Configuration de la configuration VPN avancée sur le pare-feu RV110W

Objectif

Le réseau privé virtuel (VPN) utilise le réseau public, ou Internet, pour établir un réseau privé permettant de communiquer en toute sécurité. Un IKE (Internet Key Exchange) est un protocole qui établit une communication sécurisée entre deux réseaux. Il est utilisé pour échanger une clé avant les flux de trafic, ce qui garantit l'authenticité des deux extrémités du tunnel VPN.

Les deux extrémités du VPN doivent suivre la même stratégie VPN pour communiquer entre elles.

L'objectif de ce document est d'expliquer comment ajouter un profil IKE et configurer une stratégie VPN sur le routeur sans fil RV110W.

Périphériques pertinents

·RV110W

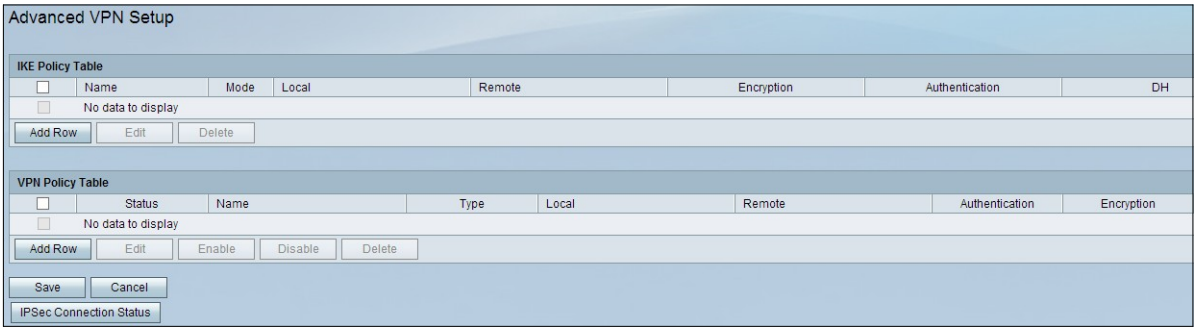
Version du logiciel

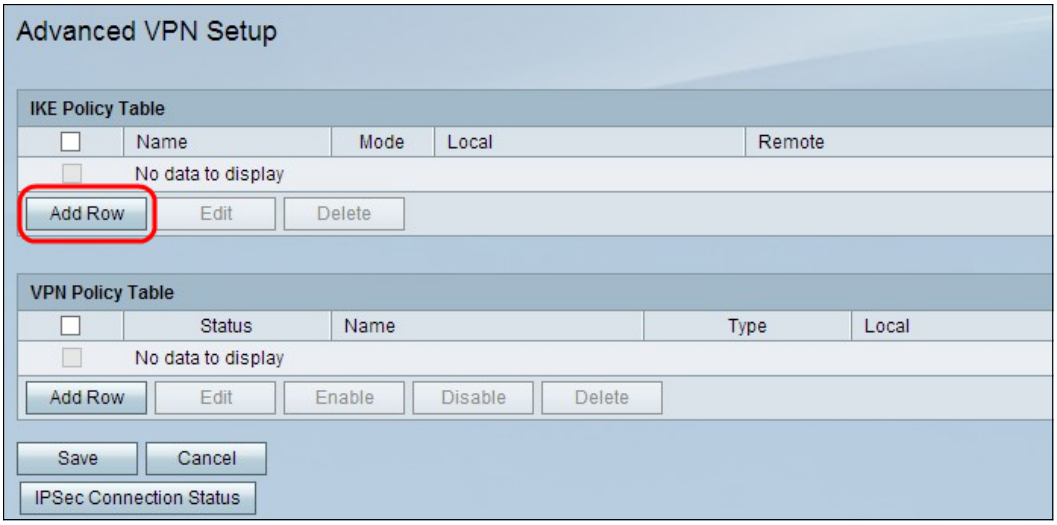
•1.2.0.9

Paramètres de stratégie IKE

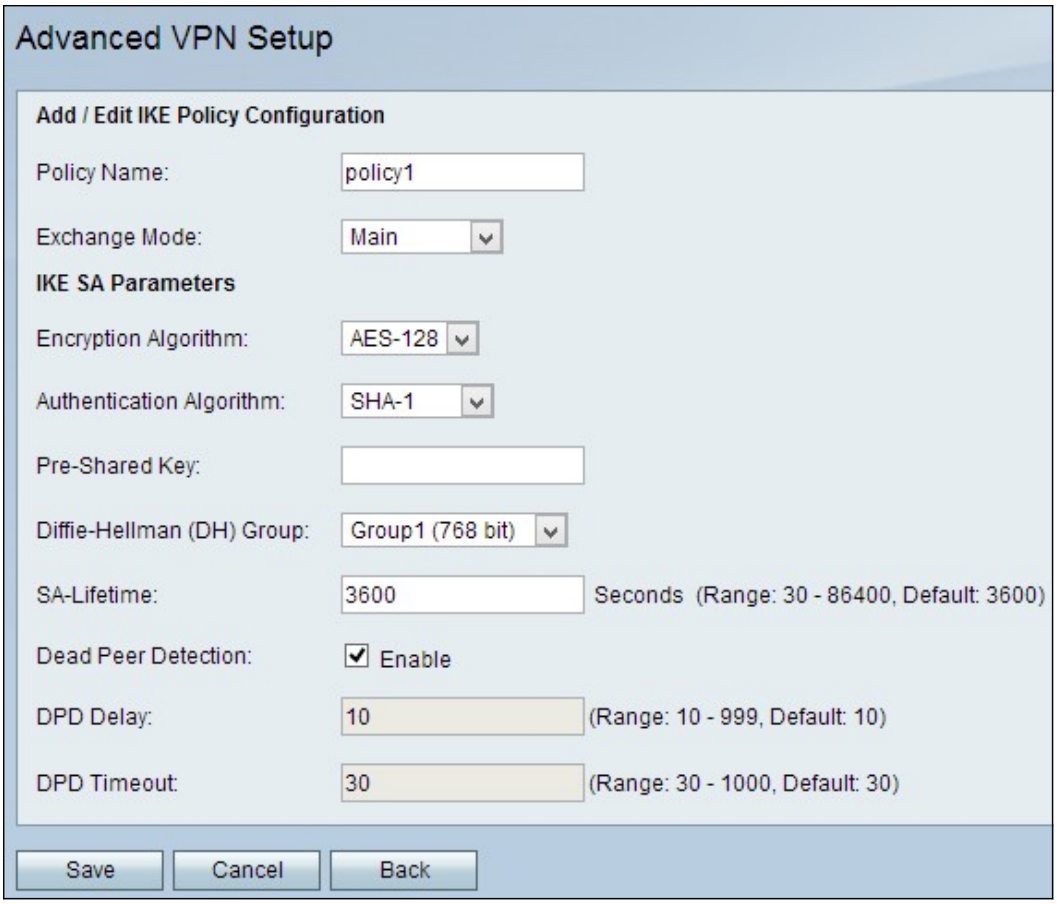
Internet Key Exchange (IKE) est un protocole utilisé pour établir une connexion sécurisée pour la communication dans un VPN. Cette connexion établie et sécurisée est appelée association de sécurité (SA). Cette procédure explique comment configurer une stratégie IKE pour la connexion VPN à utiliser pour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

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

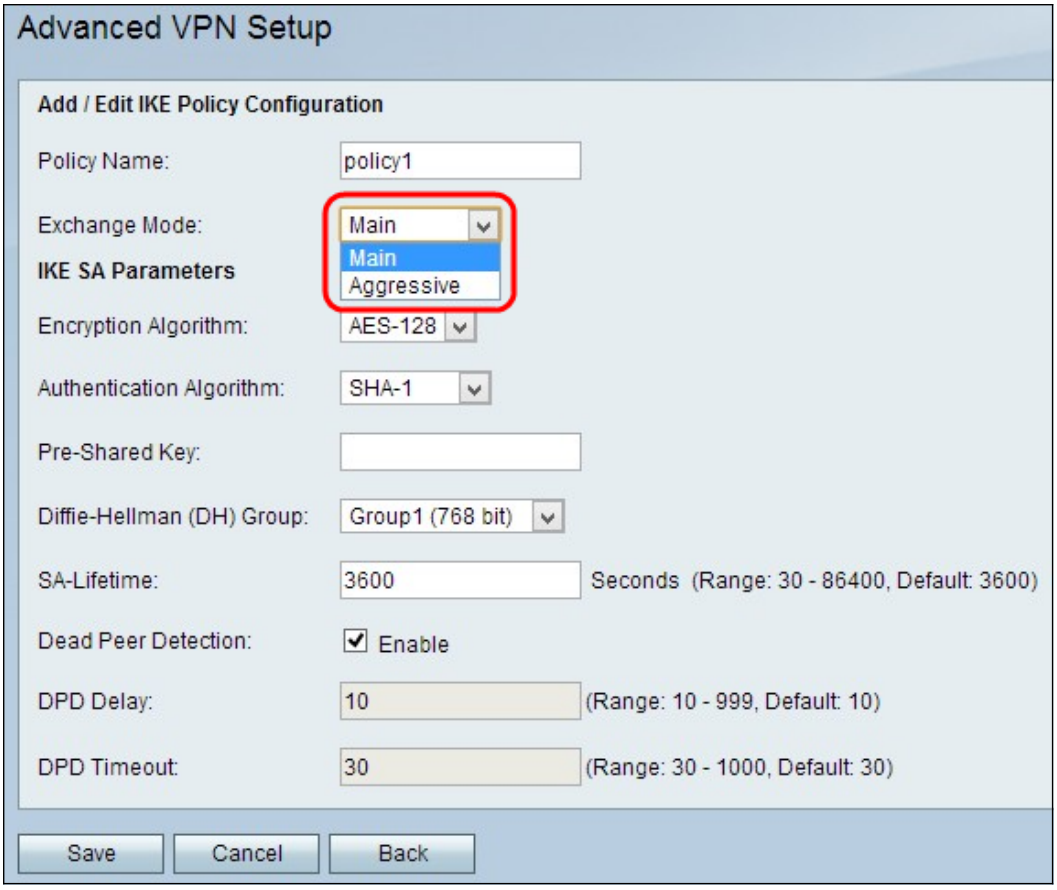




Étape 2. Cliquez sur **Ajouter une ligne** pour créer une nouvelle stratégie IKE. La page *Advanced VPN Setup* s'ouvre :



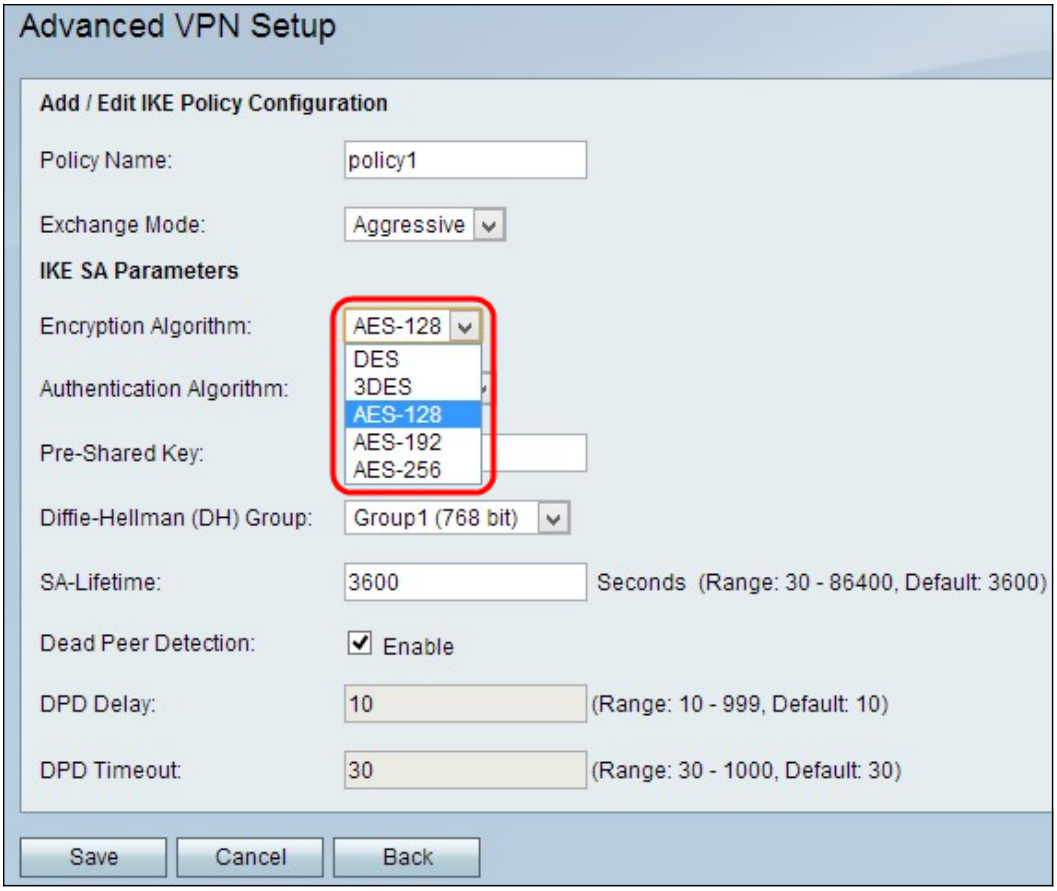
Étape 3. Dans le champ *Policy Name*, saisissez un nom pour la stratégie IKE à identifier facilement.



Étape 4. Choisissez une option dans la liste déroulante *Mode Exchange* :

·Main : 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 : 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 5. Choisissez un algorithme dans la liste déroulante *Encryption Algorithm* :

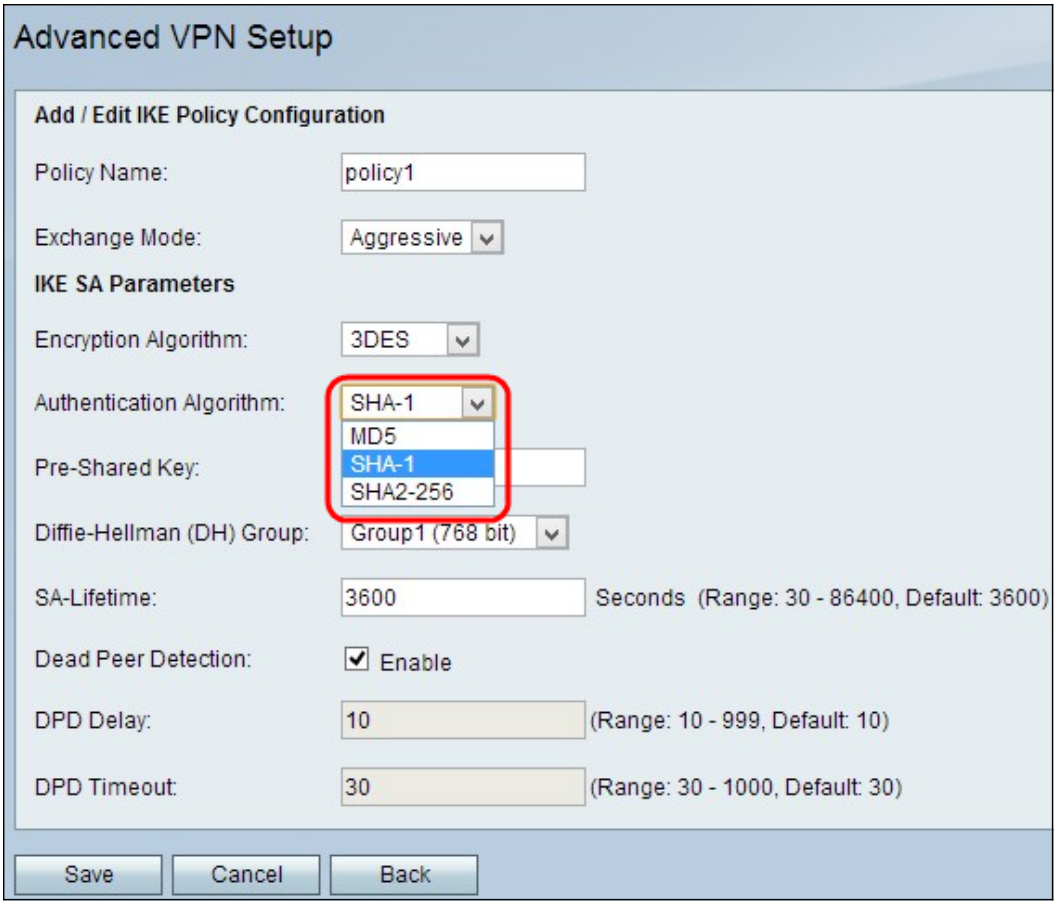
·DES - Data Encryption Standard (DES) utilise une taille de clé de 56 bits pour le chiffrement des données. DES est obsolète et ne doit être utilisée que si un terminal prend uniquement en charge cette norme.

·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. En général, AES est également plus rapide mais moins sécurisé que 3DES, mais 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.

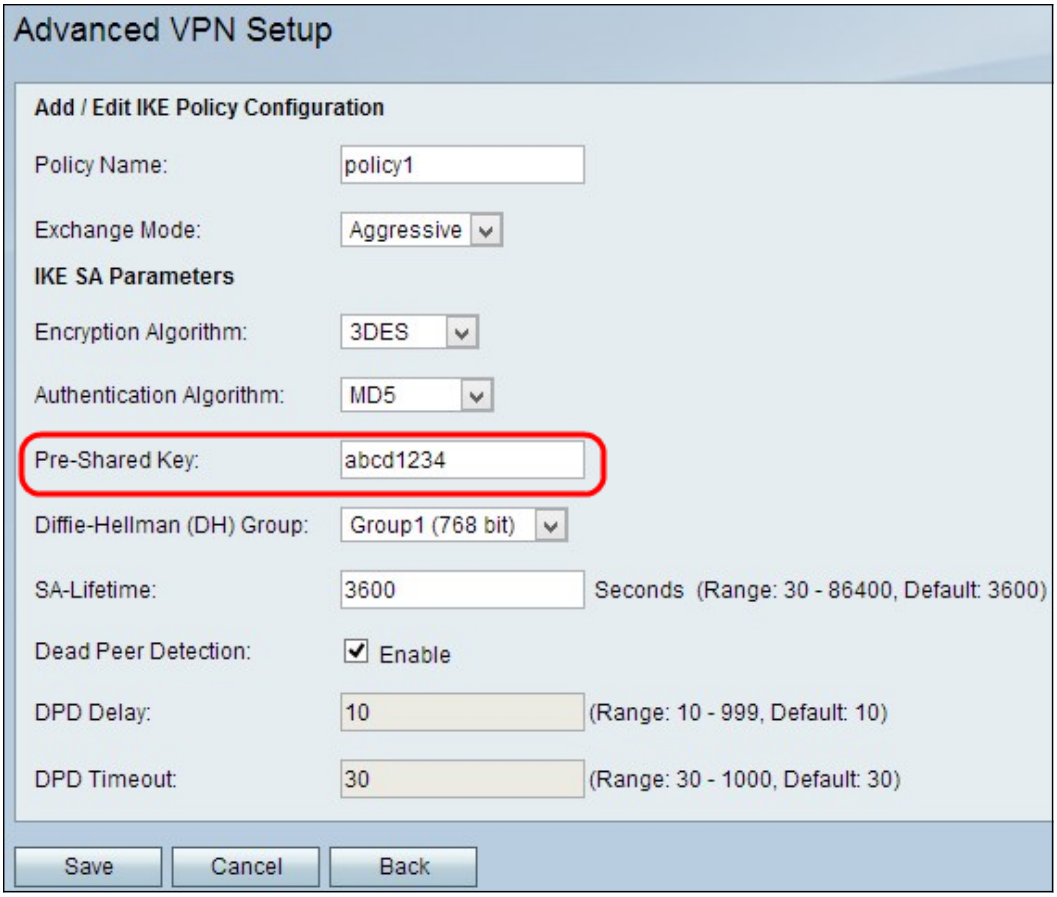


Étape 6. Choisissez l'authentification souhaitée dans la liste déroulante *Authentication Algorithm* :

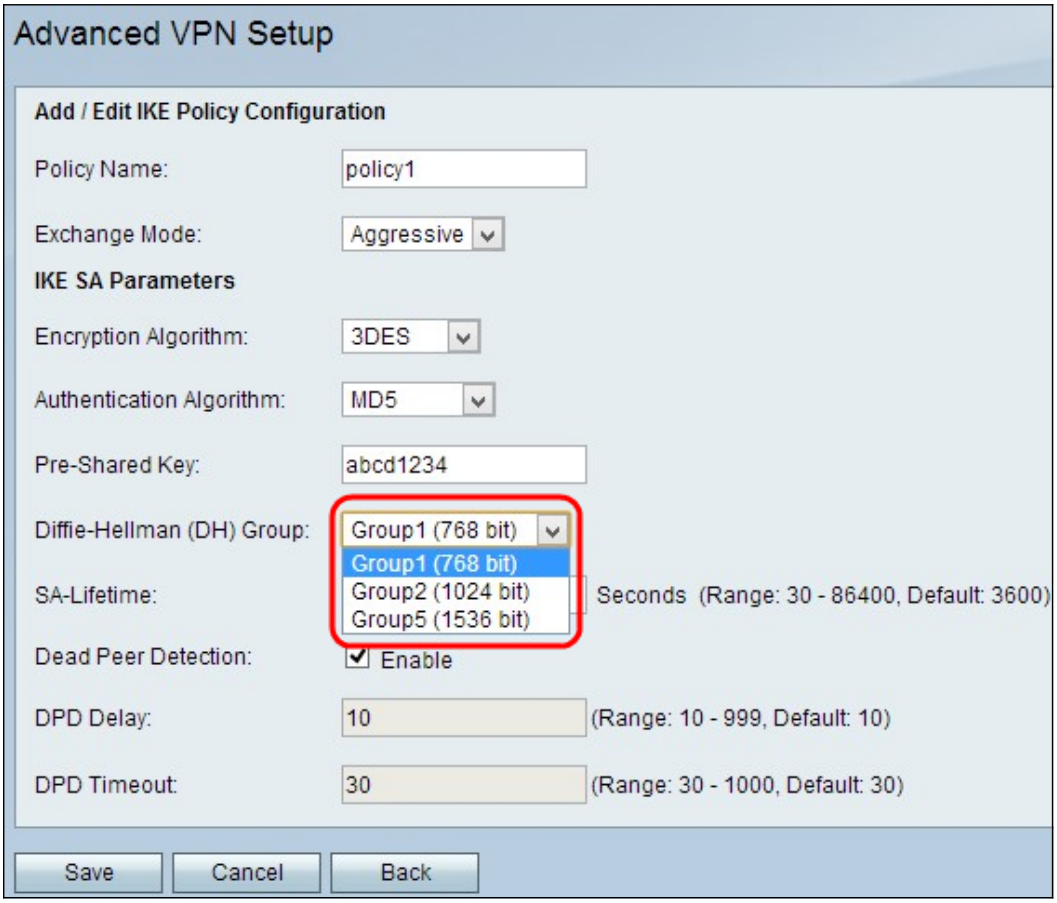
·MD5 — Message-Digest Algorithm 5 (MD5) utilise une valeur de hachage de 128 bits pour l'authentification. MD5 est moins sécurisé mais plus rapide que SHA-1 et SHA2-256.

·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 7. Dans le champ *Clé prépartagée*, saisissez une clé prépartagée que la stratégie IKE utilise.

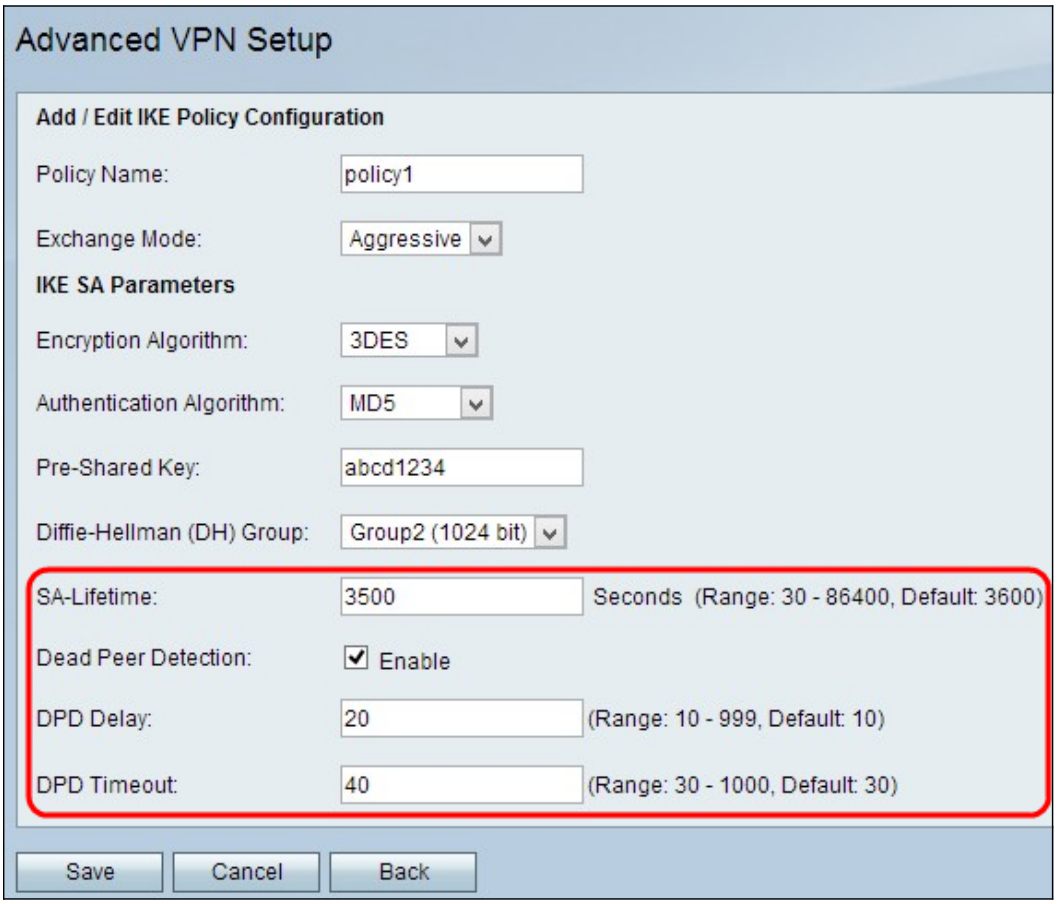


Étape 8. Dans la liste déroulante *Diffie-Hellman (DH) Group*, choisissez le groupe DH utilisé par IKE. Les hôtes d'un groupe DH peuvent échanger des clés sans connaissance mutuelle. Plus le nombre de bits du groupe est élevé, plus le groupe est sécurisé.

·Groupe 1 - 768 bits : la clé de puissance la plus faible et le groupe d'authentification le plus non sécurisé. Mais il faut moins de temps pour calculer les clés IKE. Cette option est préférable si le débit du réseau est faible.

·Groupe 2 - 1 024 bits - Clé de puissance supérieure et groupe d'authentification plus sécurisé. Mais il faut un certain temps pour calculer les clés IKE.

·Groupe 5 - 1 536 bits — Représente la clé la plus puissante et le groupe d'authentification le plus sécurisé. Il faut plus de temps pour calculer les clés IKE. Cette option est préférable si le débit du réseau est élevé.



Étape 9. Entrez la durée (en secondes) d'une SA pour le VPN avant le renouvellement de l'SA dans le champ *SA-Lifetime*.

Étape 10. (Facultatif) Cochez la case **Activer** dans le champ *Détection des homologues morts* pour activer la Détection des homologues morts. Deed Peer Detection surveille les homologues IKE pour voir si un homologue a cessé de fonctionner. La détection d'homologue mort empêche le gaspillage de ressources réseau sur les homologues inactifs.

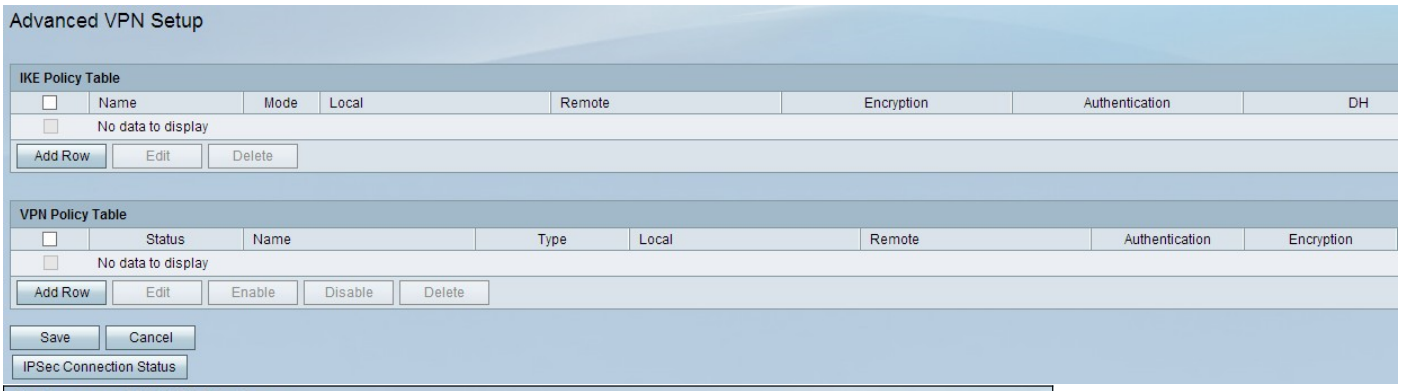
Étape 11. (Facultatif) Si vous avez activé la détection d'homologue de transaction à l'étape 9, entrez la fréquence (en secondes) à laquelle l'homologue est vérifié pour l'activité dans le champ *Délai d'homologue de transaction*.

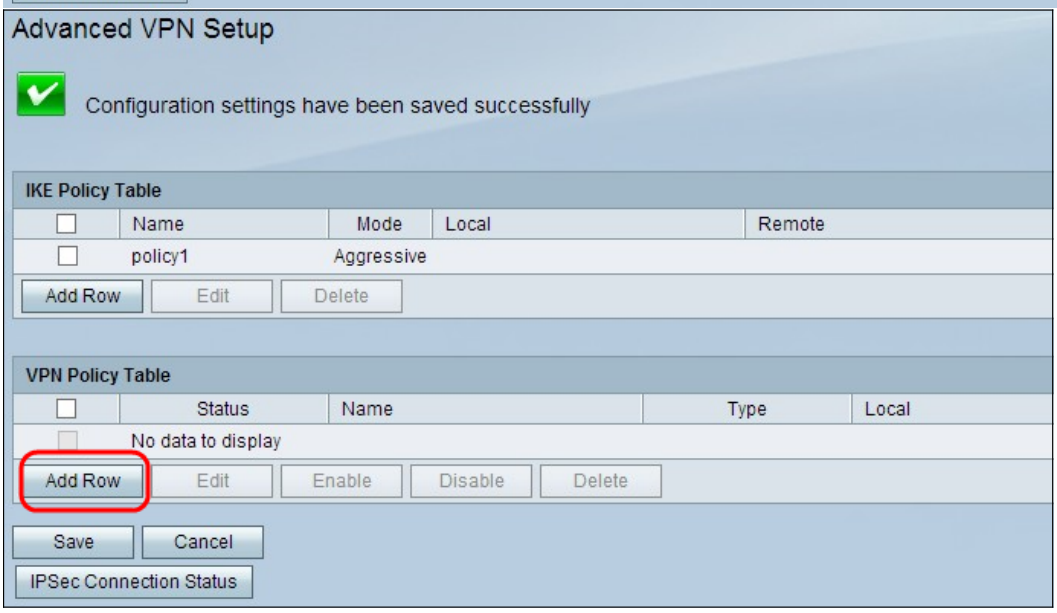
Étape 12. (Facultatif) Si vous avez activé la détection d'homologue de transaction à l'étape 9, saisissez le nombre de secondes à attendre avant qu'un homologue inactif ne soit supprimé dans le champ Deed Peer Detection Timeout.

Étape 13. Cliquez sur **Enregistrer** pour appliquer tous les paramètres.

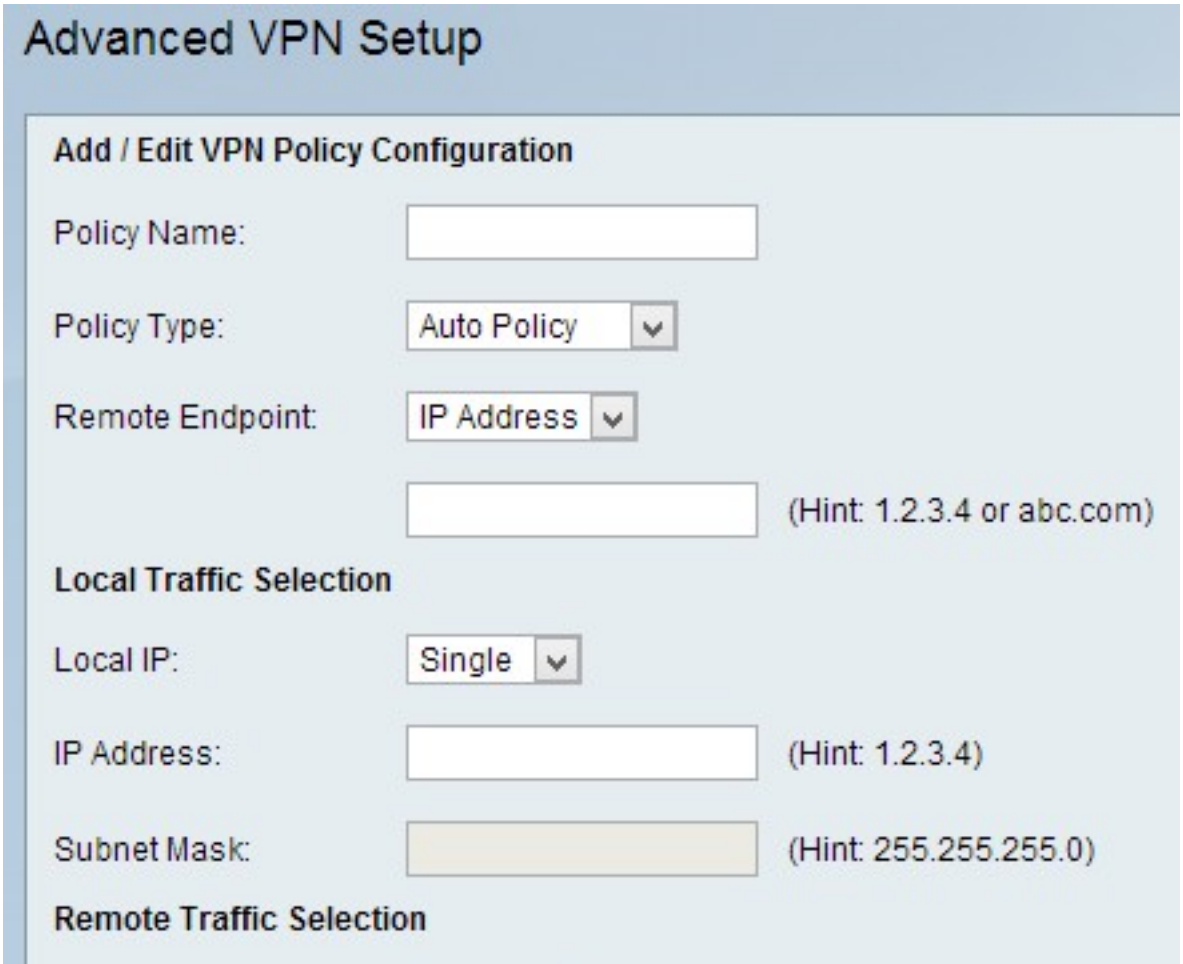
Configuration de la stratégie VPN

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

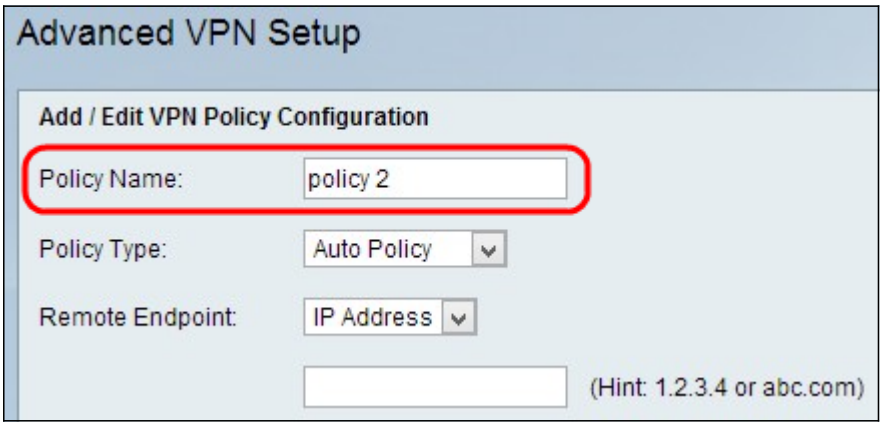




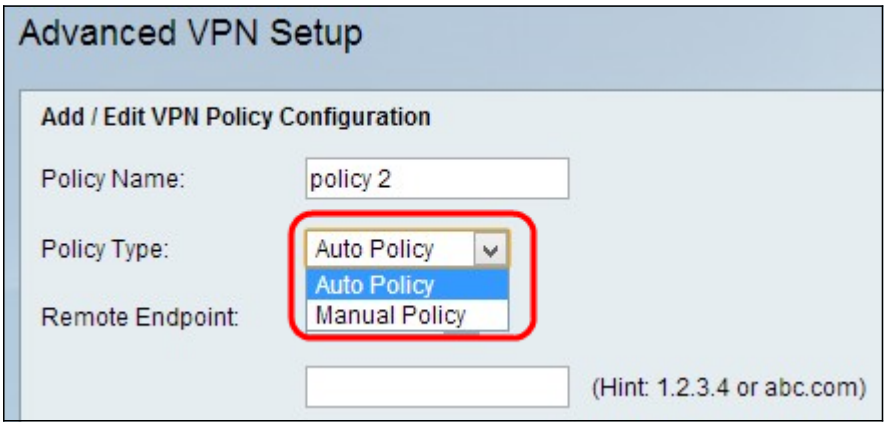
Étape 2. Cliquez sur **Add** Row dans la *table VPN Policy Table*. La fenêtre *Advanced VPN Policy Setup* s'affiche :



Ajouter/Modifier la configuration de la stratégie VPN



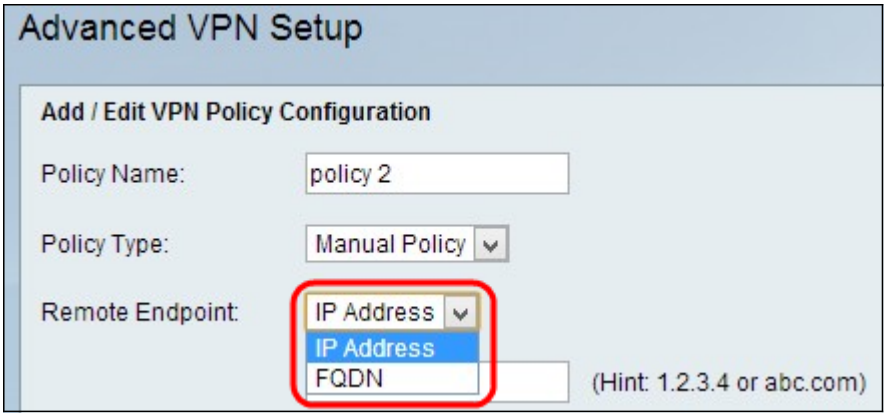
Étape 1. Entrez un nom unique pour la stratégie dans le champ *Nom de la stratégie* pour l'identifier facilement.



Étape 2. Choisissez le type de stratégie approprié dans la liste déroulante *Type de stratégie*.

·Auto Policy : les paramètres peuvent être définis automatiquement. Dans ce cas, en plus des politiques, il est nécessaire que le protocole IKE (Internet Key Exchange) négocie entre les deux points d'extrémité VPN.

·Manual Policy : dans ce cas, tous les paramètres qui incluent les paramètres des clés du tunnel VPN sont entrés manuellement pour chaque point d'extrémité.



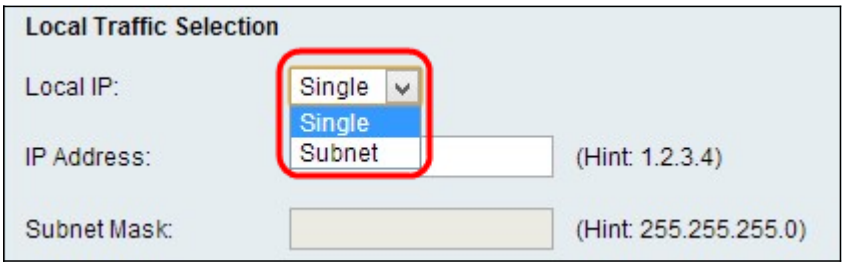
Étape 3. Choisissez le type d'identificateur IP qui identifie la passerelle au niveau du point de terminaison distant dans la liste déroulante *Remote Endpoint*.

·IP Address : adresse IP de la passerelle sur le point d'extrémité distant. Si vous choisissez cette option, saisissez l'adresse IP dans le champ.

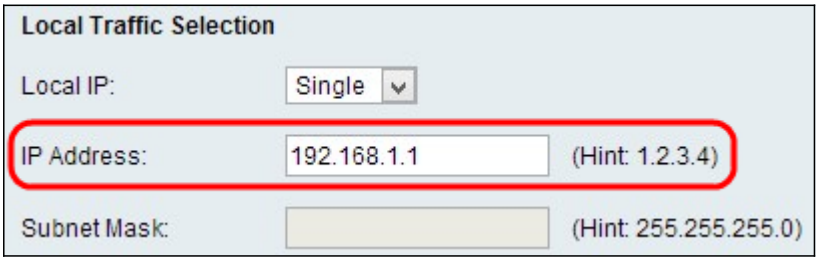
·FQDN (Fully Qualified Domain Name) : saisissez le nom de domaine complet de la passerelle sur

le point d'extrémité distant. Si vous choisissez cette option, saisissez le nom de domaine complet dans le champ prévu à cet effet.

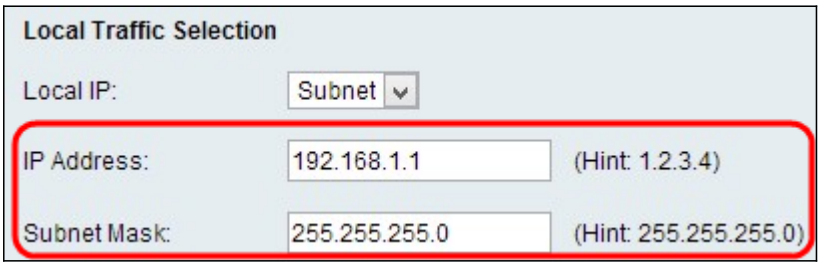
Sélection du trafic local



Étape 1. Choisissez le type d'identificateur que vous voulez fournir pour le point de terminaison dans la liste déroulante *Local IP*.

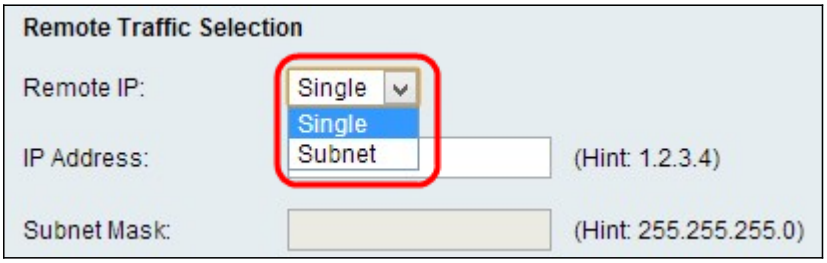


·unique : limite la stratégie à un hôte. Si vous choisissez cette option, saisissez l'adresse IP dans le champ *Adresse IP*.



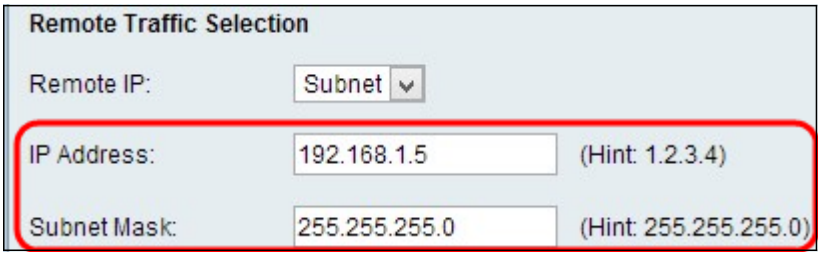
·Subnet : masque qui définit les limites d'une adresse IP. Cela permet uniquement aux hôtes du sous-réseau spécifié de se connecter au VPN. Pour se connecter au VPN, un ordinateur est sélectionné par une opération AND logique. Un ordinateur est sélectionné si l'adresse IP se situe dans la même plage que celle requise. Si vous choisissez cette option, saisissez l'adresse IP et le sous-réseau dans le champ IP address and Subnet.

Sélection du trafic distant



Étape 1. Choisissez le type d'identificateur que vous voulez fournir pour le point de terminaison dans la liste déroulante *Local IP* :

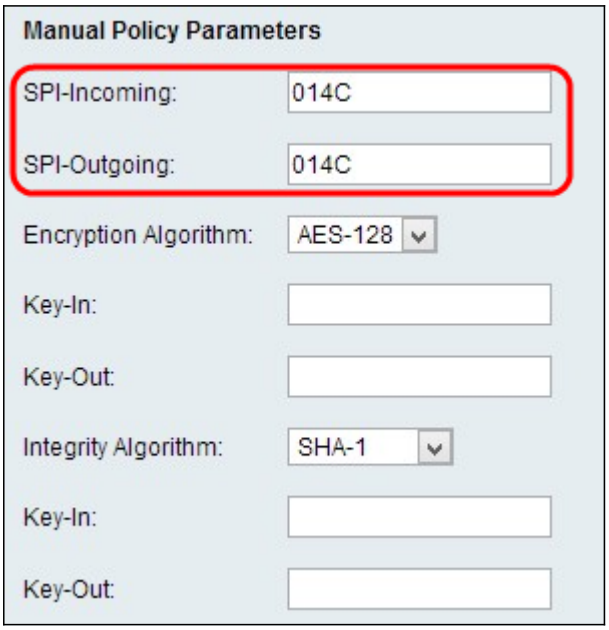
·unique : limite la stratégie à un hôte. Si vous choisissez cette option, saisissez l'adresse IP dans le champ *Adresse IP*.



·Subnet : masque qui définit les limites d'une adresse IP. Cela permet uniquement aux hôtes du sous-réseau spécifié de se connecter au VPN. Pour se connecter au VPN, un ordinateur est sélectionné par une opération AND logique. Un ordinateur est sélectionné si l'adresse IP se situe dans la même plage que celle requise. Si vous choisissez cette option, saisissez l'adresse IP et le sous-réseau dans le champ IP address and Subnet.

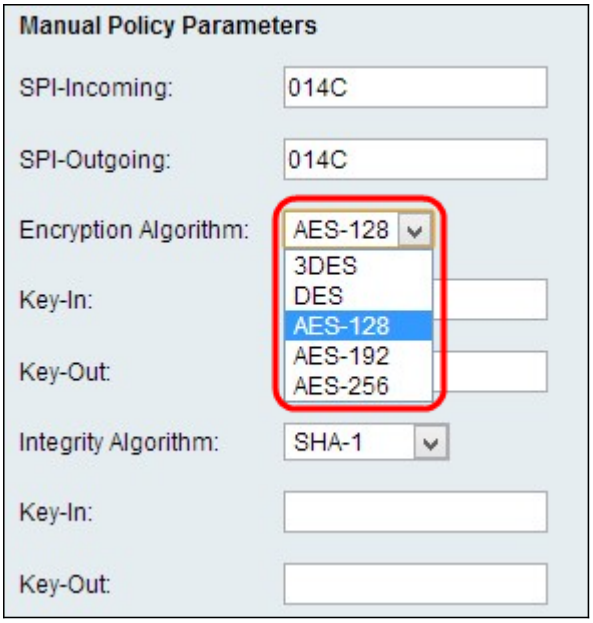
Paramètres de stratégie manuels

Pour configurer des paramètres de stratégie manuels, sélectionnez **Stratégie manuelle** dans la liste déroulante *Type de stratégie* à l'étape 2 de la section *Ajouter/Modifier une configuration de stratégie VPN*.



Étape 1. Entrez une valeur hexadécimale comprise entre 3 et 8 dans le champ *SPI-Incoming*. SPI (Stateful Packet Inspection) est une technologie appelée inspection approfondie des paquets. SPI met en oeuvre un certain nombre de fonctions de sécurité qui contribuent à sécuriser votre réseau informatique. La valeur SPI-Incoming correspond à la valeur SPI-Outgoing du périphérique précédent. Toute valeur est acceptable, à condition que le point de terminaison VPN distant ait la même valeur dans son champ *SPI-Outgoing*.

Étape 2. Entrez une valeur hexadécimale comprise entre 3 et 8 dans le champ *SPI-Sortant*.



Étape 3. Sélectionnez l'algorithme de chiffrement approprié dans la liste déroulante Encryption Algorithm.

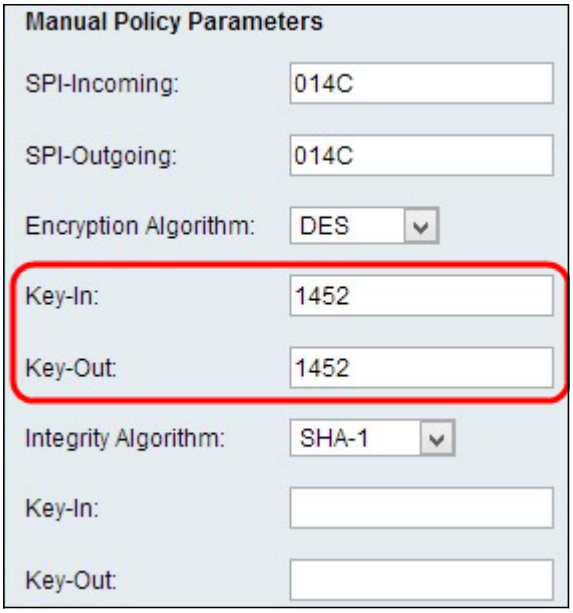
·DES - Data Encryption Standard (DES) utilise une taille de clé de 56 bits pour le chiffrement des données. DES est obsolète et ne doit être utilisée que si un terminal prend uniquement en charge cette norme.

·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 en fonction de l'arrondi 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. En général, AES est également plus rapide mais moins sécurisé que 3DES, mais 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.

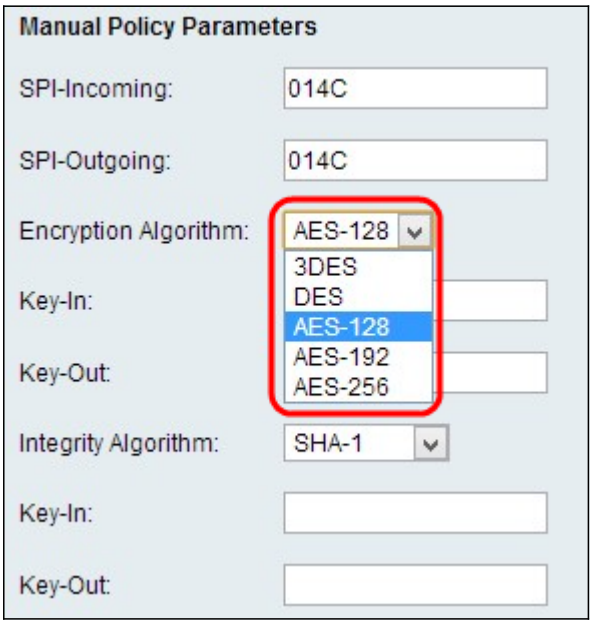
·AES-192 — AES-192 utilise une clé 192 bits pour le chiffrement AES. AES-192 est plus lent mais plus sécurisé que AES-128, et AES-192 est plus rapide mais moins sécurisé que AES-256.

·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 4. Entrez la clé de chiffrement de la stratégie entrante dans le champ *Key-In*. La longueur de la clé dépend de l'algorithme choisi à l'étape 3.

Étape 5. Entrez la clé de chiffrement de la stratégie sortante dans le champ *Clé sortante*.

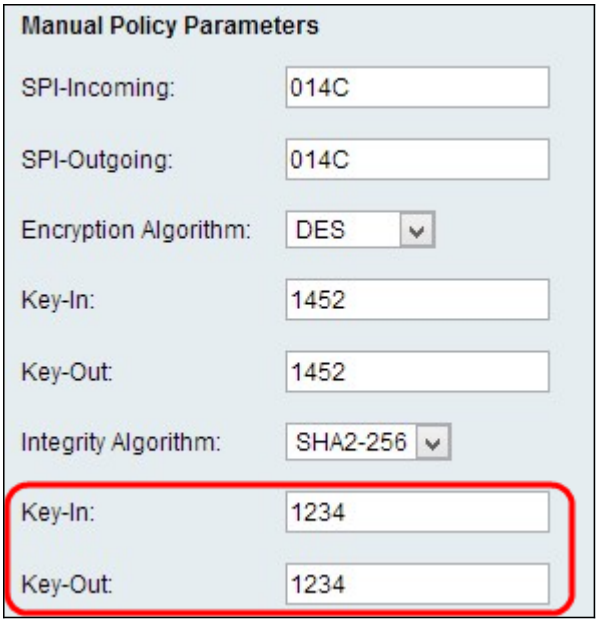


Étape 6. Choisissez l'algorithme d'intégrité approprié dans la liste déroulante *Integrity Algorithm*. Cet algorithme vérifie l'intégrité des données :

·MD5 — Cet algorithme spécifie la longueur de clé à 16 caractères. L'algorithme Message-Digest 5 (MD5) n'est pas résistant aux collisions et convient aux applications telles que les certificats SSL ou les signatures numériques qui s'appuient sur cette propriété. MD5 compresse tout flux d'octets en une valeur de 128 bits, mais SHA la compresse en une valeur de 160 bits. MD5 est un peu moins cher à calculer, mais MD5 est une version plus ancienne de l'algorithme de hachage et est vulnérable aux attaques de collision.

·SHA1 — Secure Hash Algorithm version 1 (SHA1) est une fonction de hachage de 160 bits qui est plus sécurisée que MD5, mais qui prend plus de temps à calculer.

·SHA2-256 — Cet algorithme spécifie la longueur de clé à 32 caractères.

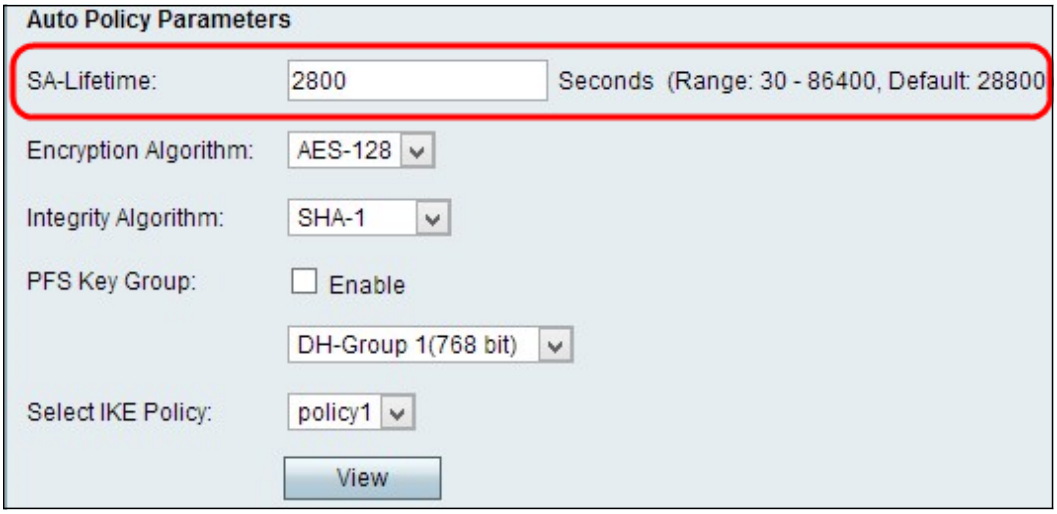


Étape 7. Entrez la clé d'intégrité (pour ESP avec le mode Intégrité) de la stratégie entrante. La longueur de la clé dépend de l'algorithme choisi à l'étape 6.

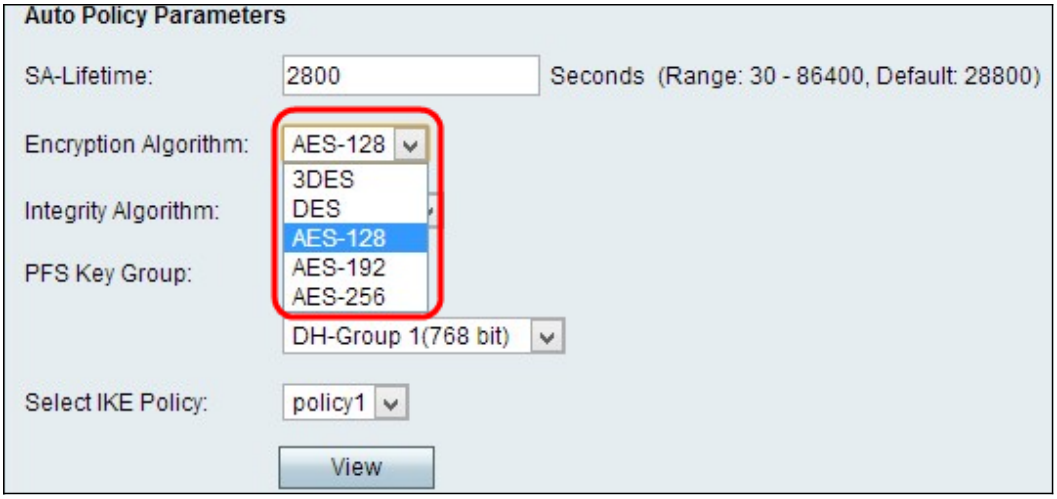
Étape 8. Saisissez la clé d'intégrité de la stratégie sortante dans le champ Clé sortante. La connexion VPN est configurée pour le trafic sortant vers le trafic entrant. Par conséquent, les clés sortantes d'une extrémité doivent correspondre aux clés entrantes de l'autre extrémité.

Note: SPI-Incoming and Outgoing, Encryption Algorithm, Integrity Algorithm et Keys doivent être identiques à l'autre extrémité du tunnel VPN pour une connexion réussie.

Paramètres de stratégie automatique



Étape 1. Saisissez la durée de l'association de sécurité (SA) en secondes dans le champ SA Lifetime. La durée de vie de l'association de sécurité est définie lorsque n'importe quelle clé a atteint sa durée de vie, toute association de sécurité associée est automatiquement renégociée.



Étape 2. Sélectionnez l'algorithme de chiffrement approprié dans la liste déroulante Encryption Algorithm :

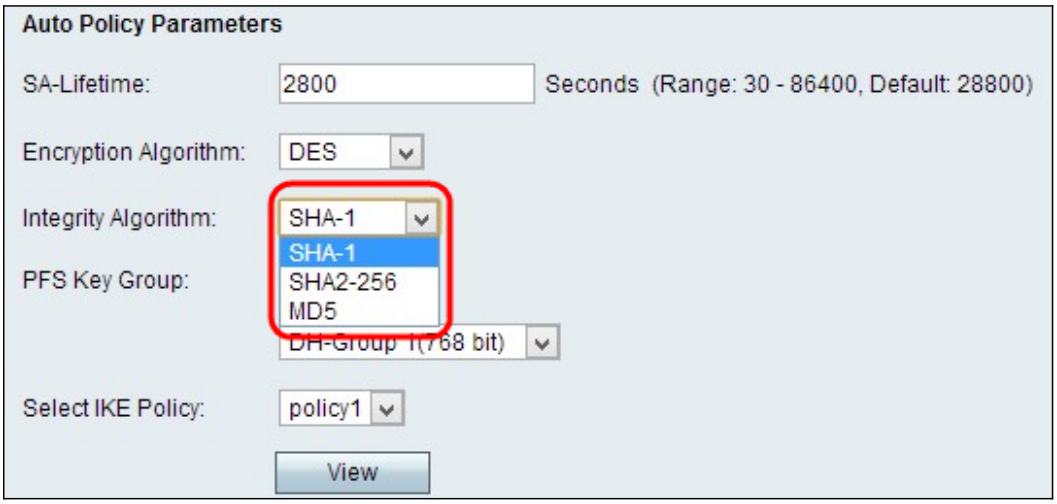
·DES - Data Encryption Standard (DES) utilise une taille de clé de 56 bits pour le chiffrement des données. DES est obsolète et ne doit être utilisée que si un terminal prend uniquement en charge cette norme.

