PIX 6.x: Ejemplo de Paso de Túnel IPSec a través de un Firewall PIX con el Uso de la Lista de Acceso y con la Configuración NAT

Contenido

Introducción

Este documento proporciona una configuración de ejemplo de un túnel IPSec a través de un firewall que realiza la Conversión de Dirección de Red (NAT). **Esta configuración no funciona con la traducción de direcciones de puerto (PAT) si utiliza versiones de software del IOS® de Cisco anteriores y no incluidas 12.2(13)T.** Este tipo de configuración se puede utilizar para tunelizar el tráfico IP. No se puede utilizar para cifrar el tráfico que no pasa a través de un firewall, como IPX o las actualizaciones de ruteo. La tunelización Generic routing encapsulation (GRE) es apropiada para ese tipo de configuración. En el ejemplo de este documento, los routers Cisco 2621 y 3660 son los puntos finales de tunelización IPSec que unen dos redes privadas, con conductos o Listas de control de acceso (ACL) en el PIX en medio para permitir el tráfico IPSec.

Nota: NAT es una traducción de dirección uno a uno, que no debe confundirse con PAT, que es una traducción de muchos (dentro del firewall) a uno. Consulte Verificación del Funcionamiento de NAT y Troubleshooting básico de NAT o Cómo funciona NAT para obtener más información sobre el funcionamiento y la configuración de NAT.

Nota: Es posible que IPSec con PAT no funcione correctamente porque el dispositivo de extremo del túnel externo no puede manejar varios túneles desde una dirección IP. Debe ponerse en contacto con su proveedor para determinar si los dispositivos de terminal de túnel funcionan con PAT. Además, en las versiones 12.2(13)T y posteriores, la función de transparencia NAT también se puede utilizar para PAT. Consulte Transparencia NAT IPSec para obtener más información. Consulte Soporte para IPSec ESP a través de NAT para obtener más información sobre estas

funciones en las versiones 12.2(13)T y posteriores. Además, antes de abrir un caso con el TAC, consulte Preguntas frecuentes sobre NAT, que tiene muchas respuestas a preguntas comunes.

Consulte Ejemplo de Paso de Túnel IPSec a través de un Dispositivo de Seguridad con el Uso de la Lista de Acceso y MPF con Configuración NAT para obtener más información sobre cómo configurar un túnel IPSec a través de un firewall con NAT en la versión 7.x de PIX/ASA.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Versión 12.0.7.T del software del IOS de Cisco [hasta pero sin incluir 12.2(13)T]Consulte IPSec NAT Transparency para ver las versiones más recientes.
- Router Cisco 2621 que ejecuta la versión 12.4 del software del IOS de Cisco
- Cisco 3660 Router que ejecuta Cisco IOS Software Release 12.4
- Cisco PIX Firewall que ejecuta 6.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.

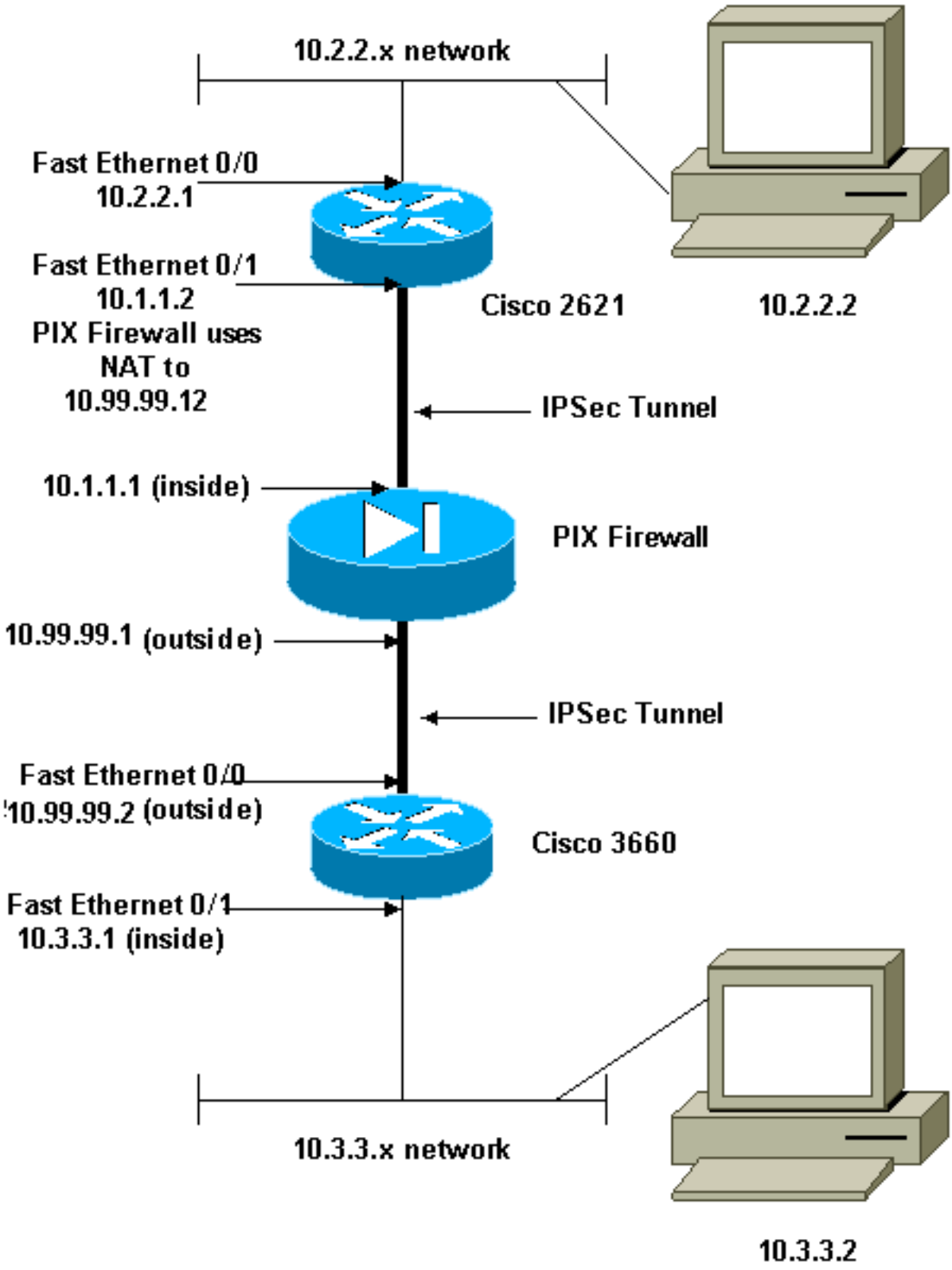
Configurar

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

Nota: Use la Command Lookup Tool (sólo clientes registrados) para obtener más información sobre los comandos utilizados en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Nota: Los esquemas de direccionamiento IP utilizados en esta configuración no son legalmente enrutables en Internet. Estas son direcciones RFC 1918 que se han utilizado en un entorno de laboratorio.

Configuraciones

En este documento, se utilizan estas configuraciones:

- Configuración de Cisco 2621
- Configuración parcial de Cisco PIX Firewall

- Configuración del 3660 de Cisco

Configuración de Cisco 2621

```
Current configuration:
 !
 version 12.4
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname goss-2621
 !
 ip subnet-zero
 !
 ip audit notify log
 ip audit po max-events 100
 isdn voice-call-failure 0
 cns event-service server
 !
 !--- IKE Policy crypto isakmp policy 10
  hash md5
  authentication pre-share
 crypto isakmp key cisco123 address 10.99.99.2
 !
 crypto ipsec transform-set myset esp-des esp-md5-hmac
 !
 crypto map mymap local-address FastEthernet0/1
 !--- IPSec Policy crypto map mymap 10 ipsec-isakmp
  set peer 10.99.99.2
  set transform-set myset
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101
 !
 controller T1 1/0
 !
 interface FastEthernet0/0
  ip address 10.2.2.1 255.255.255.0
  no ip directed-broadcast
  duplex auto
  speed auto
 !
 interface FastEthernet0/1
  ip address 10.1.1.2 255.255.255.0
  no ip directed-broadcast
  duplex auto
  speed auto
 !--- Apply to interface. crypto map mymap
 !
 ip classless
 ip route 0.0.0.0 0.0.0.0 10.1.1.1
 no ip http server
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.2.2.0 0.0.0.255 10.3.3.0 0.0.0.255
 line con 0
  transport input none
 line aux 0
 line vty 0 4
 !
 no scheduler allocate
```

```
 end
```

Configuración parcial de Cisco PIX Firewall

```
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
!--- The fixup protocol esp-ike command is disabled by
default.

fixup protocol esp-ike

ip address outside 10.99.99.1 255.255.255.0
 ip address inside 10.1.1.1 255.255.255.0
 !--- Range of registered IP addresses for use. global
(outside) 1 10.99.99.50-10.99.99.60 !--- Translate any
internal source address when !--- going out to the
Internet. nat (inside) 1 0.0.0.0 0.0.0.0 0 0
 static (inside,outside) 10.99.99.12 10.1.1.2 netmask
255.255.255.255 0 0

 !--- or access-list acl-out permit esp host 10.99.99.2
host 10.99.99.12
 access-list acl-out permit udp host 10.99.99.2 host
10.99.99.12 eq isakmp
 access-list acl-out permit udp host 10.99.99.2 host
10.99.99.12 eq 4500
!--- It is important to permit UDP port 4500 for NAT-T
because the PIX is acting !--- as a NAT device between
the routers. access-group acl-out in interface outside
isakmp enable outside isakmp enable inside Command
configured in order to enable NAT-T isakmp nat-traversal
20 route outside 0.0.0.0 0.0.0.0 99.99.99.2 1 route
inside 10.2.2.0 255.255.255.0 10.1.1.2 1
```

Nota: El comando **fixup protocol esp-ike** está inhabilitado de forma predeterminada. Si se ejecuta un comando **fixup protocol esp-ike**, el fixup se enciende y el firewall PIX conserva el puerto de origen del Intercambio de claves de Internet (IKE). También crea una traducción PAT para el tráfico ESP. Además, si el dispositivo esp-ike está activado, la Asociación de seguridad de Internet y el protocolo de administración de claves (ISAKMP) no se pueden habilitar en ninguna interfaz.

Configuración del 3660 de Cisco

```
version 12.4
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname goss-3660
 !
```

```
 ip subnet-zero
 !
 cns event-service server
 !
 !--- IKE Policy crypto isakmp policy 10
  hash md5
  authentication pre-share
 crypto isakmp key cisco123 address 10.99.99.12
 !
 crypto ipsec transform-set myset esp-des esp-md5-hmac
 !
 crypto map mymap local-address FastEthernet0/0
 !--- IPSec Policy crypto map mymap 10 ipsec-isakmp
  set peer 10.99.99.12
  set transform-set myset
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101
 !
 interface FastEthernet0/0
  ip address 10.99.99.2 255.255.255.0
  no ip directed-broadcast
  ip nat outside
  duplex auto
  speed auto
 !--- Apply to interface. crypto map mymap
 !
 interface FastEthernet0/1
  ip address 10.3.3.1 255.255.255.0
  no ip directed-broadcast
  ip nat inside
  duplex auto
  speed auto
 !
 interface Ethernet3/0
  no ip address
  no ip directed-broadcast
  shutdown
 !
 interface Serial3/0
  no ip address
  no ip directed-broadcast
  no ip mroute-cache
  shutdown
 !
 interface Ethernet3/1
  no ip address
  no ip directed-broadcast
 interface Ethernet4/0
  no ip address
  no ip directed-broadcast
  shutdown
 !
 interface TokenRing4/0
  no ip address
  no ip directed-broadcast
  shutdown
  ring-speed 16
 !
 !--- Pool from which inside hosts translate to !--- the
globally unique 10.99.99.0/24 network. ip nat pool
OUTSIDE 10.99.99.70 10.99.99.80 netmask 255.255.255.0
 !--- Except the private network from the NAT process.
ip nat inside source route-map nonat pool OUTSIDE
```

```
 ip classless
 ip route 0.0.0.0 0.0.0.0 10.99.99.1
 no ip http server
 !
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
 access-list 101 deny   ip 10.3.3.0 0.0.0.255 any
 !--- Except the private network from the NAT process.
access-list 110 deny   ip 10.3.3.0 0.0.0.255 10.2.2.0
0.0.0.255
 access-list 110 permit ip 10.3.3.0 0.0.0.255 any
 route-map nonat permit 10
  match ip address 110
 !
 line con 0
  transport input none
 line aux 0
 line vty 0 4
 !
 end
```

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.

- **show crypto ipsec sa**: muestra las asociaciones de seguridad de la fase 2.
- **show crypto isakmp sa — Muestra las asociaciones de seguridad de la fase 1.**
- **show crypto engine connections active**: utilícelo para ver los paquetes cifrados y descifrados.

Troubleshoot

Use esta sección para resolver problemas de configuración.

Comandos para resolución de problemas

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos **debug**.

- **debug crypto engine — muestra el tráfico codificado.**
- **debug crypto ipsec**: se utiliza para ver las negociaciones IPSec de la fase 2.
- **debug crypto isakmp**: utilice para ver las negociaciones ISAKMP de la fase 1.

Verificación de las asociaciones de seguridad

- **clear crypto isakmp**: borra las asociaciones de seguridad IKE.
- **clear crypto ipsec sa**: borra las asociaciones de seguridad IPSec.

Información Relacionada

- Dispositivos de seguridad Cisco PIX de la serie 500
- Referencias de Comandos de Cisco Secure PIX Firewall
- Página de Soporte de NAT
- Solicitud de comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems