

# Configurazione di IPSec tra tre router tramite indirizzi privati

## 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](#)

Questo documento descrive una configurazione con mesh completa con tre router che utilizzano indirizzi privati. Nell'esempio vengono illustrate le seguenti caratteristiche:

- Encapsulating Security Payload (ESP) - Solo DES (Data Encryption Standard)
- Chiavi già condivise
- Reti private dietro ogni router: 192.168.1.0, 192.168.2.0 e 192.168.3.0
- configurazione mappa crittografica e criteri isakmp
- Il traffico del tunnel definito con i comandi **access-list** e **route-map**. Oltre a Port Address Translation (PAT), le route map possono essere applicate a un NAT (Network Address Translation) statico uno-a-uno sul software Cisco IOS® versione 12.2(4)T2 e successive. Per ulteriori informazioni, fare riferimento a [NAT - Possibilità di utilizzare le route map con panoramica della funzionalità di traduzione statica](#).

**Nota:** la tecnologia di crittografia è soggetta ai controlli sulle esportazioni. È tua responsabilità conoscere la legge relativa all'esportazione della tecnologia di crittografia. In caso di domande sul controllo delle esportazioni, invia un'e-mail a [export@cisco.com](mailto:export@cisco.com).

## [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 12.3(7)T.
- Router Cisco configurati con IPSec.

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](#).

