

Configurazione di IPsec (Hub and Spoke) da PIX a PIX

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Cancella associazioni di protezione](#)

[Informazioni correlate](#)

[Introduzione](#)

Questa configurazione consente a un Cisco Secure PIX Firewall centrale di comunicare con le reti dietro altre due scatole PIX Firewall tramite tunnel VPN su Internet o su qualsiasi rete pubblica utilizzando IPsec. Le due reti esterne non hanno bisogno di comunicare tra loro, ma c'è connettività alla rete centrale. Le due reti esterne non sono in grado di comunicare tra loro passando attraverso il PIX centrale perché il PIX non instrada il traffico ricevuto su un'interfaccia verso la stessa interfaccia. In caso sia necessario che le reti esterne comunichino tra loro, è necessaria una configurazione a maglia completa, anziché la configurazione hub e spoke mostrata in questo documento. Potrebbero essere già presenti istruzioni **nat 1**, **global**, **static** e **conduit** sui PIX. In questo esempio viene illustrata solo l'aggiunta della crittografia.

[Prerequisiti](#)

[Requisiti](#)

Affinché IPsec funzioni, è *necessario* stabilire la connettività tra gli endpoint del tunnel prima di avviare questa configurazione.

[Componenti usati](#)

Le informazioni di questo documento si basano sulle versioni 5.1.x, 5.2.x e 6.3.3 di PIX Firewall.

Nota: il comando `show version` deve indicare che la crittografia è abilitata.

