Configuração de gateway para VPN (Virtual Private Network) de gateway em RV320 e RV325 VPN Router Series

Objetivo

As VPNs são usadas para formar conexões muito seguras em dois endpoints, através da 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 pareça fazer parte da mesma rede remota 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 lados da conexão para que seja estabelecida uma conexão VPN gateway a gateway bem-sucedida. A finalidade deste artigo é guiá-lo com a configuração de uma conexão VPN de gateway a gateway na série de roteadores VPN RV32x.

Dispositivos aplicáveis

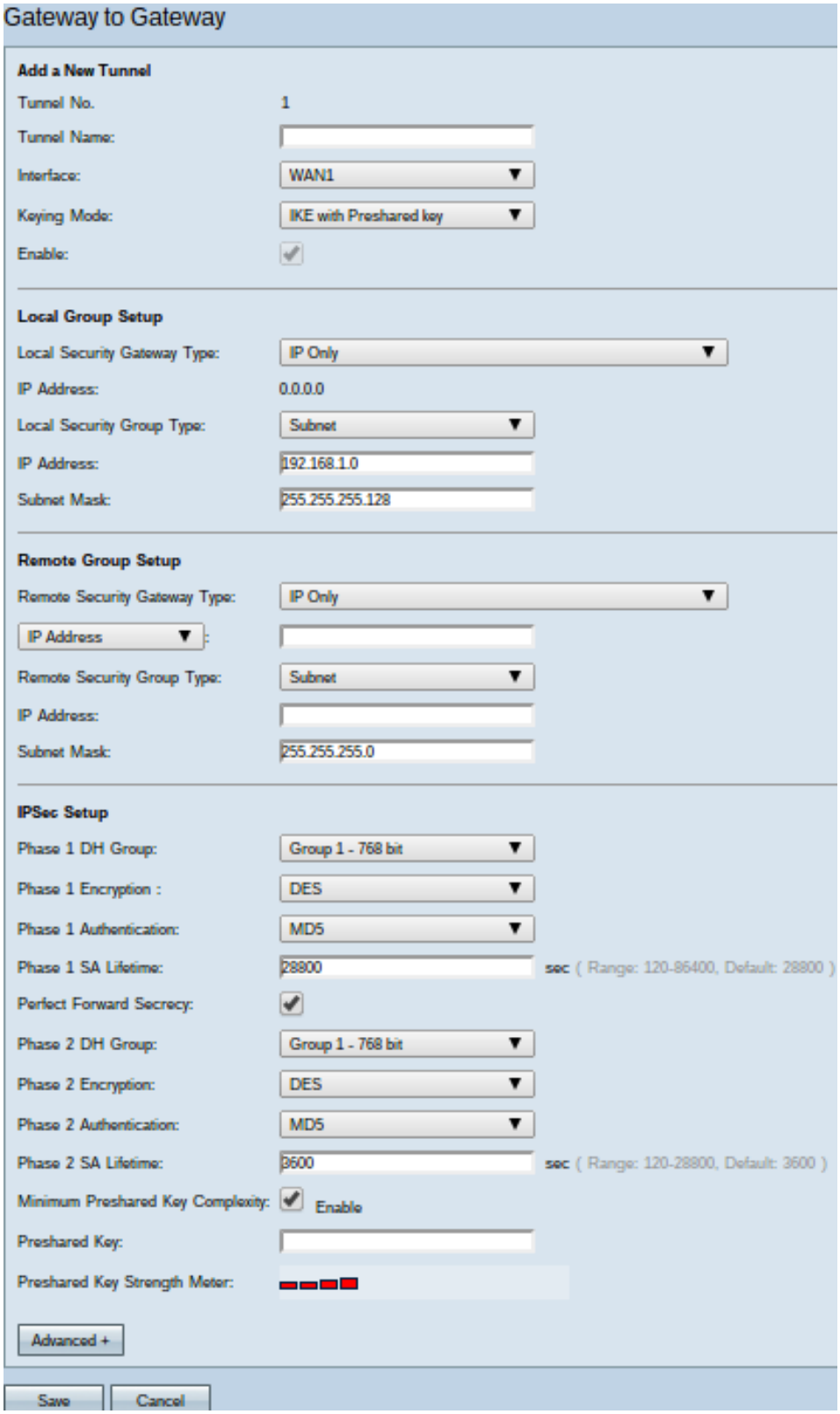
RV320 Roteador VPN WAN duplo
Roteador VPN WAN duplo RV325 Gigabit

Versão de software

•v1.1.0.09

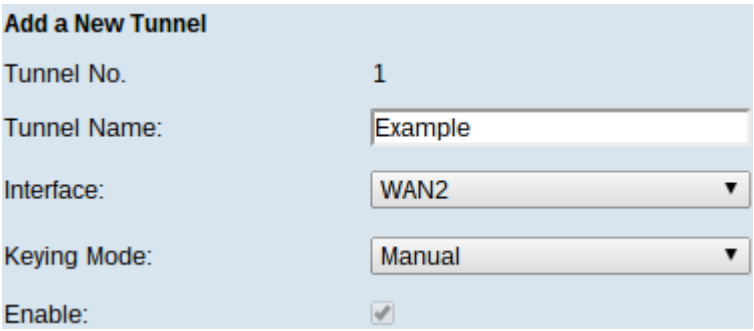
Gateway para Gateway

Etapa 1. Faça login no Utilitário de configuração da Web e escolha **VPN > Gateway to Gateway**. A página *Gateway to Gateway* é aberta:



Para que a conexão VPN funcione corretamente, os valores de Internet Protocol Security (IPSec) em ambos os lados da conexão devem ser os mesmos. Os dois lados da conexão devem pertencer a redes locais (LANs) diferentes e pelo menos um dos roteadores deve ser identificável por um endereço IP estático ou um nome de host DNS dinâmico.

Adicionar novo túnel



Túnel nº — Exibe o túnel atual que será criado. O roteador suporta 100 túneis.

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 do roteador.

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

USB1 — A porta USB1 do roteador. Só funciona se houver um dongle USB 3G/4G/LTE conectado à porta.

USB2 — A porta USB2 do roteador. Só funciona se houver um dongle USB 3G/4G/LTE conectado à porta.

Etapa 3. Na lista suspensa Modo de chaveamento, escolha a segurança do túnel a ser usada.

Manual — Essa opção permite que você configure manualmente a chave em vez de negociar a chave com o outro lado da conexão VPN.

IKE com chave pré-compartilhada — Escolha essa opção para ativar o Internet Key Exchange Protocol (IKE) que configura uma associação de segurança no túnel VPN. O IKE usa uma chave pré-compartilhada para autenticar um peer remoto.

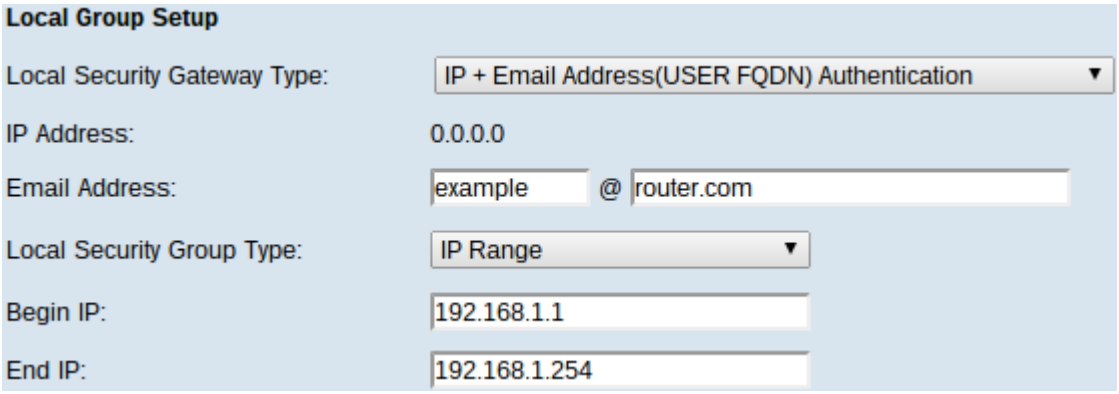
IKE com certificado — Escolha esta opção para ativar o protocolo IKE (Internet Key Exchange) com certificado que oferece uma maneira mais segura de gerar e trocar automaticamente chaves pré-compartilhadas para estabelecer comunicações mais autenticadas e seguras para o túnel.

Etapa 4. Marque a caixa de seleção Enable (Habilitar) para habilitar o túnel VPN. Por padrão, ele está ativado.

Configuração de grupo local

Essas configurações devem corresponder às configurações de "Grupo remoto" do roteador na outra extremidade do túnel VPN.

Note: Se Manual ou IKE com chave pré-compartilhada tiver sido selecionado na lista suspensa Modo de chaveamento da Etapa 3 de Adicionar um novo túnel, inicie da Etapa 1 e ignore as Etapas 2 a 4. Se IKE com certificado tiver sido selecionado, ignore a Etapa 1.



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

Somente IP — O acesso ao túnel é possível somente por meio de um IP de WAN estático. Você pode escolher essa opção se apenas o roteador tiver qualquer IP de WAN estático. O endereço IP de WAN estático é um campo gerado automaticamente.

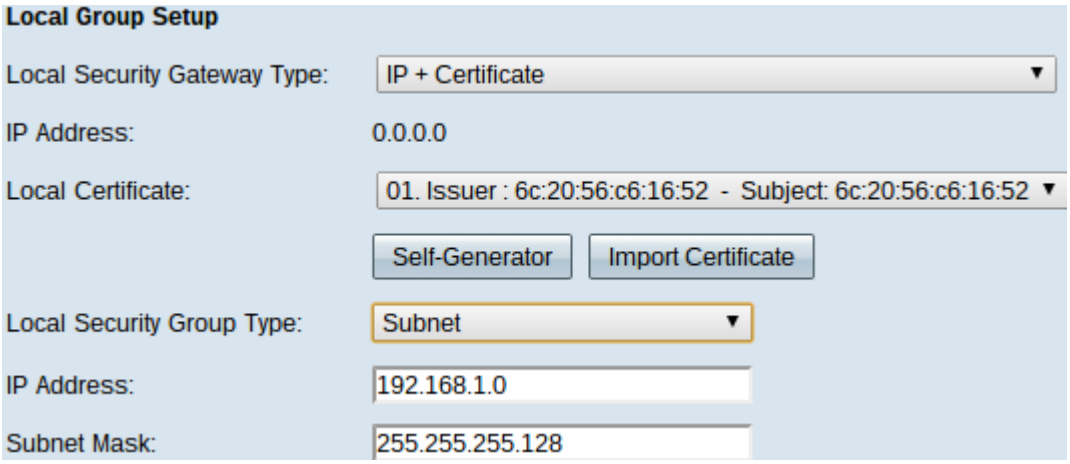
Autenticação IP + nome de domínio (FQDN) — O acesso ao túnel é possível por meio de um endereço IP estático e um domínio registrado. Se você escolher essa opção, digite o nome do domínio registrado no campo Domain Name (Nome do domínio). O endereço IP de WAN estático é um campo gerado automaticamente.

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 de WAN estático é um campo gerado automaticamente.

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).

Note: As alterações a seguir na área Configuração do grupo local mudam ao trabalhar com IKE com certificado.



A lista suspensa Tipo de gateway de segurança local torna-se ineditável e exibe IP + certificado. Este é o recurso de LAN que pode usar o túnel.
O campo Endereço IP exibe o endereço IP da WAN do dispositivo. Não é editável pelo

usuário.

Etapa 2. Escolha um certificado na lista suspensa Certificado local. Os certificados proporcionam uma segurança de autenticação mais forte nas conexões VPN.

Etapa 3. (Opcional) Clique no botão **Self-Generator** para exibir a janela *Certificate Generator* para configurar e gerar certificados.

Etapa 4. (Opcional) Clique no botão **Importar certificado** para exibir a janela *Meu certificado* para exibir e configurar certificados.

Etapa 5. Na lista suspensa Tipo de grupo de segurança local, escolha uma das seguintes opções:

Endereço IP — Essa opção permite especificar um dispositivo que pode usar esse túnel VPN. Você só precisa digitar o endereço IP do dispositivo no campo IP address (Endereço IP).

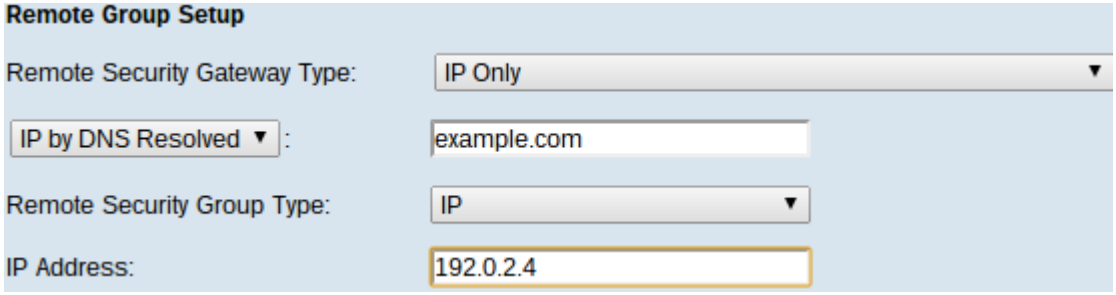
Sub-rede — Escolha esta opção para permitir que todos os dispositivos que pertencem à mesma sub-rede usem o túnel VPN. Você precisa inserir o endereço IP da rede no campo Endereço IP e sua respectiva máscara de sub-rede no campo Máscara de sub-rede.

Intervalo de IPs — Escolha esta opção para especificar um intervalo de dispositivos que podem usar o túnel VPN. Você precisa inserir o primeiro endereço IP e o último endereço IP do intervalo de dispositivos no campo Begin IP (IP inicial) e End IP (IP final).

Configuração do grupo remoto

Essas configurações devem corresponder às configurações do "Local Group Setup" do roteador na outra extremidade do túnel VPN.

Note: Se Manual ou IKE com chave pré-compartilhada tiver sido selecionado na lista suspensa Modo de chaveamento da Etapa 3 de Adicionar um novo túnel, inicie da Etapa 1 e ignore as Etapas 2 a 5. Ou se IKE com certificado foi selecionado ignore a Etapa 1.



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

Somente IP — O acesso ao túnel é possível somente 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. 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 de um domínio registrado do roteador. Se você souber o

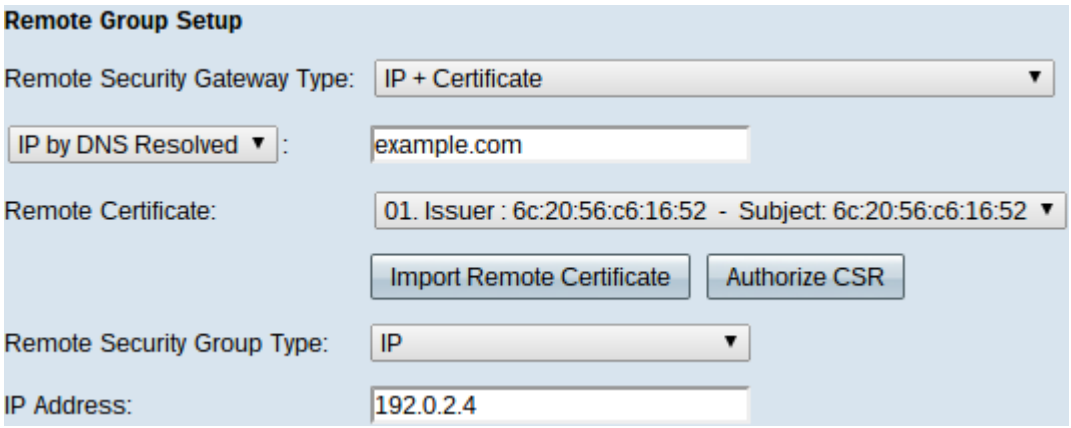
endereço IP do roteador remoto, escolha o endereço IP na lista suspensa diretamente abaixo do campo Tipo de gateway de segurança remota e insira o endereço. Escolha IP por DNS Resolvido se você não souber o endereço IP, mas souber o nome do domínio e insira o nome do domínio do roteador no campo IP by DNS Resolvido. Se você escolher essa opção, digite o nome do domínio registrado no campo Domain Name (Nome do domínio).

Autenticação IP + endereço de email (FQDN do USUÁRIO) — O acesso ao túnel é possível por meio de um endereço IP estático e um endereço de email.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).
Note: Se ambos os roteadores tiverem endereços IP dinâmicos, NÃO escolha Endereço IP Dinâmico + Endereço de E-mail para ambos os gateways.

Note: As seguintes alterações na área Configuração do grupo remoto mudam ao trabalhar com IKE com Certificado.



A lista suspensa Tipo de gateway de segurança remota se torna ineditável e exibe IP + certificado. Este é o recurso de LAN que pode usar o túnel.

Etapa 2. 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 remoto no campo IP by DNS Resolvido

Etapa 3. Escolha um certificado na lista suspensa Certificado remoto. Os certificados proporcionam uma segurança de autenticação mais forte nas conexões VPN.

Etapa 4. (Opcional) Clique no botão **Importar certificado remoto** para importar um novo certificado.

Etapa 5. (Opcional) Clique no botão **Autorizar CSR** para identificar o certificado com uma solicitação de assinatura digital.

Etapa 6. Na lista suspensa Tipo de grupo de segurança local, escolha uma das seguintes opções:

Endereço IP — Essa opção permite especificar um dispositivo que pode usar esse túnel VPN. Você só precisa digitar o endereço IP do dispositivo no campo IP address (Endereço IP).

Sub-rede — Escolha esta opção para permitir que todos os dispositivos que pertencem à mesma sub-rede usem o túnel VPN. Você precisa inserir o endereço IP da rede no campo Endereço IP e sua respectiva máscara de sub-rede no campo Máscara de sub-rede.

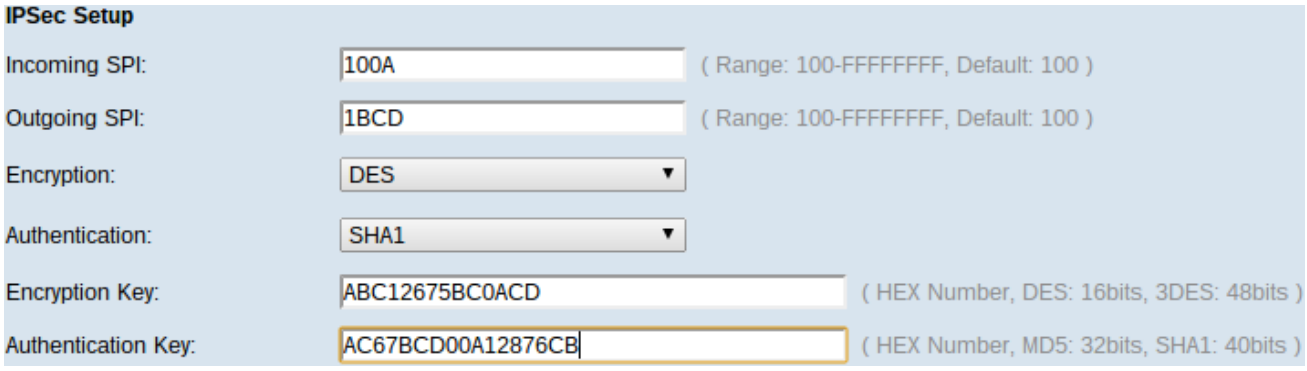
Intervalo de IPs — Escolha esta opção para especificar um intervalo de dispositivos que podem usar o túnel VPN. Você precisa inserir o primeiro endereço IP e o último endereço IP do intervalo de dispositivos. No campo Begin IP (IP inicial) e End IP (IP final).

Configuração do IPSec

Para que a criptografia seja configurada corretamente entre as duas extremidades do túnel VPN, ambas devem ter exatamente as mesmas configurações. Nesse caso, o IPSec cria uma autenticação segura entre os dois dispositivos. Fá-lo em duas fases.

Configuração de IPSec para modo de chave manual

Disponível somente se Manual tiver sido selecionado na lista suspensa Modo de Chaveamento da Etapa 3 de Adicionar um Novo Túnel. Este é um modo de segurança personalizado para gerar uma nova chave de segurança por si mesmo e para não negociar com a chave. É o melhor a ser usado durante a solução de problemas e o ambiente estático pequeno.



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, carga de segurança de encapsulamento) que, juntos, determinam a proteção para o pacote recebido. Você pode inserir de 100 a ffffffff.

Etapa 2. Insira o valor hexadecimal exclusivo para SPI no campo SPI de saída. O SPI é transportado no cabeçalho ESP que, em conjunto, determinam a proteção do pacote de saída. Você pode inserir de 100 a ffffffff.

Note: O SPI de entrada e saída deve corresponder entre si em ambas as extremidades para estabelecer um túnel.

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

DES — DES (Data Encryption Standard, Padrão de Criptografia de Dados) é um método de criptografia de 56 bits antigo, mais compatível com versões anteriores, que não é tão seguro quanto fácil de quebrar.

3DES — 3DES (Triple Data Encryption Standard) é um método de criptografia simples de 168 bits para aumentar o tamanho da chave através da criptografia dos dados por três vezes, o que oferece mais segurança do que DES.

Etapa 4. Escolha o método de autenticação apropriado na lista suspensa Autenticação. A autenticação recomendada é SHA1. O túnel VPN precisa usar o mesmo método de autenticação para as duas extremidades.

MD5 — MD5 (Message Digest Algorithm-5) representa uma função hash hexadecimal de 32 dígitos que fornece proteção aos dados contra ataques mal-intencionados pelo cálculo da soma de verificação.

SHA1 — SHA1 (Secure Hash Algorithm versão 1) é uma função de hash de 160 bits mais segura que MD5.

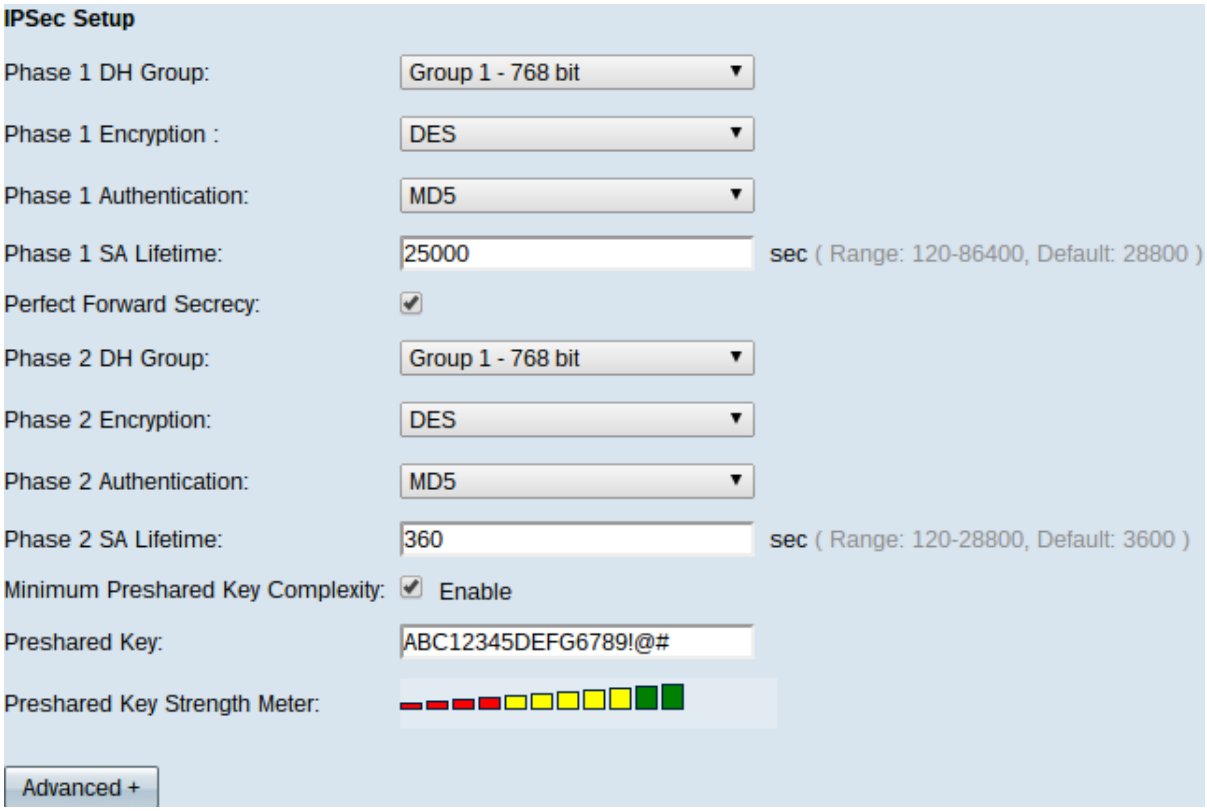
Etapa 5. Insira a chave para criptografar e descriptografar dados no campo Chave de criptografia. Se você escolher DES como método de criptografia na etapa 3, insira um valor hexadecimal de 16 dígitos. Se você escolher 3DES como método de criptografia na etapa 3, insira um valor hexadecimal de 40 dígitos.

Etapa 6. Insira uma chave pré-compartilhada para autenticar o tráfego no campo Authentication Key (Chave de autenticação). Se você escolher MD5 como método de autenticação na Etapa 4, insira um valor hexadecimal de 32 dígitos. Se você escolher SHA como método de autenticação na Etapa 4, insira um valor hexadecimal de 40 dígitos. O túnel VPN precisa usar a mesma chave pré-compartilhada para ambas extremidades.

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

Configuração de IPSec para IKE com chave pré-compartilhada

Disponível somente se IKE com chave pré-compartilhada tiver sido selecionado na lista suspensa Modo de chaveamento da Etapa 3 de Adicionar um novo túnel.



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. Diffie-Hellman (DH) é um protocolo de troca de chave de criptografia usado durante a conexão da Fase 1 para compartilhar uma chave secreta para autenticar a comunicação.

Grupo 1 - 768 bits — Representa a chave de maior intensidade 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.

Grupo 2 - 1024 bits — Representa uma chave de maior intensidade e um grupo de autenticação mais seguro. Ele precisa de algum tempo para computar as chaves IKE.

Grupo 5 - 1536 bits — Representa a menor chave forte e o grupo de autenticação mais inseguro. Ele precisa de menos tempo para computar as chaves IKE. É preferível se a velocidade da rede for baixa.

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 DES (Data Encryption Standard, Padrão de Criptografia de Dados) é um método de criptografia antigo de 56 bits, que não é um método de criptografia muito seguro no mundo de hoje.

3DES — O 3DES (Triple Data Encryption Standard) é um método de criptografia simples e de 168 bits para aumentar o tamanho da chave através da criptografia dos dados por três vezes, o que oferece 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 — É um método de criptografia de 192 bits que transforma o texto simples em

texto cifrado através de repetições de 12 ciclos.

AES-256 — É um método de criptografia de 256 bits que transforma o texto simples em texto cifrado através de repetições de 14 ciclos.

Etapa 3. Escolha o método de autenticação 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 — O algoritmo MD5 (Message Digest Algorithm-5) representa uma função hash hexadecimal de 32 dígitos que fornece proteção aos dados contra ataques mal-intencionados pelo cálculo da soma de verificação.

SHA1 — Uma função de hash de 160 bits mais segura que MD5.

Etapa 4. Insira o tempo em segundos durante o qual o túnel VPN permanece ativo no campo Período de vida da SA da Fase 1.

Etapa 5. Marque a caixa de seleção Perfect Forward Secsecret para fornecer mais proteção às chaves. Essa opção permite gerar uma nova chave se alguma chave for comprometida. Os dados criptografados são danificados apenas pela chave comprometida. Então, ela fornece comunicação mais segura e autêntica, pois protege outras chaves, embora uma chave esteja 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 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. DH é um protocolo de troca de chave criptográfica que é usado durante a conexão da Fase 1 para compartilhar a chave secreta para autenticar a comunicação.

Grupo 1 - 768 bits — Representa a chave de maior intensidade 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.

Grupo 2 - 1024 bits — Representa uma chave de maior intensidade e um grupo de autenticação mais seguro. Ele precisa de algum tempo para computar as chaves IKE.

Grupo 5 - 1536 bits — Representa a menor chave forte e o grupo de autenticação mais inseguro. Ele precisa de menos tempo para computar as chaves IKE. É preferível se a velocidade da rede for baixa.

Note: Como nenhuma chave nova não é gerada, você não precisa configurar o Grupo DH da Fase 2 se desmarcar Perfect Forward Secsecret na Etapa 5.

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.

DES — DES é um método de criptografia antigo de 56 bits, que não é um método de criptografia muito seguro no mundo de hoje.