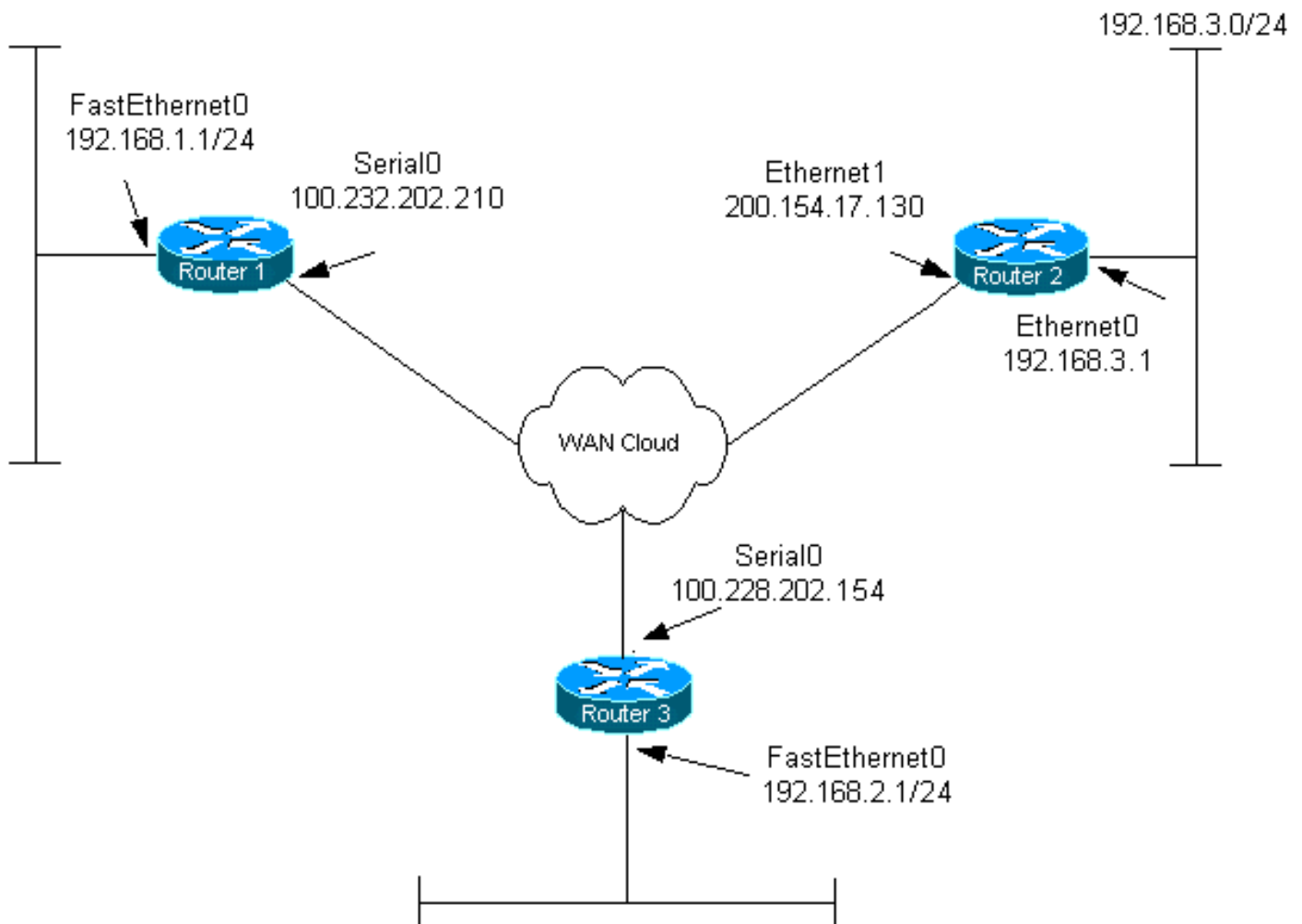
## Configurazione

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 questa impostazione di rete:



## Configurazioni

Nel documento vengono usate queste configurazioni:

- [Router 1](#)
- [Router 2](#)
- [Router 3](#)

### Router 1

```

Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router1
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!

```

```
ip audit po max-events 100
no ftp-server write-enable
!

!--- Configure Internet Key Exchange (IKE) policy and !-
-- pre-shared keys for each peer. !--- IKE policy
defined for peers. crypto isakmp policy 4
authentication pre-share

!--- Pre-shared keys for different peers. crypto isakmp
key xxxxxx1234 address 100.228.202.154
crypto isakmp key xxxxxx1234 address 200.154.17.130
!
!

!--- IPsec policies: crypto ipsec transform-set encrypt-
des esp-des
!
!
crypto map combined local-address Serial0

!--- Set the peer, transform-set and encryption traffic
for tunnel peers. crypto map combined 20 ipsec-isakmp
  set peer 100.228.202.154
  set transform-set encrypt-des
  match address 106
crypto map combined 30 ipsec-isakmp
  set peer 200.154.17.130
  set transform-set encrypt-des
  match address 105
!
!
interface Serial0
  ip address 100.232.202.210 255.255.255.252
  ip nat outside
  serial restart-delay 0

!--- Apply the crypto map to the interface. crypto map
combined
!
interface FastEthernet0
  ip address 192.168.1.1 255.255.255.0
  ip nat inside
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.232.202.209
no ip http server
no ip http secure-server
!

!--- Define traffic for NAT. ip nat inside source route-
map nonat interface Serial0 overload

!--- Access control list (ACL) that shows traffic to
encrypt over the tunnel. access-list 105 permit ip
192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
access-list 106 permit ip 192.168.1.0 0.0.0.255
192.168.2.0 0.0.0.255

!--- ACL to avoid the traffic through NAT over the
tunnel. access-list 150 deny ip 192.168.1.0 0.0.0.255
192.168.2.0 0.0.0.255
access-list 150 deny ip 192.168.1.0 0.0.0.255
192.168.3.0 0.0.0.255
```

```
!--- ACL to perform NAT on the traffic that does not go
over the tunnel. access-list 150 permit ip 192.168.1.0
0.0.0.255 any

!--- Do not perform NAT on the IPSec traffic. route-map
nonat permit 10
  match ip address 150
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

## Router 2

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router2
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!

!--- Configure IKE policy and pre-shared keys for each
peer. !--- IKE policy defined for peers. crypto isakmp
policy 4
  authentication pre-share

!--- Pre-shared keys for different peers. crypto isakmp
key xxxxxx1234 address 100.228.202.154
crypto isakmp key xxxxxx1234 address 100.232.202.210
!
!

!--- IPSec policies. crypto ipsec transform-set encrypt-
des esp-des
!
!
crypto map combined local-address Ethernet1

!--- Set the peer, transform-set and encryption traffic
for tunnel peers. crypto map combined 7 ipsec-isakmp
set peer 100.232.202.210
```

```

    set transform-set encrypt-des
    match address 105

crypto map combined 8 ipsec-isakmp
    set peer 100.228.202.154
    set transform-set encrypt-des
    match address 106
!
!
!
interface Ethernet0
    ip address 192.168.3.1 255.255.255.0
    ip nat inside
!
interface Ethernet1
    ip address 200.154.17.130 255.255.255.224
    ip nat outside

!--- Apply the crypto map to the interface. crypto map
combined
!
ip classless
ip route 0.0.0.0 0.0.0.0 200.154.17.129
no ip http server
no ip http secure-server
!

!--- Define traffic for NAT. ip nat inside source route-
map nonat interface Ethernet1 overload

!--- ACL shows traffic to encrypt over the tunnel.
access-list 105 permit ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255
access-list 106 permit ip 192.168.3.0 0.0.0.255
192.168.2.0 0.0.0.255

!--- ACL to avoid the traffic through NAT over the
tunnel. access-list 150 deny ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255
access-list 150 deny ip 192.168.3.0 0.0.0.255
192.168.2.0 0.0.0.255

!--- ACL to perform NAT on the traffic that does not go
over the tunnel. access-list 150 permit ip any any

!--- Do not perform NAT on the IPsec traffic. route-map
nonat permit 10
    match ip address 150
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end

