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.

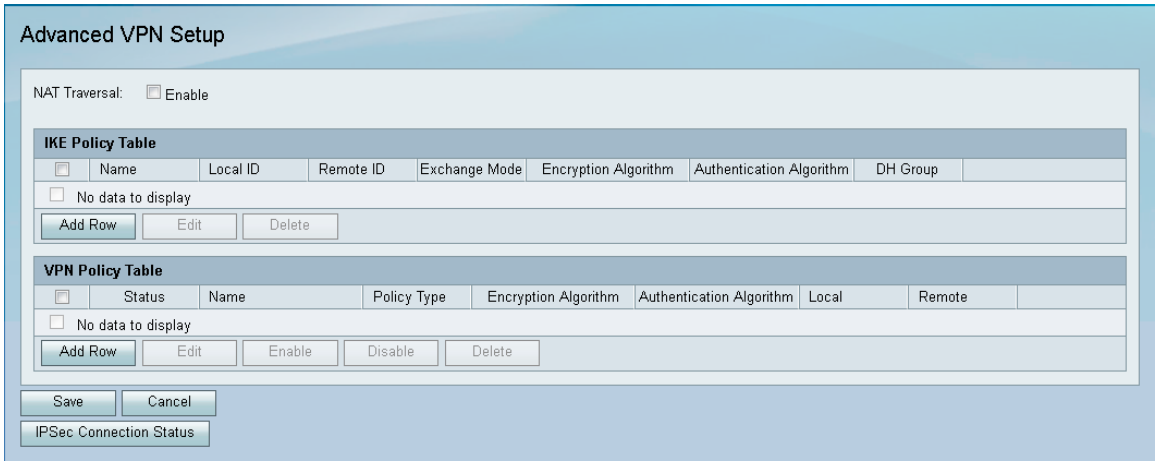
O objetivo deste documento é mostrar como adicionar um perfil IKE aos RV130 e RV130W VPN Routers.

Dispositivos aplicáveis

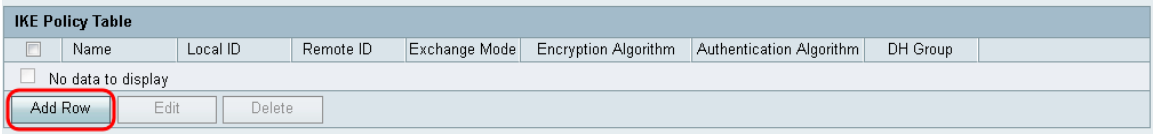
RV130
RV130W

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:

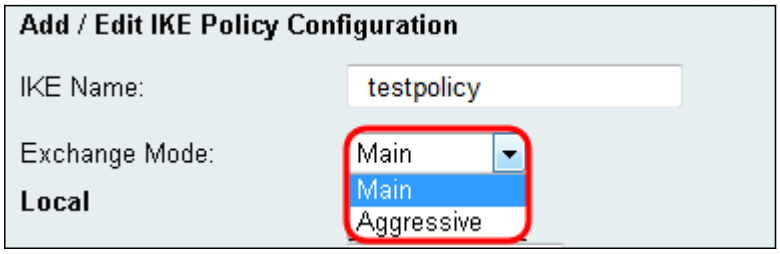


Etapa 2. Na Tabela de Políticas IKE, clique em **Adicionar Linha**. Uma nova janela será exibida:



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

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

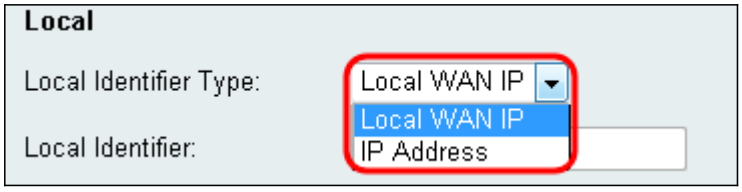


As opções disponíveis são definidas da seguinte forma:

·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.

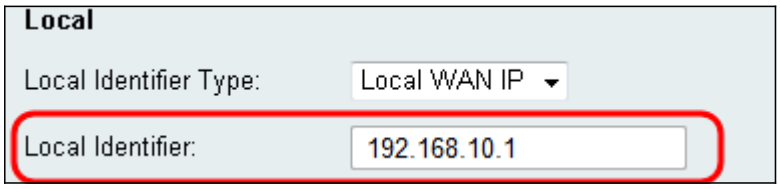


As opções disponíveis são definidas da seguinte forma:

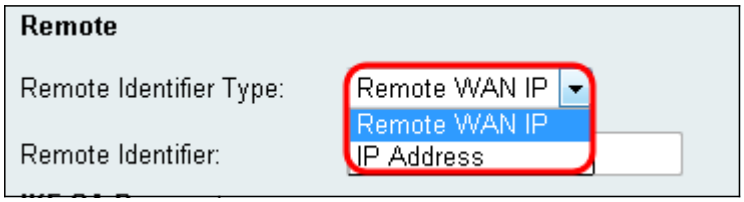
·IP de WAN local (Internet) — Conecta-se pela Internet.

·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*.



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

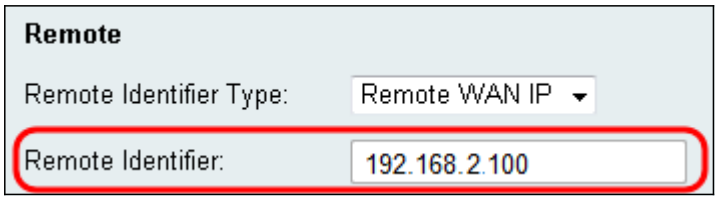


As opções disponíveis são definidas da seguinte forma:

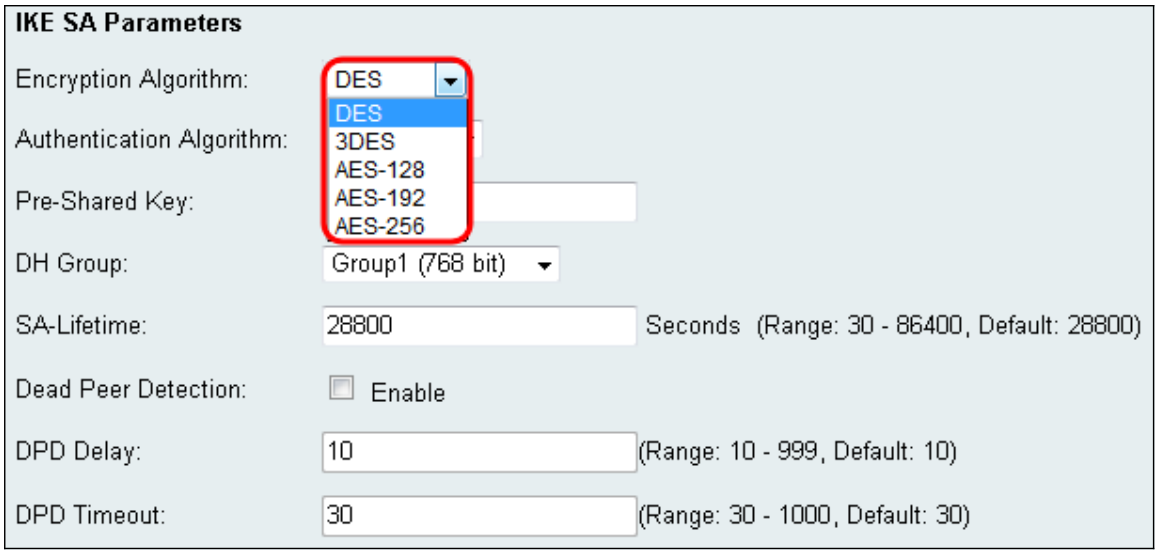
·IP de WAN local (Internet) — Conecta-se pela Internet.

·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*.



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



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.

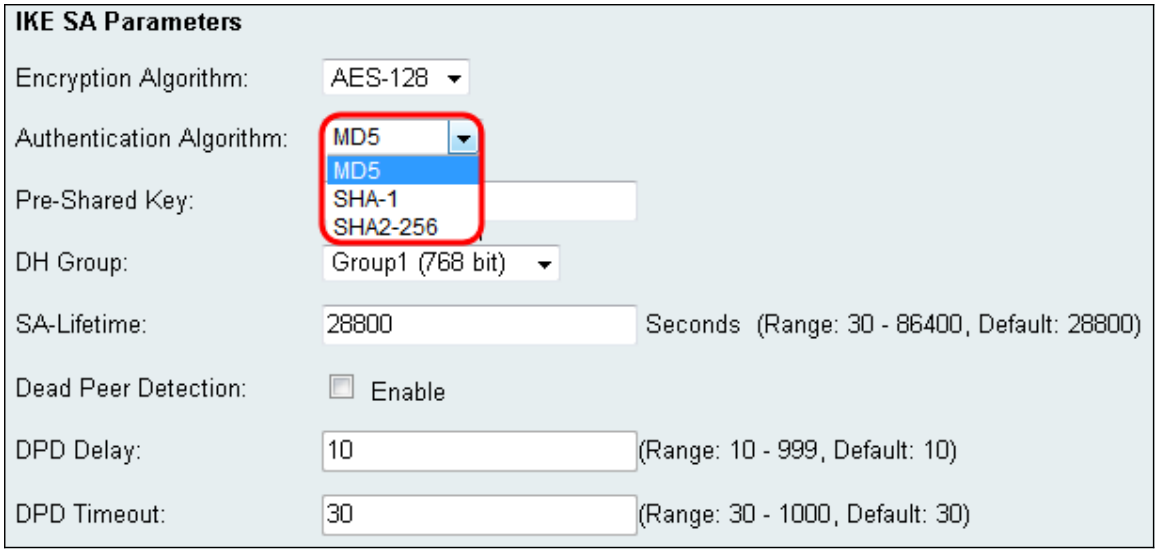
AES-128 — Advanced Encryption Standard usa uma chave de 128 bits.

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.



As opções disponíveis são definidas da seguinte forma:

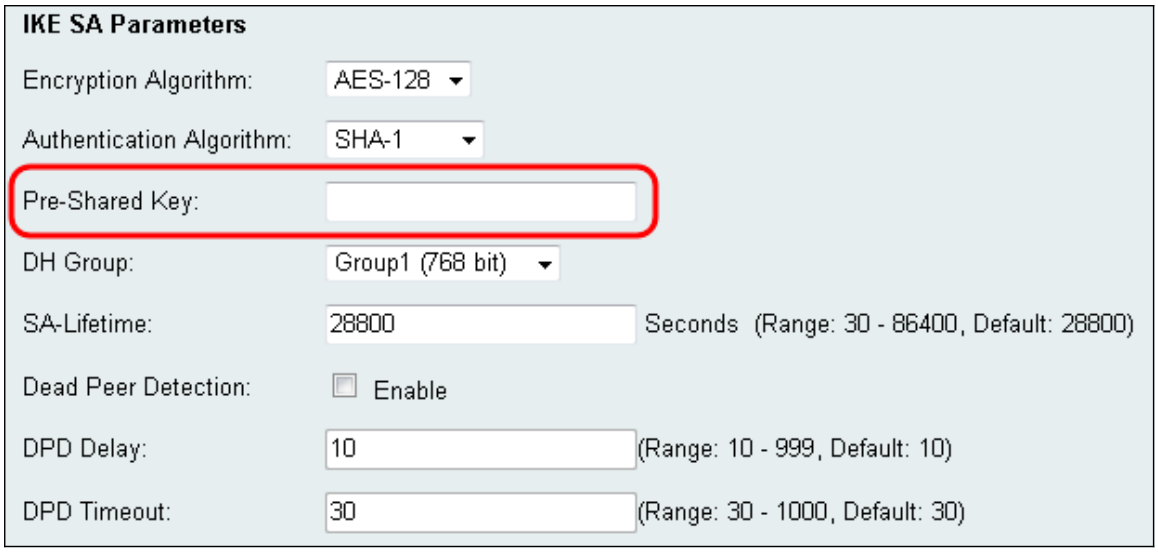
·MD5 — O algoritmo Message Digest possui um valor de hash de 128 bits.

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

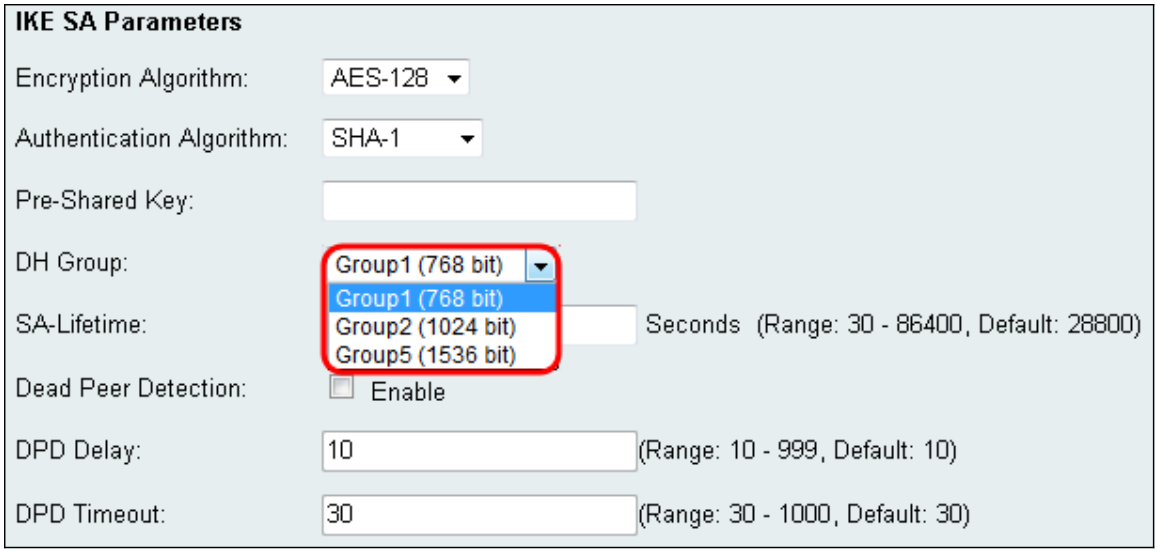
·SHA2-256 — Algoritmo de hash seguro com um valor de hash de 256 bits.

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.

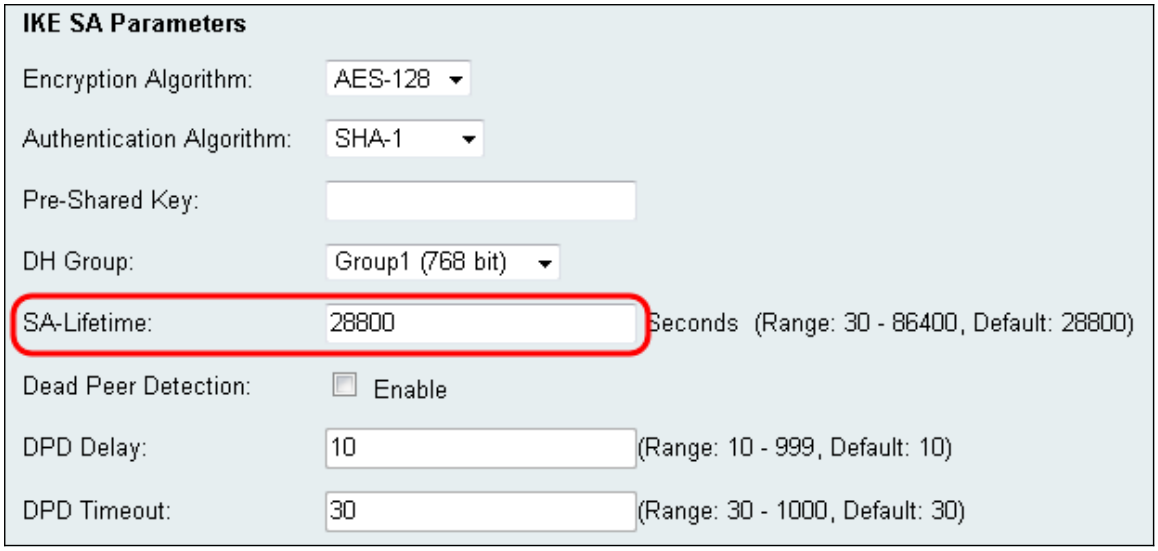
Etapa 11. No campo *Pre-Shared Key*, digite uma senha com 8 a 49 caracteres.



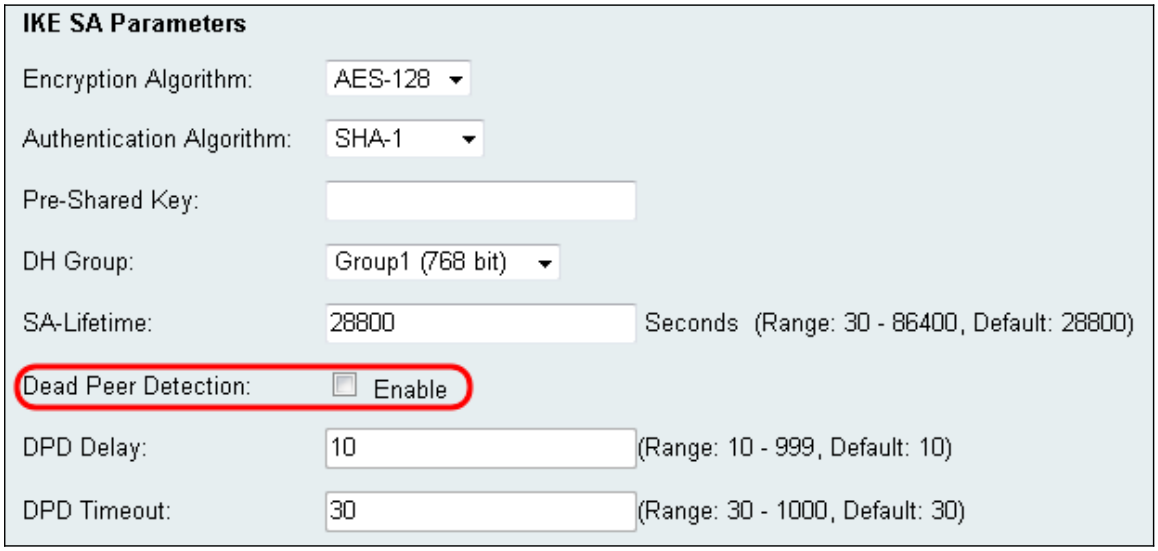
Etapa 12. No menu suspenso *Grupo DH*, escolha um grupo DH. O número de bits indica o nível de segurança. As duas extremidades da conexão devem estar no mesmo grupo.



