Configuration VPN (Virtual Private Network) de passerelle vers passerelle sur les gammes de routeurs RV320 et RV325

Objectif

Les VPN sont utilisés pour établir des connexions très sécurisées sur deux points d'extrémité, sur Internet public ou partagé, via ce qu'on appelle un tunnel VPN. Plus précisément, une connexion VPN passerelle à passerelle permet à deux routeurs de se connecter en toute sécurité et à un client d'une extrémité de faire logiquement partie du même réseau distant de l'autre extrémité. Cela permet de partager plus facilement et en toute sécurité les données et les ressources sur Internet. La configuration doit être effectuée des deux côtés de la connexion pour qu'une connexion VPN passerelle à passerelle soit établie. L'objectif de cet article est de vous guider dans la configuration d'une connexion VPN passerelle à passerelle sur la gamme de routeurs VPN RV32x.

Périphériques pertinents

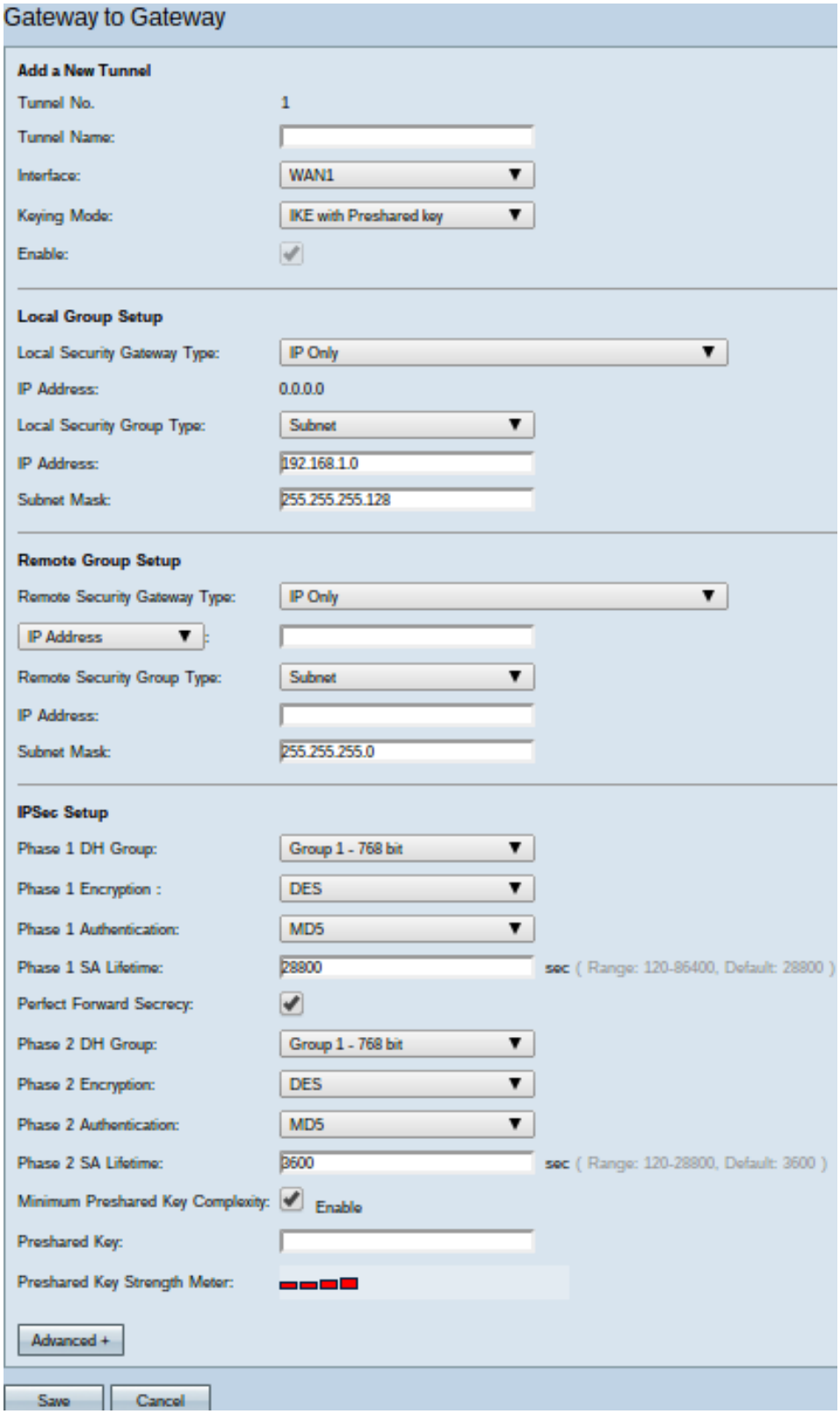
Routeur VPN double WAN · RV320
Routeur VPN double WAN Gigabit · RV325

Version du logiciel

•v 1.1.0.09

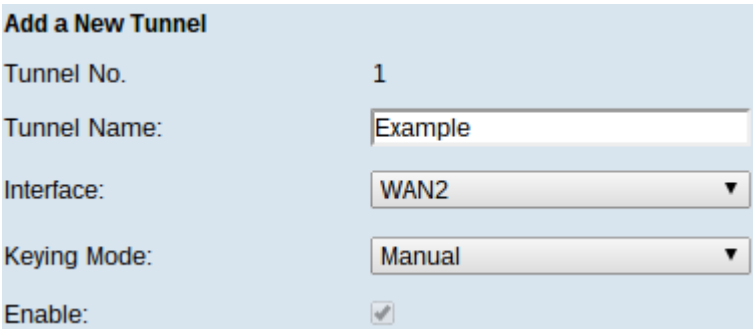
Passerelle vers passerelle

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **VPN > Gateway to Gateway**. La page *Passerelle vers passerelle* s'ouvre :



Pour que la connexion VPN fonctionne correctement, les valeurs IPSec (Internet Protocol Security) des deux côtés de la connexion doivent être identiques. Les deux côtés de la connexion doivent appartenir à différents réseaux locaux (LAN) et au moins un des routeurs doit être identifiable par une adresse IP statique ou un nom d'hôte DNS dynamique.

Ajouter un nouveau tunnel



N° de tunnel · — Affiche le tunnel en cours qui va être créé. Le routeur prend en charge 100 tunnels.

Étape 1. Entrez un nom pour le tunnel VPN dans le champ Tunnel Name. Il n'est pas nécessaire qu'il corresponde au nom utilisé à l'autre extrémité du tunnel.

Étape 2. Dans la liste déroulante Interface, sélectionnez le port WAN (Wide Area Network) à utiliser pour le tunnel.

·WAN1 : port WAN dédié du routeur.

·WAN2 : port WAN2/DMZ du routeur. Ne s'affiche dans le menu déroulant que s'il a été configuré en tant que WAN et non en tant que port DMZ (Demilitarize Zone).

·USB1 : port USB1 du routeur. Fonctionne uniquement si une clé USB 3G/4G/LTE est connectée au port.

·USB2 : port USB2 du routeur. Fonctionne uniquement si une clé USB 3G/4G/LTE est connectée au port.

Étape 3. Dans la liste déroulante Keying Mode, sélectionnez la sécurité du tunnel à utiliser.

·Manual : cette option vous permet de configurer manuellement la clé au lieu de négocier la clé avec l'autre côté de la connexion VPN.

·IKE avec clé prépartagée : sélectionnez cette option pour activer le protocole IKE (Internet Key Exchange Protocol) qui configure une association de sécurité dans le tunnel VPN. IKE utilise une clé pré-partagée pour authentifier un homologue distant.

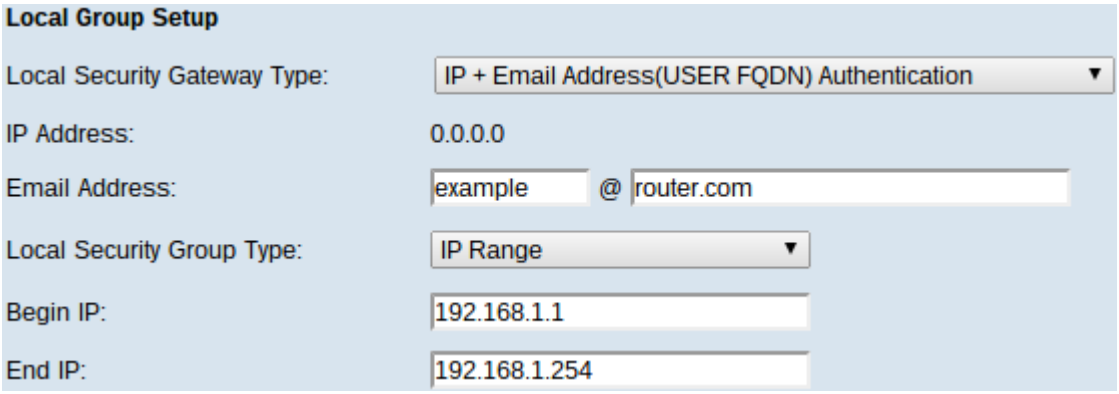
·IKE avec certificat : sélectionnez cette option pour activer le protocole IKE (Internet Key Exchange) avec certificat qui offre un moyen plus sécurisé de générer et d'échanger automatiquement des clés pré-partagées afin d'établir des communications plus authentifiées et plus sécurisées pour le tunnel.

Étape 4. Cochez la case Activer pour activer le tunnel VPN. Par défaut, il est activé.

Configuration du groupe local

Ces paramètres doivent correspondre aux paramètres de configuration du groupe distant du routeur situé à l'autre extrémité du tunnel VPN.

Note: Si Manual ou IKE avec clé prépartagée a été sélectionné dans la liste déroulante Keying Mode de l'étape 3 de Add a New Tunnel start de l'étape 1 et ignorez les étapes 2 à 4. Si IKE avec certificat a été sélectionné, ignorez l'étape 1.



Étape 1. Dans la liste déroulante Local Security Gateway Type (Type de passerelle de sécurité locale), sélectionnez la méthode d'identification du routeur pour établir le tunnel VPN.

·IP Only : l'accès au tunnel est possible via une adresse IP WAN statique uniquement. Vous pouvez choisir cette option si seul le routeur possède une adresse IP WAN statique. L'adresse IP WAN statique est un champ généré automatiquement.

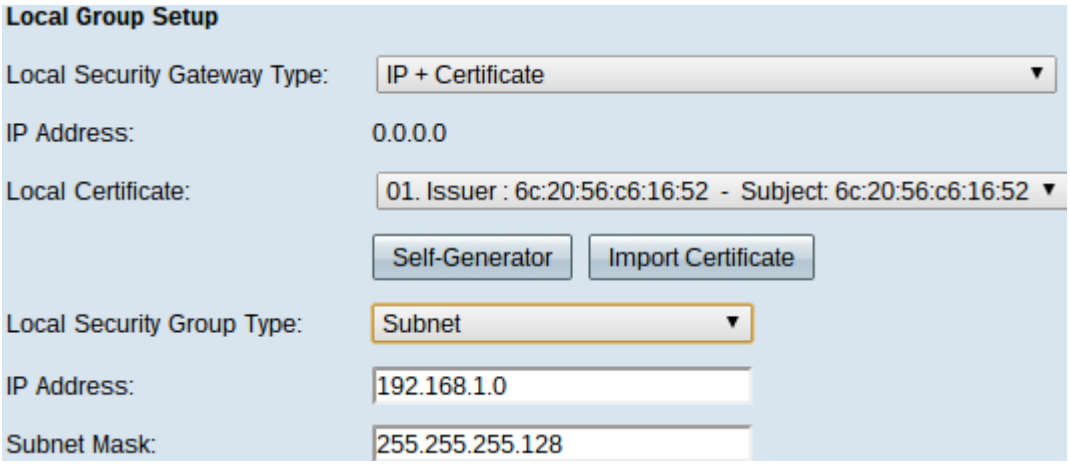
Authentification · IP + Domain Name (FQDN) : l'accès au tunnel est possible via une adresse IP statique et un domaine enregistré. Si vous choisissez cette option, saisissez le nom du domaine enregistré dans le champ Domain Name (nom de domaine). L'adresse IP WAN statique est un champ généré automatiquement.

Authentification · IP + E-mail Addr. (USER FQDN) : l'accès au tunnel est possible par le biais d'une adresse IP statique et d'une adresse e-mail. Si vous choisissez cette option, saisissez l'adresse courriel dans le champ Email Address. L'adresse IP WAN statique est un champ généré automatiquement.

Authentification · Dynamic IP + Domain Name (FQDN) : l'accès au tunnel est possible via une adresse IP dynamique et un domaine enregistré. Si vous choisissez cette option, saisissez le nom du domaine enregistré dans le champ Domain Name (nom de domaine).

·Authentification FQDN (Dynamic IP + Email Addr.) (USER FQDN) : l'accès au tunnel est possible par le biais d'une adresse IP dynamique et d'une adresse e-mail. Si vous choisissez cette option, saisissez l'adresse courriel dans le champ Email Address.

Note: Les modifications suivantes apportées à la zone Configuration du groupe local changent lors de l'utilisation d'IKE avec certificat.



La liste déroulante Local Security Gateway Type devient inmodifiable et affiche IP + Certificate. Il s'agit de la ressource LAN qui peut utiliser le tunnel.

Le champ IP Address affiche l'adresse IP WAN du périphérique. Il n'est pas modifiable par l'utilisateur.

Étape 2. Sélectionnez un certificat dans la liste déroulante Certificat local. Les certificats offrent une sécurité d'authentification renforcée sur les connexions VPN.

Étape 3. (Facultatif) Cliquez sur le bouton **Auto-générateur** pour afficher la fenêtre *Générateur de certificats* pour configurer et générer des certificats.

Étape 4. (Facultatif) Cliquez sur le bouton **Importer le certificat** pour afficher la fenêtre *Mon certificat* pour afficher et configurer les certificats.

Étape 5. Dans la liste déroulante Local Security Group Type, sélectionnez l'une des options suivantes :

·IP Address : cette option vous permet de spécifier un périphérique pouvant utiliser ce tunnel VPN. Vous devez seulement entrer l'adresse IP du périphérique dans le champ d'adresse IP.

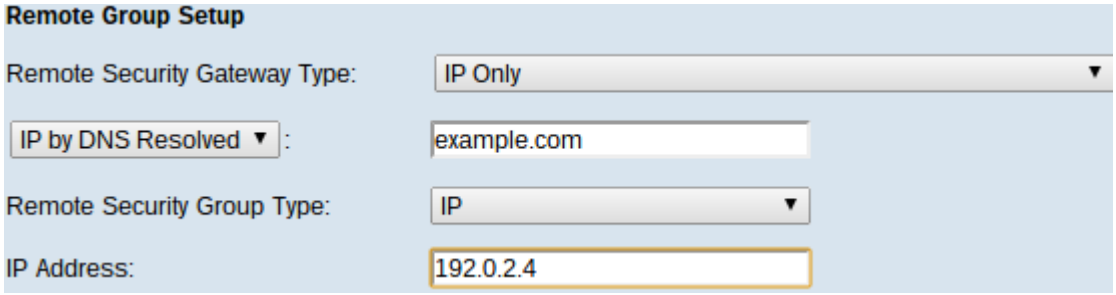
·Subnet : sélectionnez cette option pour autoriser tous les périphériques appartenant au même sous-réseau à utiliser le tunnel VPN. Vous devez entrer l'adresse IP du réseau dans le champ IP Address (Adresse IP) et son masque de sous-réseau respectif dans le champ Subnet Mask (Masque de sous-réseau).

·IP Range : sélectionnez cette option pour spécifier une plage de périphériques pouvant utiliser le tunnel VPN. Vous devez entrer la première adresse IP et la dernière adresse IP de la plage de périphériques dans les champs Begin IP et End IP.

Configuration du groupe distant

Ces paramètres doivent correspondre aux paramètres de configuration de groupe local du routeur situé à l'autre extrémité du tunnel VPN.

Note: Si Manual ou IKE avec clé prépartagée a été sélectionné dans la liste déroulante Keying Mode de l'étape 3 de Add a New Tunnel start de l'étape 1 et ignorez les étapes 2 à 5. Ou si IKE avec certificat a été sélectionné, ignorez l'étape 1.



Étape 1. Dans la liste déroulante Remote Security Gateway Type, sélectionnez la méthode permettant d'identifier l'autre routeur pour établir le tunnel VPN.

·IP Only : l'accès au tunnel est possible via une adresse IP WAN statique uniquement. Si vous connaissez l'adresse IP du routeur distant, choisissez l'adresse IP dans la liste déroulante située directement sous le champ Remote Security Gateway Type et saisissez l'adresse. Choisissez IP by DNS Resolved si vous ne connaissez pas l'adresse IP mais que vous connaissez le nom de domaine et saisissez le nom de domaine du routeur dans le champ IP by DNS Resolved.

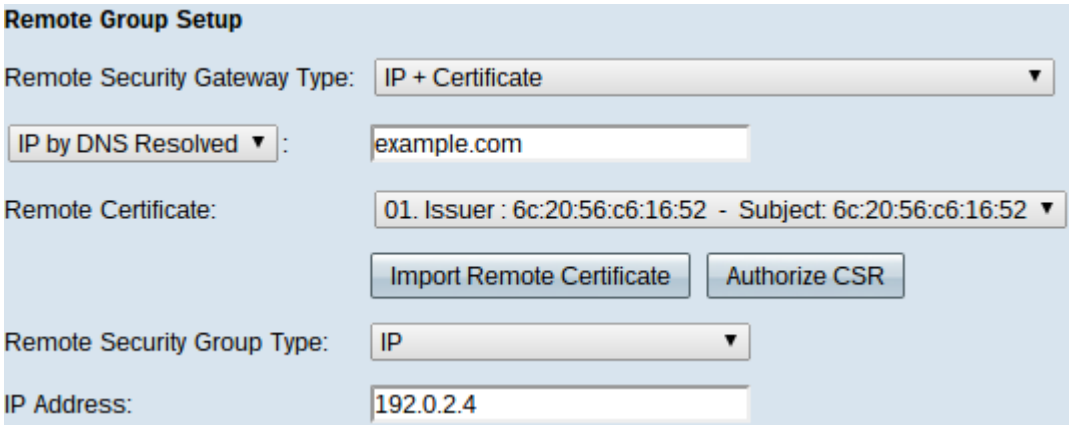
Authentification · IP + Domain Name (FQDN) : l'accès au tunnel est possible via une adresse IP statique et un domaine enregistré du routeur. Si vous connaissez l'adresse IP du routeur distant, choisissez l'adresse IP dans la liste déroulante située directement sous le champ Remote Security Gateway Type et saisissez l'adresse. Choisissez IP by DNS Resolved si vous ne connaissez pas l'adresse IP mais que vous connaissez le nom de domaine et saisissez le nom de domaine du routeur dans le champ IP by DNS Resolved. Si vous choisissez cette option, saisissez le nom du domaine enregistré dans le champ Domain Name (nom de domaine).

Authentification · IP + Email Addr. (USER FQDN) : l'accès au tunnel est possible par le biais d'une adresse IP statique et d'une adresse e-mail.Si vous connaissez l'adresse IP du routeur distant, choisissez l'adresse IP dans la liste déroulante située directement sous le champ Remote Security Gateway Type et saisissez l'adresse. Choisissez IP by DNS Resolved si vous ne connaissez pas l'adresse IP mais que vous connaissez le nom de domaine et saisissez le nom de domaine du routeur dans le champ IP by DNS Resolved. Saisissez l'adresse de messagerie dans le champ Email Address (Adresse de messagerie).

Authentification · Dynamic IP + Domain Name (FQDN) : l'accès au tunnel est possible via une adresse IP dynamique et un domaine enregistré. Si vous choisissez cette option, saisissez le nom du domaine enregistré dans le champ Domain Name (nom de domaine).

·Authentification FQDN (Dynamic IP + Email Addr.) (USER FQDN) : l'accès au tunnel est possible par le biais d'une adresse IP dynamique et d'une adresse e-mail. Si vous choisissez cette option, saisissez l'adresse courriel dans le champ Email Address.
Note: Si les deux routeurs ont des adresses IP dynamiques NE choisissez PAS Dynamic IP + Email Address pour les deux passerelles.

Note: Les modifications suivantes apportées à la zone de configuration du groupe distant sont apportées lors de l'utilisation d'IKE avec certificat.



La liste déroulante Remote Security Gateway Type devient inmodifiable et affiche IP + Certificate. Il s'agit de la ressource LAN qui peut utiliser le tunnel.

Étape 2. Si vous connaissez l'adresse IP du routeur distant, choisissez l'adresse IP dans la liste déroulante située directement sous le champ Remote Security Gateway Type et saisissez l'adresse. Choisissez IP by DNS Resolved si vous ne connaissez pas l'adresse IP mais que vous connaissez le nom de domaine et saisissez le nom de domaine du routeur distant dans le champ IP by DNS Resolved

Étape 3. Sélectionnez un certificat dans la liste déroulante Certificat distant. Les certificats offrent une sécurité d'authentification renforcée sur les connexions VPN.

Étape 4. (Facultatif) Cliquez sur le bouton **Importer un certificat distant** pour importer un nouveau certificat.

Étape 5. (Facultatif) Cliquez sur le bouton **Autoriser CSR** pour identifier le certificat avec une demande de signature numérique.

Étape 6. Dans la liste déroulante Local Security Group Type, sélectionnez l'une des options suivantes :

·IP Address : cette option vous permet de spécifier un périphérique pouvant utiliser ce tunnel VPN. Vous devez seulement entrer l'adresse IP du périphérique dans le champ d'adresse IP.

·Subnet : sélectionnez cette option pour autoriser tous les périphériques appartenant au même sous-réseau à utiliser le tunnel VPN. Vous devez entrer l'adresse IP du réseau dans le champ IP Address (Adresse IP) et son masque de sous-réseau respectif dans le champ Subnet Mask (Masque de sous-réseau).

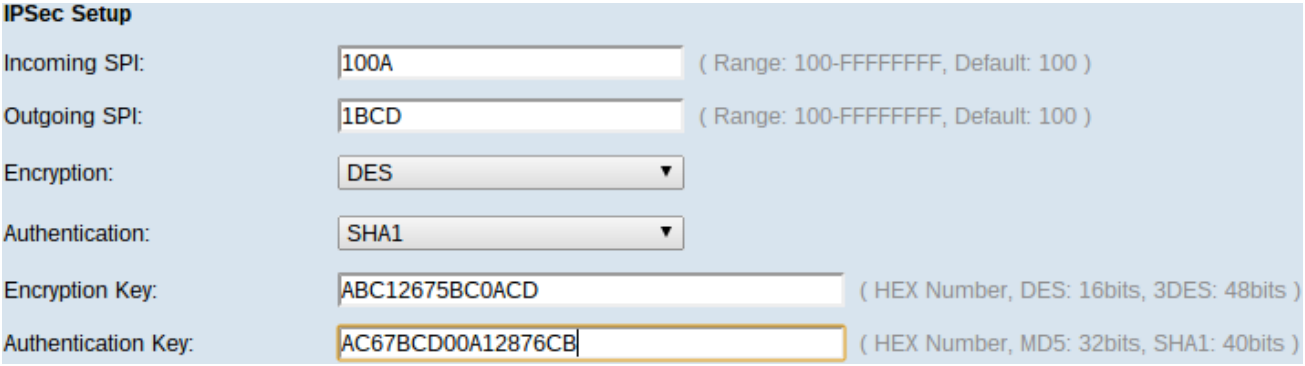
·IP Range : sélectionnez cette option pour spécifier une plage de périphériques pouvant utiliser le tunnel VPN. Vous devez entrer la première adresse IP et la dernière adresse IP de la plage de périphériques. Dans le champ Begin IP et End IP.

Configuration IPSec

Pour que le chiffrement soit correctement configuré entre les deux extrémités du tunnel VPN, les deux paramètres doivent être identiques. Dans ce cas, IPSec crée une authentification sécurisée entre les deux périphériques. Il le fait en deux phases.

Configuration d'IPSec pour le mode Clé manuelle

Disponible uniquement si Manual a été sélectionné dans la liste déroulante Keying Mode de l'étape 3 de Add a New Tunnel. Il s'agit d'un mode de sécurité personnalisé permettant de générer une nouvelle clé de sécurité par vous-même et de ne pas négocier avec la clé. Il est conseillé d'utiliser ce mode pendant un dépannage et dans des petits environnements statiques.



Étape 1. Saisissez la valeur hexadécimale unique pour l'index de paramètre de sécurité entrant (SPI) dans le champ SPI entrant. SPI est transporté dans l'en-tête du protocole ESP (Encapsulating Security Payload) qui détermine ensemble la protection du paquet entrant. Vous pouvez saisir de 100 à ffffffff.

Étape 2. Saisissez la valeur hexadécimale unique pour SPI dans le champ Outgoing SPI. SPI est transporté dans l'en-tête ESP qui détermine ensemble la protection du paquet sortant. Vous pouvez saisir de 100 à ffffffff.

Note: Les SPI entrants et sortants doivent s'apparier aux deux extrémités afin d'établir un tunnel.

Étape 3. Choisissez la méthode de cryptage appropriée dans la liste déroulante Encryption (Cryptage). Le chiffrement recommandé est 3DES. Le tunnel VPN doit utiliser la même méthode de chiffrement pour ses deux extrémités.

·DES - DES (Data Encryption Standard) est une méthode de cryptage 56 bits ancienne, plus rétrocompatible, qui n'est pas aussi sécurisée qu'il est facile à casser.

·3DES - 3DES (Triple Data Encryption Standard) est une méthode de cryptage simple de 168 bits qui permet d'augmenter la taille de la clé en cryptant les données trois fois, ce qui renforce la sécurité par rapport aux DES.

Étape 4. Sélectionnez la méthode d'authentification appropriée dans la liste déroulante Authentification. L'authentification recommandée est SHA1. Le tunnel VPN doit utiliser la même méthode d’authentification pour ses deux extrémités.

·MD5 — MD5 (Message Digest Algorithm-5) représente une fonction de hachage hexadécimal à 32 chiffres qui protège les données contre les attaques malveillantes par le calcul de la somme de contrôle.

·SHA1 — SHA1 (Secure Hash Algorithm version 1) est une fonction de hachage de 160 bits plus sécurisée que MD5.

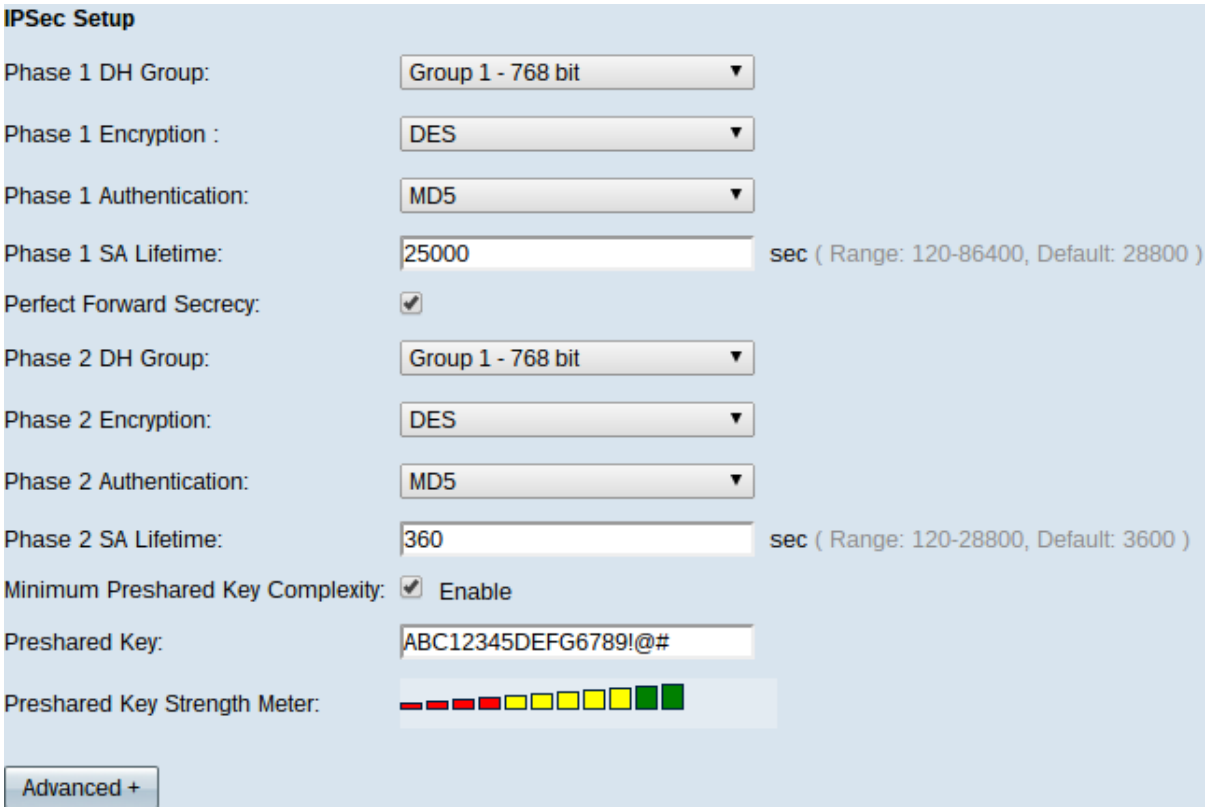
Étape 5. Saisissez la clé pour chiffrer et déchiffrer les données dans le champ Encryption Key (Clé de chiffrement). Si vous choisissez la méthode de chiffrement DES, à l’étape 3, saisissez une valeur hexadécimale de 16 chiffres. Si vous choisissez la méthode de chiffrement 3DES, à l’étape 3, saisissez une valeur hexadécimale de 40 chiffres.

Étape 6. Entrez une clé pré-partagée pour authentifier le trafic dans le champ Authentication Key. Si vous choisissez MD5 comme méthode d'authentification à l'étape 4, entrez une valeur hexadécimale à 32 chiffres. Si vous choisissez SHA comme méthode d'authentification à l'étape 4, entrez une valeur hexadécimale à 40 chiffres. Le tunnel VPN doit utiliser la même clé prépartagée pour ses deux extrémités.

Étape 7. Cliquez sur **Save pour enregistrer les paramètres.**

Configuration IPSec pour IKE avec clé prépartagée

Disponible uniquement si IKE avec clé prépartagée a été sélectionné dans la liste déroulante Mode de clé de l'étape 3 de l'ajout d'un nouveau tunnel.



Étape 1. Sélectionnez le groupe DH de phase 1 approprié dans la liste déroulante Groupe DH de phase 1. La phase 1 est utilisée pour établir le simplex, l'association de sécurité logique (SA) entre les deux extrémités du tunnel afin de prendre en charge la communication sécurisée de l'authentification. Diffie-Hellman (DH) est un protocole d'échange de clé de chiffrement utilisé lors de la connexion de phase 1 pour partager une clé secrète afin d'authentifier la communication.

·Groupe 1 - 768 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.

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

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

Étape 2. Choisissez le chiffrement de phase 1 approprié pour chiffrer la clé dans la liste déroulante de chiffrement de phase 1. Les normes AES-128, AES-192 ou AES-256 sont recommandées. Le tunnel VPN doit utiliser la même méthode de chiffrement pour ses deux extrémités.

·DES - Data Encryption Standard (DES) est une ancienne méthode de cryptage 56 bits qui n'est pas très sécurisée dans le monde d'aujourd'hui.

·3DES - La norme 3DES (Triple Data Encryption Standard) est une méthode de cryptage simple de 168 bits qui permet d'augmenter la taille de la clé en cryptant les données trois fois, ce qui assure plus de sécurité que DES.

·AES-128 — Advanced Encryption Standard (AES) est une méthode de cryptage 128 bits qui transforme le texte brut en texte chiffré à l'aide de répétitions de 10 cycles.

·AES-192 : méthode de cryptage 192 bits qui transforme le texte brut en texte chiffré en 12 cycles de répétitions.

·AES-256 — Méthode de cryptage 256 bits qui transforme le texte brut en texte chiffré à l'aide de répétitions de 14 cycles.

Étape 3. Sélectionnez la méthode d'authentification appropriée dans la liste déroulante Phase 1 Authentication. Le tunnel VPN doit utiliser la même méthode d'authentification pour ses deux extrémités. SHA1 est recommandé.

·MD5 — Message Digest Algorithm-5 (MD5) représente une fonction de hachage hexadécimal à 32 chiffres qui fournit une protection aux données contre les attaques malveillantes par le calcul de la somme de contrôle.

·SHA1 : fonction de hachage 160 bits plus sécurisée que MD5.

Étape 4. Saisissez la durée en secondes pendant laquelle le tunnel VPN reste actif dans le champ Durée de vie de l'association de sécurité de phase 1.

Étape 5. Cochez la case Perfect Forward Secrecy pour mieux protéger les clés. Cette option permet de générer une nouvelle clé si une clé est compromise. Les données chiffrées sont uniquement compromises par le biais de la clé compromise. Par conséquent, cela assure donc une communication plus sécurisée et authentifiée en sécurisant d'autres clés, même si une clé est compromise. Il s'agit d'une action recommandée, car elle fournit plus de sécurité.

Étape 6. Choisissez le groupe DH de phase 2 approprié dans la liste déroulante Groupe DH de phase 2. La phase 1 est utilisée pour établir le simplex, l'association de sécurité logique (SA) entre les deux extrémités du tunnel afin de prendre en charge la communication sécurisée de l'authentification. DH est un protocole d'échange de clés cryptographiques utilisé lors de la connexion de phase 1 pour partager une clé secrète afin d'authentifier la communication.

·Groupe 1 - 768 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.

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

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

Note: Comme aucune nouvelle clé n'est générée, vous n'avez pas besoin de configurer le groupe DH de phase 2 si vous décochez Perfect Forward Secrecy à l'étape 5.

Étape 7. Choisissez le chiffrement de phase 2 approprié pour chiffrer la clé dans la liste déroulante de chiffrement de phase 2. Les normes AES-128, AES-192 ou AES-256 sont recommandées. Le tunnel VPN doit utiliser la même méthode de chiffrement pour ses deux extrémités.

·DES — DES est une ancienne méthode de cryptage 56 bits qui n'est pas très sécurisée dans le monde d'aujourd'hui.

·3DES - 3DES est une méthode de cryptage simple et 168 bits qui permet d'augmenter la

taille de la clé en cryptant les données trois fois, ce qui fournit plus de sécurité que DES.

·AES-128 — AES est une méthode de cryptage 128 bits qui transforme le texte brut en texte chiffré à l'aide de répétitions de 10 cycles.

·AES-192 : méthode de cryptage 192 bits qui transforme le texte brut en texte chiffré en 12 cycles de répétitions.

·AES-256 — Méthode de cryptage 256 bits qui transforme le texte brut en texte chiffré à l'aide de répétitions de 14 cycles.

Étape 8. Choisissez la méthode d'authentification appropriée dans la liste déroulante Phase 2 Authentication. Le tunnel VPN doit utiliser la même méthode d'authentification pour ses deux extrémités.

·MD5 — MD5 représente une fonction de hachage hexadécimal à 32 chiffres qui protège les données contre les attaques malveillantes par le calcul de la somme de contrôle.

·SHA1 — Secure Hash Algorithm version 1 (SHA1) est une fonction de hachage de 160 bits plus sécurisée que MD5.

·Null : aucune méthode d'authentification n'est utilisée.

Étape 9. Saisissez la durée en secondes pendant laquelle le tunnel VPN reste actif dans le champ Durée de vie de l'association de sécurité de phase 2.

Étape 10. Activez la case à cocher Minimum Preshared Key Complexity (complexité minimale des clés prépartagées) si vous souhaitez activer la mesure de force pour la clé prépartagée.

Étape 11. Saisissez une clé précédemment partagée par les homologues IKE dans le champ Preshared Key. Jusqu'à 30 caractères hexadécimaux et caractères peuvent être utilisés comme clé prépartagée. Le tunnel VPN doit utiliser la même clé prépartagée pour ses deux extrémités.

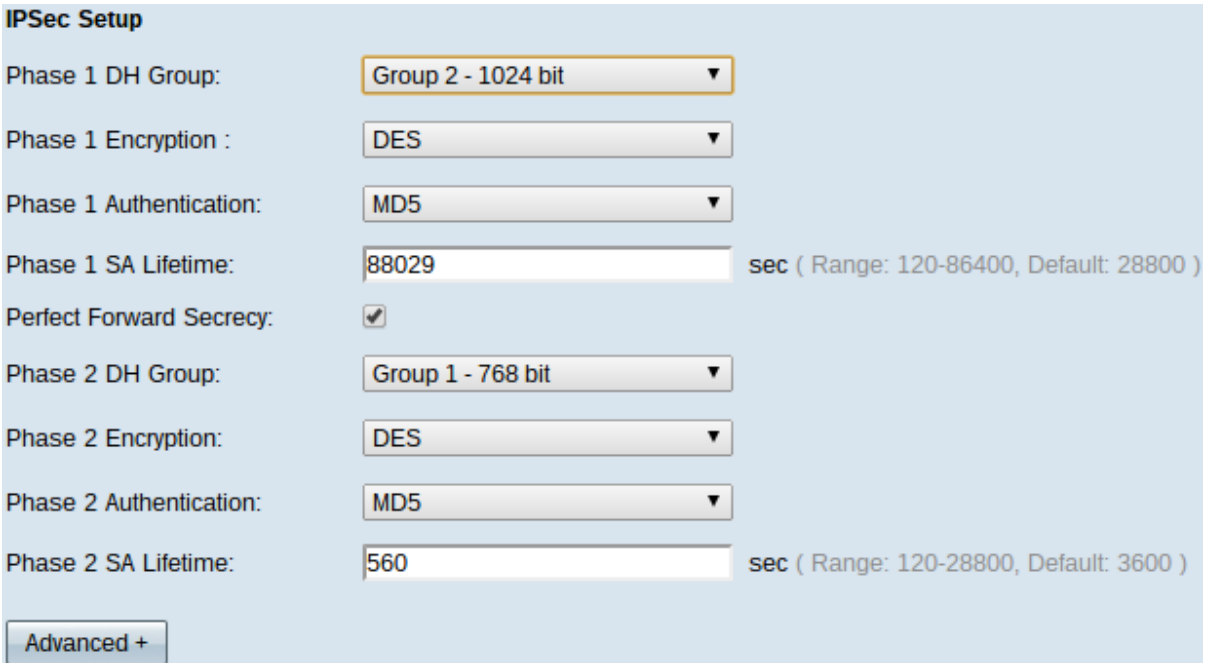
Note: Il est fortement recommandé de modifier fréquemment la clé pré-partagée entre les homologues IKE afin que le VPN reste sécurisé.

La valeur de la clé pré-partagée indique la force de la clé pré-partagée par le biais de barres de couleurs. La couleur rouge indique une puissance faible, la couleur jaune, une puissance acceptable et le vert, une puissance élevée.

Étape 12. Cliquez sur **Save pour enregistrer les paramètres.**

Configuration IPSec pour IKE avec certificat

Disponible uniquement si IKE avec certificat a été sélectionné dans la liste déroulante Keying Mode de l'étape 3 de Add a New Tunnel.



Étape 1. Sélectionnez le groupe DH de phase 1 approprié dans la liste déroulante Groupe DH de phase 1. La phase 1 est utilisée pour établir l'association de sécurité logique simplex entre les deux extrémités du tunnel afin de prendre en charge la communication d'authentification sécurisée. DH est un protocole d'échange de clés cryptographiques utilisé lors de la connexion de phase 1 pour partager une clé secrète afin d'authentifier la communication.

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

·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 faible et le groupe d'authentification le plus non sécurisé. Il faut moins de temps pour calculer les clés IKE. Cette option est préférable si le débit du réseau est faible.

Étape 2. Choisissez le chiffrement de phase 1 approprié pour chiffrer la clé dans la liste déroulante de chiffrement de phase 1. Les normes AES-128, AES-192 ou AES-256 sont recommandées. Le tunnel VPN doit utiliser la même méthode de chiffrement pour ses deux extrémités.

·DES — DES est une ancienne méthode de cryptage 56 bits qui n'est pas très sécurisée dans le monde d'aujourd'hui.

·3DES - 3DES est une méthode de cryptage simple et 168 bits qui permet d'augmenter la taille de la clé en cryptant les données trois fois, ce qui fournit plus de sécurité que DES.

·AES-128 — AES est une méthode de cryptage 128 bits qui transforme le texte brut en texte chiffré à l'aide de répétitions de 10 cycles.

·AES-192 : méthode de cryptage 192 bits qui transforme le texte brut en texte chiffré en 12 cycles de répétitions.

·AES-256 — Méthode de cryptage 256 bits qui transforme le texte brut en texte chiffré à l'aide de répétitions de 14 cycles.

Étape 3. Sélectionnez la méthode d'authentification appropriée dans la liste déroulante Phase 1 Authentication. Le tunnel VPN doit utiliser la même méthode d'authentification pour ses deux extrémités. SHA1 est recommandé.

·MD5 — MD5 représente une fonction de hachage hexadécimal à 32 chiffres qui protège les données contre les attaques malveillantes par le calcul de la somme de contrôle.

·SHA1 : fonction de hachage 160 bits plus sécurisée que MD5.

Étape 4. Saisissez la durée en secondes pendant laquelle le tunnel VPN reste actif dans le champ Durée de vie de l'association de sécurité de phase 1.

Étape 5. Cochez la case Perfect Forward Secrecy pour mieux protéger les clés. Cette option permet de générer une nouvelle clé si une clé est compromise. Les données chiffrées sont uniquement compromises par le biais de la clé compromise. Il fournit donc des communications plus sécurisées et authentifiées tout en sécurisant les autres clés lorsqu'une autre clé est compromise. Il s'agit d'une action recommandée, car elle fournit plus de sécurité.

Étape 6. Choisissez le groupe DH de phase 2 approprié dans la liste déroulante Groupe DH de phase 2. La phase 1 est utilisée pour établir l'association de sécurité logique simplex entre les deux extrémités du tunnel afin de prendre en charge la communication d'authentification sécurisée. DH est un protocole d'échange de clés cryptographiques utilisé lors de la connexion de phase 1 pour partager une clé secrète afin d'authentifier la communication.

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

·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 faible et le groupe d'authentification le plus non sécurisé. Il faut moins de temps pour calculer les clés IKE. Cette option est préférable si le débit du réseau est faible.

Note: Comme aucune nouvelle clé n'est générée, vous n'avez pas besoin de configurer le groupe DH de phase 2 si vous avez décoché Perfect Forward Secrecy à l'étape 5.

Étape 7. Choisissez le chiffrement de phase 2 approprié pour chiffrer la clé dans la liste déroulante de chiffrement de phase 2. Les normes AES-128, AES-192 ou AES-256 sont recommandées. Le tunnel VPN doit utiliser la même méthode de chiffrement pour ses deux extrémités.

·DES — DES est une ancienne méthode de cryptage 56 bits qui n'est pas très sécurisée dans le monde d'aujourd'hui.

·3DES - 3DES est une méthode de cryptage simple et 168 bits qui permet d'augmenter la taille de la clé en cryptant les données trois fois, ce qui fournit plus de sécurité que DES.

·AES-128 — AES est une méthode de cryptage 128 bits qui transforme le texte brut en texte chiffré à l'aide de répétitions de 10 cycles.

·AES-192 : méthode de cryptage 192 bits qui transforme le texte brut en texte chiffré en 12

cycles de répétitions.

·AES-256 — Méthode de cryptage 256 bits qui transforme le texte brut en texte chiffré à l'aide de répétitions de 14 cycles.

Étape 8. Choisissez la méthode d'authentification appropriée dans la liste déroulante Phase 2 Authentication. Le tunnel VPN doit utiliser la même méthode d'authentification pour ses deux extrémités.

·MD5 — MD5 représente une fonction de hachage hexadécimal à 32 chiffres qui protège les données contre les attaques malveillantes par le calcul de la somme de contrôle.

·SHA1 — SHA1 est une fonction de hachage de 160 bits plus sécurisée que MD5.

·Null : aucune méthode d'authentification n'est utilisée.

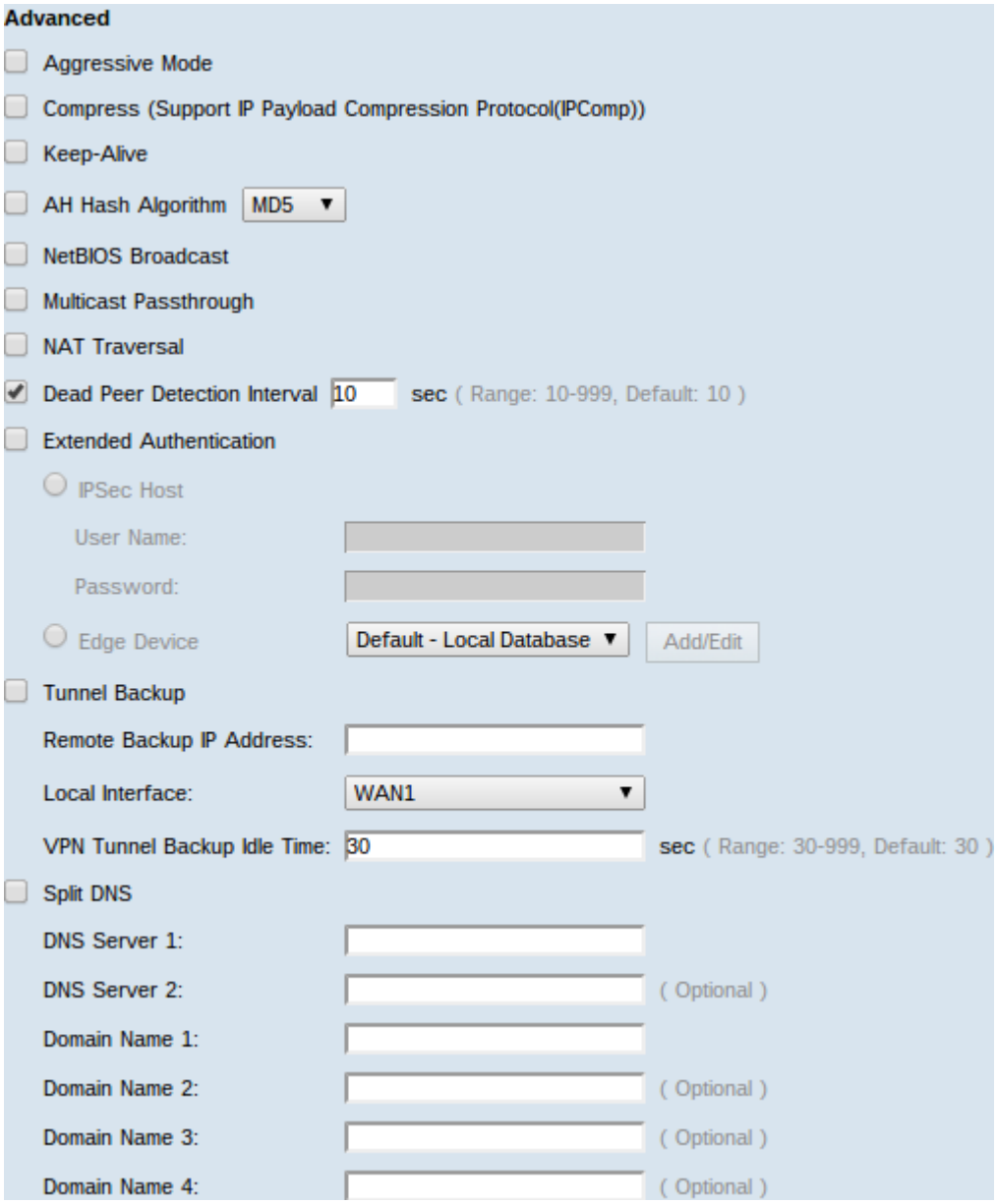
Étape 9. Saisissez la durée en secondes pendant laquelle le tunnel VPN reste actif dans le champ Durée de vie de l'association de sécurité de phase 2.

Étape 10. Cliquez sur **Save pour enregistrer les paramètres.**

(Facultatif) Configuration avancée IPSec pour IKE avec certificat et IKE avec clé prépartagée

Les options avancées sont disponibles si IKE avec certificat ou IKE avec clé pré-partagée a été sélectionné dans la liste déroulante Keying Mode de l'étape 3 de Add a New Tunnel. Les mêmes paramètres sont disponibles pour les deux types de modes de frappe.

Étape 1. Cliquez sur le bouton **Avancé+** pour afficher les options IPSec avancées.



Étape 2. Cochez la case Aggressive Mode si la vitesse de votre réseau est faible. Il échange les ID des points d'extrémité du tunnel en texte clair pendant la connexion SA, ce qui nécessite moins de temps pour échanger mais moins de sécurité.

Étape 3. Cochez la case Compress (Support IP Payload Compression Protocol (IPComp)) si vous voulez compresser la taille du datagramme IP. IPComp est un protocole de compression IP utilisé pour compresser la taille du datagramme IP, si la vitesse du réseau est faible et que l'utilisateur souhaite transmettre rapidement les données sans perte via le réseau lent.

Étape 4.Cochez la case Keep-Alive si vous voulez toujours que la connexion du tunnel VPN reste active. Il permet de rétablir immédiatement les connexions si une connexion devient inactive.

Étape 5. Cochez la case Algorithme de hachage AH si vous voulez authentifier l'en-tête d'authentification (AH). AH assure l'authentification à l'origine des données, l'intégrité des données via la somme de contrôle et la protection est étendue à l'en-tête IP. Le tunnel doit avoir le même algorithme pour les deux côtés.

·MD5 — MD5 représente une fonction de hachage hexadécimal à 128 chiffres qui protège les données contre les attaques malveillantes par le calcul de la somme de contrôle.

·SHA1 — SHA1 est une fonction de hachage de 160 bits plus sécurisée que MD5.

Étape 6. Vérifiez la diffusion NetBIOS (NetBIOS Broadcast) si vous souhaitez autoriser le trafic non routable via le tunnel VPN. La case est décochée par défaut. NetBIOS est utilisé pour détecter les ressources réseau, telles que les imprimantes, les ordinateurs, etc. dans le réseau, via certaines applications logicielles et des fonctionnalités Windows telles que le voisinage réseau.

Étape 7. Si votre routeur VPN se trouve derrière une passerelle NAT, cochez cette case pour activer la traversée NAT. La traduction d'adresses de réseau (NAT) permet aux utilisateurs disposant d'adresses LAN privées d'accéder aux ressources Internet en utilisant une adresse IP routable publiquement comme adresse source. Cependant, pour le trafic entrant, la passerelle NAT ne dispose pas d'une méthode automatique de traduction de l'adresse IP publique vers une destination particulière sur le réseau local privé. Ce problème empêche les échanges IPSec réussis. NAT traversal configure cette traduction entrante. Le même paramètre doit être utilisé aux deux extrémités du tunnel.

Étape 8. Cochez la case Dead Peer Detection Interval (intervalle de détection des homologues inactifs) pour vérifier l'activité du tunnel VPN via des messages Hello ou ACK, de manière régulière. Si vous cochez cette case, entrez la durée ou l'intervalle en secondes des messages Hello que vous souhaitez.

Étape 9. Cochez la case Extended Authentication pour utiliser un nom d'utilisateur et un mot de passe d'hôte IPSec pour authentifier les clients VPN ou pour utiliser la base de données trouvée dans User Management. Cette option doit être activée sur les deux périphériques pour qu'elle fonctionne. Cliquez sur la case d'option **Hôte IPSec** pour utiliser l'hôte et le nom d'utilisateur IPSec et entrez le nom d'utilisateur et le mot de passe dans le champ Nom d'utilisateur et Mot de passe. Ou cliquez sur la case d'option **Périphérique Edge** pour utiliser une base de données. Sélectionnez la base de données souhaitée dans la liste déroulante Périphérique de périphérie.

Étape 10. Cochez la case Tunnel Backup (Sauvegarde du tunnel) pour activer la sauvegarde du tunnel. Cette fonctionnalité est disponible lorsque l'intervalle de détection des homologues morts a été vérifié. Cette fonctionnalité permet au périphérique de rétablir le tunnel VPN via une autre interface WAN ou adresse IP.

·Remote Backup IP Address : adresse IP alternative pour l'homologue distant. Saisissez-le ou l'adresse IP WAN déjà définie pour la passerelle distante dans ce champ.

·Local Interface : interface WAN utilisée pour rétablir la connexion. Sélectionnez l'interface souhaitée dans la liste déroulante.

·VPN Tunnel Backup Idle Time : heure choisie pour quand utiliser le tunnel de sauvegarde si le tunnel principal n'est pas connecté. Saisissez-le en secondes.

Étape 11. Cochez la case Split DNS pour activer le DNS fractionné. Cette fonctionnalité permet d'envoyer une requête DNS à un serveur DNS défini en fonction de noms de domaine spécifiés. Entrez les noms de serveur DNS dans les champs DNS Server 1 et DNS Server 2 et saisissez les noms de domaine dans les champs Domain Name #.

Étape 12. Cliquez sur **Enregistrer** pour terminer la configuration du périphérique.