

Verifique o status da VPN nos roteadores VPN RV016 RV042 RV042G e RV082

Objetivo

Uma Rede Virtual Privada (VPN) é uma conexão segura entre dois pontos finais. A VPN cria um túnel seguro entre esses dois pontos finais e fornece segurança ao tráfego de dados ao longo do túnel. Uma Rede Virtual Privada (VPN) é uma conexão segura estabelecida dentro de uma rede ou entre redes. Para que esse túnel funcione corretamente, a configuração da VPN em ambos os lados da conexão deve ser executada com cuidado e algumas informações devem ser correspondentes. O objetivo deste documento é explicar como verificar o status de VPN nos roteadores VPN RV016, RV042, RV042G e RV082. As VPNs servem para isolar o tráfego entre hosts e redes especificados do tráfego de hosts e redes não autorizados.

Dispositivos aplicáveis

• RV016
• RV042
• RV042G
• RV082

Versão de software

• 4.2.1.02

Parâmetros de VPN comuns a verificar

Para que uma conexão VPN funcione corretamente, as duas extremidades da conexão devem atender aos mesmos requisitos. Quando há uma falha na conexão VPN, há duas coisas que você pode verificar que podem fazer a diferença. Estas são:

- Os conflitos de endereço IP local entre os dois pontos finais de VPN.
- Há diferenças nas configurações de criptografia e autenticação dos dois endpoints.

A próxima seção explicará como verificar o esquema de endereços IP de uma VPN e como fazer as alterações corretas.

Alterar o endereço IP da LAN do roteador

A interface LAN de ambas as extremidades da conexão VPN deve fazer parte de um endereço de rede diferente. Se ambas as partes pertencerem ao mesmo endereço de rede, a conexão VPN não funcionará. As etapas a seguir explicam como fazer alterações no seu endereço IP LAN em RV042, RV042G e RV082 VPN Routers.

Etapa 1. Inicie a sessão no utilitário de configuração baseado na Web e selecione **Setup > Network**. A página *Rede* é aberta:

Network

Host Name : (Required by some ISPs)

Domain Name : (Required by some ISPs)

IP Mode

| Mode | WAN | LAN |
|--|---------------|---------------|
| <input checked="" type="radio"/> IPv4 Only | IPv4 | IPv4 |
| <input type="radio"/> Dual-Stack IP | IPv4 and IPv6 | IPv4 and IPv6 |

IPv4

IPv6

LAN Setting

MAC Address : 64:9E:F3:88:C6:A4

Device IP Address :

Subnet Mask :

Multiple Subnet : Enable

WAN Setting

| Interface | Connection Type | Configuration |
|-----------|----------------------------|---|
| WAN1 | Obtain an IP automatically |  |
| WAN2 | Obtain an IP automatically |  |

DMZ Setting

Enable DMZ

Etapa 2. Em Configuração de LAN, no campo Endereço IP do dispositivo, insira um endereço IP que pertença a um endereço de rede diferente da outra extremidade da conexão VPN.

LAN Setting

MAC Address : 64:9E:F3:88:C6:A4

Device IP Address :

Subnet Mask : ▼

Multiple Subnet :

WAN Setting

| Interface | Connection Type | Configuration |
|-----------|----------------------------|---|
| WAN1 | Obtain an IP automatically |  |
| WAN2 | Obtain an IP automatically |  |

Etapa 3. Na lista suspensa Máscara de sub-rede, escolha a máscara de sub-rede apropriada para sua conexão VPN.

Etapa 4. (Opcional) Para habilitar o uso de várias sub-redes, no campo Várias Sub-redes, marque a caixa de seleção Habilitar.

Etapa 5. Clique em **Salvar** para aplicar as novas configurações.

Verifique os parâmetros de segurança da conexão VPN

A configuração de segurança da conexão VPN deve ser a mesma em cada extremidade da conexão. As próximas etapas explicam como verificar esses parâmetros nos roteadores VPN RV042, RV042G e RV082.

Etapa 1. Faça login no utilitário de configuração baseado na Web e escolha **VPN > Gateway to Gateway**. A página *Gateway to Gateway* é aberta.

Gateway To Gateway

Add a New Tunnel

Tunnel No. 1

Tunnel Name : TestTunnel

Interface : WAN1

Enable :

Local Group Setup

Local Security Gateway Type : IP Only

IP Address : 156.26.31.119

Local Security Group Type : Subnet

IP Address : 192.168.1.0

Subnet Mask : 255.255.255.0

Remote Group Setup

Remote Security Gateway Type : IP Only

IP Address : 192.0.2.2

Remote Security Group Type : Subnet

IP Address : 192.168.2.0

Subnet Mask : 255.255.255.0

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 : 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 : VPNkey

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

Advanced +

Save

Cancel

Etapa 2. Verifique os parâmetros a seguir. Verifique se ambas as extremidades da conexão VPN têm as mesmas configurações:

- O Tipo de Grupo de Segurança Local é o mesmo que o segmento LAN do roteador local.
- Remote Security Group Type é o mesmo que o segmento LAN do roteador remoto.
- Remote Security Gateway Type é o endereço IP de WAN/Internet do roteador remoto.
- Os campos de configuração do IPSec devem corresponder em ambos os lados do túnel VPN.
- A chave pré-compartilhada deve ser a mesma em ambos os lados do túnel VPN.

Etapa 3. (Opcional) Clique em **Avançado+** para obter mais propriedades de segurança. Como antes, essas configurações devem ser as mesmas em ambos os lados da conexão.

Etapa 4. Clique em **Salvar** para aplicar as novas configurações se algo tiver sido alterado.

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.