3DES — 3DES é um método de criptografia simples de 168 bits para aumentar o tamanho da chave por meio da criptografia dos dados por três vezes, o que oferece mais segurança que o DES.

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

AES-192 — É um método de criptografia de 192 bits que transforma o texto simples em texto cifrado através de repetições de 12 ciclos.

AES-256 — É um método de criptografia de 256 bits que transforma o texto simples em texto cifrado através de repetições de 14 ciclos.

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 as duas extremidades.

MD5 — MD5 representa uma função hash hexadecimal de 32 dígitos que fornece proteção aos dados contra ataques mal-intencionados pelo cálculo de checksum.

SHA1 — O Secure Hash Algorithm versão 1 (SHA1) é uma função de hash de 160 bits mais segura que o MD5.

Nulo — Nenhum método de autenticação é usado.

Etapa 9. Insira o tempo em segundos durante o qual o túnel VPN permanece ativo no campo Período de vida da SA da Fase 2.

Etapa 10. Marque a caixa de seleção Minimum Preshared Key Complexity (Complexidade mínima de chave pré-compartilhada) se deseja ativar o medidor de força da chave pré-compartilhada.

Etapa 11. Insira uma chave compartilhada anteriormente entre os pares IKE no campo Presshared Key (Chave pré-compartilhada). Até 30 hexadecimais e caracteres podem ser usados como uma chave pré-compartilhada. O túnel VPN precisa usar a mesma chave pré-compartilhada para ambas extremidades.

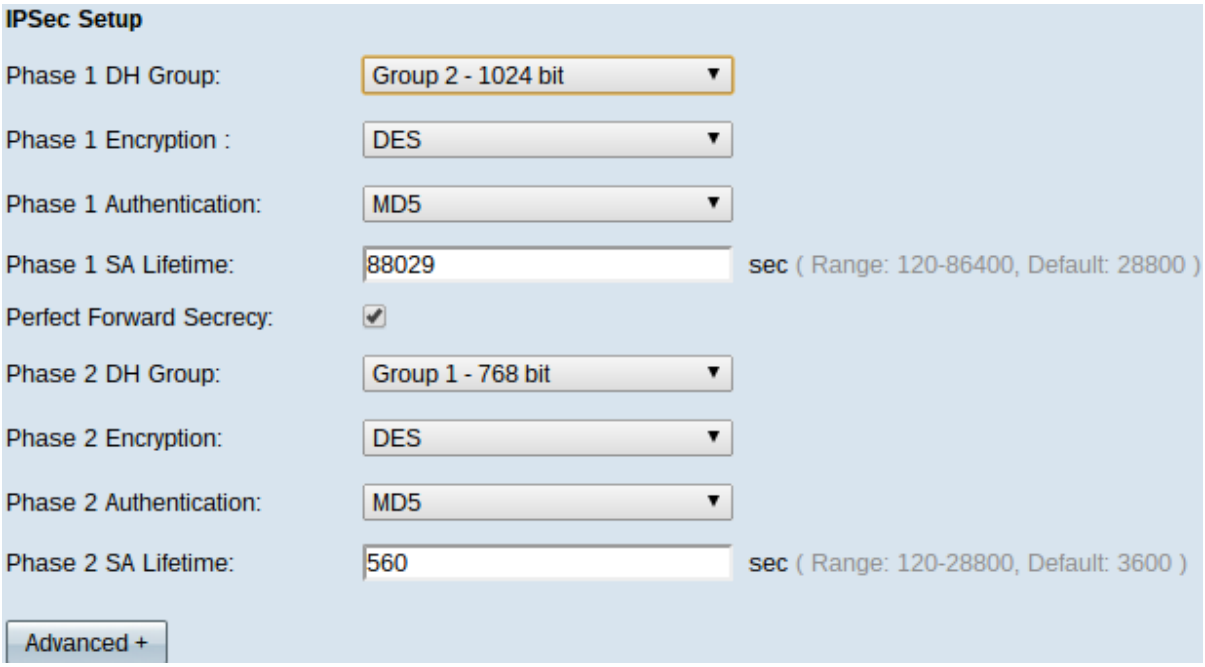
Note: É altamente recomendável alterar frequentemente a chave pré-compartilhada entre os peers IKE para que a VPN permaneça segura.

O Medidor de força da chave pré-compartilhada mostra a força da chave pré-compartilhada através das barras de cor. O vermelho indica uma força fraca, amarelo indica força aceitável e verde indica força alta.

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

Configuração de IPSec para IKE com certificado

Disponível somente se IKE com certificado tiver sido selecionado na lista suspensa Modo de chaveamento da Etapa 3 de Adicionar um novo túnel.



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 SA (Security Association) lógica e simplex entre as duas extremidades do túnel para suportar a comunicação de autenticação segura. DH é um protocolo de troca de chave criptográfica que é usado durante a conexão da Fase 1 para compartilhar a chave secreta para autenticar a comunicação.

Grupo 1 - 768 bits — Representa a chave de maior intensidade e o grupo de autenticação mais seguro. Mas precisa de mais tempo para computar as chaves IKE. É preferível se a velocidade da rede for alta.

Grupo 2 - 1024 bits — Representa uma chave de maior intensidade e um grupo de autenticação mais seguro. Mas precisa de algum tempo para computar as chaves de IKE.

Grupo 5 - 1536 bits — Representa a menor chave forte e o grupo de autenticação mais inseguro. Ele precisa de menos tempo para computar as chaves IKE. É preferível se a velocidade da rede for baixa.

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 — DES é um método de criptografia antigo de 56 bits, que não é um método de criptografia muito seguro no mundo de hoje.

3DES — 3DES é um método de criptografia simples de 168 bits para aumentar o tamanho da chave por meio da criptografia dos dados por três vezes, o que oferece mais segurança que o DES.

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

AES-192 — É um método de criptografia de 192 bits que transforma o texto simples em texto cifrado através de repetições de 12 ciclos.

