

Configurar um único cliente para a VPN (Virtual Private Network) de gateway nos roteadores VPN RV320 e RV325

Objetivo

O objetivo deste documento é mostrar a você como configurar um único cliente para o gateway Virtual Private Network (VPN) em RV32x Series VPN Routers.

Introduction

Uma VPN é uma rede privada usada para conectar virtualmente um usuário remoto através de uma rede pública. Um tipo de VPN é uma VPN cliente-gateway. Uma VPN cliente-gateway é uma conexão entre um usuário remoto e a rede. O cliente é configurado no dispositivo do usuário com software cliente VPN. Permite que os usuários se conectem remotamente a uma rede com segurança.

Dispositivos aplicáveis

- Roteador VPN WAN duplo RV320
- Roteador VPN WAN duplo RV325 Gigabit

Versão de software

- v1.1.0.09

Configurar um único cliente para gateway VPN

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

Client to Gateway

Add a New Tunnel

Tunnel Group VPN Easy VPN

Tunnel No.

1

Tunnel Name:

Interface:

WAN1

Keying Mode:

IKE with Preshared key

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

:

Etapa 2. Clique no botão de opção **Tunnel** para adicionar um único túnel para o cliente ao gateway VPN.

Client to Gateway

Add a New Tunnel

Tunnel

Group VPN

Easy VPN

Tunnel No. 1

Tunnel Name:

Interface:

Keying Mode:

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:

:

Adicionar novo túnel

Client to Gateway

Add a New Tunnel

Tunnel Group VPN Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

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 :

Note: Tunnel No - Representa o número do túnel. Esse número é gerado automaticamente.

Etapa 1. Digite o nome do túnel no campo *Nome do túnel*.

Etapa 2. Escolha a interface através da qual o cliente remoto acessa a VPN na lista suspensa *Interface*.

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1
WAN1
WAN2
USB1
USB2

Keying Mode:

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

Etapa 3. Escolha o modo apropriado de gerenciamento de chaves para garantir a segurança na lista suspensa *Modo de chave*. O modo padrão é IKE with Preshared key (IKE com chave pré-compartilhada).

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key
Manual
IKE with Preshared key
IKE with Certificate

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

As opções são definidas da seguinte forma:

- Manual - Modo de segurança personalizado para gerar uma nova chave de segurança sozinho e nenhuma negociação com a chave. Ele é melhor para ser usado durante a solução de problemas ou 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 uma comunicação autenticada para o túnel.
- O protocolo IKE com certificado - Internet Key Exchange (IKE) com certificado é um método mais seguro para gerar e trocar automaticamente chaves pré-compartilhadas para estabelecer uma comunicação mais segura para o túnel.

Etapa 4. Marque a caixa de seleção **Habilitar** para habilitar o cliente para o gateway VPN. Por padrão, ele é ativado.

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No.

Tunnel Name:

Interface:

Keying Mode:

Enable:

Local Group Setup

Local Security Gateway Type:

Domain Name:

Local Security Group Type:

IP Address:

Etapa 5. Para salvar as configurações que você tem até agora, role para baixo e clique em **Salvar** para salvar as configurações.

Configuração de grupo local

Configuração de grupo local com manual ou IKE com chave pré-compartilhada

Note: Siga as etapas abaixo se você escolheu Manual ou IKE com chave pré-compartilhada na lista suspensa *Keying Mode* na Etapa 3 da seção *Add a New Tunnel*.

Etapa 1. Escolha o método de identificação de roteador apropriado na lista suspensa *Local Security Gateway* para estabelecer um túnel VPN.

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No.: 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Gateway Type: IP Only

IP Address: 192.168.1.1

Local Security Group Type: Subnet

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

As opções são definidas da seguinte forma:

- 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 estático da WAN é 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 estático da WAN é 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 estático da WAN é 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 de Endereço de Email e IP Dinâmico (FQDN do USUÁRIO) - 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).
- Endereço IP - Representa o endereço IP da interface WAN. É um campo somente leitura.