·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 en fonction de l'arrondi 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. En général, AES est également plus rapide mais moins sécurisé que 3DES, mais 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.



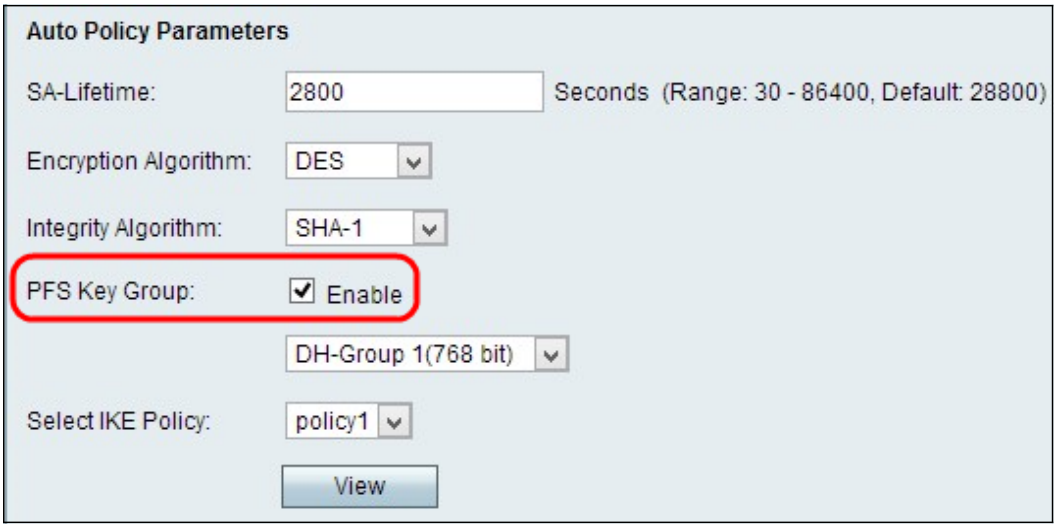
Étape 3. Sélectionnez l'algorithme d'intégrité approprié dans la liste déroulante Algorithme d'intégrité. Cet algorithme vérifie l'intégrité des données.

·MD5 — Cet algorithme spécifie la longueur de clé à 16 caractères. L'algorithme Message-Digest 5 (MD5) n'est pas résistant aux collisions et convient aux applications telles que les certificats SSL

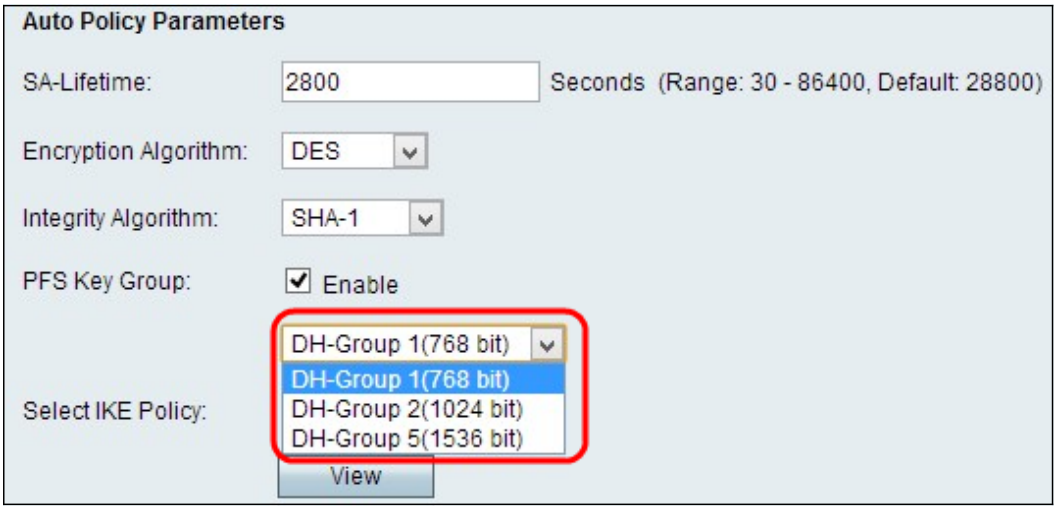
ou les signatures numériques qui s'appuient sur cette propriété. MD5 compresse tout flux d'octets en une valeur de 128 bits, mais SHA la compresse en une valeur de 160 bits. MD5 est un peu moins cher à calculer, mais MD5 est une version plus ancienne de l'algorithme de hachage et est vulnérable aux attaques de collision.

·SHA1 — Secure Hash Algorithm version 1 (SHA1) est une fonction de hachage de 160 bits qui est plus sécurisée que MD5, mais qui prend plus de temps à calculer.

·SHA2-256 — Cet algorithme spécifie la longueur de clé à 32 caractères.



Étape 4. (Facultatif) Cochez la case **Activer** dans le champ *Groupe de clés PFS* pour activer Perfect Forward Secrecy, qui est d'améliorer la sécurité.

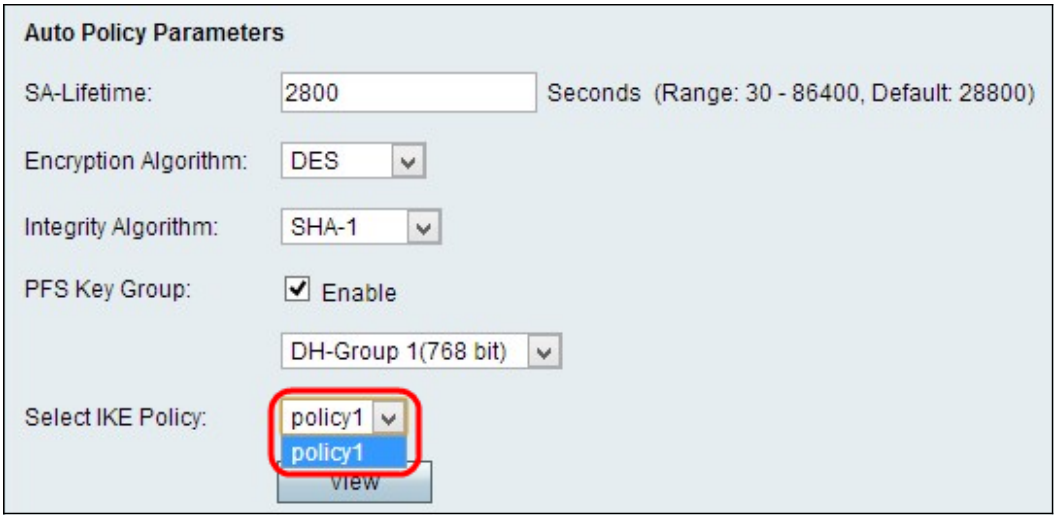


Étape 5. Si vous avez coché **Activer** à l'étape 4, sélectionnez l'échange de clés Diffie-Hellman approprié dans la liste déroulante du champ *Groupe de clés PFS*.

·Groupe 1 - 768 bits — Représente la clé la plus faible et le groupe d'authentification le plus non sécurisé. Mais il faut moins de temps pour calculer les clés IKE. Cette option est préférable si le débit du réseau est faible.

·Groupe 2 - 1 024 bits — Représente une clé de résistance supérieure et un groupe d'authentification plus sécurisé. Mais il faut un certain temps pour calculer les clés IKE.

·Groupe 5 - 1 536 bits — Représente la clé la plus puissante et le groupe d'authentification le plus sécurisé. Il faut plus de temps pour calculer les clés IKE. Cette option est préférable si le débit du réseau est élevé.



Étape 6. Choisissez la stratégie IKE appropriée dans la liste déroulante *Sélectionner une 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). Pour qu'un VPN fonctionne correctement, les stratégies IKE pour les deux points d'extrémité doivent être identiques.

Étape 7. Cliquez sur **Enregistrer** pour appliquer tous les paramètres.

Note: SA -Lifetime, Encryption Algorithm, Integrity Algorithm, PFS Key Group et IKE Policy doivent être identiques à l'autre extrémité du tunnel VPN pour une connexion réussie.

Si vous voulez voir d'autres articles sur le RV110W, cliquez ici.