Configuration VPN avancée sur RV215W

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. Cet article explique comment configurer la configuration VPN avancée sur le RV215W.

Périphériques pertinents

·RV215W

Version du logiciel

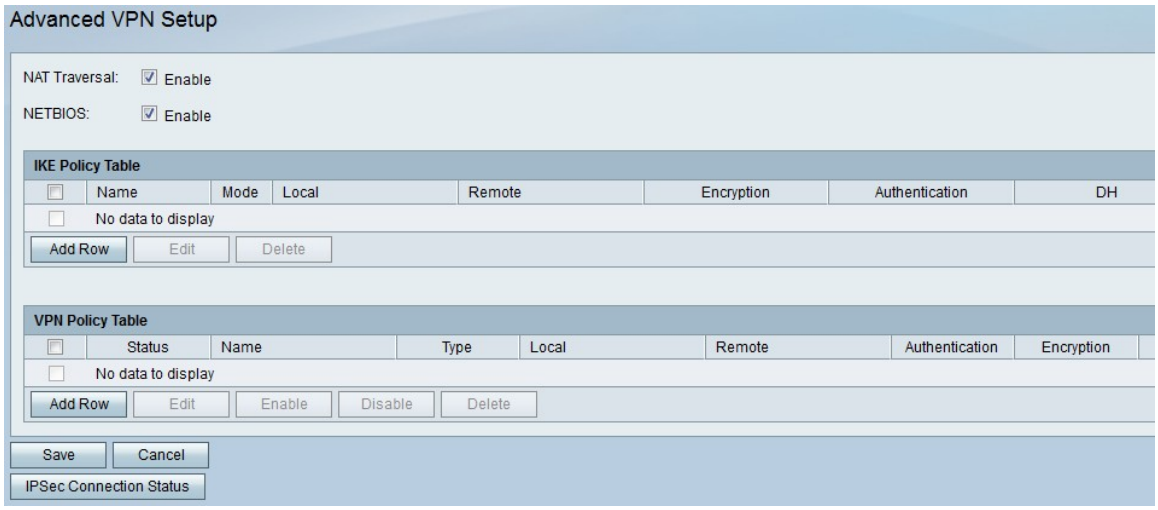
•1.1.0.5

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 :



