PIX: Toegang tot de PDM via een externe interface via een VPN-tunnel

Inhoud

Inleiding

Deze voorbeeldconfiguratie documenteert hoe u een LAN-to-LAN VPN-tunnel kunt configureren met behulp van twee PIX-firewalls. PIX Devices Manager (PDM) loopt op de externe PIX-verbinding via de externe interface aan de openbare zijde en versleutelt zowel het reguliere netwerk als het PDM-verkeer.

PDM is een op een browser gebaseerd configuratiegereedschap dat u moet helpen om uw PIX-firewall met een GUI in te stellen, te configureren en te bewaken. U hebt geen uitgebreide kennis nodig van de PIX Firewall opdrachtregel interface (CLI).

Voorwaarden

Vereisten

Dit document vereist een basisbegrip van IPsec-encryptie en PDM.

Zorg ervoor dat alle apparaten die in uw topologie worden gebruikt, voldoen aan de vereisten die in Cisco PIX Firewall Installatie Guide, versie 6.3 worden beschreven.

Gebruikte componenten

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

- Cisco PIX-firewall-softwarerelease 6.3(1)en 6.3(3)
- PIX A en PIX B zijn Cisco PIX-firewall 515E
- PIX B gebruikt PDM versie 2.1(1)**Opmerking:** PDM 3.0 werkt niet met PIX-firewallsoftwareversies eerder dan versie 6.3. PDM versie 3.0 is één afbeelding die alleen PIX-firewall versie 6.3 ondersteunt.**Opmerking:** Policy NAT-configuraties force PDM 3.0 in monitormodus. Policy NAT wordt ondersteund in PDM versie 4.0 en hoger.**Opmerking:** Wanneer u wordt gevraagd om een gebruikersnaam en wachtwoord voor PIX Apparaatbeheer (PDM), vereisen de standaardinstellingen geen gebruikersnaam. Als u een wachtwoord invoert dat eerder is ingesteld, voert u dat wachtwoord in als het PDM-wachtwoord. Als er geen wachtwoord wordt ingeschakeld, laat u zowel de gebruikersnaam als de wachtwoordinvoer leeg en klikt u op **OK** om door te gaan.

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.

