

Configurar a VPN (Advanced Virtual Private Network) no firewall RV110W

Objetivo

A VPN (Virtual Private Network) usa a rede pública, ou a Internet, para estabelecer uma rede privada para se comunicar com segurança. Um Internet Key Exchange (IKE) é um protocolo que estabelece a comunicação segura entre duas redes. Ele é usado para trocar uma chave antes do tráfego fluir, o que garante autenticidade para ambas as extremidades do túnel VPN.

Ambas as extremidades da VPN devem seguir a mesma política de VPN para se comunicarem com êxito.

O objetivo deste documento é explicar como adicionar um perfil IKE e configurar a política VPN no RV110W Wireless Router.

Dispositivos aplicáveis

RV110W

Versão de software

•1.2.0.9

Configurações de política IKE

O Internet Key Exchange (IKE) é um protocolo usado para estabelecer uma conexão segura para comunicação em uma VPN. Essa conexão estabelecida e segura é chamada de associação de segurança (SA). Este procedimento explica como configurar uma política IKE para a conexão VPN a ser usada para segurança. Para que uma VPN funcione corretamente, as políticas de IKE para ambos os terminais devem ser idênticas.

Etapa 1. Faça login no utilitário de configuração da Web e escolha **VPN > Advanced VPN Setup**. A página *Advanced VPN Setup* é aberta:

Advanced VPN Setup

IKE Policy Table							
<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input type="checkbox"/>	No data to display						
<input type="button" value="Add Row"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>					

VPN Policy Table							
<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input type="checkbox"/>	No data to display						
<input type="button" value="Add Row"/>	<input type="button" value="Edit"/>	<input type="button" value="Enable"/>	<input type="button" value="Disable"/>	<input type="button" value="Delete"/>			

Advanced VPN Setup

IKE Policy Table

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

VPN Policy Table

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

Etapa 2. Clique em **Adicionar linha** para criar uma nova política IKE. A página *Advanced VPN Setup* é aberta:

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode: ▼

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

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

Etapa 3. No campo *Nome da política*, insira um nome para a política IKE a ser facilmente identificada.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode: Main
Main
Aggressive

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

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

Etapa 4. Escolha uma opção na lista suspensa *Exchange Mode*:

Main — Permite que a política IKE opere de forma mais segura, mas mais lenta que o modo agressivo. Escolha esta opção se for necessária uma conexão VPN mais segura.

Agressivo - Permite que a política IKE opere mais rápido, mas com menos segurança que o modo principal. Escolha esta opção se for necessária uma conexão VPN mais rápida.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

IKE SA Parameters

Encryption Algorithm: (dropdown menu open showing: AES-128, DES, 3DES, AES-128, AES-192, AES-256)

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

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

Dead Peer Detection: Enable

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

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

Etapa 5. Escolha um algoritmo na lista suspensa *Encryption Algorithm*:

DES — O Data Encryption Standard (DES) usa um tamanho de chave de 56 bits para criptografia de dados. O DES está desatualizado e deve ser usado apenas se um endpoint for compatível apenas com DES.

3DES — 3DES (Triple Data Encryption Standard) executa DES três vezes, mas varia o tamanho da chave de 168 bits para 112 bits e de 112 bits para 56 bits, dependendo do ciclo de DES executado. O 3DES é mais seguro que o DES e o AES.

AES-128 — Advanced Encryption Standard com chave de 128 bits (AES-128) usa uma chave de 128 bits para criptografia AES. O AES é mais rápido e mais seguro que o DES. Em geral, o AES também é mais rápido, mas menos seguro que o 3DES, mas alguns tipos de hardware permitem que o 3DES seja mais rápido. O AES-128 é mais rápido, mas menos seguro que o AES-192 e o AES-256.

AES-192 — AES-192 usa uma chave de 192 bits para a criptografia AES. O AES-192 é mais lento, mas mais seguro do que o AES-128, e o AES-192 é mais rápido, mas menos seguro do que o AES-256.

AES-256 — AES-256 usa uma chave de 256 bits para a criptografia AES. O AES-256 é mais lento, mas mais seguro que o AES-128 e o AES-192.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

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

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

Etapa 6. Escolha a autenticação desejada na lista suspensa *Authentication Algorithm*:

MD5 — O Message-Digest Algorithm 5 (MD5) usa um valor de hash de 128 bits para a autenticação. MD5 é menos seguro, mas mais rápido que SHA-1 e SHA2-256.

SHA-1 — A Secure Hash Function 1 (SHA-1) usa um valor de hash de 160 bits para autenticação. O SHA-1 é mais lento, mas mais seguro que o MD5, e o SHA-1 é mais rápido, mas menos seguro que o SHA2-256.

SHA2-256 — Algoritmo Hash Seguro 2 com um valor hash de 256 bits (SHA2-256) usa um valor hash de 256 bits para autenticação. SHA2-256 é mais lento, mas seguro que MD5 e SHA-1.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

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

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

Passo 7. No campo *Pre-Shared Key*, insira uma chave pré-compartilhada que a política IKE usa.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

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

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

Etapa 8. Na lista suspensa *Grupo Diffie-Hellman (DH)*, escolha qual grupo DH o IKE usa. Os hosts em um grupo DH podem trocar chaves sem se conhecerem. Quanto mais alto o número de bits do grupo, mais seguro o grupo estará.

Grupo 1 - 768 bits — A chave de força mais baixa e o grupo de autenticação mais inseguro.

Porém, leva menos tempo para computar as chaves de IKE. Essa opção é preferida se a velocidade da rede for baixa.

Grupo 2 - 1024 bits — A chave de maior força e o grupo de autenticação mais seguro. Mas precisa de algum tempo para computar as chaves de IKE.

Grupo 5 - 1536 bits — Representa a chave de força mais alta e o grupo de autenticação mais seguro. Precisa de mais tempo para computar as chaves de IKE. É preferível se a velocidade da rede for alta.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

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

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

Etapa 9. Digite o tempo (em segundos) que um SA para a VPN dura antes do SA ser renovado no campo *SA-Lifetime*.

Etapa 10. (Opcional) Marque a caixa de seleção **Habilitar** no campo *Dead Peer Detection* para habilitar a Dead Peer Detection. A Dead Peer Detection monitora os pares IKE para ver se um peer deixou de funcionar. A Detecção de Pares Mortos evita o desperdício de recursos de rede em pares inativos.

Etapa 11. (Opcional) Se você habilitou a Detecção de Peer Deed na Etapa 9, insira a frequência (em segundos) com que o peer é verificado quanto à atividade no campo *Deed Peer Delay*.

Etapa 12. (Opcional) Se você habilitou a Deed Peer Detection na Etapa 9, insira quantos segundos aguardar antes que um peer inativo seja descartado no campo Deed Peer Detection Timeout.

Etapa 13. Clique em **Salvar** para aplicar todas as configurações.

Configuração de política de VPN

Etapa 1. Faça login no utilitário de configuração da Web e escolha **VPN > Advanced VPN Setup**.

A página *Advanced VPN Setup (Configuração de VPN Avançada)* é aberta:

The screenshot shows the 'Advanced VPN Setup' interface. At the top, there is a section for 'IKE Policy Table' with a table containing columns for Name, Mode, Local, Remote, Encryption, Authentication, and DH. Below the table are 'Add Row', 'Edit', and 'Delete' buttons. The next section is 'VPN Policy Table' with columns for Status, Name, Type, Local, Remote, Authentication, and Encryption. It also has 'Add Row', 'Edit', 'Enable', 'Disable', and 'Delete' buttons. At the bottom of this section are 'Save' and 'Cancel' buttons, and an 'IPSec Connection Status' button.

This screenshot shows the 'Advanced VPN Setup' page after a successful save. A green checkmark icon is followed by the text 'Configuration settings have been saved successfully'. Below this, the 'IKE Policy Table' is shown with one row: 'policy1' with 'Aggressive' mode. The 'VPN Policy Table' is currently empty, and the 'Add Row' button is highlighted with a red circle. The 'Save' and 'Cancel' buttons are visible at the bottom.

Etapa 2. Clique em **Add Row** (Adicionar linha) na *Tabela de políticas de VPN*. A janela *Advanced VPN Policy Setup (Configuração avançada de política de VPN)* é exibida:

The screenshot shows the 'Advanced VPN Policy Setup' page. The title is 'Advanced VPN Setup'. The main heading is 'Add / Edit VPN Policy Configuration'. The form contains the following fields:

- Policy Name:** A text input field.
- Policy Type:** A dropdown menu with 'Auto Policy' selected.
- Remote Endpoint:** A dropdown menu with 'IP Address' selected, followed by a text input field with a hint '(Hint: 1.2.3.4 or abc.com)'.
- Local Traffic Selection:**
 - Local IP:** A dropdown menu with 'Single' selected.
 - IP Address:** A text input field with a hint '(Hint: 1.2.3.4)'.
 - Subnet Mask:** A text input field with a hint '(Hint: 255.255.255.0)'.
- Remote Traffic Selection:**
 - Remote IP:** A dropdown menu with 'Single' selected.

Adicionar/Editar configuração de política de VPN



Advanced VPN Setup

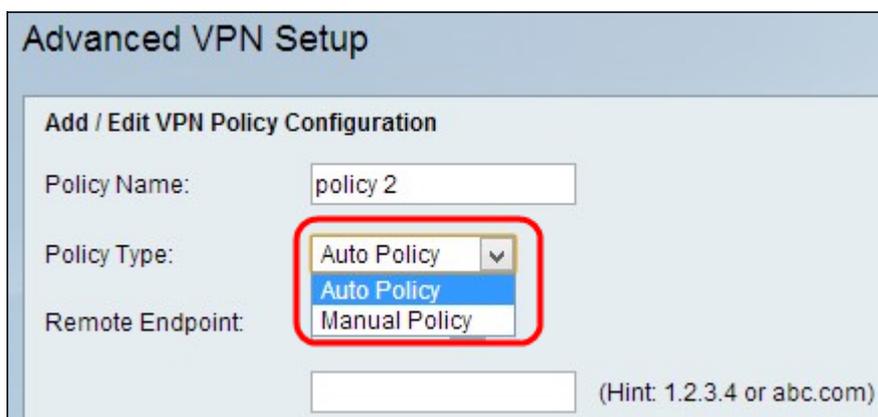
Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint: (Hint: 1.2.3.4 or abc.com)

Etapa 1. Insira um nome exclusivo para a política no campo *Nome da política* para identificá-la facilmente.



Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

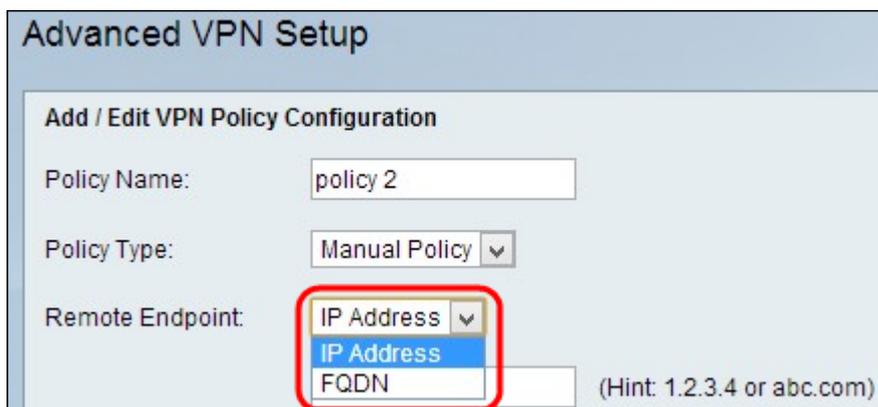
Policy Type:

Remote Endpoint: (Hint: 1.2.3.4 or abc.com)

Etapa 2. Escolha o tipo de política apropriado na lista suspensa *Tipo de política*.

Política automática — Os parâmetros podem ser definidos automaticamente. Nesse caso, além das políticas, é necessário que o protocolo IKE (Internet Key Exchange) negocie entre os dois pontos finais de VPN.

Política manual — Nesse caso, todas as configurações que incluem configurações para chaves para o túnel VPN são inseridas manualmente para cada endpoint.



Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint: (Hint: 1.2.3.4 or abc.com)

Etapa 3. Escolha o tipo de identificador de IP que identifica o gateway no endpoint remoto na lista suspensa *Remote Endpoint*.

Endereço IP — endereço IP do gateway no endpoint remoto. Se você escolher essa opção, insira o endereço IP no campo.

FQDN (Fully Qualified Domain Name, Nome de domínio totalmente qualificado) — Insira o nome

de domínio totalmente qualificado do gateway no endpoint remoto. Se você escolher essa opção, insira o nome de domínio totalmente qualificado no campo fornecido.

