

# Configure o Group Client para Gateway Virtual Private Network (VPN) nas séries RV320 e RV325 de roteadores VPN

## Objetivo

Uma VPN (Virtual Private Network) é uma rede privada usada para conectar virtualmente os dispositivos do usuário remoto através da rede pública para fornecer segurança. Um dos tipos de VPNs é uma VPN cliente-gateway. Com o cliente-gateway, você pode conectar remotamente diferentes filiais da sua empresa localizadas em áreas geográficas diferentes para transmitir e receber os dados entre as áreas com mais segurança. A VPN de grupo fornece uma configuração fácil da VPN, pois elimina a configuração da VPN para cada usuário. O RV32x VPN Router Series pode suportar um máximo de dois grupos VPN.

O objetivo deste documento é explicar como configurar um cliente de grupo para VPN de gateway em RV32x Series VPN Routers .

## Dispositivos aplicáveis

RV320 Roteador VPN WAN duplo  
Roteador VPN WAN duplo RV325 Gigabit

## Versão de software

•v1.1.0.09

## Configurar o cliente do grupo para a VPN do gateway

Etapa 1. Faça login no utilitário de configuração do roteador 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 **Group VPN** para adicionar um grupo de VPN cliente a gateway.



### Client to Gateway

**Add a New Group VPN**

Tunnel  Group VPN  Easy VPN

Group No. 1

Tunnel Name: tunnel\_1

Interface: WAN1

Keying Mode: IKE with Preshared key

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: DomainName(FQDN)

Domain Name:

**Note:** Grupo N° - Representa o número do grupo. É um campo gerado automaticamente.

Etapa 2. Escolha a interface apropriada através da qual o grupo VPN se conecta ao gateway na lista suspensa *Interface*.

### Client to Gateway

**Add a New Group VPN**

Tunnel     Group VPN     Easy VPN

Group No.    1

Tunnel Name:    tunnel\_1

Interface:    WAN1  
WAN1  
WAN2  
USB1  
USB2

Keying Mode:

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:    DomainName(FQDN)

Domain Name:

Etapa 3. Marque a caixa de seleção **Habilitar** para habilitar a VPN de gateway para gateway. Por padrão, ele está ativado.



### Client to Gateway

**Add a New Group VPN**

Tunnel   
 Group VPN   
 Easy VPN

Group No. 1

Tunnel Name: tunnel\_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

---

**Local Group Setup**

Local Security Group Type: Subnet

IP Address: Subnet

Subnet Mask: 255.255.255.0

---

**Remote Client Setup**

Remote Client: DomainName(FQDN)

Domain Name:

As opções disponíveis são definidas da seguinte forma:

**IP** — Somente um dispositivo LAN específico pode acessar o túnel. Se você escolher esta opção, digite o endereço IP do dispositivo de LAN no campo IP Address (Endereço IP). 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 o primeiro e o último endereços IP para o intervalo nos campos *Start IP* e *End IP* respectivamente. O intervalo padrão é de 192.168.1.0 a 192.168.1.254.

Etapa 2. Para salvar as configurações até agora e deixar o restante como padrão, role para baixo e clique em **Salvar** para salvar as configurações.

## Configuração de cliente remoto

Etapa 1. Escolha o usuário ou grupo de usuários da LAN remota apropriado que podem acessar o túnel VPN na lista suspensa *Tipo de grupo de segurança remota*.

**Client to Gateway**

**Add a New Group VPN**

Tunnel   
 Group VPN   
 Easy VPN

Group No. 1

Tunnel Name: tunnel\_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

---

**Local Group Setup**

Local Security Group Type: IP

IP Address: 192.168.3.0

---

**Remote Client Setup**

Remote Client: 
DomainName(FQDN)
  
DomainName(FQDN)
  
Email Address(USER FQDN)
  
Microsoft XP/2000 VPN Client

Domain Name:

As opções disponíveis são definidas da seguinte forma:

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

**Autenticação de End. de Email(USER FQDN)** — O acesso ao túnel é possível por meio de um endereço de email. 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 de software cliente que é um software Microsoft XP ou 2000 VPN Client incorporado.

Etapa 2. Para salvar as configurações até agora e deixar o restante como padrão, role para baixo e clique em **Salvar** para salvar as configurações.