```

### Configurazione router 3

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router3
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!

!--- Configure IKE policy and pre-shared keys for each
peer. !--- IKE policy defined for peers. crypto isakmp
policy 4
    authentication pre-share

!--- Pre-shared keys for different peers. crypto isakmp
key xxxxxx1234 address 100.232.202.210
crypto isakmp key xxxxxx1234 address 200.154.17.130
!
!

!--- IPsec policies: crypto ipsec transform-set encrypt-
des esp-des
!
!

!--- Set the peer, transform-set and encryption traffic
for tunnel peers. crypto map combined local-address
Serial0
crypto map combined 7 ipsec-isakmp
    set peer 100.232.202.210
    set transform-set encrypt-des
    match address 106
crypto map combined 8 ipsec-isakmp
    set peer 200.154.17.130
    set transform-set encrypt-des
    match address 105
!
!
interface Serial0
    ip address 100.228.202.154 255.255.255.252
    ip nat outside
    serial restart-delay 0

!--- Apply the crypto map to the interface. crypto map
combined
!
    interface FastEthernet0
    ip address 192.168.2.1 255.255.255.0
    ip nat inside
!
```

```

ip classless
ip route 0.0.0.0 0.0.0.0 100.228.202.153
no ip http server
no ip http secure-server
!

!--- Define traffic for NAT. ip nat inside source route-
map nonat interface Serial0 overload

!--- ACL that shows traffic to encrypt over the tunnel.
access-list 105 permit ip 192.168.2.0 0.0.0.255
192.168.3.0 0.0.0.255
access-list 106 permit ip 192.168.2.0 0.0.0.255
192.168.1.0 0.0.0.255

!--- ACL to avoid the traffic through NAT over the
tunnel. access-list 150 deny ip 192.168.2.0 0.0.0.255
192.168.3.0 0.0.0.255
access-list 150 deny ip 192.168.2.0 0.0.0.255
192.168.1.0 0.0.0.255

!--- ACL to perform NAT on the traffic that does not go
over the tunnel. access-list 150 permit ip 192.168.2.0
0.0.0.255 any

!--- Do not perform NAT on the IPSec traffic. route-map
nonat permit 10
    match ip address 150
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
    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 engine connections active**: visualizza i pacchetti crittografati e decrittografati tra peer IPsec.
- **show crypto isakmp sa**: visualizza tutte le associazioni di sicurezza (SA) IKE correnti in un peer.
- **show crypto ipsec sa**: visualizza le impostazioni utilizzate dalle associazioni di protezione (SA) correnti (IPsec).



## Risoluzione dei problemi

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

### Comandi per la risoluzione dei problemi

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

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

**Nota:** i seguenti debug devono essere in esecuzione su entrambi i router IPsec (peer). La cancellazione delle associazioni di protezione deve essere eseguita su entrambi i peer.

- **debug crypto isakmp:** visualizza gli errori durante la fase 1.
- **debug crypto ipsec:** visualizza gli errori durante la fase 2.
- **debug crypto engine:** visualizza le informazioni provenienti dal crypto engine.
- **clear crypto connection *id [slot] / RSM / vip*** - Termina una sessione crittografata in corso. Le sessioni crittografate in genere terminano quando si verifica il timeout della sessione. Per informazioni sul valore connection-id, usare il comando **show crypto cisco connections**.
- **clear crypto isakmp:** cancella le SA di fase 1.
- **clear crypto sa:** cancella le SA di fase 2.

### Informazioni correlate

- [Pagina di supporto per IPsec](#)
- [Supporto tecnico – Cisco Systems](#)