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

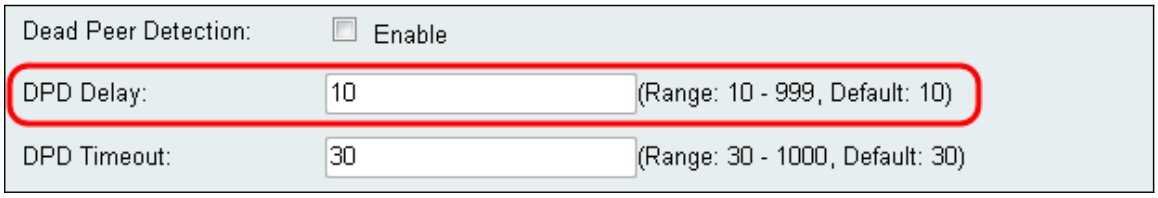


Etapa 14. (Opcional) Marque a caixa de seleção **Enable** no campo *Dead Peer Detection* se quiser desativar uma conexão com o peer inativo. Vá para a etapa 17 se você não tiver ativado a Detecção de peer inativo.



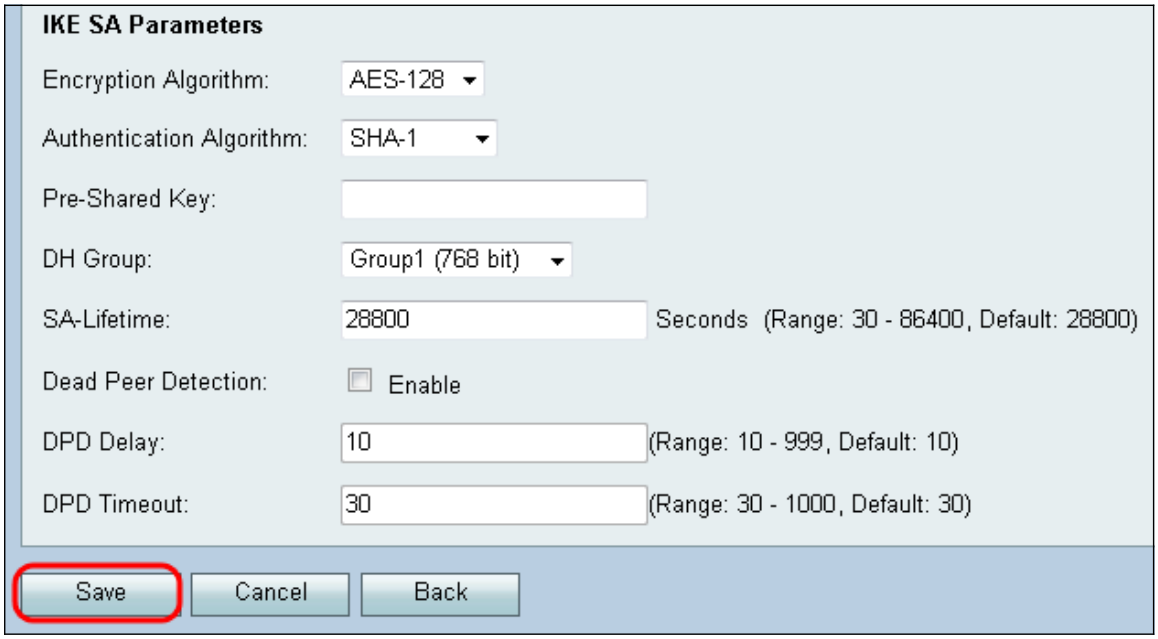
Etapa 15. (Opcional) Se você ativou a Detecção de ponto morto, insira um valor no campo

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



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.

Etapa 17. Clique em **Salvar** para salvar as alterações.



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.