PIX 6.x: Dynamische IPsec tussen een PIX-firewall die automatisch wordt aangepakt en de dynamisch benaderde IOS-router met NAT-configuratievoorbeeld

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor de manier waarop de PIX dynamische IPsec-verbindingen kan accepteren. De router op afstand voert Netwerkadresomzetting (NAT) uit indien er een privé-netwerk met 10.1.1.x toegang tot het internet heeft. Verkeer van 10.1.1.x naar privaat netwerk 192.168.1.x achter de PIX wordt van het NAT-proces uitgesloten. De router kan verbindingen aan PIX in werking stellen, maar PIX kan geen verbindingen aan de router in werking stellen.

Deze configuratie gebruikt een PIX-firewall om dynamische IPsec LAN-to-LAN (L2L) tunnels te maken met een Cisco IOS® router die dynamische IP-adressen ontvangt op hun openbare interface (externe interface). Dynamic Host Configuration Protocol (DHCP) biedt een mechanisme om IP-adressen dynamisch van de Service provider (ISP) toe te wijzen. Dit staat IP adressen toe om opnieuw te worden gebruikt wanneer de hosts deze niet langer nodig hebben.

Raadpleeg Router-to-PIX Dynamic-to-Static IPsec met NAT Configuration Voorbeeld voor meer informatie over een scenario waarin de router dynamische IPsec-verbindingen accepteert van een PIX security applicatie die 6.x draait.

Raadpleeg IPsec tussen een statische IOS-router en een Dynamic PIX/ASA 7.x met NAT-configuratievoorbeeld om de PIX/ASA security applicatie in staat te stellen om dynamische IPsec-verbindingen van de Cisco IOS-router te accepteren.

Raadpleeg IPsec tussen een statische PIX/ASA 7.x en een dynamische IOS-router met NAT-configuratievoorbeeld om meer te weten te komen over hetzelfde scenario waarin PIX/ASA security applicatie softwareversie 7.x en hoger uitvoert.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS-softwarerelease 12.4
- Cisco PIX-firewall-softwarerelease 6.3.1
- Cisco Secure PIX-firewall 5155E
- Cisco 7206 router

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

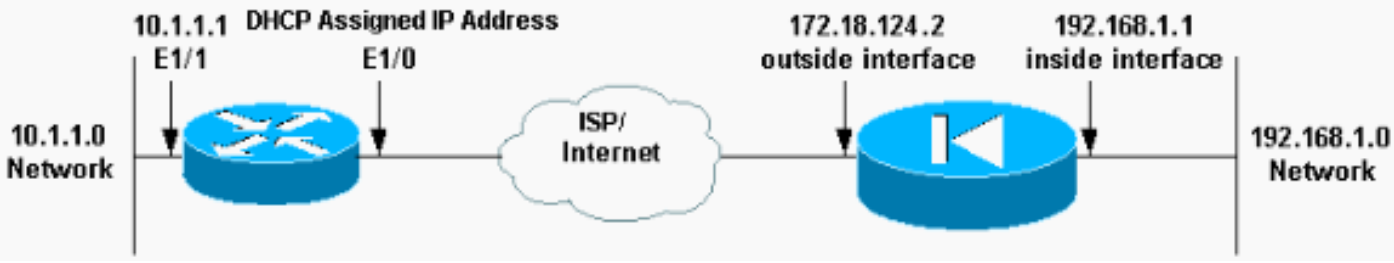
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

N.B.: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Netwerkdiagram

Dit document maakt gebruik van deze netwerkinstellingen.



Configuraties

Dit document gebruikt deze configuraties.

- Elf (PIX)
- Mop (Cisco 7204 router)

Elf (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#
```

Mop (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
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

U kunt deze **show** opdrachten op PIX en op de router uitvoeren.

- **toon crypto isakmp sa**-Toont alle huidige IKE security associaties (SAs) bij een peer.
- **toon crypto ipsec sa**-Toont de instellingen die worden gebruikt door huidige (IPsec) SA's.
- **tonen de crypto motor verbindingen actief**-toont huidige verbindingen en informatie betreffende gecodeerde en gedecrypteerde pakketten (slechts router).

Je moet SA's op beide peers ontruimen.

- De opdrachten PIX worden in de configuratie-modus uitgevoerd.**duidelijke crypto isakmp sa** — ontslaat de fase 1 SA's.**duidelijke crypto ipsec sa** — ontslaat de fase 2 SA's.
- De routeropdrachten worden in modus voor toegangsrechten uitgevoerd.**duidelijke crypto isakmp** - ontruimt de fase 1 SA's.**duidelijke crypto sa** — ontruimt de fase 2 SA's.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opdrachten voor probleemoplossing

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

- **toon crypto isakmp sa**-toont alle huidige IKE SAs bij een peer.
- **toon crypto ipsec sa**-Toont de instellingen die worden gebruikt door huidige (IPsec) SA's.
- **tonen de crypto motor verbindingen actief**-toont huidige verbindingen en informatie betreffende gecodeerde en gedecrypteerde pakketten (slechts router).

Gerelateerde informatie

- Ondersteuning van IPsec-onderhandeling/IKE-protocollen
- PIX 500 Series security applicaties
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems