

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

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshooting](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

Introducción

Este documento proporciona una configuración de muestra que le muestre cómo permitir al router IOS® para validar las conexiones dinámicas del IPSec de un firewall PIX. El router remoto realiza el Network Address Translation (NAT) si la red privada 10.0.0.x accede Internet. El tráfico de 10.0.0.x a la red privada 10.1.0.x detrás del PIX se excluye del proceso NAT. El firewall PIX puede iniciar las conexiones al router, pero el router no puede iniciar las conexiones al PIX.

Esta configuración utiliza a un router del Cisco IOS para crear los túneles dinámicos del LAN a LAN del IPSec (L2L) con un firewall PIX 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 servicios de Internet (ISP). Esto permite que los IP Addresses sean reutilizados cuando los host los necesitan no más.

Refiera a [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](#) para más información sobre el escenario donde el PIX valida las conexiones dinámicas del IPSec del router.

Refiera al [PIX/ASA 7.x y posterior: IPSec dinámico entre un PIX estáticamente dirigido y un router IOS dinámicamente dirigido 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 IOS.

Refiera al [PIX/ASA 7.x y posterior: IPsec dinámico entre un router IOS estáticamente dirigido y un PIX dinámicamente dirigido 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.

- Versión 12.4 del Cisco IOS ® Software
- Versión de Software Cisco PIX Firewall 6.3.4
- Cisco Secure PIX Firewall 515E
- Cisco 2811 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](#)

En este documento, se utiliza esta configuración de red:

[Configuraciones](#)

En este documento, se utilizan estas configuraciones:

- [PIX 515E](#)
- [R2 \(Cisco 2811 Router\)](#)

PIX 515E

```
PIX Version 6.3(4)
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 shut
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX515E
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
names

!--- The access control list (ACL) to avoid NAT on the
IPsec packets. access-list NO-NAT permit ip 10.1.0.0
255.255.255.0 10.0.0.0 255.255.255.0
!--- The ACL to apply on crypto map. !--- Include the
private-network-to-private-network traffic !--- in the
encryption process. access-list 101 permit ip 10.1.0.0
255.255.255.0 10.0.0.0 255.255.255.0
pager lines 24
logging on
mtu outside 1500
mtu inside 1500
mtu intf2 1500
!--- ISP will providthe the Outside IP address.
ip address outside dhcp

ip address inside 10.1.0.3 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list NO-NAT
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 10.0.0.0 255.255.255.0 172.16.1.5 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 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 TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec

!--- IPsec configuration, Phase 2. crypto ipsec
transform-set DYN-TS esp-des esp-md5-hmac
crypto map IPSEC 10 ipsec-isakmp
crypto map IPSEC 10 match address 101
crypto map IPSEC 10 set peer 10.95.49.1
crypto map IPSEC 10 set transform-set DYN-TS
crypto map IPSEC interface outside
!--- Internet Security Association and Key Management
Protocol (ISAKMP) !--- policy, Phase 1. !--- Note: In
real show run output, the pre-shared key appears as
*****.

isakmp enable outside
isakmp key cisco123 address 10.95.49.1 netmask
255.255.255.255
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
console timeout 0
terminal width 80
Cryptochecksum:f0294298e214a947fc2e03f173e4a405
: end
```

R2 (Cisco 2811 Router)

```
R2#show running-configuration
Building configuration...

Current configuration : 1916 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname r1800
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
```

```
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
!
no ip dhcp use vrf connected
!
!
no ip ips deny-action ips-interface
!
no ftp-server write-enable
!
!
!--- ISAKMP policy, Phase 1. crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key 6 cisco123 address 0.0.0.0 0.0.0.0
!
!
!--- IPsec policy, Phase 2. crypto ipsec transform-set
DYN-TS esp-des esp-md5-hmac
!
crypto dynamic-map DYN 10
set transform-set DYN-TS
match address 101
!
!
crypto map IPSEC 10 ipsec-isakmp dynamic DYN
!
!
!
interface FastEthernet0/0
ip address 10.95.49.1 255.255.255.0
ip nat outside
ip virtual-reassembly
load-interval 30
duplex auto
speed auto
crypto map IPSEC
!
interface FastEthernet0/1
ip address 10.0.0.1 255.255.255.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
!
ip classless
ip route 10.1.0.0 255.255.255.0 10.95.49.2
!
ip http server
no ip http secure-server
!--- Except the private network from the NAT process. ip
nat inside source list 102 interface FastEthernet0/0
overload
!
!--- Include the private-network-to-private-network !---
traffic in the encryption process. access-list 101
permit ip 10.0.0.0 0.0.0.255 10.1.0.0 0.0.0.255

!--- Except the private network from the NAT process.
access-list 102 deny ip 10.0.0.0 0.0.0.255 10.1.0.0
0.0.0.255
```

```
access-list 102 permit ip 10.0.0.0 0.0.0.255 any
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
exec-timeout 0 0
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.

- **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.

Realice estos 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.

Realice estos 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

Use esta sección para resolver 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**.

- **muestre isakmp crypto sa** — Vea todo el IKE actual SA 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

- [Soluciones a los Problemas más frecuentes de IPSec VPN L2L y de Acceso Remoto](#)
- [Cisco PIX Firewall Software](#)
- [Referencias de Comandos de Cisco Secure PIX Firewall](#)
- [Avisos de campos de productos de seguridad \(incluido PIX\)](#)
- [Solicitudes de Comentarios \(RFC\)](#)
- [Negociación IPSec/Protocolos IKE](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)