Seleção de tráfego local



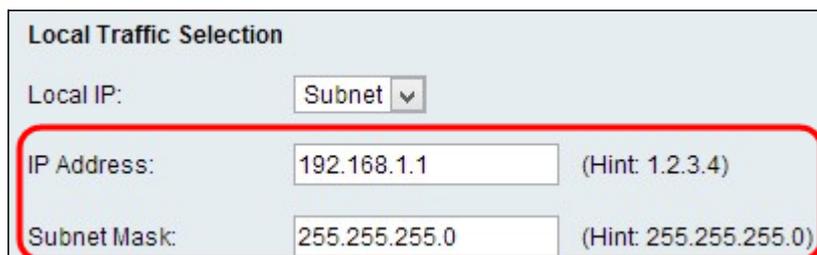
The screenshot shows the 'Local Traffic Selection' form. The 'Local IP:' dropdown menu is open, showing three options: 'Single', 'Single', and 'Subnet'. The 'Single' option is highlighted in blue. The 'IP Address:' and 'Subnet Mask:' fields are empty. There are hints for the IP address (1.2.3.4) and Subnet Mask (255.255.255.0).

Etapa 1. Escolha o tipo de identificador que você deseja fornecer para o ponto final na lista suspensa *IP local*.



The screenshot shows the 'Local Traffic Selection' form. The 'Local IP:' dropdown menu is set to 'Single'. The 'IP Address:' field contains the value '192.168.1.1' and is highlighted with a red box. The 'Subnet Mask:' field is empty. There are hints for the IP address (1.2.3.4) and Subnet Mask (255.255.255.0).

Single - Isso limita a política a um host. Se você escolher essa opção, insira o endereço IP no campo *IP address (Endereço IP)*.



The screenshot shows the 'Local Traffic Selection' form. The 'Local IP:' dropdown menu is set to 'Subnet'. The 'IP Address:' field contains the value '192.168.1.1' and the 'Subnet Mask:' field contains the value '255.255.255.0'. Both fields are highlighted with a red box. There are hints for the IP address (1.2.3.4) and Subnet Mask (255.255.255.0).

Sub-rede — Esta é uma máscara que define os limites de um IP. Isso permite que os hosts da sub-rede especificada se conectem à VPN. Para se conectar à VPN, um computador é selecionado por uma operação AND lógica. Um computador é selecionado se o IP cair no mesmo intervalo necessário. Se você escolher essa opção, insira o endereço IP e a sub-rede no campo *Endereço IP e Sub-rede*.

Seleção de tráfego remoto



The screenshot shows the 'Remote Traffic Selection' form. The 'Remote IP:' dropdown menu is open, showing three options: 'Single', 'Single', and 'Subnet'. The 'Single' option is highlighted in blue. The 'IP Address:' and 'Subnet Mask:' fields are empty. There are hints for the IP address (1.2.3.4) and Subnet Mask (255.255.255.0).

Etapa 1. Escolha o tipo de identificador que você deseja fornecer para o ponto final na lista suspensa *IP local*:

Remote Traffic Selection

Remote IP: ▼

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Single - Isso limita a política a um host. Se você escolher essa opção, insira o endereço IP no campo *IP address (Endereço IP)*.

Remote Traffic Selection

Remote IP: ▼

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Sub-rede — Esta é uma máscara que define os limites de um IP. Isso permite que os hosts da sub-rede especificada se conectem à VPN. Para se conectar à VPN, um computador é selecionado por uma operação AND lógica. Um computador é selecionado se o IP cair no mesmo intervalo necessário. Se você escolher essa opção, insira o endereço IP e a sub-rede no campo *Endereço IP e Sub-rede*.

Parâmetros de política manual

Para configurar parâmetros de política manual, escolha **Política manual** na lista suspensa *Tipo de política* na Etapa 2 da seção *Adicionar/editar configuração de política de VPN*.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm: ▼

Key-In:

Key-Out:

Integrity Algorithm: ▼

Key-In:

Key-Out:

Etapa 1. Insira um valor hexadecimal entre 3 e 8 no campo *SPI-Entrada*. O Stateful Packet Inspection (SPI) é uma tecnologia chamada Deep Packet Inspection. O SPI implementa vários recursos de segurança que ajudam a manter a rede do seu computador segura. O valor SPI-Incoming corresponde ao SPI-Outgoing do dispositivo anterior. Qualquer valor é aceitável, desde que o ponto de extremidade VPN remoto tenha o mesmo valor em seu campo *SPI-Saída*.

Etapa 2. Insira um valor hexadecimal entre 3 e 8 no campo *SPI-Saída*.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm: AES-128 ▼
3DES
DES
AES-128
AES-192
AES-256

Key-In:

Key-Out:

Integrity Algorithm: ▼

Key-In:

Key-Out:

Etapa 3. Escolha o algoritmo de criptografia apropriado na lista suspensa Algoritmo de criptografia.

DES — O Data Encryption Standard (DES) usa um tamanho de chave de 56 bits para criptografia de dados. O DES está desatualizado e deve ser usado apenas se um endpoint for compatível apenas com DES.

3DES — 3DES (Triple Data Encryption Standard) executa DES três vezes, mas varia o tamanho da chave de 168 bits para 112 bits e de 112 bits para 56 bits com base no ciclo de DES executado. O 3DES é mais seguro que o DES e o AES.

AES-128 — Advanced Encryption Standard com chave de 128 bits (AES-128) usa uma chave de 128 bits para criptografia AES. O AES é mais rápido e mais seguro que o DES. Em geral, o AES também é mais rápido, mas menos seguro que o 3DES, mas alguns tipos de hardware permitem que o 3DES seja mais rápido. O AES-128 é mais rápido, mas menos seguro que o AES-192 e o AES-256.

AES-192 — AES-192 usa uma chave de 192 bits para a criptografia AES. O AES-192 é mais lento, mas mais seguro do que o AES-128, e o AES-192 é mais rápido, mas menos seguro do que o AES-256.

AES-256 — AES-256 usa uma chave de 256 bits para a criptografia AES. O AES-256 é mais lento, mas mais seguro que o AES-128 e o AES-192.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

Etapa 4. Insira a chave de criptografia da política de entrada no campo *Key-In*. O comprimento da chave depende do algoritmo escolhido na Etapa 3.

Etapa 5. Insira a chave de criptografia da política de saída no campo *Key-Out* (*Saída Chave*).

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

Etapa 6. Escolha o algoritmo de integridade apropriado na lista suspensa *Algoritmo de integridade*. Esse algoritmo verificará a integridade dos dados:

MD5 — Este algoritmo especifica o comprimento da chave como 16 caracteres. O Message-Digest Algorithm cinco (MD5) não é resistente a colisões e é adequado para aplicações como certificados SSL ou assinaturas digitais que dependem desta propriedade. MD5 compacta qualquer fluxo de byte em um valor de 128 bits, mas o SHA o compacta em um valor de 160 bits. MD5 é um pouco mais barato de computar, no entanto, MD5 é uma versão mais antiga do algoritmo de hash e está vulnerável a ataques de colisão.

SHA1 — O Secure Hash Algorithm versão 1 (SHA1) é uma função de hash de 160 bits mais segura que o MD5, mas leva mais tempo para computar.

SHA2-256 — Este algoritmo especifica o comprimento da chave como 32 caracteres.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

Passo 7. Insira a chave de integridade (para ESP com modo de Integridade) para a política de entrada. O comprimento da chave depende do algoritmo escolhido na Etapa 6.

Etapa 8. Insira a chave de integridade da política de saída no campo Key-Out. A conexão VPN está configurada para saída para entrada, portanto, as chaves de saída de uma extremidade precisam corresponder às chaves de entrada na outra extremidade.

Note: SPI-Entrada e Saída, Algoritmo de Criptografia, Algoritmo de Integridade e Chaves precisam ser iguais na outra extremidade do túnel VPN para uma conexão bem-sucedida.

Parâmetros de política automática

Auto Policy Parameters

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

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: Enable

Select IKE Policy:

Etapa 1. Insira a duração da associação de segurança (SA) em segundos no campo SA Lifetime. A vida útil do SA é quando qualquer chave atingiu sua vida útil, qualquer SA associado é renegociado automaticamente.

Etapa 2. Escolha o algoritmo de criptografia apropriado na lista suspensa Algoritmo de criptografia:

DES — O Data Encryption Standard (DES) usa um tamanho de chave de 56 bits para criptografia de dados. O DES está desatualizado e deve ser usado apenas se um endpoint for compatível apenas com DES.

3DES — 3DES (Triple Data Encryption Standard) executa DES três vezes, mas varia o tamanho da chave de 168 bits para 112 bits e de 112 bits para 56 bits com base no ciclo de DES executado. O 3DES é mais seguro que o DES e o AES.

AES-128 — Advanced Encryption Standard com chave de 128 bits (AES-128) usa uma chave de 128 bits para criptografia AES. O AES é mais rápido e mais seguro que o DES. Em geral, o AES também é mais rápido, mas menos seguro que o 3DES, mas alguns tipos de hardware permitem que o 3DES seja mais rápido. O AES-128 é mais rápido, mas menos seguro que o AES-192 e o AES-256.

AES-192 — AES-192 usa uma chave de 192 bits para a criptografia AES. O AES-192 é mais lento, mas mais seguro do que o AES-128, e o AES-192 é mais rápido, mas menos seguro do que o AES-256.

AES-256 — AES-256 usa uma chave de 256 bits para a criptografia AES. O AES-256 é mais lento, mas mais seguro que o AES-128 e o AES-192.

Etapa 3. Escolha o Algoritmo de integridade apropriado na lista suspensa Algoritmo de integridade. Esse algoritmo verifica a integridade dos dados.

MD5 — Este algoritmo especifica o comprimento da chave como 16 caracteres. O Message-

Digest Algorithm cinco (MD5) não é resistente a colisões e é adequado para aplicações como certificados SSL ou assinaturas digitais que dependem desta propriedade. MD5 compacta qualquer fluxo de byte em um valor de 128 bits, mas o SHA o compacta em um valor de 160 bits. MD5 é um pouco mais barato de computar, no entanto, MD5 é uma versão mais antiga do algoritmo de hash e está vulnerável a ataques de colisão.

SHA1 — O Secure Hash Algorithm versão 1 (SHA1) é uma função de hash de 160 bits mais segura que o MD5, mas leva mais tempo para computar.

SHA2-256 — Este algoritmo especifica o comprimento da chave como 32 caracteres.

Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: DES

Integrity Algorithm: SHA-1

PFS Key Group: Enable

DH-Group 1(768 bit)

Select IKE Policy: policy1

View

Etapa 4. (Opcional) Marque a caixa de seleção **Habilitar** no campo *Grupo de Chave PFS* para habilitar o Segredo de Encaminhamento Perfeito, que é para melhorar a segurança.

Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: DES

Integrity Algorithm: SHA-1

PFS Key Group: Enable

Select IKE Policy: DH-Group 1(768 bit)

DH-Group 1(768 bit)

DH-Group 2(1024 bit)

DH-Group 5(1536 bit)

View

Etapa 5. Se você marcou **Enable** na Etapa 4, escolha a chave de troca Diffie-Hellman apropriada na lista suspensa do campo *PFS Key Group*.

Grupo 1 - 768 bits — Representa a menor chave de força e o grupo de autenticação mais inseguro. Mas precisa de menos tempo para computar as chaves de IKE. É preferível se a velocidade da rede for baixa.

Grupo 2 - 1024 bits — Representa uma chave de maior intensidade e um grupo de autenticação mais seguro. Mas precisa de algum tempo para computar as chaves de IKE.

Grupo 5 - 1536 bits — Representa a chave de força mais alta e o grupo de autenticação mais seguro. Precisa de mais tempo para computar as chaves de IKE. É preferível se a velocidade da rede for alta.

Auto Policy Parameters

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

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: Enable

Select IKE Policy:

Etapa 6. Escolha a Política IKE apropriada na lista suspensa *Selecionar política IKE*. O Internet Key Exchange (IKE) é um protocolo usado para estabelecer uma conexão segura para comunicação em uma VPN. Essa conexão estabelecida e segura é chamada de associação de segurança (SA). Para que uma VPN funcione corretamente, as políticas de IKE para ambos os terminais devem ser idênticas.

Passo 7. Clique em **Salvar** para aplicar todas as configurações.

Note: SA-Lifetime, Encryption Algorithm, Integrity Algorithm, PFS Key Group e a política IKE precisam ser iguais na outra extremidade do túnel VPN para uma conexão bem-sucedida.

Se quiser ver mais artigos no RV110W, clique [aqui](#).