

Configuración de IPsec de router a router (claves previamente compartidas) en túnel GRE con firewall IOS y NAT

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

Introducción

Este documento ilustra una configuración de Cisco IOS® Firewall básica con Traducción de Dirección de Red (NAT). Esta configuración permite que el tráfico se inicie desde el interior de las redes 10.1.1.x y 172.16.1.x hacia Internet y que sea "NATed" en el trayecto. Se agrega un túnel GRE (Generic Routing Encapsulation) para tunelizar el tráfico IP e IPX entre dos redes privadas. Cuando un paquete llega a la interfaz de salida del router y si se envía por debajo del túnel, primero se encapsula mediante GRE y a continuación se cifra mediante IPsec. Es decir, cualquier tráfico que se permita entrar en el túnel GRE también es cifrado mediante IPsec.

Para configurar el túnel GRE sobre IPsec con OSPF (Open Shortest Path First), consulte [Configuración de un Túnel GRE sobre IPsec con OSPF](#).

Para configurar un diseño IPsec hub y spoke entre tres routers, refiérase a [Configuración del Hub de Router a Router IPsec y Spoke con Comunicación entre los Spokes](#).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Software Cisco IOS versión 12.2(21a) y 12.3(5a)
- Cisco 3725 y 3640

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco para obtener más información sobre las convenciones del documento.](#)

Antecedentes

Los consejos de esta sección le ayudan a implementar la configuración:

- Implemente NAT en ambos routers para probar la conectividad a Internet.
- Agregue GRE a la configuración y prueba. El tráfico no cifrado debe fluir entre las redes privadas.
- Agregue IPsec a la configuración y prueba. El tráfico entre las redes privadas debe ser encriptación.
- Agregue el Cisco IOS Firewall a las interfaces externas, la lista de inspección saliente y la lista de acceso entrante, y realice la prueba.
- Si utiliza una versión del software Cisco IOS anterior a 12.1.4, debe permitir el tráfico IP entre 172.16.1.x y - 10.0.0.0 en la lista de acceso 103. Consulte Cisco bug ID [CSCdu58486](#) (sólo [clientes registrados](#)) y Cisco bug ID [CSCdm01118](#) (sólo [clientes registrados](#)) para obtener más información.

Configurar

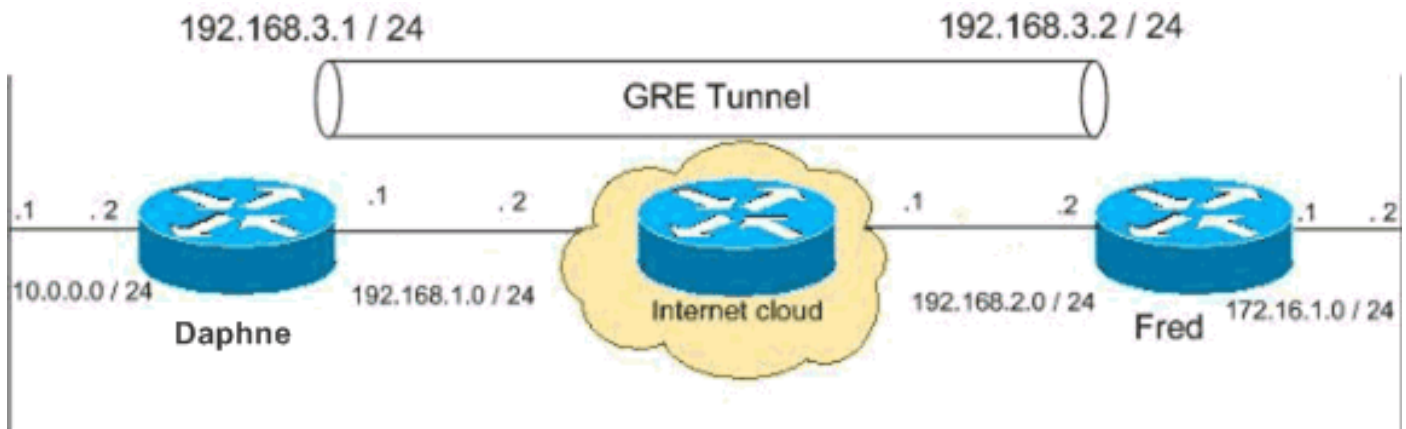
En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use la [Command Lookup Tool](#) (sólo [clientes registrados](#)) para obtener más información sobre los comandos utilizados en este documento.

Nota: Los esquemas de direccionamiento IP utilizados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que se han utilizado en un entorno de laboratorio.

Diagrama de la red

Este documento utiliza esta configuración de red:



Configuraciones

Este documento usa estas configuraciones.

- [Configuración de Daphne](#)
- [Configuración de Fred](#)

Configuración de 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$XKZR118vcId11ZGzhhbz5C/
!
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

```

Configuración de Fred

```

version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname fred
!
enable secret 5 $1$AtxD$MycLGaJvF/tAIFXkikCes1
!
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 supressed. !
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
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\) \(OIT\) soporta ciertos comandos show.](#) Utilice la OIT para ver un análisis del resultado del comando show.

Intente hacer ping a un host en la subred remota - 10.0.0.x desde un host en la red 172.16.1.x para verificar la configuración de VPN. Este tráfico debe atravesar el túnel GRE y cifrarse.

Utilice el comando **show crypto ipsec sa** para verificar que el túnel IPsec esté activo. Primero verifique que los números SPI sean diferentes a 0. También debería ver un aumento en los contadores `pkts encrypt` y `pkts decrypt`.

- **show crypto ipsec sa:** verifica que el túnel IPsec esté activo.
- **show access-lists 103:** verifica que la configuración de Cisco IOS Firewall funcione correctamente.
- **show ip nat translations:** verifica que NAT funcione correctamente.

```
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:
```

Para verificar que la configuración de Cisco IOS Firewall funciona correctamente, ejecute primero 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)
```

Luego, desde un host en la red 172.16.1.x, intente realizar Telnet a un host remoto en Internet. Primero puede verificar que NAT funciona correctamente. La dirección local de 172.16.1.2 se ha traducido a 192.168.2.10.

```
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

Cuando vuelve a comprobar la lista de acceso, verá que se agrega dinámicamente una línea adicional.

```
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)
```

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

[La herramienta Output Interpreter Tool \(clientes registrados solamente\) \(OIT\) soporta ciertos comandos show.](#) Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte [Información Importante sobre Comandos Debug](#) antes de utilizar los comandos debug.

NAT:

- **debug ip nat *access-list number***—Muestra información sobre los paquetes IP traducidos por la función IP NAT.

:

- **debug crypto ipsec** — Muestra eventos de IPSec.
- **debug crypto isakmp** — Muestra mensajes acerca de eventos de intercambio de claves por Internet (IKE).

- **debug crypto engine** — Muestra información del motor de criptografía.

CBAC:

- **debug ip inspect {protocol | detailed}**—Muestra mensajes acerca de los eventos de Cisco IOS Firewall.

Listas de acceso:

- **debug ip packet** (sin **ip route-cache** en la interfaz): muestra la información general de depuración IP y las transacciones de seguridad de la opción de seguridad IP (IPSO).

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-JK903S-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/wwl/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: Si esta configuración se implementa en pasos, el comando **debug** a utilizar depende de la parte defectuosa.

[Información Relacionada](#)

- [Negociación IPSec/Protocolos IKE](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)