PIX/ASA 7.X: Agregar un túnel nuevo o acceso remoto a una VPN L2L existente

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.

Prerequisites

Requirements

Asegúrese de configurar correctamente el túnel VPN IPSEC L2L que está actualmente operativo antes de intentar 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 ejecutan código 7.x
- Un dispositivo de seguridad PIX que ejecuta código 7.x

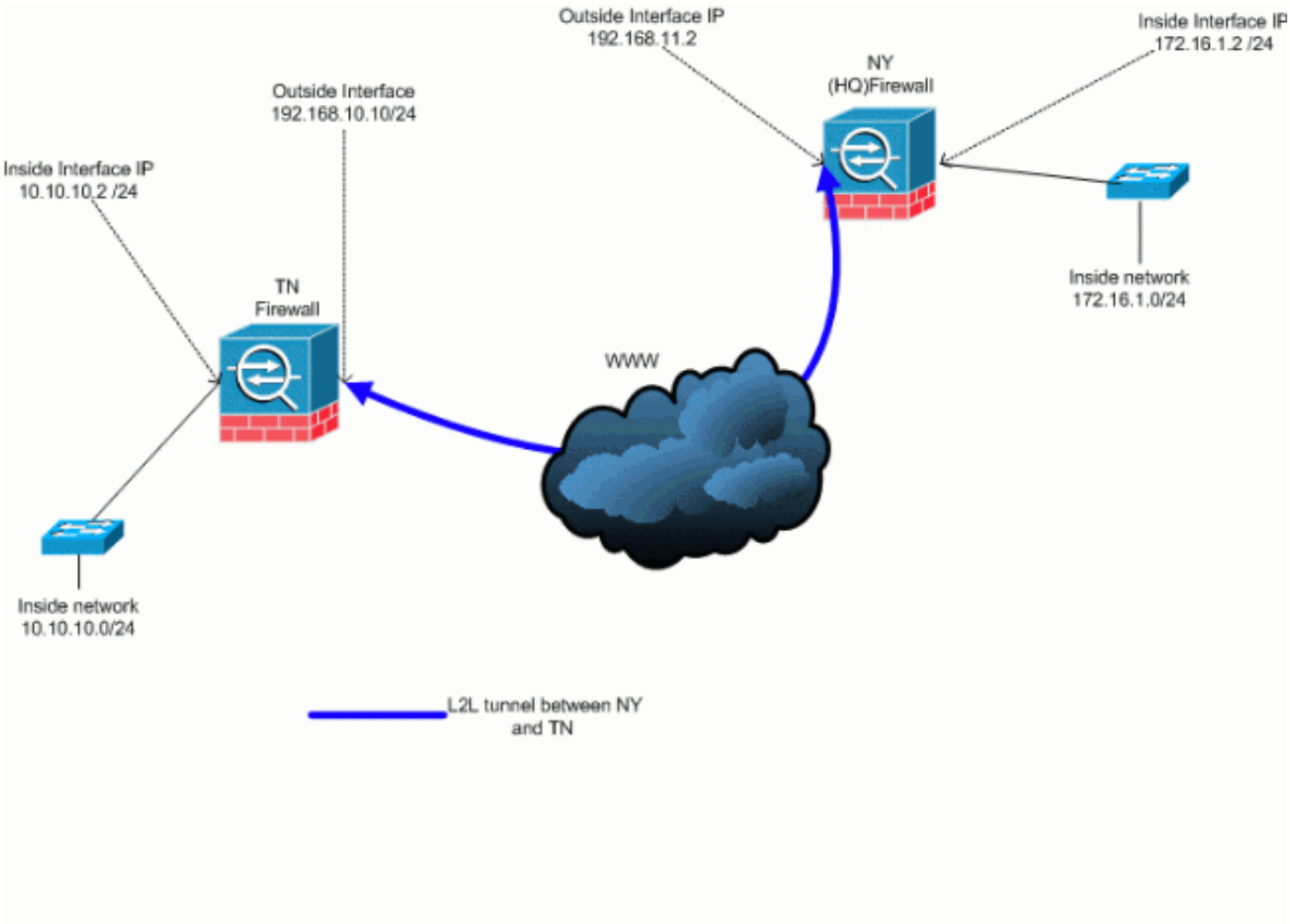
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

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:



Este resultado es la configuración actual en ejecución del dispositivo de seguridad NY (HUB). En esta configuración, hay un túnel L2L IPSec configurado entre NY(HQ) y TN.

Configuración actual del firewall 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, existe un túnel L2L configurado entre la oficina de NY(HQ) y la oficina de TN. Su empresa ha abierto recientemente una nueva oficina ubicada en TX. Esta nueva oficina requiere conectividad con los recursos locales ubicados en las oficinas de NY y TN. Además, existe un requisito adicional para permitir a los empleados la oportunidad de trabajar desde casa y acceder de forma segura a los recursos que se encuentran en la red interna de forma remota. En este ejemplo, se configura un nuevo túnel VPN, así como un servidor VPN de acceso remoto ubicado en la oficina de NY.

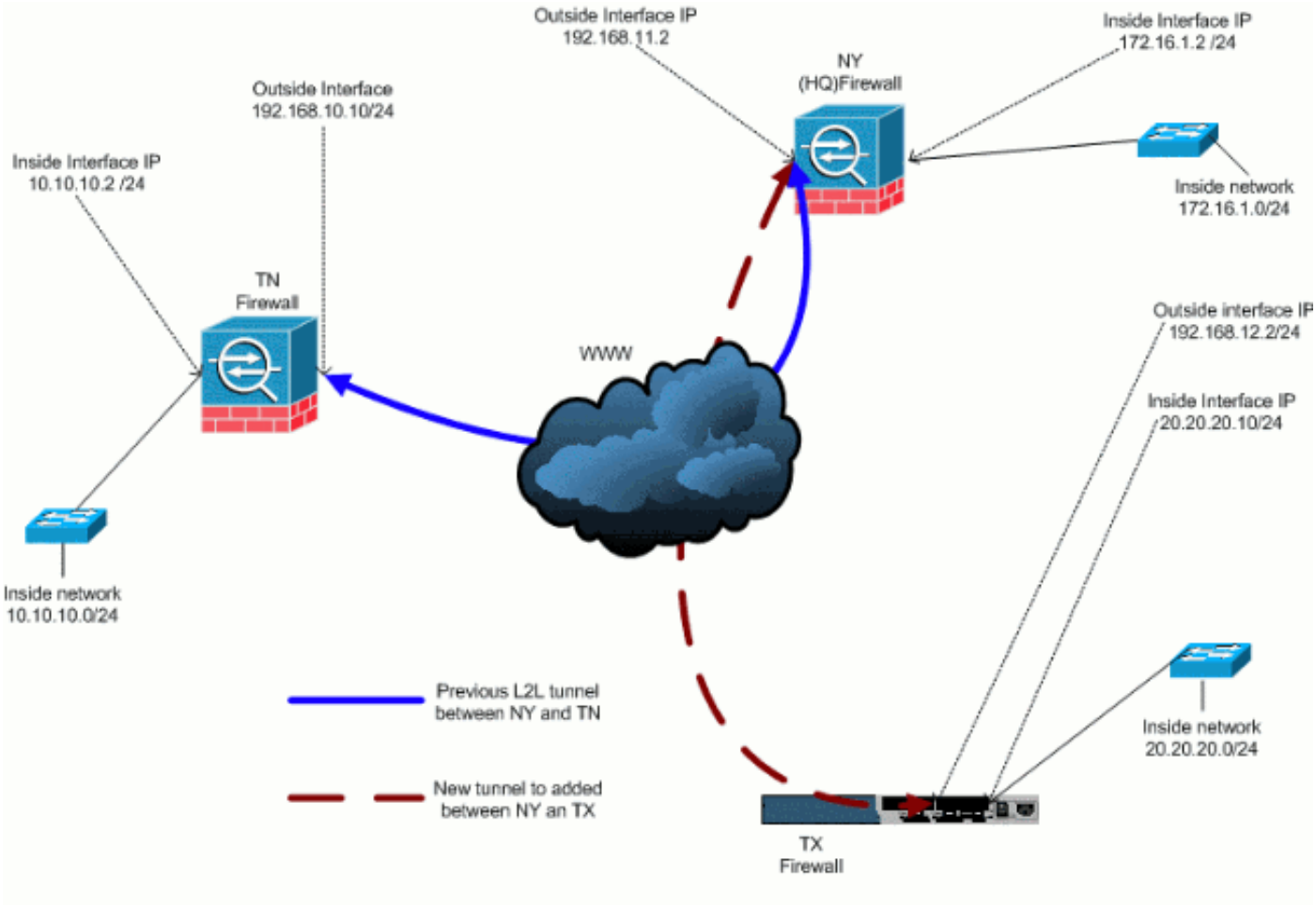
En este ejemplo, se utilizan dos comandos para permitir la comunicación entre las redes VPN e identificar el tráfico que se debe tunelizar o cifrar. Esto le permite tener acceso a Internet sin tener que enviar ese tráfico a través del túnel VPN. Para configurar estas dos opciones, ejecute los comandos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