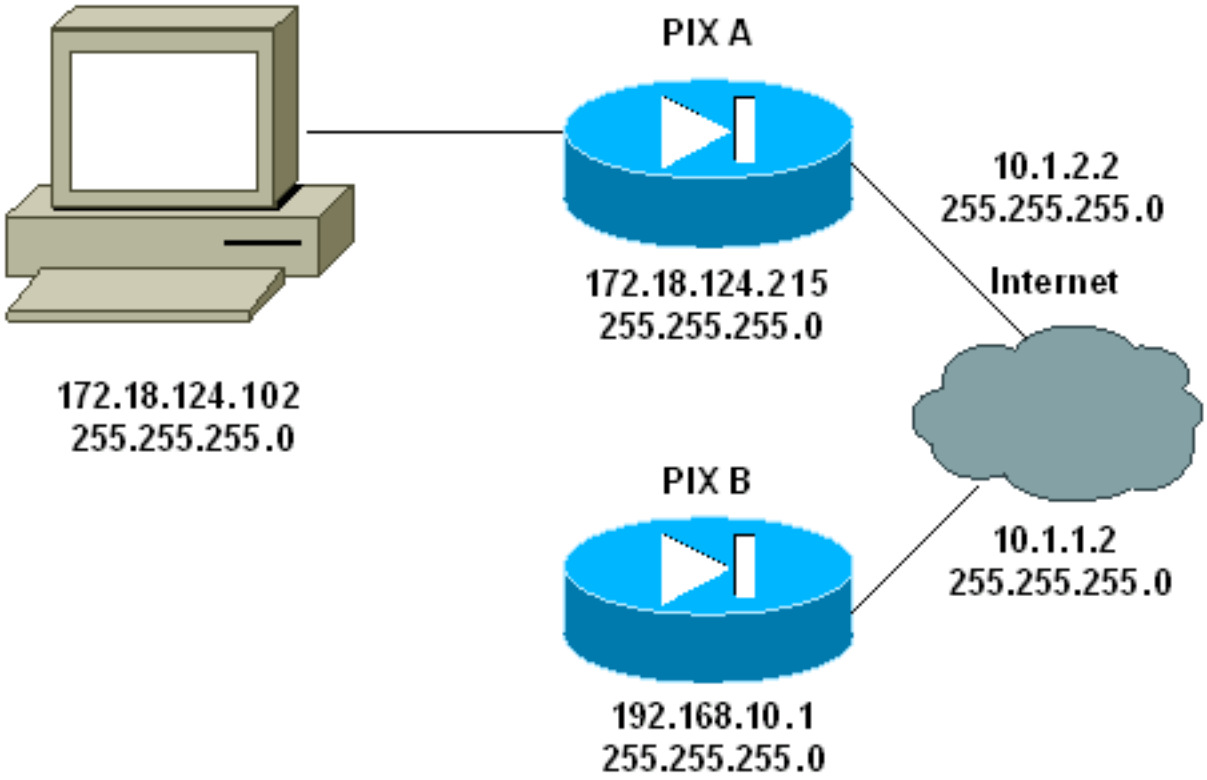
Configureren

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

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt deze configuraties:

- PIX A
- PIX B

PIX A

```
PIX A

PIX Version 6.3(3)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIXA
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!--- Allow traffic from the host PC that is going to !--
- run the PDM to the outside interface of PIX B. access-
list 101 permit ip host 172.18.124.102 host 10.1.1.2
!--- Allow traffic from the private network behind PIX A
!--- to access the private network behind PIX B. access-
list 101 permit ip 172.18.124.0 255.255.255.0
192.168.10.0 255.255.255.0
```

```
pager lines 24
interface ethernet0 10baset
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside 10.1.2.2 255.255.255.0
ip address inside 172.18.124.215 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
!--- Do not use NAT !--- on traffic which matches access
control list (ACL) 101. nat (inside) 0 access-list 101
!--- Configures a default route towards the gateway
router. route outside 0.0.0.0 0.0.0.0 10.1.2.1 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
!--- Enable the HTTP server required to run PDM. http
server enable
!--- This is the interface name and IP address of the
host or !--- network that initiates the HTTP connection.
http 172.18.124.102 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- Implicitly permit any packet that came from an
IPsec !--- tunnel and bypass the checking of an
associated access-list, conduit, or !--- access-group
command statement for IPsec connections. sysopt
connection permit-ipsec
!--- Specify IPsec (phase 2) transform set. crypto ipsec
transform-set vpn esp-3des esp-md5-hmac
!--- Specify IPsec (phase 2) attributes. crypto map vpn
10 ipsec-isakmp
crypto map vpn 10 match address 101
crypto map vpn 10 set peer 10.1.1.2
crypto map vpn 10 set transform-set vpn
crypto map vpn interface outside
!--- Specify ISAKMP (phase 1) attributes. isakmp enable
outside
isakmp key ******** address 10.1.1.2 netmask
255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
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:24e43efa87d6ef07dfabe097b82b5b40
: end
[OK]
PIXA(config)#
```