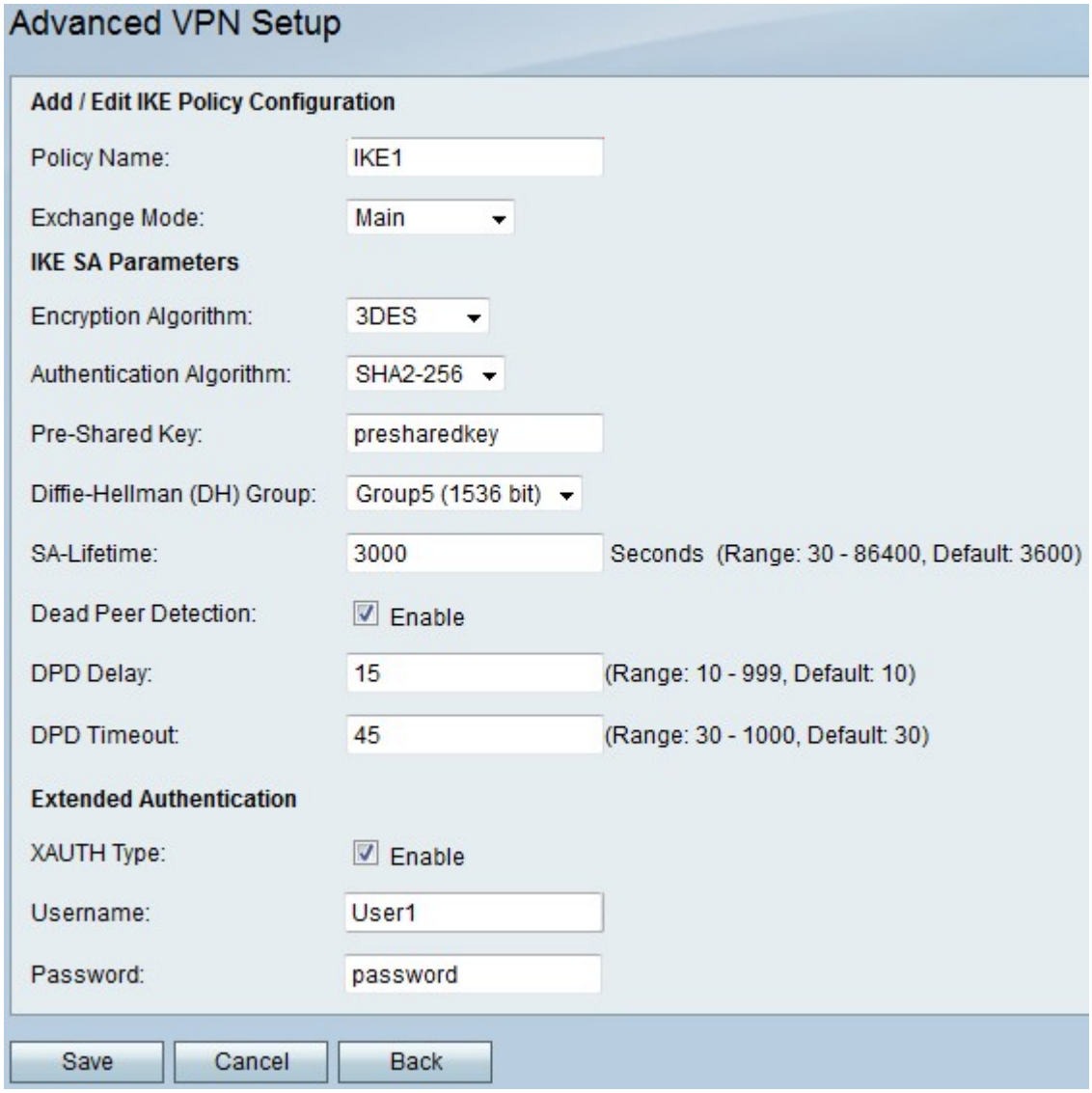
Étape 2. (Facultatif) Cochez la case **Activer** dans le champ Traversée NAT si vous voulez activer la traversée NAT (Network Address Translation) pour la connexion VPN. NAT Traversal permet d'établir une connexion VPN entre les passerelles qui utilisent NAT. Sélectionnez cette option si votre connexion VPN passe par une passerelle compatible NAT.

Étape 3. (Facultatif) Cochez la case **Activer** dans le champ NETBIOS si vous voulez 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.

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 établie et sécurisée 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.

Étape 1. Dans la table des stratégies IKE, cliquez sur **Ajouter une ligne** pour créer une nouvelle stratégie IKE. Pour modifier une stratégie IKE, cochez la case correspondant à la stratégie et cliquez sur **Modifier**. La page *Advanced VPN Setup* change :

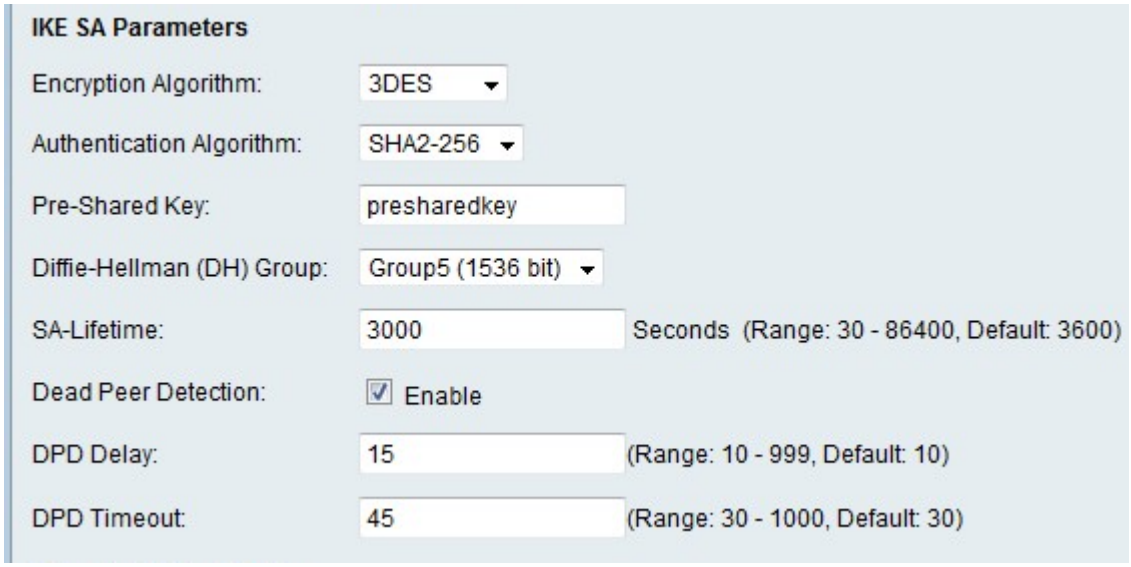


Étape 2. Dans le champ Policy Name, saisissez un nom pour la stratégie IKE.

Étape 3. Dans la liste déroulante Mode Exchange, sélectionnez une option.

·Main : cette option permet à la stratégie IKE de fonctionner en mode plus sécurisé mais 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 de manière moins sécurisée que le mode principal. Sélectionnez cette option si une connexion VPN plus rapide est nécessaire.



Étape 4. Dans la liste déroulante Encryption Algorithm, sélectionnez une option.

·DES - Data Encryption Standard (DES) est une 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 - La norme 3DES (Triple Data Encryption Standard) est une méthode de cryptage 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 qu'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. En général, AES est également plus rapide et plus sécurisé que 3DES. 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. La norme AES-192 est plus lente mais plus sécurisée que la norme AES-128, et plus rapide mais moins sécurisée que la norme 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 5. Dans la liste déroulante Authentication Algorithm, sélectionnez une option.

·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 — La fonction de hachage sécurisé 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 — Secure Hash Algorithm 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 sûr que MD5 et SHA-1.

Étape 6. Dans le champ Pre-Shared Key (Clé prépartagée), saisissez une clé prépartagée utilisée par la stratégie IKE.

Étape 7. 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

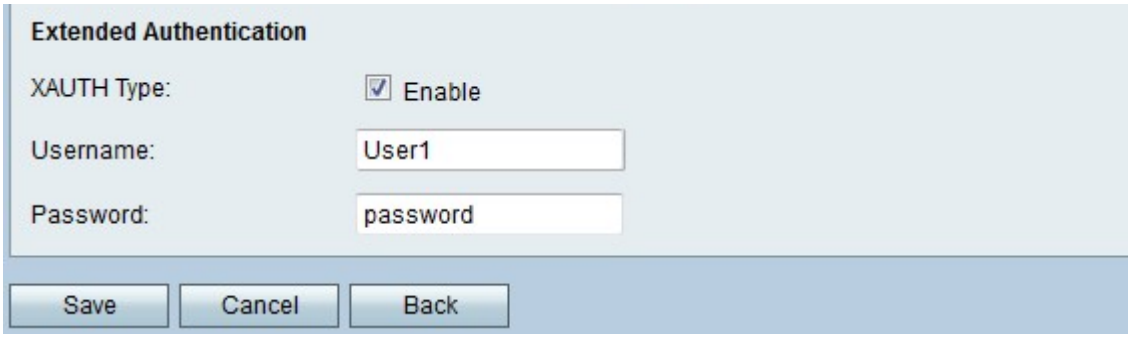
mutuelle. Plus le nombre de bits du groupe est élevé, plus le groupe est sécurisé.

Étape 8. Dans le champ SA-Lifetime, saisissez la durée en secondes pendant laquelle une SA pour le VPN dure avant le renouvellement de l'SA.

Étape 9. (Facultatif) Cochez la case **Activer** dans le champ 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. DPD empêche le gaspillage de ressources réseau sur les homologues inactifs.

Étape 10. (Facultatif) Si vous avez activé DPD à l'étape 9, entrez la fréquence (en secondes) à laquelle l'homologue est vérifié pour l'activité dans le champ DPD Delay.

Étape 11. (Facultatif) Si vous avez activé DPD à l'étape 9, saisissez le nombre de secondes à attendre avant qu'un homologue inactif ne soit supprimé dans le champ DPD Timeout.



Étape 12. (Facultatif) Cochez la case **Activer** dans le champ Type XAUTH pour activer l'authentification étendue (XAUTH). XAUTH permet à plusieurs utilisateurs d'utiliser une seule stratégie VPN plutôt qu'une stratégie VPN pour chaque utilisateur.

Étape 13. (Facultatif) Si vous avez activé XAUTH à l'étape 12, saisissez le nom d'utilisateur à utiliser pour la stratégie dans le champ Nom d'utilisateur.

Étape 14. (Facultatif) Si vous avez activé XAUTH à l'étape 12, saisissez le mot de passe à utiliser pour la stratégie dans le champ Password (Mot de passe).

Étape 15. Click **Save**. La page *Advanced VPN Setup* d'origine réapparaît.

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.

Étape 1. Dans la table des stratégies VPN, cliquez sur **Ajouter une ligne** pour créer une nouvelle stratégie VPN. Pour modifier une stratégie VPN, cochez la case correspondant à la stratégie et cliquez sur **Modifier**. La page *Advanced VPN Setup* change :

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name: VPN1

Policy Type: Manual Policy

Remote Endpoint: IP Address

209.165.201.1 (Hint: 1.2.3.4 or abc.com)

Local Traffic Selection

Local IP: Subnet

IP Address: 192.168.1.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

Remote Traffic Selection

Remote IP: Subnet

IP Address: 192.168.2.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

Manual Policy Parameters

SPI-Incoming: 0xABCD

SPI-Outgoing: 0x1234

Encryption Algorithm: AES-256

Key-In: 123456789012345678!

Key-Out: 123456789012345678!

Integrity Algorithm: SHA2-256

Key-In: 123456789012345678!

Key-Out: 123456789012345678!

Auto Policy Parameters

SA-Lifetime: 20000 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: AES-256

Integrity Algorithm: SHA2-256

PFS Key Group: Enable

DH-Group 1(768 bit)

Select IKE Policy: IKE1

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.

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

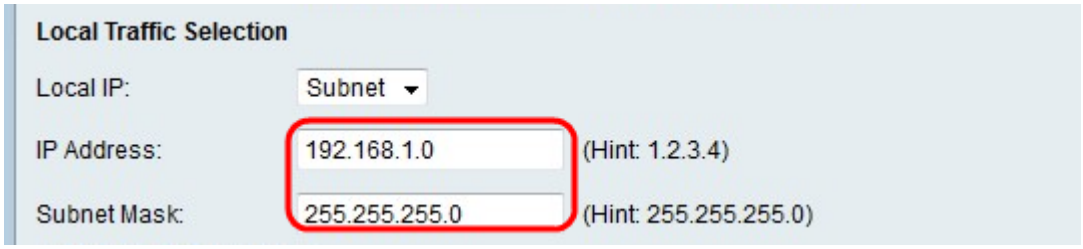
·Auto Policy : cette option utilise une stratégie IKE pour l'intégrité des données et les échanges de clés de chiffrement.

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

·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. Dans la liste déroulante Local IP, sélectionnez une option.

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

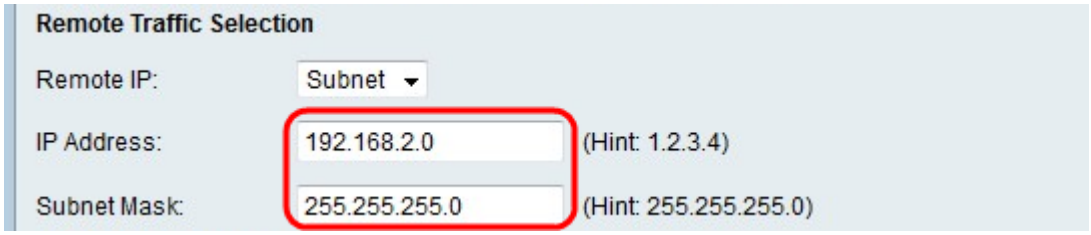
Étape 8. (Facultatif) Si vous avez sélectionné Sous-réseau à l'étape 6, saisissez le masque de sous-réseau du sous-réseau local dans le champ Masque de sous-réseau.

Étape 9. Dans la liste déroulante Remote IP, sélectionnez une option.

·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

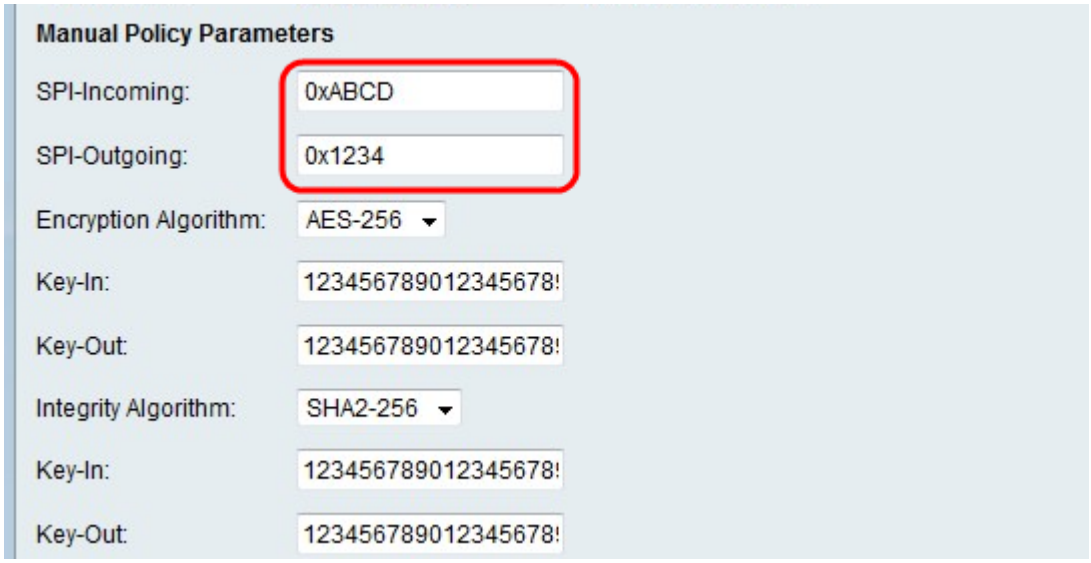
VPN distant.



Étape 10. 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 11. (Facultatif) Si vous avez sélectionné Sous-réseau à l'étape 9, saisissez le masque de sous-réseau du sous-réseau distant dans le champ Masque de sous-réseau.

Note: Si vous avez sélectionné Politique manuelle à l'étape 3, exécutez les étapes 12 à 19 ; sinon, passez à l'étape 20.



Étape 12. 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.

Étape 13. Dans le champ SPI-Outgoing, saisissez trois à huit caractères hexadécimaux pour la balise SPI pour le trafic sortant sur la connexion VPN.

Étape 14. Dans la liste déroulante Encryption Algorithm, sélectionnez une option.

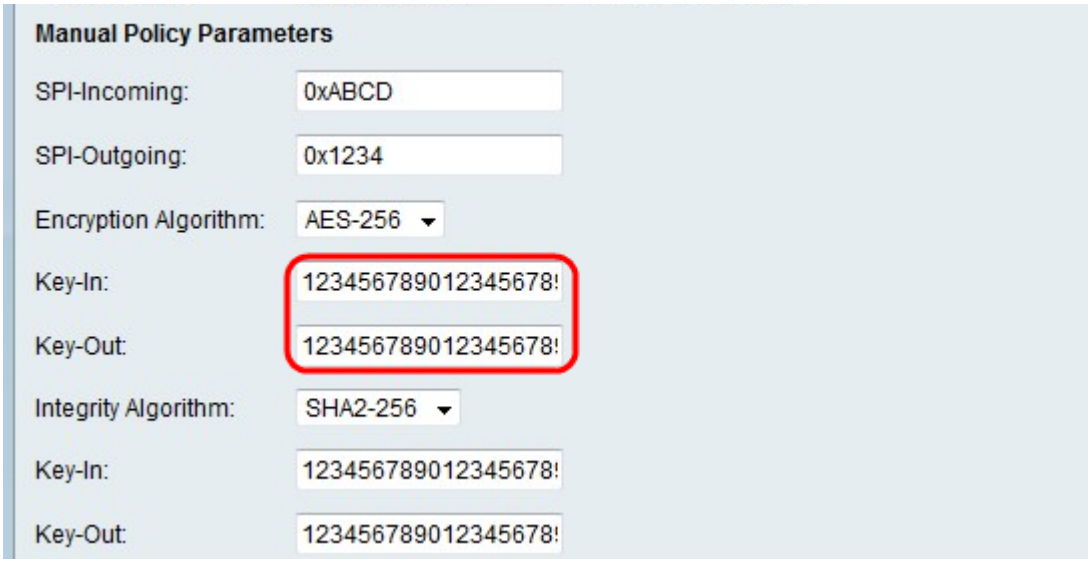
·DES - Data Encryption Standard (DES) est une ancienne méthode de cryptage 56 bits qui n'est pas une méthode de cryptage très sécurisée, mais qui peut être requise pour la rétrocompatibilité.

·3DES - La norme 3DES (Triple Data Encryption Standard) est une méthode de cryptage 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 qu'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. En général, AES est également plus rapide et plus sécurisé que 3DES. 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. La norme AES-192 est plus lente mais plus sécurisée que la norme AES-128, et plus rapide mais moins sécurisée que la norme 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 le champ Key-In, saisissez une clé pour la stratégie entrante. La longueur de la clé dépend de l'algorithme choisi à l'étape 14.

·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.

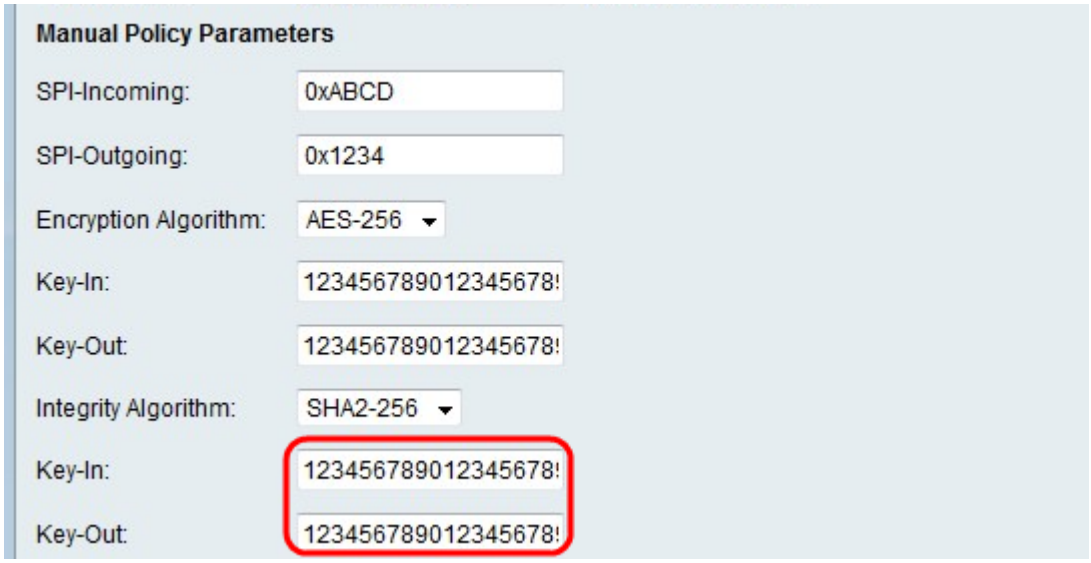
Étape 16. Dans le champ Key-Out, saisissez une clé pour la stratégie sortante. La longueur de la clé dépend de l'algorithme choisi à l'étape 14. Les longueurs de clé sont identiques à celles de l'étape 15.

Étape 17. Dans la liste déroulante Integrity Algorithm, sélectionnez une option.

·MD5 — Message-Digest Algorithm 5 (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 — La fonction de hachage sécurisé 1 (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 — Secure Hash Algorithm 2 avec une valeur de hachage de 256 bits (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.



Étape 18. 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 17.

·MD5 utilise une clé de 16 caractères.

·SHA-1 utilise une clé de 20 caractères.

·SHA2-256 utilise une clé de 32 caractères.

Étape 19. 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 17. Les longueurs de clé sont identiques à celles de l'étape 18.

Note: Si vous avez sélectionné Stratégie automatique à l'étape 3, exécutez les étapes 20 à 25 ; sinon, passez à l'étape 26.

Étape 20. Dans le champ SA-Lifetime, saisissez la durée en secondes pendant laquelle la SA dure avant le renouvellement.

Étape 21. Dans la liste déroulante Encryption Algorithm, sélectionnez une option.

·DES - Data Encryption Standard (DES) est une 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 - La norme 3DES (Triple Data Encryption Standard) est une méthode de cryptage

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 qu'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. En général, AES est également plus rapide et plus sécurisé que 3DES. 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. La norme AES-192 est plus lente mais plus sécurisée que la norme AES-128, et plus rapide mais moins sécurisée que la norme 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 22. Dans la liste déroulante Integrity Algorithm, sélectionnez une option.

·MD5 — Message-Digest Algorithm 5 (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 — La fonction de hachage sécurisé 1 (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 — Secure Hash Algorithm 2 avec une valeur de hachage de 256 bits (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.

Étape 23. Cochez la case **Activer** dans le groupe de clés PFS pour activer Perfect Forward Secrecy (PFS). Le protocole PFS augmente la sécurité VPN, mais ralentit la vitesse de connexion.

Étape 24. (Facultatif) Si vous avez choisi d'activer PFS à l'étape 23, sélectionnez un groupe Diffie-Hellman (DH) à rejoindre pour la liste déroulante ci-dessous. Plus le numéro de groupe est élevé, plus le groupe est sécurisé.

Étape 25. Dans la liste déroulante Select IKE Policy, sélectionnez la stratégie IKE à utiliser pour la stratégie VPN.

Note: Si vous cliquez sur **Affichage**, vous êtes dirigé vers la section Configuration IKE de la page *Configuration VPN avancée*.

Étape 26. Click **Save**. La page *Advanced VPN Setup* d'origine réapparaît.

Étape 27. Click **Save**.