

Configurer une connexion de réseau privé virtuel (VPN) site à site sur un routeur RV340 ou RV345

Objectif

Un réseau privé virtuel (VPN) est la connexion entre le réseau local et un hôte distant via Internet. Les hôtes locaux et distants peuvent être un ordinateur ou un autre réseau dont les paramètres ont été synchronisés pour leur permettre de communiquer. Ceci est vrai sur tous les types de VPN. Elle permet généralement aux deux réseaux d'accéder aux ressources des deux côtés de la connexion. Une connexion VPN est généralement utilisée pour connecter un second bureau au bureau central, ou pour permettre à un télétravailleur de se connecter au réseau informatique du bureau, même s'il n'est pas physiquement connecté à l'infrastructure réseau. Les télétravailleurs se connectent généralement via un client logiciel VPN comme AnyConnect, Shrew Soft, GreenBow et bien d'autres.

Cet article vise à vous montrer comment configurer une connexion VPN site à site entre un routeur RV340 et un routeur RV345. Il appellera le routeur principal le routeur local et le routeur secondaire le routeur distant. Assurez-vous d'avoir un accès distant ou physique au routeur secondaire.

Les réseaux locaux doivent se trouver sur des sous-réseaux différents (par exemple 192.168.1.x et 192.168.2.x) ou sur des réseaux totalement différents (par exemple 192.168.1.x et 10.10.1.x). Si les deux réseaux se trouvaient sur le même sous-réseau, les routeurs n'essaieraient jamais d'envoyer des paquets sur le VPN.

Périphériques pertinents

- RV340
- RV340W
- RV345
- RV345P

Version du logiciel

- 1.0.03.15

Notice spéciale : Structure de licence - Firmware versions 1.0.3.15 et ultérieures.

AnyConnect est facturé uniquement pour les licences client.

Vous devez acheter une ou plusieurs licences client auprès d'un partenaire comme CDW ou dans le cadre de l'achat d'appareils par votre entreprise. Il existe des options pour un utilisateur (L-AC-PLS-3Y-S5) ou des ensembles de licences d'un an pour 25 utilisateurs (AC-PLS-P-25-S). D'autres options de licences sont également disponibles, y compris des licences permanentes. Pour plus d'information sur les licences, consultez les liens dans la section Renseignements relatifs aux licences ci-dessous.

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

Configurer une connexion VPN

Routeur local

Étape 1. Connectez-vous à l'utilitaire Web du routeur local et choisissez VPN > Site-to-Site.

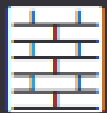
Remarque : dans cet exemple, un routeur RV340 est utilisé.



LAN



Routing



Firewall



VPN

1

VPN Status

IPSec Profiles

Site-to-Site

2

Client-to-Site

Teleworker VPN Client

PPTP Server

Étape 2. Cliquez sur l'icône Plus.

Site to Site Table



Connection Name Remote Endpoint Interface IPsec Profile Local Traffic Selection Remote Traffic Selection Sta

Étape 3. Assurez-vous que la case Activer est cochée. Elle est cochée par défaut.

Basic Settings Advanced Settings Failover

Enable:

Connection Name: Please Input Connection Name

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

Étape 4. Entrez le nom de la connexion dans le champ Connection Name.

Remarque : dans cet exemple, le nom est TestVPN1.

Basic Settings Advanced Settings Failover

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

Étape 5. Sélectionnez les paramètres de sécurité de la connexion dans la liste déroulante Profil IPsec. Les options dépendent des profils IPsec créés. Pour obtenir des instructions sur la création d'un profil IPsec, cliquez [ici](#).

Remarque : dans cet exemple, CiscoTestVPN est sélectionné.

Basic Settings Advanced Settings Failover

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

Étape 6. Sélectionnez l'interface à utiliser par le routeur local. Les options sont les suivantes :

- WAN1 : cette option utilise l'adresse IP de l'interface WAN1 (Wide Area Network 1) du routeur local pour la connexion VPN.
- WAN2 : cette option utilise l'adresse IP de l'interface WAN2 du routeur local pour la

connexion VPN. Le WAN2 n'est pas disponible dans les routeurs à un seul WAN.

- USB1 : cette option utilise l'adresse IP de l'interface USB1 (Universal Serial Bus 1) du routeur local pour la connexion VPN.
- USB2 : cette option utilise l'adresse IP de l'interface USB2 du routeur local pour la connexion VPN. USB2 n'est pas disponible sur les routeurs USB simples.

Remarque : dans cet exemple, WAN1 est choisi.

The screenshot shows a configuration interface with three tabs: 'Basic Settings' (active), 'Advanced Settings', and 'Failover'. The 'Basic Settings' section contains the following fields:

- Enable:** A checkbox that is checked.
- Connection Name:** A text input field containing 'TestVPN1'.
- IPsec Profile:** A dropdown menu showing 'CiscoTestVPN'. To the right of the dropdown, the text 'Auto (IKEv1) Profile is Chosen.' is displayed.
- Interface:** A dropdown menu showing 'WAN1', which is highlighted with a green border.
- Remote Endpoint:** A dropdown menu showing 'Static IP'.
- Below the 'Remote Endpoint' dropdown, there is an empty rectangular input field with a red border.

Étape 7. Choisissez l'identificateur de l'interface WAN du routeur distant. Les options sont les suivantes :

- Static IP : cette option permet au routeur local d'utiliser l'adresse IP statique du routeur distant lors de l'établissement d'une connexion VPN. Si cette option est sélectionnée sur le routeur local, le routeur distant doit également être configuré avec la même option.
- FQDN : cette option utilise le nom de domaine complet (FQDN) du routeur distant lors de l'établissement de la connexion VPN.
- Dynamic IP : cette option utilise l'adresse IP dynamique du routeur distant lors de l'établissement d'une connexion VPN.

Remarque : l'identificateur d'interface sur le routeur distant doit être identique à l'identificateur d'interface du routeur local. Dans cet exemple, l'adresse IP statique est choisie.

Basic Settings Advanced Settings Failover

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

Étape 8. Saisissez l'adresse IP de l'interface WAN du routeur distant.

Remarque : Dans cet exemple, l'adresse IP 124.123.122.123 est utilisée.

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

Étape 9. Sélectionnez la case d'option correspondant à la méthode d'authentification IKE (Internet Key Exchange) dont vous avez besoin. Les options sont les suivantes :

- Preshared Key : cette option signifie que la connexion nécessite un mot de passe pour être établie. La clé pré-partagée doit être identique aux deux extrémités de la connexion VPN.
- Certificate : cette option signifie que la méthode d'authentification utilise un certificat généré par le routeur au lieu d'un mot de passe lors de la connexion.

Remarque : dans cet exemple, la clé pré-partagée est sélectionnée.

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter:

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable

Certificate:

Étape 10. Saisissez la clé pré-partagée pour la connexion VPN dans le champ Preshared Key (Clé pré-partagée).

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter:

Minimum Pre-shared Key Complexity: Enable


Show Pre-shared Key: Enable

Certificate:

Étape 11. (Facultatif) Décochez la case Minimum Preshared Key Complexity Enable si vous souhaitez utiliser un mot de passe simple pour la connexion VPN. Cette option est activée par défaut.

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable

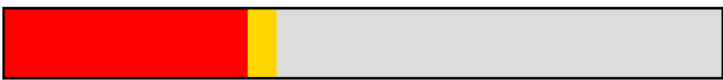
Show Pre-shared Key: Enable

Certificate:

Étape 12. (Facultatif) Cochez la case Afficher le texte brut lorsque vous modifiez Activer pour afficher la clé pré-partagée en texte brut. Cette option est désactivée par défaut.

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable

Certificate:

Étape 13. Sélectionnez le type d'identificateur du réseau local dans la liste déroulante Type d'identificateur local. Les options sont les suivantes :

- Local WAN IP : cette option identifie le réseau local via l'adresse IP WAN de l'interface.
- IP Address : cette option identifie le réseau local via l'adresse IP locale.
- Local FQDN : cette option identifie le réseau local via le FQDN, le cas échéant.
- Local User FQDN : cette option identifie le réseau local via le nom de domaine complet de l'utilisateur, qui peut être son adresse e-mail.

Remarque : dans cet exemple, l'adresse IP est choisie.

Local Group Setup

Local Identifier Type:

Local Identifier:

Local IP Type:

IP Address:

Subnet Mask:

Étape 14. Saisissez l'identificateur du réseau local dans le champ Identificateur local.

Remarque : dans cet exemple, 124.123.122.121 est entré.

Local Group Setup

Local Identifier Type:

Local Identifier:

Local IP Type:

IP Address:

Subnet Mask:

Étape 15. Sélectionnez le type d'adresse IP auquel le client VPN peut accéder dans la liste déroulante Local IP Type. Les options sont les suivantes :

- Subnet : cette option permet au côté distant du VPN d'accéder aux hôtes locaux dans le sous-réseau spécifié.
- IP Address : cette option permet au côté distant du VPN d'accéder à l'hôte local avec l'adresse IP spécifiée.
- Any : cette option permet au côté distant du VPN d'accéder à n'importe quel hôte local.

Remarque : dans cet exemple, Subnet est sélectionné.

Local Group Setup

Local Identifier Type:	<input type="text" value="IP Address"/>
Local Identifier:	<input type="text" value="124.123.122.121"/>
Local IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text" value="Subnet"/>
Subnet Mask:	<input type="text" value="IP Address"/>

Étape 16. Saisissez l'adresse IP du réseau ou de l'hôte auquel le client VPN doit accéder dans le champ IP Address.

Remarque : dans cet exemple, l'adresse IP est 10.10.10.1.

Local Group Setup

Local Identifier Type:	<input type="text" value="IP Address"/>
Local Identifier:	<input type="text" value="124.123.122.121"/>
Local IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text" value="10.10.10.1"/>
Subnet Mask:	<input type="text"/>

Étape 17. Saisissez le masque de sous-réseau de l'adresse IP dans le champ Subnet Mask.

Remarque : dans cet exemple, le masque de sous-réseau est 255.255.255.0.

Local Group Setup

Local Identifier Type:

IP Address

Local Identifier:

124.123.122.121

Local IP Type:

Subnet

IP Address:

10.10.10.1

Subnet Mask:

255.255.255.0

Étape 18. Sélectionnez le type d'identificateur distant dans la liste déroulante. Les options sont les suivantes :

- Remote WAN IP : cette option identifie le réseau distant via l'adresse IP WAN de l'interface.
- Remote FQDN : cette option identifie le réseau distant via le FQDN, le cas échéant.
- Remote User FQDN : cette option identifie le réseau distant via le nom de domaine complet de l'utilisateur, qui peut être son adresse e-mail.

Remarque : dans cet exemple, Remote WAN IP est sélectionné.

Remote Group Setup

Remote Identifier Type:

Remote WAN IP

Remote Identifier:

Remote WAN IP

Remote FQDN

Remote User FQDN

Subnet

Remote IP Type:

IP Address:

Subnet Mask:

Étape 19. Saisissez l'adresse IP WAN du routeur distant dans le champ Remote Identifier.

Remarque : dans cet exemple, l'identificateur distant est 124.123.122.123.

Remote Group Setup

Remote Identifier Type:

Remote WAN IP

Remote Identifier:

124.123.122.123

Remote IP Type:

Subnet

IP Address:

Subnet Mask:

Étape 20. Sélectionnez le type de réseau auquel le réseau local doit accéder dans la liste déroulante Remote IP Type. Les options sont les suivantes :

- IP Address : cette option permet aux hôtes locaux d'accéder à l'hôte distant avec l'adresse IP spécifiée.
- Subnet : cette option permet aux hôtes locaux d'accéder aux ressources de l'hôte distant avec le sous-réseau spécifié.
- Any : cette option permet aux hôtes locaux d'accéder aux ressources de l'hôte distant avec n'importe quelle adresse IP.

Remote Group Setup

Remote Identifier Type: Remote WAN IP

Remote Identifier: 124.123.122.123

Remote IP Type: Subnet

IP Address:

Subnet Mask:

- Subnet
- IP Address
- IP Group
- Any

Étape 21. Saisissez l'adresse IP LAN du réseau distant dans le champ IP Address.

Remarque : dans cet exemple, l'adresse IP est 192.168.2.1.

Remote Group Setup

Remote Identifier Type: Remote WAN IP

Remote Identifier: 124.123.122.123

Remote IP Type: Subnet

IP Address: 192.168.2.1

Subnet Mask:

Étape 22. Entrez le masque de sous-réseau du réseau distant dans le champ Subnet Mask.

Remarque : dans cet exemple, le masque de sous-réseau est 255.255.255.0.

Remote Group Setup

Remote Identifier Type:	Remote WAN IP
Remote Identifier:	124.123.122.123
Remote IP Type:	Subnet
IP Address:	192.168.2.1
Subnet Mask:	255.255.255.0

Étape 23. Cliquez sur Apply.






Add/Edit a New Connection Apply Cancel

Local IP Type:	Subnet
IP Address:	10.10.10.1
Subnet Mask:	255.255.255.0

Remote Group Setup

Remote Identifier Type:	Remote WAN IP
Remote Identifier:	124.123.122.123
Remote IP Type:	Subnet
IP Address:	192.168.2.1
Subnet Mask:	255.255.255.0

Étape 24. Cliquez sur Save.

  cisco (admin) English   

Vous devez maintenant avoir configuré les paramètres VPN sur le routeur local.

Routeur distant

Étape 1. Déterminez les paramètres VPN du routeur local, tels que :

- Interface des routeurs local et distant à utiliser pour la connexion VPN.
- Adresse IP (Internet Protocol) de réseau étendu (WAN) du routeur local et distant.
- Adresse de réseau local (LAN) et masque de sous-réseau du réseau local et distant.
- Clé, mot de passe ou certificat pré-partagé pour la connexion VPN.
- Paramètres de sécurité du routeur local.
- Exemption de pare-feu pour la connexion VPN.

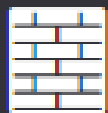
Étape 2. Connectez-vous à l'utilitaire Web du routeur et choisissez VPN > IPSec Profiles.



LAN



Routing



Firewall



VPN

1

VPN Status

IPSec Profiles

2

Site-to-Site

Client-to-Site

Teleworker VPN Client

PPTP Server

Étape 3. Configurez les paramètres de sécurité VPN du routeur distant, en fonction des paramètres de sécurité VPN du routeur local. [Pour des instructions, cliquez ici.](#)

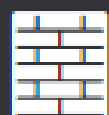
Étape 4. Dans l'utilitaire Web du routeur local, choisissez VPN > Site-to-Site.



LAN



Routing



Firewall



VPN

1

VPN Status

IPSec Profiles

Site-to-Site

2

Client-to-Site

Teleworker VPN Client

PPTP Server

Étape 5. Cliquez sur l'icône Plus.

Site to Site Table



Connection Name Remote Endpoint Interface IPsec Profile Local Traffic Selection Remote Traffic Selection Sta

Étape 6. Assurez-vous que la case Activer est cochée. Elle est cochée par défaut.

Enable:



Connection Name:

Please Input Connection Name

IPsec Profile:

Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

Étape 7. Entrez le nom de la connexion VPN dans le champ Connection Name. Le nom de connexion du routeur distant peut être différent du nom de connexion spécifié dans le routeur local.

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

Remarque : dans cet exemple, le nom de la connexion est TestVPN.

Étape 8. Sélectionnez le profil IPsec dans la liste déroulante. Les options dépendent des profils IPsec créés. Pour obtenir des instructions sur la création d'un profil IPsec, cliquez [ici](#).

Remarque : dans cet exemple, CiscoTestVPN est sélectionné.

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

Étape 9. Sélectionnez l'interface que le routeur distant utilisera pour la connexion VPN dans la liste déroulante. Les options sont les suivantes :

- WAN1 : cette option utilise l'adresse IP de l'interface WAN1 (Wide Area Network 1) du routeur distant pour la connexion VPN.
- WAN2 : cette option utilise l'adresse IP de l'interface WAN2 du routeur distant pour la connexion VPN. Le WAN2 n'est pas disponible dans les routeurs à un seul WAN.
- USB1 : cette option utilise l'adresse IP de l'interface USB1 (Universal Serial Bus 1) du routeur distant pour la connexion VPN.
- USB2 : cette option utilise l'adresse IP de l'interface USB2 du routeur distant pour la connexion VPN. USB2 n'est pas disponible sur les routeurs USB simples.

Remarque : dans cet exemple, WAN1 est choisi.

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

Étape 10. Choisissez l'identificateur de l'interface WAN du routeur local dans la liste déroulante Remote Endpoint. Les options sont les suivantes :

- Static IP : cette option permet au routeur distant d'utiliser l'adresse IP statique du routeur local lors de l'établissement d'une connexion VPN. Si cette option est sélectionnée sur le routeur local, le routeur distant doit également être configuré avec la même option.
- FQDN : cette option utilise le nom de domaine complet (FQDN) de la route locale lors de l'établissement de la connexion VPN.
- Dynamic IP : cette option utilise l'adresse IP dynamique du routeur local lors de l'établissement d'une connexion VPN.

Remarque : l'identificateur d'interface sur le routeur distant doit être identique à l'identificateur d'interface du routeur local. Dans cet exemple, l'adresse IP statique est choisie.

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

Étape 11. Saisissez l'adresse IP WAN du routeur local.

Remarque : dans cet exemple, l'adresse IP est 124.123.122.121.

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:


Étape 12. Sélectionnez la case d'option correspondant à la méthode d'authentification IKE (Internet Key Exchange) dont vous avez besoin. Les options sont les suivantes :

- Preshared Key : cette option signifie que la connexion nécessite un mot de passe pour être établie. La clé pré-partagée doit être identique aux deux extrémités de la connexion VPN.
- Certificate : cette option signifie que la méthode d'authentification utilise un certificat généré par le routeur au lieu d'un mot de passe lors de la connexion.

Remarque : dans cet exemple, la clé pré-partagée est sélectionnée.

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable

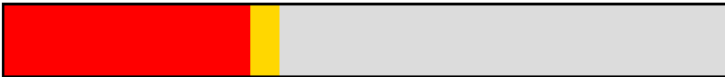
Show Pre-shared Key: Enable

Certificate:

Étape 13. Saisissez la clé pré-partagée pour la connexion VPN dans le champ Preshared Key (Clé pré-partagée).

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable

Certificate:

Étape 14. (Facultatif) Décochez la case Minimum Preshared Key Complexity (Complexité

minimale de la clé prépartagée) Enable (Activer) si vous souhaitez utiliser un mot de passe simple pour la connexion VPN. Cette option est activée par défaut.

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter:



Minimum Pre-shared Key Complexity:

Enable

Show Pre-shared Key:

Enable

Certificate:

Étape 15. (Facultatif) Cochez la case Afficher le texte brut lors de la modification Activer pour afficher la clé pré-partagée en texte brut. Cette option est désactivée par défaut.

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter:



Minimum Pre-shared Key Complexity:

Enable

Show Pre-shared Key:

Enable

Certificate:

Étape 16. Choisissez le type d'identificateur du réseau distant dans la liste déroulante Local Identifier Type du routeur distant. Les options sont les suivantes :

- Local WAN IP : cette option identifie le réseau distant via l'adresse IP WAN de l'interface.
- IP Address : cette option identifie le réseau distant via l'adresse IP locale.
- Local FQDN : cette option identifie le réseau distant via le FQDN, le cas échéant.
- Local User FQDN : cette option identifie le réseau distant via le nom de domaine complet de l'utilisateur, qui peut être son adresse e-mail.

Remarque : dans cet exemple, l'adresse IP est choisie.

Local Group Setup

Local Identifier Type:	<input type="text" value="IP Address"/>
Local Identifier:	<input type="text" value="Local WAN IP"/> <input type="text" value="IP Address"/> <input type="text" value="Local FQDN"/> <input type="text" value="Local User FQDN"/>
Local IP Type:	
IP Address:	<input type="text"/>
Subnet Mask:	<input type="text"/>

Étape 17. Entrez l'identificateur du réseau distant dans le champ Local Identifier du routeur distant.

Remarque : dans cet exemple, 124.123.122.123 est entré.

Local Group Setup

Local Identifier Type:	<input type="text" value="IP Address"/>
Local Identifier:	<input type="text" value="124.123.122.123"/>
Local IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text"/>
Subnet Mask:	<input type="text"/>

Étape 18. Sélectionnez le type d'adresse IP auquel le client VPN peut accéder dans la liste déroulante Local IP Type. Les options sont les suivantes :

- Subnet : cette option permet au côté local du VPN d'accéder aux hôtes distants dans le sous-réseau spécifié.
- IP Address : cette option permet au côté local du VPN d'accéder à l'hôte distant avec l'adresse IP spécifiée.
- Any : cette option permet au côté local du VPN d'accéder à n'importe quel hôte distant.

Local Group Setup

Local Identifier Type:	<input type="text" value="IP Address"/>
Local Identifier:	<input type="text" value="124.123.122.123"/>
Local IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text" value="Subnet"/>
Subnet Mask:	<input type="text" value="IP Address"/>

- Subnet
- IP Address
- IP Group
- GRE Interface
- Any

Remarque : dans cet exemple, Subnet est sélectionné.

Étape 19. Saisissez l'adresse IP du réseau ou de l'hôte auquel le client VPN doit accéder dans le champ IP Address.

Remarque : dans cet exemple, l'adresse IP est 192.168.2.1.

Local Group Setup

Local Identifier Type:	<input type="text" value="IP Address"/>
Local Identifier:	<input type="text" value="124.123.122.123"/>
Local IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text" value="192.168.2.1"/>
Subnet Mask:	<input type="text"/>

Étape 20. Saisissez le masque de sous-réseau de l'adresse IP dans le champ Subnet Mask.

Remarque : dans cet exemple, le masque de sous-réseau est 255.255.255.0.

Local Group Setup

Local Identifier Type:	<input type="text" value="IP Address"/>
Local Identifier:	<input type="text" value="124.123.122.123"/>
Local IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text" value="192.168.2.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>

Étape 21. Sélectionnez le type d'identificateur local dans la liste déroulante. Les options sont les suivantes :

- Remote WAN IP : cette option identifie le réseau local via l'adresse IP WAN de l'interface.
- Remote FQDN : cette option identifie le réseau local via le nom de domaine complet (FQDN), le cas échéant.
- Remote User FQDN : cette option identifie le réseau local via le nom de domaine complet de l'utilisateur, qui peut être son adresse e-mail.

Remarque : dans cet exemple, Remote WAN IP est sélectionné.

Remote Group Setup

Remote Identifier Type:	<input type="text" value="Remote WAN IP"/>
Remote Identifier:	<input type="text" value="124.123.122.121"/>
Remote IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text" value="10.10.10.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>

Étape 22. Cliquez sur Apply.

Add/Edit a New Connection

Apply

Cancel

Local IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text" value="192.168.2.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>

Remote Group Setup

Remote Identifier Type:	<input type="text" value="Remote WAN IP"/>
Remote Identifier:	<input type="text" value="124.123.122.121"/>
Remote IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text" value="10.10.10.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>

Étape 23. Cliquez sur Save.



cisco (admin)

English



Vous devez maintenant avoir configuré les paramètres VPN sur le routeur distant.

[Visionner une vidéo connexe à cet article...](#)

[Cliquez ici pour consulter les autres discussions techniques \(Tech Talks\) de Cisco](#)

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.