La tunelización dividida permite a un cliente IPSec de acceso remoto dirigir paquetes condicionalmente a través de un túnel IPSec en forma encriptada, o a una interfaz de red en forma de texto claro. Con la tunelización dividida habilitada, los paquetes que no están enlazados a destinos en el otro lado del túnel IPSec no tienen que ser cifrados, enviados a través del túnel, descifrados y luego enrutados a un destino final. Este comando aplica esta política de tunelización dividida a una red especificada. El valor predeterminado es tunelizar todo el tráfico. Para establecer una política de tunelización dividida, ejecute el comando **split-tunnel-policy** en el modo de configuración de política de grupo. Para quitar la política de túnel dividido de la configuración, ejecute la forma **no** de este comando.

El dispositivo de seguridad incluye una función que permite a un cliente VPN enviar tráfico protegido por IPSec a otros usuarios de VPN permitiendo que dicho tráfico entre y salga de la misma interfaz. También denominada hairpinning, esta función se puede considerar como radios VPN (clientes) que se conectan a través de un hub VPN (dispositivo de seguridad). En otra aplicación, esta función puede redirigir el tráfico VPN entrante a través de la misma interfaz que el tráfico no cifrado. Esto es útil, por ejemplo, para un cliente VPN que no tiene tunelización dividida pero necesita acceder a una VPN y navegar por la web. Para configurar esta función, ejecute el comando **same-security-traffic** ***intra-interface*** en el modo de configuración global.

Agregar un túnel L2L adicional a la configuración

Este es el diagrama de red para esta configuración:



Step-by-Step Instructions

Esta sección proporciona los procedimientos necesarios que se deben realizar en el dispositivo de seguridad HUB (NY Firewall). Consulte PIX/ASA 7.x: Ejemplo de Configuración Simple de Túnel VPN PIX a PIX para obtener más información sobre cómo configurar el cliente spoke (Firewall TX).

Complete estos pasos:

1. Cree estas dos nuevas listas de acceso que serán utilizadas por el mapa crypto 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
    20.20.20.0 255.255.255.0


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
```

   Advertencia: Para que la comunicación tenga lugar, el otro lado del túnel debe tener lo contrario de esta entrada de lista de control de acceso (ACL) para esa red en particular.
2. Agregue estas entradas a la sentencia no nat para eximir el nating entre estas redes:

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


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
```

Advertencia: Para que la comunicación tenga lugar, el otro lado del túnel debe tener lo contrario de esta entrada ACL para esa red en particular.

3. Ejecute este comando para habilitar un host en la red TX VPN para que tenga acceso al túnel TN VPN:

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

Esto permite a los peers VPN comunicarse entre sí.

4. Cree la configuración de mapa criptográfico para el nuevo túnel VPN. Utilice el mismo conjunto de transformación que se utilizó en la primera configuración de VPN, ya que todos los valores de la fase 2 son iguales.

```
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. Cree el grupo de túnel especificado para este túnel junto con los atributos necesarios para conectarse al host remoto.

```
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
```

Nota: La clave previamente compartida debe coincidir exactamente en ambos lados del túnel.

6. Ahora que ha configurado el nuevo túnel, debe enviar tráfico interesante a través del túnel para activarlo. Para realizar esto, ejecute el comando **source ping** para hacer ping a un host en la red interna del túnel remoto.En este ejemplo, se hace ping a una estación de trabajo del otro lado del túnel con la dirección 20.20.20.16. Esto activa el túnel entre NY y TX. Ahora, hay dos túneles conectados a la oficina central. Si no tiene acceso a un sistema detrás del túnel, consulte Soluciones de Troubleshooting de VPN IPSec Más Comunes para encontrar una solución alternativa con respecto al uso de `management-access`.

Ejemplo de configuración

Ejemplo de configuración 1

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

 : Saved
:
ASA Version 7.2(2)
!
hostname ASA-NY-HQ
```

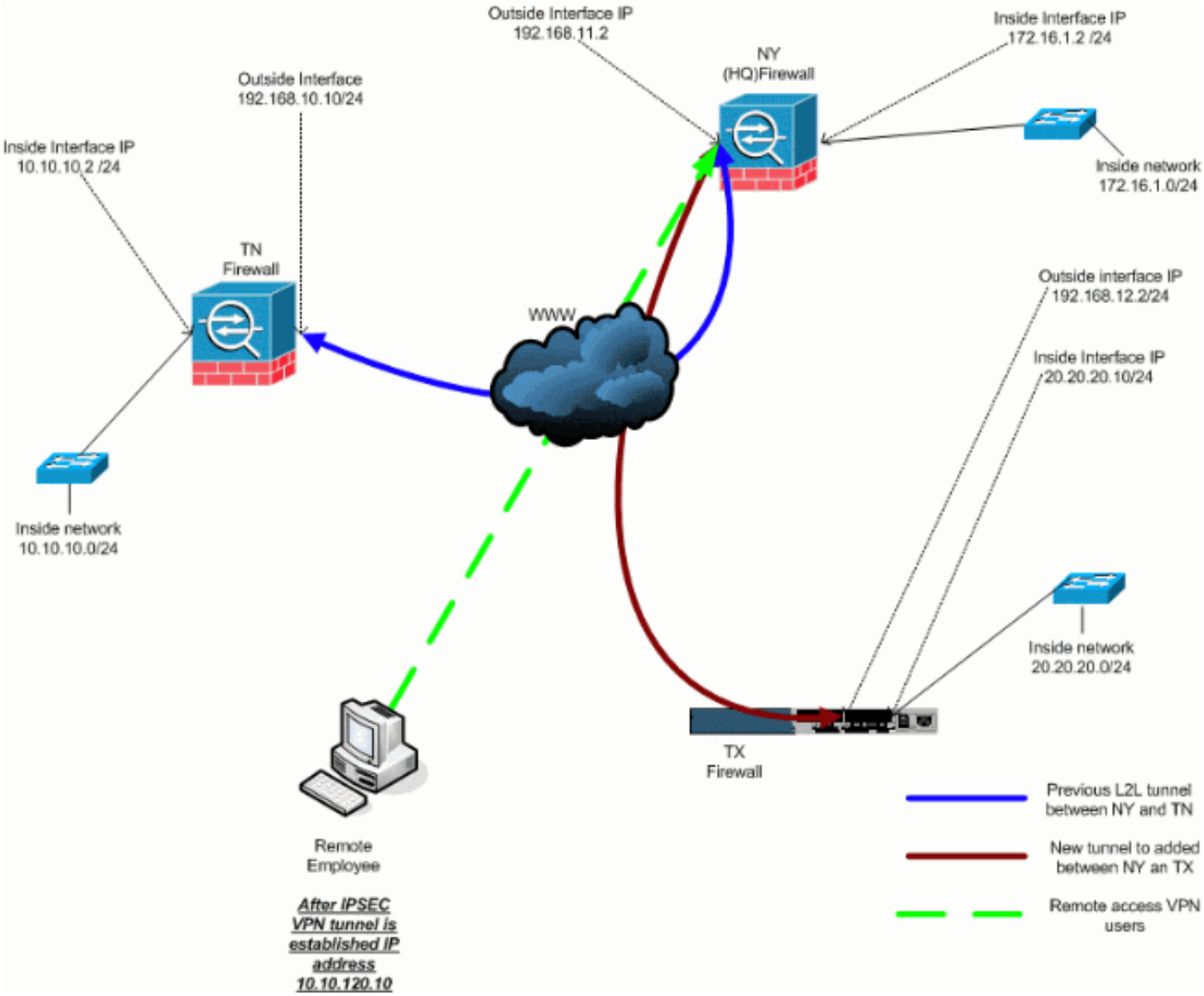
```
domain-name corp2.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.11.1 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet0/2
 shutdown
 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#
```

