

PIX/ASA 7.x: Esempio di configurazione di aggiunta/rimozione di una rete in un tunnel VPN L2L esistente

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Prodotti correlati](#)

[Convenzioni](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Aggiunta di una rete al tunnel IPsec](#)

[Rimozione della rete dal tunnel IPsec](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene fornita una configurazione di esempio per aggiungere una nuova rete a un tunnel VPN esistente.

[Prerequisiti](#)

[Requisiti](#)

Prima di provare la configurazione, verificare di disporre di un'appliance di sicurezza PIX/ASA con codice 7.x.

[Componenti usati](#)

Per la stesura del documento, sono stati usati due dispositivi Cisco 5500 Security Appliance.

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.

[Prodotti correlati](#)

Questa configurazione può essere utilizzata anche con l'appliance di sicurezza PIX 500.

[Convenzioni](#)

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

[Premesse](#)

Attualmente è presente un tunnel VPN da LAN a LAN (L2L) tra l'ufficio NY e l'ufficio TN. L'ufficio di NY ha appena aggiunto una nuova rete che sarà utilizzata dal gruppo di sviluppo CSI. Questo gruppo richiede l'accesso alle risorse che risiedono nell'ufficio TN. La procedura consiste nell'aggiungere la nuova rete al tunnel VPN già esistente.

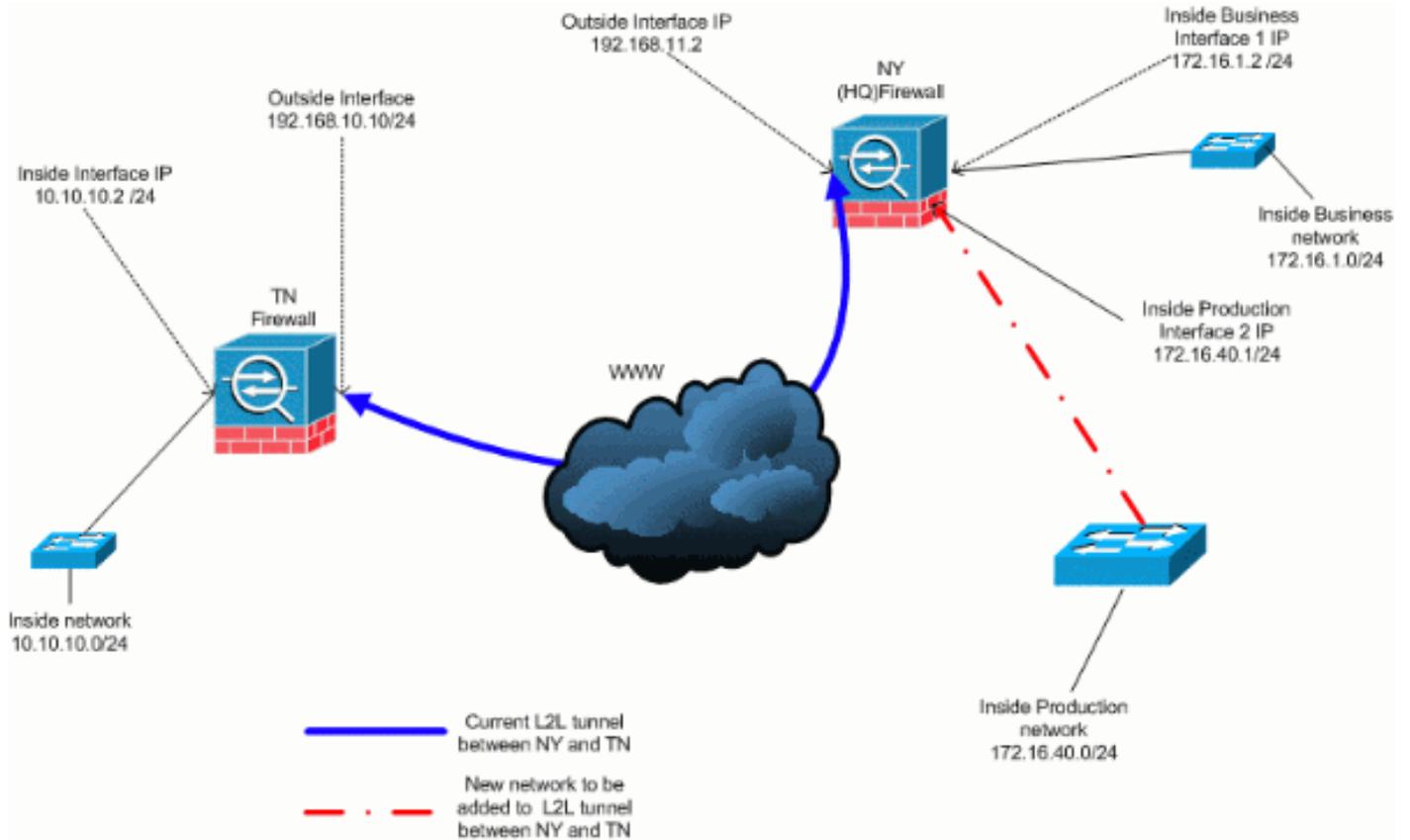
[Configurazione](#)

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:



Aggiunta di una rete al tunnel IPsec

Nel documento viene usata questa configurazione:

Configurazione firewall NY (HQ)

```

ASA-NY-HQ#show running-config

: Saved
:
ASA Version 7.2(2)
!
hostname ASA-NY-HQ
domain-name corp2.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.11.2 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet0/2
 nameif Cisco
 security-level 70
 ip address 172.16.40.2 255.255.255.0

```

```
!  
interface Ethernet0/3  
  shutdown  
  no nameif  
  no security-level  
  no ip address  
!  
interface Management0/0  
  shutdown  
  no nameif  
  no security-level  
  no ip address  
!  
passwd 2KFQnbNIdI.2KYOU encrypted  
ftp mode passive  
dns server-group DefaultDNS  
  domain-name corp2.com  
access-list inside_nat0_outbound extended permit ip  
172.16.1.0  
 255.255.255.0 10.10.10.0 255.255.255.0  
  
!--- You must be sure that you configure the !---  
opposite of these access control lists !--- on the other  
end of the VPN tunnel. access-list inside_nat0_outbound  
extended permit ip 172.16.40.0  
255.255.255.0 10.10.10.0 255.255.255.0  
  
access-list outside_20_cryptomap extended permit ip  
172.16.1.0  
 255.255.255.0 10.10.10.0 255.255.255.0  
  
!--- You must be sure that you configure the !---  
opposite of these access control lists !--- on the other  
end of the VPN tunnel. access-list outside_20_cryptomap  
extended permit ip 172.16.40.0  
255.255.255.0 10.10.10.0 255.255.255.0  
  
!--- Output is suppressed. nat-control global (outside)  
1 interface nat (inside) 0 access-list  
inside_nat0_outbound nat (inside) 1 172.16.1.0  
255.255.255.0 !--- The new network is also required to  
have access to the Internet. !--- So enter an entry into  
the NAT statement for this new network. nat (inside) 1  
172.16.40.0 255.255.255.0  
  
route outside 0.0.0.0 0.0.0.0 192.168.11.100 1  
timeout xlate 3:00:00  
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00  
icmp 0:00:02  
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp  
0:05:00 mgcp-pat 0:05:00  
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00  
sip-disconnect 0:02:00  
timeout uauth 0:05:00 absolute  
no snmp-server location  
no snmp-server contact  
snmp-server enable traps snmp authentication linkup  
linkdown coldstart  
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-  
sha-hmac  
crypto map outside_map 20 match address  
outside_20_cryptomap  
crypto map outside_map 20 set peer 192.168.10.10  
crypto map outside_map 20 set transform-set ESP-3DES-SHA
```

```
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp nat-traversal 20
tunnel-group 192.168.10.10 type ipsec-l2l
tunnel-group 192.168.10.10 ipsec-attributes
 pre-shared-key *
!--- Output is suppressed. : end ASA-NY-HQ#
```

Rimozione della rete dal tunnel IPsec

Utilizzare questa procedura per rimuovere la rete dalla configurazione del tunnel IPsec. In questo caso, tenere presente che la rete 172.16.40.0/24 è stata rimossa dalla configurazione di NY (HQ) Security Appliance.

1. Prima di rimuovere la rete dal tunnel, interrompere la connessione IPsec, che cancella anche le associazioni di protezione correlate alla fase 2.

```
ASA-NY-HQ# clear crypto ipsec sa
```

Cancella le associazioni di protezione relative alla fase 1 come indicato di seguito

```
ASA-NY-HQ# clear crypto isakmp sa
```

2. Rimuovere l'ACL del traffico interessante per il tunnel IPsec.

```
ASA-NY-HQ(config)# no access-list outside_20_cryptomap extended permit ip 172.16.40.0
255.255.255.0 10.10.10.0 255.255.255.0
```

3. Rimuovere l'ACL (inside_nat0_outbound), in quanto il traffico viene escluso dal nat.

```
ASA-NY-HQ(config)# no access-list inside_nat0_outbound extended permit ip 172.16.40.0
255.255.255.0 10.10.10.0 255.255.255.0
```

4. Cancellate la traslazione NAT come mostrato

```
ASA-NY-HQ# clear xlate
```

5. Ogni volta che si modifica la configurazione del tunnel, rimuovere e applicare nuovamente i comandi crypto per usare la configurazione più recente nell'interfaccia esterna

```
ASA-NY-HQ(config)# crypto map outside_map interface outside
ASA-NY-HQ(config)# crypto isakmp enable outside
```

6. Salvare la configurazione attiva sulla memoria flash "**write memory**".
7. Seguire la stessa procedura per l'altra appliance di sicurezza end-TN per rimuovere le configurazioni.
8. Avviare il tunnel IPsec e verificare la connessione.

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**.

- ping all'interno della versione
172.16.40.20

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 172.16.40.20, timeout is 2 seconds:  
?!!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

- show crypto isakmp
sa

```
Active SA: 1  
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)  
Total IKE SA: 1  
  
1 IKE Peer: 192.168.10.10  
Type   : L2L           Role   : initiator  
Rekey : no           State  : MM_ACTIVE
```

- show crypto ipsec
sa

```

Interface: outside
Crypto map tag: outside_map, seq num: 20, local addr: 192.168.11.1

access-list outside_20_cryptomap permit ip 172.16.1.0 255.255.255.0 172.16.40.0 255.255.255.0
Local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.16.40.0/255.255.255.0/0/0)
current_peer: 192.168.10.10

#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: 4, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUS sent: 0, #PMTUS rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.11.2, remote crypto endpt.: 192.168.10.10

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: 4C0547DE

Inbound esp sas:
spi: 0x0EB40138 (246677816)
transform: esp-3des esp-sha-hmac none
in use settings = {L2L, Tunnel, }
slot: 0, conn_id: 2, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4274999/28476)
IV size: 8 bytes
replay detection support: Y
outbound esp sas:
spi: 0x4C0547DE (1275414494)
transform: esp-3des esp-sha-hmac none
in use settings = {L2L, Tunnel, }
slot: 0, conn_id: 2, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4274999/28476)
IV size: 8 bytes
replay detection support: Y

Crypto map tag: outside_map, seq num: 20, local addr: 192.168.11.1

access-list outside_20_cryptomap permit ip 172.16.1.0 255.255.255.0 10.10.10.0 255.255.255.0
Local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
current_peer: 192.168.10.10

#pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 14, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUS sent: 0, #PMTUS rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.11.2, remote crypto endpt.: 192.168.10.10

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: 5CC4DE89

Inbound esp sas:
spi: 0xF48286AD (4102194861)
transform: esp-3des esp-sha-hmac none
in use settings = {L2L, Tunnel, }
slot: 0, conn_id: 2, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4274999/28271)
IV size: 8 bytes
replay detection support: Y
outbound esp sas:
spi: 0x5CC4DE89 (1556405897)
transform: esp-3des esp-sha-hmac none
in use settings = {L2L, Tunnel, }
slot: 0, conn_id: 2, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4274998/28271)
IV size: 8 bytes
replay detection support: Y

```

[Risoluzione dei problemi](#)

Per ulteriori informazioni sulla risoluzione dei problemi, consultare i seguenti documenti:

- [Soluzioni di risoluzione dei problemi VPN IPsec](#)
- [descrizione e uso dei comandi di debug](#)
- [Risoluzione dei problemi di connessione tramite PIX e ASA](#)

[Informazioni correlate](#)

- [Introduzione alla crittografia di protezione IP \(IPsec\)](#)
- [Negoziazione IPsec/pagina di supporto del protocollo IKE](#)
- [Guida di riferimento ai comandi di Security Appliance](#)
- [Configurazione degli elenchi di accesso IP](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)