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

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Gateway Type: Dynamic IP + Domain Name(FQDN) Authentication

Domain Name: domain_1

Local Security Group Type: Subnet

IP Address:

Subnet Mask: 255.255.255.0

- IP - Apenas 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). O IP padrão é 192.168.1.0.
- 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 de IP - Um intervalo de dispositivos LAN pode acessar o túnel. Se você escolher essa opção, insira os endereços IP inicial e final nos campos *IP inicial* e *IP final* respectivamente. O intervalo padrão é de 192.168.1.0 a 192.168.1.254.

Etapa 3. Para salvar as configurações que você tem até agora, role para baixo e clique em **Salvar** para salvar as configurações.

Configuração de grupo local com IKE com certificado para VPN de túnel

Note: Siga as etapas abaixo se você escolheu IKE com certificado na lista suspensa *Modo de chaveamento* na Etapa 3 da seção *Adicionar um novo túnel*.

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Certificate

Enable:

Local Group Setup

Local Security Gateway Type: IP + Certificate

IP Address: 0.0.0.0

Local Certificate: 01. Issuer: 6c:20:56:c6:16:52 - Subject: 6c:20:56:c6:16:52

Local Security Group Type: IP

IP Address: 192.168.2.1

- Tipo de gateway de segurança local - O acesso ao túnel é possível por meio do IP com um certificado.
- Endereço IP - Representa o endereço IP da interface WAN. É um campo somente leitura.

Etapa 1. Escolha o certificado local apropriado para identificar o roteador na lista suspensa *Certificado local*. Clique em **Self-Generator** para gerar o certificado automaticamente ou clique em **Import Certificate** para importar um novo certificado.

Nota: Para saber mais sobre como gerar certificados automaticamente, consulte *Gerar certificados em roteadores RV320* e para saber como importar certificados, consulte *Configurar meu certificado em roteadores RV320*.

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Certificate

Enable:

Local Group Setup

Local Security Gateway Type: IP + Certificate

IP Address: 0.0.0.0

Local Certificate: 01. Issuer: 6c:20:56:c6:16:52 - Subject: 6c:20:56:c6:16:52

Local Security Group Type: IP

IP Address:

IP

IP

Subnet

IP Range

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

- IP - Apenas 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). 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 os endereços IP inicial e final nos campos IP inicial e final, respectivamente. O intervalo padrão é de 192.168.1.0 a 192.168.1.254.

Etapa 3. Para salvar as configurações que você tem até agora, role para baixo e clique em **Salvar** para salvar as configurações.

Configuração de cliente remoto

Configuração de cliente remoto com manual ou IKE com chave pré-compartilhada

Nota: Siga as etapas abaixo se você escolheu Manual ou IKE com chave pré-compartilhada na lista suspensa *Modo de chaveamento* na Etapa 3 da seção *Adicionar um novo túnel*.

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Gateway Type: IP Only

IP Address: 0.0.0.0

Local Security Group Type: IP

IP Address: 192.168.2.1

Remote Client Setup

Remote Security Gateway Type: IP Only

IP Address :

IPSec Setup

Phase 1 DH Group: Group 1 - 768 bit

Etapa 1. Escolha o método de identificação de cliente apropriado para estabelecer um túnel VPN na lista suspensa *Remote Security Gateway*. O padrão é IP somente.

- IP Only (Somente IP) - o acesso ao túnel é possível somente através de um IP de WAN do cliente. Você pode escolher essa opção apenas se souber o IP de WAN estático ou o nome de domínio do cliente. Escolha IP Address (Endereço IP) na lista suspensa e insira o IP estático do cliente no campo adjacente ou escolha IP by DNS Resolvido (IP por DNS resolvido) na lista suspensa e insira o nome de domínio do endereço IP no campo adjacente. Através do servidor DNS local do endereço IP, o roteador pode recuperar o endereço IP automaticamente.

Note: Se você escolher Manual na lista suspensa *Keying Mode* na Etapa 3 na seção Add a New Tunnel Through Tunnel (Adicionar um novo túnel através de túnel) ou Group VPN (VPN de grupo), esta será a única opção disponível.

- 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. Se você escolher essa opção, digite o nome do domínio registrado no campo Domain Name (Nome do domínio). Escolha IP Address (Endereço IP) na lista suspensa e insira o IP estático do cliente no campo adjacente ou escolha IP by DNS Resolvido (IP por

DNS resolvido) na lista suspensa e insira o nome de domínio do endereço IP no campo adjacente. Através do servidor DNS local do endereço IP, o roteador pode recuperar o endereço IP automaticamente.

- Autenticação IP + E-mail Addr (USER FQDN) - O acesso ao túnel é possível por meio de um endereço IP estático do cliente 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). Escolha IP Address (Endereço IP) na lista suspensa e insira o IP estático do cliente no campo adjacente ou escolha IP by DNS Resolvido (IP por DNS resolvido) na lista suspensa e insira o nome de domínio do endereço IP no campo adjacente. Através do servidor DNS local do endereço IP, o roteador pode recuperar o endereço IP 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 do cliente e um domínio registrado. Se você escolher essa opção, digite o nome do domínio registrado no campo Domain Name (Nome do domínio).
- Autenticação de Endereço de Email e IP Dinâmico (FQDN do USUÁRIO) - O acesso ao túnel é possível por meio de um endereço IP dinâmico do cliente 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. Para salvar as configurações que você tem até agora, role para baixo e clique em **Salvar** para salvar as configurações.

Configuração de grupo remoto com IKE com certificado

Nota: Siga as etapas abaixo se você escolheu IKE com certificado na lista suspensa *Modo de Chaveamento* na Etapa 3 da seção *Adicionar um Novo Túnel*.

The image shows a configuration interface with two sections: 'Local Group Setup' and 'Remote Client Setup'. The 'Remote Client Setup' section is highlighted with a red border.

Local Group Setup

Local Security Gateway Type: IP + Certificate

IP Address: 0.0.0.0

Local Certificate: 01. Issuer : 6c:20:56:c6:16:52 - Subject: 6c:20:56:c6:16:52

Buttons: Self-Generator, Import Certificate

Local Security Group Type: Subnet

IP Address: 192.168.3.1

Subnet Mask: 255.255.255.0

Remote Client Setup

Remote Security Gateway Type: IP + Certificate

IP Address: 192.168.3.2

Remote Certificate: 01. Issuer : 6c:20:56:c6:16:52 - Subject: 6c:20:56:c6:16:52

Buttons: Import Remote Certificate, Authorize CSR

- Tipo de gateway de segurança remota - a identificação do cliente é possível por meio do IP com um certificado para estabelecer a conexão VPN.

Etapa 1. Escolha **IP Address** ou **IP by DNS Resolved** na lista suspensa.

- Endereço IP - O acesso ao túnel é possível somente por meio do IP estático da WAN do cliente. Você pode escolher essa opção apenas se souber o IP de WAN estático do cliente. Insira o IP estático do cliente no campo *IP address*.
- IP By DNS Resolved - Útil se você não souber o endereço IP do cliente, mas souber o domínio desse endereço IP. Insira o nome de domínio do endereço IP. Através do servidor DNS local do endereço IP, o roteador pode recuperar o endereço IP automaticamente.

Etapa 2. Escolha o certificado remoto apropriado na lista suspensa *Certificado remoto*. Clique em **Importar certificado remoto** para importar um novo certificado ou clique em **Autorizar CSR** para identificar o certificado com uma solicitação de assinatura digital.

Note: Para saber mais sobre como importar um novo certificado, consulte *Exibir/Adicionar Certificado SSL Confiável em Roteadores RV320*, e para saber mais sobre CSR autorizado, consulte *Solicitação de Assinatura de Certificado (CSR) em Roteadores RV320*.

Etapa 3. Para salvar as configurações que você tem até agora, role para baixo e clique em **Salvar** para salvar as configurações.

Configuração do IPSec

Configuração de IPSec com chave manual

Nota: Siga as etapas abaixo se você escolheu Manual na lista suspensa *Keying Mode* na Etapa 3 da seção *Add a New Tunnel*.

Remote Client Setup

Remote Security Gateway Type: IP Only

IP Address : 192.168.3.2

IPSec Setup

Incoming SPI: 1023ac (Range: 100-FFFFFFFF, Default: 100)

Outgoing SPI: 1023cb (Range: 100-FFFFFFFF, Default: 100)

Encryption: DES

Authentication: MD5

Encryption Key: (HEX Number, DES: 16bits, 3DES: 48bits)

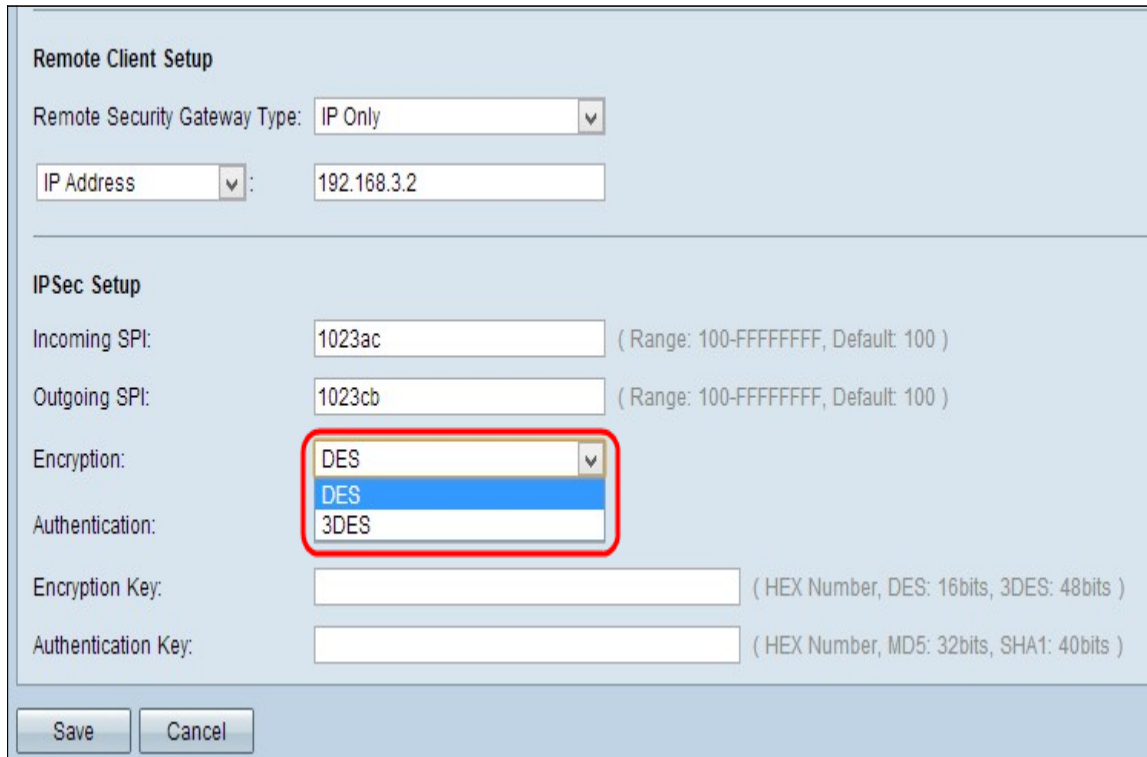
Authentication Key: (HEX Number, MD5: 32bits, SHA1: 40bits)

Etapa 1. Insira o valor hexadecimal exclusivo para o 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), que, em conjunto, determina a associação de segurança (SA) para o pacote recebido. O intervalo é de 100 a ffffff, com o padrão sendo

100.

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 de Payload de Segurança de Encapsulamento (ESP - Encapsulating Security Payload Protocol) que, em conjunto, determina a associação de segurança (SA - Security Association) para o pacote de saída. O intervalo é de 100 a ffffff, com o padrão sendo 100.

Note: O SPI de Entrada do dispositivo conectado e o SPI de Saída da outra extremidade do túnel devem corresponder um ao outro para estabelecer um túnel.



Remote Client Setup

Remote Security Gateway Type: IP Only

IP Address: 192.168.3.2

IPSec Setup

Incoming SPI: 1023ac (Range: 100-FFFFFFF, Default: 100)

Outgoing SPI: 1023cb (Range: 100-FFFFFFF, Default: 100)

Encryption: DES

Authentication: 3DES

Encryption Key: (HEX Number, DES: 16bits, 3DES: 48bits)

Authentication Key: (HEX Number, MD5: 32bits, SHA1: 40bits)

Save Cancel

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 - O DES (Data Encryption Standard, Padrão de Criptografia de Dados) é um método de criptografia de 56 bits, antigo e compatível com versões anteriores, que não é tão seguro.
- 3DES - O 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 o DES.

Remote Client Setup

Remote Security Gateway Type: IP Only

IP Address: 192.168.3.2

IPSec Setup

Incoming SPI: 1023ac (Range: 100-FFFFFFFF, Default: 100)

Outgoing SPI: 1023cb (Range: 100-FFFFFFFF, Default: 100)

Encryption: DES

Authentication: MD5

Encryption Key: (HEX Number, DES: 16bits, 3DES: 48bits)

Authentication Key: (HEX Number, MD5: 32bits, SHA1: 40bits)

Save Cancel

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 - Message Digest Algorithm-5 (MD5) representa uma função hash hexadecimal de 32 dígitos 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.

Remote Client Setup

Remote Security Gateway Type: IP Only

IP Address: 192.168.3.2

IPSec Setup

Incoming SPI: 1023ac (Range: 100-FFFFFFFF, Default: 100)

Outgoing SPI: 1023cb (Range: 100-FFFFFFFF, Default: 100)

Encryption: DES

Authentication: SHA1

Encryption Key: adbc234987bc (HEX Number, DES: 16bits, 3DES: 48bits)

Authentication Key: 233445bcfacffb (HEX Number, MD5: 32bits, SHA1: 40bits)

Save Cancel

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

Passo 7. Para salvar as configurações que você tem até agora, role para baixo e clique em **Salvar** para salvar as configurações.

Configuração de IPSec com IKE com chave pré-compartilhada ou IKE com certificado

Nota: Siga as etapas abaixo se você escolheu IKE com chave pré-compartilhada ou IKE com certificado na lista suspensa *Modo de chaveamento* na Etapa 3 da seção *Adicionar um novo túnel*.

Remote Client Setup

Remote Security Gateway Type: IP Only

IP Address: 192.168.3.2

IPSec Setup

Phase 1 DH Group: Group 1 - 768 bit

Phase 1 Encryption: [Empty]

Phase 1 Authentication: MD5

Phase 1 SA Lifetime: 28800 sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group: Group 1 - 768 bit

Phase 2 Encryption: DES

Phase 2 Authentication: MD5

Phase 2 SA Lifetime: 3600 sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key: [Empty]

Preshared Key Strength Meter: [Progress bar]

Advanced +

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) simplex entre as duas extremidades do túnel para suportar a comunicação autêntica e segura. Diffie-Hellman (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 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

Phase 1 DH Group: Group 1 - 768 bit

Phase 1 Encryption : DES

Phase 1 Authentication: 3DES

Phase 1 SA Lifetime: 28800 sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group: Group 1 - 768 bit

