# Configurazione di IPsec (chiavi pre-condivise) da router a router sul tunnel GRE con IOS Firewall e NAT

## Sommario



## Introduzione

In questo documento viene illustrata una configurazione di base di Cisco IOS® Firewall con Network Address Translation (NAT). Questa configurazione consente di avviare il traffico dall'interno delle reti 10.1.1.x e 172.16.1.x verso Internet e NATed durante il percorso. Al traffico IP e IPX del tunnel tra due reti private viene aggiunto un tunnel GRE (Generic Routing Encapsulation). Quando un pacchetto arriva all'interfaccia in uscita del router e viene inviato attraverso il tunnel, viene prima incapsulato tramite GRE e quindi criptato con IPsec. In altre parole, tutto il traffico autorizzato ad accedere al tunnel GRE viene anche criptato da IPsec.

Per configurare il tunnel GRE su IPsec con Open Shortest Path First (OSPF), fare riferimento alla configurazione di un tunnel GRE su IPSec con OSPF.

Per configurare una progettazione IPsec hub e spoke tra tre router, fare riferimento alla configurazione di un hub router-router IPsec e di uno spoke con comunicazione tra gli spoke.

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

# Premesse

I suggerimenti in questa sezione consentono di implementare la configurazione:

- Implementare il protocollo NAT su entrambi i router per verificare la connettività Internet.
- Aggiungere il GRE alla configurazione e al test. Il traffico non crittografato deve passare tra le reti private.
- Aggiungere IPSec alla configurazione e al test. Il traffico tra le reti private deve essere crittografato.
- Aggiungere Cisco IOS Firewall alle interfacce esterne, all'elenco di controllo delle connessioni in uscita e all'elenco degli accessi in entrata e verificare.
- Se si usa una versione del software Cisco IOS precedente alla 12.1.4, è necessario autorizzare il traffico IP tra le versioni 172.16.1.x e - 10.0.0.0 nell'elenco degli accessi 103. Per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCdu58486 (solo utenti registrati) e all'ID bug Cisco CSCdm01118 (solo utenti registrati).

# Configurazione

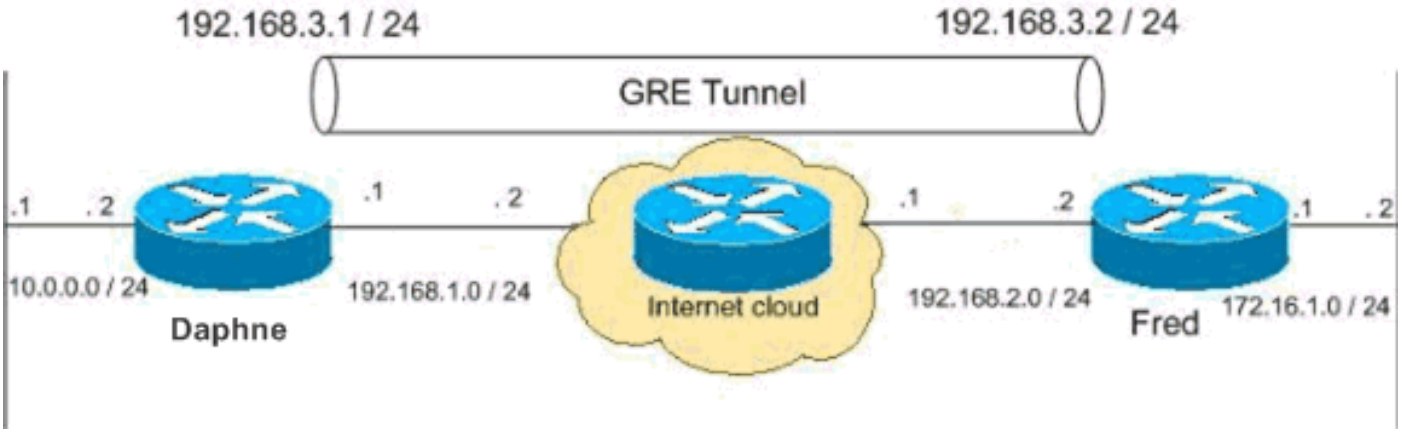
In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

**Nota:** per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

**Nota:** Gli schemi di indirizzamento IP utilizzati in questa configurazione non sono indirizzabili legalmente su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

## Esempio di rete

Nel documento viene usata questa impostazione di rete.




## Configurazioni

Nel documento vengono usate queste configurazioni.

- Configurazione Daphne
- Fred Configuration

**Configurazione 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$XKZR118vcId11ZGzhbz5C/
!
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
```

## Fred Configuration

```
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
```

## Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Provare a eseguire il ping di un host nella subnet remota - 10.0.0.x da un host nella rete 172.16.1.x per controllare la configurazione VPN. Il traffico deve passare attraverso il tunnel GRE ed essere crittografato.

Per verificare che il tunnel IPsec sia attivo, usare il comando **show crypto ipsec sa**. Verificare innanzitutto che i numeri SPI siano diversi da 0. È inoltre necessario verificare un aumento dei contatori `pkts encrypt` e `pkts decrypt`.

- **show crypto ipsec sa**: verifica che il tunnel IPsec sia attivo.
- **show access-lists 103**: verifica che la configurazione di Cisco IOS Firewall funzioni correttamente.
- **show ip nat translation**: verifica che NAT funzioni correttamente.

```
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:
```

Per verificare che la configurazione di Cisco IOS Firewall funzioni correttamente, eseguire prima questo 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)
```

Quindi, da un host della rete 172.16.1.x, provare a connettersi a Telnet a un host remoto su Internet. È possibile verificare innanzitutto che NAT funzioni correttamente. L'indirizzo locale 172.16.1.2 è stato tradotto in 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
```

Quando si controlla nuovamente l'elenco degli accessi, si osserverà che viene aggiunta dinamicamente una riga in più.

```
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)
```

# Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

## Comandi per la risoluzione dei problemi

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

**Nota:** consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

### NAT:

- **debug ip nat *access-list number*: visualizza le informazioni sui pacchetti IP convertiti dalla funzionalità IP NAT.**

### IPSec:

- **debug crypto ipsec**: visualizza gli eventi IPsec.
- **debug crypto isakmp**: visualizza i messaggi sugli eventi IKE (Internet Key Exchange).
- **debug crypto engine**: visualizza le informazioni provenienti dal crypto engine.

## CBAC:

- **debug ip inspect {*protocol* | detail}**: visualizza i messaggi relativi agli eventi di Cisco IOS Firewall.

## Elenchi di accesso:

- **debug ip packet** (**senza ip route-cache** sull'interfaccia): visualizza le informazioni generali sul debug IP e le transazioni di sicurezza IPSO (IP security option).

```
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/wwl/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/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:** se questa configurazione viene implementata nei passaggi, il comando **debug** da utilizzare dipende dalla parte che ha generato l'errore.

# Informazioni correlate

- Negoziazione IPSec/protocolli IKE
- Documentazione e supporto tecnico – Cisco Systems