

# Configurar um perfil de segurança de protocolo de Internet (IPSec) em um roteador RV34x Series

## Objetivo

O IPSec (Internet Protocol Security) fornece túneis seguros entre dois pares, como dois roteadores. Os pacotes considerados sensíveis e que devem ser enviados através desses túneis seguros, bem como os parâmetros que devem ser usados para proteger esses pacotes sensíveis, devem ser definidos especificando as características desses túneis. Em seguida, quando o peer IPsec vê um pacote tão sensível, ele configura o túnel seguro apropriado e envia o pacote através desse túnel para o peer remoto.

Quando o IPsec é implementado em um firewall ou roteador, ele fornece uma segurança forte que pode ser aplicada a todo o tráfego que atravessa o perímetro. O tráfego em uma empresa ou grupo de trabalho não incorre na sobrecarga de processamento relacionado à segurança.

O objetivo deste documento é mostrar como configurar o perfil de IPSec em um roteador RV34x Series.

## Dispositivos aplicáveis

- Série RV34x

## Versão de software

- 1.0.1.16

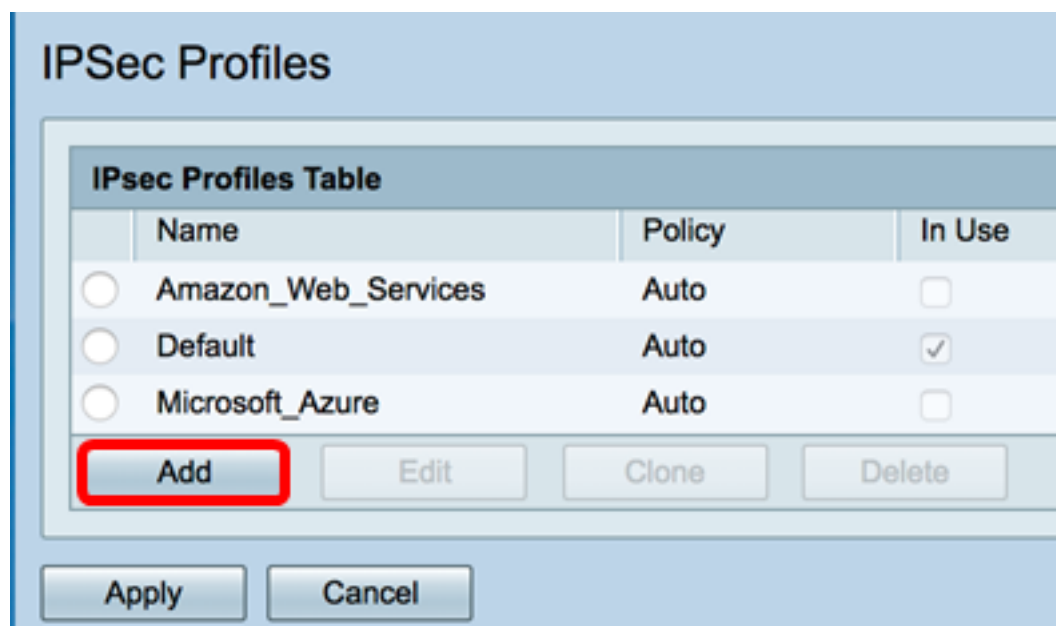
## Configurar perfil de IPSec

### Criar um perfil IPSec

Etapa 1. Faça login no utilitário baseado na Web do roteador e escolha **VPN > IPSec Profiles**.

