

Tunnel LAN-LAN IPSec tra un Catalyst 6500 con VPN Service Module e un esempio di configurazione del firewall PIX

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione per IPSec con accesso di livello 2 o porta trunk](#)

[Configurazione per IPSec tramite porta di routing](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene descritto come creare un tunnel IPSec da LAN a LAN tra uno switch Cisco Catalyst serie 6500 con IPSec VPN Service Module (W) e un firewall Cisco PIX.

[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(14)SY2 per Catalyst serie 6000 Supervisor Engine, con IPSec VPN Service Module
- Software Cisco PIX Firewall versione 6.3(3)

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

Il Catalyst 6500 VPN Service Module ha due porte Gigabit Ethernet (GE) senza connettori visibili esternamente. Queste porte sono indirizzabili solo a scopo di configurazione. La porta 1 è sempre la porta interna. Questa porta gestisce tutto il traffico da e verso la rete interna. La seconda porta (porta 2) gestisce tutto il traffico da e verso la WAN o le reti esterne. Queste due porte sono sempre configurate in modalità trunking 802.1Q. Il modulo del servizio VPN utilizza una tecnica chiamata Bump In The Wire (BITW) per il flusso dei pacchetti.

I pacchetti vengono elaborati da una coppia di VLAN, una sul layer 3 all'interno della VLAN e una sul layer 2 all'esterno della VLAN. I pacchetti, dall'interno all'esterno, vengono instradati alla VLAN interna tramite un metodo denominato EARL (Encoded Address Recognition Logic). Dopo aver crittografato i pacchetti, il modulo del servizio VPN utilizza la VLAN esterna corrispondente. Nel processo di decrittografia, i pacchetti dall'esterno all'interno vengono collegati al modulo del servizio VPN utilizzando la VLAN esterna. Dopo che il modulo del servizio VPN ha decrittografato il pacchetto e mappato la VLAN alla VLAN interna corrispondente, EARL instrada il pacchetto alla porta LAN appropriata. Il layer 3 all'interno della VLAN e il layer 2 all'esterno della VLAN sono uniti al comando **crypto connect vlan**. Sugli switch Catalyst serie 6500 sono disponibili tre tipi di porte:

- **Porte di routing:** per impostazione predefinita, tutte le porte Ethernet sono porte di routing in Cisco IOS. A queste porte è associata una VLAN nascosta.
- **Porte di accesso:** a queste porte è associata una VLAN esterna o VLAN Trunk Protocol (VTP). È possibile associare più porte a una VLAN definita.
- **Porte trunk:** queste porte trasportano molte VLAN esterne o VTP, sulle quali tutti i pacchetti sono incapsulati con un'intestazione 802.1Q.

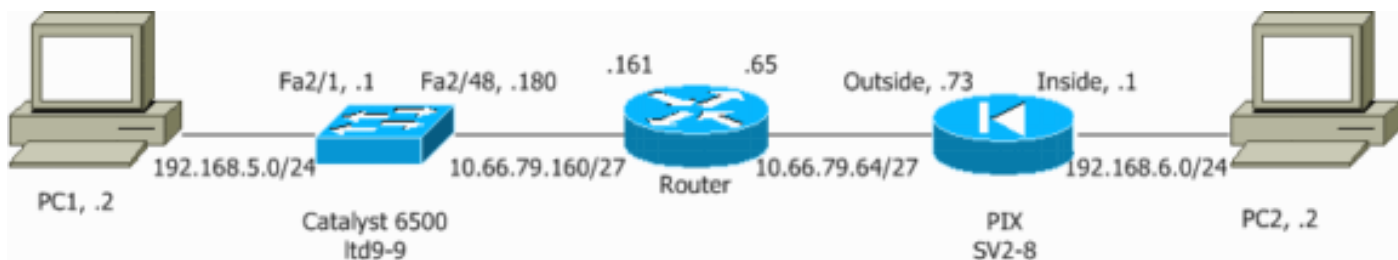
Configurazione

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:



Configurazione per IPSec con accesso di livello 2 o porta trunk

Per configurare IPSec con l'ausilio di una porta di accesso di livello 2 o di una porta trunk per l'interfaccia fisica esterna, eseguire la procedura seguente.