Agregar una VPN de acceso remoto a la configuración

Este es el diagrama de red para esta configuración:



Step-by-Step Instructions

Esta sección proporciona los procedimientos necesarios para agregar capacidad de acceso remoto y permitir que los usuarios remotos accedan a todos los sitios. Consulte ASDM PIX/ASA 7.x: Restrinja el Acceso a la Red de Usuarios VPN de Acceso Remoto para obtener más información sobre cómo configurar el servidor de acceso remoto y restringir el acceso.

Complete estos pasos:

1. Cree un conjunto de direcciones IP que se utilizará para los clientes que se conectan a través del túnel VPN. Además, cree un usuario básico para acceder a la VPN una vez que se complete la configuración.

```
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. Evite que se detecte tráfico específico.

```
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
```

   Observe que la comunicación nat entre túneles VPN está exenta en este ejemplo.

3. Permitir la comunicación entre los túneles L2L que ya se han creado.

```
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
```

   Esto permite a los usuarios de acceso remoto comunicarse con las redes detrás de los túneles especificados.**Advertencia:** Para que la comunicación tenga lugar, el otro lado del túnel debe tener lo contrario de esta entrada ACL para esa red en particular.

4. Configure el tráfico que se cifrará y se enviará a través del túnel 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. Configure la autenticación local y la información de políticas, como victorias, dns y protocolos IPSec, para los clientes 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. Establezca IPSec y atributos generales, como claves previamente compartidas y conjuntos de direcciones IP, que serán utilizados por el túnel VPN de 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. Cree la política de túnel dividido que utilizará la ACL creada en el paso 4 para especificar qué tráfico se cifrará y pasará a través del túnel.

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

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

8. Configure el criyto para asignar la información requerida a la creación del túnel 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
```

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.

- **ping inside x.x.x.x (dirección IP del host en el lado opuesto del túnel)**: este comando permite enviar tráfico por el túnel utilizando la dirección de origen de la interfaz interna.

Troubleshoot

Consulte estos documentos para obtener información que puede utilizar para resolver problemas de su configuración:

- Soluciones de resolución de problemas de VPN IPSec más comunes
- Resolución de problemas de seguridad de IP – Información y uso de los comandos de depuración
- Solución de problemas de conexiones a través de PIX y ASA

Información Relacionada

- Una Introducción al Cifrado de Seguridad IP (IPSec)
- Página de Soporte de IPSec Negotiation/IKE Protocols
- Referencias de Comandos de Cisco ASA 5500 Series Adaptive Security Appliances
- Soporte Técnico y Documentación - Cisco Systems