

Configuração VPN avançada em RV215W

Objetivo

Uma VPN (Virtual Private Network) é uma conexão segura estabelecida dentro de uma rede ou entre redes. As VPNs servem para isolar o tráfego entre hosts e redes especificados do tráfego de hosts e redes não autorizados. Este artigo explica como configurar o Advanced VPN Setup no RV215W.

Dispositivos aplicáveis

RV215W

Versão de software

•1.1.0.5

Configuração de VPN avançada

Configurações iniciais

Este procedimento explica como configurar as definições iniciais da Configuração VPN Avançada.

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

NAT Traversal: Enable

NETBIOS: Enable

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

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

Save Cancel

IPsec Connection Status

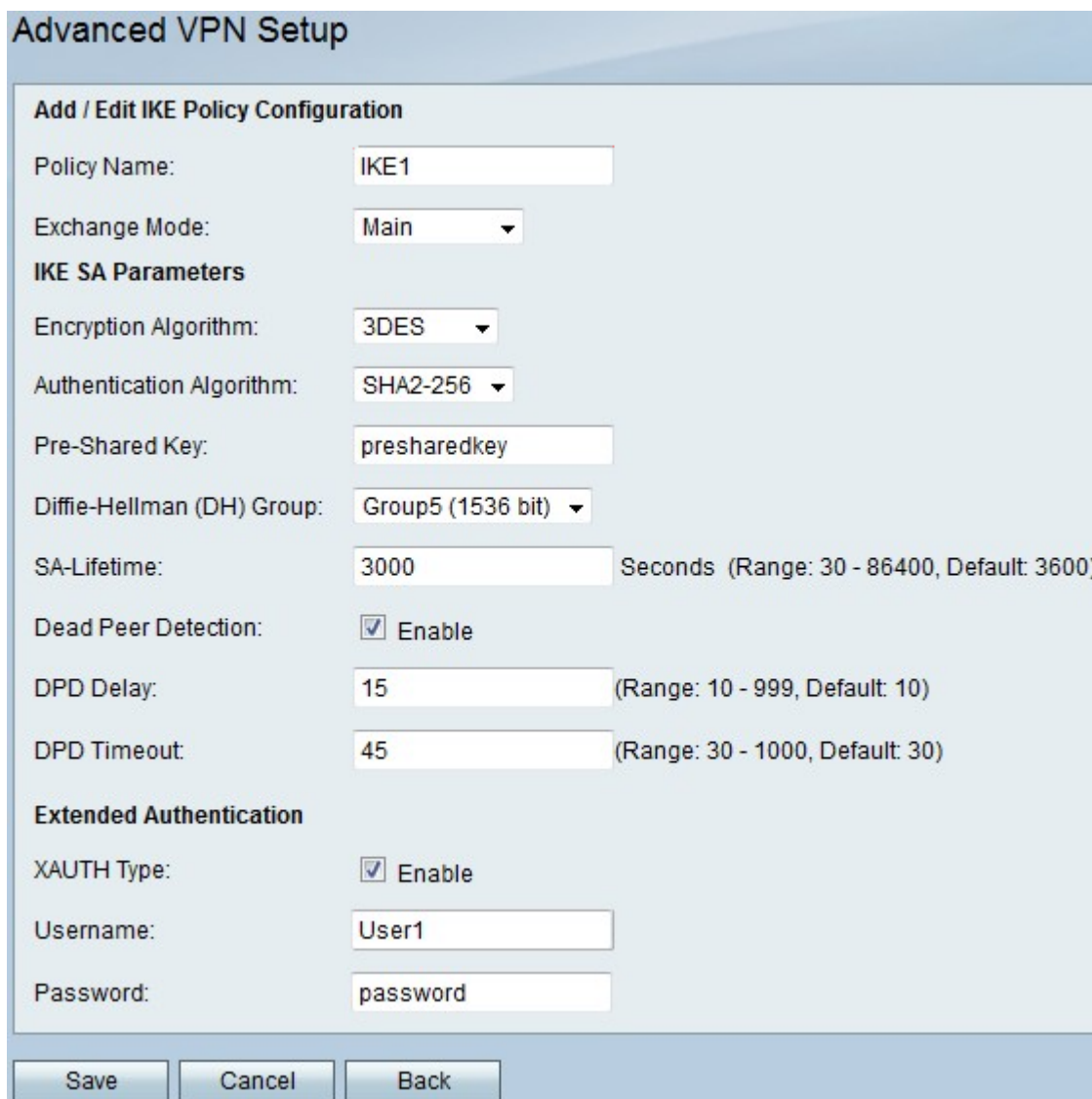
Etapa 2. (Opcional) Marque a caixa de seleção **Habilitar** no campo NAT Traversal se desejar habilitar o NAT (Network Address Translation) Traversal para a conexão VPN. O NAT Traversal permite que uma conexão VPN seja feita entre gateways que usam NAT. Escolha esta opção se sua conexão VPN passar por um gateway ativado para NAT.

Etapa 3. (Opcional) Marque a caixa de seleção **Habilitar** no campo NETBIOS se quiser habilitar os broadcasts do Network Basic Input/Output System (NetBIOS) a serem enviados através da conexão VPN. O NetBIOS permite que os hosts se comuniquem entre si dentro de uma LAN.

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. Na Tabela de Políticas IKE, clique em **Adicionar Linha** para criar uma nova política IKE. Para editar uma diretiva IKE, marque a caixa de seleção da diretiva e clique em **Editar**. A página *Advanced VPN Setup* é alterada:



The screenshot shows the 'Advanced VPN Setup' interface for configuring an IKE policy. The title is 'Advanced VPN Setup'. Below it is a section titled 'Add / Edit IKE Policy Configuration'. The form contains the following fields and options:

- Policy Name:** IKE1
- Exchange Mode:** Main (dropdown menu)
- IKE SA Parameters**
 - Encryption Algorithm:** 3DES (dropdown menu)
 - Authentication Algorithm:** SHA2-256 (dropdown menu)
 - Pre-Shared Key:** presharedkey
 - Diffie-Hellman (DH) Group:** Group5 (1536 bit) (dropdown menu)
 - SA-Lifetime:** 3000 Seconds (Range: 30 - 86400, Default: 3600)
 - Dead Peer Detection:** Enable
 - DPD Delay:** 15 (Range: 10 - 999, Default: 10)
 - DPD Timeout:** 45 (Range: 30 - 1000, Default: 30)
- Extended Authentication**
 - XAUTH Type:** Enable
 - Username:** User1
 - Password:** password

At the bottom of the form are three buttons: 'Save', 'Cancel', and 'Back'.

Etapa 2. No campo Nome da política, insira um nome para a política IKE.

Etapa 3. Na lista suspensa Modo de troca, escolha uma opção.

Main - (Principal) Esta opção permite que a política IKE opere de forma mais segura, mas mais lenta do que o modo agressivo. Escolha esta opção se for necessária uma conexão VPN mais segura.

Agressivo — Essa opção 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.

IKE SA Parameters	
Encryption Algorithm:	3DES ▼
Authentication Algorithm:	SHA2-256 ▼
Pre-Shared Key:	presharedkey
Diffie-Hellman (DH) Group:	Group5 (1536 bit) ▼
SA-Lifetime:	3000 Seconds (Range: 30 - 86400, Default: 3600)
Dead Peer Detection:	<input checked="" type="checkbox"/> Enable
DPD Delay:	15 (Range: 10 - 999, Default: 10)
DPD Timeout:	45 (Range: 30 - 1000, Default: 30)

Etapa 4. Na lista suspensa Algoritmo de criptografia, escolha uma opção.

DES — Data Encryption Standard (DES) é um método de criptografia antigo de 56 bits que não é um método de criptografia muito seguro, mas pode ser necessário para compatibilidade com versões anteriores.

3DES — O 3DES (Triple Data Encryption Standard) é um método de criptografia simples de 168 bits usado para aumentar o tamanho da chave porque criptografa os dados três vezes. Isso oferece mais segurança que o DES, mas menos segurança que 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 e mais seguro que o 3DES. 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 que o AES-128, e mais rápido, mas menos seguro 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 5. Na lista suspensa Algoritmo de autenticação, escolha uma opção.

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 — Secure Hash Function 1 (SHA-1) use um valor 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.

Etapa 6. No campo Pre-Shared Key (Chave pré-compartilhada), insira uma chave pré-compartilhada que a política IKE usa.

Passo 7. 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

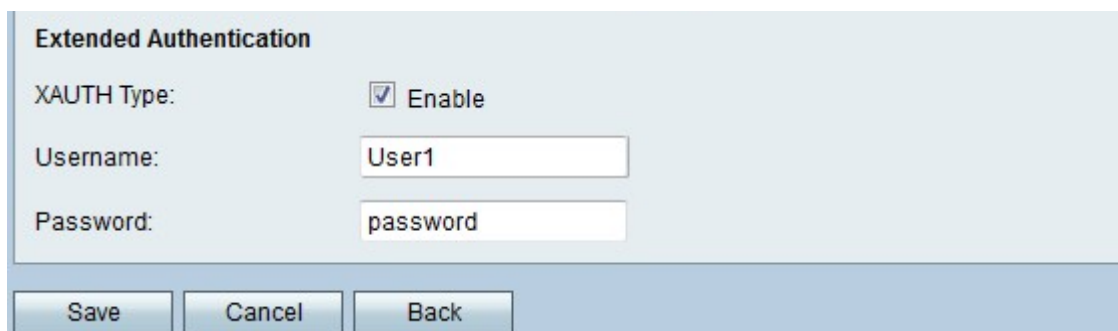
número de bits do grupo, mais seguro o grupo estará.

Etapa 8. No campo SA-Lifetime, insira por quanto tempo, em segundos, um SA para a VPN dura antes do SA ser renovado.

Etapa 9. (Opcional) Marque a caixa de seleção **Habilitar** no campo Dead Peer Detection (Detecção de ponto morto) para habilitar a Dead Peer Detection (DPD). O DPD monitora os pares IKE para ver se um peer deixou de funcionar. O DPD evita o desperdício de recursos de rede em peers inativos.

Etapa 10. (Opcional) Se você habilitou o DPD na Etapa 9, insira a frequência (em segundos) com que o peer é verificado quanto à atividade no campo DPD Delay.

Etapa 11. (Opcional) Se você habilitou o DPD na Etapa 9, insira quantos segundos aguardar antes que um peer inativo seja descartado no campo Tempo limite de DPD.



The screenshot shows a configuration window titled "Extended Authentication". It has three input fields: "XAUTH Type:" with a checked checkbox and the text "Enable"; "Username:" with a text box containing "User1"; and "Password:" with a text box containing "password". At the bottom, there are three buttons: "Save", "Cancel", and "Back".

Etapa 12. (Opcional) Marque a caixa de seleção **Habilitar** no campo Tipo de XAUTH para habilitar a Autenticação Estendida (XAUTH). O XAUTH permite que vários usuários usem uma única política de VPN em vez de uma política de VPN para cada usuário.

Etapa 13. (Opcional) Se você ativou XAUTH na Etapa 12, digite o nome de usuário a ser usado para a política no campo Nome de usuário.

Etapa 14. (Opcional) Se você ativou XAUTH na Etapa 12, digite a senha a ser usada para a diretiva no campo Senha.

Etapa 15. Click **Save**. A página *Advanced VPN Setup* original é exibida novamente.

Configurações de política de VPN

Este procedimento explica como configurar uma política de VPN para a conexão VPN a ser usada. Para que uma VPN funcione corretamente, as políticas de VPN para ambos os terminais devem ser idênticas.

Etapa 1. Na Tabela de Políticas de VPN, clique em **Adicionar Linha** para criar uma nova política de VPN. Para editar uma política de VPN, marque a caixa de seleção da diretiva e clique em **Editar**. A página *Advanced VPN Setup* é alterada:

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint:

(Hint: 1.2.3.4 or abc.com)

Local Traffic Selection

Local IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Remote Traffic Selection

Remote IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

Auto Policy Parameters

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

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: Enable

Select IKE Policy:

Etapa 2. No campo Nome da política, insira um nome para a política de VPN.

Etapa 3. Na lista suspensa Tipo de política, escolha uma opção.

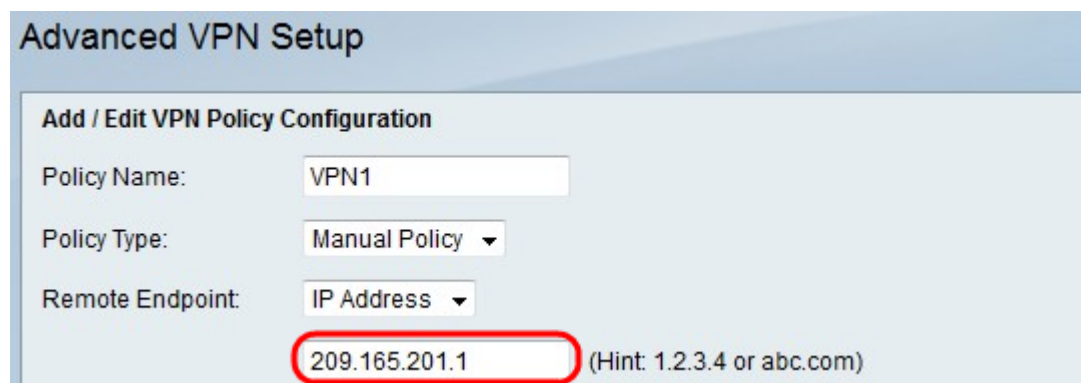
Política manual — Essa opção permite configurar as chaves para criptografia e integridade de dados.

Política automática — Esta opção usa uma política IKE para trocas de chaves de criptografia e integridade de dados.

Etapa 4. Na lista suspensa Ponto de extremidade remoto, escolha uma opção.

Endereço IP — Essa opção identifica a rede remota por um endereço IP público.

FQDN — Essa opção usa um Nome de domínio totalmente qualificado (FQDN) para identificar a rede remota.



Advanced VPN Setup

Add / Edit VPN Policy Configuration

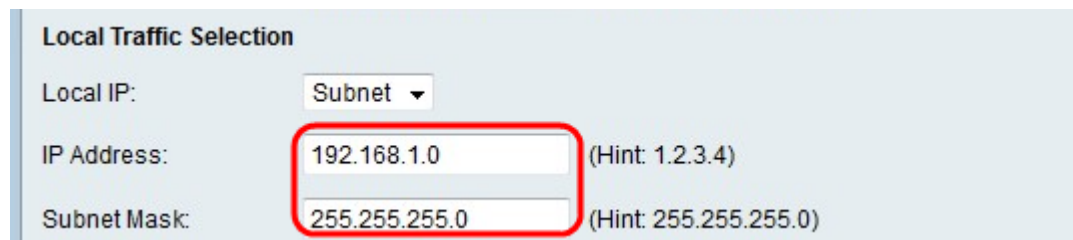
Policy Name:

Policy Type:

Remote Endpoint:

(Hint: 1.2.3.4 or abc.com)

Etapa 5. No campo de entrada de texto abaixo da lista suspensa Ponto de extremidade remoto, insira o endereço IP público ou o nome de domínio do endereço remoto.



Local Traffic Selection

Local IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Etapa 6. Na lista suspensa IP local, escolha uma opção.

Single - Esta opção usa um único host como ponto de conexão VPN local.

Sub-rede — Esta opção usa uma sub-rede da rede local como ponto de conexão VPN local.

Passo 7. No campo Endereço IP, insira o endereço IP do host ou da sub-rede da sub-rede ou do host local.

Etapa 8. (Opcional) Se você escolher a sub-rede na Etapa 6, insira a máscara de sub-rede para a sub-rede local no campo Máscara de sub-rede.

Etapa 9. Na lista suspensa IP remoto, escolha uma opção.

Single - Esta opção usa um único host como ponto de conexão VPN remota.

Sub-rede — Esta opção usa uma sub-rede da rede remota como ponto de conexão VPN

remota.

The screenshot shows a configuration form titled "Remote Traffic Selection". It contains three input fields: "Remote IP:" with a dropdown menu set to "Subnet"; "IP Address:" with the value "192.168.2.0" and a hint "(Hint: 1.2.3.4)"; and "Subnet Mask:" with the value "255.255.255.0" and a hint "(Hint: 255.255.255.0)". A red rectangle highlights the IP Address and Subnet Mask fields.

Etapa 10. No campo Endereço IP, insira o endereço IP do host ou da sub-rede da sub-rede ou do host remoto.

Etapa 11. (Opcional) Se você escolher a sub-rede na Etapa 9, insira a máscara de sub-rede para a sub-rede remota no campo Máscara de sub-rede.

Note: Se você escolher a Política manual na etapa 3, execute as etapas de 12 a 19; caso contrário, pule a Etapa 20.

The screenshot shows a configuration form titled "Manual Policy Parameters". It contains several input fields: "SPI-Incoming:" with the value "0xABCD"; "SPI-Outgoing:" with the value "0x1234"; "Encryption Algorithm:" with a dropdown menu set to "AES-256"; "Key-In:" with the value "123456789012345678!"; "Key-Out:" with the value "123456789012345678!"; "Integrity Algorithm:" with a dropdown menu set to "SHA2-256"; "Key-In:" with the value "123456789012345678!"; and "Key-Out:" with the value "123456789012345678!". A red rectangle highlights the SPI-Incoming and SPI-Outgoing fields.

Etapa 12. No campo SPI-Incoming, insira de três a oito caracteres hexadecimais para a tag Security Parameter Index (SPI) para o tráfego de entrada na conexão VPN. A marca SPI é usada para distinguir o tráfego de uma sessão do tráfego de outras sessões.

Etapa 13. No campo SPI-Saída, insira de três a oito caracteres hexadecimais para tag SPI para tráfego de saída na conexão VPN.

Etapa 14. Na lista suspensa Algoritmo de criptografia, escolha uma opção.

DES — Data Encryption Standard (DES) é um método de criptografia antigo de 56 bits que não é um método de criptografia muito seguro, mas pode ser necessário para compatibilidade com versões anteriores.

3DES — O 3DES (Triple Data Encryption Standard) é um método de criptografia simples de 168 bits usado para aumentar o tamanho da chave porque criptografa os dados três vezes. Isso oferece mais segurança que o DES, mas menos segurança que 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 e mais seguro que o 3DES. 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 que o AES-128, e mais rápido, mas menos seguro 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.

The image shows a configuration window titled "Manual Policy Parameters". It contains several input fields and dropdown menus. The "Key-In" field for the encryption algorithm is highlighted with a red rectangular box. The values in the fields are as follows:

Field	Value
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!

Etapa 15. No campo Key-In, insira uma chave para a política de entrada. O comprimento da chave depende do algoritmo escolhido na Etapa 14.

- O DES usa uma chave de 8 caracteres.
- O 3DES usa uma chave de 24 caracteres.
- O AES-128 usa uma chave de 12 caracteres.
- O AES-192 usa uma chave de 24 caracteres.
- O AES-256 usa uma chave de 32 caracteres.

Etapa 16. No campo Key-Out, insira uma chave para a política de saída. O comprimento da chave depende do algoritmo escolhido na Etapa 14. Os comprimentos principais são os mesmos da Etapa 15.

Etapa 17. Na lista suspensa Algoritmo de integridade, escolha uma opção.

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

SHA-1 — Secure Hash Function 1 (SHA-1) use um valor de hash de 160 bits para a integridade dos dados. 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 a integridade dos dados. SHA2-256 é mais lento, mas seguro que MD5 e SHA-1.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

Etapa 18. No campo Key-In, insira uma chave para a política de entrada. O comprimento da chave depende do algoritmo escolhido na Etapa 17.

MD5 usa uma chave de 16 caracteres.

SHA-1 usa uma chave de 20 caracteres.

SHA2-256 usa uma chave de 32 caracteres.

Etapa 19. No campo Key-Out, insira uma chave para a política de saída. O comprimento da chave depende do algoritmo escolhido na Etapa 17. Os comprimentos principais são os mesmos da Etapa 18.

Note: Se você escolheu Auto Policy na Etapa 3, execute as Etapas 20 a 25; Caso contrário, vá para o passo 26.

Auto Policy Parameters

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

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: Enable

Select IKE Policy:

Etapa 20. No campo SA-Lifetime, insira por quanto tempo, em segundos, o SA dura antes da renovação.

Etapa 21. Na lista suspensa Algoritmo de criptografia, escolha uma opção.

DES — Data Encryption Standard (DES) é um método de criptografia antigo de 56 bits que não é um método de criptografia muito seguro, mas pode ser necessário para compatibilidade com versões anteriores.

3DES — O 3DES (Triple Data Encryption Standard) é um método de criptografia simples

de 168 bits usado para aumentar o tamanho da chave porque criptografa os dados três vezes. Isso oferece mais segurança que o DES, mas menos segurança que 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 e mais seguro que o 3DES. 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 que o AES-128, e mais rápido, mas menos seguro 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 22. Na lista suspensa Algoritmo de integridade, escolha uma opção.

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

SHA-1 — Secure Hash Function 1 (SHA-1) use um valor de hash de 160 bits para a integridade dos dados. 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 a integridade dos dados. SHA2-256 é mais lento, mas seguro que MD5 e SHA-1.

Etapa 23. Marque a caixa de seleção **Enable** no PFS Key Group (Grupo de chaves PFS) para ativar o Perfect Forward Secrecy (PFS). O PFS aumenta a segurança da VPN, mas retarda a velocidade da conexão.

Etapa 24. (Opcional) Se você optou por ativar o PFS na Etapa 23, escolha um grupo Diffie-Hellman (DH) para participar da lista suspensa abaixo. Quanto maior o número do grupo, mais seguro o grupo estará.

Etapa 25. Na lista suspensa Selecionar política IKE, escolha qual política IKE usar para a política VPN.

Note: Se você clicar em **View**, será direcionado para a seção de configuração IKE da página *Advanced VPN Setup*.

Etapa 26. Click **Save**. A página *Advanced VPN Setup* original é exibida novamente.

Etapa 27. Click **Save**.