

# Configuration avancée d'un réseau privé virtuel (VPN) sur un routeur RV130 ou RV130W

## Objectif

Un réseau privé virtuel (VPN) est une connexion sécurisée établie au sein d'un réseau ou entre des réseaux. Les VPN servent à isoler le trafic entre les hôtes et les réseaux spécifiés du trafic des hôtes et des réseaux non autorisés. Un VPN site à site (passerelle à passerelle) connecte des réseaux entiers entre eux, assurant ainsi la sécurité en créant un tunnel sur un domaine public appelé Internet. Chaque site n'a besoin que d'une connexion locale au même réseau public, ce qui permet d'économiser de l'argent sur de longues lignes louées- privées.

Les VPN sont avantageux pour les entreprises car ils sont hautement évolutifs, simplifient la topologie du réseau et améliorent la productivité en réduisant les temps de déplacement et les coûts pour les utilisateurs distants.

IKE (Internet Key Exchange) est un protocole utilisé pour établir une connexion sécurisée pour la communication dans un VPN. Cette connexion sécurisée est appelée association de sécurité (SA). Vous pouvez créer des stratégies IKE pour définir les paramètres de sécurité à utiliser dans ce processus, tels que l'authentification de l'homologue, les algorithmes de chiffrement, etc. Pour qu'un VPN fonctionne correctement, les stratégies IKE des deux points d'extrémité doivent être identiques.

Cet article explique comment configurer la configuration VPN avancée sur un routeur RV130 ou RV130W, qui couvre les paramètres de stratégie IKE et de stratégie VPN.

## Périphériques pertinents

- RV130
- RV130W

## Version du logiciel

- 1.0.3.22

## Configurer la configuration VPN avancée

### Ajouter/Modifier les paramètres de stratégie IKE (Internet Key Exchange)

Étape 1. Connectez-vous à l'utilitaire Web et choisissez **VPN > Site-to-Site IPSec VPN > Advanced VPN Setup**.

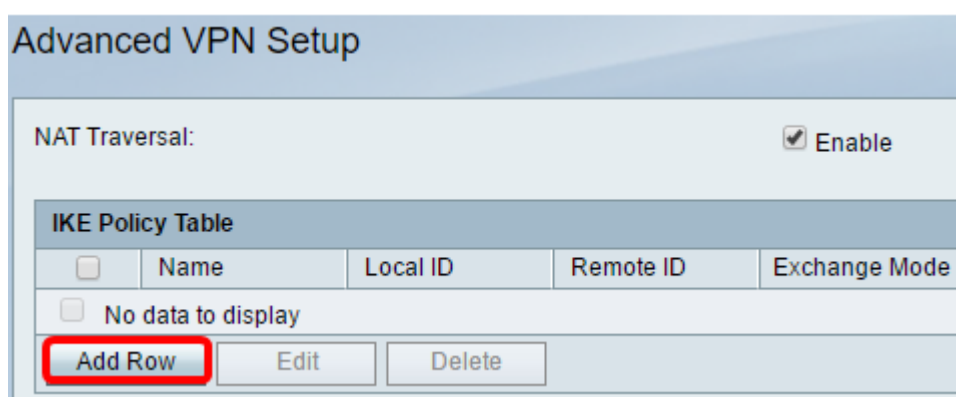


Étape 2. (Facultatif) Cochez la case **Enable** dans NAT Traversal si vous souhaitez activer la traduction d'adresses de réseau (NAT) Traversal pour la connexion VPN. La fonction NAT Traversal permet d'établir une connexion VPN entre des passerelles qui utilisent NAT. Choisissez cette option si votre connexion VPN passe par une passerelle compatible NAT.



Étape 3. Dans la table de stratégie IKE, cliquez sur **Add Row** pour créer une nouvelle stratégie IKE.

**Note:** Si des paramètres de base ont été configurés, le tableau ci-dessous contient les paramètres VPN de base créés. Vous pouvez modifier une stratégie IKE existante en cochant la case correspondant à la stratégie et en cliquant sur **Edit**. La page Advanced VPN Setup change :



Étape 4. Dans le champ *IKE Name*, entrez un nom unique pour la stratégie IKE.

**Note:** Si les paramètres de base ont été configurés, le nom de connexion créé est défini comme le nom IKE. Dans cet exemple, VPN1 est le nom IKE choisi.

## Advanced VPN Setup

**Add / Edit IKE Policy Configuration**

IKE Name:

Exchange Mode:

**Local**

Local Identifier Type:

Local Identifier:

**Remote**

Remote Identifier Type:

Remote Identifier:

**IKE SA Parameters**

Encryption Algorithm:

Authentication Algorithm:

Authentication Method:

Pre-Shared Key:

DH Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

Étape 5. Dans la liste déroulante Exchange Mode, sélectionnez une option.

- Main : cette option permet à la stratégie IKE de négocier le tunnel VPN avec une sécurité supérieure à celle du mode agressif. Cliquez sur cette option si une connexion VPN plus sécurisée est prioritaire sur la vitesse de négociation.
- Aggressive : cette option permet à la stratégie IKE d'établir une connexion plus rapide mais moins sécurisée que le mode principal. Cliquez sur cette option si une connexion VPN plus rapide est prioritaire sur une sécurité élevée.

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

## Advanced VPN Setup

### Add / Edit IKE Policy Configuration

IKE Name:	<input type="text" value="VPN1"/>
Exchange Mode:	<input type="text" value="Main"/>
Local	
Local Identifier Type:	<input type="text" value="Local WAN IP"/>

Étape 6. Faites votre choix dans la liste déroulante Type d'identificateur local pour identifier ou spécifier le protocole ISAKMP (Internet Security Association and Key Management Protocol) de votre routeur local. Les options sont les suivantes :

- Local WAN IP : le routeur utilise l'adresse IP WAN (Wide Area Network) locale comme identificateur principal. Cette option permet de se connecter via Internet. Si vous choisissez cette option, le champ *Identificateur local* est grisé ci-dessous.
- IP Address : cliquez sur ce bouton pour saisir une adresse IP dans le champ *Local Identifier*.
- FQDN : un nom de domaine complet (FQDN) ou votre nom de domaine tel que <http://www.example.com> vous permet d'entrer votre nom de domaine ou votre adresse IP dans le champ *Identificateur local*.
- User-FQDN : cette option est une adresse e-mail utilisateur telle que user@email.com. Entrez un nom de domaine ou une adresse IP dans le champ *Local Identifier*.
- DER ASN1 DN : cette option est un type d'identificateur pour le nom distinctif (DN) qui utilise la notation de syntaxe abstraite 1 des règles de codage distinctives (DER ASN1) pour transmettre des informations. Cela se produit lorsque le tunnel VPN est associé à un certificat utilisateur. Si cette option est sélectionnée, entrez un nom de domaine ou une adresse IP dans le champ *Local Identifier*.