1. Aggiungere le VLAN interne alla porta interna del modulo di servizio VPN. Si supponga che il modulo del servizio VPN si trovi sullo slot 4. Usare la VLAN 100 come VLAN interna e la VLAN 209 come VLAN esterna. Configurare le porte GE del modulo di servizio VPN nel modo seguente:

```
interface GigabitEthernet4/1
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,100,1002-1005
switchport mode trunk
cdp enable
```

```
interface GigabitEthernet4/2
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,209,1002-1005
switchport mode trunk
cdp enable
spanning-tree portfast trunk
```

2. Aggiungere l'interfaccia VLAN 100 e l'interfaccia a cui viene terminato il tunnel (in questo caso interfaccia VLAN 209, come mostrato di seguito).

```
interface Vlan100
ip address 10.66.79.180 255.255.255.224
```

```
interface Vlan209
no ip address
crypto connect vlan 100
```

3. Configurare la porta fisica esterna come porta di accesso o porta trunk (in questo caso, Fast Ethernet 2/48, come mostrato di seguito).

```
!--- This is the configuration that uses an access port. interface FastEthernet2/48
no ip address
switchport
switchport access vlan 209
switchport mode access
```

```
!--- This is the configuration that uses a trunk port. interface FastEthernet2/48
```

```
no ip address switchport
switchport trunk encapsulation dot1q
switchport mode trunk
```

4. Creare il NAT di bypass. Aggiungere queste voci all'istruzione no nat per esentare le connessioni tra queste reti:

```
access-list inside_nat0_outbound permit ip 192.168.5.0 0.0.0.255
192.168.6.0 0.0.0.255
global (outside) 1 interface
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 192.168.5.0 255.255.255.0
```

5. Creare la configurazione crittografica e l'elenco di controllo di accesso (ACL) che definisce il traffico da crittografare. Creare un ACL crittografico (in questo caso, ACL 100 - Traffico interessante) che definisca il traffico dalla rete interna 192.168.5.0/24 alla rete remota 192.168.6.0/24, come mostrato di seguito:

```
access-list 100 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
```

Definire le proposte di criteri ISAKMP (Internet Security Association and Key Management Protocol), ad esempio:

```
crypto isakmp policy 1
hash md5
authentication pre-share
group 2
```

Utilizzare questo comando (in questo esempio) per utilizzare e definire le chiavi già condivise:

```
crypto isakmp key cisco address 10.66.79.73
```

Definire le proposte IPsec nel modo seguente:

```
crypto ipsec transform-set cisco esp-des esp-md5-hmac
```

Creare l'istruzione per la mappa crittografica, nel modo seguente:

```
crypto map cisco 10 ipsec-isakmp
set peer 10.66.79.73
set transform-set cisco
match address 100
```

6. Applicare la mappa crittografica all'interfaccia VLAN 100, nel modo seguente:

```
interface vlan100
crypto map cisco
```

Vengono utilizzate le seguenti configurazioni:

- [Catalyst 6500](#)
- [PIX Firewall](#)

Catalyst 6500

```

!--- Define the Phase 1 policy. crypto isakmp policy 1
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco address 10.66.79.73
!
!
!--- Define the encryption policy for this setup. crypto
ipsec transform-set cisco esp-des esp-md5-hmac
!
!--- Define a static crypto map entry for the peer !---
with mode ipsec-isakmp. !--- This indicates that
Internet Key Exchange (IKE) !--- is used to establish
the IPsec !--- security associations (SAs) to protect
the traffic !--- specified by this crypto map entry.
crypto map cisco 10 ipsec-isakmp
  set peer 10.66.79.73
  set transform-set cisco
  match address 100
!
!
no spanning-tree vlan 100
!
!
!
interface FastEthernet2/1
  ip address 192.168.5.1 255.255.255.0
!
!--- This is the outside Layer 2 port that allows !---
VLAN 209 traffic to enter. interface FastEthernet2/48 no
ip address switchport switchport trunk encapsulation
dot1q switchport mode trunk ! interface
GigabitEthernet4/1 no ip address flowcontrol receive on
flowcontrol send off switchport switchport trunk
encapsulation dot1q !--- VLAN 100 is defined as the
Interface VLAN (IVLAN).  switchport trunk allowed vlan
1,100,1002-1005
  switchport mode trunk
  cdp enable
!
interface GigabitEthernet4/2
  no ip address
  flowcontrol receive on
  flowcontrol send off
  switchport
  switchport trunk encapsulation dot1q
!--- The Port VLAN (PVLAN) configuration is handled
transparently by !--- the VPN service module without
user configuration !--- or involvement. It also is not
shown in the configuration. !--- Note: For every IVLAN,
a corresponding PVLAN exists.

  switchport trunk allowed vlan 1,209,1002-1005
  switchport mode trunk
  cdp enable
  spanning-tree portfast trunk
!
interface Vlan1
  no ip address
  shutdown
!
!--- This is the IVLAN that is configured to intercept
the traffic !--- destined to the secure port on which
the inside port !--- of the VPN service module is the

```

```

only port present. interface Vlan100 ip address
10.66.79.180 255.255.255.224 crypto map cisco
!--- This is the secure port that is a virtual Layer 3
interface. !--- This interface purposely does not have a
Layer 3 IP address !--- configured. This is normal for
the BITW process. !--- The IP address is moved from this
interface to the VLAN 100 to !--- accomplish BITW. This
brings the VPN service module into !--- the packet path.
interface Vlan209 no ip address crypto connect vlan 100
!
ip classless

global (outside) 1 interface
!--- NAT 0 prevents NAT for networks specified in the
ACL inside_nat0_outbound. nat (inside) 0 access-list
inside_nat0_outbound nat (inside) 1 192.168.5.0
255.255.255.0 !--- Configure the routing so that the
device !--- is directed to reach its destination
network. ip route 0.0.0.0 0.0.0.0 10.66.79.161
!--- This access list (inside_nat0_outbound) is used
with the nat zero command. !--- This prevents traffic
which matches the access list from undergoing !---
network address translation (NAT). The traffic specified
by this ACL is !--- traffic that is to be encrypted and
!--- sent across the VPN tunnel. This ACL is
intentionally !--- the same as (100). !--- Two separate
access lists should always be used in this
configuration. access-list inside_nat0_outbound permit
ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255

!--- This is the crypto ACL. access-list 100 permit ip
192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255

```

PIX Firewall

```

SV2-8(config)# show run
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
interface ethernet6 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
nameif ethernet3 intf3 security15
nameif ethernet4 intf4 security20
nameif ethernet5 intf5 security25
nameif ethernet6 intf6 security30
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname SV2-8
domain-name cisco.com
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389

```

```
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
!--- This is the traffic to the router. access-list 100
permit ip 192.168.6.0 255.255.255.0 192.168.5.0
255.255.255.0
access-list nonat permit ip 192.168.6.0 255.255.255.0
192.168.5.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
mtu intf6 1500
ip address outside 10.66.79.73 255.255.255.224
ip address inside 192.168.6.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
no ip address intf3
no ip address intf4
no ip address intf5
no ip address intf6
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
no failover ip address intf6
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 192.168.6.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 10.66.79.65 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- These are IPsec policies. sysopt connection permit-
ipsec
crypto ipsec transform-set cisco esp-des esp-md5-hmac
```

```

crypto map cisco 10 ipsec-isakmp
crypto map cisco 10 match address 100
crypto map cisco 10 set peer 10.66.79.180
crypto map cisco 10 set transform-set cisco
crypto map cisco interface outside
!--- These are IKE policies. isakmp enable outside
isakmp key ***** address 10.66.79.180 netmask
255.255.255.255
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:244c86c9beab00bda8f790502ca74db9
: end

```

Configurazione per IPSec tramite porta di routing

Per configurare IPSec con l'ausilio di una porta di routing di layer 3 per l'interfaccia fisica esterna, eseguire la procedura seguente.

1. Aggiungere le VLAN interne alla porta interna del modulo di servizio VPN. Si supponga che il modulo del servizio VPN si trovi sullo slot 4. Usare la VLAN 100 come VLAN interna e la VLAN 209 come VLAN esterna. Configurare le porte GE del modulo di servizio VPN nel modo seguente:

```

interface GigabitEthernet4/1
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,100,1002-1005
switchport mode trunk
cdp enable

```

```

interface GigabitEthernet4/2
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,209,1002-1005
switchport mode trunk
cdp enable
spanning-tree portfast trunk

```

2. Aggiungere l'interfaccia VLAN 100 e l'interfaccia a cui viene terminato il tunnel (in questo caso Fast Ethernet 2/48, come mostrato di seguito).

```

interface Vlan100
ip address 10.66.79.180 255.255.255.224

```

```

interface FastEthernet2/48
no ip address
crypto connect vlan 100

```


3. Creare il NAT di bypass. Aggiungere queste voci all'istruzione no nat per esentare le connessioni tra queste reti:

```
access-list inside_nat0_outbound permit ip 192.168.5.0 0.0.0.255
192.168.6.0 0.0.0.255
global (outside) 1 interface
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 192.168.5.0 255.255.255.0
```

4. Creare la configurazione crittografica e l'ACL che definisce il traffico da crittografare. Creare un ACL (in questo caso, ACL 100) che definisca il traffico dalla rete interna 192.168.5.0/24 alla rete remota 192.168.6.0/24, come mostrato di seguito:

```
access-list 100 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
```

Definire le proposte di policy ISAKMP nel modo seguente:

```
crypto isakmp policy 1
hash md5
authentication pre-share
group 2
```

Utilizzare questo comando (in questo esempio) per utilizzare e definire le chiavi già condivise:

```
crypto isakmp key cisco address 10.66.79.73
```

Definire le proposte IPsec nel modo seguente:

```
crypto ipsec transform-set cisco esp-des esp-md5-hmac
```

Creare l'istruzione per la mappa crittografica, nel modo seguente:

```
crypto map cisco 10 ipsec-isakmp
set peer 10.66.79.73
set transform-set cisco
match address 100
```

5. Applicare la mappa crittografica all'interfaccia VLAN 100, nel modo seguente:

```
interface vlan100
crypto map cisco
```

Vengono utilizzate le seguenti configurazioni:

- [Catalyst 6500](#)
- [PIX Firewall](#)

Catalyst 6500

```
!--- Define the Phase 1 policy. crypto isakmp policy 1
hash md5
authentication pre-share
group 2
crypto isakmp key cisco address 10.66.79.73
```

```

!
!
!--- Define the encryption policy for this setup. crypto
ipsec transform-set cisco esp-des esp-md5-hmac
!
!--- Define a static crypto map entry for the peer !---
with mode ipsec-isakmp. !--- This indicates that IKE is
used to establish the !--- IPSec SAs to protect the
traffic !--- specified by this crypto map entry. crypto
map cisco 10 ipsec-isakmp
  set peer 10.66.79.73
  set transform-set cisco
  match address 100
!
!
no spanning-tree vlan 100
!
!
!
interface FastEthernet2/1
  ip address 192.168.5.1 255.255.255.0
!
!--- This is the secure port that is configured in
routed port mode. !--- This routed port mode does not
have a Layer 3 IP address !--- configured. This is
normal for the BITW process. !--- The IP address is
moved from this interface to the VLAN 100 to !---
accomplish BITW. This brings the VPN service module into
!--- the packet path. This is the Layer 2 port VLAN on
which the !--- outside port of the VPN service module
also belongs. ! interface FastEthernet2/48 no ip address
crypto connect vlan 100
!
interface GigabitEthernet4/1
  no ip address
  flowcontrol receive on
  flowcontrol send off
  switchport
  switchport trunk encapsulation dot1q
!--- VLAN 100 is defined as the IVLAN. switchport trunk
allowed vlan 1,100,1002-1005
  switchport mode trunk
  cdp enable
!
interface GigabitEthernet4/2
  no ip address
  flowcontrol receive on
  flowcontrol send off
  switchport
  switchport trunk encapsulation dot1q
!--- The PVLAN configuration is handled transparently by
the !--- VPN service module without user configuration
!--- or involvement. It also is not shown in the
configuration. !--- Note: For every IVLAN, a
corresponding PVLAN exists.

switchport trunk allowed vlan 1,209,1002-1005
  switchport mode trunk
  cdp enable
  spanning-tree portfast trunk
!
interface Vlan1
  no ip address
  shutdown

```

```

!
!--- This is the IVLAN that is configured to intercept
the traffic !--- destined to the secure port on which
the inside port of the !--- VPN service module is the
only port present. interface Vlan100 ip address
10.66.79.180 255.255.255.224 crypto map cisco
!--- This is the secure port that is a virtual Layer 3
interface. !--- This interface purposely does not have a
Layer 3 IP address !--- configured. This is normal for
the BITW process. !--- The IP address is moved from this
interface to the VLAN 100 to !--- accomplish BITW. This
brings the VPN service module into !--- the packet path.
! ip classless global (outside) 1 interface !--- NAT 0
prevents NAT for networks specified in the ACL
inside_nat0_outbound. nat (inside) 0 access-list
inside_nat0_outbound nat (inside) 1 192.168.6.0
255.255.255.0 !--- Configure the routing so that the
device !--- is directed to reach its destination
network. ip route 0.0.0.0 0.0.0.0 10.66.79.161
!
!--- This access list (inside_nat0_outbound) is used
with the nat zero command. !--- This prevents traffic
which matches the access list from undergoing !---
network address translation (NAT). The traffic specified
by this ACL is !--- traffic that is to be encrypted and
!--- sent across the VPN tunnel. This ACL is
intentionally !--- the same as (100). !--- Two separate
access lists should always be used in this
configuration.

access-list inside_nat0_outbound permit ip 192.168.5.0
0.0.0.255 192.168.6.0 0.0.0.255

!--- This is the crypto ACL. access-list 100 permit ip
192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255

```

PIX Firewall

```

SV2-8(config)# show run
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
interface ethernet6 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
nameif ethernet3 intf3 security15
nameif ethernet4 intf4 security20
nameif ethernet5 intf5 security25
nameif ethernet6 intf6 security30
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname SV2-8
domain-name cisco.com
fixup protocol dns maximum-length 512

```

```
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
!--- This is the traffic to the router. access-list 100
permit ip 192.168.6.0 255.255.255.0 192.168.5.0
255.255.255.0
access-list nonat permit ip 192.168.6.0 255.255.255.0
192.168.5.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
mtu intf6 1500
ip address outside 10.66.79.73 255.255.255.224
ip address inside 192.168.6.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
no ip address intf3
no ip address intf4
no ip address intf5
no ip address intf6
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
no failover ip address intf6
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 192.168.6.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 10.66.79.65 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
```

```
no snmp-server enable traps
floodguard enable
!--- These are IPsec policies. sysopt connection permit-
ipsec
crypto ipsec transform-set cisco esp-des esp-md5-hmac
crypto map cisco 10 ipsec-isakmp
crypto map cisco 10 match address 100
crypto map cisco 10 set peer 10.66.79.180
crypto map cisco 10 set transform-set cisco
crypto map cisco interface outside
!--- These are IKE policies. isakmp enable outside
isakmp key ***** address 10.66.79.180 netmask
255.255.255.255
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:244c86c9beab00bda8f790502ca74db9
: end
```

Verifica

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

Lo [strumento Output Interpreter](#) (solo utenti [registrati](#)) (OIT) supporta alcuni comandi **show**. Usare l'OIT per 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 protezione IKE correnti in un peer.
- **show crypto vlan**: visualizza la VLAN associata alla configurazione crittografica.
- **show crypto eli**: visualizza le statistiche del modulo del servizio VPN.

Per ulteriori informazioni sulla verifica e la risoluzione dei problemi relativi a IPsec, consultare il documento sulla [risoluzione dei problemi di protezione IP - descrizione e uso dei comandi di debug](#).

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 della fase 1.
- **debug crypto engine**: visualizza il traffico crittografato.
- **clear crypto isakmp**: cancella le SA correlate alla fase 1.
- **clear crypto sa**: cancella le SA relative alla fase 2.

Per ulteriori informazioni sulla verifica e la risoluzione dei problemi relativi a IPsec, consultare il documento sulla [risoluzione dei problemi di protezione IP - descrizione e uso dei comandi di debug](#).

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](#)