

# PIX/ASA 7.x: Een netwerk toevoegen of verwijderen op een bestaand L2L VPN-tunnelconfiguratievoorbeld

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Verwante producten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Netwerk toevoegen aan de IPSec-tunnelbouw](#)

[Netwerk uit IPSec-tunnels verwijderen](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

## [Inleiding](#)

Dit document biedt een voorbeeldconfiguratie voor het toevoegen van een nieuw netwerk aan een bestaande VPN-tunnel.

## [Voorwaarden](#)

### [Vereisten](#)

Zorg ervoor dat u een PIX/ASA security applicatie hebt die 7.x code draait voordat u deze configuratie probeert.

### [Gebruikte componenten](#)

De informatie in dit document is gebaseerd op twee Cisco 5500 security applicatieapparaten.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## [Verwante producten](#)

Deze configuratie kan ook worden gebruikt bij de PIX 500 security applicatie.

## [Conventies](#)

Raadpleeg de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

## [Achtergrondinformatie](#)

Er is momenteel een LAN-to-LAN (L2L) VPN-tunnel die tussen het NY- en het TN-kantoor ligt. Het NY-kantoor heeft zojuist een nieuw netwerk toegevoegd dat door de CSI-ontwikkelingsgroep kan worden gebruikt. Deze groep vereist toegang tot middelen die in het TN kantoor wonen. De taak is om het nieuwe netwerk aan de reeds bestaande VPN-tunnel toe te voegen.

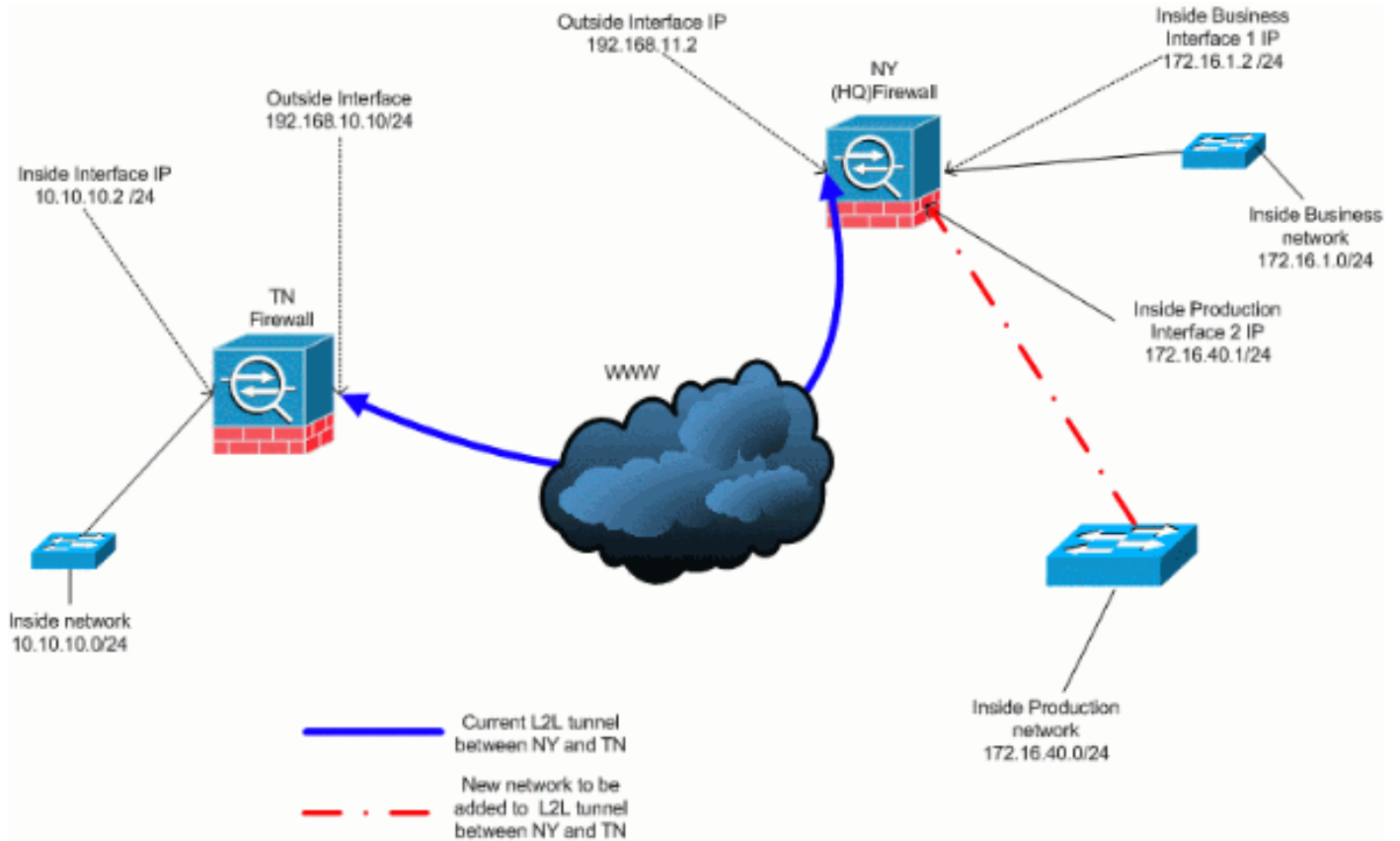
## [Configureren](#)

