PIX 6.x: IPSec dinámico entre un firewall PIX estáticamente dirigido y el router IOS dinámicamente dirigido con el ejemplo de la configuración del NAT

Contenido

Introducción

Este documento proporciona una configuración de muestra para que cómo permita al PIX para validar las conexiones dinámicas del IPSec. El router remoto realiza la Traducción de Dirección de Red (NAT) si la red privada 10.1.1.x tiene acceso a Internet. El tráfico de 10.1.1.x a la red privada 192.168.1.x detrás del PIX se excluye del proceso NAT. El router puede iniciar conexiones al PIX pero el PIX no puede iniciar conexiones al router.

Esta configuración utiliza un firewall PIX para crear los túneles dinámicos del LAN a LAN del IPSec (L2L) con un router de Cisco IOS® que reciba los IP Address dinámicos en su interfaz pública (interfaz exterior). El Protocolo de configuración dinámica de host (DHCP) proporciona un mecanismo para afectar un aparato los IP Addresses dinámicamente del proveedor de servicio (ISP). Esto permite que los IP Addresses sean reutilizados cuando los host los necesitan no más.

Refiera al Router-a-PIX IPSec dinámico a estático con el ejemplo de la configuración del NAT para más información sobre un escenario donde el router valida las conexiones dinámicas del IPSec de un dispositivo de seguridad PIX que ejecute 6.x.

Refiera al IPSec entre un router IOS estático y un PIX/ASA dinámico 7.x con el ejemplo de la configuración del NAT para permitir al dispositivo de seguridad del PIX/ASA para validar las conexiones dinámicas del IPSec del router del Cisco IOS.

Refiera al IPSec entre un PIX/ASA estático 7.x y un router IOS dinámico con el ejemplo de la configuración del NAT para aprender un escenario más casi igual donde el dispositivo de seguridad del PIX/ASA funciona con la versión de software 7.x y posterior.

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 Release 12.4
- Versión de Software Cisco PIX Firewall 6.3.1
- Cisco Secure PIX Firewall 515E
- Cisco 7206 Router

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.

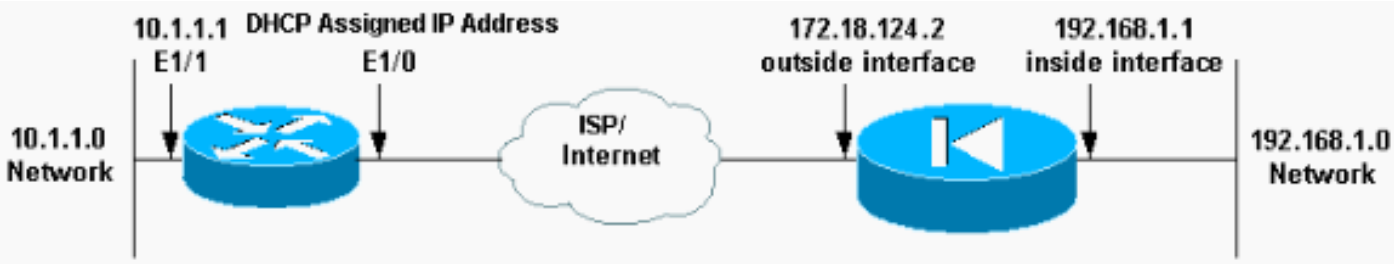
Configurar

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

Este documento utiliza esta configuración de red:



Configuraciones

Este documento usa estas configuraciones.

- Duende (PIX)
- Fregona (Cisco 7204 Router)

Duende (PIX)

```
Building configuration...
: Saved
:
PIX Version 6.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname elf
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!--- Access control list (ACL) to avoid NAT on the IPsec
packets. access-list nonat permit ip 192.168.1.0
255.255.255.0 10.1.1.0 255.255.255.0
pager lines 24
logging on
logging buffered debugging
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
mtu outside 1500
mtu inside 1500
mtu intf2 1500
ip address outside 172.18.124.2 255.255.255.0
ip address inside 192.168.1.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address intf2 0.0.0.0
pdm history enable
arp timeout 14400
global (outside) 1 interface
!-- Binds ACL nonat to the NAT statement to avoid NAT on
the IPsec packets nat (inside) 0 access-list nonat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
!--- Permits Internet Control Message Protocol (ICMP)
traffic for testing. !--- Do not enable it in a live
network. conduit permit icmp any any
route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
```

```
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00
h323 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol tacacs+
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
!--- IPsec configuration crypto ipsec transform-set
router-set esp-des esp-md5-hmac
crypto dynamic-map cisco 1 set transform-set router-set
crypto map dyn-map 10 ipsec-isakmp dynamic cisco
crypto map dyn-map interface outside
isakmp enable outside
!--- Internet Security Association and Key Management
Protocol (ISAKMP) !--- policy for accepting dynamic
connections from remote PIX. !--- Note: In real show run
output, the pre-shared key appears as *******. isakmp
key cisco123 address 0.0.0.0 netmask 0.0.0.0
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:eeb67d5df47045f7e6ac4aa090aab683
: end
[OK]
elf#
```

Fregona (Cisco 7204 Router)

```
mop#show running-configuration
Building configuration...

Current configuration : 1916 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mop
!
!
ip subnet-zero
!
!
no ip domain-lookup
!
ip cef
ip audit notify log
ip audit po max-events 100
!
!--- Internet Key Exchange (IKE) policies crypto isakmp
policy 1
```

```
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 172.18.124.2
!
!
!--- IPsec policies crypto ipsec transform-set pix-set
esp-des esp-md5-hmac
!
crypto map pix 10 ipsec-isakmp
 set peer 172.18.124.2
 set transform-set pix-set
 match address 101
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/0
ip address dhcp
ip nat outside
duplex half
crypto map pix
!
interface Ethernet1/1
ip address 10.1.1.1 255.255.255.0
ip nat inside
duplex half
!
!--- Except the private network from the NAT process. ip
nat inside source route-map nonat interface Ethernet1/0
overload
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet1/0
no ip http server
ip pim bidir-enable
!
!--- Include the private-network-to-private-network !---
traffic in the encryption process. access-list 101
permit ip 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255
!--- Except the private network from the NAT process.
access-list 110 deny ip 10.1.1.0 0.0.0.255 192.168.1.0
0.0.0.255
access-list 110 permit ip 10.1.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
!
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.

Usted puede funcionar con estos **comandos show** en el PIX y en el router.

- show crypto isakmp sa: muestra todas las asociaciones actuales de seguridad IKE (SA) de un par.
- **muestre IPSec crypto sa** — Muestra las configuraciones usadas por (IPSec) los SA actuales.
- **active del show crypto engine connections** — Conexiones actuales e información de las demostraciones con respecto a los paquetes encriptados y desencriptados (router solamente).

Debe verificar las asociaciones de seguridad en ambos pares.

- Realizan a los comandos pix en el modo de configuración.**clear crypto isakmp sa** : borra las SA de la fase 1.**clear crypto ipsec sa** — Borra la fase 2 SA.
- Realizan a los comandos router en el enable mode.**borre el isakmp crypto** — Borra la fase 1 SA.**borre el sa crypto** — Borra la fase 2 SA.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

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.

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

- **show crypto isakmp sa** — Muestra todas las IKE SAs actuales en un par.
- **muestre IPSec crypto sa** — Muestra las configuraciones usadas por (IPSec) los SA actuales.
- **active del show crypto engine connections** — Conexiones actuales e información de las demostraciones con respecto a los paquetes encriptados y desencriptados (router solamente).

Información Relacionada

- Página de Soporte de IPSec Negotiation/IKE Protocols
- Dispositivos de seguridad de la serie PIX 500
- Referencias de Comandos de Cisco Secure PIX Firewall
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems