

Configurazione di IPSec Router-to-Router con mesh completa

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

In questa configurazione di esempio viene mostrata la crittografia a maglia completa tra tre router tramite l'utilizzo di una mappa crittografica su ogni router per le reti dietro ognuno dei due peer.

La crittografia deve essere effettuata da:

- da rete 160.160.160.x a rete 170.170.170.x
- da rete 160.160.160.x a rete 180.180.180.x
- da rete 170.170.170.x a rete 180.180.180.x

[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® versione 12.2.7C e 12.2.8(T)4
- Cisco 2500 e 3600 router

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](#).

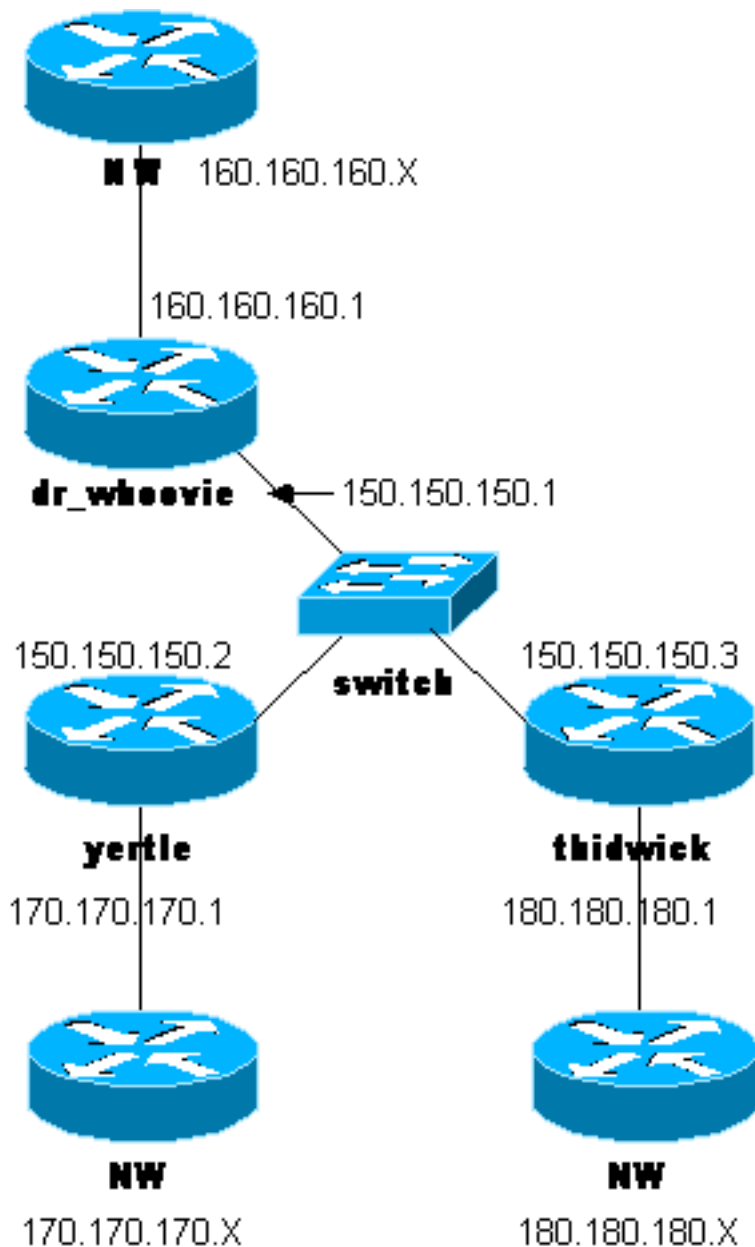
[Configurazione](#)

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](#)).

[Esempio di rete](#)

Nel documento viene usata l'impostazione di rete mostrata nel diagramma.



Configurazioni

Nel documento vengono usate queste configurazioni.

- [Configurazione Dr_Whoovie](#)
- [Configurazione delle iterazioni](#)
- [Configurazione Thidwick](#)

Nota: queste configurazioni sono state recentemente testate con il codice corrente (novembre 2003) all'interno del documento.

Configurazione Dr_Whoovie

```

Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!

```

```
hostname dr_whoovie
!
enable secret 5 $1$KxKv$cbqKsZtQTLJLGPn.tErFZ1
enable password ww
!
ip subnet-zero
!
cns event-service server
!
!--- Internet Key Exchange (IKE) Policies: crypto isakmp
policy 1
authentication pre-share
crypto isakmp key cisco123 address 150.150.150.3
crypto isakmp key cisco123 address 150.150.150.2
!
!--- IPsec Policies: crypto ipsec transform-set 170cisco
esp-des esp-md5-hmac
crypto ipsec transform-set 180cisco esp-des esp-md5-hmac
!
crypto map ETH0 17 ipsec-isakmp
set peer 150.150.150.2
set transform-set 170cisco
!--- Include the 160.160.160.x to 170.170.170.x network
!--- in the encryption process. match address 170
crypto map ETH0 18 ipsec-isakmp
set peer 150.150.150.3
set transform-set 180cisco
!--- Include the 160.160.160.x to 180.180.180.x network
!--- in the encryption process. match address 180
!
interface Ethernet0
ip address 150.150.150.1 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no mop enabled
crypto map ETH0
!
interface Ethernet1
no ip address
no ip directed-broadcast
shutdown
!
interface Serial0
ip address 160.160.160.1 255.255.255.0
no ip directed-broadcast
no ip mroute-cache
no fair-queue
!
interface Serial1
no ip address
no ip directed-broadcast
clockrate 4000000
!
ip classless
ip route 170.170.170.0 255.255.255.0 150.150.150.2
ip route 180.180.180.0 255.255.255.0 150.150.150.3
no ip http server
!
!--- Include the 160.160.160.x to 170.170.170.x network
!--- in the encryption process. access-list 170 permit
ip 160.160.160.0 0.0.0.255 170.170.170.0 0.0.0.255
!--- Include the 160.160.160.x to 180.180.180.x network
!--- in the encryption process. access-list 180 permit
```

```
ip 160.160.160.0 0.0.0.255 180.180.180.0 0.0.0.255
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
line con 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

Configurazione delle iterazioni

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname yertle
!
enable secret 5 $1$me5Q$2kF5zKlPPTvHEBdGiEZ9m/
enable password ww
!
ip subnet-zero
!
cns event-service server
!
!--- IKE Policies: crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco123 address 150.150.150.3
crypto isakmp key cisco123 address 150.150.150.1
!
!--- IPsec Policies: crypto ipsec transform-set 160cisco
esp-des esp-md5-hmac
crypto ipsec transform-set 180cisco esp-des esp-md5-hmac
!
crypto map ETH0 16 ipsec-isakmp
set peer 150.150.150.1
set transform-set 160cisco
!--- Include the 170.170.170.x to 160.160.160.x network
!--- in the encryption process. match address 160
crypto map ETH0 18 ipsec-isakmp
set peer 150.150.150.3
set transform-set 180cisco
!--- Include the 170.170.170.x to 180.180.180.x network
!--- in the encryption process. match address 180
!
interface Ethernet0
ip address 150.150.150.2 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no mop enabled
crypto map ETH0
!
interface Serial0
no ip address
no ip directed-broadcast
no ip mroute-cache
```

```

shutdown
no fair-queue
!
interface Serial1
ip address 170.170.170.1 255.255.255.0
no ip directed-broadcast
!
ip classless
ip route 160.160.160.0 255.255.255.0 150.150.150.1
ip route 180.180.180.0 255.255.255.0 150.150.150.3
no ip http server
!
!--- Include the 170.170.170.x to 160.160.160.x network
!--- in the encryption process. access-list 160 permit
ip 170.170.170.0 0.0.0.255 160.160.160.0 0.0.0.255
!--- Include the 170.170.170.x to 180.180.180.x network
!--- in the encryption process. access-list 180 permit
ip 170.170.170.0 0.0.0.255 180.180.180.0 0.0.0.255
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
line con 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end

```

Configurazione Thidwick

```

Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname thidwick
!
enable secret 5 $l$Pcpo$fj4FNS1dEDY9lGg3Ne6FK1
enable password ww
!
ip subnet-zero
!
isdn switch-type basic-5ess
isdn voice-call-failure 0
cns event-service server
!
!--- IKE Policies: crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco123 address 150.150.150.1
crypto isakmp key cisco123 address 150.150.150.2
!
!--- IPSec Policies: crypto ipsec transform-set 160cisco
esp-des esp-md5-hmac
crypto ipsec transform-set 170cisco esp-des esp-md5-hmac
!
crypto map ETH0 16 ipsec-isakmp
set peer 150.150.150.1
set transform-set 160cisco
!--- Include the 180.180.180.x to 160.160.160.x network

```

```

!--- in the encryption process. match address 160
crypto map ETH0 17 ipsec-isakmp
set peer 150.150.150.2
set transform-set 170cisco
!--- Include the 180.180.180.x to 170.170.170.x network
!--- in the encryption process. match address 170
!
interface Ethernet0
ip address 150.150.150.3 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no mop enabled
crypto map ETH0
!
interface Serial0
no ip address
no ip directed-broadcast
no ip mroute-cache
no fair-queue
clockrate 4000000
!
interface Serial1
ip address 180.180.180.1 255.255.255.0
no ip directed-broadcast
clockrate 4000000
!
interface BRI0
no ip address
no ip directed-broadcast
shutdown
isdn switch-type basic-5ess
!
ip classless
ip route 160.160.160.0 255.255.255.0 150.150.150.1
ip route 170.170.170.0 255.255.255.0 150.150.150.2
no ip http server
!
!--- Include the 180.180.180.x to 160.160.160.x network
!--- in the encryption process. access-list 160 permit
ip 180.180.180.0 0.0.0.255 160.160.160.0 0.0.0.255
!--- Include the 180.180.180.x to 170.170.170.x network
!--- in the encryption process. access-list 170 permit
ip 180.180.180.0 0.0.0.255 170.170.170.0 0.0.0.255
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
line con 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end

```

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show** sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

- **show crypto ipsec sa**: visualizza le impostazioni utilizzate dalle associazioni di protezione [IPSec] correnti.
- **show crypto isakmp sa**: visualizza tutte le associazioni di sicurezza IKE correnti in un peer.

Risoluzione dei problemi

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

Comandi per la risoluzione dei problemi

Nota: prima di usare i comandi di **debug**, consultare le [informazioni importanti sui comandi di debug](#).

- **debug crypto ipsec**: visualizza le negoziazioni IPsec della fase 2.
- **debug crypto isakmp**: visualizza le negoziazioni ISAKMP (Internet Security Association and Key Management Protocol) della fase 1.
- **debug crypto engine**: visualizza il traffico crittografato.
- **clear crypto isakmp**: cancella le associazioni di sicurezza correlate alla fase 1.
- **clear crypto sa**: cancella le associazioni di sicurezza correlate alla fase 2.

Informazioni correlate

- [Pagina di supporto per IPsec](#)
- [Configurazione di IPsec Network Security](#)
- [Configurazione del protocollo di protezione di Internet Key Exchange](#)
- [Supporto tecnico – Cisco Systems](#)