

PIX/ASA 7.X : Ajouter un nouveau tunnel ou un accès à distance à un VPN LAN à LAN existant

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Diagramme du réseau](#)

[Informations générales](#)

[Ajouter un tunnel L2L supplémentaire à la configuration](#)

[Step-by-Step Instructions](#)

[Exemple de configuration](#)

[Ajouter un VPN d'accès à distance à la configuration](#)

[Step-by-Step Instructions](#)

[Exemple de configuration](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

[Introduction](#)

Ce document présente les étapes nécessaires pour ajouter un nouveau tunnel VPN ou un VPN d'accès à distance à une configuration site à site (L2L) qui existe déjà dans le VPN. Référez-vous aux dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500 - Exemples de configuration et TechNotes pour plus d'informations sur la façon de créer les tunnels VPN IPsec initiaux et pour d'autres exemples de configuration.

[Conditions préalables](#)

[Conditions requises](#)

Assurez-vous de configurer correctement le tunnel VPN L2L IPSEC qui est actuellement opérationnel avant de tenter cette configuration.

[Components Used](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Deux appliances de sécurité ASA exécutant le code 7.x
- Un dispositif de sécurité PIX qui exécute le code 7.x

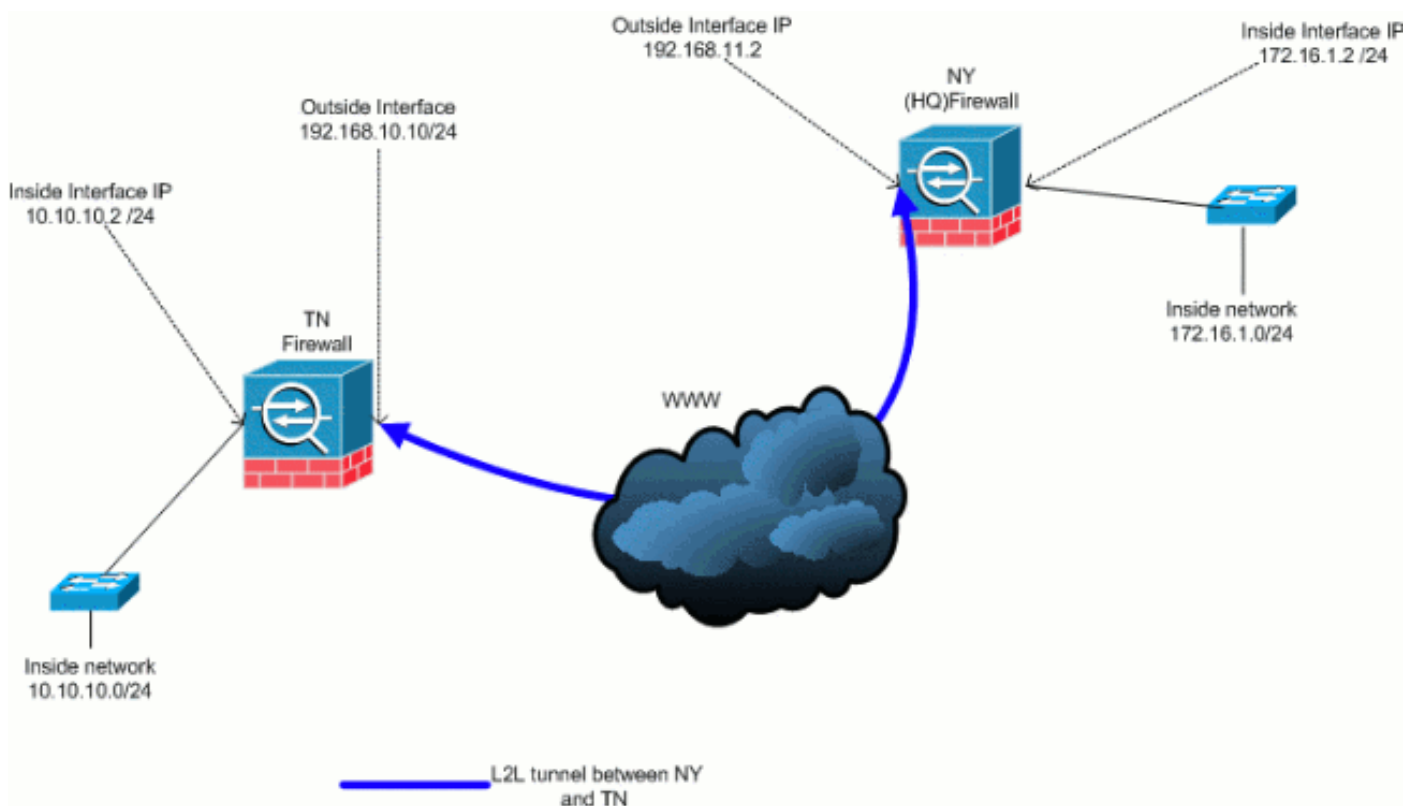
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Cette sortie correspond à la configuration en cours de l'appliance de sécurité NY (HUB). Dans cette configuration, un tunnel L2L IPsec est configuré entre NY(HQ) et TN.

Configuration actuelle du pare-feu 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  
  shutdown  
  no nameif  
  no security-level  
  no ip address  
!  
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  
access-list outside_20_cryptomap extended permit ip  
172.16.1.0 255.255.255.0  
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 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 * telnet timeout 1440 ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map type inspect
dns preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global prompt hostname context
Cryptochecksum:a3aa2afb37dcad447031b7b0c8ea65d3 : end
ASA-NY-HQ#
```

Informations générales

Il existe actuellement un tunnel L2L entre le bureau de NY(HQ) et le bureau de TN. Votre entreprise vient d'ouvrir un nouveau bureau situé à TX. Ce nouveau bureau nécessite une connectivité aux ressources locales situées dans les bureaux de New York et de TN. En outre, il est nécessaire de permettre aux employés de travailler à domicile et d'accéder en toute sécurité aux ressources situées sur le réseau interne à distance. Dans cet exemple, un nouveau tunnel VPN est configuré ainsi qu'un serveur VPN d'accès à distance situé dans le bureau de NY.

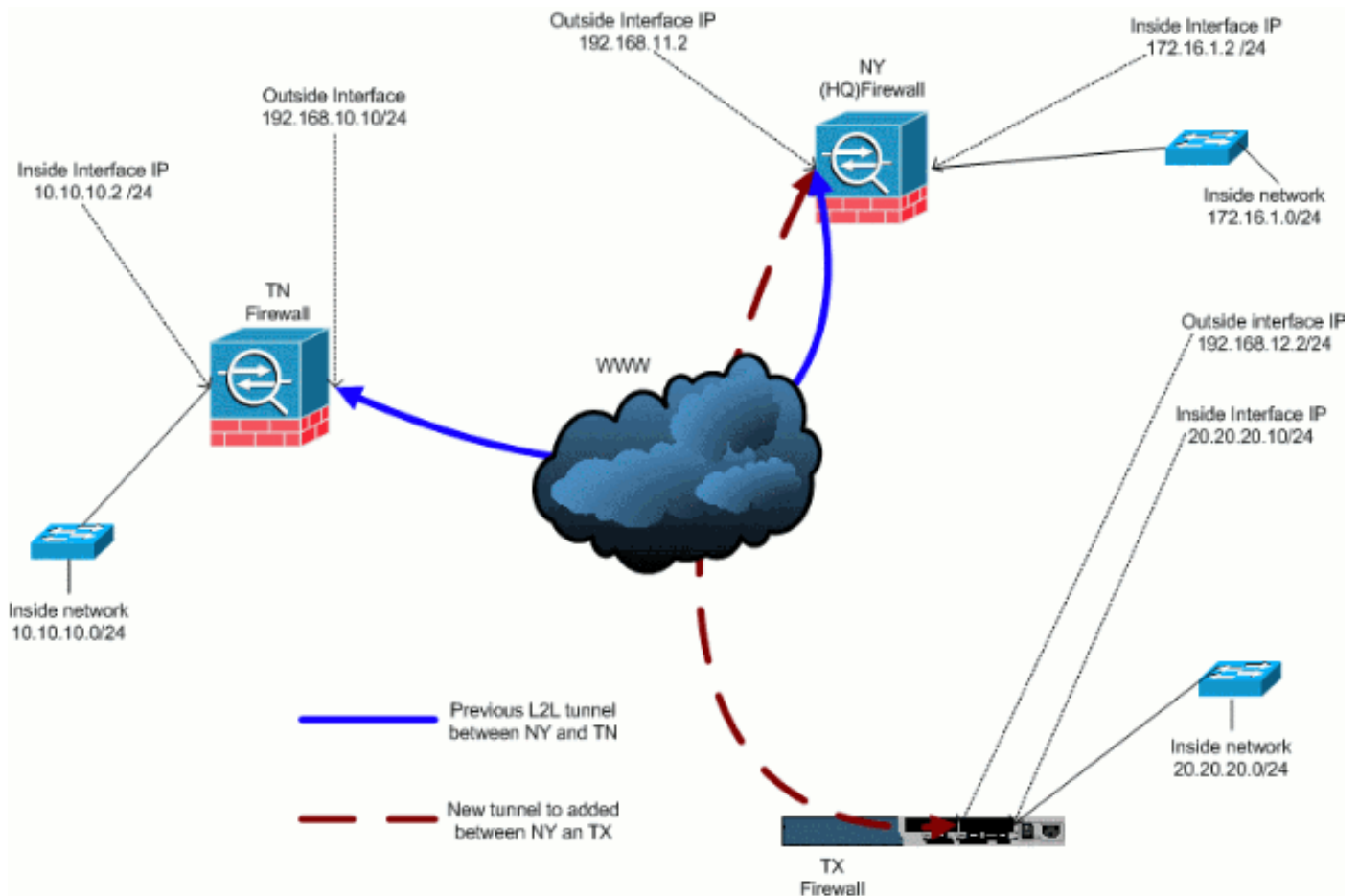
Dans cet exemple, deux commandes sont utilisées afin de permettre la communication entre les réseaux VPN et identifier le trafic qui doit être tunnelisé ou chiffré. Cela vous permet d'accéder à Internet sans avoir à envoyer ce trafic via le tunnel VPN. Afin de configurer ces deux options, émettez les commandes **split-tunnel** et **same-security-traffic**.

La transmission tunnel partagée permet à un client IPSec à accès distant de diriger conditionnellement des paquets via un tunnel IPSec sous forme cryptée, ou vers une interface réseau sous forme de texte clair. Avec la transmission tunnel partagée activée, les paquets non liés aux destinations de l'autre côté du tunnel IPSec n'ont pas besoin d'être chiffrés, envoyés à travers le tunnel, décryptés, puis routés vers une destination finale. Cette commande applique cette stratégie de fractionnement en canaux à un réseau spécifié. La valeur par défaut est de tunnel tout le trafic. Afin de définir une stratégie de fractionnement en canaux, émettez la commande **split-tunnel-policy** en mode de configuration group-policy. Afin de supprimer la stratégie de fractionnement en canaux de la configuration, émettez la forme **no** de cette commande.

L'apppliance de sécurité inclut une fonctionnalité qui permet à un client VPN d'envoyer du trafic protégé par IPSec à d'autres utilisateurs VPN en autorisant ce trafic à entrer et à sortir de la même interface. Également appelée reconnexion, cette fonctionnalité peut être considérée comme des rayons VPN (clients) qui se connectent via un concentrateur VPN (dispositif de sécurité). Dans une autre application, cette fonctionnalité peut rediriger le trafic VPN entrant vers la même interface que le trafic non chiffré. Ceci est utile, par exemple, pour un client VPN qui ne dispose pas de transmission tunnel partagée mais qui doit à la fois accéder à un VPN et naviguer sur le Web. Afin de configurer cette fonctionnalité, émettez la commande **same-security-traffic intra-interface en mode de configuration globale**.

Ajouter un tunnel L2L supplémentaire à la configuration

Voici le schéma de réseau pour cette configuration :



Step-by-Step Instructions

Cette section fournit les procédures requises qui doivent être exécutées sur l'appliance de sécurité HUB (NY Firewall). Référez-vous à [PIX/ASA 7.x : Exemple de configuration de tunnel VPN PIX-to-PIX simple](#) pour plus d'informations sur la configuration du client en étoile (Pare-feu TX).

Procédez comme suit :

1. Créez ces deux nouvelles listes d'accès à utiliser par la carte de chiffrement afin de définir le trafic intéressant :

```
ASA-NY-HQ(config)#access-list outside_30_cryptomap
  extended permit ip 172.16.1.0 255.255.255.0
    20.20.20.0 255.255.255.0
```

```
ASA-NY-HQ(config)#access-list outside_30_cryptomap
  extended permit ip 10.10.10.0 255.255.255.0
    20.20.20.0 255.255.255.0
```

Avertissement : Pour que la communication ait lieu, l'autre côté du tunnel doit avoir l'entrée opposée à cette liste de contrôle d'accès (ACL) pour ce réseau particulier.

2. Ajoutez ces entrées à l'instruction no nat afin d'exempter la liaison entre ces réseaux :

```
ASA-NY-HQ(config)#access-list inside_nat0_outbound
  extended permit ip 172.16.1.0 255.255.255.0
    20.20.20.0 255.255.255.0
```

```
ASA-NY-HQ(config)#access-list inside_nat0_outbound
  extended permit ip 10.10.10.0 255.255.255.0
    20.20.20.0 255.255.255.0
```

```
ASA-NY-HQ(config)#access-list inside_nat0_outbound
  extended permit ip 20.20.20.0 255.255.255.0
    10.10.10.0 255.255.255.0
```

Avertissement : pour que la communication ait lieu, l'autre côté du tunnel doit avoir l'inverse de cette entrée de liste de contrôle d'accès pour ce réseau particulier.

3. Émettez cette commande afin de permettre à un hôte sur le réseau VPN TX d'avoir accès au tunnel VPN TN :

```
ASA-NY-HQ(config)#same-security-traffic permit
  intra-interface
```

Cela permet aux homologues VPN de communiquer entre eux.

4. Créez la configuration de la carte de chiffrement pour le nouveau tunnel VPN. Utilisez le même jeu de transformation qui a été utilisé dans la première configuration VPN, car tous les paramètres de la phase 2 sont identiques.

```
ASA-NY-HQ(config)#crypto map outside_map 30 match
  address outside_30_cryptomap
```

```
ASA-NY-HQ(config)#crypto map outside_map 30 set
  peer 192.168.12.2
```

```
ASA-NY-HQ(config)#crypto map outside_map 30 set
  transform-set
  ESP-3DES-SHA
```

5. Créez le groupe de tunnels spécifié pour ce tunnel avec les attributs nécessaires à la connexion à l'hôte distant.

```
ASA-NY-HQ(config)#tunnel-group 192.168.12.2 type
  ipsec-l2l
```

```
ASA-NY-HQ(config)#tunnel-group 192.168.12.2
  ipsec-attributes
```

```
ASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key
  cisco123
```

Remarque : La clé pré-partagée doit correspondre exactement des deux côtés du tunnel.

6. Maintenant que vous avez configuré le nouveau tunnel, vous devez envoyer un trafic intéressant à travers le tunnel pour le faire démarrer. Pour ce faire, exécutez la commande **source ping** pour envoyer une requête ping à un hôte sur le réseau interne du tunnel distant. Dans cet exemple, une station de travail de l'autre côté du tunnel avec l'adresse 20.20.20.16 est envoyée par ping. Ceci amène le tunnel entre NY et TX. Maintenant, il y a deux tunnels connectés au bureau du siège social. Si vous n'avez pas accès à un système derrière le tunnel, référez-vous à [Solutions de dépannage VPN IPSec les plus courantes](#) pour trouver une autre solution en ce qui concerne l'utilisation de `management-access`.

Exemple de configuration

Exemple de configuration 1

```
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 192.168.11.1 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
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
same-security-traffic permit intra-interface
access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip
10.10.10.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip
20.20.20.0 255.255.255.0 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
access-list outside_20_cryptomap extended permit ip
20.20.20.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list outside_30_cryptomap extended permit ip
172.16.1.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list outside_30_cryptomap extended permit ip
10.10.10.0 255.255.255.0 20.20.20.0
255.255.255.0
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
```

```
mtu man 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
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
route outside 0.0.0.0 0.0.0.0 192.168.11.1 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
username sidney password 3xsopMX9gN5Wnf1W encrypted
privilege 15
aaa authentication telnet console LOCAL
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 30 match address
outside_30_cryptomap
crypto map outside_map 30 set peer 192.168.12.2
crypto map outside_map 30 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 *
tunnel-group 192.168.12.2 type ipsec-l2l
tunnel-group 192.168.12.2 ipsec-attributes
  pre-shared-key *
telnet timeout 1440
ssh timeout 5
console timeout 0
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
```



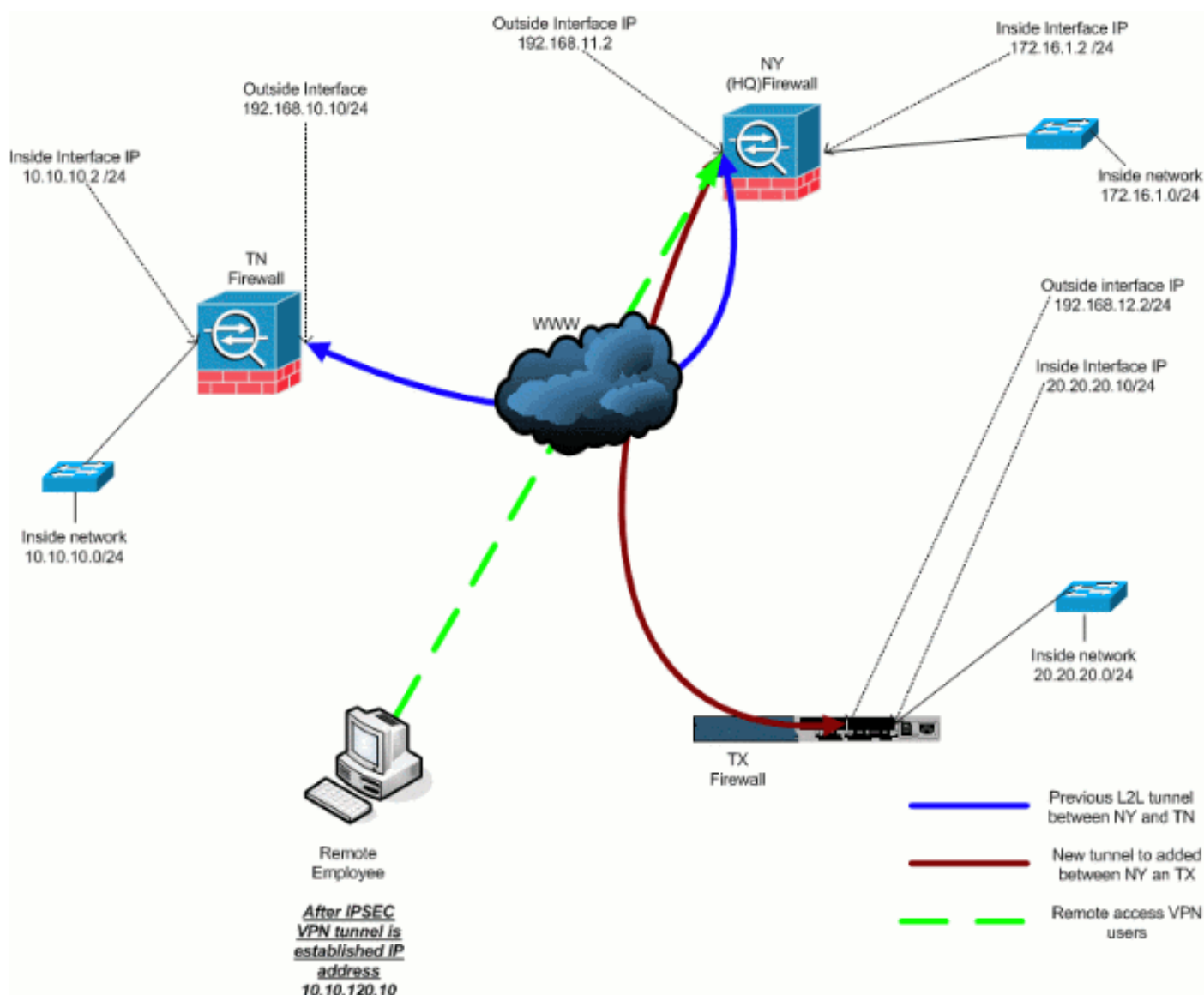
```

inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:5a184c8e5e6aa30d4108a55ac0ead3ae
: end
ASA-NY-HQ#

```

Ajouter un VPN d'accès à distance à la configuration

Voici le schéma de réseau pour cette configuration :



Step-by-Step Instructions

Cette section décrit les procédures requises pour ajouter une fonctionnalité d'accès à distance et permettre aux utilisateurs distants d'accéder à tous les sites. Reportez-vous à [PIX/ASA 7.x ASDM : Restreindre l'accès réseau des utilisateurs VPN d'accès à distance](#) pour plus d'informations sur la façon de configurer le serveur d'accès à distance et de restreindre l'accès.

Procédez comme suit :

1. Créez un pool d'adresses IP à utiliser pour les clients qui se connectent via le tunnel VPN. Créez également un utilisateur de base afin d'accéder au VPN une fois la configuration terminée.

```
ASA-NY-HQ(config)#ip local pool Hill-V-IP
10.10.120.10-10.10.120.100 mask 255.255.255.0
```

```
ASA-NY-HQ(config)#username cisco password
cisco111
```

2. Exempter le trafic spécifique d'être lié.

```
ASA-NY-HQ(config)#access-list
inside_nat0_outbound extended permit ip 172.16.1.0
255.255.255.0 10.10.120.0 255.255.255.0
```

```
ASA-NY-HQ(config)#access-list
inside_nat0_outbound extended permit ip 10.10.120.0
255.255.255.0 10.10.10.0 255.255.255.0
```

```
ASA-NY-HQ(config)#access-list
inside_nat0_outbound extended permit ip 10.10.120.0
255.255.255.0 20.20.20.0 255.255.255.0
```

Notez que la communication nat entre tunnels VPN est exemptée dans cet exemple.

3. Autoriser la communication entre les tunnels L2L déjà créés.

```
ASA-NY-HQ(config)#access-list
outside_20_cryptomap extended permit ip 10.10.120.0
255.255.255.0 10.10.10.0 255.255.255.0
```

```
ASA-NY-HQ(config)#access-list
outside_30_cryptomap extended permit ip 10.10.120.0
255.255.255.0 20.20.20.0 255.255.255.0
```

Cela permet aux utilisateurs d'accès distant de communiquer avec les réseaux situés derrière les tunnels spécifiés. **Avertissement** : pour que la communication ait lieu, l'autre côté du tunnel doit avoir l'inverse de cette entrée de liste de contrôle d'accès pour ce réseau particulier.

4. Configurez le trafic qui sera chiffré et envoyé via le tunnel VPN.

```
ASA-NY-HQ(config)#access-list
Hillvalley_splitunnel standard permit 172.16.1.0
255.255.255.0
```

```
ASA-NY-HQ(config)#access-list
Hillvalley_splitunnel standard permit 10.10.10.0
255.255.255.0
```

```
ASA-NY-HQ(config)#access-list
Hillvalley_splitunnel standard permit 20.20.20.0
255.255.255.0
```

5. Configurez l'authentification locale et les informations de stratégie, telles que les protocoles

wins, dns et IPSec, pour les clients VPN.

```
ASA-NY-HQ(config)#group-policy Hillvalley
  internal
```

```
ASA-NY-HQ(config)#group-policy Hillvalley
  attributes
```

```
ASA-NY-HQ(config-group-policy)#wins-server
value 10.10.10.20
```

```
ASA-NY-HQ(config-group-policy)#dns-server value
10.10.10.20
```

```
ASA-NY-HQ(config-group-policy)#vpn-tunnel-protocol
IPSec
```

6. Définissez les attributs IPSec et généraux, tels que les clés pré-partagées et les pools d'adresses IP, qui seront utilisés par le tunnel VPN Hillvalley.

```
ASA-NY-HQ(config)#tunnel-group Hillvalley
  ipsec-attributes
```

```
ASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key
cisco1234
```

```
ASA-NY-HQ(config)#tunnel-group Hillvalley
  general-attributes
```

```
ASA-NY-HQ(config-tunnel-general)#address-pool
Hill-V-IP
```

```
ASA-NY-HQ(config-tunnel-general)#default-group-policy
Hillvalley
```

7. Créez la stratégie de tunnel partagé qui utilisera la liste de contrôle d'accès créée à l'étape 4 afin de spécifier le trafic qui sera chiffré et transmis via le tunnel.

```
ASA-NY-HQ(config)#split-tunnel-policy
tunnelspecified
```

```
ASA-NY-HQ(config)#split-tunnel-network-list value
Hillvalley_splittunnel
```

8. Configurez les informations de cryptage requises pour la création du tunnel VPN.

```
ASA-NY-HQ(config)#crypto ipsec transform-set
Hill-trans esp-3des esp-sha-hmac
```

```
ASA-NY-HQ(config)#crypto dynamic-map
  outside_dyn_map 20 set transform-set
Hill-trans
```

```
ASA-NY-HQ(config)#crypto dynamic-map dyn_map 20
  set reverse-route
```

```
ASA-NY-HQ(config)#crypto map outside_map 65535
  ipsec-isakmp dynamic
  outside_dyn_map
```

[Exemple de configuration](#)

Exemple de configuration 2

```
ASA-NY-HQ#show running-config
```

```
: Saved
```

```
hostname ASA-NY-HQ
```

```
ASA Version 7.2(2)
```

```
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
```

```
 shutdown
```

```
 no nameif
```

```
 no security-level
```

```
 no ip address
```

```
!
```

```
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
```

```
same-security-traffic permit intra-interface
```

```
!--- This is required for communication between VPN peers. access-list inside_nat0_outbound extended permit
```