## Configuração do IPSec

Etapa 1. Escolha o grupo Diffie-Hellman (DH) apropriado na lista suspensa *Grupo DH 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 é um protocolo de troca de chave criptográfica que é usado na conexão da Fase 1 para compartilhar uma chave secreta a fim autenticar a comunicação.

**Remote Client Setup**

Remote Client:

---

**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:

As opções disponíveis são definidas da seguinte forma:

Group1 (768 bits) — Calcula a chave mais rapidamente, mas é a menos segura.

Group2 (1024 bits) — Calcula a chave mais lentamente, mas é mais seguro que Group1.

Group5 (1536 bits) — Calcula a chave com o menor tempo, mas é a mais segura.

Etapa 2. Escolha o método de criptografia apropriado para criptografar a chave na lista suspensa *Phase 1 Encryption*. O AES-128 é recomendado por sua alta segurança e rápido desempenho. O túnel VPN precisa usar o mesmo método de criptografia para as duas extremidades.

**Remote Client Setup**

Remote Client:

---

**IPSec Setup**

Phase 1 DH Group:

Phase 1 Encryption : 

- DES
- DES
- 3DES
- AES-128
- AES-192
- AES-256

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:

As opções disponíveis são definidas da seguinte forma:

**DES** — Data Encryption Standard (DES) é um método de criptografia antigo de 56 bits que não é um método de criptografia muito seguro, mas pode ser necessário para compatibilidade com versões anteriores.

**3DES** — O 3DES (Triple Data Encryption Standard) é um método de criptografia simples de 168 bits usado para aumentar o tamanho da chave porque criptografa os dados três vezes. Isso oferece mais segurança que o DES, mas menos segurança que o AES.

**AES-128** — Advanced Encryption Standard com chave de 128 bits (AES-128) usa uma chave de 128 bits para criptografia AES. O AES é mais rápido e mais seguro que o DES. Em geral, o AES também é mais rápido e mais seguro que o 3DES. O AES-128 é mais rápido, mas menos seguro que o AES-192 e o AES-256.

**AES-192** — AES-192 usa uma chave de 192 bits para a criptografia AES. O AES-192 é mais lento, mas mais seguro que o AES-128, e mais rápido, mas menos seguro que o AES-256.

**AES-256** — AES-256 usa uma chave de 256 bits para a criptografia AES. O AES-256 é mais lento, mas mais seguro que o AES-128 e o AES-192.

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.

**Remote Client Setup**

Remote Client:

---

**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:

As opções disponíveis são definidas da seguinte forma:

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

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

Etapa 4. No campo *SA Life Time da Fase 1*, insira a quantidade de tempo em segundos durante o qual o túnel VPN permanece ativo na Fase 1. O tempo padrão é 28.800 segundos.

**Remote Client Setup**

Remote Client:

---

**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:

Etapa 5. (Opcional) Para fornecer mais proteção às chaves, marque a caixa de seleção **Perfect Forward Secsecret**. Essa opção permite gerar uma nova chave se alguma chave for comprometida. Essa é uma ação recomendada, pois fornece mais segurança.

**Nota:** Se você desmarcar **Perfect Forward Secsecret** na Etapa 5, não será necessário configurar o Grupo DH da Fase 2.

Etapa 6. Escolha o grupo DH apropriado na lista suspensa *Grupo DH Fase 2*.

**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:

As opções disponíveis são definidas da seguinte forma:

Group1 (768 bits) — Calcula a chave mais rapidamente, mas é a menos segura.

Group2 (1024 bits) — Calcula a chave mais lentamente, mas é mais seguro que Group1.

Group5 (1536 bits) — Calcula a chave com o menor tempo, mas é a mais segura.

Etapa 2. Escolha o método de criptografia apropriado para criptografar a chave na lista suspensa *Phase 1 Encryption*. O AES-128 é recomendado por sua alta segurança e rápido desempenho. O túnel VPN precisa usar o mesmo método de criptografia para as duas extremidades.

**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: 

- DES
- DES
- 3DES
- AES-128
- AES-192
- AES-256

Phase 2 Authentication:

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

Minimum Preshared Key Complexity:  Enable

Preshared Key:

As opções disponíveis são definidas da seguinte forma:

**DES** — Data Encryption Standard (DES) é um método de criptografia antigo de 56 bits que não é um método de criptografia muito seguro, mas pode ser necessário para compatibilidade com versões anteriores.

**3DES** — O 3DES (Triple Data Encryption Standard) é um método de criptografia simples de 168 bits usado para aumentar o tamanho da chave porque criptografa os dados três vezes. Isso oferece mais segurança que o DES, mas menos segurança que o AES.

**AES-128** — Advanced Encryption Standard com chave de 128 bits (AES-128) usa uma chave de 128 bits para criptografia AES. O AES é mais rápido e mais seguro que o DES. Em geral, o AES também é mais rápido e mais seguro que o 3DES. O AES-128 é mais rápido, mas menos seguro que o AES-192 e o AES-256.

**AES-192** — AES-192 usa uma chave de 192 bits para a criptografia AES. O AES-192 é mais lento, mas mais seguro que o AES-128, e mais rápido, mas menos seguro que o AES-256.

**AES-256** — AES-256 usa uma chave de 256 bits para a criptografia AES. O AES-256 é mais lento, mas mais seguro que o AES-128 e o AES-192.

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.

**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:

As opções disponíveis são definidas da seguinte forma:

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

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

Etapa 9. No campo *Vida útil SA da Fase 2*, insira o tempo em segundos durante o qual o túnel VPN permanece ativo na Fase 2. O tempo padrão é 3600 segundos.

**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 10. (Opcional) Se quiser ativar o medidor de força para a chave pré-compartilhada, marque a caixa de seleção **Mínimo de complexidade da chave pré-compartilhada**.

**Note:** Se você marcar a caixa de seleção **Mínimo de complexidade de chave pré-compartilhada**, o *Medidor de força de chave pré-compartilhada* mostrará a força da chave pré-compartilhada através de barras coloridas. Vermelho indica intensidade fraca, amarelo indica intensidade aceitável e verde indica força forte.

Etapa 11. Digite a chave desejada no campo *Preshared Key (Chave pré-compartilhada)*. Até 30 hexadecimais podem ser usados como a 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.

Etapa 12. Para salvar as configurações até agora e deixar o restante como padrão, role para baixo e clique em **Salvar** para salvar as configurações.

## Configuração avançada

Etapa 1. Clique em **Avançado** para definir as configurações avançadas.

**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:

**Advanced +**

A área *Avançado* é exibida com novos campos disponíveis.

Phase 2 Authentication:

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

Minimum Preshared Key Complexity:  Enable

Preshared Key:

Preshared Key Strength Meter:

**Advanced -**

**Advanced**

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm
- NetBIOS Broadcast
- NAT Traversal

Etapa 2. (Opcional) Marque a caixa de seleção **Modo agressivo** se sua velocidade de rede estiver baixa. O Modo agressivo troca as IDs dos pontos finais do túnel em texto claro durante a conexão SA, o que requer menos tempo para troca, mas é menos seguro.

Etapa 3. (Opcional) 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 IP usado para compactar o tamanho dos datagramas IP se a velocidade da rede for baixa e se o usuário quiser transmitir os dados rapidamente sem nenhuma perda.

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

Etapa 5. (Opcional) Marque a caixa de seleção **AH Hash Algorithm** se desejar que a autenticação para a origem dos dados, a integridade dos dados por meio de checksum e a proteção estendida no cabeçalho IP. Em seguida, escolha o método de autenticação apropriado na lista suspensa. O túnel deve ter o mesmo algoritmo para ambos os lados.

As opções disponíveis são definidas da seguinte forma:

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

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

Etapa 6. Marque a caixa de seleção **NetBIOS Broadcast** se quiser permitir tráfego não roteável através do túnel VPN. O padrão é desmarcado. O NetBIOS é usado para detectar recursos de rede, como impressoras, computadores, etc., na rede através de aplicativos de software e recursos do Windows, como o Network Neighborhood.

Passo 7. (Opcional) Marque a caixa de seleção **NAT Traversal** se quiser acessar a Internet de sua LAN privada via endereço IP público. O NAT Traversal é usado para fazer com que os endereços IP privados de sistemas internos apareçam como endereços IP públicos para proteger os endereços IP privados de qualquer ataque ou descoberta mal-intencionada.

Etapa 8. Clique em **Save (Salvar)** para salvar as configurações.