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

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie die aangeeft hoe u de IOS® router in staat kunt stellen om dynamische IPsec-verbindingen van een PIX-firewall te aanvaarden. De router op afstand voert Netwerkadresomzetting (NAT) uit indien er een privé-netwerk met 10.0.0.x toegang tot het internet heeft. Het verkeer van 10.0.0.x naar privaat netwerk 10.1.0.x achter de PIX wordt van het NAT-proces uitgesloten. De PIX-firewall kan verbindingen naar de router openen, maar de router kan geen verbindingen naar PIX openen.

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

Raadpleeg PIX 6.x: Dynamische IPsec tussen een Static Adressated PIX Firewall en de Dynamisch Adresseerbare IOS-router met NAT Configuration Voorbeeld voor meer informatie over het scenario waarin PIX dynamische IPsec-verbindingen van de router accepteert.

Raadpleeg PIX/ASA 7.x en hoger: Dynamische IPsec tussen een Static Adpressed PIX en een Dynamisch Geadresseerde IOS-router met NAT Configuration Voorbeeld om de PIX/ASA security applicatie in staat te stellen om dynamische IPsec-verbindingen van de IOS-router te accepteren.

Raadpleeg PIX/ASA 7.x en hoger: Dynamische IPsec tussen een automatisch geadresseerde IOS-router en een dynamisch geadresseerde PIX met NAT-configuratievoorbeeld om meer te weten te komen over hetzelfde scenario waarin de 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 6.3.4
- Cisco Secure PIX-firewall 5155E
- Cisco 2811 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.

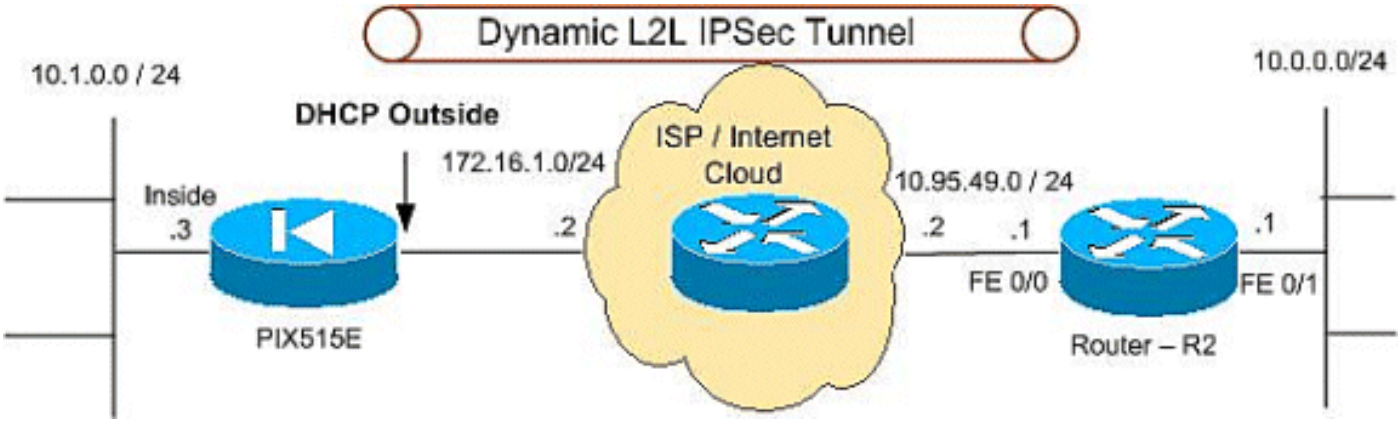
Configureren

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

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt deze configuraties:

- 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
```

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.

- **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.

Voer deze PIX-opdrachten in configuratie-modus uit.

- **duidelijke crypto isakmp sa** — ontslaat de fase 1 SA's.
- **duidelijke crypto ipsec sa** — ontslaat de fase 2 SA's.

Voer deze routeropdrachten in om de modus te activeren.

- **duidelijke crypto isakmp** - ontruimt de fase 1 SA's.
- **duidelijke crypto sa** — ontruimt de fase 2 SA's.

Problemen oplossen

Gebruik dit gedeelte om de configuratie van het probleem op te lossen.

Opdrachten voor troubleshooting

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**—Bekijk 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

- Meest gebruikelijke L2L- en IPSec VPN-oplossingen voor probleemoplossing
- Cisco PIX-firewallsoftware
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Verzoeken om opmerkingen (RFC's)
- IPsec-onderhandeling/IKE-protocollen