

Configurando o IPSec de roteador a roteador (chaves pré-compartilhada) no túnel GRE com firewall de IOS e NAT

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento ilustra uma configuração básica de Firewall do Cisco IOS® com Tradução de Endereço de Rede (NAT). Esta configuração permite que o tráfego seja iniciado de dentro das redes 10.1.1.x e 172.16.1.x até a Internet e com NAT por todo o caminho. Um túnel de encapsulamento de roteamento genérico (GRE) é adicionado a um tráfego de túnel IP e IPX entre duas redes privadas. Quando um pacote chega na interface externa do roteador e é enviado pelo túnel, ele é primeiro encapsulado usando GRE e, depois, criptografado com IPsec. Em outras palavras, qualquer tráfego permitido a entrar no túnel de GRE também é criptografado pelo IPsec.

A fim configurar o túnel GRE sobre o IPsec com Open Shortest Path First (OSPF), refira [configurar um túnel GRE sobre o IPsec com OSPF](#).

A fim configurar um projeto do IPsec do hub and spoke entre três Roteadores, refira [configurar o hub and spoke do roteador para roteador do IPsec com uma comunicação entre o spokes](#).

[Pré-requisitos](#)

[Requisitos](#)

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco IOS Software Release 12.2(21a) e 12.3(5a)
- Cisco 3725 e 3640

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Informações de Apoio

As pontas nesta seção ajudam-no a executar a configuração:

- Execute o NAT em ambo o Roteadores para testar a conectividade de Internet.
- Adicionar o GRE à configuração e teste-o. O tráfego não codificado deve fluir entre as redes privadas.
- Adicionar o IPsec à configuração e teste-o. O tráfego entre as redes privadas deve ser criptografado.
- Adicionar o Cisco IOS Firewall às interfaces externas, o de partida inspecionam a lista e a lista de acessos de entrada, e testam-nos.
- Se você usa um Cisco IOS Software Release mais cedo de 12.1.4, você precisa de permitir o tráfego IP entre 172.16.1.x e - 10.0.0.0 na lista de acessos 103. Refira a identificação de bug Cisco [CSCdu58486 \(clientes registrados somente\)](#) e a identificação de bug Cisco [CSCdm01118 \(clientes registrados somente\)](#) para mais informação.

Configurar

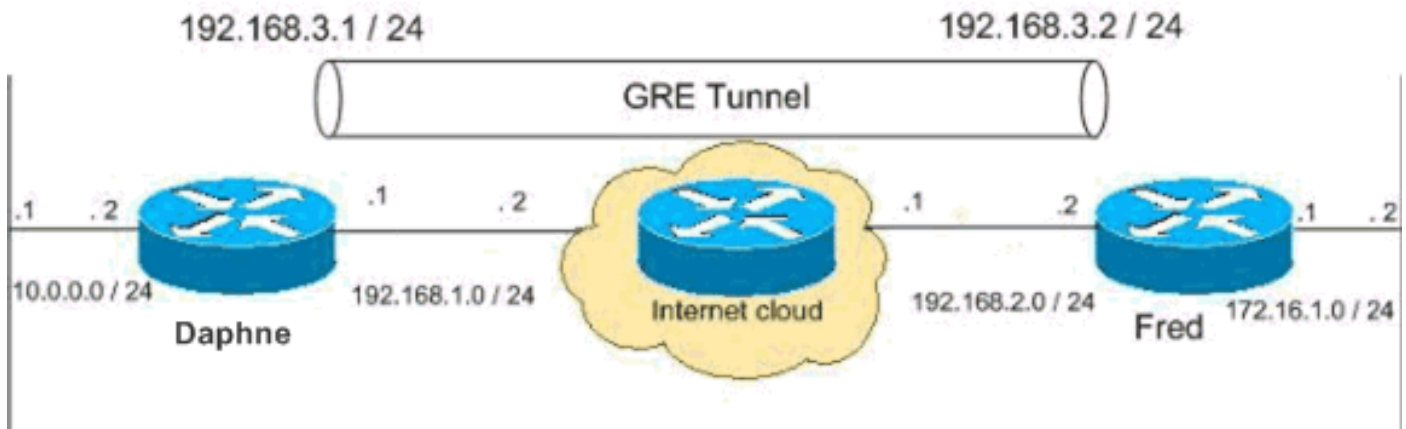
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a ferramenta [Command Lookup Tool \(apenas para clientes registrados\)](#) para obter mais informações sobre os comandos usados neste documento.

Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços da RFC1918 que foram usados em um ambiente de laboratório.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede.



Configurações

Este documento utiliza estas configurações.

- [Configuração Daphne](#)
- [Configuração Fred](#)

Configuração Daphne

```

version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname daphne
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$r2sh$XKZR118vcId11ZGzgbz5C/
!
no aaa new-model
ip subnet-zero
!
!
!--- This is the Cisco IOS Firewall configuration and
what to inspect. !--- This is applied outbound on the
external interface. ip inspect name myfw tcp
ip inspect name myfw udp
ip inspect name myfw ftp
ip inspect name myfw realaudio
ip inspect name myfw smtp
ip inspect name myfw streamworks
ip inspect name myfw vdolive
ip inspect name myfw tftp
ip inspect name myfw rcmd
ip inspect name myfw http
ip telnet source-interface FastEthernet0/0
!
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
!
!--- This is the IPsec configuration. ! crypto isakmp
policy 10
authentication pre-share

```

```

crypto isakmp key ciscokey address 192.168.2.2
!
!
crypto ipsec transform-set to_fred esp-des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp

    set peer 192.168.2.2
    set transform-set to_fred
    match address 101
!
!
!
!
!
!--- This is one end of the GRE tunnel. ! interface
Tunnel0

ip address 192.168.3.1 255.255.255.0
!--- Associate the tunnel with the physical interface.
tunnel source FastEthernet0/1

tunnel destination 192.168.2.2

!--- This is the internal network. interface
FastEthernet0/0
ip address 10.0.0.2 255.255.255.0
    ip nat inside
    speed 100
    full-duplex
!
!--- This is the external interface and one end of the
GRE tunnel. interface FastEthernet0/1
ip address 192.168.1.1 255.255.255.0
    ip access-group 103 in
    ip nat outside
    ip inspect myfw out
    speed 100
    full-duplex
    crypto map myvpn
!
!--- Define the NAT pool.
ip nat pool ourpool 192.168.1.10 192.168.1.20 netmask
255.255.255.0
ip nat inside source route-map nonat pool ourpool
overload
ip classless

ip route 0.0.0.0 0.0.0.0 192.168.1.2

!--- Force the private network traffic into the tunnel.
- ip route 172.16.1.0 255.255.255.0 192.168.3.2 ip http
server no ip http secure-server ! ! !--- All traffic
that enters the GRE tunnel is encrypted by IPsec. !---
Other ACE statements are not necessary. access-list 101
permit gre host 192.168.1.1 host 192.168.2.2 !--- Access
list for security reasons. Allow !--- IPsec and GRE
traffic between the private networks.
access-list 103 permit gre host 192.168.2.2 host
192.168.1.1
access-list 103 permit esp host 192.168.2.2 host
192.168.1.1
access-list 103 permit udp host 192.168.2.2 eq isakmp
host 192.168.1.1

```

```
access-list 103 deny ip any any log

!--- See the Background Information section if you use
!--- a Cisco IOS Software release earlier than 12.1.4
for access list 103. access-list 175 deny ip 10.0.0.0
0.0.0.255 172.16.1.0 0.0.0.255 access-list 175 permit ip
10.0.0.0 0.0.0.255 any !--- Use access list in route-map
to address what to NAT. route-map nonat permit 10
  match ip address 175
!
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  password ww
  login
!
!
end
```

Configuração Fred

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname fred
!
enable secret 5 $1$AtxD$MycLGaJvF/tAIFXkikCesl
!
ip subnet-zero
!
!
ip telnet source-interface FastEthernet0/0
!
ip inspect name myfw tcp
ip inspect name myfw udp
ip inspect name myfw ftp
ip inspect name myfw realaudio
ip inspect name myfw smtp
ip inspect name myfw streamworks
ip inspect name myfw vdolive
ip inspect name myfw tftp
ip inspect name myfw rcmd
ip inspect name myfw http
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 10
  authentication pre-share
-
crypto isakmp key ciscokey address 192.168.1.1
!
!
crypto ipsec transform-set to_daphne esp-des esp-md5-
hmac
!
crypto map myvpn 10 ipsec-isakmp

set peer 192.168.1.1
  set transform-set to_daphne
  match address 101
```

```
!  
call rsvp-sync  
!  
!  
!  
!  
!  
!  
!  
!  
interface Tunnel0  
-  
ip address 192.168.3.2 255.255.255.0  
tunnel source FastEthernet0/1  
-  
tunnel destination 192.168.1.1  
!  
interface FastEthernet0/0  
ip address 172.16.1.1 255.255.255.0  
ip nat inside  
speed 100  
full-duplex  
!  
interface Serial0/0  
no ip address  
clockrate 2000000  
!  
interface FastEthernet0/1  
  
ip address 192.168.2.2 255.255.255.0  
ip access-group 103 in  
ip nat outside  
ip inspect myfw out  
speed 100  
full-duplex  
crypto map myvpn  
!  
  
!--- Output is suppressed. !  
ip nat pool ourpool 192.168.2.10 192.168.2.20 netmask  
255.255.255.0  
ip nat inside source route-map nonat pool ourpool  
overload  
ip classless  
  
ip route 0.0.0.0 0.0.0.0 192.168.2.1  
ip route 10.0.0.0 255.255.255.0 192.168.3.1  
ip http server  
!  
  
access-list 101 permit gre host 192.168.2.2 host  
192.168.1.1  
access-list 103 permit gre host 192.168.1.1 host  
192.168.2.2  
access-list 103 permit udp host 192.168.1.1 eq isakmp  
host 192.168.2.2  
access-list 103 permit esp host 192.168.1.1 host  
192.168.2.2  
access-list 175 deny ip 172.16.1.0 0.0.0.255 10.0.0.0  
0.0.0.255  
access-list 175 permit ip 172.16.1.0 0.0.0.255 any  
  
route-map nonat permit 10
```

```
match ip address 175
!
!
!
dial-peer cor custom
!
!
!
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  password ww
  login
!
end
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Tente sibilhar um host na sub-rede remota - 10.0.0.x de um host na rede 172.16.1.x a fim verificar a configuração de VPN. Este tráfego deve atravessar o túnel GRE e ser cifrado.

Use o **comando show crypto ipsec sa** para verificar que o túnel de IPsec está acima. Primeira verificação que os números SPI são diferentes do que 0. Você deve igualmente ver que um aumento nos pacotes para cifrar e os pacotes decifram contadores.

- **mostre IPsec cripto sa** — Verifica que o túnel de IPsec está acima.
- **mostre as listas de acesso 103** — Verifica que a configuração do Cisco IOS Firewall trabalha corretamente.
- **mostre a IP traduções nat** — Verifica que o NAT trabalha corretamente.

```
fred#show crypto ipsec sa
```

```
interface: FastEthernet0/1
```

```
Crypto map tag: myvpn, local addr. 192.168.2.2
```

```
local ident (addr/mask/prot/port): (192.168.2.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/47/0)
current_peer: 192.168.1.1
  PERMIT, flags={transport_parent,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

-
local crypto endpt.: 192.168.2.2, remote crypto endpt.: 192.168.1.1
path mtu 1500, media mtu 1500
current outbound spi: 0
```

inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:

-

```
local ident (addr/mask/prot/port): (192.168.2.2/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
current_peer: 192.168.1.1
  PERMIT, flags={origin_is_acl,parent_is_transport,}
#pkts encaps: 42, #pkts encrypt: 42, #pkts digest 42
#pkts decaps: 39, #pkts decrypt: 39, #pkts verify 39
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 2, #recv errors 0
```

```
local crypto endpt.: 192.168.2.2, remote crypto endpt.: 192.168.1.1
path mtu 1500, media mtu 1500
current outbound spi: 3C371F6D
```

inbound esp sas:

```
spi: 0xF06835A9(4033361321)
  transform: esp-des esp-md5-hmac ,
  in use settings = {Tunnel, }
  slot: 0, conn id: 940, flow_id: 1, crypto map: myvpn
  sa timing: remaining key lifetime (k/sec): (4607998/2559)
  IV size: 8 bytes
  replay detection support: Y
```

inbound ah sas:

inbound pcp sas:

outbound esp sas:

```
spi: 0x3C371F6D(1010245485)
  transform: esp-des esp-md5-hmac ,
  in use settings = {Tunnel, }
  slot: 0, conn id: 941, flow_id: 2, crypto map: myvpn
  sa timing: remaining key lifetime (k/sec): (4607998/2559)
  IV size: 8 bytes
  replay detection support: Y
```

outbound ah sas:

outbound pcp sas:

A fim verificar que a configuração do Cisco IOS Firewall trabalha corretamente, emita primeiramente este comando.

```
fred#show access-lists 103
```

```
Extended IP access list 103
```

```
  permit gre host 192.168.1.1 host 192.168.2.2 (4 matches)
```



```
permit udp host 192.168.1.1 eq isakmp host 192.168.2.2 (4 matches)
permit esp host 192.168.1.1 host 192.168.2.2 (4 matches)
```

