

# Configurações de política de Internet Key Exchange (IKE) em roteadores VPN RV130 e RV130W

## Objetivo

O Internet Key Exchange (IKE) é um protocolo que estabelece a comunicação segura entre duas redes. Com o IKE, os pacotes são criptografados e bloqueados e desbloqueados com chaves usadas por duas partes.

Você precisa criar uma política de Internet Key Exchange antes de configurar uma política de VPN. Consulte [VPN Policy Configuration on RV130 and RV130W](#) para obter mais informações.

O objetivo deste documento é mostrar como adicionar um perfil IKE aos RV130 e RV130W VPN Routers.

## Dispositivos aplicáveis

RV130  
RV130W

## Fases processuais

Etapa 1. Use o Router Configuration Utility para escolher **VPN > Site-to-Site IPSec VPN > Advanced VPN Setup** no menu à esquerda. A página *Advanced VPN Setup* é exibida:

Advanced VPN Setup

NAT Traversal:  Enable

**IKE Policy Table**

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm	Authentication Algorithm	DH Group	
<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	Policy Type	Encryption Algorithm	Authentication Algorithm	Local	Remote	
<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"/>								

Etapa 2. Na Tabela de Políticas IKE, clique em **Adicionar Linha**. Uma nova janela será exibida:

**IKE Policy Table**

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm	Authentication Algorithm	DH Group	
<input type="checkbox"/>	No data to display							
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>								

Etapa 3. Digite um nome para a política IKE no campo *Nome IKE*.

**Add / Edit IKE Policy Configuration**

IKE Name:

Exchange Mode:

Etapa 4. No menu suspenso *Exchange Mode*, escolha o modo no qual uma troca de chaves é usada para estabelecer comunicação segura.

**Add / Edit IKE Policy Configuration**

IKE Name:

Exchange Mode:

**Local**

- Main
- Aggressive

As opções disponíveis são definidas da seguinte forma:

- Principal — protege a identidade dos colegas para aumentar a segurança.
- Agressivo — não oferece proteção à identidade do colega, mas fornece uma conexão mais rápida.

Etapa 5. No menu suspenso *Local Identifier Type*, escolha o tipo de identidade do perfil.

**Local**

Local Identifier Type:

Local Identifier:

- Local WAN IP
- IP Address

As opções disponíveis são definidas da seguinte forma:

- IP de WAN local (Internet) — Conecta-se pela Internet.
- Endereço IP — sequência única de números separados por pontos que identifica cada máquina usando o Internet Protocol para se comunicar em uma rede.

Etapa 6. (Opcional) Se **Endereço IP** estiver selecionado na lista suspensa na etapa 5, insira o endereço IP local no campo *Identificador local*.

**Local**

Local Identifier Type:

Local Identifier:

Etapa 7. No menu suspenso *Remote Identifier Type*, escolha o tipo de identidade do perfil.

**Remote**

Remote Identifier Type:

Remote Identifier:

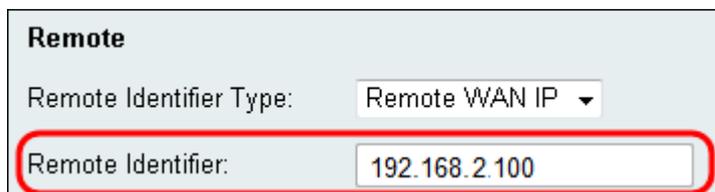
- Remote WAN IP
- IP Address

As opções disponíveis são definidas da seguinte forma:

·IP de WAN local (Internet) — Conecta-se pela Internet.

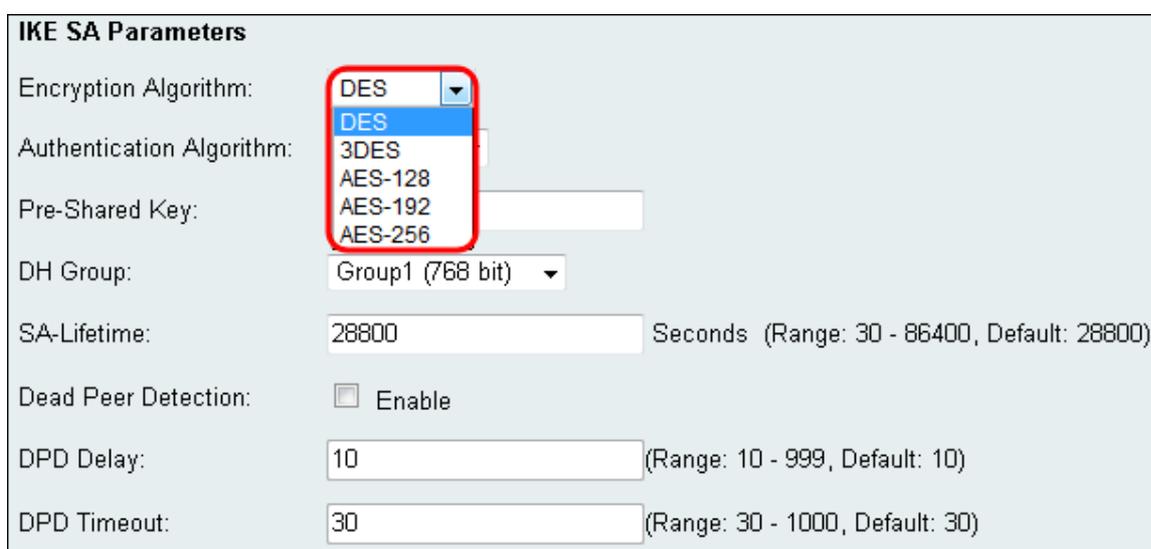
·Endereço IP — sequência única de números separados por pontos que identifica cada máquina usando o Internet Protocol para se comunicar em uma rede.