Phase 2 Encryption: DES

Phase 2 Authentication: MD5

Phase 2 SA Lifetime: 3600 sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter:

Advanced +

Etapa 2. Escolha a Encriptação de Fase 1 apropriada para encriptar a chave a partir da lista suspensa *Criptografia de Fase 1*. 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 - O DES (Data Encryption Standard, Padrão de Criptografia de Dados) é um método de criptografia antigo de 56 bits, que não é muito seguro.
- 3DES - O 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 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 repetição.
- AES-192 - AES (Advanced Encryption Standard) é um método de criptografia de 192 bits que transforma o texto simples em texto cifrado por 12 ciclos de repetição.
- 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 repetição.

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication: (MD5, MD5, SHA1)

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter:

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

- MD5 - Message Digest Algorithm-5 (MD5) representa uma função hash hexadecimal de 32 dígitos 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.

IPSec Setup

Phase 1 DH Group: Group 1 - 768 bit

Phase 1 Encryption: AES-128

Phase 1 Authentication: SHA1

Phase 1 SA Lifetime: 2870 sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group: Group 1 - 768 bit


Phase 2 Encryption: DES

Phase 2 Authentication: MD5

Phase 2 SA Lifetime: 3600 sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter: 

Advanced +

Etapa 4. Insira a quantidade de tempo em segundos, na Fase 1, o túnel VPN permanece ativo no campo *SA Lifetime da Fase 1*. O tempo padrão é 28800 segundos.

Etapa 5. Marque a caixa de seleção **Perfect Forward Secret** 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.

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

- Group 1 - 768 bit
- Group 1 - 768 bit
- Group 2 - 1024 bit
- Group 5 - 1536 bit

Phase 2 Encryption:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter:

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. Diffie-Hellman (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 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

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity:

Preshared Key:

Preshared Key Strength Meter: ■ ■ ■ ■

Passo 7. Escolha a Criptografia de Fase 2 apropriada para criptografar a chave na lista suspensa *Criptografia de 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 - O DES (Data Encryption Standard, Padrão de Criptografia de Dados) é um método de criptografia antigo de 56 bits, que não é muito seguro.
- 3DES - O 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 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 12 ciclos de repetições.
- 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.

IPSec Setup

Phase 1 DH Group: Group 1 - 768 bit

Phase 1 Encryption: AES-128

Phase 1 Authentication: SHA1

Phase 1 SA Lifetime: 2870 sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group: Group 2 - 1024 bit

Phase 2 Encryption: AES-128

Phase 2 Authentication: MD5

Phase 2 SA Lifetime: 3600 sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter:

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 - Message Digest Algorithm-5 (MD5) representa uma função hash hexadecimal de 32 dígitos 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.
- Null (Nulo) - Nenhum método de autenticação é usado.

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter:

Etapa 9. Digite a quantidade de tempo em segundos, na Fase 2, o túnel VPN permanece ativo no campo Vida útil do SA da Fase 2. O tempo padrão é 3600 segundos.

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 que é compartilhada anteriormente entre os pares IKE no campo *Preshared Key (Chave pré-compartilhada)*. Até 30 caracteres alfanuméricos 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 segura.

- Medidor de força da 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. Se você marcar a caixa de seleção **Mínimo de complexidade de chave pré-compartilhada** na Etapa 10 da seção Configuração de IPSec, então somente o Medidor de força de chave pré-compartilhada será exibido.

Note: Se você escolher IKE com chave pré-compartilhada na lista suspensa *Keying Mode* na Etapa 3 para *Add a New Tunnel* section, então somente você poderá ter a opção de configurar a Etapa 10, a Etapa 11 e visualizar o Preshared Key Strength Meter.

Etapa 12. Para salvar as configurações que você tem até agora, role para baixo e clique em **Salvar** para salvar as configurações.

Configuração avançada com IKE com chave pré-compartilhada ou IKE com certificado

As configurações avançadas são possíveis somente para IKE com chave pré-compartilhada e IKE com chave de certificação. A configuração da chave Manual não tem configurações avançadas.

The screenshot shows the 'IPSec Setup' configuration window. It contains the following fields and options:

- Phase 1 DH Group: Group 1 - 768 bit
- Phase 1 Encryption: AES-128
- Phase 1 Authentication: SHA1
- Phase 1 SA Lifetime: 2870 sec (Range: 120-86400, Default: 28800)
- Perfect Forward Secrecy:
- Phase 2 DH Group: Group 2 - 1024 bit
- Phase 2 Encryption: AES-128
- Phase 2 Authentication: MD5
- Phase 2 SA Lifetime: 350 sec (Range: 120-28800, Default: 3600)
- Minimum Preshared Key Complexity: Enable
- Preshared Key: abcd1234ght
- Preshared Key Strength Meter: A visual indicator showing four bars, with the first two red and the last two yellow.

The 'Advanced +' button is highlighted with a red circle. At the bottom of the window are 'Save' and 'Cancel' buttons.

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

The image shows a configuration window titled "Advanced" with several options. A red rectangle highlights the following settings:

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm: SHA1
- NetBIOS Broadcast
- NAT Traversal
- Dead Peer Detection Interval: 15 sec (Range: 10-999, Default: 10)

Other visible options include:

- Extended Authentication
 - IPsec Host
 - User Name:
 - Password:
 - Edge Device: Default - Local Database
- Mode Configuration

Buttons at the bottom: Save, Cancel.

Etapa 2. Marque a caixa de seleção **Aggressive Mode (Modo agressivo)** se a velocidade da rede for 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))** 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 - Message Digest Algorithm-5 (MD5) representa uma função hash hexadecimal de 128 dígitos 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.

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** se quiser acessar a Internet de sua LAN privada por meio de endereço IP público. O NAT Traversal é usado para exibir os endereços IP privados dos sistemas internos como endereços IP públicos para proteger os endereços IP privados de qualquer ataque ou descoberta mal-intencionada.

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, digite a duração ou o intervalo das mensagens de saudação desejadas.

The screenshot shows the 'Advanced' configuration window for a VPN. The 'Extended Authentication' section is highlighted with a red border. It contains the following options:

- Extended Authentication
 - IPSec Host
 - User Name:
 - Password:
 - Edge Device
 - Default - Local Database (dropdown menu)
 - Add/Edit button
- Mode Configuration

At the bottom of the window are 'Save' and 'Cancel' buttons.

Etapa 9. Verifique a **Autenticação Estendida** para fornecer mais segurança e autenticação à conexão VPN. Clique no botão de opção apropriado para estender a autenticação da conexão VPN.

- Host IPSec - Autenticação estendida através do host IPSec. Se você escolher essa opção, insira o nome de usuário do host IPSec no campo Nome de usuário e uma senha no campo Senha.
- Edge Device - Autenticação estendida através do dispositivo de borda. Se você escolher essa opção, escolha o banco de dados que contém o dispositivo de borda na lista suspensa. Para adicionar ou editar o banco de dados, clique em **Adicionar/Editar**.

Note: Para saber mais sobre como adicionar ou editar o banco de dados local, consulte *User and Domain Management Configuration on RV320 Router*.

Etapa 10. Verifique **Mode Configuration** para fornecer o endereço IP para o solicitante de túnel de entrada.

Note: As Etapas 9 a 11 estão disponíveis para o modo de chaveamento pré-compartilhado IKE para VPN de túnel.

Etapa 11. Clique em **Save (Salvar)** para salvar as configurações.

Conclusão

Agora você aprendeu as etapas para configurar um único cliente para gateway VPN em RV32x Series VPN Routers

Exibir um vídeo relacionado a este artigo...

[Clique aqui para ver outras palestras técnicas da Cisco](#)