Configuração de Gateway para Gateway VPN em RV016, RV042, RV042G e RV082 VPN Routers

Objetivo

Uma VPN (Virtual Private Network) é usada para formar uma conexão segura entre dois pontos de extremidade em uma Internet pública ou compartilhada, através do que é chamado de túnel VPN. Mais especificamente, uma conexão VPN de gateway a gateway permite que dois roteadores se conectem com segurança e que um cliente em uma extremidade apareça logicamente como se fizesse parte da rede na outra extremidade. Isso permite que os dados e recursos sejam compartilhados com mais facilidade e segurança pela Internet.

A configuração deve ser feita em ambos os roteadores para habilitar uma VPN de gateway para gateway. As configurações feitas nas seções *Local Group Setup* e *Remote Group Setup* devem ser revertidas entre os dois roteadores para que o grupo local de um seja o grupo remoto do outro.

O objetivo deste documento é explicar como configurar o Gateway-to-Gateway VPN em RV016, RV042, RV042G e RV082 VPN Series Routers.

Dispositivos aplicáveis

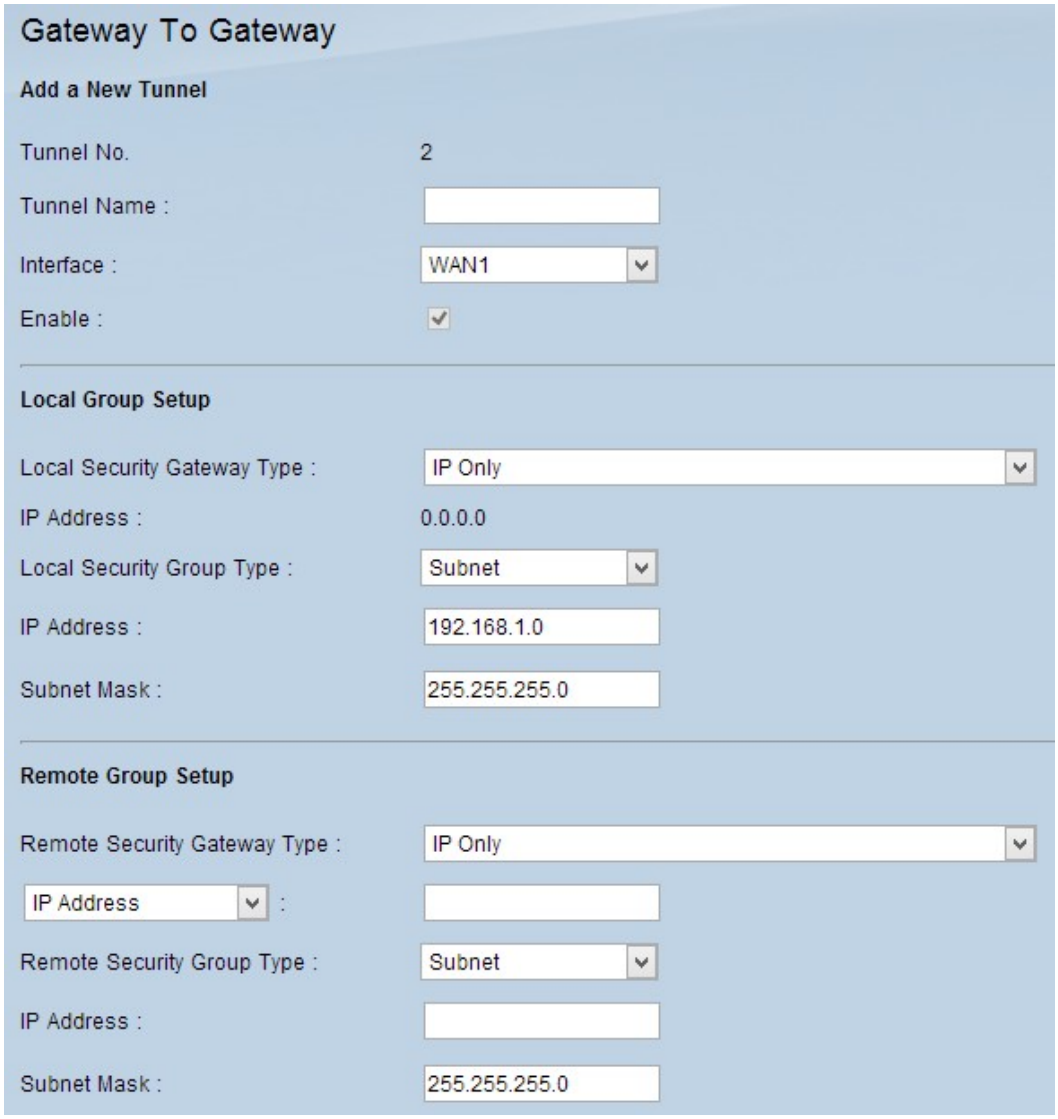
- RV016
- RV042
- RV042G
- RV082

Versão de software

- v4.2.2.08

Configurar Gateway para Gateway VPN

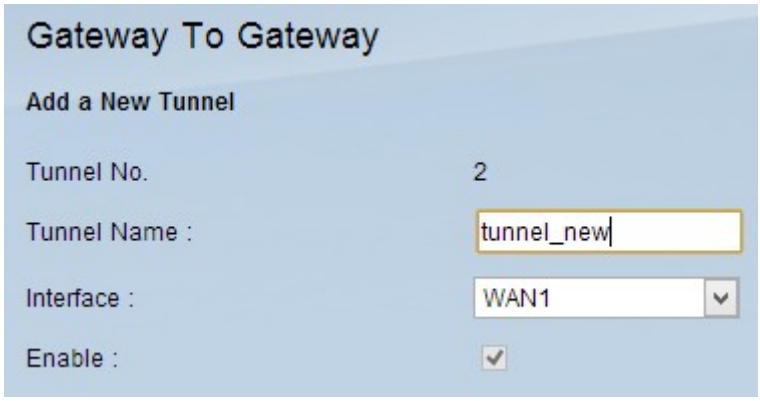
Etapa 1. Faça login no Router Configuration Utility e escolha **VPN > Gateway to Gateway**. A página *Gateway to Gateway* é aberta:



Para configurar o gateway para o gateway VPN, os seguintes recursos precisam ser configurados:

1. Adicionar novo túnel
2. Configuração de grupo local
3. Configuração do grupo remoto
4. Configuração do IPSec

Adicionar novo túnel



O túnel nº é um campo somente leitura que exibe o túnel atual que será criado.

Etapa 1. Insira um nome para o túnel VPN no campo Tunnel Name (Nome do túnel). Ele não precisa corresponder ao nome usado na outra extremidade do túnel.

Etapa 2. Na lista suspensa Interface, escolha a porta WAN (Wide Area Network, Rede de longa distância) a ser usada para o túnel.