Então de um host na rede 172.16.1.x, tente ao telnet a um host remoto no Internet. Você pode a primeira verificação que o NAT trabalha corretamente. O endereço local de 172.16.1.2 foi traduzido a 192.168.2.10.

```
fred#show access-lists 103
```

```
Extended IP access list 103
```

```
permit gre host 192.168.1.1 host 192.168.2.2 (4 matches)
permit udp host 192.168.1.1 eq isakmp host 192.168.2.2 (4 matches)
permit esp host 192.168.1.1 host 192.168.2.2 (4 matches)
```

```
fred#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
tcp  192.168.2.10:11006   172.16.1.2:11006  192.168.2.1:23    192.168.2.1:23
```

Quando você verifica a lista de acesso outra vez, você vê que uma linha extra está adicionada dinamicamente.

```
fred#show access-lists 103
```

```
Extended IP access list 103
```

```
permit tcp host 192.168.2.1 eq telnet host 192.168.2.10 eq 11006 (11 matches)
permit gre host 192.168.1.1 host 192.168.2.2 (4 matches)
permit udp host 192.168.1.1 eq isakmp host 192.168.2.2 (4 matches)
permit esp host 192.168.1.1 host 192.168.2.2 (4 matches)
```

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

NAT:

- **debug ip nat access-list number** - exibe informações sobre os pacotes IP traduzidos pelo recurso IP NAT.

IPsec:

- **debug crypto ipsec** — Exibe eventos de IPsec.
- **debug crypto isakmp** — Exibe mensagens sobre eventos de Intercâmbio de chave de Internet (IKE).
- **debug crypto engine** — Exibe informações a partir do cripto mecanismo.

CBAC:

- **debug ip inspect {protocolo | }** — mensagens detalhadas dos indicadores sobre eventos do

Cisco IOS Firewall.

Listas de acesso:

- debug ip packet (sem cache da rota de ip na interface)- Exibe informações gerais de depuração de IP e transações de segurança de IPSO (opção de segurança de IP).

daphne#**show version**

```
Cisco Internetwork Operating System Software
IOS (tm) 3700 Software (C3725-ADVSECURITYK9-M), Version 12.3(5a), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Mon 24-Nov-03 20:36 by kellythw
Image text-base: 0x60008AF4, data-base: 0x613C6000
```

```
ROM: System Bootstrap, Version 12.2(8r)T2, RELEASE SOFTWARE (fc1)
```

```
daphne uptime is 6 days, 19 hours, 39 minutes
System returned to ROM by reload
System image file is "flash:c3725-advsecurityk9-mz.123-5a.bin"
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wvl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

```
cisco 3725 (R7000) processor (revision 0.1) with 196608K/65536K bytes of memory.
Processor board ID JHY0727K212
R7000 CPU at 240MHz, Implementation 39, Rev 3.3, 256KB L2 Cache
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
1 Virtual Private Network (VPN) Module(s)
DRAM configuration is 64 bits wide with parity disabled.
55K bytes of non-volatile configuration memory.
125952K bytes of ATA System CompactFlash (Read/Write)
```

```
Configuration register is 0x2002
```

fred#**show version**

```
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-JK9O3S-M), Version 12.2(21a), RELEASE SOFTWARE (fc2)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Fri 09-Jan-04 16:23 by kellmill
Image text-base: 0x60008930, data-base: 0x615DE000
```

```
ROM: System Bootstrap, Version 11.1(20)AA2, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
```

```
fred uptime is 6 days, 19 hours, 36 minutes
System returned to ROM by reload
```

System image file is "flash:c3640-jk9o3s-mz.122-21a.bin"

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wvl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

cisco 3640 (R4700) processor (revision 0x00) with 124928K/6144K bytes of memory.
Processor board ID 25120505
R4700 CPU at 100Mhz, Implementation 33, Rev 1.0
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
2 FastEthernet/IEEE 802.3 interface(s)
4 Serial network interface(s)
4 Serial(sync/async) network interface(s)
1 Virtual Private Network (VPN) Module(s)
DRAM configuration is 64 bits wide with parity disabled.
125K bytes of non-volatile configuration memory.
32768K bytes of processor board System flash (Read/Write)

Configuration register is 0x2002

Nota: Se esta configuração é executada nas etapas, o comando **debug** usar-se depende da peça em falta.

[Informações Relacionadas](#)

- [Negociação IPsec/Protocolos IKE](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)