AES-256 — É um método de criptografia de 256 bits que transforma o texto simples em texto cifrado através de repetições de 14 ciclos.

Etapa 3. Escolha o método de autenticação 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 — MD5 representa uma função hash hexadecimal de 32 dígitos que fornece proteção aos dados contra ataques mal-intencionados pelo cálculo de checksum.

SHA1 — Uma função de hash de 160 bits mais segura que MD5.

Etapa 4. Insira o tempo em segundos durante o qual o túnel VPN permanece ativo no campo Período de vida da SA da Fase 1.

Etapa 5. Marque a caixa de seleção Perfect Forward Secsecret para fornecer mais proteção às chaves. Essa opção permite gerar uma nova chave se alguma chave for comprometida. Os dados criptografados são danificados apenas pela chave comprometida. Assim, ele fornece uma comunicação mais segura e autenticada, pois protege outras chaves quando outra chave é 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 1 é usada para estabelecer o SA lógico e simples entre as duas extremidades do túnel para suportar a comunicação de autenticação segura. DH é um protocolo de troca de chave criptográfica que é usado durante a conexão da Fase 1 para compartilhar a chave secreta para autenticar a comunicação.

Grupo 1 - 768 bits — Representa a chave de maior intensidade e o grupo de autenticação mais seguro. Mas precisa de mais tempo para computar as chaves IKE. É preferível se a velocidade da rede for alta.

Grupo 2 - 1024 bits — Representa uma chave de maior intensidade e um grupo de autenticação mais seguro. Mas precisa de algum tempo para computar as chaves de IKE.

Grupo 5 - 1536 bits — Representa a menor chave forte e o grupo de autenticação mais inseguro. Ele precisa de menos tempo para computar as chaves IKE. É preferível se a velocidade da rede for baixa.

Note: Como nenhuma chave nova não é gerada, você não precisa configurar o Grupo DH da Fase 2 se você desmarcou Perfect Forward Secsecret na Etapa 5.

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.

DES — DES é um método de criptografia antigo de 56 bits, que não é um método de criptografia muito seguro no mundo de hoje.

3DES — 3DES é um método de criptografia simples de 168 bits para aumentar o tamanho da chave por meio da criptografia dos dados por três vezes, o que oferece mais segurança que o DES.

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

AES-192 — É um método de criptografia de 192 bits que transforma o texto simples em texto cifrado através de repetições de 12 ciclos.

AES-256 — É um método de criptografia de 256 bits que transforma o texto simples em texto cifrado através de repetições de 14 ciclos.

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 as duas extremidades.

MD5 — MD5 representa uma função hash hexadecimal de 32 dígitos que fornece proteção aos dados contra ataques mal-intencionados pelo cálculo de checksum.

SHA1 — SHA1 é uma função de hash de 160 bits mais segura que MD5.

Nulo — Nenhum método de autenticação é usado.

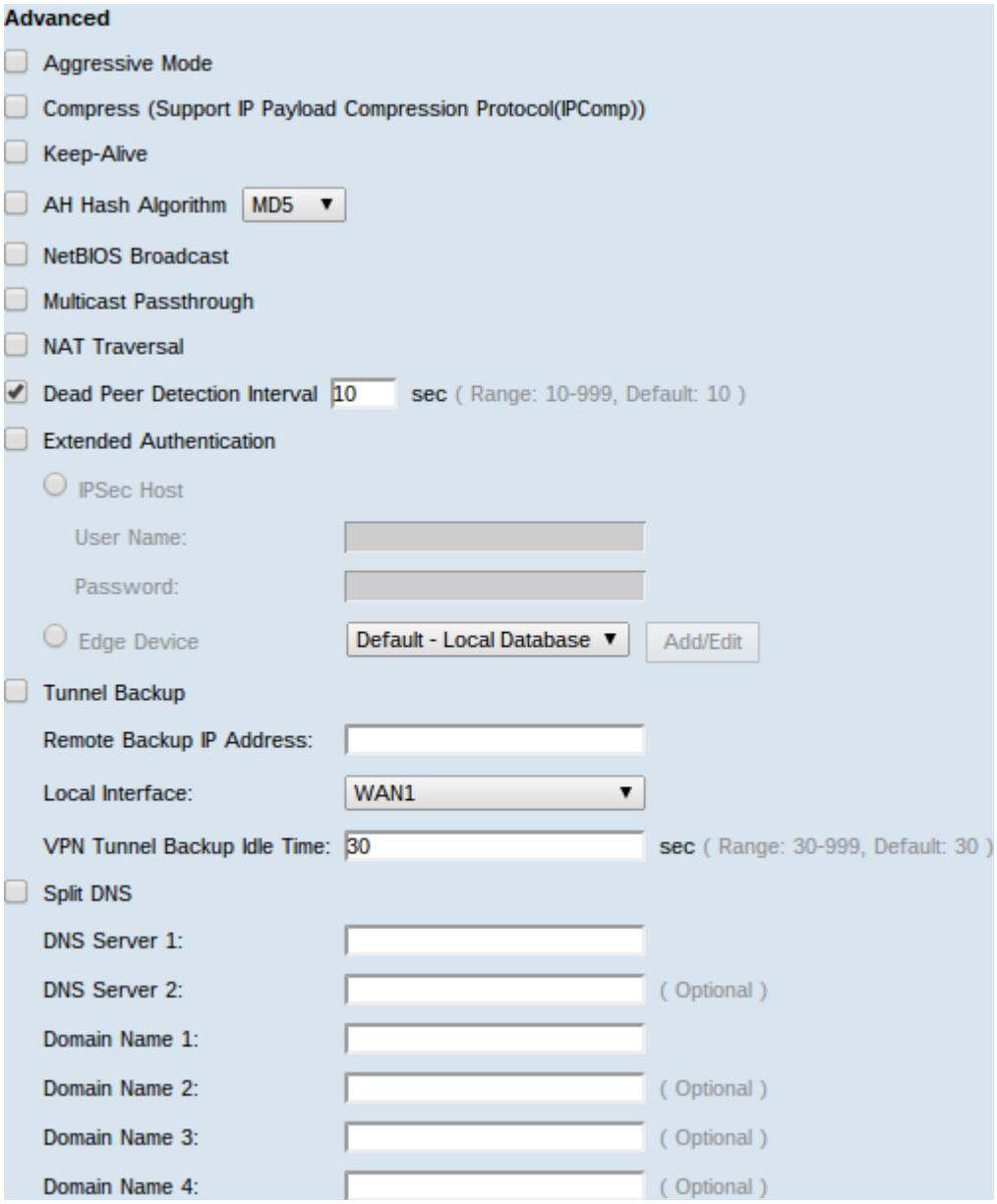
Etapa 9. Insira o tempo em segundos durante o qual o túnel VPN permanece ativo no campo Período de vida da SA da Fase 2.

Etapa 10. Clique em **Save (Salvar) para salvar as configurações.**

(Opcional) Configuração avançada de IPSec para IKE com certificado e IKE com chave pré-compartilhada

As opções avançadas estarão disponíveis se IKE com certificado ou IKE com chave pré-carregada tiver sido selecionado na lista suspensa Modo de chaveamento da Etapa 3 de Adicionar um novo túnel. As mesmas configurações estão disponíveis para os dois tipos de modos de chaveamento.

Etapa 1. Clique no botão **Avançado+** para exibir as opções avançadas de IPSec.



Etapa 2. Marque a caixa de seleção Modo agressivo se a velocidade da rede estiver baixa. Ele troca as IDs dos pontos finais do túnel em texto claro durante a conexão SA, o que requer menos tempo para troca, mas menos segurança.

Etapa 3. Marque a caixa de seleção Compress (Support IP Payload Compression Protocol (IPComp)) (Comprimir [protocolo de compressão de payload IP]) se quiser compactar o tamanho do datagrama IP. O IPComp é um protocolo de compactação IP usado para compactar o tamanho do datagrama IP, se a velocidade da rede for baixa e o usuário quiser transmitir os dados rapidamente, sem nenhuma perda, através da rede lenta.

Etapa 4.Marque a caixa de seleção Keep-Alive se você sempre quiser que a conexão do túnel VPN permaneça ativa. Ele ajuda a restabelecer as conexões imediatamente se alguma conexão ficar inativa.

Etapa 5. Marque a caixa de seleção AH Hash Algorithm se quiser autenticar o Authenticate Header (AH). O AH fornece autenticação para a origem dos dados, a integridade dos dados através do checksum e a proteção é estendida no cabeçalho IP. O túnel deve ter o mesmo algoritmo para ambos os lados.

MD5 — MD5 representa uma função hash hexadecimal de 128 dígitos que fornece proteção aos dados contra ataques mal-intencionados pelo cálculo de checksum.

SHA1 — SHA1 é uma função de hash de 160 bits mais segura que MD5.

Etapa 6. Marque NetBios Broadcast (Transmissão NetBIOS) se desejar permitir o tráfego não roteável pelo túnel VPN. O padrão é desmarcado. NetBIOS é usado para detectar recursos de rede (como impressoras, computadores etc.) na rede por meio de alguns aplicativos de software e recursos do Windows, como o ambiente de rede.

Passo 7. Se o roteador VPN estiver por trás de um gateway NAT, marque a caixa para ativar a passagem NAT. A Network Address Translation (NAT) permite que os usuários com endereços LAN privados acessem recursos da Internet usando um endereço IP publicamente roteável como o endereço de origem. No entanto, para o tráfego de entrada, o gateway NAT não tem um método automático de converter o endereço IP público em um destino específico na LAN privada. Esse problema evita trocas bem-sucedidas de IPSec. O NAT Traversal configura essa conversão de entrada. A mesma configuração deve ser usada em ambas as extremidades do túnel.

Etapa 8. Marque Dead Peer Detection Interval (Intervalo de detecção de par inativo) para verificar a atividade do túnel VPN por Hello ou ACK de forma periódica. Se você marcar essa caixa de seleção, insira a duração ou o intervalo em segundos das mensagens de saudação desejadas.

Etapa 9. Marque Autenticação Estendida para usar um nome de usuário e senha de host IPSec para autenticar clientes VPN ou para usar o banco de dados encontrado no Gerenciamento de Usuário. Isso deve ser ativado em ambos os dispositivos para que funcione. Clique no botão de opção **Host IPSec** para usar o nome de usuário e o host IPSec e insira o nome de usuário e a senha no campo Nome de usuário e no campo Senha. Ou clique no botão de opção **Edge Device** para usar um banco de dados. Escolha o banco de dados desejado na lista suspensa Dispositivo de borda.

Etapa 10. Marque a caixa de seleção Tunnel Backup (Backup de túnel) para habilitar o backup de túnel. Este recurso está disponível quando o Intervalo de detecção de peer inoperante foi verificado. O recurso permite que o dispositivo restabeleça o túnel VPN através de uma interface WAN alternativa ou endereço IP.

Remote Backup IP Address — Um IP alternativo para o peer remoto. Insira ou o IP da WAN já definido para o gateway remoto neste campo.

Local Interface — A interface WAN usada para restabelecer a conexão. Escolha a interface desejada na lista suspensa.

Tempo ocioso de backup do túnel VPN — O tempo escolhido para quando usar o túnel de backup se o túnel primário não estiver conectado. Digite-o em segundos.

Etapa 11. Marque a caixa de seleção Dividir DNS para ativar o DNS dividido. Este recurso permite enviar solicitação DNS a um servidor DNS definido com base em nomes de domínio especificados. Insira os nomes dos servidores DNS nos campos Servidor DNS 1 e Servidor DNS 2 e insira os nomes de domínio nos campos Número do nome do domínio.

Etapa 12. Clique em **Salvar** para concluir a configuração do dispositivo.