PIX/ASA 7.X: Agregue un nuevo túnel o Acceso Remoto a un L2L existente VPN

Contenido

Introducción

Este documento proporciona los pasos necesarios para agregar un nuevo túnel VPN o una VPN de acceso remoto a una configuración VPN L2L que ya existe. Consulte Cisco ASA 5500 Series Adaptive Security Appliances - Ejemplos de Configuración y Lista de Notas Técnicas para obtener información sobre cómo crear los túneles IPSec VPN iniciales y más ejemplos de configuración.

prerrequisitos

Requisitos

Asegúrese de que usted configure correctamente el túnel del IPSEC VPN L2L que es actualmente operativo antes de que usted intente esta configuración.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dos dispositivos de seguridad ASA que funcionan con el código 7.x
- Un dispositivo de seguridad PIX que funciona con el código 7.x

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Esta salida es la Configuración actual de ejecución. del dispositivo de seguridad NY (CONCENTRADOR). En esta configuración, hay un túnel del IPSec L2L configurado entre NY(HQ) y el TN.

Configuración de escudo de protección actual 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#
```

Antecedentes

Actualmente, hay una configuración de túnel existente L2L entre la oficina NY(HQ) y la oficina TN. Su compañía ha abierto recientemente una nueva oficina que está situada en el TX. Esta nueva oficina requiere la Conectividad a los recursos locales que están situados en las oficinas NY y TN. Además, hay un requisito adicional de no prohibir a los empleados la oportunidad de trabajar del hogar y de acceder con seguridad los recursos que están situados en la red interna remotamente. En este ejemplo, se configura un nuevo túnel VPN así como un servidor del VPN de acceso remoto que está situado en el oficina NY.

En este ejemplo, se utilizan para permitir la comunicación entre las redes VPN e identificar el tráfico que debe ser tunneled o se cifran dos comandos. Esto le permite para tener acceso a Internet sin tener que enviar ese tráfico a través del túnel VPN. Para configurar estas dos opciones, publique el **túnel dividido** y los **comandos same-security-traffic**.

El Túnel dividido permite que un cliente IPSec del acceso remoto dirija condicional los paquetes sobre un túnel IPsec en la forma encriptada, o a una interfaz de la red en la forma de texto claro. Con el Túnel dividido habilitado, los paquetes no limitados para los destinos en el otro lado del túnel IPsec no tienen que ser cifrados, enviado a través del túnel, desencriptaron, y entonces ruteado a un destino final. Este comando aplica esta directiva del Túnel dividido a una red específicada. El valor por defecto es hacer un túnel todo el tráfico. Para fijar una directiva del Túnel dividido, publique el comando de la fractura-túnel-**directiva** en el modo de configuración de la grupo-directiva. Para quitar la fractura-Tunelización-directiva de la configuración, no publique la **ninguna** forma de este comando.

El dispositivo de seguridad incluye una característica que permita que un cliente VPN envíe el tráfico protegido por IPSec a otros usuarios de VPN permitiendo tal tráfico dentro y fuera de la misma interfaz. El hairpinning también llamado, esta característica se puede pensar en como spokes VPN (clientes) que conecta a través de un concentrador VPN (dispositivo de seguridad). En otra aplicación, esta característica puede reorientar el tráfico entrante VPN se retira a través de la misma interfaz que el tráfico no encriptado. Esto es útil, por ejemplo, a un cliente VPN que no tenga el Túnel dividido sino necesidades para acceder un VPN y para hojear la red. Para configurar esta característica, publique el *comando intra-interface del* **trafico de seguridad igual** en el modo de configuración global.

Agregue un túnel adicional L2L a la configuración

Éste es el diagrama de la red para esta configuración:

Instrucciones Paso a Paso

Esta sección proporciona los procedimientos requeridos que se deben realizar en el dispositivo de seguridad del CONCENTRADOR (Firewall NY). Refiera al PIX/ASA 7.x: Ejemplo de configuración del Túnel VPN PIX a PIX sencillo para más información sobre cómo configurar al cliente del spoke (Firewall TX).

Complete estos pasos:

1. Cree estas dos nuevas listas de acceso que se utilizarán por la correspondencia de criptografía para definir el tráfico interesante:`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`**Advertencia:** Para que la comunicación ocurra, el otro lado del túnel debe tener el contrario de esta entrada del Access Control List (ACL) para esa red determinada.
2. Agregue estas entradas a la ninguna sentencia NAT para eximir nating entre estas redes:`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`**Advertencia:** Para que la comunicación ocurra, el otro lado del túnel debe tener el contrario de esta entrada ACL para esa red determinada.
3. Publique este comando para permitir a un host en la red VPN TX para tener acceso al túnel TN VPN:`ASA-NY-HQ(config)#same-security-traffic permit intra-interface`Esto permite que los pares VPN hablen entre uno a.
4. Cree la configuración de la correspondencia de criptografía para el nuevo túnel VPN. Utilice lo mismo transforman el conjunto que fue utilizado en la primera configuración VPN, como todas las configuraciones de la fase 2 son lo mismo.`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. Cree al grupo de túnel que se especifica para este túnel junto con los atributos necesarios para conectar con el host remoto.`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`**Nota:** La clave previamente compartida debe hacer juego exactamente a ambos lados del túnel.
6. Ahora que usted ha configurado el nuevo túnel, usted debe enviar el tráfico interesante a través del túnel para traerlo para arriba. Para realizar esto, publique el **comando ping de la fuente** de hacer ping un host en la red interna del túnel remoto.En este ejemplo, un puesto de trabajo en el otro lado del túnel con el direccionamiento 20.20.20.16 se hace ping. Esto trae el túnel para arriba entre el NY y el TX. Ahora, hay dos túneles conectados con la oficina HQ. Si usted no tiene acceso a un sistema detrás del túnel, refiera a la mayoría de las soluciones del troubleshooting del IPSec comunes VPN para encontrar una solución alternativa por lo que se refiere a usar el `Acceso de administración`.

Ejemplo de configuración

Ejemplo de configuración 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#
```

Agregue un VPN de acceso remoto a la configuración

Éste es el diagrama de la red para esta configuración:

Instrucciones Paso a Paso

Esta sección proporciona los procedimientos requeridos para agregar la capacidad de Acceso Remoto y para permitir que los usuarios remotos accedan todos los sitios. Refiera al ASDM del PIX/ASA 7.x: Restrinja el acceso a la red de los usuarios del VPN de acceso remoto para más información sobre cómo configurar el Remote Access Server y restringir el acceso.

Complete estos pasos:

1. Cree un pool de la dirección IP que se utilizará para los clientes que conectan vía el túnel VPN. También, cree a un usuario básico para acceder el VPN una vez que se completa la configuración.`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. Exima el tráfico específico 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`Note que la comunicación nacional entre los túneles VPN está eximida en este ejemplo.
3. Permita la comunicación entre los túneles L2L que se crean ya.`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`Esto no prohibe a usuarios de acceso remoto la capacidad de comunicar con las redes detrás de los túneles especificados.**Advertencia:** Para que la comunicación ocurra, el otro lado del túnel debe tener el contrario de esta entrada ACL para esa red determinada.
4. Configure el tráfico que será cifrado y enviado a través del túnel 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. Configure la autenticación local y la información de política, tal como triunfos, dns y los Protocolos IPSec, para los clientes 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. Fije el IPSec y los atributos generales, tales como claves previamente compartidas y pools de la dirección IP, que serán utilizados por el túnel de Hillvalley VPN.
```
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. Cree la directiva del túnel dividido que utilizará el ACL creado en el paso 4 para especificar qué tráfico será cifrado y pasado a través del túnel.
```
ASA-NY-HQ(config)#split-tunnel-policy
 tunnelspecifiedASA-NY-HQ(config)#split-tunnel-network-list value
 Hillvalley_splitunnel
```

8. Configure la información de mapa del cryto requerida a la creación de túnel 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
```

Ejemplo de configuración

Ejemplo de configuración 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#
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **haga ping dentro de x.x.x.x (dirección IP del host en el lado opuesto del túnel) — este** comando permite que usted envíe el tráfico abajo del túnel usando una dirección de origen de la interfaz interior.

Troubleshooting

Refiera a estos documentos para la información que usted puede utilizar para resolver problemas su configuración:

- La mayoría de las soluciones del troubleshooting del IPSec comunes VPN
- Resolución de problemas de seguridad de IP – Información y uso de los comandos de depuración
- Conexiones del Troubleshooting con el PIX y el ASA

Información Relacionada

- Una Introducción al Cifrado de Seguridad IP (IPSec)
- Página de Soporte de IPSec Negotiation/IKE Protocols
- Referencias de comandos del Dispositivos de seguridad adaptable Cisco ASA de la serie 5500
- Soporte Técnico y Documentación - Cisco Systems