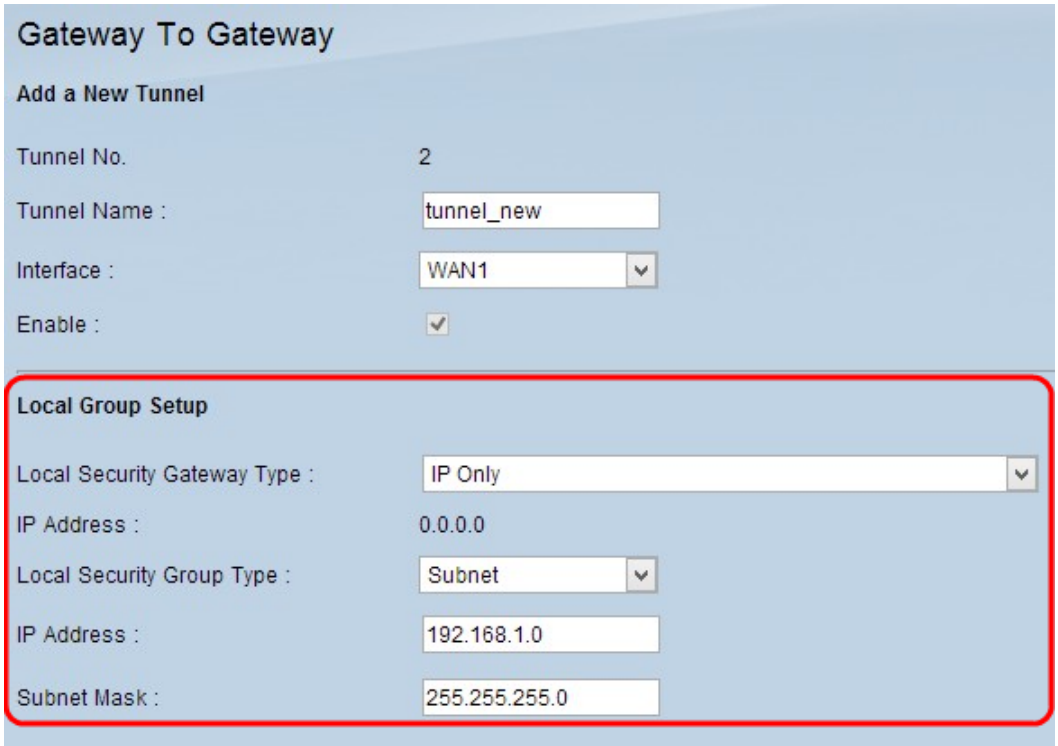
WAN1 — A porta WAN dedicada dos roteadores VPN série RV0XX.

WAN2 — A porta WAN2/DMZ dos roteadores VPN série RV0XX. Somente será exibido no menu suspenso se tiver sido configurado como uma WAN e não como uma porta DMZ (Demilitarize Zone, Zona desmilitarizada).

Etapa 3. (Opcional) Para habilitar a VPN, marque a caixa de seleção no campo **Habilitar**. A VPN está habilitada por padrão.

Configuração de grupo local

Note: A configuração para a configuração do grupo local em um roteador deve ser a mesma da configuração para a configuração do grupo remoto no outro roteador.



Etapa 1. Escolha o método de identificação de roteador apropriado para estabelecer um túnel VPN na lista suspensa Tipo de gateway de segurança local.

Somente IP — O roteador local (este roteador) é reconhecido por um endereço IP estático. Você só pode escolher essa opção se o roteador tiver um IP de WAN estático. O endereço IP estático da WAN é exibido automaticamente no campo Endereço IP.

Autenticação IP + nome de domínio (FQDN) — O acesso ao túnel é possível por meio de um endereço IP estático e um domínio registrado. Se você escolher essa opção, digite o nome do domínio registrado no campo Domain Name (Nome do domínio). O endereço IP estático da WAN é exibido automaticamente no campo Endereço IP.

Autenticação IP + E-mail Addr (USER FQDN) — O acesso ao túnel é possível por meio de um endereço IP estático e um endereço de e-mail. Se você escolher esta opção, digite o endereço de e-mail no campo Email Address (Endereço de e-mail). O endereço IP estático da WAN é exibido automaticamente no campo Endereço IP.

Autenticação de IP dinâmico + nome de domínio (FQDN) — O acesso ao túnel é possível por meio de um endereço IP dinâmico e de um domínio registrado. Se você escolher essa opção, digite o nome do domínio registrado no campo Domain Name (Nome do domínio).

Autenticação IP dinâmica + endereço de e-mail (USER FQDN) — O acesso ao túnel é possível por meio de um endereço IP dinâmico e um endereço de e-mail. Se você escolher esta opção, digite o endereço de e-mail no campo Email Address (Endereço de e-mail).

Etapa 2. Escolha o usuário ou grupo de usuários da LAN local apropriado que podem acessar o túnel VPN na lista suspensa Grupo de segurança local. O padrão é Subnet (Sub-rede).

IP — Somente um dispositivo de LAN pode acessar o túnel VPN. Se você escolher esta opção, digite o endereço IP do dispositivo de LAN no campo IP Address (Endereço IP).

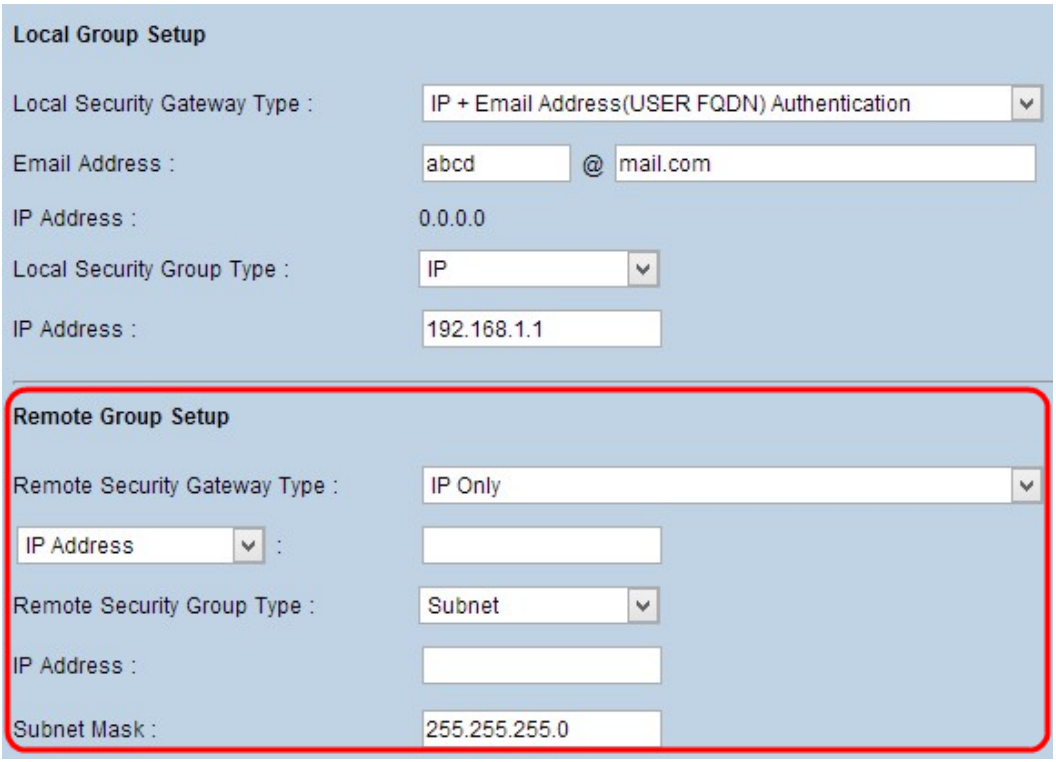
Sub-rede - Todos os dispositivos de LAN em uma sub-rede específica podem acessar o túnel. Se você escolher essa opção, insira o endereço IP da sub-rede e a máscara de sub-rede dos dispositivos da LAN no campo Endereço IP e Máscara de sub-rede, respectivamente. O valor padrão é 255.255.255.0.

Intervalo de IP — Um intervalo de dispositivos LAN pode acessar o túnel. Se você escolher essa opção, insira o endereço IP inicial e final nos campos Begin IP (IP inicial) e End IP (IP final), respectivamente.

Etapa 3. Clique em Save (Salvar) para salvar as configurações.

Configuração do grupo remoto

Note: A configuração para a configuração do grupo remoto em um roteador deve ser a mesma da configuração para a configuração do grupo local no outro roteador.



Etapa 1. Na lista suspensa Tipo de gateway de segurança remota, escolha o método para identificar o roteador remoto para estabelecer o túnel VPN.

Somente IP — O acesso ao túnel é possível por meio de um IP de WAN estático. Se você souber o endereço IP do roteador remoto, escolha o endereço IP na lista suspensa diretamente abaixo do campo Tipo de gateway de segurança remota e insira o endereço IP. Escolha IP por DNS Resolvido se você não souber o endereço IP, mas souber o nome do domínio e insira o nome do domínio do roteador no campo IP by DNS Resolvido.