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

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

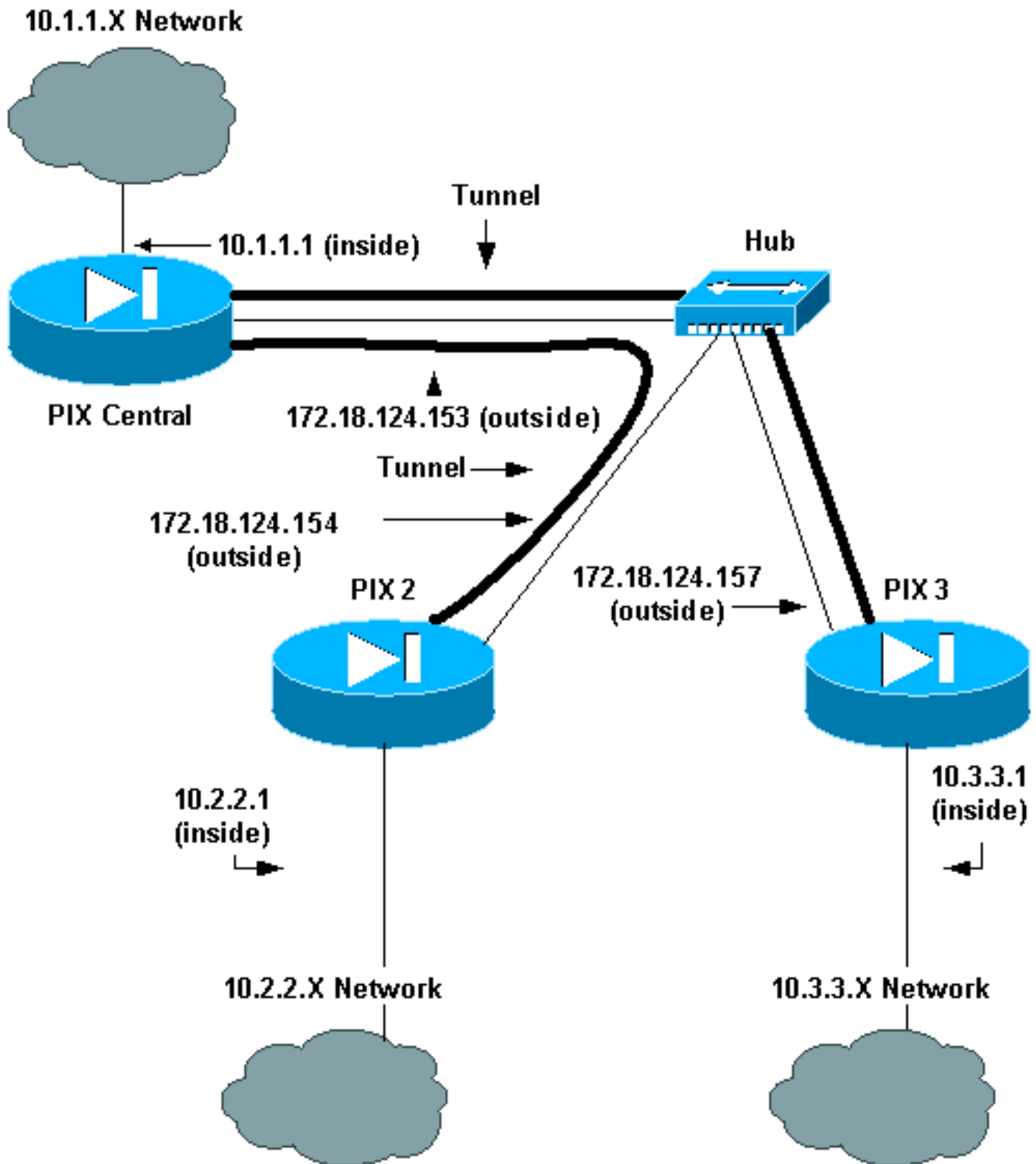
Configurazione

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 questa sezione, 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:

- [PIX Central](#)
- [PIX 2](#)
- [PIX 3](#)

PIX Central

Building configuration...
: Saved

```
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix-central
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 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 traffic to PIX 2. access-list 120 permit ip
10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
!--- This is traffic to PIX 3. access-list 130 permit ip
10.1.1.0 255.255.255.0 10.3.3.0 255.255.255.0
!--- Do not do Network Address Translation (NAT) on
traffic to other PIXes. access-list 100 permit ip
10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
access-list 100 permit ip 10.1.1.0 255.255.255.0
10.3.3.0 255.255.255.0
pager lines 24
logging on
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.153 255.255.255.0
ip address inside 10.1.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
!--- Do not do NAT on traffic to other PIXes. nat
(inside) 0 access-list 100
route outside 0.0.0.0 0.0.0.0 172.18.124.1 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
snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-des esp-md5-hmac
!--- This is traffic to PIX 2. crypto map newmap 20
ipsec-isakmp
crypto map newmap 20 match address 120
```

```
crypto map newmap 20 set peer 172.18.124.154
crypto map newmap 20 set transform-set myset
!--- This is traffic to PIX 3. crypto map newmap 30
ipsec-isakmp
crypto map newmap 30 match address 130
crypto map newmap 30 set peer 172.18.124.157
crypto map newmap 30 set transform-set myset
crypto map newmap interface outside
isakmp enable outside
isakmp key ***** address 172.18.124.154 netmask
255.255.255.255
    no-xauth no-config-mode
isakmp key ***** address 172.18.124.157 netmask
255.255.255.255
    no-xauth no-config-mode
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 1000
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

PIX 2

```
Building configuration...
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix2
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 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 traffic to PIX Central. access-list 110
permit ip 10.2.2.0 255.255.255.0 10.1.1.0 255.255.255.0
!--- Do not do NAT on traffic to PIX Central. access-
list 100 permit ip 10.2.2.0 255.255.255.0 10.1.1.0
255.255.255.0
pager lines 24
logging on
mtu outside 1500
```

```
mtu inside 1500
ip address outside 172.18.124.154 255.255.255.0
ip address inside 10.2.2.1 255.255.255.0
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
pdm history enable
arp timeout 14400
!--- Do not do NAT on traffic to PIX Central. nat
(inside) 0 access-list 100
route outside 0.0.0.0 0.0.0.0 172.18.124.1 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
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-des esp-md5-hmac
!--- This is traffic to PIX Central. crypto map newmap
10 ipsec-isakmp
crypto map newmap 10 match address 110
crypto map newmap 10 set peer 172.18.124.153
crypto map newmap 10 set transform-set myset
crypto map newmap interface outside
isakmp enable outside
isakmp key ***** address 172.18.124.153 netmask
255.255.255.255
no-xauth no-config-mode
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 1000
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

PIX 3

```
Building configuration...
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
```

```
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix3
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 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 traffic to PIX Central. access-list 110
permit ip 10.3.3.0 255.255.255.0 10.1.1.0 255.255.255.0
!--- Do not do NAT on traffic to PIX Central. access-
list 100 permit ip 10.3.3.0 255.255.255.0 10.1.1.0
255.255.255.0
pager lines 24
logging on
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.157 255.255.255.0
ip address inside 10.3.3.1 255.255.255.0
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
pdm history enable
arp timeout 14400
!--- Do not do NAT on traffic to PIX Central. nat
(inside) 0 access-list 100
route outside 0.0.0.0 0.0.0.0 172.18.124.1 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
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-des esp-md5-hmac
!--- This is traffic to PIX Central. crypto map newmap
10 ipsec-isakmp
crypto map newmap 10 match address 110
crypto map newmap 10 set peer 172.18.124.153
crypto map newmap 10 set transform-set myset
crypto map newmap interface outside
isakmp enable outside
```

```

isakmp key ***** address 172.18.124.153 netmask
255.255.255.255
    no-xauth no-config-mode
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 1000
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:aa3bbd8c6275d214b153e1e0bc0173e4
: 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**.

- **show crypto ipsec sa**: visualizza lo stato corrente delle associazioni di sicurezza (SA) IPsec ed è utile per determinare se il traffico è crittografato.