PIX B

```
PIX B
PIX Version 6.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIXB
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80P
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!--- Allow traffic from the host PC that is going to !--
- run the PDM to the outside interface of PIX B. access-
list 101 permit ip host 10.1.1.2 host 172.18.124.102
!--- Allow traffic from the private network behind PIX A
!--- to access the private network behind PIX B. access-
list 101 permit ip 192.168.10.0 255.255.255.0
172.18.124.0 255.255.255.0
pager lines 24
interface ethernet0 10baset
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside 10.1.1.2 255.255.255.0
ip address inside 192.168.10.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
!--- Assists PDM with network topology discovery by
associating an external !--- network object with an
interface. Note: The pdm location !--- command does not
control which host can launch PDM.

pdm location 172.18.124.102 255.255.255.255 outside
pdm history enable
arp timeout 14400
!--- Do not use NAT on traffic which matches ACL 101.
nat (inside) 0 access-list 101
!--- Configures a default route towards the gateway
router. route outside 0.0.0.0 0.0.0.0 10.1.1.1 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
!--- Enables the HTTP server required to run PDM. http
server enable
!--- This is the interface name and IP address of the
host or !--- network that initiates the HTTP connection.
http 172.18.124.102 255.255.255.255 outside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
```

```
!--- Implicitly permit any packet that came from an
IPsec !--- tunnel and bypass the checking of an
associated access-list, conduit, or !--- access-group
command statement for IPsec connections. sysopt
connection permit-ipsec
!--- Specify IPsec (phase 2) transform set. crypto ipsec
transform-set vpn esp-3des esp-md5-hmac
!--- Specify IPsec (phase 2) attributes. crypto map vpn
10 ipsec-isakmp
crypto map vpn 10 match address 101
crypto map vpn 10 set peer 10.1.2.2
crypto map vpn 10 set transform-set vpn
crypto map vpn interface outside
isakmp enable outside
!--- Specify ISAKMP (phase 1) attributes. isakmp key
******** address 10.1.2.2 netmask 255.255.255.255
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
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:d5ba4da0d610d0c6140e1b781abef9d0
: end
[OK]
PIXB(config)#
```

Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw 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/show isakmp sa —verifieert die fase 1.
- toon crypto ipsec sa—verifieert die fase 2.
- toont crypto motor —Hiermee geeft u gebruiksstatistieken weer voor de cryptografiemotor die de firewall gebruikt.

Overzicht van opdrachten

Wanneer VPN-opdrachten in de PIX-bestanden zijn geplaatst, moet een VPN-tunnel zich realiseren wanneer het verkeer tussen de PDM-pc (17.2.18.124.102) en de externe interface van PIX B (10.1.1.2) passeert. Op dit punt kan de PDM PC naar https://10.1.1.2 gaan en de PDM interface van PIX B via de VPN-tunnel bereiken.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen. Raadpleeg PIX-apparaatbeheer voor probleemoplossing bij problemen met PDM.

Voorbeeld van output van foutopsporing

toon crypto isakmp sa

Deze uitvoer toont een tunnel die wordt gevormd tussen 10.1.1.2 en 10.1.2.2.

```
PIXA#show crypto isakmp sa
Total     : 1
Embryonic : 0
        dst         src         state     pending    created
        10.1.1.2    10.1.2.2    QM_IDLE         0           1
```

show crypto ipsec sa

Deze output toont een tunnel die verkeer doorgeeft tussen 10.1.1.2 en 172.18.124.102.

```
PIXA#show crypto ipsec sa

interface: outside
    Crypto map tag: vpn, local addr. 10.1.2.2

   local  ident (addr/mask/prot/port): (172.18.124.102/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.2/255.255.255.255/0/0)
   current_peer: 10.1.1.2
>     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 14472, #pkts encrypt: 14472, #pkts digest 14472
    #pkts decaps: 16931, #pkts decrypt: 16931, #pkts verify 16931
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 9, #recv errors 0

     local crypto endpt.: 10.1.2.2, remote crypto endpt.: 10.1.1.2
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 4acd5c2a

     inbound esp sas:
      spi: 0xcff9696a(3489229162)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (4600238/15069)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x4acd5c2a(1254972458)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 1, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (4607562/15069)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:
```

```
outbound pcp sas:
```

Gerelateerde informatie

- PIX-opdracht
- Cisco PIX 500 Series security applicaties
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems