape 4. Saisissez l'adresse IP du DNS principal dans le champ prévu à cet effet. Par défaut, cette adresse IP est déjà fournie.

SSLVPN Group Policy - Add/Edit

Basic Settings

Policy Name:

Group1Policy

Primary DNS:

192.168.1.1

Remarque : dans cet exemple, 192.168.1.1 est utilisé.

Étape 5. (Facultatif) Entrez l'adresse IP du DNS secondaire dans le champ prévu à cet effet. Cela servira de sauvegarde en cas d'échec du DNS principal.

SSLVPN Group Policy - Add/Edit

Basic Settings

Policy Name:

Group1Policy

Primary DNS:

192.168.1.1

Secondary DNS:

192.168.1.2

Remarque : dans cet exemple, 192.168.1.2 est utilisé.

Étape 6. (Facultatif) Entrez l'adresse IP du WINS principal dans le champ prévu à cet effet.

SSLVPN Group Policy - Add/Edit

Basic Settings

Policy Name:

Group1Policy

Primary DNS:

192.168.1.1

Secondary DNS:

192.168.1.2

Primary WINS:

192.168.1.1

Remarque : dans cet exemple, 192.168.1.1 est utilisé.

Étape 7. (Facultatif) Entrez l'adresse IP du WINS secondaire dans le champ prévu à cet effet.

SSLVPN Group Policy - Add/Edit

Basic Settings

Policy Name:	<input type="text" value="Group1Policy"/>
Primary DNS:	<input type="text" value="192.168.1.1"/>
Secondary DNS:	<input type="text" value="192.168.1.2"/>
Primary WINS:	<input type="text" value="192.168.1.1"/>
Secondary WINS:	<input type="text" value="192.168.1.2"/>

Remarque : dans cet exemple, 192.168.1.2 est utilisé.

Étape 8. (Facultatif) Entrez une description de la règle dans le champ Description.

SSLVPN Group Policy - Add/Edit

Basic Settings

Policy Name:	<input type="text" value="Group 1 Policy"/>
Primary DNS:	<input type="text" value="192.168.1.1"/>
Secondary DNS:	<input type="text" value="192.168.1.2"/>
Primary WINS:	<input type="text" value="192.168.1.1"/>
Secondary WINS:	<input type="text" value="192.168.1.2"/>
Description:	<input type="text" value="Group policy with split tunnel"/>

Remarque : dans cet exemple, la stratégie de groupe avec tunnel partagé est utilisée.

Étape 9. (Facultatif) Cliquez sur une case d'option pour sélectionner la stratégie de proxy IE afin d'activer les paramètres de proxy Microsoft Internet Explorer (MSIE) pour établir un tunnel VPN. Les options sont les suivantes :

- Aucun - Permet au navigateur d'utiliser aucun paramètre de proxy.
- Auto : permet au navigateur de détecter automatiquement les paramètres du proxy.
- Bypass-local : permet au navigateur de contourner les paramètres de proxy configurés sur l'utilisateur distant.
- Disabled : désactive les paramètres du proxy MSIE.

IE Proxy Settings

IE Proxy Policy: None Auto Bypass-local Disabled

Remarque : dans cet exemple, Disabled est sélectionné. Voici la configuration par défaut .

Étape 10. (Facultatif) Dans la zone Split Tunneling Settings, cochez la case Enable Split Tunneling pour permettre l'envoi direct non chiffré du trafic destiné à Internet vers Internet. La transmission tunnel complète envoie tout le trafic au périphérique final, où il est ensuite acheminé vers les ressources de destination, éliminant ainsi le réseau d'entreprise du chemin d'accès Web.

Split Tunneling Settings

Enable Split Tunneling

Étape 11. (Facultatif) Cliquez sur une case d'option pour choisir d'inclure ou d'exclure le trafic lors de l'application de la transmission tunnel partagée.

Split Tunneling Settings

1 Enable Split Tunneling

Split Selection Include Traffic Exclude Traffic

Remarque : dans cet exemple, l'option Include Traffic est sélectionnée.

Étape 12. Dans le tableau Réseau partagé, cliquez sur le bouton Ajouter pour ajouter une exception Réseau partagé.

Split Network Table



Étape 13. Saisissez l'adresse IP du réseau dans le champ prévu à cet effet.

Split Tunneling Settings

Enable Split Tunneling

Split Selection

Include Traffic

Exclude Traffic

Split Network Table



Remarque : dans cet exemple, 192.168.1.0 est utilisé.

Étape 14. Dans la table Split DNS, cliquez sur le bouton Add pour ajouter une exception Split DNS.

Split DNS Table



Étape 15. Saisissez le nom de domaine dans le champ prévu à cet effet, puis cliquez sur Apply.

Split DNS Table



Vérification de la connectivité VPN AnyConnect

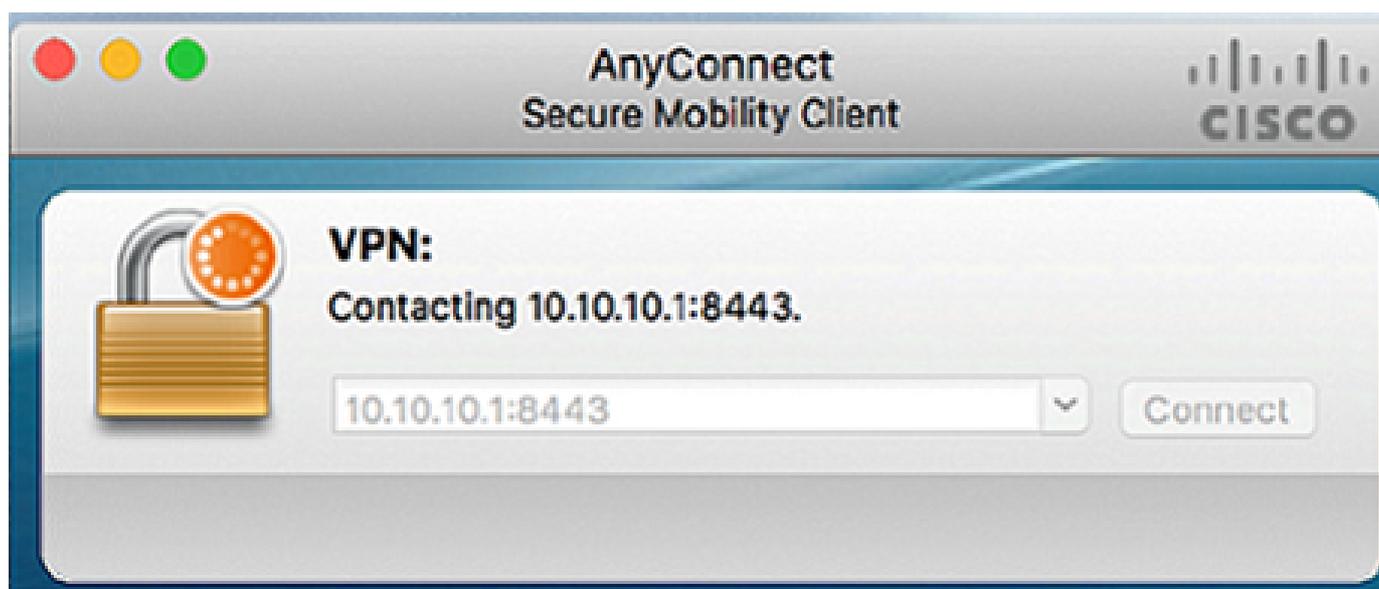
Étape 1. Cliquez sur l'icône AnyConnect Secure Mobility Client.



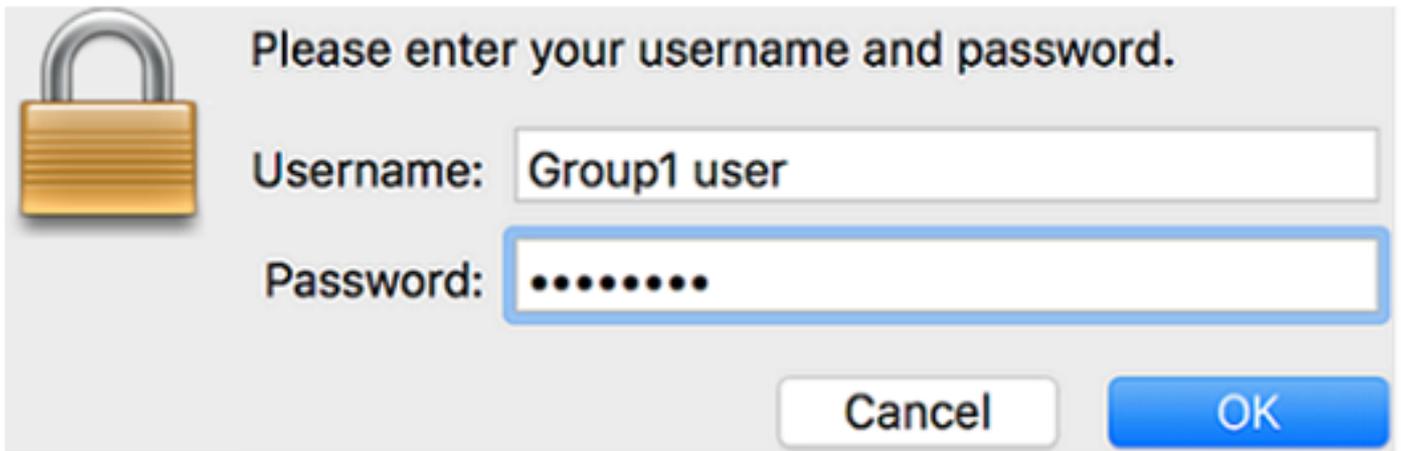
Étape 2. Dans la fenêtre AnyConnect Secure Mobility Client, entrez l'adresse IP de la passerelle et le numéro de port de la passerelle séparés par deux points (:), puis cliquez sur Connect.



Remarque : dans cet exemple, 10.10.10.1:8443 est utilisé. Le logiciel indique maintenant qu'il contacte le réseau distant.



Étape 3. Entrez vos nom d'utilisateur et mot de passe de serveur dans les champs respectifs, puis cliquez sur OK.



Please enter your username and password.

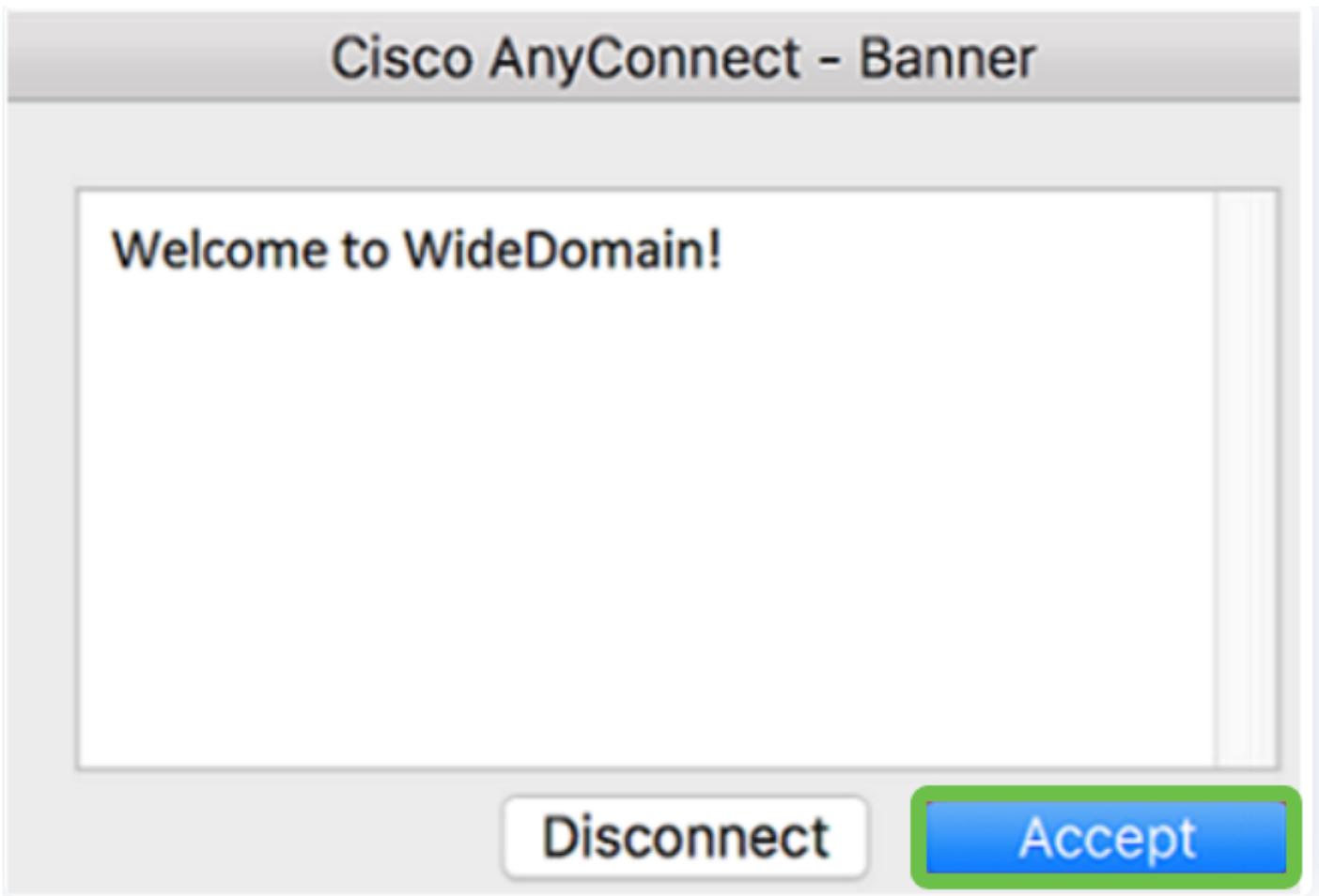
Username: Group1 user

Password:

Cancel OK

Remarque : dans cet exemple, l'utilisateur Group1 est utilisé comme nom d'utilisateur.

Étape 4. Dès que la connexion est établie, la bannière de connexion apparaît. Cliquez sur Accepter.

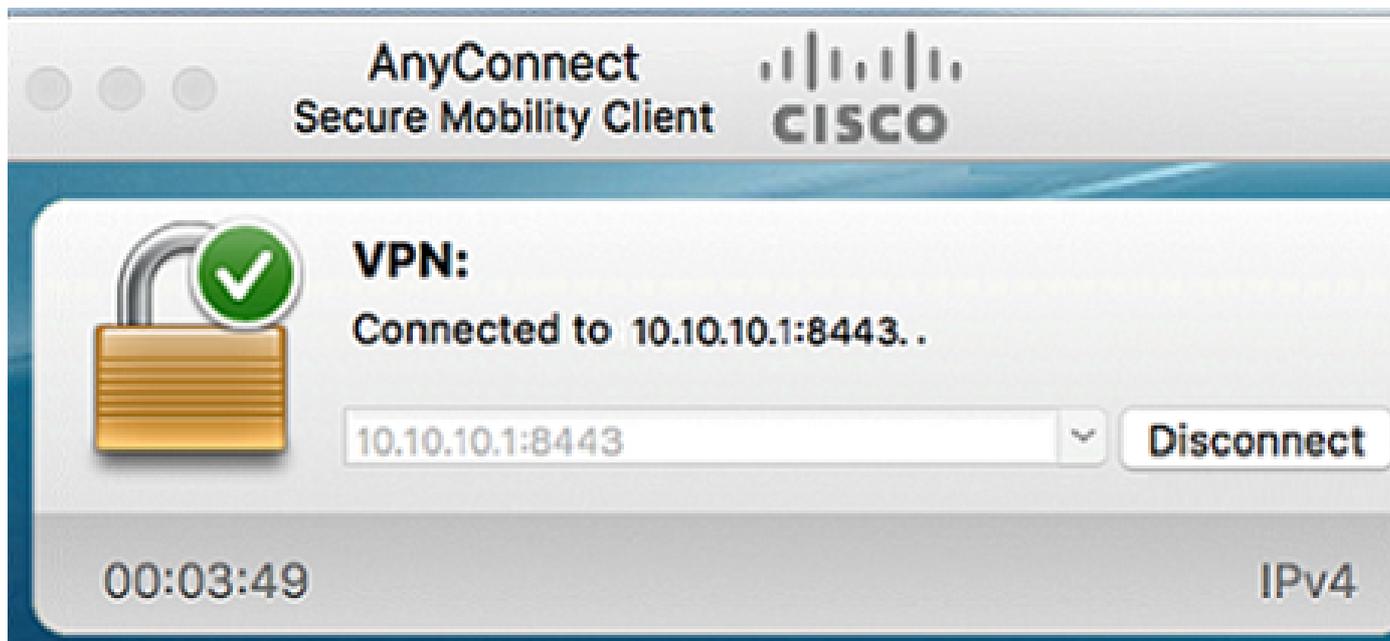


Cisco AnyConnect - Banner

Welcome to WideDomain!

Disconnect Accept

La fenêtre AnyConnect doit maintenant indiquer que la connexion VPN au réseau a réussi.



Étape 5. (Facultatif) Pour vous déconnecter du réseau, cliquez sur Disconnect.

Vous devez maintenant avoir correctement configuré la connectivité VPN AnyConnect à l'aide d'un routeur de la gamme RV34x.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.