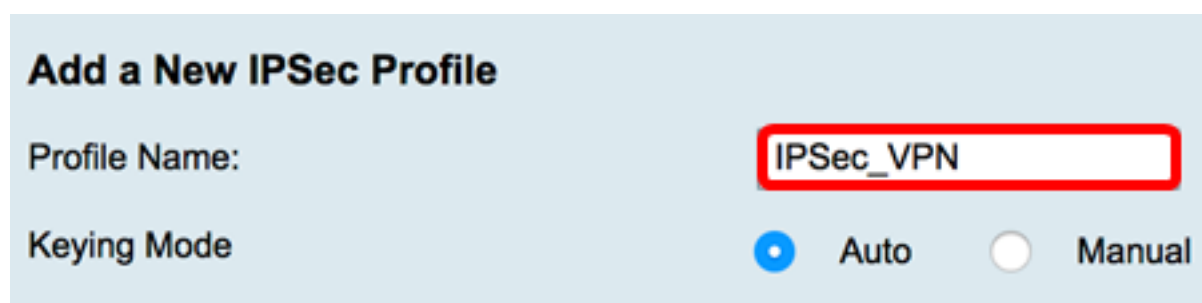


Etapa 2. A Tabela de perfis IPsec mostra os perfis existentes. Clique em **Adicionar** para criar um novo perfil.



Etapa 3. Crie um nome para o perfil no campo *Nome do perfil*. O nome do perfil deve conter apenas caracteres alfanuméricos e um sublinhado (\_) para caracteres especiais.

**Note:** Neste exemplo, IPsec\_VPN é usado como o nome do perfil IPsec.



Etapa 4. Clique em um botão de opção para determinar o método de troca de chaves que o perfil usará para autenticar. As opções são:

- Automático — Os parâmetros de política são definidos automaticamente. Esta opção usa uma política de Internet Key Exchange (IKE) para troca de chaves de criptografia e integridade de dados. Se isso for selecionado, as configurações na área Parâmetros de política automática serão ativadas. Clique [aqui](#) para definir as configurações automáticas.
- Manual — Esta opção permite que você configure manualmente as chaves para criptografia e integridade de dados para o túnel VPN (Virtual Private Network). Se isso for selecionado, as configurações na área Parâmetros de política manual serão ativadas. Clique [aqui](#) para definir as configurações manuais.

**Note:** Para este exemplo, Auto foi escolhido.

## Add a New IPsec Profile

Profile Name:

IPsec\_VPN

Keying Mode



Auto



Manual

### Configurar as configurações automáticas

Etapa 1. Na área Opções da Fase 1, escolha o grupo Diffie-Hellman (DH) apropriado a ser usado com a chave na Fase 1 na lista suspensa Grupo DH. Diffie-Hellman é um protocolo de troca de chave criptográfica que é usado na conexão para trocar conjuntos de chaves pré-compartilhadas. A força do algoritmo é determinada por bits. As opções são:

- Group2 - 1024 bits — Calcula a chave mais lentamente, mas é mais seguro que Group1.
- Group5 - 1536 bits — Calcula a chave com o menor tempo, mas é a mais segura.

**Note:** Neste exemplo, o bit Group2-1024 é escolhido.

### Phase I Options

DH Group:

✓ Group2 - 1024 bit

Group5 - 1536 bit

Encryption:

Etapa 2. Na lista suspensa Criptografia, escolha o método de criptografia apropriado para criptografar e descriptografar a carga útil de segurança de encapsulamento (ESP) e o protocolo ISAKMP (Internet Security Association and Key Management Protocol). As opções são:

- 3DES — Triple Data Encryption Standard (Padrão triplo de criptografia de dados).
- AES-128 — O Advanced Encryption Standard usa uma chave de 128 bits.
- AES-192 — O Advanced Encryption Standard usa uma chave de 192 bits.
- AES-256 — O Advanced Encryption Standard usa uma chave de 256 bits.

**Observação:** AES é o método padrão de criptografia sobre DES e 3DES por seu maior desempenho e segurança. O aumento da chave AES aumentará a segurança com um desempenho ininterrupto. Para este exemplo, AES-256 é escolhido.

