PIX/ASA 7.x: Agregue/quite una red en un ejemplo existente de la configuración del túnel L2L VPN

Contenido

Introducción

Este documento proporciona una configuración de muestra para que cómo agregue una nueva red a un túnel existente VPN.

prerrequisitos

Requisitos

Asegúrese de que usted tenga un dispositivo de seguridad del PIX/ASA que funcione con el código 7.x antes de que usted intente esta configuración.

Componentes Utilizados

La información en este documento se basa en dos dispositivos del dispositivo de seguridad del Cisco 5500.

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.

Productos Relacionados

Esta configuración se puede también utilizar con el dispositivo de seguridad PIX 500.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

Hay actualmente un túnel del LAN a LAN (L2L) VPN que está entre la oficina NY y TN. La oficina NY acaba de agregar una nueva red que se utilizará por el grupo del desarrollo de CSI. Este grupo requiere el acceso a los recursos que residen en la oficina TN. La tarea a mano es agregar la nueva red al túnel ya existente VPN.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Agregar la red al túnel IPsec

Este documento usa esta configuración:

Config 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 nameif Cisco
security-level 70 ip address 172.16.40.2 255.255.255.0 !
interface Ethernet0/3 shutdown no nameif no security-
level no ip address ! interface Management0/0 shutdown
no nameif no security-level no ip address ! passwd
2KFQnbNIdI.2KYOU encrypted ftp mode passive dns server-
group DefaultDNS domain-name corp2.com access-list
inside_nat0_outbound extended permit ip 172.16.1.0
255.255.255.0 10.10.10.0 255.255.255.0 !--- You must be
sure that you configure the !--- opposite of these
```

```
access control lists !--- on the other end of the VPN
tunnel. access-list inside_nat0_outbound extended permit
ip 172.16.40.0 255.255.255.0 10.10.10.0 255.255.255.0
access-list outside_20_cryptomap extended permit ip
172.16.1.0 255.255.255.0 10.10.10.0 255.255.255.0 !---
You must be sure that you configure the !--- opposite of
these access control lists !--- on the other end of the
VPN tunnel. access-list outside_20_cryptomap extended
permit ip 172.16.40.0 255.255.255.0 10.10.10.0
255.255.255.0 !--- Output is suppressed. nat-control
global (outside) 1 interface nat (inside) 0 access-list
inside_nat0_outbound nat (inside) 1 172.16.1.0
255.255.255.0 !--- The new network is also required to
have access to the Internet. !--- So enter an entry into
the NAT statement for this new network. nat (inside) 1
172.16.40.0 255.255.255.0 route outside 0.0.0.0 0.0.0.0
192.168.11.100 1 timeout xlate 3:00:00 timeout conn
1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media
0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute no snmp-server location
no snmp-server contact snmp-server enable traps snmp
authentication linkup linkdown coldstart crypto ipsec
transform-set ESP-3DES-SHA esp-3des esp-sha-hmac crypto
map outside_map 20 match address outside_20_cryptomap
crypto map outside_map 20 set peer 192.168.10.10 crypto
map outside_map 20 set transform-set ESP-3DES-SHA crypto
map outside_map interface outside crypto isakmp enable
outside crypto isakmp policy 10 authentication pre-share
encryption 3des hash sha group 2 lifetime 86400 crypto
isakmp nat-traversal 20 tunnel-group 192.168.10.10 type
ipsec-l2l tunnel-group 192.168.10.10 ipsec-attributes
pre-shared-key * !--- Output is suppressed. : end ASA-
NY-HQ#
```

Eliminación de la red del túnel IPsec

Utilice esto camina para quitar la red de la configuración del túnel IPsec. Aquí, considere que la red 172.16.40.0/24 se ha quitado de la configuración del aparato NY (HQ) Secuirty.

1. Antes quite la red del túnel, derriban conexión IPSec, que también borra las asociaciones de seguridad relacionadas con la fase 2.
   ASA-NY-HQ# clear crypto ipsec sa Borra las asociaciones de seguridad relacionadas con la fase 1 como sigue
   ASA-NY-HQ# clear crypto isakmp sa
2. Quite el tráfico interesante ACL para el túnel IPsec.
   ASA-NY-HQ(config)# no access-list outside_20_cryptomap extended permit ip 172.16.40.0 255.255.255.0 10.10.10.0 255.255.255.0
3. Quite el ACL (inside_nat0_outbound), puesto que el tráfico se excluye del nacional.
   ASA-NY-HQ(config)# no access-list inside_nat0_outbound extended permit ip 172.16.40.0 255.255.255.0 10.10.10.0 255.255.255.0
4. Borre la traducción de NAT como se muestra
   ASA-NY-HQ# clear xlate
5. Cuando usted modifica nunca la configuración del túnel, quite y reaplique este los comandos crypto de tomar configuración más posterior de la interfaz exterior
   ASA-NY-HQ(config)# crypto map outside_map interface outside ASA-NY-HQ(config)# crypto isakmp enable outside

6. Salve la configuración activa al flash **“escriben la memoria”**.
7. Siga el mismo procedimiento para el otro extremo - dispositivo de seguridad TN para quitar las configuraciones.
8. Inicie el túnel IPsec y verifique la conexión.

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 172.16.40.20**
- **show crypto isakmp sa**
- **show crypto ipsec sa**

Troubleshooting

Refiera a estos documentos para más información de Troubleshooting:

- IPSec VPN que resuelve problemas las soluciones
- Entendiendo y con los comandos debug
- Resolver problemas las conexiones con el PIX y el ASA

Información Relacionada

- **Una Introducción al Cifrado de Seguridad IP (IPSec)**
- **Página de Soporte del Protocolo IKE/la Negociación de IPSec**
- **Referencia de comandos del dispositivo de seguridad**
- **Configuración de Listas de Acceso IP**
- **Soporte Técnico y Documentación - Cisco Systems**