Autenticação IP + nome de domínio (FQDN) — O acesso ao túnel é possível por meio de um endereço IP estático e um domínio registrado para o roteador. Se você souber o endereço IP do roteador remoto, escolha o endereço IP na lista suspensa diretamente abaixo do campo Tipo de gateway de segurança remota e insira o endereço. Escolha IP por DNS Resolvido se você não souber o endereço IP, mas souber o nome do domínio e insira o nome do domínio do roteador no campo IP by DNS Resolvido. Insira o nome de domínio do roteador no campo Nome do domínio, independentemente do método escolhido para identificá-lo.

Autenticação IP + endereço de e-mail (USER FQDN) — O acesso ao túnel é possível por meio de um endereço IP estático e um endereço de e-mail. Se você souber o endereço IP do roteador remoto, escolha o endereço IP na lista suspensa diretamente abaixo do campo Tipo de gateway de segurança remota e insira o endereço. Escolha IP por DNS Resolvido se você não souber o endereço IP, mas souber o nome do domínio e insira o nome do domínio do roteador no campo IP by DNS Resolvido. Digite o endereço de e-mail no campo Endereço de e-mail.

Autenticação de IP dinâmico + nome de domínio (FQDN) — O acesso ao túnel é possível por meio de um endereço IP dinâmico e de um domínio registrado. Se você escolher essa opção, digite o nome do domínio registrado no campo Domain Name (Nome do domínio).

Autenticação IP dinâmica + endereço de e-mail (USER FQDN) — O acesso ao túnel é possível por meio de um endereço IP dinâmico e um endereço de e-mail. Se você escolher esta opção, digite o endereço de e-mail no campo Email Address (Endereço de e-mail).

Etapa 2. Escolha o usuário ou grupo de usuários da LAN remota apropriado que podem acessar o túnel VPN na lista suspensa Tipo de grupo de segurança remota.

IP — Somente um dispositivo LAN específico pode acessar o túnel. Se você escolher esta opção, digite o endereço IP do dispositivo de LAN no campo IP Address (Endereço IP).

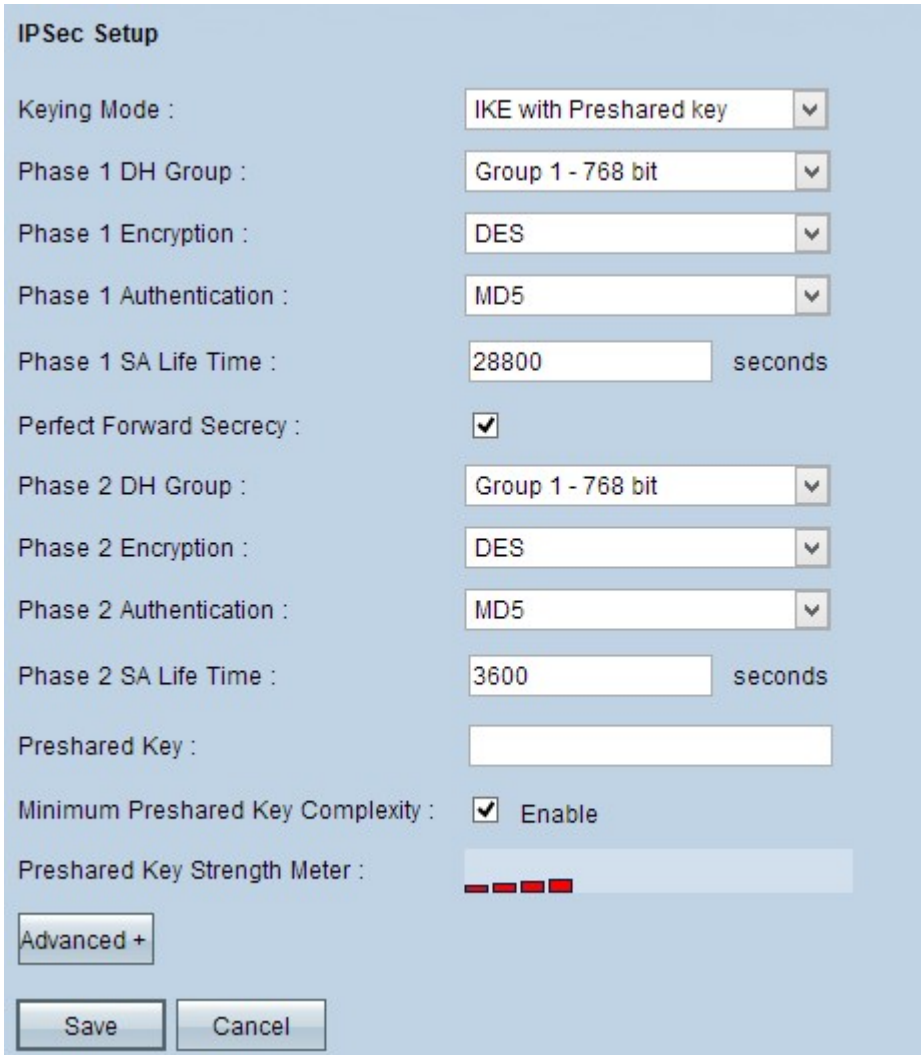
Sub-rede - Todos os dispositivos de LAN em uma sub-rede específica podem acessar o túnel. Se você escolher essa opção, insira o endereço IP da sub-rede e a máscara de sub-rede dos dispositivos da LAN no campo Endereço IP e Máscara de sub-rede, respectivamente.

Intervalo de IP — Um intervalo de dispositivos LAN pode acessar o túnel. Se você escolher essa opção, insira o endereço IP inicial e final nos campos Begin IP (IP inicial) e End IP (IP final), respectivamente.

Note: Os dois roteadores nas extremidades do túnel não podem estar na mesma sub-rede.

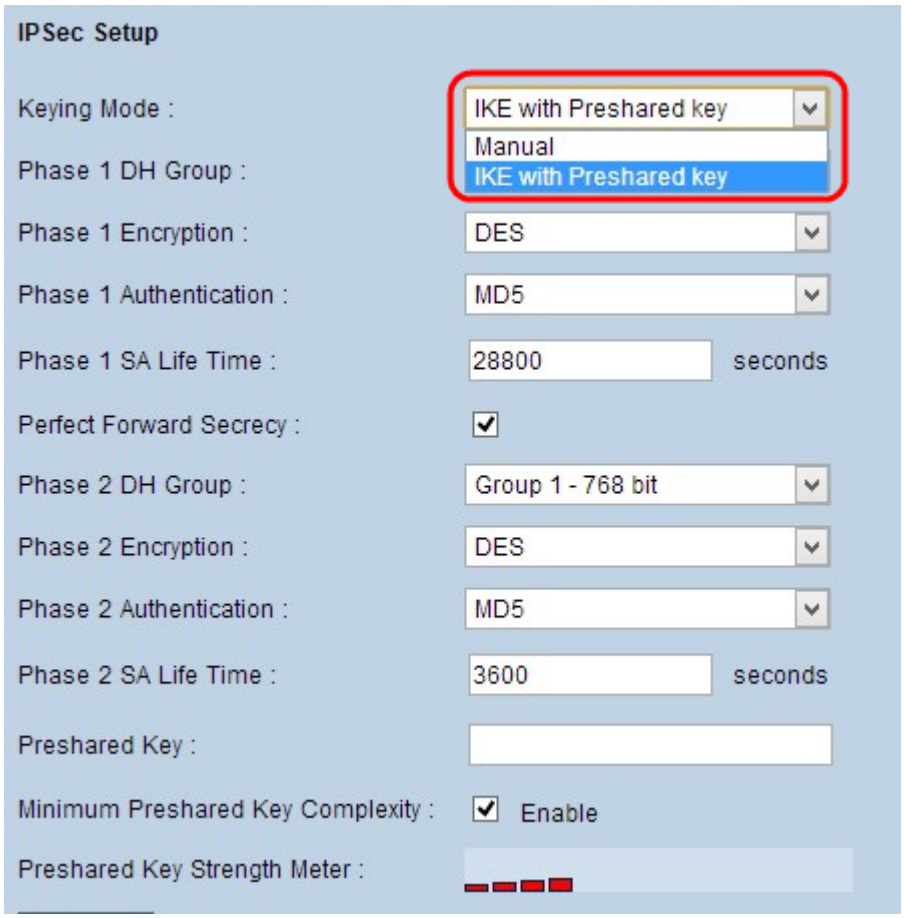
Etapa 3. Clique em Save (Salvar) para salvar as configurações.

Configuração do IPSec



Internet Protocol Security (IPSec) é um protocolo de segurança de camada de Internet que fornece segurança de ponta a ponta, por meio de autenticação e criptografia durante qualquer sessão de comunicação.

Note: As duas extremidades da VPN precisam ter os mesmos métodos de criptografia, descriptografia e autenticação para funcionar corretamente. Insira as mesmas configurações de IPSec para ambos os roteadores.

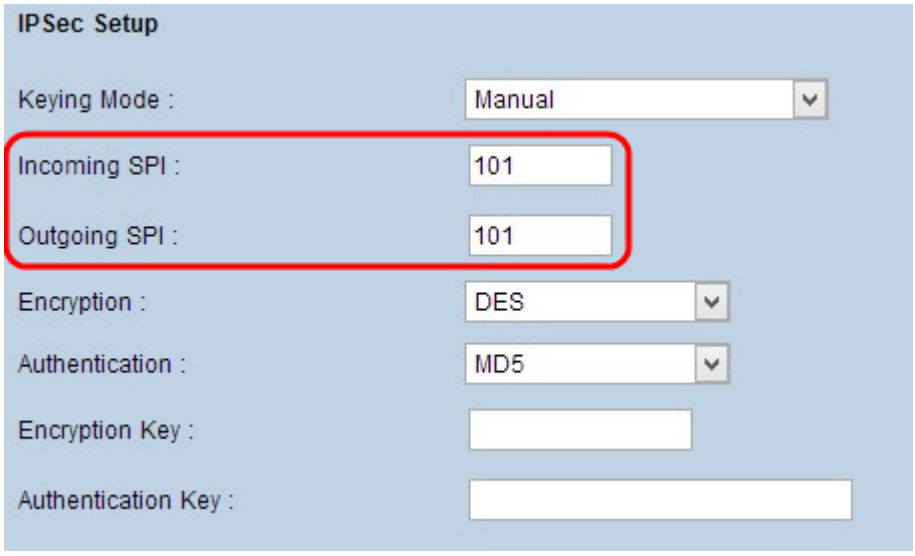


Etapa 1. Escolha o modo apropriado de gerenciamento de chaves para garantir a segurança na lista suspensa Modo de chaveamento. O modo padrão é IKE with Preshared key (IKE com chave pré-compartilhada).

Manual · — Um modo de segurança personalizado para gerar uma nova chave de segurança por si próprio e sem negociação com a chave. É o melhor a ser usado durante a solução de problemas e em um pequeno ambiente estático.

·IKE com chave pré-compartilhada — o protocolo IKE (Internet Key Exchange) é usado para gerar e trocar automaticamente uma chave pré-compartilhada para estabelecer a comunicação de autenticação para o túnel.

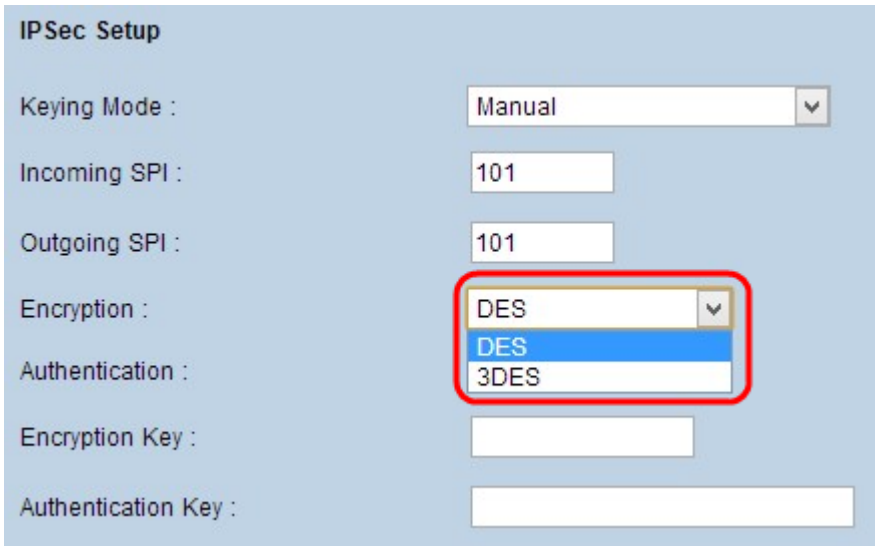
Configuração de IPSec para modo de chave manual



Etapa 1. Insira o valor hexadecimal exclusivo do Índice de parâmetro de segurança de entrada (SPI) no campo SPI de entrada. O SPI é transportado no cabeçalho do protocolo ESP (Encapsulating Security Payload Protocol) e determina a proteção do pacote recebido. Você pode inserir um valor de 100 a ffffff. O SPI de entrada do roteador local precisa corresponder ao SPI de saída do roteador remoto.

Etapa 2. Insira o valor hexadecimal exclusivo para o índice de parâmetro de segurança (SPI) de saída no campo SPI de saída. Você pode inserir um valor de 100 a ffffff. O SPI de saída do roteador remoto precisa corresponder ao SPI de entrada do roteador local.

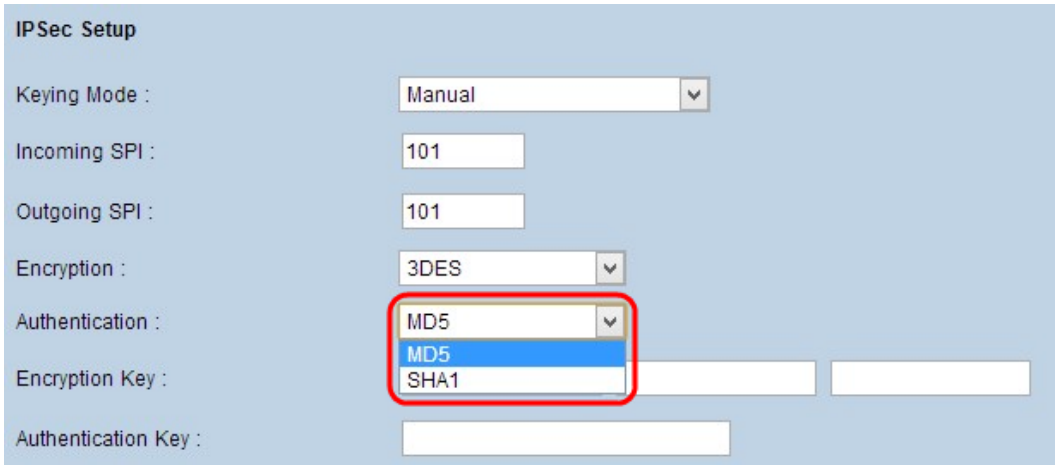
Note: Dois túneis não podem ter o mesmo SPI.



Etapa 3. Escolha o método de criptografia apropriado para os dados na lista suspensa Criptografia. A criptografia recomendada é 3DES. O túnel VPN precisa usar o mesmo método de criptografia em ambas as extremidades.

DES — O Data Encryption Standard (DES) usa um tamanho de chave de 56 bits para criptografia de dados. O DES está desatualizado e deve ser usado apenas se um endpoint for compatível apenas com DES.

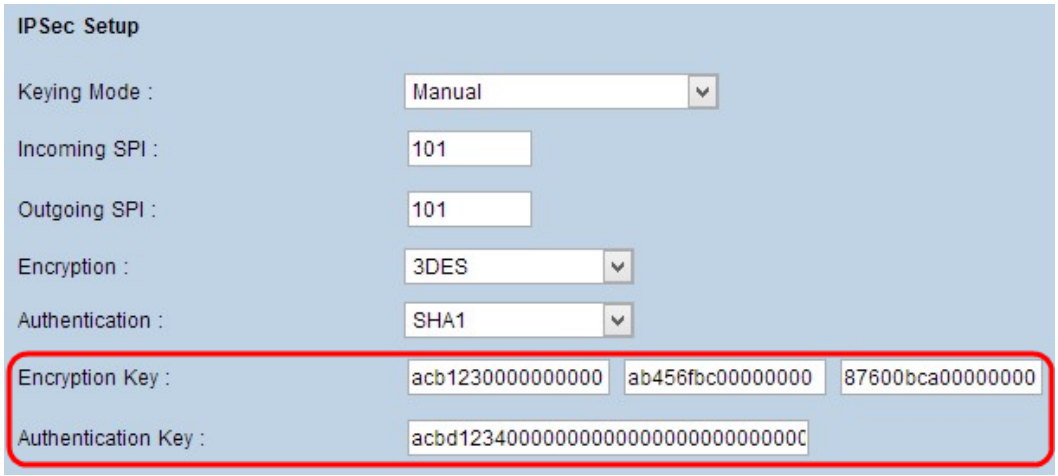
3DES — O 3DES (Triple Data Encryption Standard) é um método de criptografia simples de 168 bits. O 3DES criptografa os dados três vezes, o que fornece mais segurança que o DES.



Etapa 4. Escolha o método de autenticação apropriado para os dados na lista suspensa Autenticação. A autenticação recomendada é SHA1, pois é mais segura do que MD5. O túnel VPN precisa usar o mesmo método de autenticação para ambas as extremidades.

MD5 — Message Digest Algorithm-5 (MD5) é uma função de hash de 128 bits que fornece proteção aos dados contra ataques mal-intencionados pelo cálculo da soma de verificação.

SHA1 — O Secure Hash Algorithm versão 1 (SHA1) é uma função de hash de 160 bits mais segura que o MD5, mas leva mais tempo para computar.

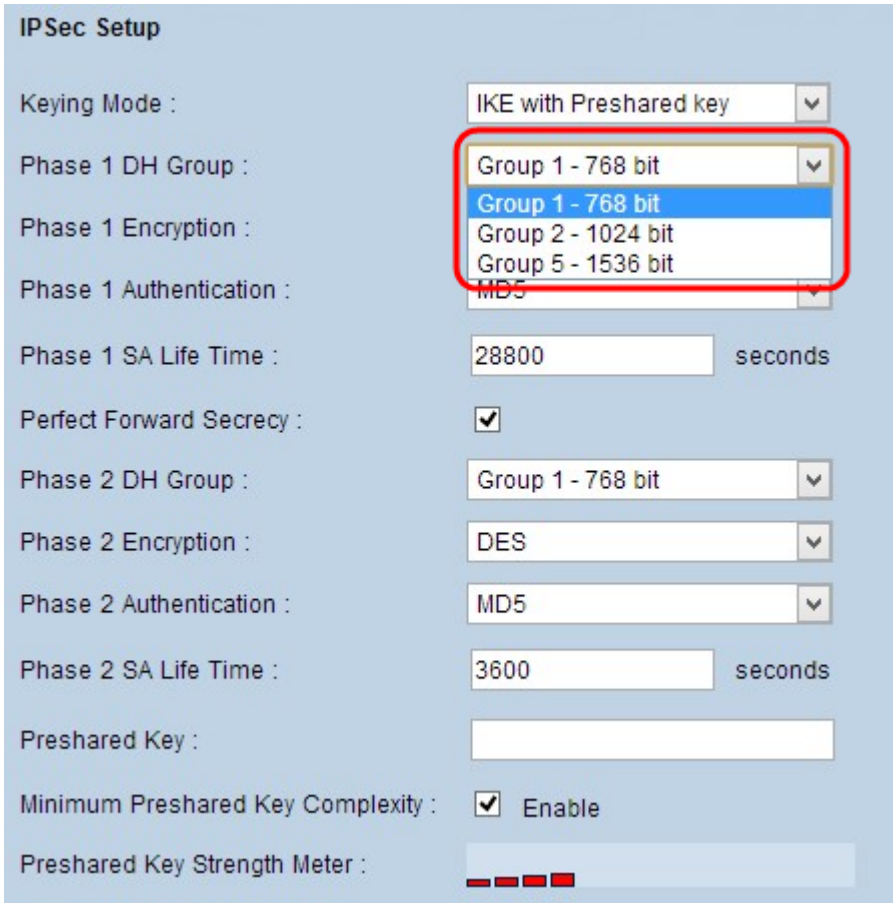


Etapa 5. Insira a chave para criptografar e descriptografar dados no campo Chave de criptografia. Se você escolher DES como método de criptografia na etapa 3, insira um valor hexadecimal de 16 dígitos. Se você escolher 3DES como método de criptografia na etapa 3, insira um valor hexadecimal de 40 dígitos.

Etapa 6. Insira uma chave pré-compartilhada para autenticar o tráfego no campo Chave de autenticação. Se você escolher o método de autenticação MD5 na etapa 4, insira o valor hexadecimal de 32 dígitos. Se você escolher SHA1 como método de autenticação na Etapa 4, insira um valor hexadecimal de 40 dígitos. Se você não adicionar dígitos suficientes, zeros serão anexados ao final até que haja dígitos suficientes. O túnel VPN precisa usar a mesma chave pré-compartilhada para ambas as extremidades.

Passo 7. Clique em **Save (Salvar) para salvar as configurações.**

Configuração do modo IKE com chave pré-compartilhada

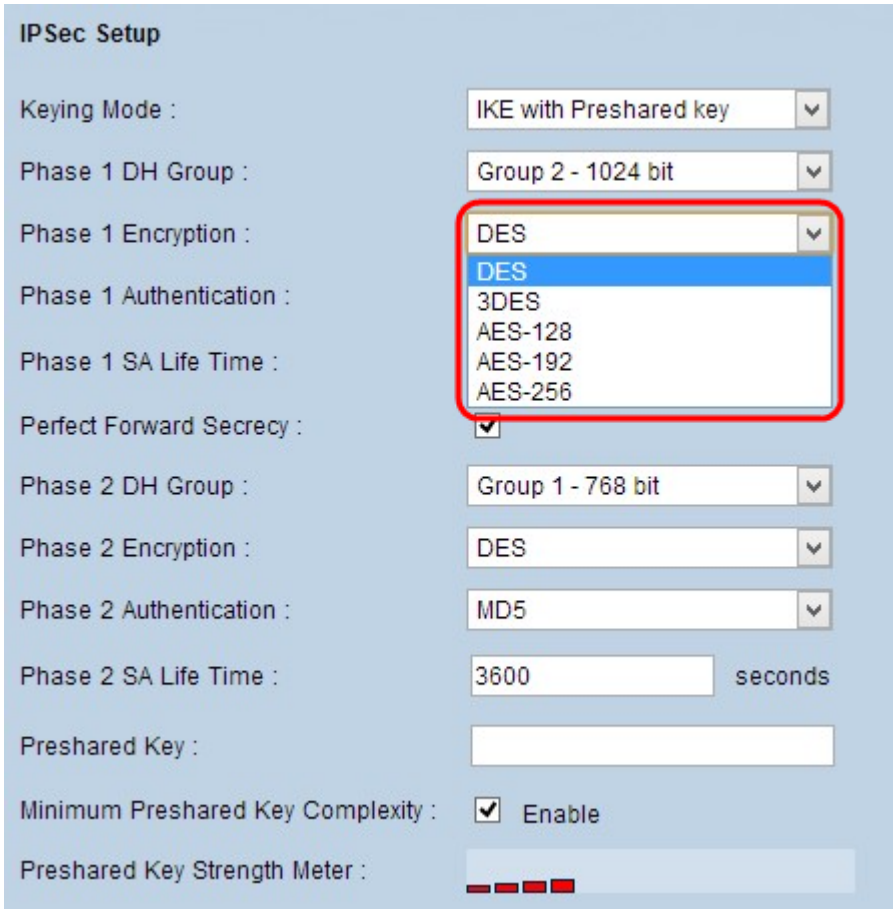


Etapa 1. Escolha o Grupo DH da Fase 1 apropriado na lista suspensa Grupo DH da Fase 1. A fase 1 é usada para estabelecer a associação de segurança lógica (SA) simples entre as duas extremidades do túnel para oferecer suporte à comunicação de autenticação segura. O Diffie-Hellman (DH) é um protocolo de troca de chaves criptográficas usado para determinar a força da chave durante a fase 1 e também compartilha a chave secreta para autenticar a comunicação.

Grupo 1 - 768 bits — A chave de força mais baixa e o grupo de autenticação mais inseguro, mas leva o menor tempo para computar as chaves IKE. Essa opção é preferida se a velocidade da rede for baixa.

Grupo 2 - 1024 bits — Uma chave de força maior e um grupo de autenticação mais seguro do que o grupo 1, mas leva mais tempo para computar as chaves IKE.

Grupo 5 - 1536 bits — A chave de força mais alta e o grupo de autenticação mais seguro. Precisa de mais tempo para computar as chaves de IKE. É preferível se a velocidade da rede for alta.



Etapa 2. Escolha a Criptografia da Fase 1 apropriada para criptografar a chave na lista suspensa de Criptografia da Fase 1. AES-128, AES-192 ou AES-256 são recomendados. O túnel VPN precisa usar o mesmo método de criptografia para as duas extremidades.

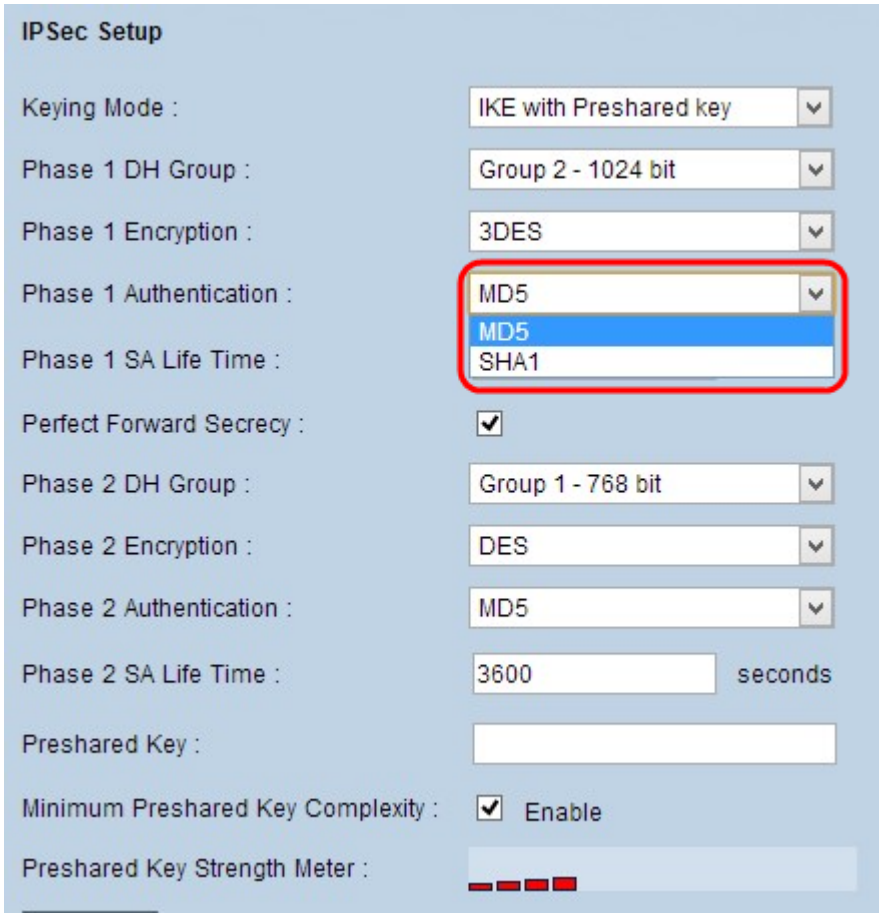
DES — O Data Encryption Standard (DES) usa um tamanho de chave de 56 bits para criptografia de dados. O DES está desatualizado e deve ser usado apenas se um endpoint for compatível apenas com DES.

3DES — O 3DES (Triple Data Encryption Standard) é um método de criptografia simples de 168 bits. O 3DES criptografa os dados três vezes, o que fornece mais segurança que o DES.

AES-128 — AES (Advanced Encryption Standard) é um método de criptografia de 128 bits que transforma o texto simples em texto cifrado através de 10 ciclos de repetições.

AES-192 — AES (Advanced Encryption Standard) é um método de criptografia de 192 bits que transforma o texto simples em texto cifrado através de repetições de 12 ciclos. O AES-192 é mais seguro que o AES-128.

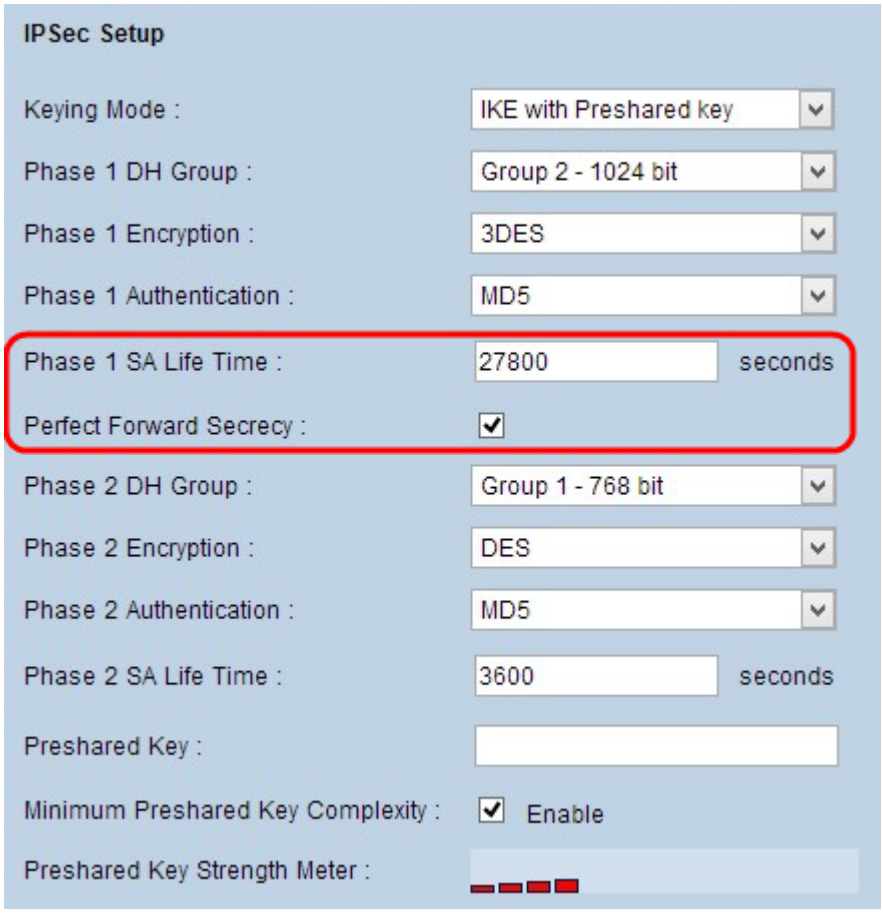
AES-256 — AES (Advanced Encryption Standard) é um método de criptografia de 256 bits que transforma o texto simples em texto cifrado através de 14 ciclos de repetições. AES-256 é o método de criptografia mais seguro.