Etapa 8. (Opcional) Se **Endereço IP** estiver selecionado na lista suspensa na Etapa 7, insira o endereço IP remoto no campo *Identificador remoto*.



The screenshot shows a configuration window titled "Remote". It contains two fields: "Remote Identifier Type" with a dropdown menu set to "Remote WAN IP", and "Remote Identifier" with a text input field containing "192.168.2.100". A red rectangular box highlights the "Remote Identifier" field.

Etapa 9. No menu suspenso *Algoritmo de criptografia*, escolha um algoritmo para criptografar suas comunicações. **AES-128** é escolhido como padrão.



The screenshot shows the "IKE SA Parameters" configuration window. The "Encryption Algorithm" dropdown menu is open, showing a list of options: DES, 3DES, AES-128, AES-192, and AES-256. The "AES-128" option is highlighted in blue. Other fields include "Authentication Algorithm", "Pre-Shared Key", "DH Group" (set to "Group1 (768 bit)"), "SA-Lifetime" (28800 seconds), "Dead Peer Detection" (unchecked), "DPD Delay" (10), and "DPD Timeout" (30).

As opções disponíveis estão listadas da seguinte forma, desde a menor até a maior segurança:

·DES — Data Encryption Standard (Padrão de criptografia de dados).

·3DES — Triple Data Encryption Standard.

AES-128 — Advanced Encryption Standard usa uma chave de 128 bits.

AES-192 — O Advanced Encryption Standard usa uma chave de 192 bits.

AES-256 — Advanced Encryption Standard usa uma chave de 256 bits.

**Note:** AES é o método padrão de criptografia sobre DES e 3DES para seu maior desempenho e segurança. O aumento da chave AES aumentará a segurança com uma queda no desempenho. AES-128 é recomendado, pois oferece o melhor compromisso entre velocidade e segurança.

Etapa 10. No menu suspenso *Authentication Algorithm*, escolha um algoritmo para autenticar suas comunicações. **SHA-1** é escolhido como padrão.

**IKE SA Parameters**

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: MD5 ▾  
 MD5  
 SHA-1  
 SHA2-256

Pre-Shared Key:

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)

As opções disponíveis são definidas da seguinte forma:

·MD5 — O algoritmo Message Digest possui um valor de hash de 128 bits.

SHA-1 — O Secure Hash Algorithm tem um valor hash de 160 bits.

·SHA2-256 — Algoritmo de hash seguro com um valor de hash de 256 bits.

**Note:** MD5 e SHA são funções hash criptográficas. Eles pegam um pedaço de dados, compactam-no e criam uma saída hexadecimal exclusiva que geralmente não é reproduzível. O MD5 não oferece praticamente nenhuma segurança contra colisões de hash e só deve ser usado em um ambiente de pequena empresa onde a resistência à colisão não é necessária. SHA1 é uma opção melhor que o MD5 porque oferece melhor segurança em velocidades inacreditavelmente mais lentas. Para obter os melhores resultados, o SHA2-256 não tem ataques conhecidos de relevância prática e oferecerá a melhor segurança. Como mencionado anteriormente, maior segurança significa velocidades mais lentas.

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

**IKE SA Parameters**

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: SHA-1 ▾

Pre-Shared Key:

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)

Etapa 12. No menu suspenso *Grupo DH*, escolha um grupo DH. O número de bits indica o nível de segurança. As duas extremidades da conexão devem estar no mesmo grupo.

**IKE SA Parameters**

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: SHA-1 ▾

Pre-Shared Key:

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)

Etapa 13. No *campo SA-Lifetime*, insira quanto tempo a Associação de Segurança será válida em segundos. O padrão é 28800 segundos.

**IKE SA Parameters**

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: SHA-1 ▾

Pre-Shared Key:

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)

Etapa 14. (Opcional) Marque a caixa de seleção **Enable** no campo *Dead Peer Detection* se quiser desativar uma conexão com o peer inativo. Vá para a etapa 17 se você não tiver ativado a Detecção de peer inativo.

**IKE SA Parameters**

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: SHA-1 ▾

Pre-Shared Key:

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)

Etapa 15. (Opcional) Se você ativou a Detecção de ponto morto, insira um valor no campo

*Atraso de DPD.* Esse valor especificará quanto tempo o roteador aguardará para verificar a conectividade do cliente.

Dead Peer Detection:	<input 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 16. (Opcional) Se você ativou a Detecção de ponto morto, insira um valor no campo *Tempo limite de DPD*. Esse valor especificará por quanto tempo o cliente permanecerá conectado até que o tempo limite seja atingido.

Dead Peer Detection:	<input 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** para salvar as alterações.

<b>IKE SA Parameters</b>	
Encryption Algorithm:	<input type="text" value="AES-128"/>
Authentication Algorithm:	<input type="text" value="SHA-1"/>
Pre-Shared Key:	<input type="text"/>
DH Group:	<input type="text" value="Group1 (768 bit)"/>
SA-Lifetime:	<input type="text" value="28800"/> Seconds (Range: 30 - 86400, Default: 28800)
Dead Peer Detection:	<input 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)
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Back"/>	

## 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.