**Note:** Dans cet exemple, Local WAN IP est sélectionné.

## Advanced VPN Setup

### Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

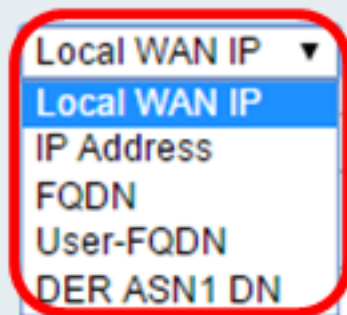
#### Local

Local Identifier Type:

Local Identifier:

#### Remote

Remote Identifier Type:



Étape 7. Faites votre choix dans la liste déroulante Remote Identifier Type pour identifier ou spécifier le protocole ISAKMP (Internet Security Association and Key Management Protocol) de votre routeur distant. Les options sont Remote WAN IP, IP Address, FQDN, User FQDN et DER ASN1 DN.

**Note:** Dans cet exemple, Remote WAN IP est sélectionné.

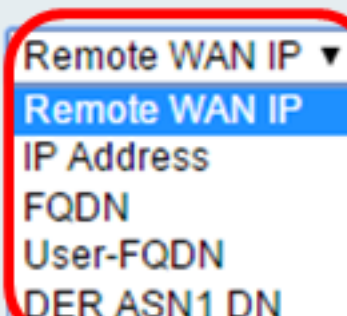
### Remote

Remote Identifier Type:

Remote Identifier:

#### IKE SA Parameters

Encryption Algorithm:

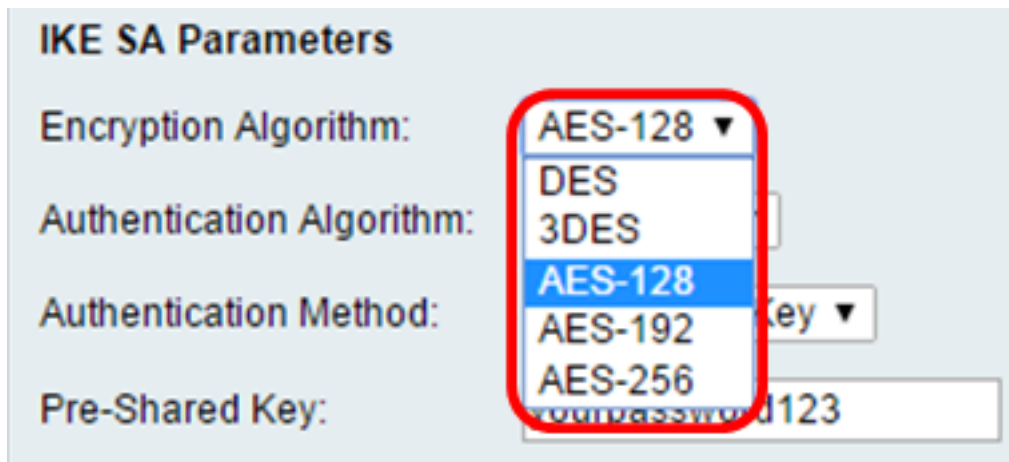


Étape 8. Choisissez une option dans la liste déroulante Algorithme de chiffrement.

- DES - Data Encryption Standard (DES) est une ancienne méthode de cryptage 56 bits qui n'est pas très sécurisée, mais qui peut être requise pour la rétrocompatibilité.
- 3DES : la norme 3DES (Triple Data Encryption Standard) est une méthode de chiffrement simple de 168 bits utilisée pour augmenter la taille de la clé, car elle chiffre les données trois fois. Cela offre plus de sécurité que DES, mais moins de sécurité que AES.
- AES-128 - Advanced Encryption Standard avec clé 128 bits (AES-128) utilise une clé 128 bits pour le cryptage AES. AES est plus rapide et plus sécurisé que DES. En général, AES est également plus rapide et plus sécurisé que 3DES. AES-128 est l'algorithme de chiffrement par défaut. Il est plus rapide mais moins sécurisé que les algorithmes AES-192 et AES-256.

- AES-192 : AES-192 utilise une clé 192 bits pour le cryptage AES. AES-192 est plus lent mais plus sécurisé que AES-128, et plus rapide mais moins sécurisé que AES-256.
- AES-256 : AES-256 utilise une clé de 256 bits pour le cryptage AES. AES-256 est plus lent mais plus sécurisé que AES-128 et AES-192.

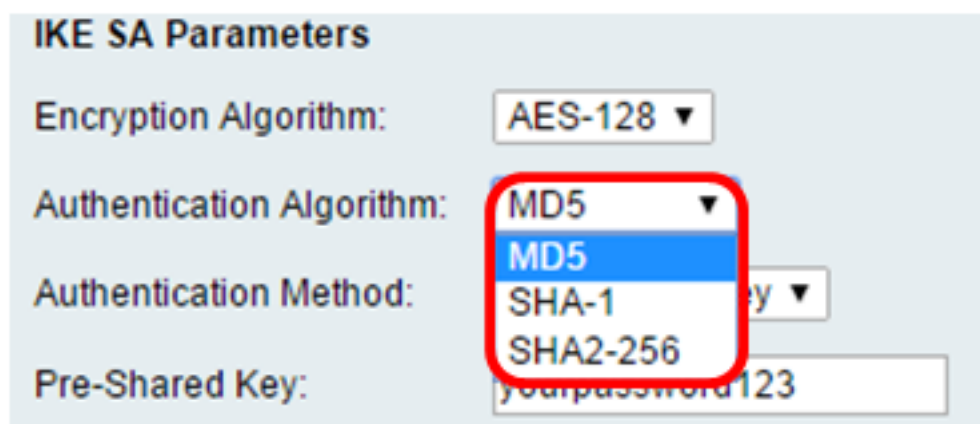
**Note:** Dans cet exemple, AES-128 est sélectionné.



Étape 9. Dans la liste déroulante Authentication Algorithm, sélectionnez l'une des options suivantes :

- MD5 - Message Digest 5 (MD5) est un algorithme d'authentification qui utilise une valeur de hachage de 128 bits pour l'authentification. MD5 est moins sécurisé, mais plus rapide que SHA-1 et SHA2-256.
- SHA-1 : la fonction SHA-1 (Secure Hash Function 1) utilise une valeur de hachage de 160 bits pour l'authentification. SHA-1 est plus lent mais plus sécurisé que MD5. SHA-1 est l'algorithme d'authentification par défaut et est plus rapide mais moins sécurisé que SHA2-256.
- SHA2-256 - L'algorithme de hachage sécurisé 2 avec une valeur de hachage de 256 bits (SHA2-256) utilise une valeur de hachage de 256 bits pour l'authentification. SHA2-256 est plus lent mais plus sécurisé que MD5 et SHA-1.

**Note:** Dans cet exemple, MD5 est choisi.

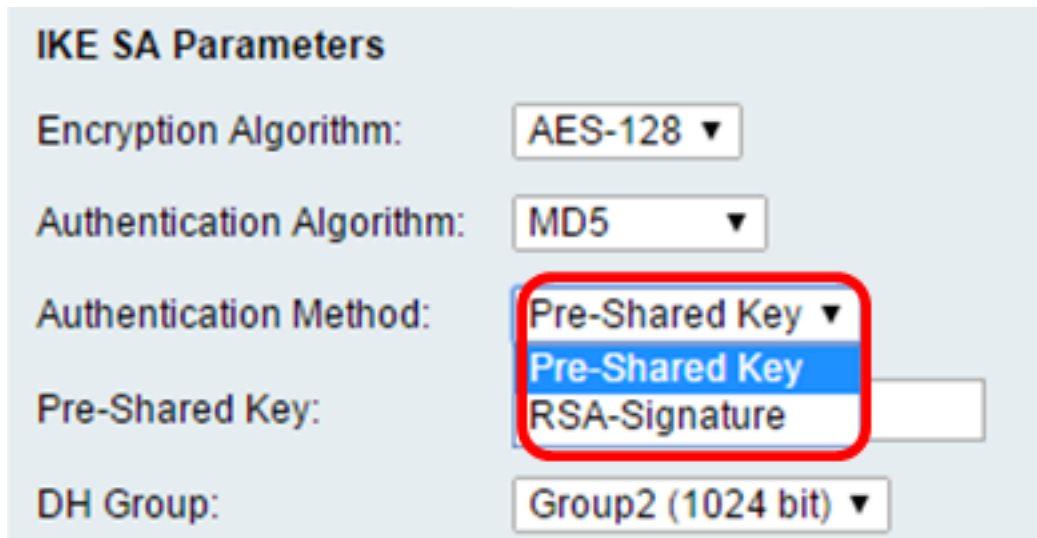


Étape 10. Dans la liste déroulante Authentication Method, choisissez parmi les options suivantes :

- Pre-Shared Key : cette option nécessite un mot de passe partagé avec l'homologue IKE.
- RSA-Signature : cette option utilise des certificats pour authentifier la connexion. Si cette

option est sélectionnée, le champ Clé pré-partagée est désactivé. Passez à l'[étape 12](#).

**Note:** Dans cet exemple, la clé pré-partagée est choisie.



**IKE SA Parameters**

Encryption Algorithm: AES-128 ▼

Authentication Algorithm: MD5 ▼

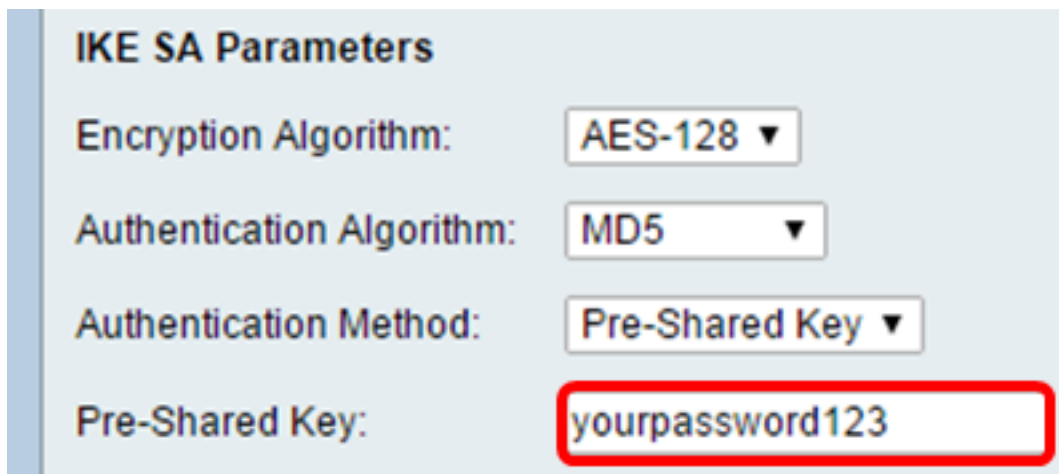
Authentication Method: Pre-Shared Key ▼  
Pre-Shared Key  
RSA-Signature

Pre-Shared Key:

DH Group: Group2 (1024 bit) ▼

Étape 11. Dans le champ *Pre-Shared Key*, saisissez un mot de passe comportant entre 8 et 49 caractères.

**Note:** Dans cet exemple, votre mot de passe 123 est utilisé.



**IKE SA Parameters**

Encryption Algorithm: AES-128 ▼

Authentication Algorithm: MD5 ▼

Authentication Method: Pre-Shared Key ▼

Pre-Shared Key: yourpassword123

[Étape 12](#). Dans la liste déroulante Groupe DH, sélectionnez l'algorithme de groupe Diffie-Hellman (DH) utilisé par l'IKE. Les hôtes d'un groupe DH peuvent échanger des clés à leur insu. Plus le nombre de bits de groupe est élevé, meilleure est la sécurité.

**Note:** Dans cet exemple, Group1 est sélectionné.



DH Group: Group1 (768 bit) ▼

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

Buttons: Save, Cancel, Back

Étape 13. Dans le champ *SA-Lifetime*, entrez la durée en secondes pendant laquelle une SA pour le VPN dure avant que la SA soit renouvelée. La plage est comprise entre 30 et 86400 secondes. Il est défini par défaut à 28800.

DH Group: Group1 (768 bit) ▼

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

Buttons: Save, Cancel, Back

[Étape 14.](#) (Facultatif) Cochez la case **Enable** Dead Peer Detection (Activer la détection des homologues morts) pour activer la détection des homologues morts (DPD). DPD surveille les homologues IKE pour voir si un homologue a cessé de fonctionner ou est toujours en vie. Si l'homologue est détecté comme étant mort, le périphérique supprime l'association de sécurité IPsec et IKE. DPD empêche le gaspillage des ressources réseau sur les homologues inactifs.

**Note:** Si vous ne souhaitez pas activer la détection d'homologue mort, passez à l'[étape 17.](#)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

Buttons: Save, Cancel, Back

Étape 15. (Facultatif) Si vous avez activé DPD à l'[étape 14](#), entrez la fréquence (en secondes) à laquelle l'activité de l'homologue est vérifiée dans le champ *Délai DPD*.

**Note:** Le délai DPD est l'intervalle en secondes entre les messages DPD R-U-THERE



consécutifs. Les messages DPD R-U-THERE sont envoyés uniquement lorsque le trafic IPsec est inactif. La valeur par défaut est 10.

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

Save Cancel Back

Étape 16. (Facultatif) Si vous avez activé DPD à l'[étape 14](#), entrez le délai d'attente en secondes avant qu'un homologue inactif ne soit abandonné dans le champ *Délai d'attente DPD*.

**Note:** Il s'agit de la durée maximale pendant laquelle le périphérique doit attendre de recevoir une réponse au message DPD avant de considérer que l'homologue est mort. La valeur par défaut est 30.

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

Save Cancel Back

[Étape 17](#). Cliquez sur **Save**.