```
pix-central#show crypto ipsec sa
```

```
interface: outside
```

```
    Crypto map tag: newmap, local addr. 172.18.124.153
```

```
    local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
```

```
    remote ident (addr/mask/prot/port): (10.3.3.0/255.255.255.0/0/0)
```

```
    current_peer: 172.18.124.157:500
```

```
        PERMIT, flags={origin_is_acl,}
```

```
!--- This verifies that encrypted packets are sent !--- and received without any errors.
```

```
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
```

```
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
```

```
    #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.: 172.18.124.153,
```

```
    remote crypto endpt.: 172.18.124.157
```

```
    path mtu 1500, ipsec overhead 56, media mtu 1500
```

```
    current outbound spi: 3bcb6913
```

```
!--- Shows inbound SAs that are established. inbound esp sas:
```

```
    spi: 0x3efbe540(1056695616)
```

```
        transform: esp-des esp-md5-hmac ,
```

```
        in use settings ={Tunnel, }
```

```
        slot: 0, conn id: 3, crypto map: newmap
```

```
        sa timing: remaining key lifetime (k/sec): (4607999/27330)
```

```
        IV size: 8 bytes
```

```
        replay detection support: Y
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
!--- Shows outbound SAs that are established. outbound esp sas:
```

```
    spi: 0x3bcb6913(1003186451)
```

```
        transform: esp-des esp-md5-hmac ,
```

```
        in use settings ={Tunnel, }
```



```
slot: 0, conn id: 4, crypto map: newmap
sa timing: remaining key lifetime (k/sec): (4607999/27321)
IV size: 8 bytes
replay detection support: Y
```

outbound ah sas:

outbound pcp sas:

```
local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
current_peer: 172.18.124.154:500
PERMIT, flags={origin_is_acl,}
```

!--- This verifies that encrypted packets are sent !--- and received without any errors.

```
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
#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.: 172.18.124.153,
remote crypto endpt.: 172.18.124.154
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: da8d556
```

!--- Shows inbound SAs that are established. inbound esp sas: spi: 0x53835c96(1401117846)

```
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: newmap
sa timing: remaining key lifetime (k/sec): (4607999/27319)
IV size: 8 bytes
replay detection support: Y
```

inbound ah sas:

inbound pcp sas:

!--- Shows outbound SAs that are established. outbound esp sas: spi: 0xda8d556c(3666695532)

```
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: newmap
sa timing: remaining key lifetime (k/sec): (4607999/27319)
IV size: 8 bytes
replay detection support: Y
```

outbound ah sas:

outbound pcp sas:

- **show crypto isakmp sa:** visualizza lo stato corrente delle associazioni di sicurezza IKE (Internet Key Exchange).

```
pix-central#show crypto isakmp sa
Total      : 2
Embryonic  : 0
dst          src          state      pending   created
-----
172.18.124.153 172.18.124.154 QM_IDLE    0         0
172.18.124.153 172.18.124.157 QM_IDLE    0         0
```

Risoluzione dei problemi

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

[Comandi per la risoluzione dei problemi](#)

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

Sul PIX (con i comandi di **debug** del **monitor di registrazione** o di **debug della console di registrazione** in esecuzione):

- **debug crypto ipsec:** esegue il debug dell'elaborazione IPsec.
- **debug crypto isakmp:** esegue il debug dell'elaborazione ISAKMP (Internet Security Association and Key Management Protocol).
- **debug crypto engine:** visualizza i messaggi di debug sui motori di crittografia, che eseguono la crittografia e la decrittografia.

[Cancella associazioni di protezione](#)

Utilizzare questi comandi nella modalità di configurazione del PIX:

- **clear [crypto] ipsec sa:** elimina le SA IPsec attive. la parola chiave **crypto** è facoltativa.
- **clear [crypto] isakmp sa:** elimina le SA IKE attive. la parola chiave **crypto** è facoltativa.

[Informazioni correlate](#)

- [Software Cisco PIX Firewall](#)
- [Riferimenti per i comandi di Cisco Secure PIX Firewall](#)
- [Avvisi sui prodotti per la sicurezza \(inclusi PIX\)](#)
- [RFC \(Requests for Comments\)](#)
- [Negoziazione IPSec/protocolli IKE](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)