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

**Opmerking:** Gebruik het [Opname Gereedschap](#) ([alleen geregistreerde](#) klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

## [Netwerkdigram](#)

Het netwerk in dit document is als volgt opgebouwd:



## Netwerk toevoegen aan de IPSec-tunnelbouw

Dit document gebruikt deze configuratie:

### NY-firewallconfiguratie (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#
```

## Netwerk uit IPSec-tunnels verwijderen

Gebruik deze stappen om het netwerk te verwijderen van de configuratie van de IPSec Tunnel. Stel hier in dat het netwerk 172.16.40.0/24 is verwijderd van de configuratie van de NY (HQ) security applicatie.

1. Scheur voordat u het netwerk uit de tunnel verwijdert, de IPSec-verbinding af, die ook de veiligheidsverenigingen in verband met fase 2 goedkeurt.

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

hecht zijn goedkeuring aan de veiligheidsverenigingen in verband met fase 1, en wel als volgt

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

2. Verwijder het interessante verkeer ACL voor de IPSec-tunnel.

```
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. Verwijder ACL (interne\_nat0\_outbound), aangezien het verkeer van de ingang wordt uitgesloten.

```
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. Verwijder de NAT-vertaling zoals aangegeven op de afbeelding.

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

5. Wanneer u ooit de tunnelconfiguratie aanpast, verwijder en pas deze crypto opdrachten opnieuw toe om de nieuwste configuratie in de externe interface te nemen

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

6. Sla de actieve configuratie op in het "schrijfgeheugen" van de flitser.
7. Volg dezelfde procedure voor het andere end-to-security apparaat om de configuraties te verwijderen.
8. Start de IPSec-tunnel en controleer de aansluiting.

## Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het [Uitvoer Tolk](#) ([uitsluitend geregistreeerde](#) klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- ingewanden op  
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
```

- toon 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

```

## [Problemen oplossen](#)

Raadpleeg deze documenten voor meer informatie over probleemoplossing:

- [IPsec VPN-probleemoplossing](#)
- [Opdrachten begrijpen en gebruiken](#)
- [Aansluitingen voor probleemoplossing via PIX en ASA](#)

## [Gerelateerde informatie](#)

- [Inleiding over IP Security \(IPsec\) encryptie](#)
- [Ondersteuning van IPsec-onderhandeling/IKE-protocol](#)
- [Opdracht voor security applicatie](#)
- [IP-toeganglijsten configureren](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)