PIX 6.x: IPsec-tunneldoorgifte via een PIX-firewall met toegangslijst en NAT-configuratiemodel

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor een IPSec-tunnel door een firewall die netwerkadresomzetting (NAT) uitvoert. **Deze configuratie werkt niet met poortadresomzetting (PAT) als u Cisco IOS®-softwarereleases gebruikt vóór en zonder 12.2(13)T.** Deze configuratie kan worden gebruikt voor tunnelverkeer van IP. Dit kan niet worden gebruikt om verkeer te versleutelen dat niet door een firewall gaat, zoals IPX of routingupdates. Generic Routing Encapsulation (GRE) tunneling is geschikt voor dat soort configuratie. In het voorbeeld in dit document, zijn Cisco 2621 en 3660 routers de IPSec-tunnelendpoints die zich bij twee particuliere netwerken aansluiten, met circuits of toegangscontrolelijsten (ACL's) op de PIX-ingang om het IPSec-verkeer toe te staan.

Opmerking: NAT is een één-op-één adresvertaling, niet om te worden verward met PAT, wat een groot aantal (binnen de firewall) is-op-één vertaling. Raadpleeg Bediening van NAT en fundamentele NAT-probleemoplossing of hoe NAT werkt voor meer informatie over de werking en configuratie van NAT.

Opmerking: IPSec met PAT werkt mogelijk niet goed omdat het apparaat voor buitentunneleindpunt geen meerdere tunnels van één IP-adres kan verwerken. U moet contact opnemen met uw verkoper om te bepalen of de tunneleindapparatuur met PAT werkt. Bovendien kan in versies 12.2(13)T en later de NAT Transparency-functie ook worden gebruikt voor PAT. Raadpleeg IPSec NAT Transparency voor meer informatie. Raadpleeg Ondersteuning voor IPSec ESP via NAT voor meer informatie over deze functies in versies 12.2(13)T en hoger. Raadpleeg

ook, voordat u een case met TAC opent, NAT vaak gestelde vragen, die veel antwoorden op gebruikelijke vragen bevat.

Raadpleeg IPsec-tunneldoorloop door een security applicatie met gebruik van toegangslijst en MPF met NAT-configuratievoorbeeld voor meer informatie over het configureren van een IPSec-tunnel door een firewall met NAT in PIX/ASA versie 7.x.

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 12.0.7.T [tot en met 12.2(13)T]Raadpleeg IPSec NAT Transparency voor meer recente versies.
- Cisco 2621 router die Cisco IOS-softwarerelease 12.4 draait
- Cisco 3660 router die Cisco IOS-softwarerelease 12.4 draait
- Cisco PIX-firewall met 6.x

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.

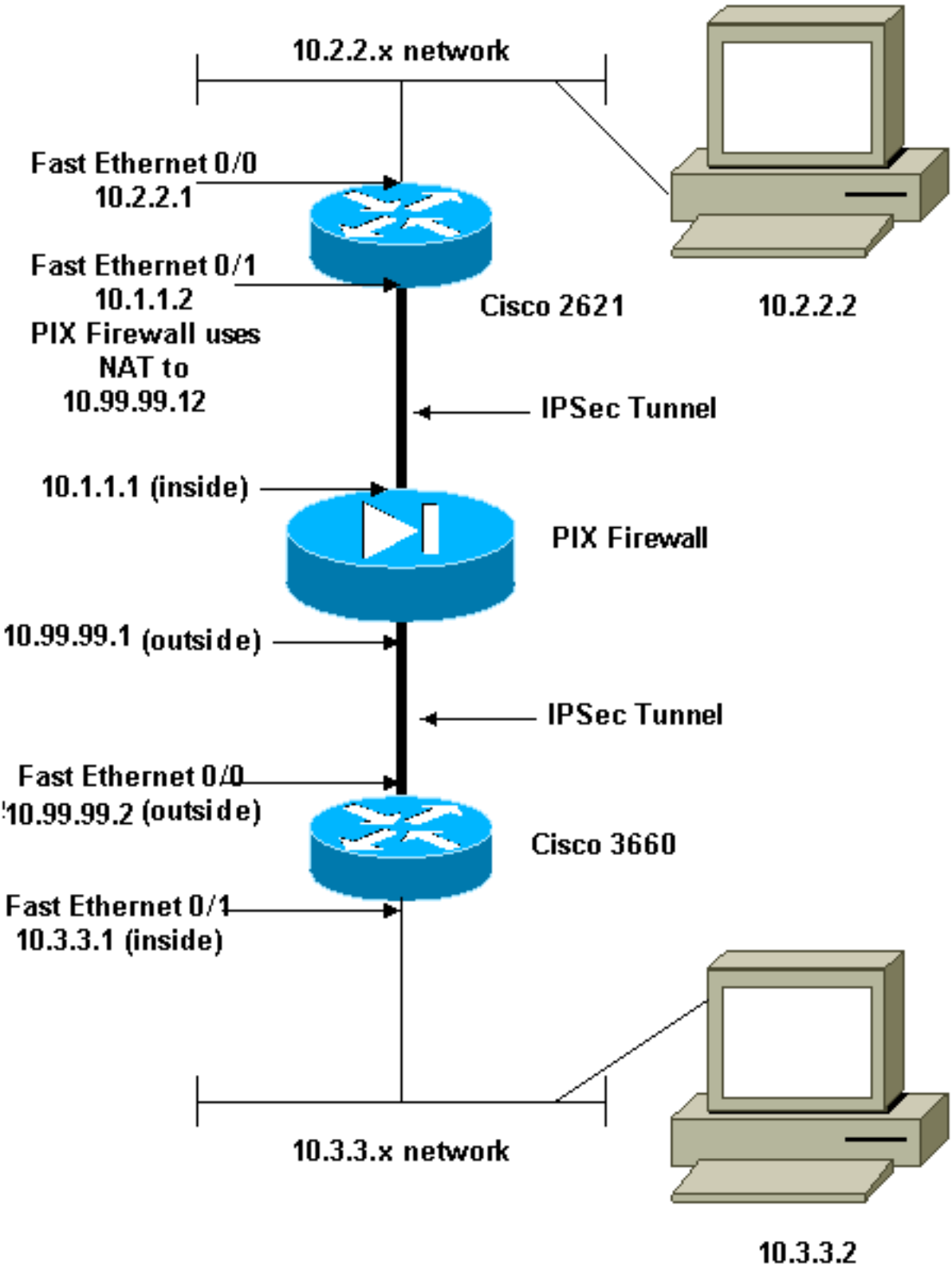
Configureren

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:



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Dit zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

Configuraties

Dit document gebruikt deze configuraties:

- Cisco 2621-configuratie
- Cisco PIX-firewallconfiguratie

- Cisco 3660-configuratie

Cisco 2621-configuratie

```
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
```

Cisco PIX-firewallconfiguratie

```
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
```

Opmerking: de opdracht Sp-**achtige** vaste **protocol** is standaard uitgeschakeld. Als een **fixup protocol esp-achtige** opdracht wordt afgegeven, wordt de fixup ingeschakeld en de PIX-firewall behoudt de bronpoort van de Internet Key Exchange (IKE). Er wordt ook een PAT-vertaling voor ESP-verkeer gemaakt. Als de evp-vormige fixup actief is, kunnen bovendien de Internet Security Association en Key Management Protocol (ISAKMP) niet op een willekeurige interface worden ingeschakeld.

Cisco 3660-configuratie

```
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
```

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 ipsec sa**-shows the fase 2 security associaties.
- **toon crypto isakmp sa** - toont de fase 1 veiligheidsassociaties.
- **Laat de crypto motor verbindingen actief**-Gebruik zien om de gecodeerde en gedecrypteerde pakketten te zien.

Problemen oplossen

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

Opdrachten voor troubleshooting

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

- **debug crypto motor** - toont het verkeer dat wordt versleuteld.
- **debug van crypto ipsec**: gebruik om de IPSec-onderhandelingen van fase 2 te zien.
- **debug van crypto isakmp** - gebruik om de ISAKMP-onderhandelingen van fase 1 te zien.

Security associaties reinigen

- **duidelijke crypto isakmp** - ontruimt de IKE veiligheidsassociaties.
- **duidelijke crypto ipsec sa**-Clears IPSec security associaties.

Gerelateerde informatie

- Cisco PIX 500 Series security applicaties
- Opdrachtreferenties van Cisco Secure PIX-firewall
- NAT-ondersteuningspagina
- Verzoek om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems