

PIX/ASA 7.x : Exemple de configuration de l'ajout ou de la suppression d'un réseau sur un tunnel VPN LAN à LAN existant

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Produits connexes](#)

[Conventions](#)

[Informations générales](#)

[Configurez](#)

[Diagramme du réseau](#)

[Ajouter le réseau au tunnel d'IPSec](#)

[Retirer le réseau du tunnel d'IPSec](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

[Introduction](#)

Ce document fournit une configuration d'échantillon pour que la façon ajoute un nouveau réseau à un tunnel VPN existant.

[Conditions préalables](#)

[Conditions requises](#)

Assurez-vous que vous avez des dispositifs de sécurité PIX/ASA qui exécutent le code 7.x avant que vous tentiez cette configuration.

[Composants utilisés](#)

Les informations dans ce document sont basées sur deux Cisco 5500 périphériques de dispositifs de sécurité.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-

vous que vous comprenez l'effet potentiel de toute commande.

[Produits connexes](#)

Cette configuration peut également être utilisée avec les dispositifs de sécurité PIX 500.

[Conventions](#)

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

[Informations générales](#)

Il y a actuellement un tunnel VPN de l'entre réseaux locaux (L2L) qui est entre le bureau NY et TN. Le bureau NY a juste ajouté un nouveau réseau à utiliser par le groupe de développement de CSI. Ce groupe a besoin de l'accès aux ressources qui résident dans le bureau TN. La tâche actuelle est d'ajouter le nouveau réseau au tunnel VPN déjà existant.

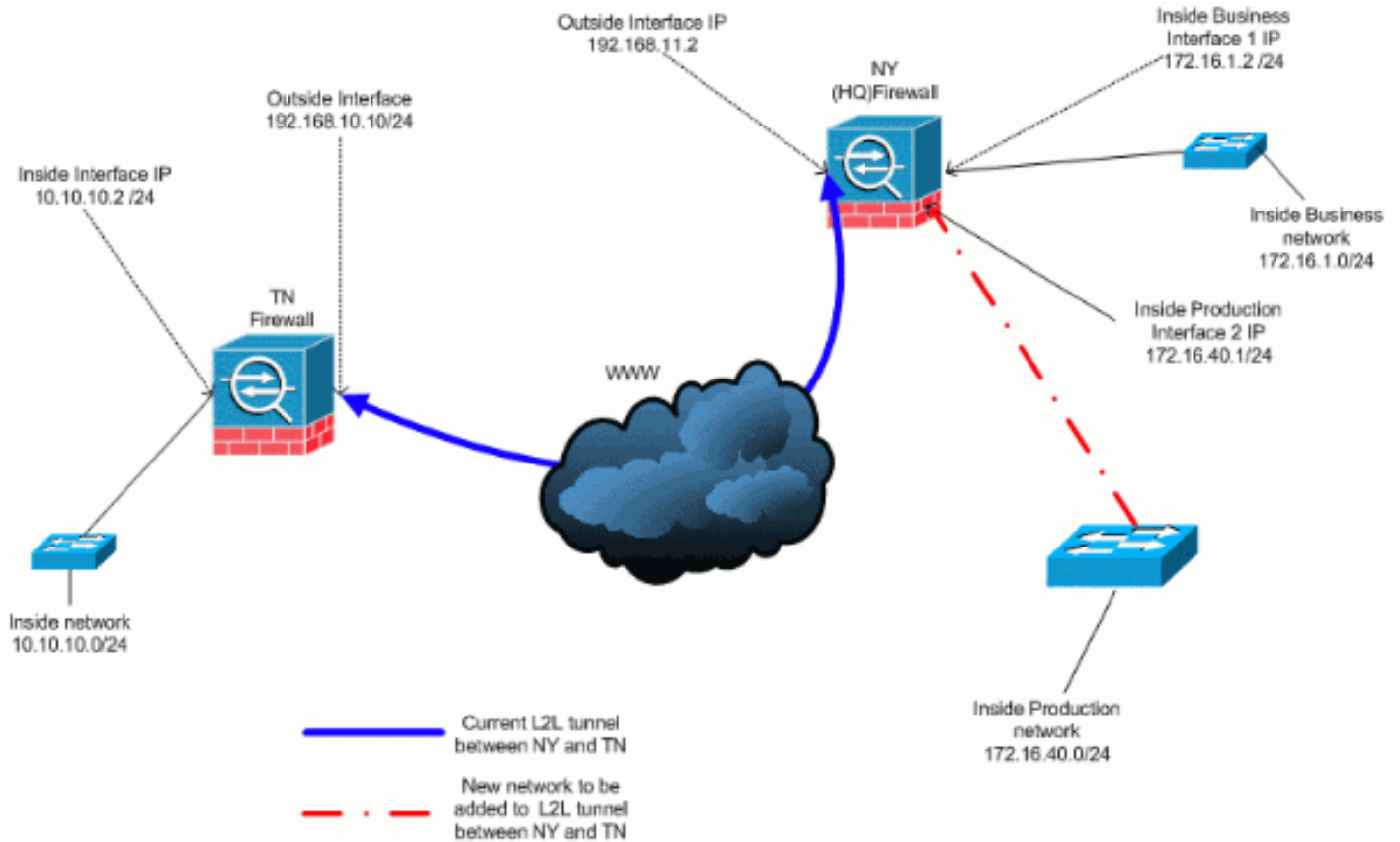
[Configurez](#)

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil [Command Lookup Tool](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

[Diagramme du réseau](#)

Ce document utilise la configuration réseau suivante :



[Ajouter le réseau au tunnel d'IPSec](#)

Ce document utilise la configuration suivante :

Config de Pare-feu NY (QG)

```

ASA-NY-HQ#show running-config : Saved : ASA Version
7.2(2) ! hostname ASA-NY-HQ domain-name corp2.com enable
password WwXYvtKrnjXqGbul 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#

```

Retirer le réseau du tunnel d'IPSec

Utilisez ceci fait un pas pour retirer le réseau de la configuration de tunnel d'IPSec. Ici, considérez que le réseau 172.16.40.0/24 a été retiré de la configuration d'appareils NY (QG) Security.

1. Avant retirez le réseau du tunnel, démolissent la connexion d'IPSec, qui autorise également les associations de sécurité liées à la phase 2.

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

Autorise les associations de sécurité liées à la phase 1 comme suit

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

2. Retirez l'ACL du trafic intéressant pour le tunnel d'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. Retirez l'ACL (inside_nat0_outbound), puisque le trafic est exclu du 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. Effacez la traduction NAT comme affichée

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

5. Quand jamais vous modifiez la configuration de tunnel, retirez et réappliquez ce les cryptos commandes de prendre la configuration la plus récente dans l'interface extérieure

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

6. Sauvegardez la configuration active à la « **write memory** » instantanée.

7. Suivez la même procédure pour l'autre extrémité - des dispositifs de sécurité TN pour retirer les configurations.

8. Initiez le tunnel d'IPSec et vérifiez la connexion.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'[Outil Interpréteur de sortie](#) (clients [enregistrés](#) uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

- **ping 172.16.40.20**
intérieur

```
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

```

Dépannez

Référez-vous à ces documents pour plus d'information de dépannage :

- [Solutions de dépannage VPN d'IPsec](#)
- [Présentation et utilisation des commandes de débogage](#)
- Dépannage des connexions via [PIX et ASA](#)

Informations connexes

- [Présentation du chiffrement IPSec \(IP Security\)](#)
- [Page de support pour Protocole IKE/Négociation IPsec](#)
- [Référence de commandes de dispositifs de sécurité](#)
- [Configuration des listes d'accès IP](#)
- [Support et documentation techniques - Cisco Systems](#)