```
ip 172.16.1.0 255.255.255.0 10.10.10.0 255.255.255.0
```

```
access-list inside_nat0_outbound extended permit ip
```

```
172.16.1.0 255.255.255.0 20.20.20.0 255.255.255.0
```

```
access-list inside_nat0_outbound extended permit ip
```

```
10.10.10.0 255.255.255.0 20.20.20.0 255.255.255.0
```

```
access-list inside_nat0_outbound extended permit ip
```

```
20.20.20.0 255.255.255.0 10.10.10.0 255.255.255.0
```

```
access-list inside_nat0_outbound extended permit ip
```

```
10.10.120.0 255.255.255.0 20.20.20.0
```

```
255.255.255.0
```

```
access-list inside_nat0_outbound extended permit ip
```

```
172.16.1.0 255.255.255.0 10.10.120.0
```

```
255.255.255.0
```

```
access-list inside_nat0_outbound extended permit ip
```

```
10.10.120.0 255.255.255.0 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
access-list outside_20_cryptomap extended permit ip
20.20.20.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list outside_20_cryptomap extended permit ip
10.10.120.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list Hillvalley_splitunnel standard permit
172.16.1.0 255.255.255.0
access-list Hillvalley_splitunnel standard permit
10.10.10.0 255.255.255.0
access-list Hillvalley_splitunnel standard permit
20.20.20.0 255.255.255.0
access-list outside_30_cryptomap extended permit ip
172.16.1.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list outside_30_cryptomap extended permit ip
10.10.10.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list outside_30_cryptomap extended permit ip
10.10.120.0 255.255.255.0 20.20.20.0
255.255.255.0
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu man 1500
ip local pool Hill-V-IP 10.10.120.10-10.10.120.100 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
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
route outside 0.0.0.0 0.0.0.0 192.168.11.1 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
group-policy Hillvalley internal
group-policy Hillvalley attributes
wins-server value 10.10.10.20
dns-server value 10.10.10.20
vpn-tunnel-protocol IPSec
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Hillvalley_splitunnel
default-domain value corp.com
username cisco password dZBmhhbNIN5q6rGK encrypted
aaa authentication telnet console LOCAL
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 ipsec transform-set Hill-trans esp-3des esp-sha-
hmac
crypto dynamic-map outside_dyn_map 20 set transform-set
Hill-trans
crypto dynamic-map dyn_map 20 set reverse-route
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 30 match address
outside_30_cryptomap
crypto map outside_map 30 set peer 192.168.12.1
crypto map outside_map 30 set transform-set ESP-3DES-SHA

crypto map outside_map 65535 ipsec-isakmp dynamic
outside_dyn_map
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 *
tunnel-group 192.168.12.2 type ipsec-l2l
tunnel-group 192.168.12.2 ipsec-attributes
  pre-shared-key *
tunnel-group Hillvalley type ipsec-ra
tunnel-group Hillvalley general-attributes
address-pool Hill-V-IP
default-group-policy Hillvalley
tunnel-group Hillvalley ipsec-attributes
pre-shared-key *
telnet timeout 1440
ssh timeout 5
console timeout 0
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
```

```
!  
service-policy global_policy global  
prompt hostname context  
Cryptochecksum:62dc631d157fb7e91217cb82dc161a48  
ASA-NY-HQ#
```

Vérification

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 inside x.x.x.x (adresse IP de l'hôte sur le côté opposé du tunnel)** : cette commande vous permet d'envoyer du trafic dans le tunnel à l'aide de l'adresse source de l'interface interne.

Dépannage

Reportez-vous aux documents suivants pour obtenir des informations que vous pouvez utiliser afin de dépanner votre configuration :

- [Solutions de dépannage VPN IPSec les plus courantes](#)
- [Dépannage de sécurité IP - Comprendre et utiliser les commandes de dépannage](#)
- [Dépannage des connexions via PIX et ASA](#)

Informations connexes

- [Présentation du chiffrement IPSec \(IP Security\)](#)
- [Page de support de la négociation IPSec/des protocoles IKE](#)
- [Références des commandes des appareils de sécurité adaptatifs de la gamme Cisco ASA 5500](#)
- [Support et documentation techniques - Cisco Systems](#)