## Advanced VPN Setup

### Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

#### Local

Local Identifier Type:

Local Identifier:

#### Remote

Remote Identifier Type:

Remote Identifier:

#### IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Authentication Method:

Pre-Shared Key:

DH Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

**Note:** La page principale Advanced VPN Setup réapparaît.

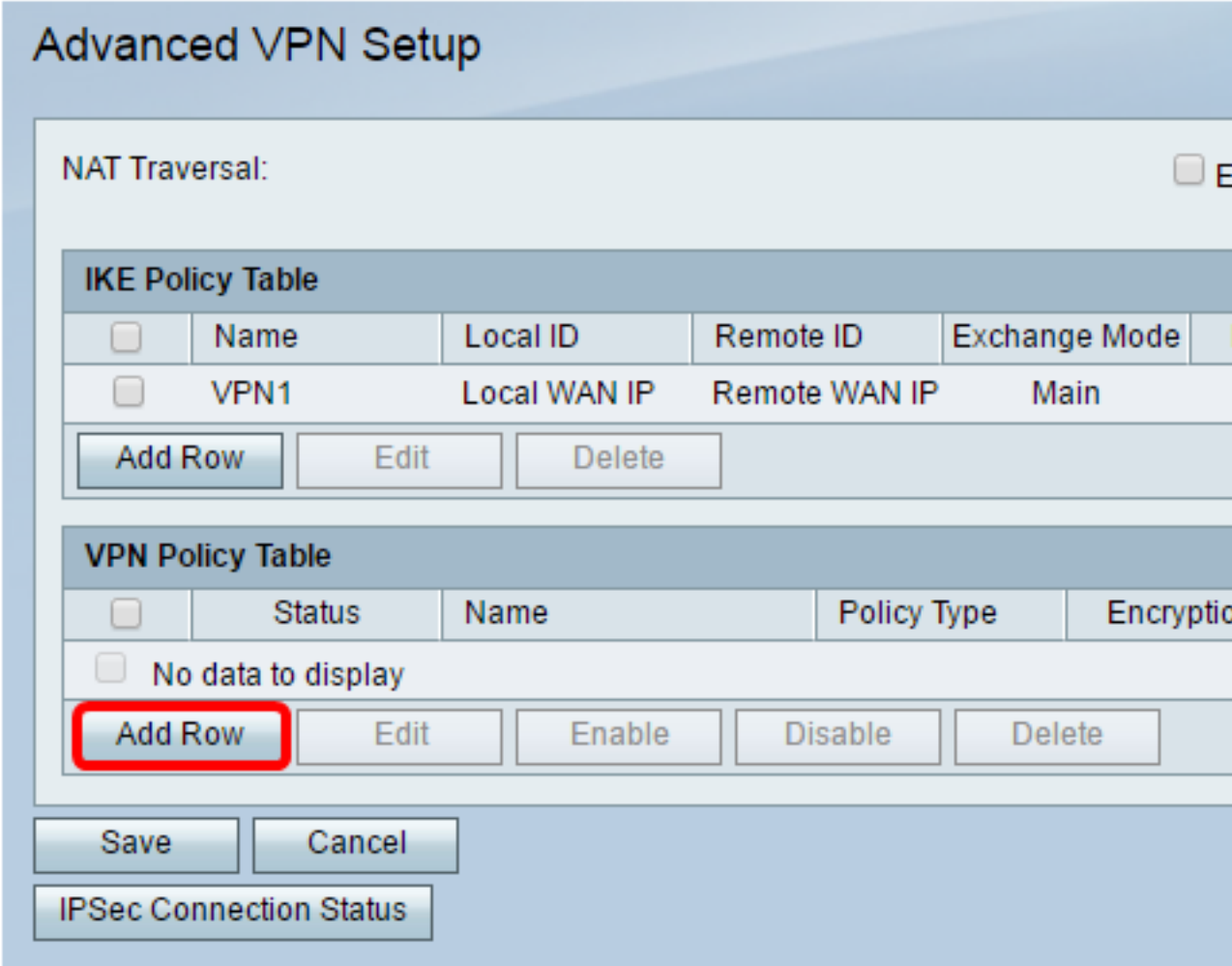
Vous devez maintenant avoir correctement configuré les paramètres de stratégie IKE sur votre routeur.

### Configuration des paramètres de stratégie VPN

**Remarque :** pour qu'un VPN fonctionne correctement, les stratégies VPN pour les deux points d'extrémité doivent être identiques.

Étape 1. Dans la table de stratégie VPN, cliquez sur **Add Row** pour créer une nouvelle stratégie VPN.

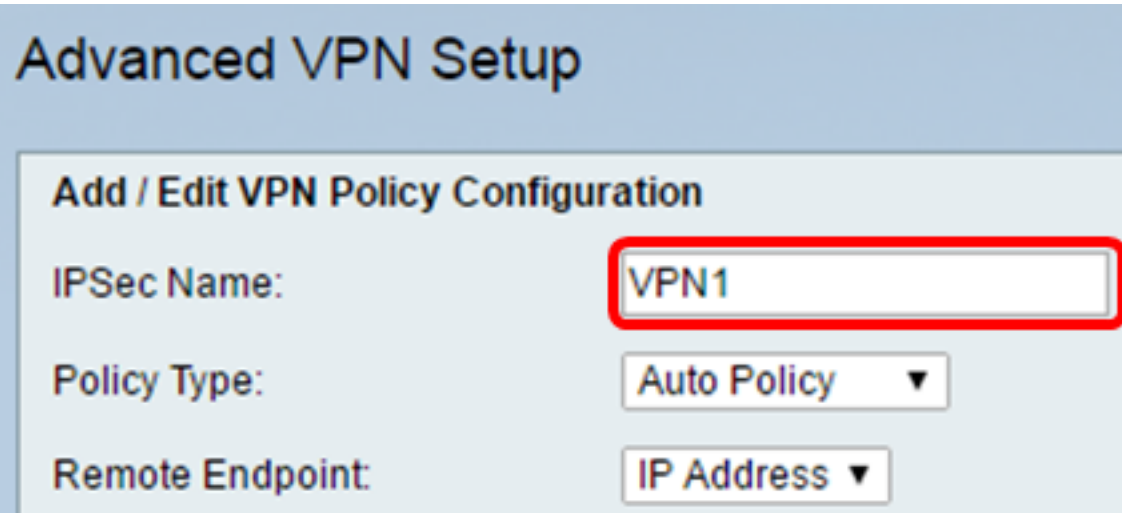
**Note:** Vous pouvez également modifier une stratégie VPN en cochant la case correspondant à la stratégie et en cliquant sur **Edit**. La page Advanced VPN Setup s'affiche :



The screenshot shows the 'Advanced VPN Setup' interface. At the top, there is a 'NAT Traversal' section with a checkbox. Below it is the 'IKE Policy Table' with columns for Name, Local ID, Remote ID, and Exchange Mode. A row for 'VPN1' is visible with columns for Local WAN IP, Remote WAN IP, and Main. Below the table are 'Add Row', 'Edit', and 'Delete' buttons. The 'VPN Policy Table' section below has columns for Status, Name, Policy Type, and Encryption. It shows 'No data to display' and has 'Add Row', 'Edit', 'Enable', 'Disable', and 'Delete' buttons. The 'Add Row' button in the VPN Policy Table is highlighted with a red box. At the bottom are 'Save', 'Cancel', and 'IPSec Connection Status' buttons.

Étape 2. Dans le champ *IPSec Name* de la zone Add/Edit VPN Configuration, entrez un nom pour la stratégie VPN.

**Note:** Dans cet exemple, VPN1 est utilisé.

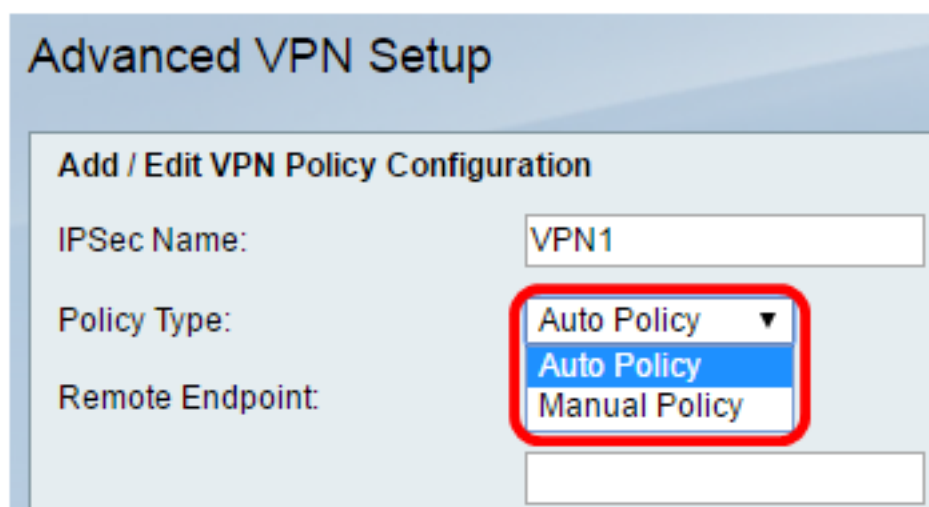


The screenshot shows the 'Advanced VPN Setup' interface, specifically the 'Add / Edit VPN Policy Configuration' section. It features three fields: 'IPSec Name' with the value 'VPN1' entered and highlighted by a red box; 'Policy Type' with a dropdown menu set to 'Auto Policy'; and 'Remote Endpoint' with a dropdown menu set to 'IP Address'.

Étape 3. Dans la liste déroulante Type de stratégie, sélectionnez une option.

- Manual Policy : cette option vous permet de configurer manuellement les clés de cryptage et d'intégrité des données pour le tunnel VPN. Si cette option est sélectionnée, les paramètres de configuration de la zone Paramètres de stratégie manuelle sont activés. Poursuivez les étapes jusqu'à Remote Traffic Selection. Cliquez [ici](#) pour connaître les étapes.
- Auto Policy : les paramètres de stratégie sont définis automatiquement. Cette option utilise une stratégie IKE 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. Cliquez [ici](#) pour connaître les étapes. Assurez-vous que votre protocole IKE négocie automatiquement entre les deux terminaux VPN.

**Note:** Dans cet exemple, Auto Policy est sélectionné.



Advanced VPN Setup

Add / Edit VPN Policy Configuration

IPSec Name: VPN1

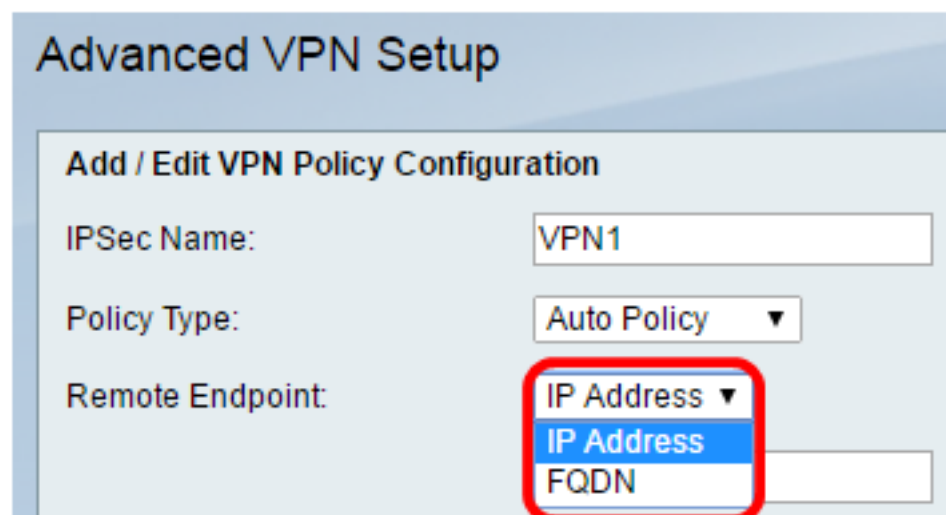
Policy Type: Auto Policy (selected)

Remote Endpoint:

Étape 4. Dans la liste déroulante Remote Endpoint, sélectionnez une option.

- IP Address : cette option identifie le réseau distant par une adresse IP publique.
- Nom de domaine complet (FQDN) : nom de domaine complet pour un ordinateur, un hôte ou Internet spécifique. Le FQDN se compose de deux parties : le nom d'hôte et le nom de domaine. Cette option ne peut être activée que si la **stratégie automatique** est sélectionnée à l'[étape 3](#).

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



Advanced VPN Setup

Add / Edit VPN Policy Configuration

IPSec Name: VPN1

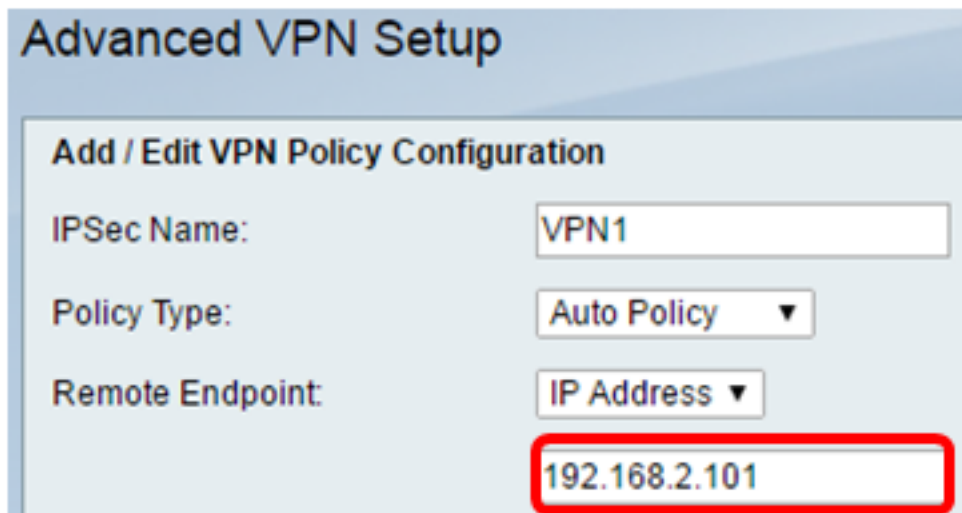
Policy Type: Auto Policy

Remote Endpoint: IP Address (selected)

Étape 5. Dans le champ *Remote Endpoint*, entrez l'adresse IP publique ou le nom de

domaine de l'adresse distante.

**Note:** Dans cet exemple, 192.168.2.101 est utilisé.



**Advanced VPN Setup**

**Add / Edit VPN Policy Configuration**

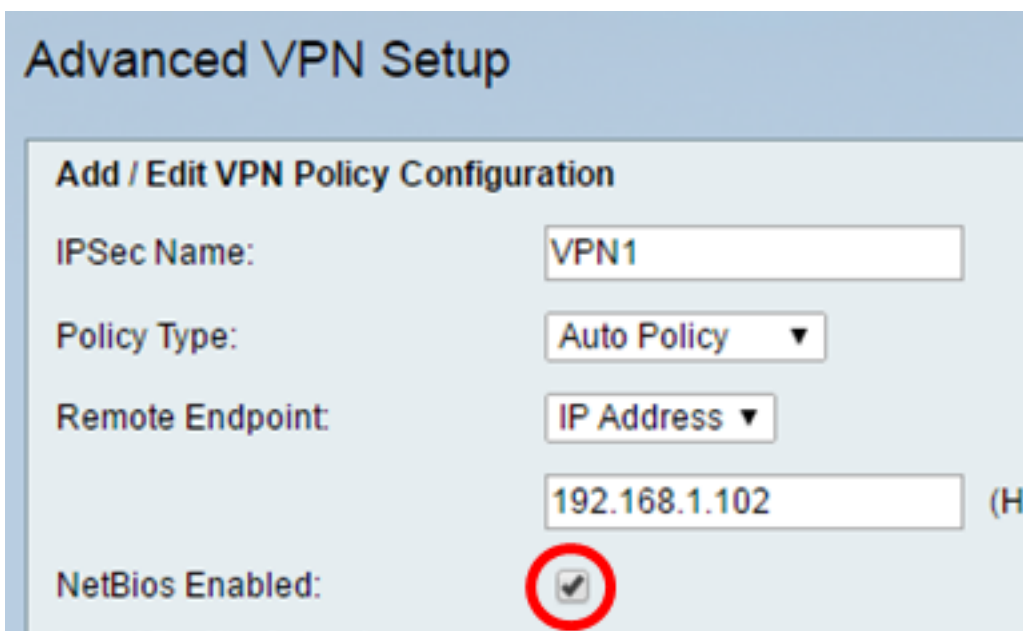
IPSec Name: VPN1

Policy Type: Auto Policy ▼

Remote Endpoint: IP Address ▼

192.168.2.101

Étape 6. (Facultatif) Cochez la case **NetBIOS Enabled** si vous souhaitez activer les diffusions NetBIOS (Network Basic Input/Output System) à envoyer via la connexion VPN. NetBIOS permet aux hôtes de communiquer entre eux au sein d'un réseau local (LAN).



**Advanced VPN Setup**

**Add / Edit VPN Policy Configuration**

IPSec Name: VPN1

Policy Type: Auto Policy ▼

Remote Endpoint: IP Address ▼

192.168.1.102 (Hi

NetBios Enabled:

Étape 7. Dans la liste déroulante Local IP sous la zone Local Traffic Selection, choisissez une option.

- Single : limite la stratégie à un hôte.
- Subnet : permet aux hôtes d'une plage d'adresses IP de se connecter au VPN.

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

**Local Traffic Selection**

Local IP:

IP Address:

Subnet Mask:

Étape 8. Dans le champ IP Address, saisissez l'adresse IP de l'hôte ou du sous-réseau local.

**Note:** Dans cet exemple, l'adresse IP de sous-réseau local 10.10.10.1 est utilisée.

**Local Traffic Selection**

Local IP:

IP Address:

Subnet Mask:

Étape 9. (Facultatif) Si Subnet est sélectionné à l'[étape 7](#), entrez le masque de sous-réseau du client dans le champ *Subnet Mask*. Le champ Subnet Mask (Masque de sous-réseau) est désactivé si Single est sélectionné à l'étape 1.

**Note:** Dans cet exemple, le masque de sous-réseau 255.255.0.0 est utilisé.

**Local Traffic Selection**

Local IP:

IP Address:

Subnet Mask:

[Étape 10](#). Dans la liste déroulante Remote IP sous la zone Remote Traffic Selection, choisissez une option.

- Single : limite la stratégie à un hôte.
- Subnet : permet aux hôtes d'une plage d'adresses IP de se connecter au VPN.

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

**Remote Traffic Selection**

Remote IP:

IP Address:

Subnet Mask:

Étape 11. Entrez la plage d'adresses IP de l'hôte qui fera partie du VPN dans le champ *IP Address*. Si **Single** est sélectionné à l'[étape 10](#), entrez une adresse IP.

**Note:** Dans l'exemple ci-dessous, 10.10.11.2 est utilisé.

**Remote Traffic Selection**

Remote IP:

IP Address:

Subnet Mask:

Étape 12. (Facultatif) Si **Subnet** est sélectionné à l'[étape 10](#), entrez le masque de sous-réseau de l'adresse IP de sous-réseau dans le champ *Subnet Mask*.

**Note:** Dans l'exemple ci-dessous, 255.255.0.0 est utilisé.

**Remote Traffic Selection**

Remote IP:

IP Address:  (Hint: 1.2.3.4)

Subnet Mask:  (Hint: 255.255.255.0)

### [Politique manuelle Paramètres](#)

**Remarque :** ces champs ne peuvent être modifiés que si l'option **Stratégie manuelle** est sélectionnée.

Étape 1. Dans le champ *SPI-Incoming*, entrez trois à huit caractères hexadécimaux pour la balise Security Parameter Index (SPI) pour le trafic entrant sur la connexion VPN. La balise SPI permet de distinguer le trafic d'une session du trafic des autres sessions.

**Note:** Pour cet exemple, 0xABCD est utilisé.



**Manual Policy Parameters**

SPI-Incoming:

SPI-Outgoing:

Étape 2. Dans le champ *SPI-Outgoing*, entrez trois à huit caractères hexadécimaux pour la balise SPI pour le trafic sortant sur la connexion VPN.

**Note:** Pour cet exemple, 0x1234 est utilisé.

**Manual Policy Parameters**

SPI-Incoming:

SPI-Outgoing:

Étape 3. Dans la liste déroulante Manual Encryption Algorithm, sélectionnez une option. Les options sont DES, 3DES, AES-128, AES-192 et AES-256.

**Note:** Dans cet exemple, AES-128 est choisi.

**Manual Policy Parameters**

SPI-Incoming:

SPI-Outgoing:

Manual Encryption Algorithm:

Key-In:

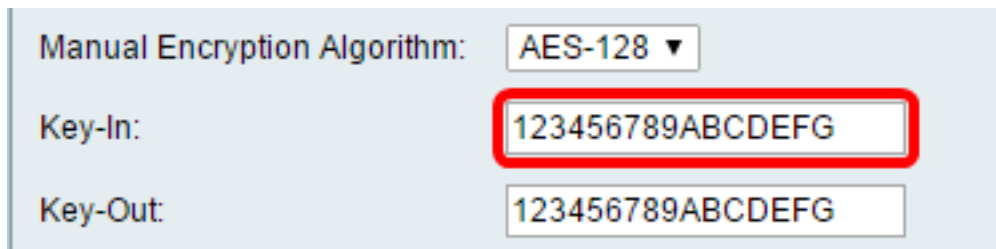
Key-Out:

Manual Integrity Algorithm:

Étape 4. Dans le champ *Key-In*, entrez une clé pour la stratégie entrante. La longueur de la clé dépend de l'algorithme choisi à l'[étape 3](#).

- DES utilise une clé à 8 caractères.
- 3DES utilise une touche de 24 caractères.
- AES-128 utilise une clé de 16 caractères.
- AES-192 utilise une clé de 24 caractères.
- AES-256 utilise une clé de 32 caractères.

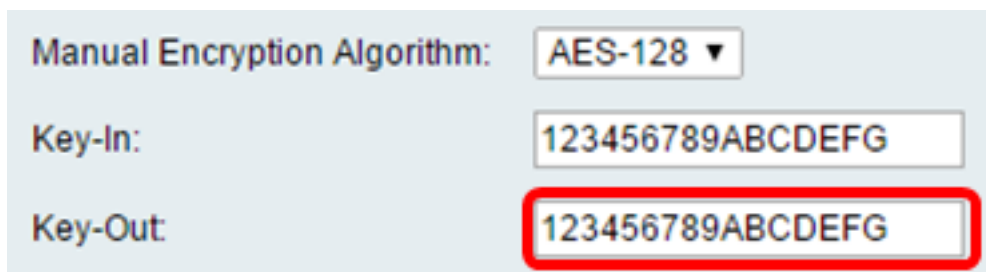
**Note:** Dans cet exemple, 123456789ABCDEFGG est utilisé.



Manual Encryption Algorithm: AES-128 ▼  
Key-In: 123456789ABCDEFGG  
Key-Out: 123456789ABCDEFGG

Étape 5. Dans le champ *Key-Out*, entrez une clé pour la stratégie sortante. La longueur de la clé dépend de l'algorithme choisi à l'[étape 3](#).

**Note:** Dans cet exemple, 123456789ABCDEFGG est utilisé.

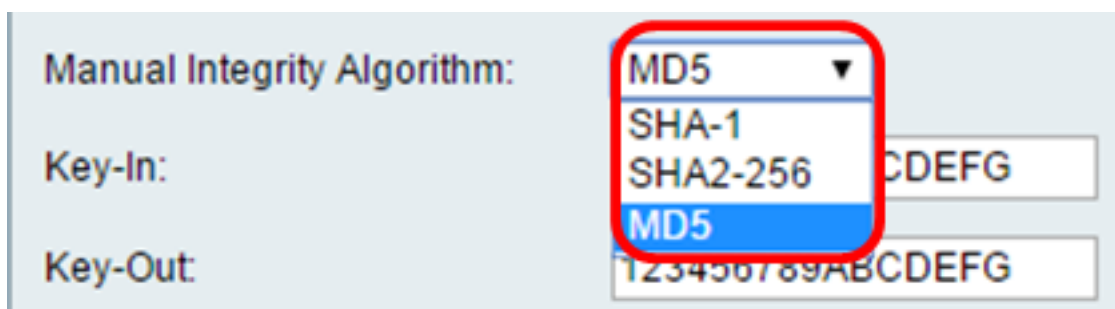


Manual Encryption Algorithm: AES-128 ▼  
Key-In: 123456789ABCDEFGG  
Key-Out: 123456789ABCDEFGG

[Étape 6](#). Dans la liste déroulante Manual Integrity Algorithm, sélectionnez une option.

- MD5 : utilise une valeur de hachage de 128 bits pour l'intégrité des données. MD5 est moins sécurisé mais plus rapide que SHA-1 et SHA2-256.
- SHA-1 : utilise une valeur de hachage de 160 bits pour l'intégrité des données. SHA-1 est plus lent mais plus sécurisé que MD5, et SHA-1 est plus rapide mais moins sécurisé que SHA2-256.
- SHA2-256 : utilise une valeur de hachage de 256 bits pour l'intégrité des données. SHA2-256 est plus lent mais plus sûr que MD5 et SHA-1.

**Note:** Dans cet exemple, MD5 est choisi.



Manual Integrity Algorithm: MD5 ▼  
Key-In: 123456789ABCDEFGG  
Key-Out: 123456789ABCDEFGG

Étape 7. Dans le *champ Key-In*, entrez une clé pour la stratégie entrante. La longueur de la clé dépend de l'algorithme choisi à l'[étape 6](#).

- MD5 utilise une clé de 16 caractères.
- SHA-1 utilise une clé de 20 caractères.
- SHA2-256 utilise une clé de 32 caractères.

**Note:** Dans cet exemple, 123456789ABCDEFGG est utilisé.

Manual Integrity Algorithm:	MD5 ▼
Key-In:	123456789ABCDEFGG
Key-Out:	123456789ABCDEFGG

Étape 8. Dans le *champ Key-Out*, entrez une clé pour la stratégie sortante. La longueur de la clé dépend de l'algorithme choisi à l'[étape 6](#).

**Note:** Dans cet exemple, 123456789ABCDEFGG est utilisé.

Manual Integrity Algorithm:	MD5 ▼
Key-In:	123456789ABCDEFGG
Key-Out:	123456789ABCDEFGG

### Auto Paramètres de stratégie

**Remarque :** avant de créer une stratégie Auto VPN, assurez-vous que vous créez la stratégie IKE en fonction de laquelle vous souhaitez créer la stratégie Auto VPN. Ces champs ne peuvent être modifiés que si la **stratégie Auto** est sélectionnée à l'[étape 3](#).

Étape 1. Dans le champ *IPSec SA-Lifetime*, entrez la durée en secondes de la SA avant le renouvellement. La plage est comprise entre 30 et 86400. La valeur par défaut est 3600.

Auto Policy Parameters	
IPSec SA Lifetime:	3600 Seconds (Range: 30 - 86400, Default 3600)
Encryption Algorithm:	AES-128 ▼
Integrity Algorithm:	SHA-1 ▼
PFS Key Group:	<input type="checkbox"/> Enable

Étape 2. Dans la liste déroulante Algorithme de chiffrement, sélectionnez une option. Les options sont les suivantes :

**Note:** Dans cet exemple, AES-128 est choisi.

- DES : ancienne méthode de cryptage 56 bits qui n'est pas une méthode de cryptage très sécurisée, mais qui peut être requise pour la rétrocompatibilité.
- 3DES : méthode de chiffrement simple de 168 bits utilisée pour augmenter la taille de la clé, car elle chiffre les données trois fois. Cela offre plus de sécurité que DES, mais moins de sécurité que AES.
- AES-128 : utilise une clé de 128 bits pour le cryptage AES. AES est plus rapide et plus

sécurisé que DES. En général, AES est également plus rapide et plus sécurisé que 3DES. AES-128 est plus rapide mais moins sécurisé que AES-192 et AES-256.

- AES-192 : utilise une clé 192 bits pour le cryptage AES. AES-192 est plus lent mais plus sécurisé que AES-128, et plus rapide mais moins sécurisé que AES-256.
- AES-256 : utilise une clé de 256 bits pour le cryptage AES. AES-256 est plus lent mais plus sécurisé que AES-128 et AES-192.
- AESGCM - Advanced Encryption Standard Le mode compteur de Galois est un mode de chiffrement par bloc de chiffrement authentifié générique. L'authentification GCM utilise des opérations particulièrement bien adaptées à une mise en oeuvre efficace dans le matériel, ce qui la rend particulièrement attrayante pour les mises en oeuvre à haut débit, ou pour les mises en oeuvre dans un circuit efficace et compact.
- AESCCM — Advanced Encryption Standard Counter with CBC-MAC Mode est un mode de chiffrement par bloc de chiffrement authentifié générique. CCM est parfaitement adapté aux mises en oeuvre logicielles compactes.

Auto Policy Parameters

IPSec SA Lifetime: 3600 Seco

Encryption Algorithm: AES-128 ▼

Integrity Algorithm:

PFS Key Group:

DH Group: (bit) ▼

Select IKE Policy:

View

Save Cancel Back

Étape 3. Dans la liste déroulante Algorithme d'intégrité, sélectionnez une option. Les options sont MD5, SHA-1 et SHA2-256.

**Note:** Dans cet exemple, SHA-1 est choisi.

Auto Policy Parameters

IPSec SA Lifetime: 3600 Seco

Encryption Algorithm: AES-128 ▼

Integrity Algorithm: SHA-1 ▼

PFS Key Group:

DH Group: (bit) ▼

Select IKE Policy: VPN1 ▼

Save Cancel Back

Étape 4. Cochez la case **Enable** dans le groupe de clés PFS pour activer Perfect Forward Secrecy (PFS). PFS augmente la sécurité VPN, mais ralentit la vitesse de connexion.

**Auto Policy Parameters**

IPSec SA Lifetime: 3600 Seconds

Encryption Algorithm: AES-128 ▼

Integrity Algorithm: SHA-1 ▼

PFS Key Group:  Enable

DH Group: Group 1(768 bit) ▼

Select IKE Policy: VPN1 ▼

View

Save Cancel Back

Étape 5. (Facultatif) Si vous avez choisi d'activer PFS à l'[étape 4](#), choisissez un groupe DH à rejoindre dans la liste déroulante Groupe DH. Plus le numéro de groupe est élevé, meilleure est la sécurité.

**Note:** Dans cet exemple, le groupe 1 est sélectionné.

**Auto Policy Parameters**

IPSec SA Lifetime: 3600 Seconds

Encryption Algorithm: AES-128 ▼

Integrity Algorithm: SHA-1 ▼

PFS Key Group:  Enable

DH Group: Group 1(768 bit) ▼

Select IKE Policy: VPN1 ▼

View

Save Cancel Back

Étape 6. Dans la liste déroulante Select IKE Policy, choisissez la stratégie IKE à utiliser pour la stratégie VPN.

**Note:** Dans cet exemple, une seule stratégie IKE a été configurée et une seule stratégie apparaît.

**Auto Policy Parameters**

IPSec SA Lifetime: 3600 Seconds (Ra)

Encryption Algorithm: AES-128 ▼

Integrity Algorithm: SHA-1 ▼

PFS Key Group:  Enable

DH Group: Group 1(768 bit) ▼

Select IKE Policy: **VPN1 ▼**

View

Save Cancel Back

Étape 7. Cliquez sur **Save**.

**Auto Policy Parameters**

IPSec SA Lifetime: 3600 Seconds (R)

Encryption Algorithm: AES-128 ▼

Integrity Algorithm: SHA-1 ▼

PFS Key Group:  Enable

DH Group: Group 1(768 bit) ▼

Select IKE Policy: VPN1 ▼

View

**Save** Cancel Back

**Note:** La page principale Advanced VPN Setup réapparaît. Un message de confirmation indiquant que les paramètres de configuration ont été correctement enregistrés doit s'afficher.

## Advanced VPN Setup



Configuration settings have been saved successfully

NAT Traversal:

### IKE Policy Table

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm
<input type="checkbox"/>	VPN1	Local WAN IP	Remote WAN IP	Main	AES-128

### VPN Policy Table

<input type="checkbox"/>	Status	Name	Policy Type	Encryption Algorithm	Authentication Alg
<input checked="" type="checkbox"/>	Disabled	VPN1	Auto Policy	AES-128	SHA-1

Étape 8. Sous le tableau VPN Policy, cochez une case pour choisir un VPN et cliquez sur **Enable**.

**Note:** La stratégie VPN configurée est désactivée par défaut.



## Advanced VPN Setup



Configuration settings have been saved successfully

NAT Traversal:

### IKE Policy Table

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm
<input type="checkbox"/>	VPN1	Local WAN IP	Remote WAN IP	Main	AES-128

Add Row

Edit

Delete

### VPN Policy Table

<input type="checkbox"/>	Status	Name	Policy Type	Encryption Algorithm	Authentication Alg
<input checked="" type="checkbox"/>	Disabled	VPN1	Auto Policy	AES-128	SHA-1

Add Row

Edit

Enable

Disable

Delete

Save

Cancel

IPSec Connection Status

Étape 9. Cliquez sur **Save**.

## Advanced VPN Setup



Configuration settings have been saved successfully

NAT Traversal:

### IKE Policy Table

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm
<input type="checkbox"/>	VPN1	Local WAN IP	Remote WAN IP	Main	AES-128

### VPN Policy Table

<input type="checkbox"/>	Status	Name	Policy Type	Encryption Algorithm	Authentication Alg
<input checked="" type="checkbox"/>	Disabled	VPN1	Auto Policy	AES-128	SHA-1

Vous devez maintenant avoir correctement configuré une stratégie VPN sur votre routeur RV130 ou RV130W.

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.