

PIX/ASA 7.x: Hinzufügen/Entfernen eines Netzwerks auf einem vorhandenen L2L-VPN-Tunnel - Konfigurationsbeispiel

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Zugehörige Produkte](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Hinzufügen des Netzwerks zum IPSec-Tunnel](#)

[Entfernen des Netzwerks aus dem IPSec-Tunnel](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

[Einführung](#)

Dieses Dokument enthält eine Beispielkonfiguration zum Hinzufügen eines neuen Netzwerks zu einem vorhandenen VPN-Tunnel.

[Voraussetzungen](#)

[Anforderungen](#)

Stellen Sie sicher, dass Sie eine PIX/ASA Security Appliance haben, die 7.x-Code ausführt, bevor Sie diese Konfiguration versuchen.

[Verwendete Komponenten](#)

Die Informationen in diesem Dokument basieren auf zwei Cisco 5500 Security Appliance-Geräten.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

[Zugehörige Produkte](#)

Diese Konfiguration kann auch mit der PIX 500 Security Appliance verwendet werden.

[Konventionen](#)

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

[Hintergrundinformationen](#)

Es gibt derzeit einen LAN-to-LAN (L2L)-VPN-Tunnel, der sich zwischen dem NY und dem TN-Büro befindet. Die NY-Niederlassung hat soeben ein neues Netzwerk für die CSI-Entwicklungsgruppe hinzugefügt. Diese Gruppe benötigt Zugriff auf Ressourcen, die sich im TN-Büro befinden. Es geht darum, das neue Netzwerk dem bereits bestehenden VPN-Tunnel hinzuzufügen.

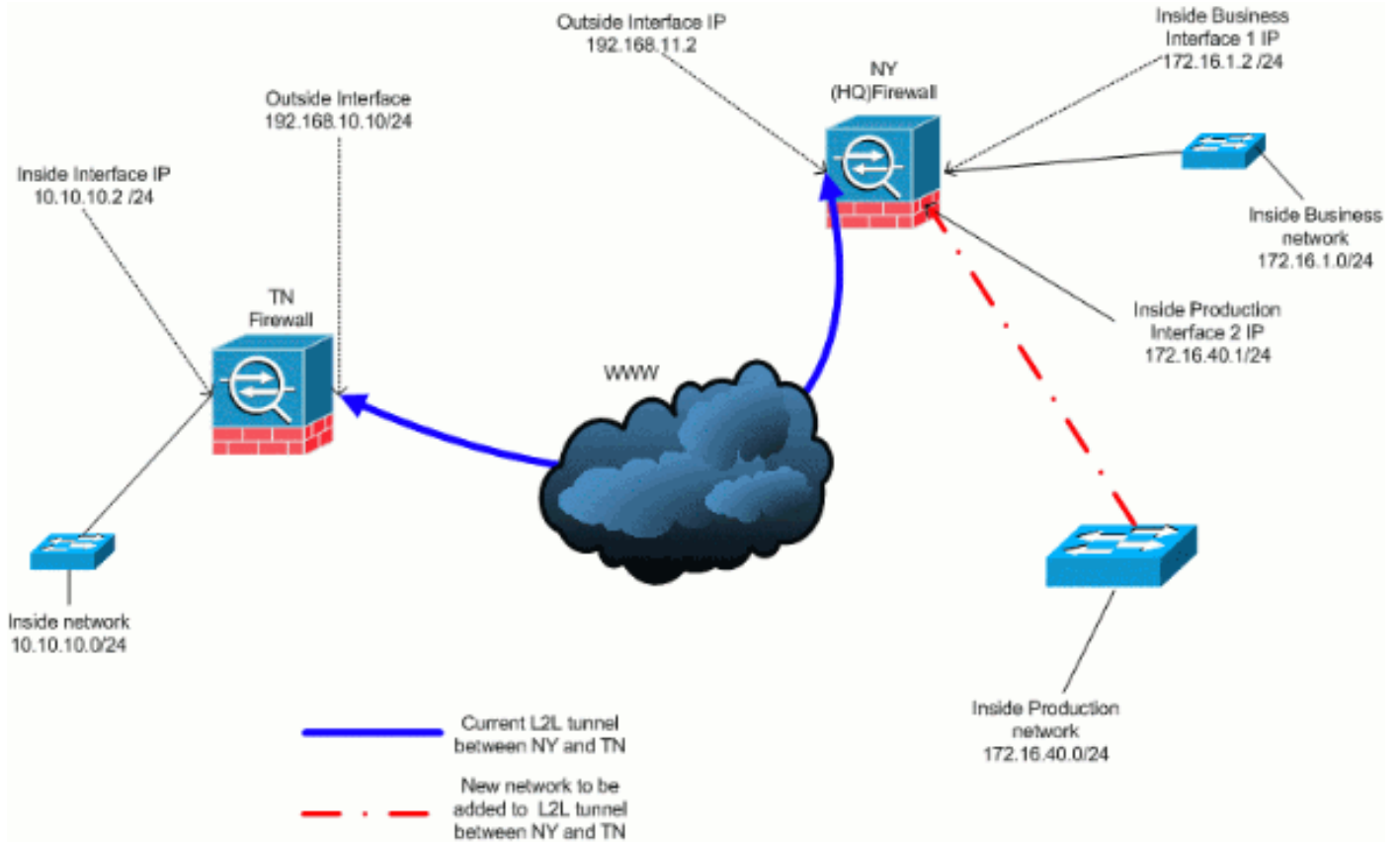
[Konfigurieren](#)

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

[Netzwerkdiagramm](#)

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Hinzufügen des Netzwerks zum IPsec-Tunnel

In diesem Dokument wird diese Konfiguration verwendet:

NY (Hauptsitz) Firewall-Konfiguration

```

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#
```

Entfernen des Netzwerks aus dem IPSec-Tunnel

Führen Sie diese Schritte aus, um das Netzwerk aus der IPSec-Tunnelkonfiguration zu entfernen. Beachten Sie hier, dass das Netzwerk 172.16.40.0/24 aus der Konfiguration der NY (HQ) Security Appliance entfernt wurde.

1. Bevor Sie das Netzwerk aus dem Tunnel entfernen, entfernen Sie die IPSec-Verbindung, die auch die Sicherheitszuordnungen für Phase 2 löscht.

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

Löscht die Sicherheitszuordnungen für Phase 1 wie folgt

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

2. Entfernen Sie die interessante Datenverkehrs-ACL für den 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. Entfernen Sie die ACL (inside_nat0_outbound), da der Datenverkehr vom NAT ausgeschlossen wird.

```
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. Löschen Sie die NAT-Übersetzung wie gezeigt.

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

5. Wenn Sie die Tunnelkonfiguration ändern, entfernen Sie diese Krypto-Befehle, und wenden Sie sie erneut an, um die neueste Konfiguration in der externen Schnittstelle durchzuführen.

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

6. Speichern Sie die aktive Konfiguration im Flash-"Schreibspeicher".
7. Befolgen Sie zum Entfernen der Konfigurationen das gleiche Verfahren für die TN Security Appliance.
8. Initiieren Sie den IPSec-Tunnel, und überprüfen Sie die Verbindung.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des Befehls show anzuzeigen**.

- Ping innerhalb von 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

```

[Fehlerbehebung](#)

Weitere Informationen zur Fehlerbehebung finden Sie in diesen Dokumenten:

- [IPsec VPN-Fehlerbehebungslösungen](#)
- [Verwenden von Debugbefehlen](#)
- [Fehlerbehebung bei Verbindungen über PIX und ASA](#)

[Zugehörige Informationen](#)

- [Einführung in die IP-Sicherheit \(IPsec\)-Verschlüsselung](#)
- [Support-Seite für IPsec-Aushandlung/IKE-Protokoll](#)
- [Befehlsreferenz zur Security Appliance](#)
- [Konfigurieren von IP-Zugriffslisten](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)