

Configurar um túnel de acesso remoto (cliente para gateway) para clientes VPN em roteadores VPN RV016, RV042, RV042G e RV082

Objetivo

Este artigo explica como configurar o túnel VPN (Virtual Private Network) de acesso remoto do cliente para o gateway, nos roteadores RV016, RV042, RV042G e RV082 VPN com a ajuda do software cliente VPN de terceiros como The Green Bow ou VPN Tracker.

Introdução

Uma VPN é uma rede privada usada para conectar virtualmente dispositivos do usuário remoto, através da rede pública com o objetivo de fornecer segurança. A VPN do túnel de acesso remoto é o processo usado para configurar uma VPN entre um computador cliente e uma rede. O cliente é configurado no desktop ou notebook dos usuários por meio do software de cliente VPN. Ele permite que os usuários se conectem de forma segura e remota à rede. A conexão VPN do cliente com o gateway é útil para funcionários remotos se conectarem à rede do escritório de forma segura e remota.

Dispositivos aplicáveis

- RV016
- RV042
- RV042G
- RV082

Versão de software

- v4.2.2.08

Configurar um túnel VPN

Etapa 1. Faça login no utilitário de configuração da Web e escolha **VPN > Client to Gateway**. A página *Client to Gateway (Cliente para gateway)* é exibida:

Client To Gateway

Add a New Tunnel

Tunnel Group VPN

Tunnel No. 1

Tunnel Name :

Interface : ▼

Enable :

Local Group Setup

Local Security Gateway Type : ▼

IP Address : 0.0.0.0

Local Security Group Type : ▼

IP Address :

Subnet Mask :

Remote Client Setup

Remote Security Gateway Type : ▼

▼ :

IPSec Setup

Adicionar novo túnel

Etapa 1. Clique no botão de opção apropriado de acordo com o tipo de túnel que deseja adicionar.

- Tunnel (Túnel) - representa um túnel para um único usuário remoto.
- Group VPN (VPN de grupo) - representa um túnel para um grupo remoto de usuários.

Client To Gateway

Add a New Tunnel

Tunnel Group VPN

Tunnel No. : 1

Tunnel Name :

Interface :

Enable :

Local Group Setup

Local Security Gateway Type :

IP Address : 0.0.0.0

Local Security Group Type :

IP Address :

Subnet Mask :

Remote Client Setup

Remote Security Gateway Type :

:

IPSec Setup

O Tunnel Number (Número do túnel) é um campo gerado automaticamente que exibe o número do túnel.

Client To Gateway

Add a New Tunnel

Tunnel Group VPN

Tunnel No. 1

Tunnel Name : tunnel_1

Interface : WAN1

Enable :

Local Group Setup

Local Security Gateway Type : IP Only

IP Address : 0.0.0.0

Local Security Group Type : Subnet

IP Address : 192.168.1.0

Subnet Mask : 255.255.255.0

Remote Client Setup

Remote Security Gateway Type : IP Only

IP Address :

IPSec Setup

Etapa 2. Digite um nome para o túnel no campo Tunnel Name (Nome do túnel).

Etapa 3. Escolha a interface WAN apropriada para usar para o túnel VPN na lista suspensa Interface.

Etapa 4. (Opcional) Para ativar a VPN, marque a caixa de seleção no campo Enable (Ativar). Por padrão, ela é sempre marcada.

Configuração de grupo local

Etapa 1. Escolha o método apropriado de identificação do roteador para estabelecer um túnel VPN na lista suspensa *Local Security Gateway*. Pule esta etapa se escolher a VPN de grupo na etapa 1 da seção *Add A New Tunnel* (Adicionar um novo túnel).

Client To Gateway

Add a New Tunnel

Tunnel Group VPN

Tunnel No. : 1

Tunnel Name : tunnel_1

Interface : WAN1

Enable :

Local Group Setup

Local Security Gateway Type : IP Only

IP Address : [auto-generated]

Local Security Group Type : [auto-generated]

IP Address : [auto-generated]

Subnet Mask : 255.255.255.0

Remote Client Setup

Remote Security Gateway Type : IP Only

IP Address : [auto-generated]

IPSec Setup

Keying Mode : IKE with Preshared key

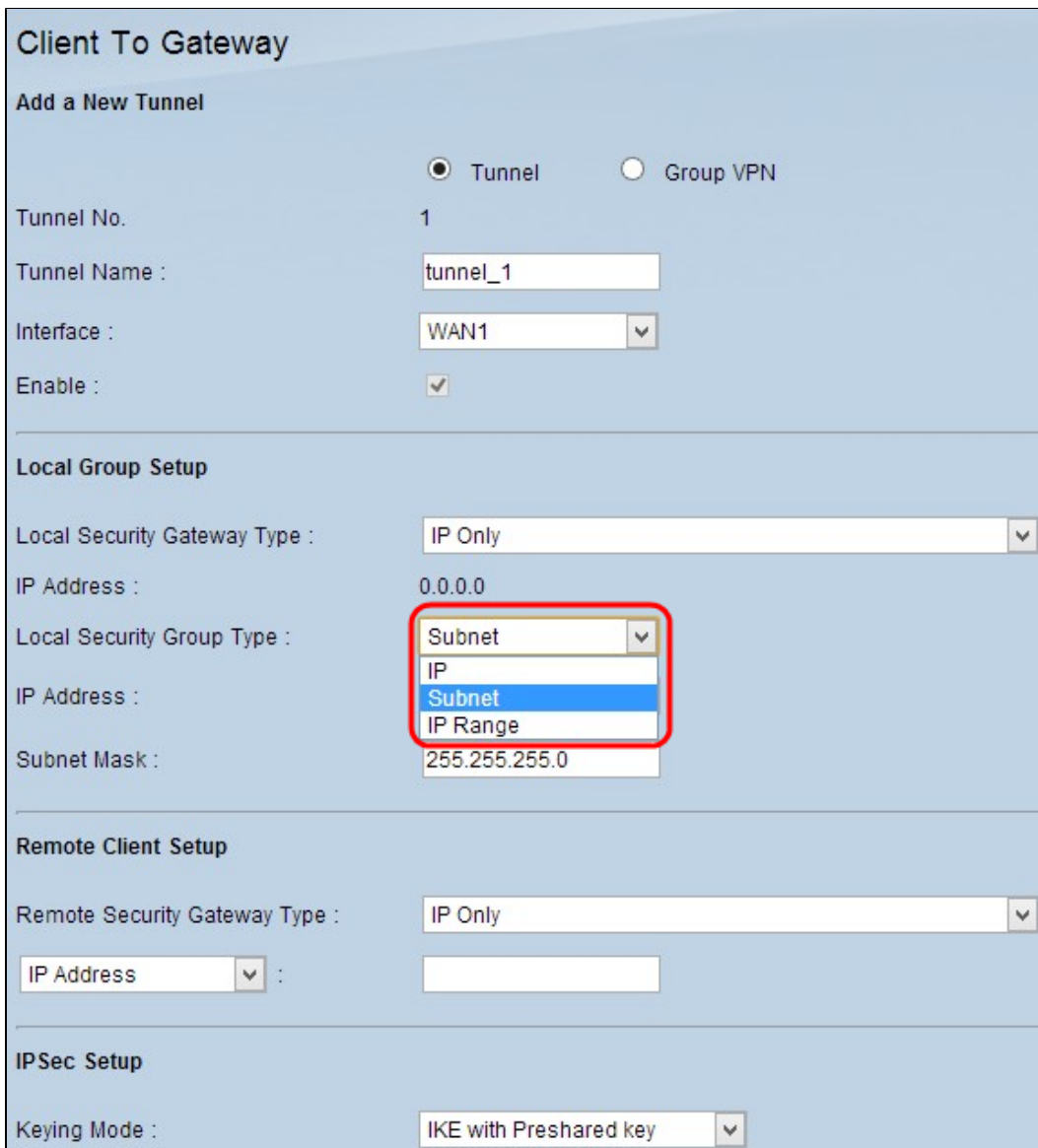
- **IP Only (Somente IP)** - o acesso ao túnel é possível através de um endereço IP de WAN estático. Você pode escolher essa opção somente se o roteador tiver um IP de WAN estático. O endereço IP de WAN estático aparece automaticamente.
- **IP + Domain Name(FQDN) Authentication (Autenticação de IP + nome de domínio[FQDN])** - o acesso ao túnel é possível através de um endereço IP estático e de um nome de domínio totalmente qualificado (FQDN) registrado. O endereço IP de WAN estático é um campo gerado automaticamente.
- **IP + E-mail Address(USER FQDN) Authentication (Autenticação de IP + endereço de e-mail [FQDN do usuário])** - o acesso ao túnel é possível através de um endereço IP estático e um endereço de e-mail. O endereço IP de WAN estático é um campo gerado automaticamente.
- **Dynamic IP + Domain Name(FQDN) Authentication (Autenticação de IP dinâmico + nome de domínio [FQDN])** - o acesso ao túnel é possível através de um endereço IP dinâmico e um domínio registrado.
- **Dynamic IP + E-mail Address(USER FQDN) Authentication (Autenticação de IP dinâmico + endereço de e-mail [FQDN do usuário])** - o acesso ao túnel é possível através de um endereço IP dinâmico e um endereço de e-mail.

Etapa 2. Insira o nome do domínio totalmente qualificado registrado no campo Domain Name (Nome de domínio) se você escolher *IP + Domain Name (FQDN) Authentication* ou *Dynamic IP + Domain Name (FQDN) Authentication (Autenticação de IP + Domain Name (FQDN))* na Etapa 1.

Etapa 3. Insira o endereço de e-mail no campo Email Address (Endereço de e-mail) se escolher *IP + E-mail Address (USER FQDN) Authentication* ou *Dynamic IP + E-mail Address (USER FQDN) Authentication* na Etapa 1.

Etapa 4. Escolha o usuário da LAN local ou o grupo de usuários apropriado que pode acessar o túnel VPN na lista suspensa *Local Security Group*. O padrão é Subnet (Sub-rede).

- IP - Somente um dispositivo de 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). O IP padrão é 192.168.1.0.
- Subnet (Sub-rede) - todos os dispositivos de LAN em uma sub-rede específica podem acessar o túnel. Se você escolher essa opção, digite o endereço IP e a máscara de sub-rede dos dispositivos de LAN nos campos IP Address (Endereço IP) e Subnet Mask (Máscara de sub-rede), respectivamente. O valor padrão é 255.255.255.0.
- Intervalo IP (IP Range) - uma faixa de dispositivos de 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. O intervalo padrão é de 192.168.1.0 a 192.168.1.254.



Client To Gateway

Add a New Tunnel

Tunnel Group VPN

Tunnel No. : 1

Tunnel Name : tunnel_1

Interface : WAN1

Enable :

Local Group Setup

Local Security Gateway Type : IP Only

IP Address : 0.0.0.0

Local Security Group Type : Subnet

IP Address :

Subnet Mask : 255.255.255.0

Remote Client Setup

Remote Security Gateway Type : IP Only

IP Address :

IPSec Setup

Keying Mode : IKE with Preshared key

Etapa 5. Clique em **Save (Salvar)** para salvar as configurações.

Configuração de cliente remoto

Etapa 1. Se escolher Tunnel (Túnel), escolha o método de identificação do cliente apropriado para estabelecer um túnel VPN na lista suspensa *Remote Security Gateway Type (Tipo de gateway de segurança local)*. O padrão é IP somente. Pule esta etapa se escolher a VPN de grupo na etapa 1 da seção *Add A New Tunnel* (Adicionar um novo túnel).

Client To Gateway

Add a New Tunnel

Tunnel Group VPN

Tunnel No. : 1

Tunnel Name :

Interface :

Enable :

Local Group Setup

Local Security Gateway Type :

IP Address : 0.0.0.0

Local Security Group Type :

IP Address :

Subnet Mask :

Remote Client Setup

Remote Security Gateway Type :

IP Address :

IPSec Setup

Keying Mode :

- IP Only (Somente IP) - o acesso ao túnel é possível somente através de um IP de WAN do cliente. Você deve saber o IP de WAN estático do cliente para usar essa opção.
- IP + Domain Name(FQDN) Authentication (Autenticação de IP + nome de domínio [FQDN]) - o acesso ao túnel é possível através de um endereço IP estático do cliente e um domínio registrado.
- IP + E-mail Address(USER FQDN) Authentication (Autenticação de IP + endereço de e-mail [FQDN do usuário]) - o acesso ao túnel é possível através de um endereço IP estático do cliente e um endereço de e-mail.
- Dynamic IP + Domain Name(FQDN) Authentication (Autenticação de IP dinâmico + nome de domínio [FQDN]) - o acesso ao túnel é possível através de um endereço IP dinâmico do cliente e um domínio registrado.
- Dynamic IP + E-mail Address(USER FQDN) Authentication (Autenticação de IP dinâmico + endereço de e-mail [FQDN do usuário]) - o acesso ao túnel é possível através de um endereço IP dinâmico do cliente e um endereço de e-mail.

Etapa 2. Insira o endereço IP do cliente remoto no campo *IP Address* se você escolher *IP Only*, *IP + Domain Name (FQDN)* ou *IP + E-mail Address (User FQDN)* na Etapa 1.

Etapa 3. Escolha a opção apropriada na lista suspensa para inserir o endereço IP se souber ou resolver o endereço IP do servidor DNS se escolher *IP Only* ou *IP + Domain Name (FQDN) Authentication* ou *IP + E-mail Address(USER FQDN) Authentication* na Etapa 1.

- IP Address (Endereço IP) - representa o endereço IP estático do cliente remoto. Insira o endereço IP no campo fornecido.
- IP by DNS Resolved (IP por DNS resolvido) - representa o nome de domínio do endereço IP que

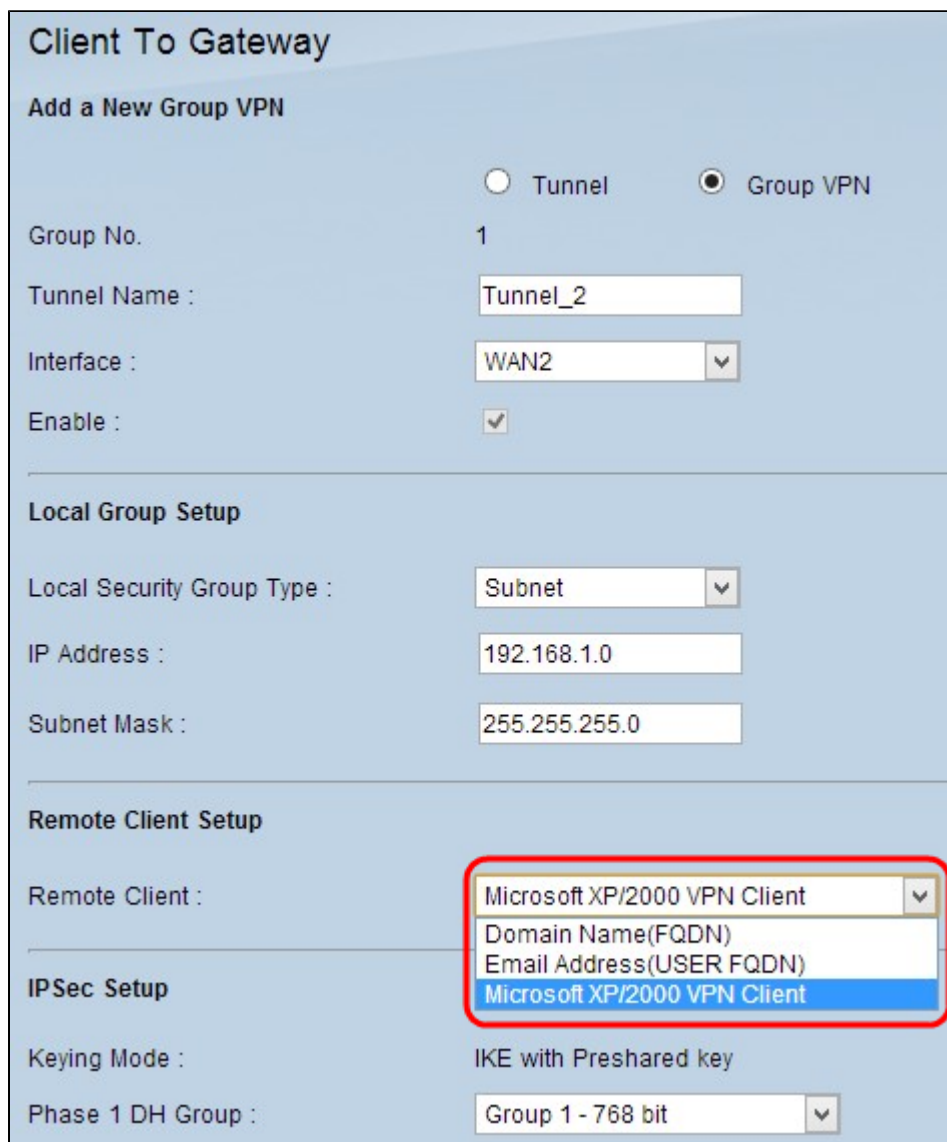
recupera o endereço IP automaticamente pelo servidor DNS local, se você não souber o endereço IP estático do cliente remoto. Digite o nome do domínio do endereço IP no campo.

Etapa 4. Insira o nome de domínio do endereço IP no campo Domain name (Nome de domínio) se escolher *IP + Domain Name (FQDN) Authentication* ou *Dynamic IP + Domain Name (FQDN) Authentication* na Etapa 1.

Etapa 5. Insira o endereço de e-mail no campo Email Address (Endereço de e-mail) se escolher *IP + E-mail Address (USER FQDN) Authentication* ou *Dynamic IP + E-mail Address (USER FQDN) Authentication* na Etapa 1.

Etapa 6. Se você escolher Group (Grupo), selecione o tipo de cliente remoto apropriado na lista suspensa *Remote Client (Cliente remoto)*. Pule esta etapa se escolher a VPN de túnel na etapa 1 da seção *Add A New Tunnel* (Adicionar um novo túnel).

- Domain Name(FQDN) (Nome de domínio [FQDN]) - o acesso ao túnel é possível através de um domínio registrado. Se você escolher essa opção, digite o nome do domínio registrado no campo Domain Name (Nome do domínio).
- End. de e-mail (FQDN do usuário) - O acesso ao túnel é possível através de um endereço de e-mail do cliente. Se você escolher esta opção, digite o endereço de e-mail no campo Email Address (Endereço de e-mail).
- Cliente VPN Microsoft XP/2000 - o acesso ao túnel é possível através do software Microsoft XP ou Microsoft Windows 2000. Usuários remotos com software VPN cliente Microsoft podem acessar o túnel pelo software.



Client To Gateway

Add a New Group VPN

Tunnel Group VPN

Group No. 1

Tunnel Name : Tunnel_2

Interface : WAN2

Enable :

Local Group Setup

Local Security Group Type : Subnet

IP Address : 192.168.1.0

Subnet Mask : 255.255.255.0

Remote Client Setup

Remote Client : Microsoft XP/2000 VPN Client

Domain Name(FQDN)

Email Address(USER FQDN)

Microsoft XP/2000 VPN Client

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 bit

Passo 7. 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.

Observação: duas extremidades da VPN precisam ter os mesmos métodos de criptografia, descriptografia e autenticação para que o IPSec funcione. Além disso, a chave de sigilo de encaminhamento perfeito deve ser a mesma em ambos os lados do túnel.

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

- Manual - um modo de segurança personalizado para gerar sozinho uma nova chave de segurança e nenhuma negociação com a chave. É o melhor a ser usado durante a solução de problemas e o ambiente estático pequeno. Se você escolher a VPN de grupo na etapa 1 da seção Add A New Tunnel (Adicionar novo túnel), essa opção estará desativada.
- IKE with Preshared key (IKE com chave pré-compartilhada) - o protocolo IKE (Internet Key Exchange) é usado para gerar e trocar automaticamente uma chave pré-compartilhada e estabelecer a comunicação de autenticação para o túnel.

Subnet Mask : 255.255.255.0

Remote Client Setup

Remote Security Gateway Type : IP Only

IP Address : 192.168.1.2

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group :

Phase 1 Encryption : DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 28800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

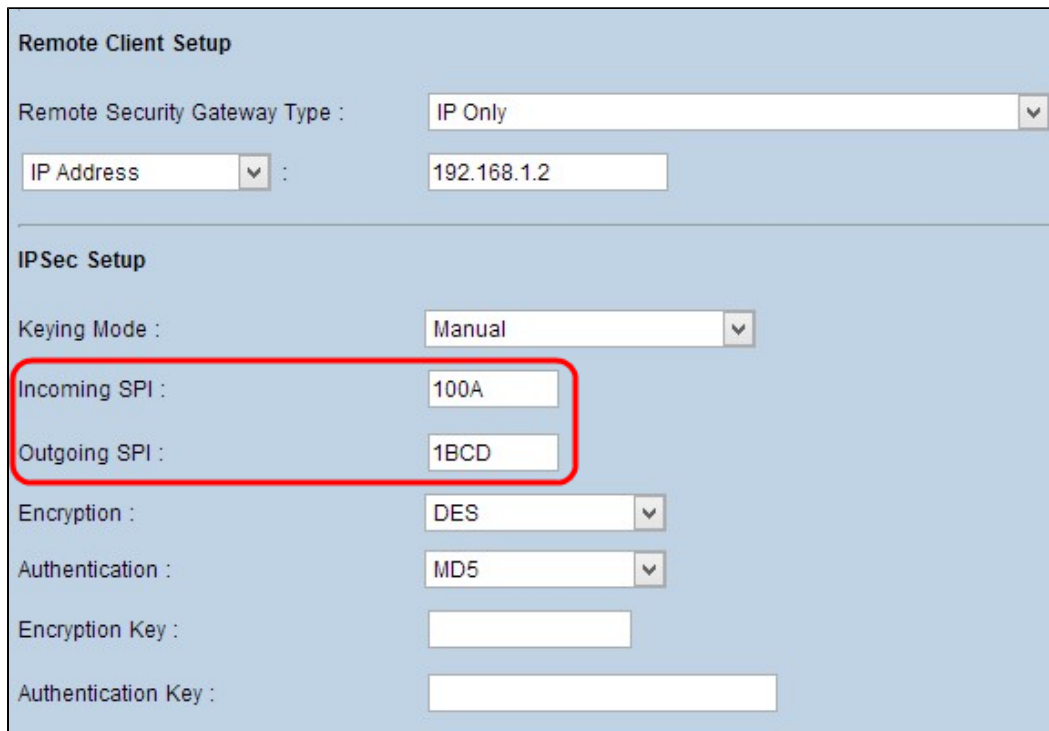
Preshared Key Strength Meter :

Advanced +

Configuração de modo de chave manual

Etapa 1. Insira o valor hexadecimal exclusivo para o Índice de parâmetro de segurança (SPI) de entrada no campo *SPI de entrada*. O SPI é transportado no cabeçalho do protocolo ESP (Encapsulating Security Payload), que, quando associado, determina a proteção para o pacote de entrada. Você pode inserir de 100 a ffffffff. 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*. O SPI é transportado no cabeçalho do protocolo ESP (Encapsulating Security Payload), que, quando associado, determina a proteção para o pacote de saída. Você pode inserir de 100 a ffffffff. O SPI de saída do roteador remoto precisa corresponder ao SPI de entrada do roteador local.



Remote Client Setup

Remote Security Gateway Type : IP Only

IP Address : 192.168.1.2

IPSec Setup

Keying Mode : Manual

Incoming SPI : 100A

Outgoing SPI : 1BCD

Encryption : DES

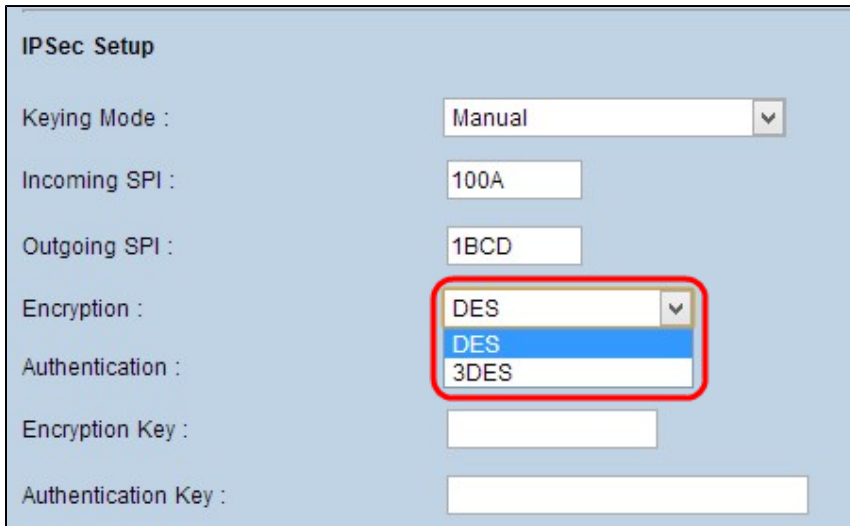
Authentication : MD5

Encryption Key :

Authentication Key :

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 para ambas as extremidades.

- DES - 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.



IPSec Setup

Keying Mode : Manual

Incoming SPI : 100A

Outgoing SPI : 1BCD

Encryption : DES

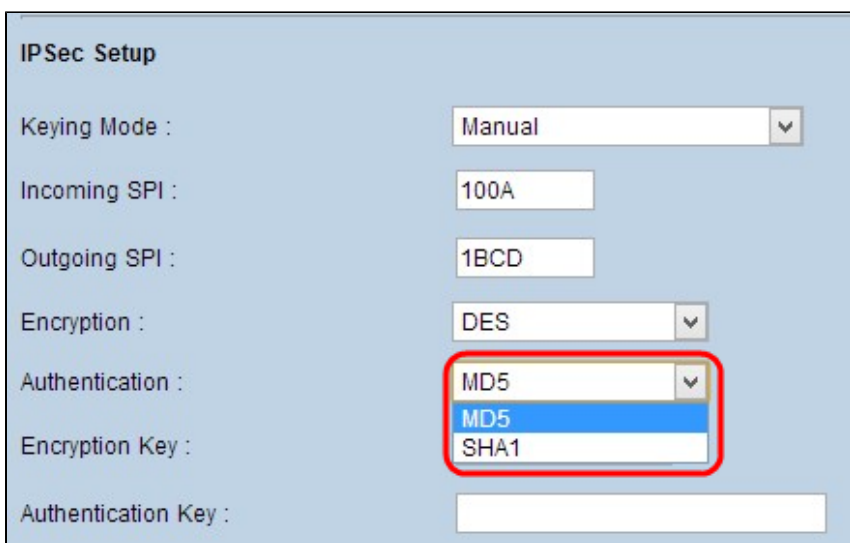
Authentication : DES
3DES

Encryption Key :

Authentication Key :

Etapa 4. Escolha o método de autenticação apropriado para os dados na lista suspensa *Authentication*. 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) representa a função de hash hexadecimal de 32 dígitos que fornece proteção aos dados contra ataques mal-intencionados pelo cálculo da soma de verificação.
- SHA1 - Secure Hash Algorithm versão 1 (SHA1) é uma função de hash de 160 bits que é mais segura que a MD5, mas leva mais tempo para ser computada.



IPSec Setup

Keying Mode : Manual

Incoming SPI : 100A

Outgoing SPI : 1BCD

Encryption : DES

Authentication : MD5
MD5
SHA1

Encryption Key :

Authentication Key :

Etapa 5. Insira a chave para criptografar e descriptografar dados no campo *Encryption Key*. 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*. Se você escolher o método de autenticação MD5 na etapa 4, insira o valor hexadecimal de 32 dígitos. Se você escolher o método de autenticação SHA na etapa 4, insira o valor hexadecimal de 40 dígitos. O túnel VPN precisa usar a mesma chave pré-compartilhada para ambas as extremidades.

IPSec Setup

Keying Mode :	Manual
Incoming SPI :	100A
Outgoing SPI :	1BCD
Encryption :	DES
Authentication :	MD5
Encryption Key :	ABC12675BC0ACD
Authentication Key :	AC67BCD00A12876CB

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. Porém, leva menos tempo para computar as chaves de IKE. Essa opção é preferida se a velocidade da rede for baixa.
- Grupo 2 - 1024 bits - a chave de força mais alta e o grupo de autenticação mais seguro. Mas precisa de algum tempo para computar as chaves de IKE.
- Grupo 5 - 1.536 bits - representa 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.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 bit

Phase 1 Encryption : Group 1 - 768 bit

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 28800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter :

Advanced +

Etapa 2. Escolha a Criptografia da fase 1 apropriada para criptografar a chave na lista suspensa *Criptografia da fase 1*. O 3DES é recomendado, pois é o método de criptografia mais seguro. O túnel VPN precisa usar o mesmo método de criptografia para as duas extremidades.

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

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 bit

Phase 1 Encryption : DES

Phase 1 Authentication : DES

Phase 1 SA Life Time : 3600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

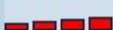
Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

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.

- MD5 - Message Digest Algorithm-5 (MD5) representa a função de hash hexadecimal de 32 dígitos que fornece proteção aos dados contra ataques mal-intencionados pelo cálculo da soma de verificação.
- SHA1 - Secure Hash Algorithm versão 1 (SHA1) é uma função de hash de 160 bits que é mais segura que a MD5, mas leva mais tempo para ser computada.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 bit

Phase 1 Encryption : DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 3600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit


Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

Advanced +

Etapa 4. Digite o tempo em segundos em que as chaves da Fase 1 são válidas e o túnel VPN permanece ativo no campo *Fase 1 SA Life Time*.

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. 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.

IPSec Setup

Keying Mode :

Phase 1 DH Group :

Phase 1 Encryption :

Phase 1 Authentication :

Phase 1 SA Life Time : seconds

Perfect Forward Secrecy :

Phase 2 DH Group :


Phase 2 Encryption :

Phase 2 Authentication :

Phase 2 SA Life Time : seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

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 para determinar a segurança do pacote de dados ao passar através dos dois endpoints.

- Grupo 1 - 768 bits - representa a chave de força mais baixa e o grupo de autenticação mais inseguro. Mas precisa de menos tempo para computar as chaves de IKE. É preferível se a velocidade da rede for baixa.
- Grupo 2 - 1024 bits - representa a chave de força mais alta e o grupo de autenticação mais seguro. Mas precisa de algum tempo para computar as chaves de IKE.
- Grupo 5 - 1.536 bits - representa 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.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : DES

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 27600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

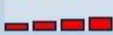
Phase 2 Encryption : MD5

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

Passo 7. Escolha a Criptografia da fase 2 apropriada para criptografar a chave na lista suspensa *Criptografia da fase 2*. O AES-256 é recomendado, pois é o método de criptografia mais seguro. O túnel VPN precisa usar o mesmo método de criptografia para as duas extremidades.

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

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : DES

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 27600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

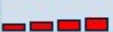
Phase 2 Encryption : DES

Phase 2 Authentication : **DES**

Phase 2 SA Life Time :

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

Advanced +

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.

- MD5 - Message Digest Algorithm-5 (MD5) representa a função de hash hexadecimal de 32 dígitos que fornece proteção aos dados contra ataques mal-intencionados pelo cálculo da soma de verificação.
- SHA1 - Secure Hash Algorithm versão 1 (SHA1) é uma função de hash de 160 bits que é mais segura que a MD5, mas leva mais tempo para ser computada.
- Null (Nulo) - Nenhum método de autenticação é usado.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : DES

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 27600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time :

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter :

Advanced +

Etapa 9. Digite o tempo em segundos em que as chaves da Fase 2 são válidas e o túnel VPN permanece ativo no campo *Fase 2 SA Life Time*.

Etapa 10. Insira uma chave compartilhada anteriormente entre os pares IKE para autenticar os pares no campo *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.

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

Etapa 11. 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. É usada para determinar a força da chave pré-compartilhada em barras de cores

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

IPSec Setup

Keying Mode :

Phase 1 DH Group :

Phase 1 Encryption :

Phase 1 Authentication :

Phase 1 SA Life Time : seconds

Perfect Forward Secrecy :

Phase 2 DH Group :

Phase 2 Encryption :

Phase 2 Authentication :

Phase 2 SA Life Time : seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter :

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

IKE avançado com configuração do modo de chave pré-compartilhada

Etapa 1. Clique em **Avançado** para exibir as configurações avançadas para IKE com chave pré-compartilhada.

Advanced

Aggressive Mode

Compress (Support IP Payload Compression Protocol(IPComp))

Keep-Alive

AH Hash Algorithm

NetBIOS Broadcast

NAT Traversal

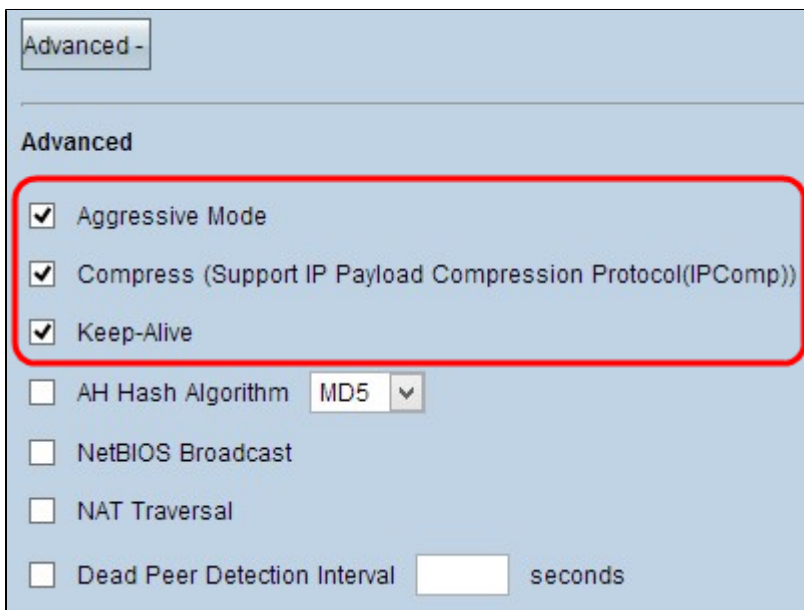
Dead Peer Detection Interval seconds

Etapa 2. Marque a caixa de seleção **Aggressive Mode (Modo agressivo)** se a velocidade da rede for **baixa**. Isso troca as IDs dos endpoints do túnel em texto não criptografado durante a conexão do SA (fase 1), o que requer menos tempo para a troca, porém oferece menor segurança.

Observação: o Modo Agressivo não está disponível para a conexão VPN de cliente de grupo para gateway.

Etapa 3. Marque a caixa de seleção **Compress (Support IP Payload Compression Protocol (IPComp))** se quiser compactar o tamanho dos datagramas IP. IPComp é um protocolo de compactação de IP usado para compactar o tamanho do datagrama IP. A compactação de IP é útil se a velocidade da rede é baixa e o usuário deseja transmitir rapidamente os dados sem qualquer perda, mesmo com a rede lenta, porém não oferece segurança.

Etapa 4. Marque a caixa de seleção **Keep-Alive (Manter ativa)**, se você quiser que a conexão do túnel VPN esteja sempre ativa. Keep Alive (Manter ativa) ajuda a restabelecer as conexões imediatamente se alguma conexão se tornar inativa.



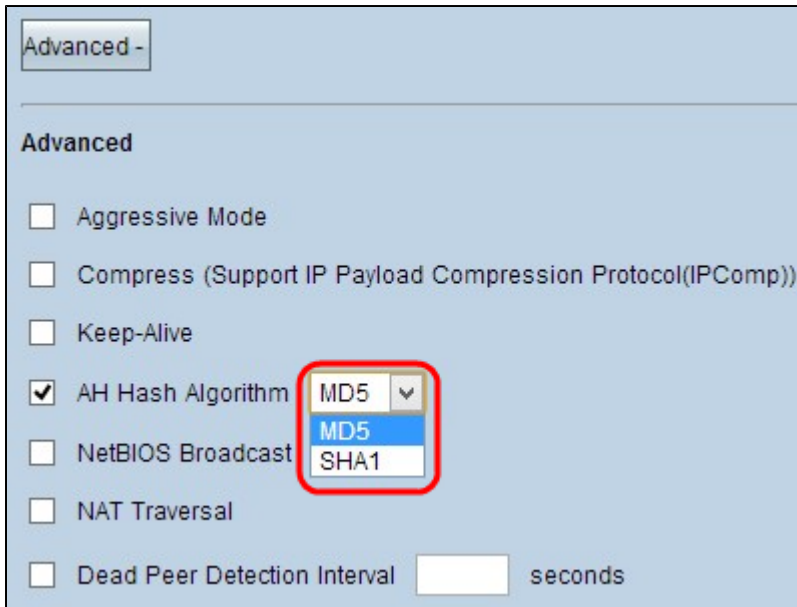
Advanced -

Advanced

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm MD5
- NetBIOS Broadcast
- NAT Traversal
- Dead Peer Detection Interval seconds

Etapa 5. Marque a caixa de seleção **AH Hash Algorithm (Algoritmo hash AH)**, se quiser ativar o **cabeçalho de autenticação (AH)**. O AH fornece autenticação para dados de origem, integridade de dados por meio de soma de verificação e proteção no cabeçalho IP. O túnel deve ter o mesmo algoritmo para ambos os lados.

- MD5 - Message Digest Algorithm-5 (MD5) representa a função de hash hexadecimal de 128 dígitos que fornece proteção aos dados contra ataques mal-intencionados pelo cálculo da soma de verificação.
- SHA1 - Secure Hash Algorithm versão 1 (SHA1) é uma função de hash de 160 bits que é mais segura que a MD5, mas leva mais tempo para ser computada.

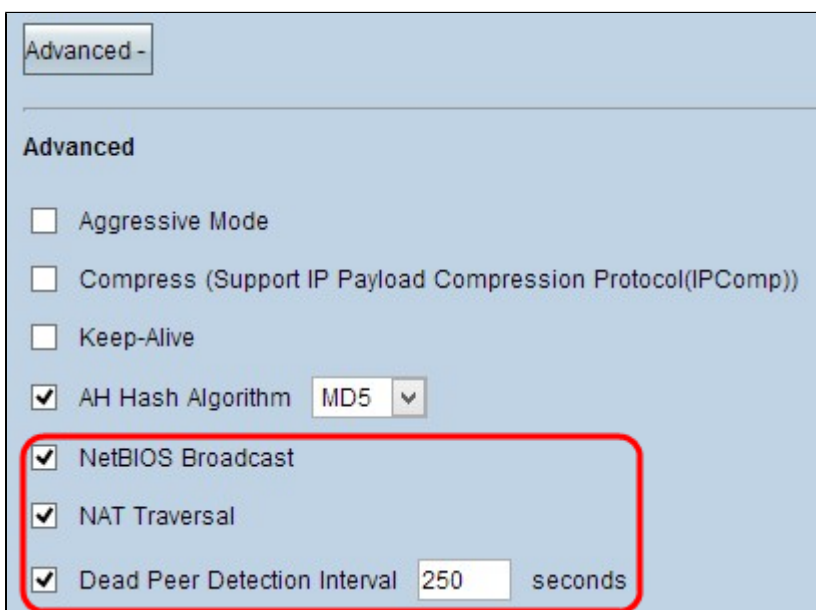


Etapa 6. Marque **NetBios Broadcast (Transmissão NetBIOS)** se desejar permitir o tráfego não roteável pelo túnel VPN. O padrão é desmarcado. NetBIOS é usado para detectar recursos de rede (como impressoras, computadores etc.) na rede por meio de alguns aplicativos de software e recursos do Windows,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

Passo 7. Marque a caixa de seleção **NAT Traversal (Travessia NAT)** se quiser acessar a Internet da LAN privada, por meio de um endereço IP público. Se o roteador VPN estiver atrás de um gateway NAT, marque essa caixa de seleção para ativar a travessia de NAT. Ambas as extremidades do túnel devem ter as mesmas configurações.

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 marcar essa caixa de seleção, insira a duração ou o intervalo desejado das mensagens de Hello.

Observação: você pode configurar o Intervalo de detecção de ponto inativo somente para uma conexão VPN de cliente para gateway, não para uma conexão VPN de cliente para gateway de grupo.



Etapa 9. Clique em **Save (Salvar)** para salvar as configurações.

Agora, você já sabe configurar o túnel de VPN de acesso remoto do cliente para o gateway nos roteadores VPN RV016, RV042, RV042G e RV082.

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.