

Configuration VPN avancée sur le routeur VPN CVR100W

Objectif

Un réseau privé virtuel (VPN) est utilisé pour connecter des points d'extrémité sur différents réseaux sur un réseau public, tel qu'Internet. Cette fonctionnalité permet aux utilisateurs distants qui ne sont pas connectés à un réseau local de se connecter au réseau en toute sécurité via Internet.

Cet article explique comment configurer le VPN avancé sur le routeur VPN CVR100W. Pour la configuration VPN de base, reportez-vous à l'article [Basic VPN Setup sur le routeur VPN CVR100W](#).

Périphériques pertinents

Routeur VPN · CVR100W

Version du logiciel

•1.0.1.19

Configuration VPN avancée

Paramètres initiaux

Cette procédure explique comment configurer les paramètres initiaux de la configuration VPN avancée.

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **VPN > Advanced VPN Setup**. La page *Advanced VPN Setup* s'ouvre :

Advanced VPN Setup

NAT Traversal: Enable

NETBIOS: Enable

IKE Policy Table

<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input type="checkbox"/>	No data to display						

Add Row Edit Delete

VPN Policy Table

<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input type="checkbox"/>	No data to display						

Add Row Edit Enable Disable Delete

Save Cancel

IPSec Connection Status

Étape 2. (Facultatif) Pour activer la traversée NAT (Network Address Translation) pour la connexion VPN, cochez la case **Enable** dans le champ NAT Traversal. NAT Traversal permet d'établir une connexion VPN entre les passerelles qui utilisent NAT. Sélectionnez

cette option si votre connexion VPN passe par une passerelle compatible NAT.

Étape 3. (Facultatif) Pour activer les diffusions NetBIOS (Network Basic Input/Output System) à envoyer via la connexion VPN, cochez la case **Enable** dans le champ NETBIOS. NetBIOS permet aux hôtes de communiquer entre eux au sein d'un réseau local.

Paramètres de stratégie IKE

Internet Key Exchange (IKE) est un protocole utilisé pour établir une connexion sécurisée pour la communication dans un VPN. Cette connexion sécurisée établie est appelée association de sécurité (SA). Cette procédure explique comment configurer une stratégie IKE pour la connexion VPN à utiliser pour la sécurité. Pour qu'un VPN fonctionne correctement, les stratégies IKE pour les deux points d'extrémité doivent être identiques.

Advanced VPN Setup

NAT Traversal: Enable

NETBIOS: Enable

IKE Policy Table

<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input type="checkbox"/>	No data to display						

Add Row Edit Delete

VPN Policy Table

<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input type="checkbox"/>	No data to display						

Add Row Edit Enable Disable Delete

Save Cancel

IPSec Connection Status

Étape 1. Dans la table des stratégies IKE, cliquez sur **Ajouter une ligne** pour créer une nouvelle stratégie IKE. La page *Advanced VPN Setup* change :

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

Respondent Mode: Respondent
 Auto Manual

Local ID:
 (Hint: 1.2.3.4 or abc.com or @user-defined string or user-defined @ string.)
 Auto Manual

Remote ID:
 (Hint: 1.2.3.4 or abc.com or @user-defined string or user-defined @ string.)
 Auto Manual

Redundancy Remote ID:
 (Hint: 1.2.3.4 or abc.com or @user-defined string or user-defined @ string.)

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime: Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection: Enable

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

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

Étape 2. Dans le champ Policy Name, saisissez un nom pour la stratégie IKE.

Étape 3. Dans la liste déroulante Exchange Mode, sélectionnez une option pour identifier le fonctionnement de la stratégie IKE.

- Main : cette option permet à la stratégie IKE de fonctionner de manière plus sécurisée. Il est plus lent que le mode agressif. Sélectionnez cette option si une connexion VPN plus sécurisée est nécessaire.

- Aggressive : cette option permet à la stratégie IKE de fonctionner plus rapidement, mais elle est moins sécurisée que le mode principal. Sélectionnez cette option si une connexion VPN plus rapide est nécessaire.

Étape 4. (Facultatif) Pour activer le mode intime, cochez la case **Défendeur**. Si le mode intime est activé, le routeur VPN CVR100W ne peut recevoir la demande VPN que depuis le point d'extrémité VPN distant.

Étape 5. Dans le champ Local ID (ID local), cliquez sur la case d'option souhaitée pour indiquer comment spécifier l'ID local.

- Auto : cette option attribue automatiquement l'ID local.

- Manual : cette option permet d'attribuer manuellement l'ID local.

Étape 6. (Facultatif) Dans la liste déroulante Local ID, sélectionnez la méthode d'identification souhaitée pour le réseau local.

- IP Address : cette option identifie le réseau local par une adresse IP publique.
- FQDN : cette option utilise un nom de domaine complet (FQDN) pour identifier le réseau local.

Étape 7. (Facultatif) Dans le champ Local ID, saisissez l'adresse IP ou le nom de domaine. L'entrée dépend de l'option choisie à l'étape 6.

Étape 8. Dans le champ Remote ID (ID distant), cliquez sur la case d'option souhaitée pour indiquer comment spécifier l'ID distant.

- Auto : cette option attribue automatiquement l'ID distant.
- Manual : cette option permet d'attribuer manuellement un ID distant.

Étape 9. (Facultatif) Dans la liste déroulante ID distant, sélectionnez la méthode d'identification souhaitée pour le réseau distant.

- IP Address : cette option identifie le réseau distant par une adresse IP publique.
- FQDN : cette option utilise un nom de domaine complet (FQDN) pour identifier le réseau distant.

Étape 10. (Facultatif) Dans le champ Remote ID, saisissez l'adresse IP ou le nom de domaine. L'entrée dépend de l'option choisie à l'étape 9.

Étape 11. Dans le champ Redundancy Remote ID, cliquez sur la case d'option souhaitée pour identifier la manière de spécifier l'ID Redundancy Remote. L'ID distant de redondance est un autre ID distant utilisé pour configurer le tunnel VPN au niveau de la passerelle distante.

- Auto : cette option attribue automatiquement l'ID distant de redondance.
- Manual : cette option permet d'attribuer manuellement l'ID distant de redondance.

Étape 12. (Facultatif) Dans la liste déroulante Redundancy Remote ID, sélectionnez la méthode d'identification souhaitée pour le réseau de redondance.

- IP Address : cette option identifie le réseau distant redondant par une adresse IP publique.
- FQDN : cette option utilise un nom de domaine complet (FQDN) pour identifier le réseau distant redondant.

Étape 13. (Facultatif) Dans le champ Redundancy Remote ID, saisissez l'adresse IP ou le nom de domaine. L'entrée dépend de l'option choisie à l'étape 12.

IKE SA Parameters	
Encryption Algorithm:	AES-128 ▼
Authentication Algorithm:	SHA-1 ▼
Pre-Shared Key:	1234abcd
Diffie-Hellman (DH) Group:	Group1 (768 bit) ▼
SA-Lifetime:	3600 Seconds (Range: 30 - 86400, Default: 3600)
Dead Peer Detection:	<input checked="" type="checkbox"/> Enable
DPD Delay:	10 Seconds (Range: 10 - 999, Default: 10)
DPD Timeout:	30 Seconds (Range: 30 - 1000, Default: 30)

Étape 14. Dans la liste déroulante Encryption Algorithm, sélectionnez une option pour négocier l'association de sécurité (SA).

- DES - Data Encryption Standard (DES) utilise une taille de clé de 56 bits pour le chiffrement des données. DES est obsolète et doit être utilisé si un seul terminal prend en charge DES uniquement.
- 3DES - La norme 3DES (Triple Data Encryption Standard) effectue des DES trois fois, mais varie la taille de la clé de 168 bits à 112 bits et de 112 bits à 56 bits selon l'arrondi des DES effectué. 3DES est plus sécurisé que DES et AES.
- AES-128 — Advanced Encryption Standard avec clé 128 bits (AES-128) utilise une clé 128 bits pour le chiffrement AES. AES est plus rapide et plus sécurisé que DES. Certains types de matériel permettent à 3DES d'être plus rapide. La norme AES-128 est plus rapide mais moins sécurisée que les normes AES-192 et AES-256.
- AES-192 — AES-192 utilise une clé 192 bits pour le chiffrement AES. AES-192 est plus lent mais plus sécurisé que AES-128, et AES-192 est plus rapide mais moins sécurisé que AES-256.
- AES-256 — AES-256 utilise une clé de 256 bits pour le chiffrement AES. AES-256 est plus lent mais plus sécurisé que AES-128 et AES-192.

Étape 15. Dans la liste déroulante Authentication Algorithm, sélectionnez une option pour authentifier l'en-tête VPN.

- MD5 — Message-Digest Algorithm 5 (MD5) 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 — Secure Hash Algorithm 1 (SHA-1) utilise une valeur de hachage de 160 bits pour l'authentification. SHA-1 est plus lent mais plus sécurisé que MD5, et SHA-1 est plus rapide mais moins sécurisé que SHA2-256.
- SHA2-256 — L'algorithme de hachage sécurisé 2 (SHA2-256) utilise une valeur de hachage de 256 bits pour l'authentification. SHA2-256 est plus lent mais plus sûr que MD5 et SHA-1.

Étape 16. Dans le champ Pre-Shared Key (Clé prépartagée), saisissez une clé prépartagée

utilisée par la stratégie IKE.

Étape 17. Dans la liste déroulante Diffie-Hellman (DH) Group, sélectionnez le groupe DH utilisé par IKE. Les hôtes d'un groupe DH peuvent échanger des clés sans connaissance mutuelle. Plus le nombre de bits du groupe est élevé, plus le groupe est sécurisé.

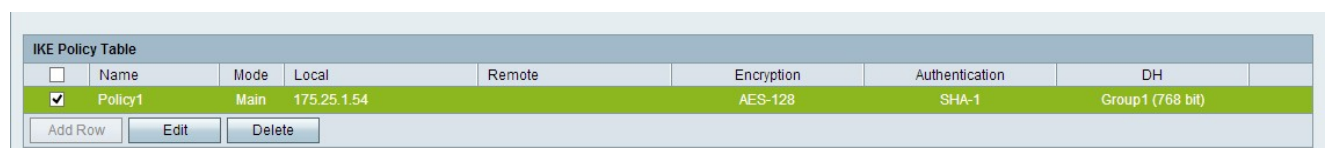
Étape 18. Dans le champ SA-Lifetime, saisissez la durée (en secondes) pendant laquelle l'association de sécurité (SA) du VPN dure avant le renouvellement de l'association de sécurité.

Étape 19. (Facultatif) Pour activer la détection DPD (Dead Peer Detection), cochez la case **Enable** dans le champ Dead Peer Detection. DPD est utilisé pour surveiller les homologues IKE afin de vérifier si un homologue a cessé de fonctionner. DPD empêche le gaspillage de ressources réseau sur les homologues inactifs.

Étape 20. (Facultatif) Pour indiquer la fréquence à laquelle l'homologue est vérifié pour l'activité, saisissez l'intervalle de temps (en secondes) dans le champ DPD Delay. Cette option est disponible si DPD est activé à l'étape 19.

Étape 21. (Facultatif) Pour indiquer le délai d'attente avant la suppression d'un homologue inactif, saisissez le délai (en secondes) dans le champ DPD Timeout. Cette option est disponible si DPD est activé à l'étape 19.

Étape 22. Cliquez sur **Save**. La page *Advanced VPN Setup* d'origine réapparaît.



<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input checked="" type="checkbox"/>	Policy1	Main	175.25.1.54		AES-128	SHA-1	Group 1 (768 bit)

Add Row Edit Delete

Étape 23. (Facultatif) Pour modifier une stratégie IKE dans la table de stratégies IKE, cochez la case correspondant à la stratégie. Ensuite, cliquez sur **Modifier**, modifiez les champs requis, puis cliquez sur **Enregistrer**.

Étape 24. (Facultatif) Pour supprimer une stratégie IKE dans la table des stratégies IKE, cochez la case correspondant à la stratégie et cliquez sur **Supprimer**. Cliquez ensuite sur **Enregistrer**.

Paramètres de stratégie VPN

Cette procédure explique comment configurer une stratégie VPN pour la connexion VPN à utiliser. Pour qu'un VPN fonctionne correctement, les stratégies VPN pour les deux points d'extrémité doivent être identiques.

Advanced VPN Setup

NAT Traversal: Enable

NETBIOS: Enable

IKE Policy Table

<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input type="checkbox"/>	Policy1	Main	175.25.1.54		AES-128	SHA-1	Group1 (768 bit)

VPN Policy Table

<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input type="checkbox"/>	No data to display						

Étape 1. Dans la table des stratégies VPN, cliquez sur **Ajouter une ligne** pour créer une nouvelle stratégie VPN. La page *Advanced VPN Setup* change :

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint:

(Hint: 1.2.3.4 or abc.com)

Redundancy Endpoint: Enable

(Hint: 1.2.3.4 or abc.com)

Rollback enable

Local Traffic Selection

Local IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Remote Traffic Selection

Remote IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

Auto Policy Parameters

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

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: Enable

Select IKE Policy:

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type: ▼

Remote Endpoint: ▼

(Hint: 1.2.3.4 or abc.com)

Redundancy Endpoint: Enable

▼

(Hint: 1.2.3.4 or abc.com)

Rollback enable

Étape 2. Dans le champ Policy Name, saisissez un nom pour la stratégie VPN.

Étape 3. Dans la liste déroulante Type de stratégie, sélectionnez une option pour identifier la manière dont les paramètres du tunnel VPN sont générés.

- Manual Policy : cette option vous permet de configurer les clés pour le chiffrement et l'intégrité des données.

- Auto Policy : cette option utilise une stratégie IKE pour l'intégrité des données et les échanges de clés de chiffrement.

Étape 4. Dans la liste déroulante Remote Endpoint, sélectionnez une option pour spécifier comment attribuer manuellement l'ID distant.

- IP Address : cette option identifie le réseau distant par une adresse IP publique.

- FQDN : cette option utilise un nom de domaine complet (FQDN) pour identifier le réseau distant.

Étape 5. Dans le champ de saisie de texte situé sous la liste déroulante Remote Endpoint, saisissez l'adresse IP publique ou le nom de domaine de l'adresse distante.

Étape 6. (Facultatif) Pour activer la redondance, cochez la case **Enable** dans le champ Redundancy Endpoint. L'option de point d'extrémité de redondance permet au routeur VPN CVR100W de se connecter à un point d'extrémité VPN de secours en cas d'échec de la connexion VPN principale.

Étape 7. (Facultatif) Pour attribuer manuellement l'ID de redondance, sélectionnez une option dans la liste déroulante Redundancy Endpoint.

- IP Address : cette option identifie le réseau distant redondant par une adresse IP publique.

- FQDN : cette option utilise un nom de domaine complet (FQDN) pour identifier le réseau distant redondant.

Étape 8. (Facultatif) Pour saisir l'adresse de redondance, dans le champ de saisie de texte situé sous la liste déroulante Redundancy Endpoint, saisissez l'adresse IP publique ou le nom de domaine.

Étape 9. (Facultatif) Pour activer la restauration, cochez la case **Rollback enable**. Cette option active la commutation automatique de la connexion VPN de secours à la connexion VPN principale lorsque la connexion VPN principale a récupéré d'une défaillance.

Local Traffic Selection		
Local IP:	<input type="text" value="Subnet"/>	
IP Address:	<input type="text" value="192.168.1.1"/>	(Hint: 1.2.3.4)
Subnet Mask:	<input type="text" value="255.255.255.0"/>	(Hint: 255.255.255.0)
Remote Traffic Selection		
Remote IP:	<input type="text" value="Subnet"/>	
IP Address:	<input type="text" value="10.1.1.1"/>	(Hint: 1.2.3.4)
Subnet Mask:	<input type="text" value="255.0.0.0"/>	(Hint: 255.255.255.0)

Étape 10. Dans la liste déroulante Local IP, sélectionnez une option pour identifier les hôtes affectés par la stratégie.

- Single : cette option utilise un hôte unique comme point de connexion VPN local.
- Subnet : cette option utilise un sous-réseau du réseau local comme point de connexion VPN local.

Étape 11. Dans le champ IP Address, saisissez l'adresse IP de l'hôte ou du sous-réseau du sous-réseau ou de l'hôte local.

Étape 12. (Facultatif) Si l'option Subnet est sélectionnée à l'étape 10, saisissez le masque de sous-réseau du sous-réseau local dans le champ Subnet Mask (Masque de sous-réseau).

Étape 13. Dans la liste déroulante Remote IP, sélectionnez une option pour identifier les hôtes affectés par la stratégie.

- Single : cette option utilise un hôte unique comme point de connexion VPN distant.
- Subnet : cette option utilise un sous-réseau du réseau distant comme point de connexion VPN distant.

Étape 14. Dans le champ IP Address, saisissez l'adresse IP de l'hôte ou du sous-réseau du sous-réseau ou de l'hôte distant.

Étape 15. (Facultatif) Si l'option Subnet est sélectionnée à l'étape 13, saisissez le masque de sous-réseau du sous-réseau distant dans le champ Subnet Mask (Masque de sous-réseau).

Manual Policy Parameters	
SPI-Incoming:	<input type="text" value="0xABCD"/>
SPI-Outgoing:	<input type="text" value="0x1234"/>
Encryption Algorithm:	<input type="text" value="AES-128"/> ▼
Key-In:	<input type="text" value="12345678ABCDE"/>
Key-Out:	<input type="text" value="12345678ABCDE"/>
Integrity Algorithm:	<input type="text" value="SHA-1"/> ▼
Key-In:	<input type="text" value="12345678ABCD"/>
Key-Out:	<input type="text" value="12345678ABCD"/>

Note: Si l'option Politique manuelle est sélectionnée à l'étape 3, exécutez les étapes 16 à 23 ; sinon, passez à l'[étape 24](#).

Étape 16. Dans le champ SPI-Incoming, saisissez trois à huit caractères hexadécimaux pour la balise SPI (Security Parameter Index) pour le trafic entrant sur la connexion VPN. La balise SPI est utilisée pour distinguer le trafic d'une session du trafic d'autres sessions. Le SPI entrant d'un côté du tunnel doit être le SPI sortant de l'autre côté du tunnel.

Étape 17. Dans le champ SPI-Outgoing, saisissez trois à huit caractères hexadécimaux pour la balise SPI pour le trafic sortant sur la connexion VPN. La balise SPI est utilisée pour distinguer le trafic d'une session du trafic d'autres sessions. Le SPI sortant d'un côté du tunnel doit être le SPI entrant de l'autre côté du tunnel.

Étape 18. Dans la liste déroulante Encryption Algorithm, sélectionnez une option pour négocier l'association de sécurité (SA).

- DES - Data Encryption Standard (DES) utilise une taille de clé de 56 bits pour le chiffrement des données. DES est obsolète et doit être utilisé si un seul terminal prend en charge DES uniquement.
- 3DES - La norme 3DES (Triple Data Encryption Standard) effectue des DES trois fois, mais varie la taille de la clé de 168 bits à 112 bits et de 112 bits à 56 bits selon l'arrondi des DES effectué. 3DES est plus sécurisé que DES et AES.
- AES-128 — Advanced Encryption Standard avec clé 128 bits (AES-128) utilise une clé 128 bits pour le chiffrement AES. AES est plus rapide et plus sécurisé que DES. Certains types de matériel permettent à 3DES d'être plus rapide. La norme AES-128 est plus rapide mais moins sécurisée que les normes AES-192 et AES-256.
- AES-192 — AES-192 utilise une clé 192 bits pour le chiffrement AES. AES-192 est plus lent mais plus sécurisé que AES-128, et AES-192 est plus rapide mais moins sécurisé que AES-256.
- AES-256 — AES-256 utilise une clé de 256 bits pour le chiffrement AES. AES-256 est plus lent mais plus sécurisé que AES-128 et AES-192.

Étape 19. Dans le champ Key-In, saisissez une clé pour la stratégie entrante. La longueur de la clé dépend de l'algorithme choisi à l'étape 18.

- DES utilise une clé de 8 caractères.
- 3DES utilise une clé de 24 caractères.
- AES-128 utilise une clé de 12 caractères.
- AES-192 utilise une clé de 24 caractères.
- AES-256 utilise une clé de 32 caractères.

Étape 20. Dans le champ Key-Out, saisissez une clé pour la stratégie sortante. La longueur de la clé dépend de l'algorithme choisi à l'étape 18. La longueur de la clé dépend de l'algorithme choisi à l'étape 18.

- DES utilise une clé de 8 caractères.
- 3DES utilise une clé de 24 caractères.
- AES-128 utilise une clé de 12 caractères.
- AES-192 utilise une clé de 24 caractères.
- AES-256 utilise une clé de 32 caractères.

Étape 21. Dans la liste déroulante Integrity Algorithm, sélectionnez une option pour authentifier l'en-tête VPN.

- MD5 — Message-Digest Algorithm 5 (MD5) 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 — Secure Hash Algorithm 1 (SHA-1) utilise une valeur de hachage de 160 bits pour l'authentification. SHA-1 est plus lent mais plus sécurisé que MD5, et SHA-1 est plus rapide mais moins sécurisé que SHA2-256.
- SHA2-256 — L'algorithme de hachage sécurisé 2 (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.

Étape 22. Dans le champ Key-In, saisissez une clé pour la stratégie entrante. La longueur de la clé dépend de l'algorithme choisi à l'étape 21.

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

Étape 23. Dans le champ Key-Out, saisissez une clé pour la stratégie sortante. La longueur de la clé dépend de l'algorithme choisi à l'étape 21. La longueur de la clé dépend de l'algorithme choisi à l'étape 21.

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

Auto Policy Parameters	
SA-Lifetime:	<input type="text" value="28800"/> Seconds (Range: 30 - 86400, Default: 28800)
Encryption Algorithm:	<input type="text" value="AES-128"/> ▼
Integrity Algorithm:	<input type="text" value="SHA-1"/> ▼
PFS Key Group:	<input checked="" type="checkbox"/> Enable
	<input type="text" value="DH-Group 1(768 bit)"/> ▼
Select IKE Policy:	<input type="text" value="Policy1"/> ▼
	<input type="button" value="View"/>

Note: Si vous avez sélectionné Stratégie automatique à l'étape 3, exécutez les étapes 24 à 29 ; sinon, passez à l'[étape 31](#).

Étape 24. Dans le champ SA-Lifetime, saisissez la durée en secondes pendant laquelle la SA dure avant le renouvellement.

Étape 25. Dans la liste déroulante Encryption Algorithm, sélectionnez une option pour négocier l'association de sécurité (SA).

- DES - Data Encryption Standard (DES) utilise une taille de clé de 56 bits pour le chiffrement des données. DES est obsolète et doit être utilisé si un seul terminal prend en charge DES uniquement.
- 3DES - La norme 3DES (Triple Data Encryption Standard) effectue des DES trois fois, mais varie la taille de la clé de 168 bits à 112 bits et de 112 bits à 56 bits selon l'arrondi des DES effectué. 3DES est plus sécurisé que DES et AES.
- AES-128 — Advanced Encryption Standard avec clé 128 bits (AES-128) utilise une clé 128 bits pour le chiffrement AES. AES est plus rapide et plus sécurisé que DES. Certains types de matériel permettent à 3DES d'être plus rapide. La norme AES-128 est plus rapide mais moins sécurisée que les normes AES-192 et AES-256.
- AES-192 — AES-192 utilise une clé 192 bits pour le chiffrement AES. AES-192 est plus lent mais plus sécurisé que AES-128, et AES-192 est plus rapide mais moins sécurisé que AES-256.
- AES-256 — AES-256 utilise une clé de 256 bits pour le chiffrement AES. AES-256 est plus lent mais plus sécurisé que AES-128 et AES-192.

Étape 26. Dans la liste déroulante Integrity Algorithm, sélectionnez une option pour authentifier l'en-tête VPN.

- MD5 — Message-Digest Algorithm 5 (MD5) 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 — Secure Hash Algorithm 1 (SHA-1) utilise une valeur de hachage de 160 bits pour l'authentification. SHA-1 est plus lent mais plus sécurisé que MD5, et SHA-1 est plus rapide mais moins sécurisé que SHA2-256.

·SHA2-256 — L'algorithme de hachage sécurisé 2 (SHA2-256) utilise une valeur de hachage de 256 bits pour l'authentification. SHA2-256 est plus lent mais plus sûr que MD5 et SHA-1.

Étape 27. Cochez la case **Activer** dans le champ Groupe de clés PFS pour activer Perfect Forward Secrecy (PFS). Le protocole PFS augmente la sécurité VPN, mais ralentit la vitesse de connexion.

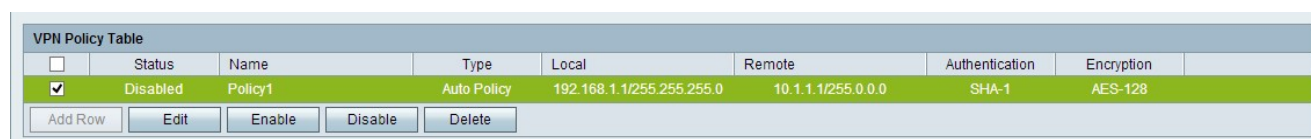
Étape 28. (Facultatif) Si vous avez choisi d'activer PFS à l'étape 27, sélectionnez un groupe Diffie-Hellman (DH) à joindre dans la liste déroulante, sous le champ Groupe de clés PFS. Plus le numéro de groupe est élevé, plus le groupe est sécurisé.

Étape 29. Dans la liste déroulante Select IKE Policy, sélectionnez la stratégie IKE à utiliser pour la stratégie VPN.

Étape 30. (Facultatif) Si vous cliquez sur **Affichage**, vous êtes dirigé vers la section Configuration IKE de la page *Configuration VPN avancée*.

Étape 31. Cliquez sur **Save**. La page *Advanced VPN Setup* d'origine réapparaît.

Étape 32. Cliquez sur **Save**.



<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input checked="" type="checkbox"/>	Disabled	Policy1	Auto Policy	192.168.1.1/255.255.255.0	10.1.1.1/255.0.0.0	SHA-1	AES-128

Étape 33. (Facultatif) Pour modifier une stratégie VPN dans la table de stratégie VPN, cochez la case correspondant à la stratégie. Cliquez ensuite sur **Modifier**, modifiez les champs requis, puis cliquez sur **Enregistrer**.

Étape 34. (Facultatif) Pour supprimer une stratégie VPN dans la table des stratégies VPN, cochez la case correspondant à la stratégie, cliquez sur **Supprimer**, puis sur **Enregistrer**.