Etapa 3. Escolha o método de autenticação da Fase 1 apropriado na lista suspensa Autenticação da Fase 1. O túnel VPN precisa usar o mesmo método de autenticação para as duas extremidades. SHA1 é recomendado.

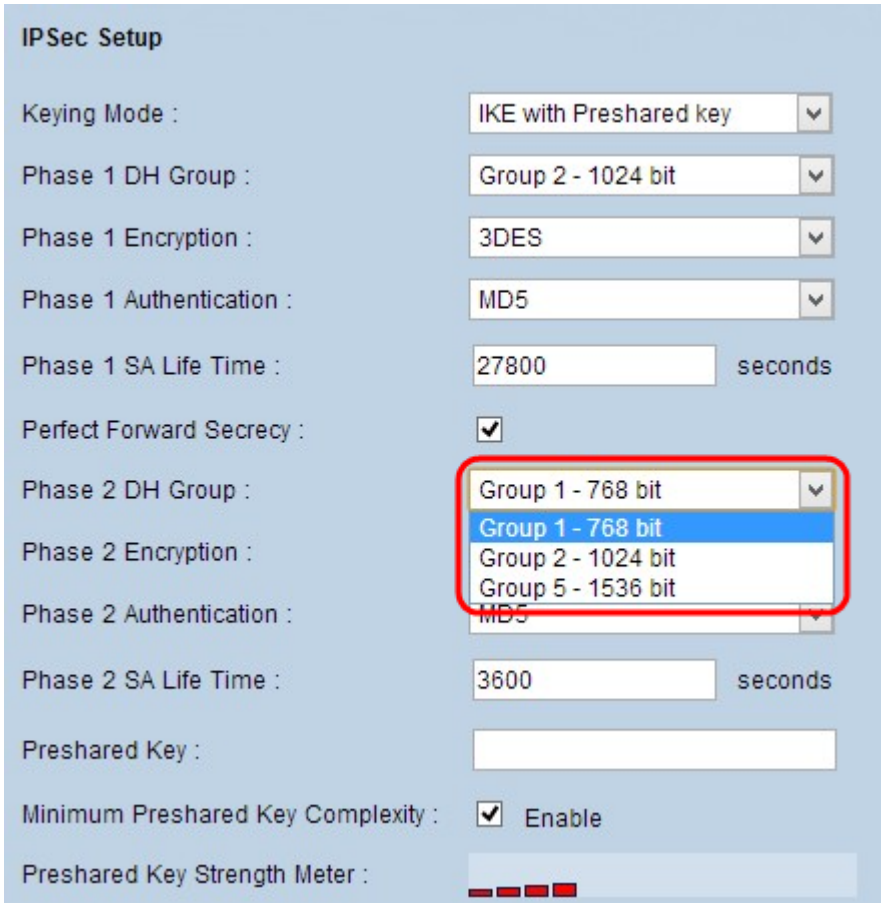
MD5 — Message Digest Algorithm-5 (MD5) é uma função de hash de 128 bits que fornece proteção aos dados contra ataques mal-intencionados pelo cálculo da soma de verificação.

SHA1 — O Secure Hash Algorithm versão 1 (SHA1) é uma função de hash de 160 bits mais segura que o MD5, mas leva mais tempo para computar.



Etapa 4. Insira a quantidade de tempo em segundos em que as chaves da Fase 1 são válidas e o túnel VPN permanece ativo no campo Período de vida da SA da Fase 1.

Etapa 5. Marque a caixa de seleção **Perfect Forward Secrecy (Sigilo total de encaminhamento) para fornecer mais proteção às chaves.** Essa opção permite que o roteador gere uma nova chave em caso de qualquer comprometimento da chave. Os dados criptografados são danificados apenas pela chave comprometida. Essa é uma ação recomendada, pois fornece mais segurança.

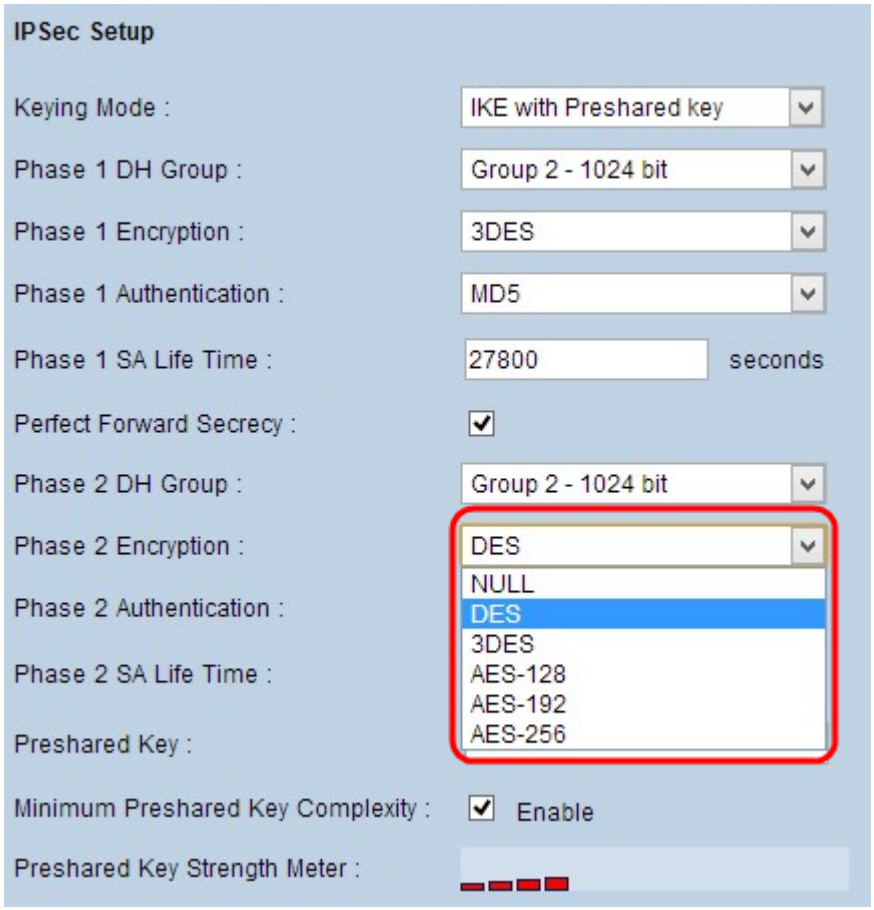


Etapa 6. Escolha o Grupo DH da Fase 2 apropriado na lista suspensa Grupo DH da Fase 2. A fase 2 usa a associação de segurança e é usada para determinar a segurança do pacote de dados à medida que ele passa pelos dois pontos finais.

Grupo 1 - 768 bits — A chave de força mais baixa e o grupo de autenticação mais inseguro, mas leva o menor tempo para computar as chaves IKE. Essa opção é preferida se a velocidade da rede for baixa.

Grupo 2 - 1024 bits — Uma chave de força maior e um grupo de autenticação mais seguro do que o grupo 1, mas leva mais tempo para computar as chaves IKE.

Grupo 5 - 1536 bits — A chave de força mais alta e o grupo de autenticação mais seguro. Precisa de mais tempo para computar as chaves de IKE. É preferível se a velocidade da rede for alta.



Passo 7. Escolha a Criptografia da Fase 2 apropriada para criptografar a chave na lista suspensa de Criptografia da Fase 2. AES-128, AES-192 ou AES-256 são recomendados. O túnel VPN precisa usar o mesmo método de criptografia para as duas extremidades.

NULL — Nenhuma criptografia é usada.

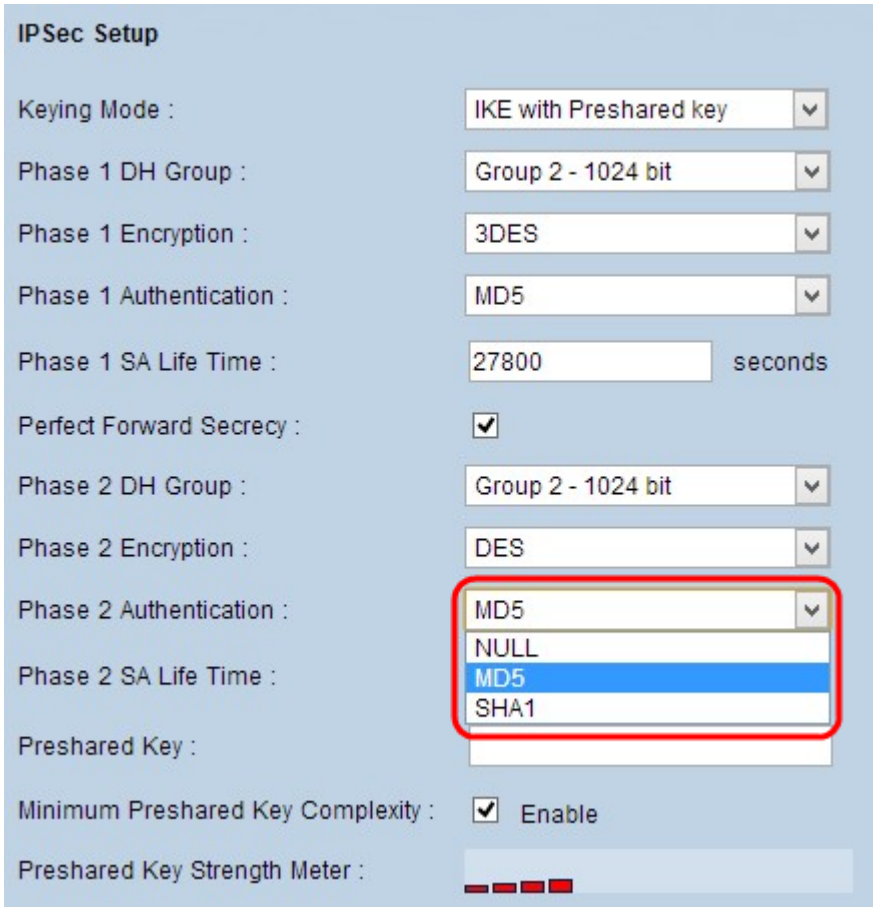
DES — O Data Encryption Standard (DES) usa um tamanho de chave de 56 bits para criptografia de dados. O DES está desatualizado e deve ser usado apenas se um endpoint for compatível apenas com DES.

3DES — O 3DES (Triple Data Encryption Standard) é um método de criptografia simples de 168 bits. O 3DES criptografa os dados três vezes, o que fornece mais segurança que o DES.

AES-128 — AES (Advanced Encryption Standard) é um método de criptografia de 128 bits que transforma o texto simples em texto cifrado através de repetições de 10 ciclos.

AES-192 — AES (Advanced Encryption Standard) é um método de criptografia de 192 bits que transforma o texto simples em texto cifrado através de 12 repetições de ciclo. AES-192 é mais seguro que AES-128.

AES-256 — AES (Advanced Encryption Standard) é um método de criptografia de 256 bits que transforma o texto simples em texto cifrado através de 14 repetições de ciclo. AES-256 é o método de criptografia mais seguro.

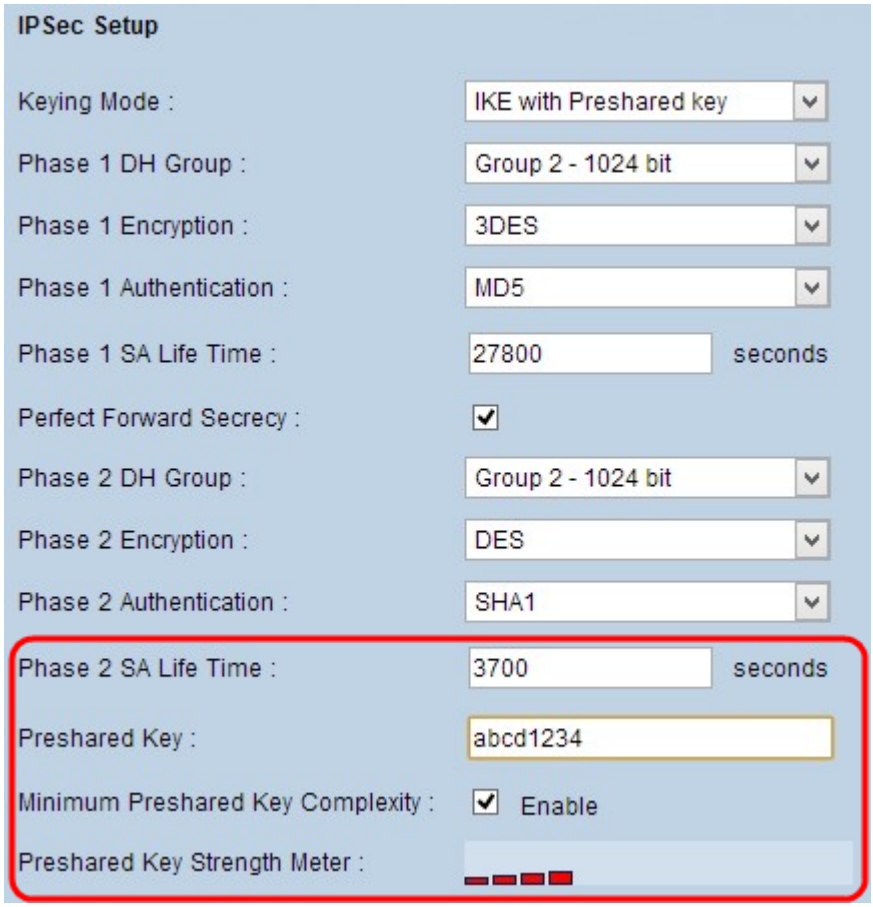


Etapa 8. Escolha o método de autenticação apropriado na lista suspensa Autenticação da Fase 2. O túnel VPN precisa usar o mesmo método de autenticação para ambas as extremidades. SHA1 é recomendado.

MD5 — Message Digest Algorithm-5 (MD5) é uma função hash hexadecimal de 128 bits que fornece proteção aos dados contra ataques mal-intencionados pelo cálculo da soma de verificação.

SHA1 — O Secure Hash Algorithm versão 1 (SHA1) é uma função de hash de 160 bits mais segura que o MD5, mas leva mais tempo para computar.

Nulo — Nenhum método de autenticação é usado.



Etapa 9. Insira a quantidade de tempo em segundos em que as chaves da Fase 2 são válidas e o túnel VPN permanece ativo no campo Período de vida da SA da Fase 2.

Etapa 10. Insira uma chave compartilhada anteriormente entre os peers IKE para autenticar os peers no campo Presshared Key (Chave pré-compartilhada). Até 30 hexadecimais e caracteres podem ser usados como chave pré-compartilhada. O túnel VPN precisa usar a mesma chave pré-compartilhada para ambas extremidades.

Note: É altamente recomendável alterar frequentemente a chave pré-compartilhada entre os peers IKE para que a VPN permaneça protegida.

Etapa 11. (Opcional) Se quiser ativar o medidor de intensidade para a chave pré-compartilhada, marque a caixa de seleção **Mínimo de complexidade da chave pré-compartilhada**. É usado para determinar a intensidade da chave pré-compartilhada através de barras coloridas.

Presshared Key Strength Meter — Mostra a força da chave pré-compartilhada através de barras coloridas. Vermelho indica intensidade fraca, amarelo indica intensidade aceitável e verde indica força forte.

Etapa 12. Clique em **Save (Salvar) para salvar as configurações.**

Note: Se você quiser configurar as opções disponíveis na seção *Avançado* para Gateway to Gateway VPN, consulte o artigo *Configuração avançada para Gateway para Gateway VPN em RV016, RV042, RV042G e RV082 VPN Routers*.

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.