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
Composants utilisés
Conventions
Diagramme du réseau
Informations générales
Ajoutez un tunnel supplémentaire L2L à la configuration
Instructions pas à pas
Exemple de configuration
Ajoutez un Accès à distance VPN à la configuration
Instructions pas à pas
Exemple de configuration
Vérifiez
Dépannez
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 que vous configurez correctement le tunnel VPN L2L IPSEC qui est actuellement opérationnel avant que vous tentiez cette configuration.

Composants utilisés

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

- Deux dispositifs de sécurité ASA qui exécutent le code 7.x
- Un dispositifs de sécurité PIX qui exécutent le code 7.x

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.

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 est la configuration en cours d'exécution des dispositifs de sécurité NY (HUB). Dans cette configuration, il y a un tunnel d'IPSec L2L configuré entre NY(HQ) et TN.

Configuration de Pare-feu du courant NY (QG)

```
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

Actuellement, il y a un tunnel existant L2L installé entre le bureau NY(HQ) et le bureau TN. Votre société a récemment ouvert un nouveau bureau qui se trouve dans TX. Ce nouveau bureau exige la Connectivité aux ressources locales qui se trouvent dans les bureaux NY et TN. En outre, il y a une condition requise supplémentaire de permettre à des employés l'occasion de fonctionner de la maison et d'accéder à sécurisé les ressources qui se trouvent sur le réseau interne à distance. Dans cet exemple, un nouveau tunnel VPN est configuré aussi bien qu'un serveur VPN d'Accès à distance qui se trouve dans le le bureau NY.

Dans cet exemple, deux commandes sont utilisées afin de permettre la transmission entre les réseaux VPN et identifier le trafic qui devrait être percé un tunnel ou chiffré. Ceci te permet d'avoir accès à l'Internet sans devoir envoyer ce trafic par le tunnel VPN. Afin de configurer ces deux options, émettez les commandes de **tunnel partagé** et de même-Sécurité-**trafic**.

La Segmentation de tunnel permet à un client d'IPSec de remote-access pour diriger conditionnellement des paquets au-dessus d'un tunnel d'IPSec sous la forme chiffrée, ou à une interface réseau sous la forme des textes clairs. La Segmentation de tunnel étant activé, des paquets non attachés pour des destinations de l'autre côté du tunnel d'IPSec ne doivent pas être chiffrés, envoyé à travers le tunnel, ont déchiffré, et alors conduit à une destination définitive. Cette commande s'applique cette stratégie de Segmentation de tunnel à un réseau spécifié. Le par défaut est de percer un tunnel tout le trafic. Afin de placer une stratégie de Segmentation de tunnel, émettez la commande de fractionnement-tunnel-**stratégie** dans le mode de configuration de stratégie de groupe. Afin d'enlever la fractionnement-Tunnellisation-stratégie de la configuration, émettez le **forme no de** cette commande.

Les dispositifs de sécurité incluent une caractéristique qui permet à un client vpn pour envoyer le trafic IPSec-protégé à d'autres utilisateurs VPN en permettant un tel trafic dans et hors de la même interface. Le hairpinning également appelé, cette caractéristique peut être considéré comme les rais VPN (clients) qui se connectent par un hub VPN (dispositifs de sécurité). Dans une autre application, cette caractéristique peut réorienter le trafic VPN entrant soutiennent par la même interface que le trafic décrypté. C'est utile, par exemple, à un client vpn qui n'a pas la Segmentation de tunnel mais les besoins pour accéder à un VPN et pour parcourir le Web. Afin de configurer cette caractéristique, émettez la commande *intra-interface du même-Sécurité*-**trafic** en mode de configuration globale.

Ajoutez un tunnel supplémentaire L2L à la configuration

C'est le schéma de réseau pour cette configuration :

Instructions pas à pas

Cette section fournit les procédures exigées qui doivent être exécutées sur les dispositifs de sécurité de HUB (Pare-feu NY). Référez-vous au PIX/ASA 7.x : Simple PIX--PIX à l'exemple de configuration de tunnel VPN pour plus d'informations sur la façon configurer le client de rai (Pare-feu TX).

Procédez comme suit :

1. Créez ces deux nouvelles Listes d'accès à utiliser par le crypto map 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 20.20.20.0 255.255.255.0ASA-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 transmission ait lieu, l'autre côté du tunnel doit avoir l'opposé de cette entrée de liste de contrôle d'accès (ACL) pour ce réseau particulier.
2. Ajoutez ces entrées à l'aucune déclaration nat afin d'exempter nating entre ces réseaux :`ASA-NY-HQ(config)#access-list inside_nat0_outbound extended permit ip 172.16.1.0 255.255.255.0 20.20.20.0 255.255.255.0ASA-NY-HQ(config)#access-list inside_nat0_outbound extended permit ip 10.10.10.0 255.255.255.0 20.20.20.0 255.255.255.0ASA-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 transmission ait lieu, l'autre côté du tunnel doit avoir l'opposé de ce rubrique de liste ACL 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`Ceci permet à des homologues VPN pour parler entre l'un l'autre.
4. Créez la configuration de crypto map pour le nouveau tunnel VPN. Utilisez le même jeu de transformations qui a été utilisé en la première configuration du VPN, comme toutes les configurations de la phase 2 sont les mêmes.`ASA-NY-HQ(config)#crypto map outside_map 30 match address outside_30_cryptomapASA-NY-HQ(config)#crypto map outside_map 30 set peer 192.168.12.2ASA-NY-HQ(config)#crypto map outside_map 30 set transform-set ESP-3DES-SHA`
5. Créez le groupe de tunnels qui est spécifié pour ce tunnel avec des attributs requis pour se connecter au serveur distant.`ASA-NY-HQ(config)#tunnel-group 192.168.12.2 type ipsec-l2lASA-NY-HQ(config)#tunnel-group 192.168.12.2 ipsec-attributesASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key cisco123`**Remarque:** Le pre-shared-key doit s'assortir exactement des deux côtés du tunnel.
6. Maintenant que vous avez configuré le nouveau tunnel, vous devez envoyer le trafic intéressant à travers le tunnel afin de l'apporter. Afin d'exécuter ceci, émettez la **commande ping de source** de cingler un hôte sur le réseau intérieur du tunnel distant.Dans cet exemple, un poste de travail de l'autre côté du tunnel avec l'adresse 20.20.20.16 est cinglé. Ceci apporte le tunnel entre NY et TX. Maintenant, il y a deux tunnels connectés au bureau QG. Si vous n'avez pas accès à un système derrière le tunnel, référez-vous à la plupart des solutions communes de dépannage VPN d'IPSec pour trouver une solution alternative en ce qui concerne utiliser Gestion-`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#
```

Ajoutez un Accès à distance VPN à la configuration

C'est le schéma de réseau pour cette configuration :

Instructions pas à pas

Cette section fournit les procédures exigées pour ajouter la capacité d'Accès à distance et pour permettre à des utilisateurs distants pour accéder à tous les sites. Référez-vous à PIX/ASA 7.x ASDM : Limitez l'accès au réseau des utilisateurs de l'Accès à distance VPN pour plus d'informations sur la façon configurer le Remote Access Server et limiter l'accès.

Procédez comme suit :

1. Créez un groupe d'adresse IP à utiliser pour les clients qui se connectent par l'intermédiaire du tunnel VPN. En outre, créez un utilisateur de base afin d'accéder au VPN une fois que la configuration est terminée.`ASA-NY-HQ(config)#ip local pool Hill-V-IP 10.10.120.10-10.10.120.100 mask 255.255.255.0ASA-NY-HQ(config)#username cisco password cisco111`
2. Le trafic spécifique exempt de nated.`ASA-NY-HQ(config)#access-list inside_nat0_outbound extended permit ip 172.16.1.0 255.255.255.0 10.10.120.0 255.255.255.0ASA-NY-HQ(config)#access-list inside_nat0_outbound extended permit ip 10.10.120.0 255.255.255.0 10.10.10.0 255.255.255.0ASA-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 transmission nat entre les tunnels VPN est exemptée dans cet exemple.
3. Permettez la transmission entre les tunnels L2L qui sont déjà créés.`ASA-NY-HQ(config)#access-list outside_20_cryptomap extended permit ip 10.10.120.0 255.255.255.0 10.10.10.0 255.255.255.0ASA-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`Ceci permet à des utilisateurs d'Accès à distance la capacité de communiquer avec des réseaux derrière les tunnels spécifiés.**Avertissement :** Pour que la transmission ait lieu, l'autre côté du tunnel doit avoir l'opposé de ce rubrique de liste ACL pour ce réseau particulier.
4. Configurez le trafic qui sera chiffré et envoyé à travers le tunnel VPN.`ASA-NY-HQ(config)#access-list Hillvalley_splitunnel standard permit 172.16.1.0 255.255.255.0ASA-NY-HQ(config)#access-list Hillvalley_splitunnel standard permit 10.10.10.0 255.255.255.0ASA-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 des wins, des

dn et des protocoles IPsecs, pour les clients vpn.`ASA-NY-HQ(config)#group-policy Hillvalley internalASA-NY-HQ(config)#group-policy Hillvalley attributesASA-NY-HQ(config-group-policy)#wins-server value 10.10.10.20ASA-NY-HQ(config-group-policy)#dns-server value 10.10.10.20ASA-NY-HQ(config-group-policy)#vpn-tunnel-protocol IPSec`

6. Placez IPSec et attributs généraux, tels que les clés pré-partagées et les groupes d'adresse IP, qui seront utilisés par le tunnel VPN de Hillvalley.`ASA-NY-HQ(config)#tunnel-group Hillvalley ipsec-attributesASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key cisco1234ASA-NY-HQ(config)#tunnel-group Hillvalley general-attributesASA-NY-HQ(config-tunnel-general)#address-pool Hill-V-IPASA-NY-HQ(config-tunnel-general)#default-group-policy Hillvalley`
7. Créez la stratégie de tunnel partagé qui utilisera l'ACL créé dans l'étape 4 afin de spécifier quel trafic sera chiffré et a traversé le tunnel.`ASA-NY-HQ(config)#split-tunnel-policy tunnelspecifiedASA-NY-HQ(config)#split-tunnel-network-list value Hillvalley_splitunnel`
8. Configurez les informations requises de carte de cryto à la création de tunnel VPN.`ASA-NY-HQ(config)#crypto ipsec transform-set Hill-trans esp-3des esp-sha-hmacASA-NY-HQ(config)#crypto dynamic-map outside_dyn_map 20 set transform-set Hill-transASA-NY-HQ(config)#crypto dynamic-map dyn_map 20 set reverse-routeASA-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#
```

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** .

- **le ping x.x.x.x intérieur (adresse IP d'hôte du bord opposé du tunnel) — cette** commande te permet pour envoyer le trafic en bas du tunnel utilisant une adresse source de l'interface interne.

Dépannez

Référez-vous à ces documents pour information que vous pouvez employer afin de dépanner votre configuration :

- La plupart des solutions communes de dépannage VPN d'IPSec
- 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 de commandes de Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500
- Support et documentation techniques - Cisco Systems