### Phase I Options

DH Group:

Encryption:

3DES

AES-128

AES-192

✓ AES-256

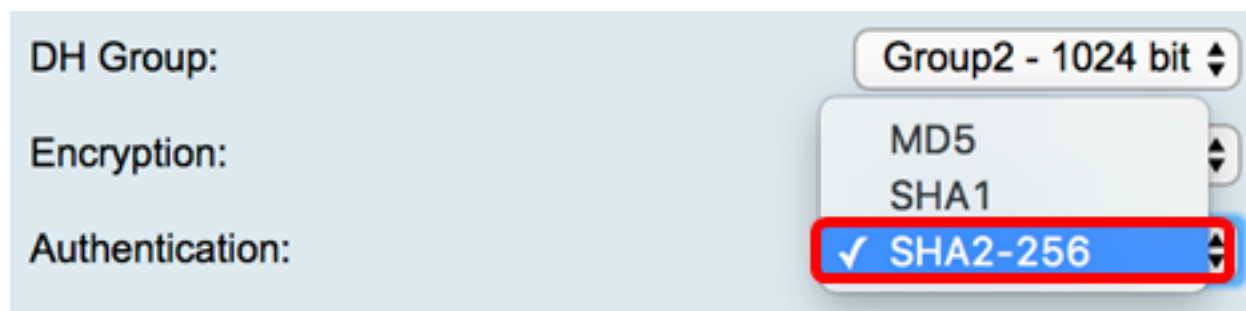
Authentication:

MD5

Etapa 3. No menu suspenso Authentication (Autenticação), escolha um método de autenticação que determinará como o ESP e o ISAKMP são autenticados. As opções são:

- MD5 — O algoritmo de resumo de mensagem tem um valor de hash de 128 bits.
- SHA-1 — O algoritmo de hash seguro tem um valor de hash de 160 bits.
- SHA2-256 — Algoritmo Hash Seguro com um valor hash de 256 bits.

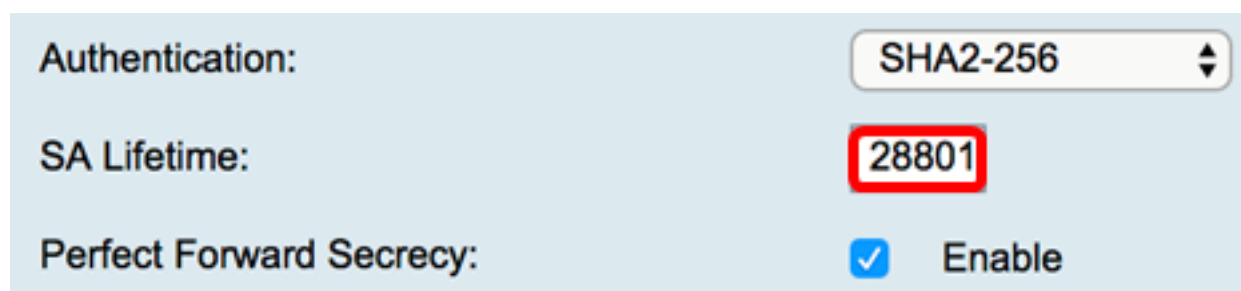
**Observação:** MD5 e SHA são funções de hash criptográfico. Eles pegam um pedaço de dados, compactam-no e criam uma saída hexadecimal exclusiva que normalmente não é reproduzível. Neste exemplo, SHA2-256 é escolhido.



A screenshot of a configuration interface showing a dropdown menu for Authentication. The menu is open, showing three options: MD5, SHA1, and SHA2-256. The SHA2-256 option is selected and highlighted with a red border. The other options are also visible in the menu. The background shows the labels 'DH Group:', 'Encryption:', and 'Authentication:'.

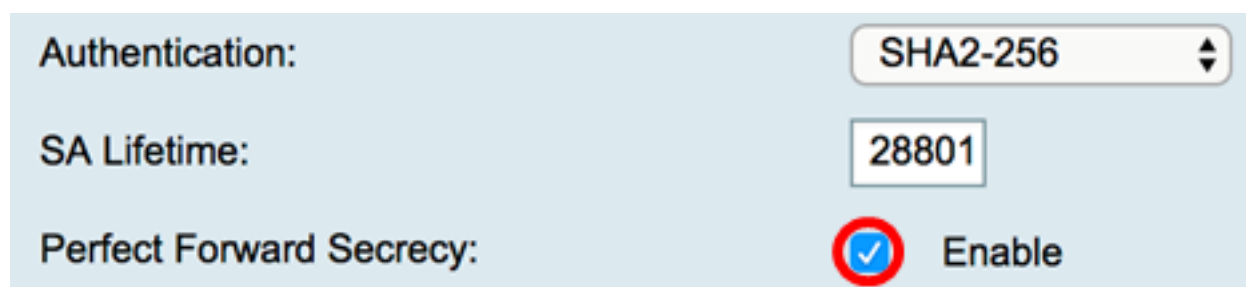
Etapa 4. No campo *Vida útil do SA*, insira um valor entre 120 e 86400. Esse é o período de tempo durante o qual a Associação de Segurança (SA) do Internet Key Exchange (IKE) permanecerá ativa nesta fase. O valor padrão é 28800.

**Note:** Neste exemplo, 28801 é usado.



A screenshot of a configuration interface showing the SA Lifetime field. The field is set to 28801, which is highlighted with a red border. The other options are SHA2-256 and Perfect Forward Secrecy: Enable.

Etapa 5. (Opcional) Marque a caixa de seleção **Habilitar segredo de encaminhamento perfeito** para gerar uma nova chave para a criptografia e autenticação de tráfego IPsec.

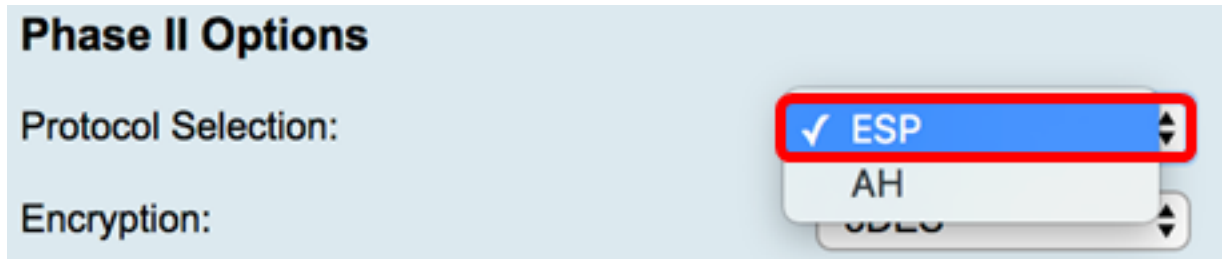


A screenshot of a configuration interface showing the Perfect Forward Secrecy checkbox. The checkbox is checked, and the text 'Enable' is visible next to it. The other options are SHA2-256 and SA Lifetime: 28801.

Etapa 6. No menu suspenso Protocol Selection (Seleção de protocolo) na área Phase II Options (Opções de fase II), escolha um tipo de protocolo para aplicar à segunda fase da negociação. As opções são:

- ESP — Se isso for escolhido, vá para a [Etapa 7](#) para escolher um método de criptografia sobre como os pacotes ESP serão criptografados e descriptografados. Um protocolo de segurança que fornece serviços de privacidade de dados, autenticação de dados opcional e serviços antirreprodução. O ESP encapsula os dados a serem protegidos.

- AH — O AH (Authentication Header, cabeçalho de autenticação) é um protocolo de segurança que fornece autenticação de dados e serviços opcionais de anti-repetição. O AH está incorporado aos dados a serem protegidos (um datagrama IP completo). Vá para a [Etapa 8](#) se esta opção for escolhida.



[Passo 7.](#) Se o ESP tiver sido escolhido na Etapa 6, escolha o método de criptografia apropriado para criptografar e descriptografar o ESP e o ISAKMP na lista suspensa Criptografia. As opções são:

- 3DES — Triple Data Encryption Standard (Padrão triplo de criptografia de dados).
- AES-128 — O Advanced Encryption Standard usa uma chave de 128 bits.
- AES-192 — O Advanced Encryption Standard usa uma chave de 192 bits.
- AES-256 — O Advanced Encryption Standard usa uma chave de 256 bits.

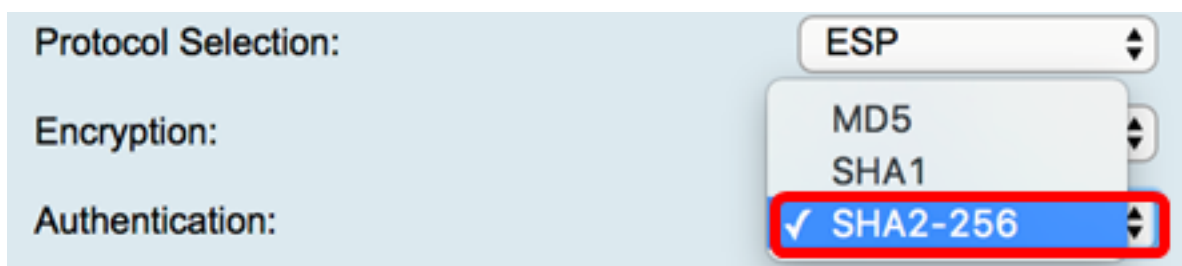
**Note:** Neste exemplo, AES-256 é escolhido.



[Etapa 8.](#) No menu suspenso Authentication (Autenticação), escolha um método de autenticação que determinará como o ESP e o ISAKMP são autenticados. As opções são:

- MD5 — O algoritmo de resumo de mensagem tem um valor de hash de 128 bits.
- SHA-1 — O algoritmo de hash seguro tem um valor de hash de 160 bits.
- SHA2-256 — Algoritmo Hash Seguro com um valor hash de 256 bits.

**Note:** Neste exemplo, SHA2-256 é usado.



Etapa 9. No campo *Vida útil do SA*, insira um valor entre 120 e 28800. Este é o período de tempo durante o qual o SA do IKE permanecerá ativo nesta fase. O valor padrão é 3600.

**Note:** Neste exemplo, 28799 é usado.

SA Lifetime:

28799

Etapa 10. Na lista suspensa Grupo DH, escolha o grupo Diffie-Hellman (DH) apropriado a ser usado com a chave na Fase 2. As opções são:

- Group2 - 1024 bits — Calcula a chave mais lentamente, mas é mais seguro que Group1.
- Group5 - 1536 bit — Calcula a chave com o menor tempo, mas é a mais segura.

**Note:** Neste exemplo, Grupo5 - 1536 bits é escolhido.

SA Lifetime:

28799

DH Group:

Group2 - 1024 bit

✓ Group5 - 1536 bit

Apply

Etapa 11. Clique em

**Note:** Você será levado de volta para a Tabela de perfis de IPsec e o perfil de IPsec recém-criado deverá aparecer agora.

## IPsec Profiles



Success. To permanently save the configuration. Go to [Configuration Management](#) page or click Save icon.

### IPsec Profiles Table

Name	Policy	In Use
<input type="radio"/> Amazon_Web_Services	Auto	<input checked="" type="checkbox"/>
<input type="radio"/> Default	Auto	<input checked="" type="checkbox"/>
<input type="radio"/> Microsoft_Azure	Auto	<input type="checkbox"/>
<input type="radio"/> IPsec_Vpn	Auto	<input type="checkbox"/>

Add

Edit

Clone

Delete

Apply

Cancel

Etapa 12. (Opcional) Para salvar a configuração permanentemente, vá para a página

Copiar/Salvar configuração ou clique no  Save ícone na parte superior da página.

Agora você deve ter configurado com êxito um perfil de IPsec automático em um roteador RV34x Series.

## [Defina as configurações manuais](#)

Etapa 1. No campo *SPI-Entrada*, insira um número hexadecimal que varia de 100 a FFFFFFFF 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.

**Note:** Para este exemplo, 0xABCD é usado.



Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a1a1212121

**Etapa 6.** Escolha uma opção na lista suspensa Algoritmo de integridade manual.

- 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. 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 — 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.

Authentication:	<input checked="" type="checkbox"/> MD5
	<input type="checkbox"/> SHA1
	<input type="checkbox"/> SHA2-256
Key-In	
Key-Out	

**Passo 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 32 caracteres.
- SHA-1 usa uma chave de 40 caracteres.
- SHA2-256 usa uma chave de 64 caracteres.

**Note:** Neste exemplo, 123456789123456789123... é usado.

Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a1a1212121

**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](#).

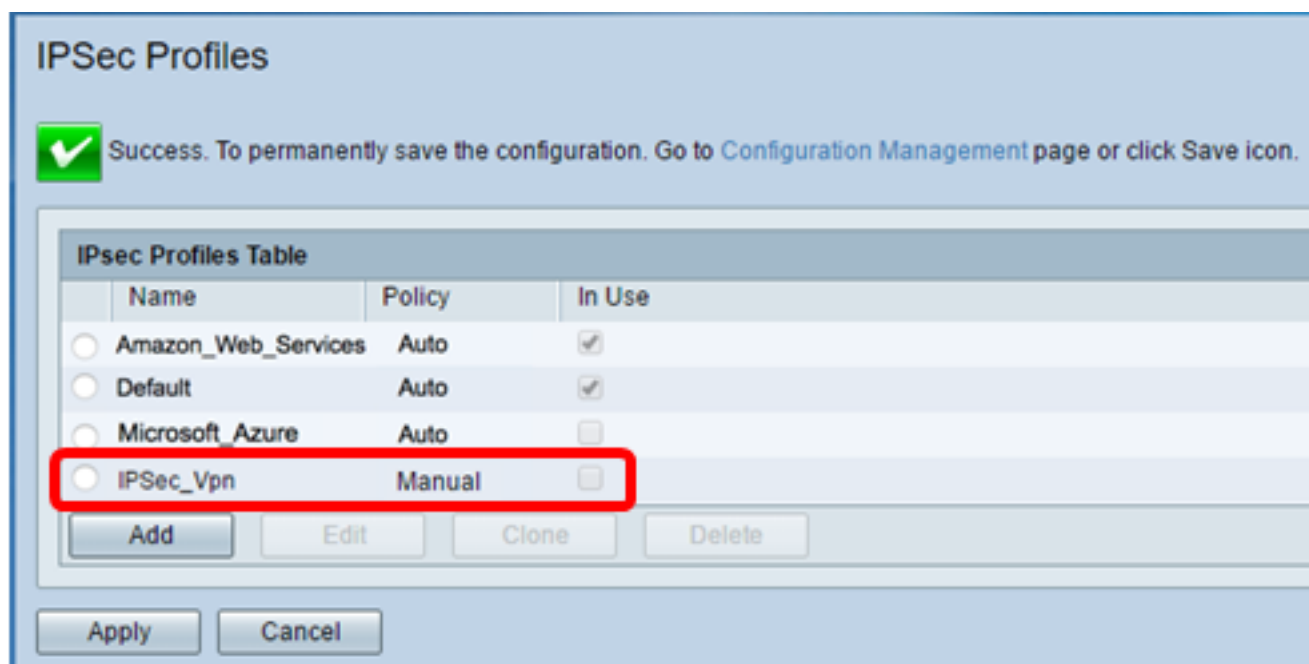
**Note:** Neste exemplo, 1a1a1a1a1a1a1a1a121212... é usado.

Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a1a1212121


**Etapa 9.** Clique em



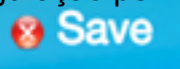
**Note:** Você será levado de volta para a Tabela de perfis de IPSec e o perfil de IPSec recém-criado deverá aparecer agora.



IPsec Profiles

 Success. To permanently save the configuration. Go to [Configuration Management](#) page or click Save icon.

IPsec Profiles Table		
Name	Policy	In Use
<input type="radio"/> Amazon_Web_Services	Auto	<input checked="" type="checkbox"/>
<input type="radio"/> Default	Auto	<input checked="" type="checkbox"/>
<input type="radio"/> Microsoft_Azure	Auto	<input type="checkbox"/>
<input type="radio"/> IPSec_Vpn	Manual	<input type="checkbox"/>

Etapa 10. (Opcional) Para salvar a configuração permanentemente, vá para a página Copiar/Salvar configuração ou clique no  ícone na parte superior da página.

Agora você deve ter configurado com êxito um perfil de IPSec manual em um roteador RV34x Series.