

Configurar Rede Virtual Privada (VPN) avançada em um roteador RV130 ou RV130W

Objetivo

Uma Rede Virtual Privada (VPN) 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. Uma VPN site a site (gateway a gateway) conecta redes inteiras entre si, mantendo a segurança criando um túnel sobre um domínio público conhecido como Internet. Cada site precisa apenas de uma conexão local com a mesma rede pública, economizando, assim, dinheiro em longas linhas privadas –.

As VPNs são benéficas para as empresas de tal forma que são altamente escaláveis, simplificam a topologia de rede e melhoram a produtividade reduzindo o tempo de viagem e o custo para usuários remotos.

O Internet Key Exchange (IKE) é um protocolo usado para estabelecer uma conexão segura para comunicação em uma VPN. Essa conexão segura é chamada de Associação de Segurança (SA). Você pode criar políticas IKE para definir os parâmetros de segurança a serem usados nesse processo, como autenticação do peer, algoritmos de criptografia etc. Para que uma VPN funcione corretamente, as políticas de IKE para ambos os pontos finais devem ser idênticas.

Este artigo tem como objetivo mostrar como configurar a Configuração de VPN Avançada em um roteador RV130 ou RV130W, que cobre as configurações de Política IKE e de Política VPN.

Dispositivos aplicáveis

RV130
RV130W

Versão de software

•1.0.3.22

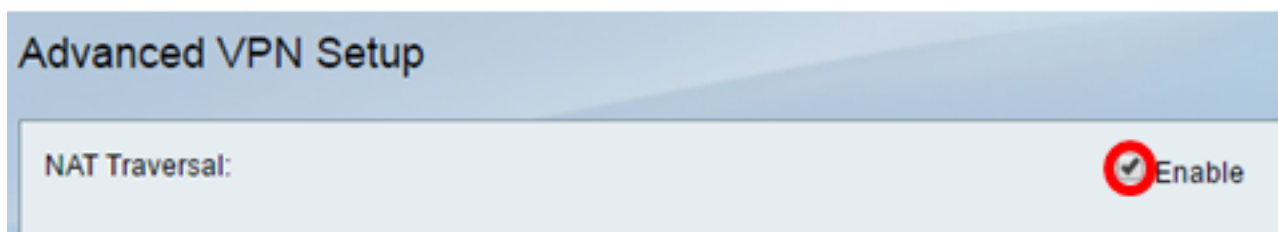
Configurar VPN avançada

Adicionar/Editar Configurações de Política de Internet Key Exchange (IKE)

Etapa 1. Inicie a sessão no utilitário baseado na Web e selecione **VPN > Site-to-Site IPSec VPN >Advanced VPN Setup**.

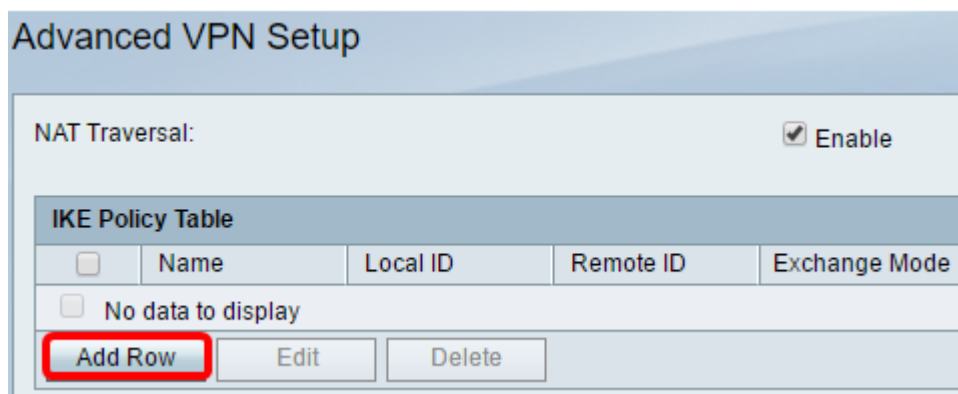


Etapa 2. (Opcional) Marque a caixa de seleção **Enable** em NAT Traversal se desejar habilitar o NAT Traversal para a conexão VPN. O NAT Traversal permite que uma conexão VPN seja feita entre gateways que usam o NAT. Escolha esta opção se sua conexão VPN passar por um gateway habilitado para NAT.



Etapa 3. Na Tabela de Políticas IKE, clique em **Adicionar Linha** para criar uma nova política IKE.

Note: Se as configurações básicas tiverem sido definidas, a tabela abaixo conterá a configuração básica de VPN criada. Você pode editar uma política IKE existente marcando a caixa de seleção da política e clicando em **Editar**. A página Advanced VPN Setup muda:



Etapa 4. No campo *Nome IKE*, digite um nome exclusivo para a política IKE.

Note: Se as configurações básicas tiverem sido definidas, o nome de conexão criado será definido como o Nome IKE. Neste exemplo, VPN1 é o nome IKE escolhido.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

Local

Local Identifier Type:

Local Identifier:

Remote

Remote Identifier Type:

Remote Identifier:

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Authentication Method:

Pre-Shared Key:

DH Group:

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

Dead Peer Detection: Enable

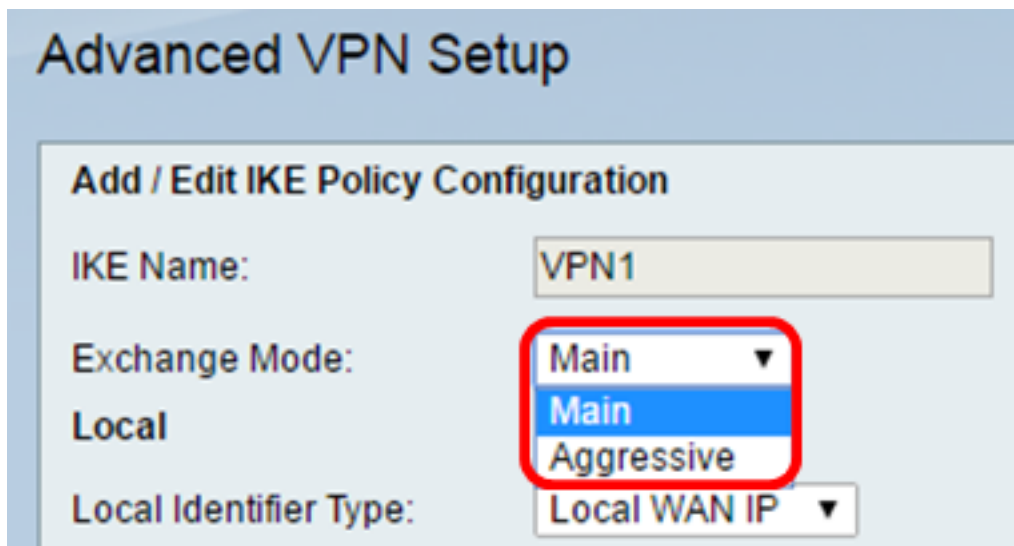
DPD Delay: (Range: 10 - 999, Default: 10)

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

Etapa 5. Na lista suspensa Exchange Mode, escolha uma opção.

- Main — Esta opção permite que a política IKE negocie o túnel VPN com segurança mais alta do que o modo agressivo. Clique nessa opção se uma conexão VPN mais segura for uma prioridade sobre uma velocidade de negociação.
- Agressiva — Esta opção permite que a política IKE estabeleça uma conexão mais rápida, porém menos segura do que o modo principal. Clique nesta opção se uma conexão VPN mais rápida for uma prioridade sobre uma segurança alta.

Note: Neste exemplo, Principal é escolhido.



Etapa 6. Escolha na lista suspensa Tipo de identificador local para identificar ou especificar o Internet Security Association and Key Management Protocol (ISAKMP) do seu roteador local. As opções são:

- IP da WAN local — O roteador usa o IP da rede de longa distância (WAN) local como o identificador principal. Essa opção se conecta pela Internet. A escolha dessa opção acinzentada o campo *Local Identifier* abaixo.
- Endereço IP — Clicar nesse botão permite inserir um endereço IP no campo *Identificador local*.
- FQDN — Um FQDN (Fully Qualified Domain Name, Nome de domínio totalmente qualificado) ou seu nome de domínio, como <http://www.example.com>, permite que você insira seu nome de domínio ou endereço IP no campo *Identificador local*.
- User-FQDN — Essa opção é um endereço de e-mail de usuário, como user@email.com. Insira um nome de domínio ou um endereço IP no campo *Local Identifier*.
- DN DER ASN1 — Esta opção é um tipo de identificador para o DN (Distinguished Name - Nome Distinto) que usa a DER ASN1 (Distinguished Encoding Rules Abstract Syntax Notation One - Notação de Sintaxe Abstrata das Regras de Codificação Distintas Um) para transmitir informações. Isso acontece quando o túnel VPN é associado a um certificado de usuário. Se essa opção for escolhida, insira um nome de domínio ou um endereço IP no campo *Local Identifier*.

Note: Neste exemplo, o IP da WAN local é escolhido.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

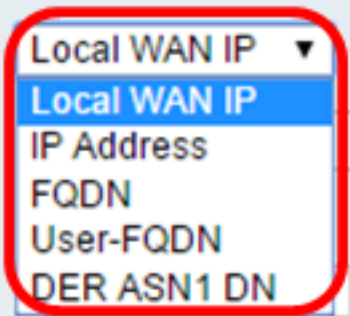
Local

Local Identifier Type:

Local Identifier:

Remote

Remote Identifier Type:



Etapa 7. Escolha na lista suspensa Remote Identifier Type para identificar ou especificar o Internet Security Association and Key Management Protocol (ISAKMP) de seu roteador remoto. As opções são Remote WAN IP, IP Address, FQDN, User FQDN e DER ASN1 DN.

Note: Neste exemplo, o IP da WAN remota é escolhido.

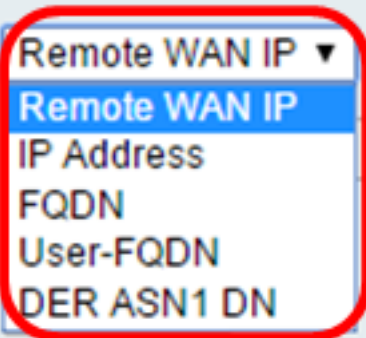
Remote

Remote Identifier Type:

Remote Identifier:

IKE SA Parameters

Encryption Algorithm:

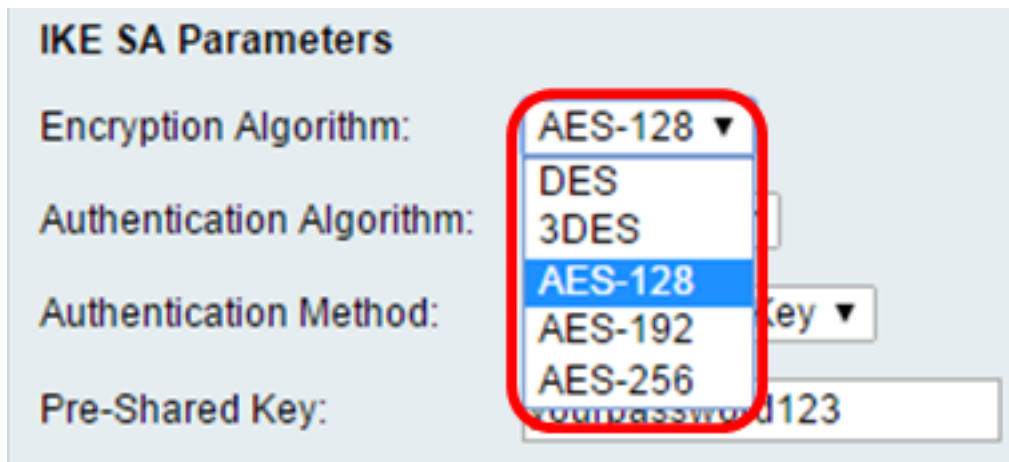


Etapa 8. Escolha uma opção na lista suspensa Algoritmo de criptografia.

- DES — O 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 fornece 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. AES-128 é o algoritmo de criptografia padrão e é mais rápido, mas menos seguro que AES-192 e 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. AES-256 é mais lento, mas mais seguro que AES-128 e AES-192.

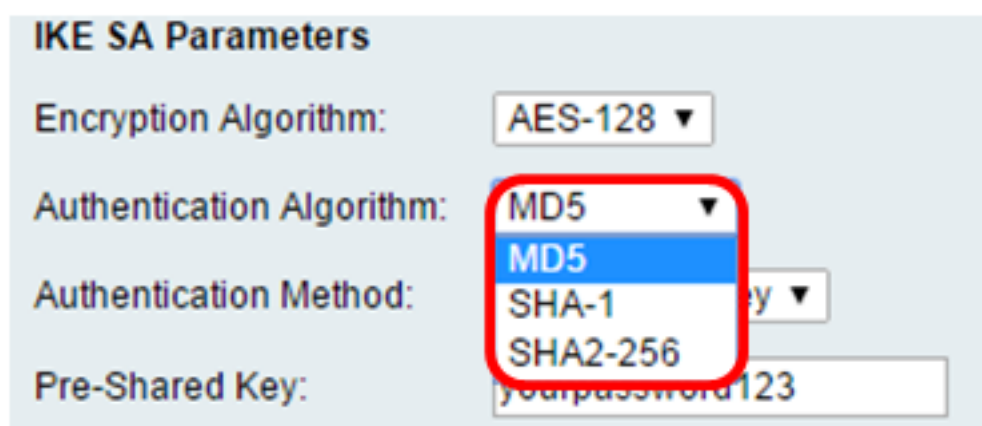
Note: Neste exemplo, AES-128 é selecionado.



Etapa 9. Na lista drop-down Algoritmo de Autenticação, escolha entre as seguintes opções:

- MD5 — O Message Digest 5 (MD5) é um algoritmo de autenticação que usa um valor de hash de 128 bits para 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. SHA-1 é mais lento, mas mais seguro que MD5. SHA-1 é o algoritmo de autenticação padrão e é mais rápido, mas menos seguro que SHA2-256.
- SHA2-256 — Algoritmo de hash seguro 2 com um valor de hash de 256 bits (SHA2-256) usa um valor de hash de 256 bits para autenticação. SHA2-256 é mais lento, mas mais seguro que MD5 e SHA-1.

Note: Neste exemplo, MD5 é escolhido.



Etapa 10. Na lista drop-down Método de Autenticação, escolha entre as seguintes opções:

- Pre-Shared Key — Esta opção exige uma senha compartilhada com o peer IKE.
- Assinatura RSA — Esta opção usa certificados para autenticar a conexão. Se essa opção for selecionada, o campo Chave pré-compartilhada será desativado. Vá para a [Etapa 12](#).

Note: Neste exemplo, a chave pré-compartilhada é escolhida.

IKE SA Parameters

Encryption Algorithm: AES-128 ▼

Authentication Algorithm: MD5 ▼

Authentication Method: Pre-Shared Key ▼

Pre-Shared Key:

DH Group: Group2 (1024 bit) ▼

Etapa 11. No campo *Pre-Shared Key*, digite uma senha com 8 a 49 caracteres.

Note: Neste exemplo, sua senha123 é usada.

IKE SA Parameters

Encryption Algorithm: AES-128 ▼

Authentication Algorithm: MD5 ▼

Authentication Method: Pre-Shared Key ▼

Pre-Shared Key:

[Etapa 12.](#) Na lista suspensa Grupo DH, escolha qual algoritmo de grupo Diffie-Hellman (DH) o IKE usará. Hosts em um grupo DH podem trocar chaves sem o conhecimento um do outro. Quanto maior o número de bits do grupo, melhor a segurança.

Note: Neste exemplo, Group1 é escolhido.

DH Group: Group1 (768 bit) ▼

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

Dead Peer Detection: Enable

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

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

Save Cancel Back

Etapa 13. No campo *SA-Lifetime*, insira quanto tempo em segundos dura uma SA para a VPN antes que a SA seja renovada. O intervalo é de 30 a 86400 segundos. O padrão é

28800.

DH Group: Group1 (768 bit) ▾
SA-Lifetime: 28800 Seconds (Range: 30 - 86400, Default: 28800)
Dead Peer Detection: Enable
DPD Delay: 10 (Range: 10 - 999, Default: 10)
DPD Timeout: 30 (Range: 30 - 1000, Default: 30)

Save Cancel Back

[Etapa 14](#). (Opcional) Marque a caixa de seleção **Enable** Dead Peer Detection para ativar a Dead Peer Detection (DPD). O DPD monitora os peers IKE para ver se um peer parou de funcionar ou ainda está ativo. Se o peer for detectado como inativo, o dispositivo excluirá a associação de segurança IPsec e IKE. O DPD evita o desperdício de recursos de rede em pares inativos.

Note: Se não quiser ativar a detecção de ponto morto, vá para a [Etapa 17](#).

Dead Peer Detection: Enable
DPD Delay: 10 (Range: 10 - 999, Default: 10)
DPD Timeout: 30 (Range: 30 - 1000, Default: 30)

Save Cancel Back

Etapa 15. (Opcional) Se você habilitou o DPD na [Etapa 14](#), insira a frequência (em segundos) com que o peer é verificado para a atividade no campo *Atraso do DPD*.

Note: O atraso de DPD é o intervalo em segundos entre mensagens R-U-THERE de DPD consecutivas. As mensagens DPD R-U-THERE são enviadas somente quando o tráfego IPsec está ocioso. O valor padrão é 10.

Dead Peer Detection: Enable
DPD Delay: 10 (Range: 10 - 999, Default: 10)
DPD Timeout: 30 (Range: 30 - 1000, Default: 30)

Save Cancel Back

Etapa 16. (Opcional) Se você habilitou o DPD na [Etapa 14](#), insira quantos segundos aguardar antes que um peer inativo seja descartado no campo *Timeout de DPD*.

Note: Esse é o tempo máximo que o dispositivo deve aguardar para receber uma resposta à mensagem DPD antes de considerar que o peer está inoperante. O valor padrão é 30.

Dead Peer Detection:	<input checked="" type="checkbox"/> Enable
DPD Delay:	<input type="text" value="10"/> (Range: 10 - 999, Default: 10)
DPD Timeout:	<input type="text" value="30"/> (Range: 30 - 1000, Default: 30)

[Etapa 17.](#) Clique em **Salvar**.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

Local

Local Identifier Type:

Local Identifier:

Remote

Remote Identifier Type:

Remote Identifier:

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Authentication Method:

Pre-Shared Key:

DH Group:

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

Dead Peer Detection: Enable

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

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

Note: A página principal Advanced VPN Setup (Configuração avançada de VPN) é exibida novamente.

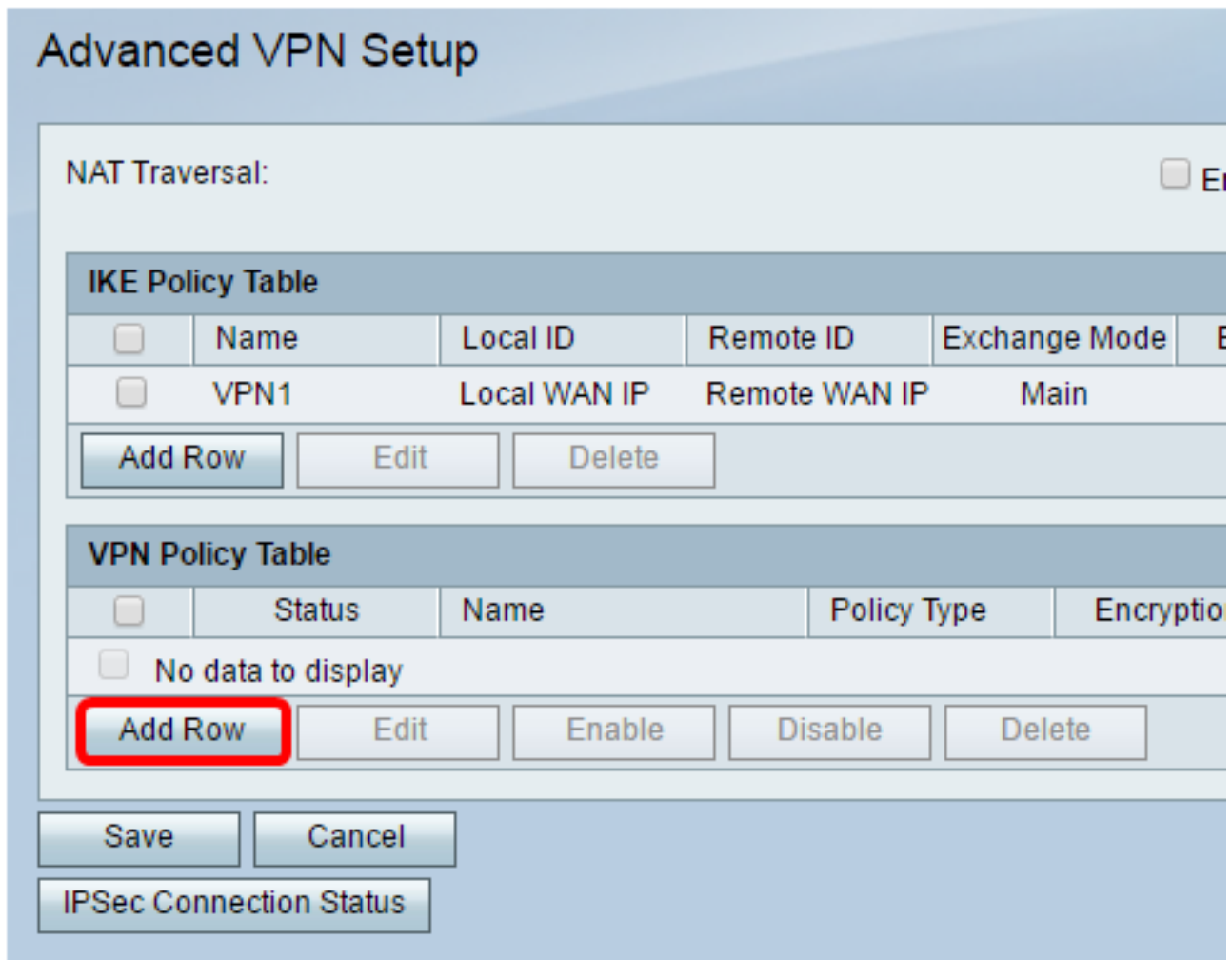
Agora você deve ter configurado com êxito as configurações de política IKE no roteador.

Definir Configurações de Política VPN

Nota: Para que uma VPN funcione corretamente, as políticas de VPN para ambos os pontos finais devem ser idênticas.

Etapa 1. Na Tabela de Políticas de VPN, clique em **Add Row** para criar uma nova política de VPN.

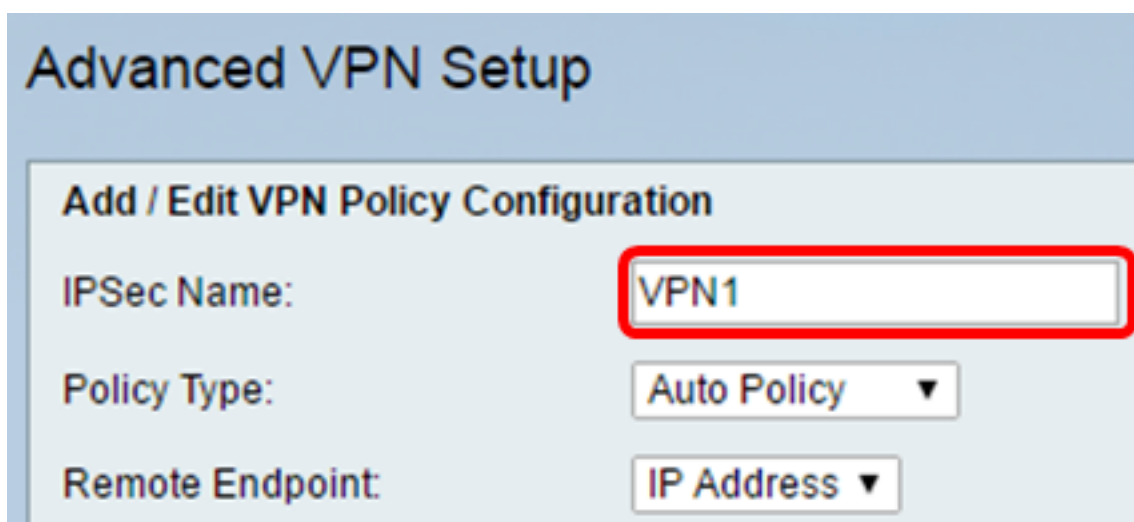
Note: Você também pode editar uma política de VPN marcando a caixa de seleção da política e clicando em **Edit**. A página Advanced VPN Setup é exibida:



The screenshot shows the 'Advanced VPN Setup' interface. At the top, there is a 'NAT Traversal' section with a checkbox. Below it is the 'IKE Policy Table' with columns for Name, Local ID, Remote ID, and Exchange Mode. A row for 'VPN1' is shown with 'Local WAN IP' and 'Remote WAN IP' as sub-headers, and 'Main' as a value. Below the table are 'Add Row', 'Edit', and 'Delete' buttons. The 'VPN Policy Table' section below has columns for Status, Name, Policy Type, and Encryption. It shows 'No data to display' and has 'Add Row', 'Edit', 'Enable', 'Disable', and 'Delete' buttons. The 'Add Row' button is highlighted with a red box. At the bottom are 'Save', 'Cancel', and 'IPSec Connection Status' buttons.

Etapa 2. No campo *IPSec Name* na área Add/Edit VPN Configuration, digite um nome para a política de VPN.

Note: Neste exemplo, o VPN1 é usado.

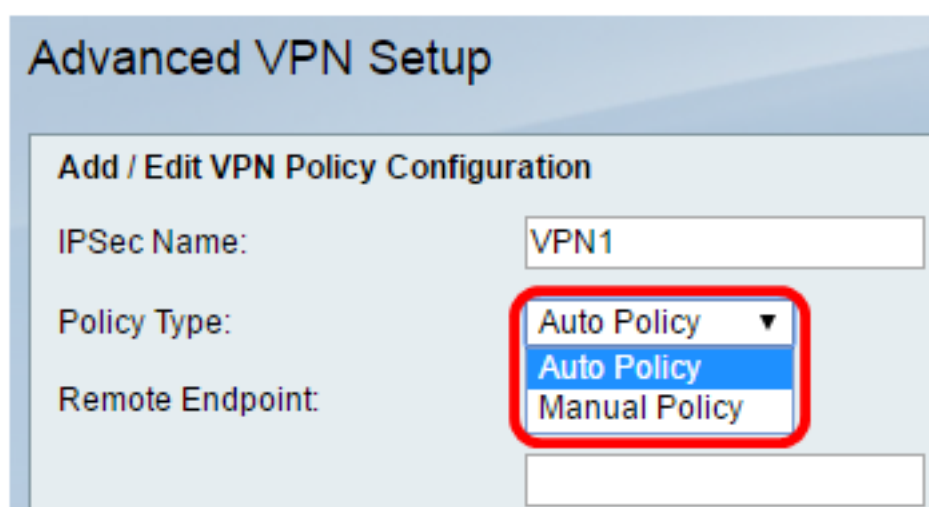


The screenshot shows the 'Advanced VPN Setup' interface, specifically the 'Add / Edit VPN Policy Configuration' section. It has three fields: 'IPSec Name' with a text input field containing 'VPN1' (highlighted with a red box), 'Policy Type' with a dropdown menu set to 'Auto Policy', and 'Remote Endpoint' with a dropdown menu set to 'IP Address'.

[Etapa 3.](#) Na lista suspensa Policy Type, selecione uma opção.

- Manual Policy (Política manual) — Esta opção permite configurar manualmente as chaves para criptografia e integridade de dados para o túnel VPN. Se essa opção for escolhida, as definições de configuração na área Parâmetros de política manual serão ativadas. Continue as etapas até a Seleção de tráfego remoto. Clique [aqui](#) para conhecer as etapas.
- Política automática — Os parâmetros da política são definidos automaticamente. Essa opção usa uma política IKE para a integridade de dados e para as trocas de chaves de criptografia. Se isso for escolhido, as definições de configuração na área Parâmetros de política automática serão ativadas. Clique [aqui](#) para conhecer as etapas. Certifique-se de que o protocolo IKE negocia automaticamente entre os dois pontos finais VPN.

Note: Neste exemplo, a Política automática é escolhida.

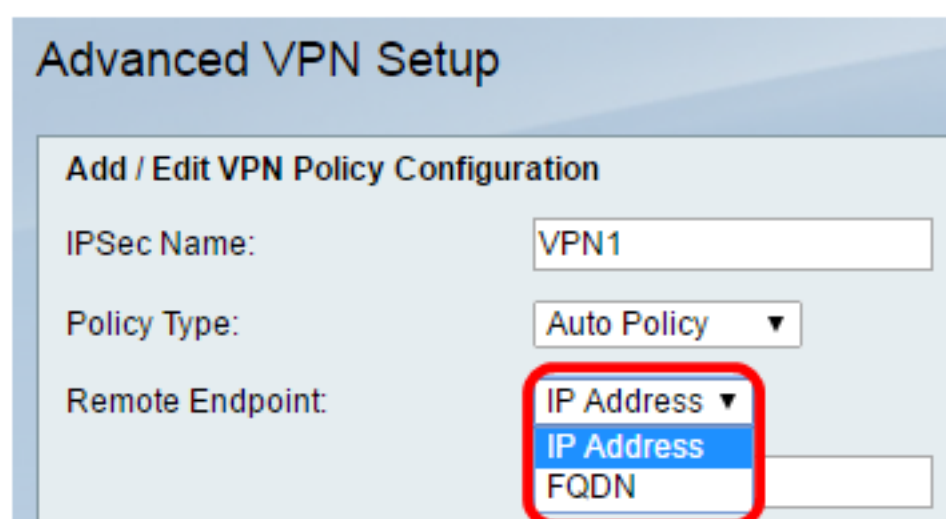


The screenshot shows the 'Advanced VPN Setup' window with the 'Add / Edit VPN Policy Configuration' section. The 'IPSec Name' field contains 'VPN1'. The 'Policy Type' dropdown menu is open, showing three options: 'Auto Policy' (highlighted in blue), 'Auto Policy', and 'Manual Policy'. A red box highlights the dropdown menu.

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

- Endereço IP — Essa opção identifica a rede remota por um endereço IP público.
- FQDN — Nome de domínio completo para um computador, host ou a Internet específicos. O FQDN consiste em duas partes: o nome do host e o nome do domínio. Essa opção só pode ser habilitada quando **Auto Policy** está selecionado na [Etapa 3](#).

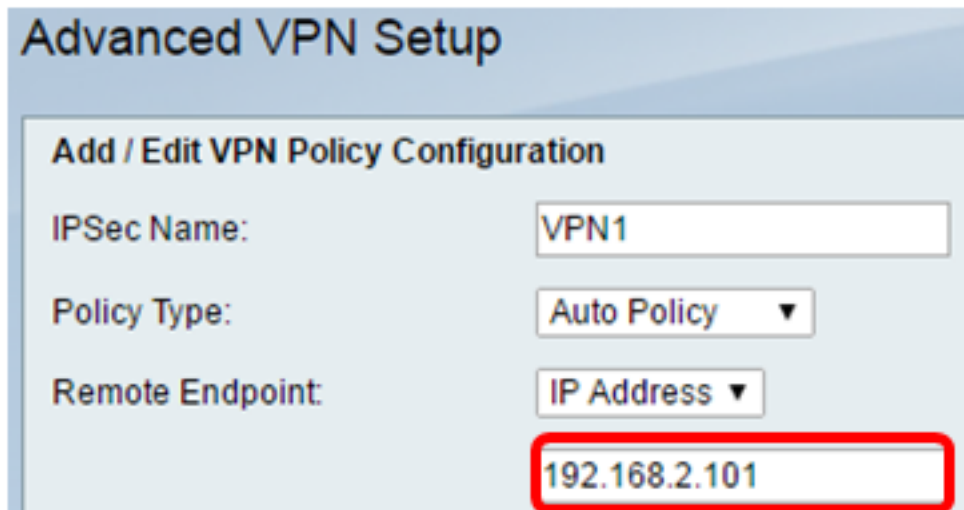
Note: Para este exemplo, o endereço IP é escolhido.



The screenshot shows the 'Advanced VPN Setup' window with the 'Add / Edit VPN Policy Configuration' section. The 'IPSec Name' field contains 'VPN1'. The 'Policy Type' dropdown menu is set to 'Auto Policy'. The 'Remote Endpoint' dropdown menu is open, showing three options: 'IP Address' (highlighted in blue), 'IP Address', and 'FQDN'. A red box highlights the dropdown menu.

Etapa 5. No campo *Ponto final remoto*, insira o endereço IP público ou o nome de domínio do endereço remoto.

Note: Neste exemplo, 192.168.2.101 é usado.



Advanced VPN Setup

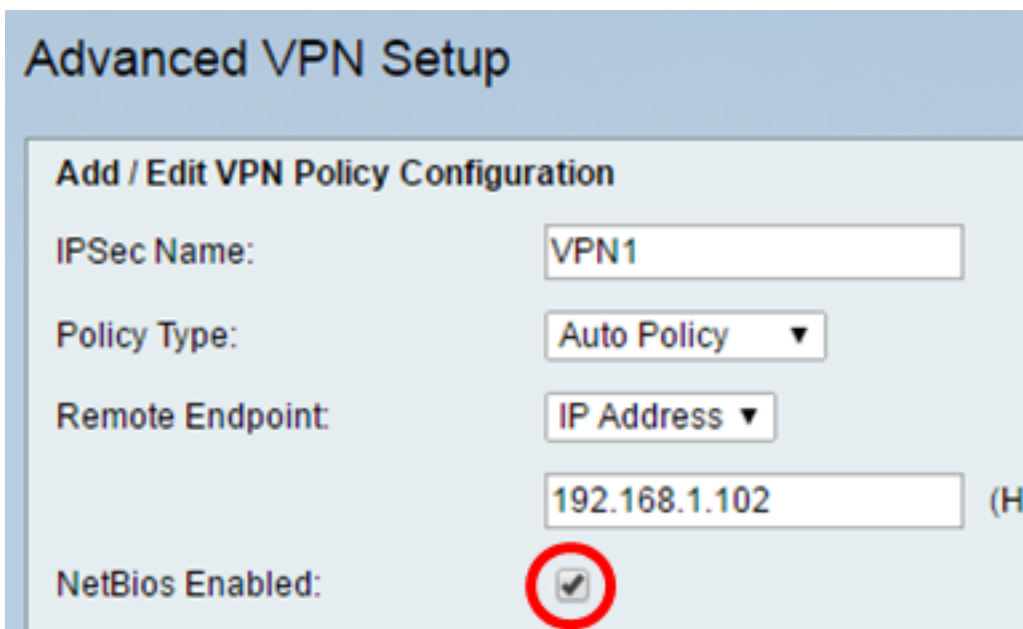
Add / Edit VPN Policy Configuration

IPsec Name:

Policy Type:

Remote Endpoint:

Etapa 6. (Opcional) Marque a caixa de seleção **NetBios Habilitado** se quiser habilitar o envio de broadcasts do Network Basic Input/Output System (NetBIOS) através da conexão VPN. O NetBIOS permite que os hosts se comuniquem entre si em uma rede local (LAN).



Advanced VPN Setup

Add / Edit VPN Policy Configuration

IPsec Name:

Policy Type:

Remote Endpoint:

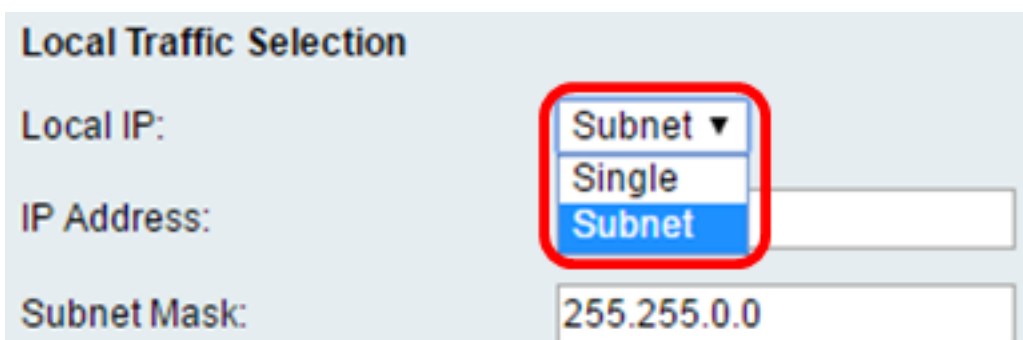
(Hi

NetBios Enabled:

[Etapa 7.](#) Na lista suspensa Local IP, na área Local Traffic Selection, escolha uma opção.

- Single — Limita a política a um host.
- Sub-rede — Permite que os hosts em um intervalo de endereços IP se conectem à VPN.

Note: Neste exemplo, Sub-rede é escolhida.



Local Traffic Selection

Local IP:

IP Address:

Subnet Mask:

Etapa 8. No campo Endereço IP, insira o endereço IP do host ou da sub-rede da sub-rede local ou do host.

Note: Neste exemplo, é usado o endereço IP da sub-rede local 10.10.10.1.



Local Traffic Selection

Local IP: Subnet ▼

IP Address: 10.10.10.1

Subnet Mask: 255.255.0.0

Etapa 9. (Opcional) Se a Sub-rede for selecionada na [Etapa 7](#), insira a máscara de sub-rede do cliente no campo *Máscara de sub-rede*. O campo Subnet Mask (Máscara de sub-rede) será desativado se Single (Único) for escolhido na Etapa 1.

Note: Neste exemplo, a máscara de sub-rede de 255.255.0.0 é usada.



Local Traffic Selection

Local IP: Subnet ▼

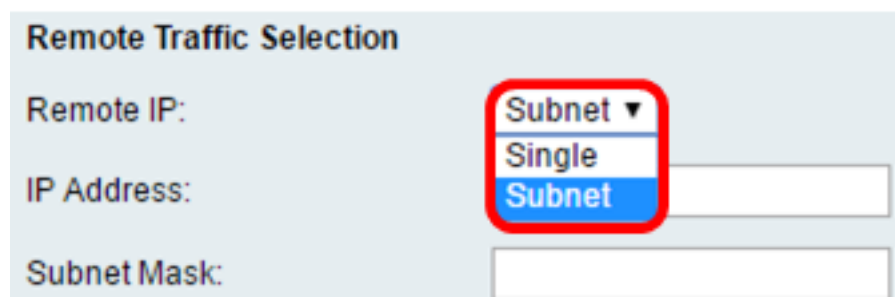
IP Address: 10.10.10.1

Subnet Mask: 255.255.0.0

[Etapa 10](#). Na lista suspensa IP remoto na área Seleção de tráfego remoto, escolha uma opção.

- Single — Limita a política a um host.
- Sub-rede — Permite que os hosts em um intervalo de endereços IP se conectem à VPN.

Note: Neste exemplo, Sub-rede é escolhida.



Remote Traffic Selection

Remote IP: Subnet ▼

IP Address: [Empty]

Subnet Mask: [Empty]

Etapa 11. Insira o intervalo de endereços IP do host que fará parte da VPN no campo *IP Address*. Se **Single** estiver selecionado na [Etapa 10](#), insira um endereço IP.

Note: No exemplo abaixo, 10.10.11.2 é usado.

Remote Traffic Selection

Remote IP: Subnet ▼

IP Address: 10.10.11.2

Subnet Mask: 255.255.0.0

Etapa 12. (Opcional) Se **Sub-rede** estiver selecionada na [Etapa 10](#), insira a máscara de sub-rede do endereço IP da sub-rede no campo [Máscara de sub-rede](#).

Note: No exemplo abaixo, 255.255.0.0 é usado.

Remote Traffic Selection

Remote IP: Subnet ▼

IP Address: 10.10.11.2 (Hint: 1.2.3.4)

Subnet Mask: 255.255.0.0 (Hint: 255.255.255.0)

[Política manual Parâmetros](#)

Observação: esses campos só poderão ser editados se a **Política manual** for escolhida.

Etapa 1. No campo *SPI-Incoming*, insira de três a oito caracteres hexadecimais para a marca 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.

Note: Para este exemplo, 0xABCD é usado.

Manual Policy Parameters

SPI-Incoming: 0xABCD

SPI-Outgoing: 0x1234

Etapa 2. No campo *SPI-Outgoing*, insira de três a oito caracteres hexadecimais para a marca SPI para o tráfego de saída na conexão VPN.

Note: Para este exemplo, 0x1234 é usado.

Manual Policy Parameters

SPI-Incoming: 0xABCD

SPI-Outgoing: 0x1234

Etapa 3. Na lista suspensa Algoritmo de criptografia manual, escolha uma opção. As opções são DES, 3DES, AES-128, AES-192 e AES-256.

Note: Neste exemplo, AES-128 é escolhido.

Manual Policy Parameters

SPI-Incoming: 0xABCD

SPI-Outgoing: 0x1234

Manual Encryption Algorithm: AES-128 ▼

Key-In: []

Key-Out: []

Manual Integrity Algorithm: []

Etapa 4. No campo *Key-In*, insira uma chave para a política de entrada. O comprimento da chave depende do algoritmo escolhido na [Etapa 3](#).

- O DES usa uma chave de 8 caracteres.
- O 3DES usa uma chave de 24 caracteres.
- AES-128 usa uma chave de 16 caracteres.
- AES-192 usa uma chave de 24 caracteres.
- AES-256 usa uma chave de 32 caracteres.

Note: Neste exemplo, 123456789ABCDEFGG é usado.

Manual Encryption Algorithm: AES-128 ▼

Key-In: 123456789ABCDEFGG

Key-Out: 123456789ABCDEFGG

Etapa 5. No campo *Key-Out*, insira uma chave para a política de saída. O comprimento da chave depende do algoritmo escolhido na [Etapa 3](#).

Note: Neste exemplo, 123456789ABCDEFGG é usado.

Manual Encryption Algorithm: AES-128 ▼
Key-In: 123456789ABCDEFGG
Key-Out: 123456789ABCDEFGG

[Etapa 6.](#) Na lista suspensa Algoritmo de integridade manual, escolha uma opção.

- 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 — Usa um valor de hash de 160 bits para a integridade dos dados. SHA-1 é mais lento, mas mais seguro que MD5, e SHA-1 é mais rápido, mas menos seguro que SHA2-256.
- SHA2-256 — Usa um valor de hash de 256 bits para a integridade dos dados. SHA2-256 é mais lento, mas seguro que MD5 e SHA-1.

Note: Neste exemplo, MD5 é escolhido.

Manual Integrity Algorithm: MD5 ▼
Key-In: CDEFG
Key-Out: 123456789ABCDEFGG

[Etapa 7.](#) No *campo Key-In*, insira uma chave para a política de entrada. O comprimento da chave depende do algoritmo escolhido na [Etapa 6](#).

- MD5 usa uma chave de 16 caracteres.
- SHA-1 usa uma chave de 20 caracteres.
- SHA2-256 usa uma chave de 32 caracteres.

Note: Neste exemplo, 123456789ABCDEFGG é usado.

Manual Integrity Algorithm: MD5 ▼
Key-In: 123456789ABCDEFGG
Key-Out: 123456789ABCDEFGG

[Etapa 8.](#) No *campo Key-Out*, insira uma chave para a política de saída. O comprimento da chave depende do algoritmo escolhido na [Etapa 6](#).

Note: Neste exemplo, 123456789ABCDEFGG é usado.

Manual Integrity Algorithm:	MD5 ▼
Key-In:	123456789ABCDEFGH
Key-Out:	123456789ABCDEFGH

[Auto Parâmetros da política](#)

Nota: Antes de criar uma política de VPN automática, certifique-se de criar a política de IKE com base na qual deseja criar a política de VPN automática. Esses campos só poderão ser editados se **Política automática** estiver selecionada na **Etapa 3**.

Etapa 1. No campo *IPSec SA-Lifetime*, insira quanto tempo, em segundos, dura a SA antes da renovação. O intervalo é de 30 a 86400. O padrão é 3600.

Auto Policy Parameters	
IPSec SA Lifetime:	3600 Seconds (Range: 30 - 86400, Default: 3600)
Encryption Algorithm:	AES-128 ▼
Integrity Algorithm:	SHA-1 ▼
PFS Key Group:	<input type="checkbox"/> Enable

Etapa 2. Na lista suspensa Algoritmo de criptografia, escolha uma opção. As opções são:

Note: Neste exemplo, AES-128 é escolhido.

- DES — 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 — Um método de criptografia simples de 168 bits usado para aumentar o tamanho da chave porque criptografa os dados três vezes. Isso fornece mais segurança que o DES, mas menos segurança que o AES.
- AES-128 — Usa uma chave de 128 bits para a 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. AES-128 é mais rápido, mas menos seguro que AES-192 e AES-256.
- 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 — Usa uma chave de 256 bits para a criptografia AES. AES-256 é mais lento, mas mais seguro que AES-128 e AES-192.
- AESGCM — Advanced Encryption Standard Galois Counter Mode é um modo genérico de codificação de bloco de criptografia autenticado. A autenticação do GCM usa operações que são particularmente adequadas para a implementação eficiente em hardware, tornando-a especialmente atraente para implementações de alta velocidade ou para implementações em um circuito compacto e eficiente.
- AESCCM — Advanced Encryption Standard Counter with CBC-MAC Mode é um modo de criptografia de bloco autenticado genérico. O CCM é adequado para uso em implementações de software compactas.

Auto Policy Parameters

IPSec SA Lifetime: 3600 Seco

Encryption Algorithm: AES-128 ▼

Integrity Algorithm: AES-128 ▼

PFS Key Group: AES-192

DH Group: AES-256 (bit) ▼

Select IKE Policy: AESGCM

View

Save Cancel Back

Etapa 3. Na lista suspensa Algoritmo de integridade, escolha uma opção. As opções são MD5, SHA-1 e SHA2-256.

Note: Neste exemplo, SHA-1 é escolhido.

Auto Policy Parameters

IPSec SA Lifetime: 3600 Seco

Encryption Algorithm: AES-128 ▼

Integrity Algorithm: SHA-1 ▼

PFS Key Group: SHA-1

DH Group: SHA2-256 (bit) ▼

Select IKE Policy: MD5

VPN1 ▼

[Etapa 4.](#) Marque a caixa de seleção **Enable** no PFS Key Group para ativar o Perfect Forward Secrecy (PFS). O PFS aumenta a segurança da VPN, mas diminui a velocidade da conexão.

Auto Policy Parameters

IPSec SA Lifetime: Seconds

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: Enable

DH Group:

Select IKE Policy:

Etapa 5. (Opcional) Se você optar por ativar o PFS na [Etapa 4](#), escolha um grupo DH para participar na lista suspensa do grupo DH. Quanto maior o número do grupo, melhor a segurança.

Note: Para este exemplo, o Grupo 1 é escolhido.

Auto Policy Parameters

IPSec SA Lifetime: Seconds

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: Enable

DH Group:

Select IKE Policy:

Etapa 6. Na lista suspensa Select IKE Policy, escolha qual política IKE usar para a política de VPN.

Note: Neste exemplo, apenas uma política IKE foi configurada, portanto apenas uma política aparece.

Auto Policy Parameters

IPSec SA Lifetime: Seconds (Ra

Encryption Algorithm: ▼

Integrity Algorithm: ▼

PFS Key Group: Enable

DH Group: ▼

Select IKE Policy: ▼

Etapa 7. Clique em **Salvar**.

Auto Policy Parameters

IPSec SA Lifetime: Seconds (R

Encryption Algorithm: ▼

Integrity Algorithm: ▼

PFS Key Group: Enable

DH Group: ▼

Select IKE Policy: ▼

Note: A página principal Advanced VPN Setup (Configuração avançada de VPN) é exibida novamente. Uma mensagem de confirmação de que as definições de configuração foram salvas com êxito deve ser exibida.

Advanced VPN Setup



Configuration settings have been saved successfully

NAT Traversal:

IKE Policy Table

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm
<input type="checkbox"/>	VPN1	Local WAN IP	Remote WAN IP	Main	AES-128

VPN Policy Table

<input type="checkbox"/>	Status	Name	Policy Type	Encryption Algorithm	Authentication Alg
<input checked="" type="checkbox"/>	Disabled	VPN1	Auto Policy	AES-128	SHA-1

Etapa 8. Na tabela VPN Policy, marque uma caixa de seleção para escolher uma VPN e clique em **Enable**.

Note: A Política de VPN configurada é desabilitada por padrão.

Advanced VPN Setup



Configuration settings have been saved successfully

NAT Traversal:

IKE Policy Table

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm
<input type="checkbox"/>	VPN1	Local WAN IP	Remote WAN IP	Main	AES-128

Add Row

Edit

Delete

VPN Policy Table

<input type="checkbox"/>	Status	Name	Policy Type	Encryption Algorithm	Authentication Alg
<input checked="" type="checkbox"/>	Disabled	VPN1	Auto Policy	AES-128	SHA-1

Add Row

Edit

Enable

Disable

Delete

Save

Cancel

IPSec Connection Status

Etapa 9. Clique em **Salvar**.

Advanced VPN Setup



Configuration settings have been saved successfully

NAT Traversal:

IKE Policy Table

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm
<input type="checkbox"/>	VPN1	Local WAN IP	Remote WAN IP	Main	AES-128

VPN Policy Table

<input type="checkbox"/>	Status	Name	Policy Type	Encryption Algorithm	Authentication Alg
<input checked="" type="checkbox"/>	Disabled	VPN1	Auto Policy	AES-128	SHA-1

Agora você deve ter configurado com êxito uma Política de VPN em seu roteador RV130 ou RV130W.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.