PIX 6.x: Paso del túnel IPsec con un firewall PIX con el uso de la lista de acceso y con el ejemplo de la configuración del 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 trabaja con el Port Address Translation (PAT) si usted utiliza las versiones de software de Cisco IOS® antes y no incluyendo de 12.2(13)T.** Este tipo de configuración puede ser utilizado para hacer un túnel 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: El NAT es una traducción de direcciones de uno a uno, no ser confundido con la PALMADITA, que es muchas (dentro del Firewall) - -uno a la traducción. Refiera a verificar el Funcionamiento de NAT y el Troubleshooting de NAT básico o cómo el NAT trabaja para más información sobre el Funcionamiento de NAT y la configuración.

Nota: El IPSec con la PALMADITA no pudo trabajar correctamente porque el dispositivo del punto final del túnel exterior no puede manejar los túneles múltiples a partir de una dirección IP. Usted necesita entrar en contacto a su vendedor para determinar si los dispositivos del punto finales del túnel funcionan con el patente. Además, en las versiones 12.2(13)T y posterior, la característica de la Transparencia NAT se puede también utilizar para el patente refiere a la Transparencia IPSec NAT para más información. Refiera al soporte para el IPSec ESP con el NAT para más

información sobre estas características en las versiones 12.2(13)T y posterior. También, antes de que usted abra un caso con TAC, refiera a las Preguntas frecuentes sobre NAT, que tiene muchas respuestas a las preguntas comunes.

Refiera al paso del túnel IPsec con un dispositivo de seguridad con el uso de la lista de acceso y el MPF con el ejemplo de la configuración del NAT para más información sobre cómo configurar un túnel IPsec con un Firewall con el NAT en la versión 7.x del PIX/ASA.

prerrequisitos

Requisitos

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.

- Cisco IOS Software Release12.0.7.T [hasta pero no incluyendo 12.2(13)T]Refiera a la Transparencia IPSec NAT para más versiones recientes.
- Cisco 2621 Router que funciona con el Cisco IOS Software Release 12.4
- Cisco 3660 Router que funciona con el Cisco IOS Software Release 12.4
- Cisco PIX Firewall que ejecuta 6.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.

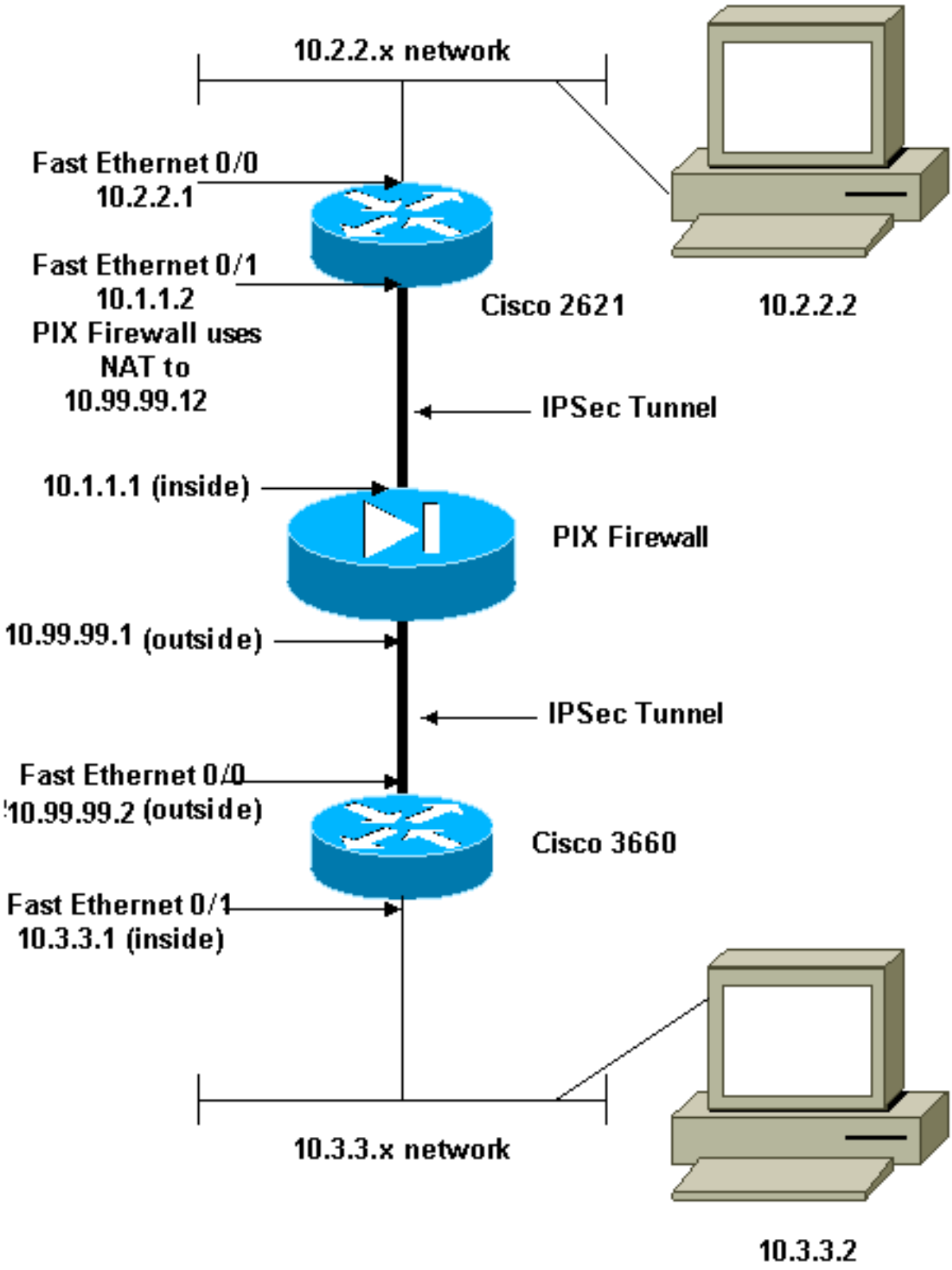
Configurar

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

Nota: Use la herramienta Command Lookup Tool (clientes registrados solamente) para encontrar más información sobre los comandos usados en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Éstos son los direccionamientos del RFC 1918 que se han utilizado en un ambiente de laboratorio.

Configuraciones

En este documento, se utilizan estas configuraciones:

- Configuración de Cisco 2621
- Configuración parcial del 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 del 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 del **fixup protocol ESP-IKE** se inhabilita por abandono. Si se publica un comando del **fixup protocol ESP-IKE**, se gira el fixup, y el firewall PIX preserva el puerto de origen del Internet Key Exchange (IKE). También crea una traducción de la PALMADITA para el tráfico ESP. Además, si el fixup ESP-IKE está prendido, el Internet Security Association and Key Management Protocol (ISAKMP) no se puede 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.
- **active del show crypto engine connections** — Utilice para ver los paquetes encriptados y desencriptados.

Troubleshooting

Use esta sección para resolver problemas de configuración.

Comandos para resolución de problemas

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- debug crypto engine — muestra el tráfico codificado.
- **IPSec del debug crypto** — Utilice para ver los IPSec Negotiations de la fase 2.
- **isakmp del debug crypto** — Utilice para ver negociaciones ISAKMP de la fase 1.

Verificación de las asociaciones de seguridad

- **borre el isakmp crypto** — Asociaciones de seguridad de los claros 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
- Request For Comments (RFC)
- Soporte Técnico y Documentación - Cisco Systems