PIX/ASA 7.x: Multicast voor de PIX-/ASA-platforms met scheidingstekens bij buitenste configuratievoorbeeld

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor multicast op Cisco adaptieve security applicatie (ASA) en/of PIX-security applicatie die versie 7.x uitvoert. In dit voorbeeld, is de multicast zender aan de buitenkant van het veiligheidsapparaat en hosts aan de binnenkant proberen het multicast verkeer te ontvangen. De hosts verzenden IGMP-rapporten om groepslidmaatschap te rapporteren, en de firewall gebruikt Protocol Independent Multicast (PIM) in duale modus als het dynamische multicast routingprotocol naar de upstream router, waarachter de bron van de stream zich bevindt.

Opmerking: FWSM/ASA biedt geen ondersteuning voor 232.x.x.x/8 als groepsnummer, aangezien het gereserveerd is voor ASA SSM. Dus FWSM/ASA staat niet toe dit te gebruiken of te verplaatsen en route wordt niet gecreëerd. Maar je kunt dit multicast verkeer nog steeds doorgeven door ASA/FWSM als je het inkapselt in GRE-tunnel.

Voorwaarden

Vereisten

Een Cisco PIX- of ASA security applicatie die softwareversie 7.0, 7.1 of 7.2 uitvoert.

Gebruikte componenten

De informatie in dit document is gebaseerd op een Cisco PIX- of Cisco ASA-firewall van versie 7.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 de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

PIX/ASA 7.x introduceert volledige PIM sparse mode en bi-directionele ondersteuning voor dynamische multicast routing door de firewall. De PIM Dense Mode wordt niet ondersteund. De 7.x-software ondersteunt nog steeds legacy multicast 'stub-mode' waarin de firewall simpelweg een IGMP-proxy tussen interfaces is, zoals werd ondersteund in PIX versie 6.x.

Deze verklaringen gelden waar voor multicast verkeer door de firewall:

- Als een toegangslijst op de interface wordt toegepast waar het multicast verkeer wordt ontvangen, moet de toegangscontrolelijst (ACL) het verkeer expliciet toestaan. Als geen toegang-lijst op de interface wordt toegepast, is de expliciete ACL ingang die het multicast verkeer toelaat niet noodzakelijk.
- De multicast gegevenspakketten worden altijd onderworpen aan de controle van het doorsturen van het pad van de firewall, ongeacht of de opdracht **reverse-pad voorwaartse** controle op de interface is ingesteld. Als er daarom geen route op de interface is die het pakje op de bron van het multicast-pakket is ontvangen, wordt het pakje ingetrokken.
- Als er geen route op de interface terug naar de bron van de multicast pakketten is, gebruikt u de opdracht om de firewall op te dragen de pakketten niet te laten vallen.

Configureren

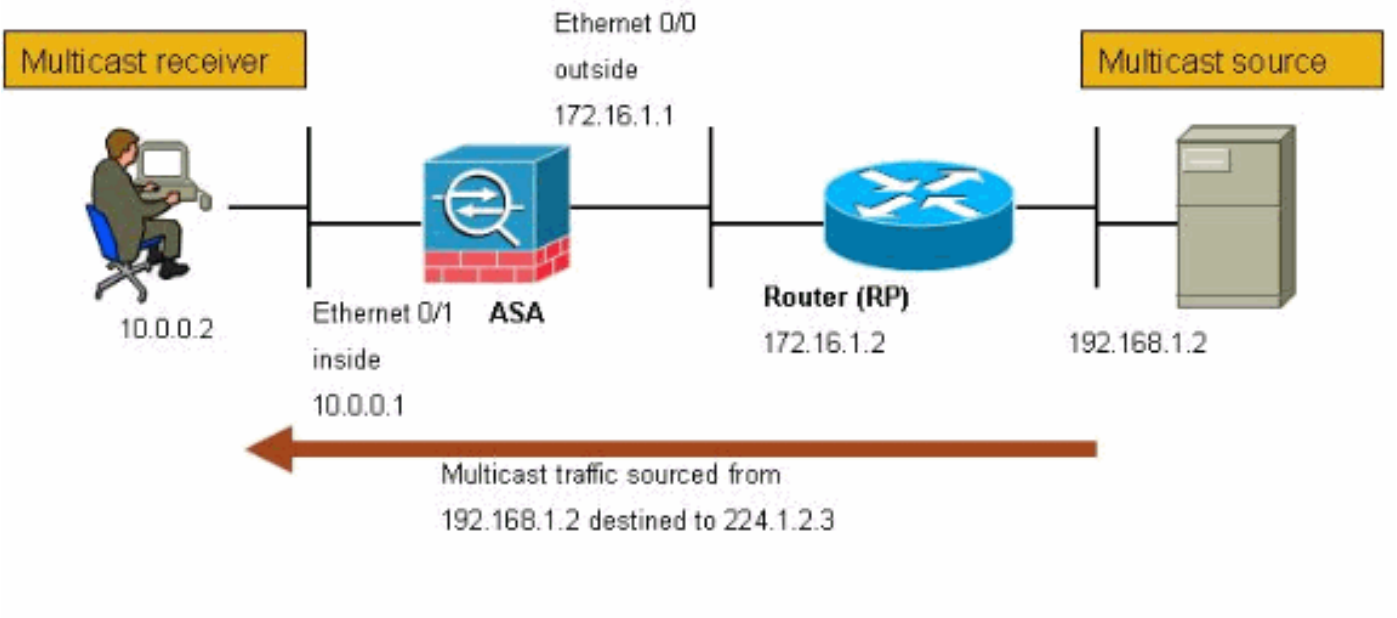
Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

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.

Het multicast verkeer komt uit 192.168.1.2 en gebruikt UDP-pakketten op poort 1234 die bestemd zijn voor groep 224.1.2.3.



Configuratie

Dit document gebruikt deze configuratie:

Cisco PIX- of ASA-firewall voor versie 7.x

```
maui-soho-01#show running-config
 SA Version 7.1(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted


 !--- The multicast-routing command enables IGMP and PIM
!--- on all interfaces of the firewall.

multicast-routing
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.0.0.1 255.255.255.0
!
interface Ethernet0/2
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
```

```
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted

!--- The rendezvous point address must be defined in the
!--- configuration in order for PIM to function
correctly. pim rp-address 172.16.1.2 boot system
disk0:/asa712-k8.bin ftp mode passive !--- It is
necessary to permit the multicast traffic with an !---
access-list entry. access-list outside_access_inbound
extended permit ip any host 224.1.2.3
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
no failover
!--- The access-list that permits the multicast traffic
is applied !--- inbound on the outside interface.
access-group outside_access_inbound in interface outside
!--- This mroute entry specifies that the multicast
sender !--- 192.168.1.2 is off the outside interface. In
this example !--- the mroute entry is necessary since
the firewall has no route to !--- the 192.168.1.2 host
on the outside interface. Otherwise, this !--- entry is
not necessary.

mroute 192.168.1.2 255.255.255.255 outside
icmp permit any outside
asdm image disk0:/asdm521.bin
no asdm history enable
arp timeout 14400
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
```

```
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
!
service-policy global_policy global
!
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**-tonen de IPv4 multicast routingtabel.

```
ciscoasa#show mroute

Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

!--- Here you see the mroute entry for the shared tree. Notice that the !--- incoming
interface specifies outside and that the outgoing interface !--- list specifies inside.

(*, 224.1.2.3), 00:00:12/never, RP 172.16.1.2, flags: SCJ
  Incoming interface: outside
  RPF nbr: 172.16.1.2
  Outgoing interface list:
    inside, Forward, 00:00:12/never

!--- Here is the source specific tree for the mroute entry.

(192.168.1.2, 224.1.2.3), 00:00:12/00:03:17, flags: SJ
  Incoming interface: outside
  RPF nbr: 0.0.0.0
  Immediate Outgoing interface list: Null
```

- **toon** conn—hiermee wordt de verbindingsstaat voor het toegewezen connectietype weergegeven.

```
!--- A connection is built through the firewall for the multicast stream. !--- In this case
the stream is sourced from the sender IP and destined !--- to the multicast group.
ciscoasa#show conn
10 in use, 12 most used
UDP out 192.168.1.2:51882 in 224.1.2.3:1234 idle 0:00:00 flags -
ciscoasa#
```

- **Toon** de **buurburen**—Beelden in de PIM buurtabel.

```
!--- When you use PIM, the neighbor devices should be seen with the !--- show pim neighbor
command.

ciscoasa#show pim neighbor
```

```
Neighbor Address  Interface          Uptime    Expires DR pri Bidir

172.16.1.2        outside            04:06:37  00:01:27 1 (DR)
```

Problemen oplossen

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

Procedure voor probleemoplossing

Volg deze instructies om uw configuratie problemen op te lossen.

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.

1. Als de multicast ontvangers rechtstreeks met de binnenkant van de firewall zijn verbonden, verzenden zij IGMP-rapporten om de multicast-stream te ontvangen. Gebruik de opdracht **igmp traffic** om te controleren of u IGMP-rapporten van binnenuit ontvangt.

```
ciscoasa#show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 04:11:08

                               Received     Sent
Valid IGMP Packets             413          244
Queries                        128          244
Reports                        159          0
Leaves                         0            0
Mtrace packets                 0            0
DVMRP packets                  0            0
PIM packets                    126          0

Errors:
Malformed Packets              0
Martian source                 0
Bad Checksums                  0

ciscoasa#
```

2. De firewall kan gedetailleerdere informatie over de IGMP gegevens weergeven door de opdracht **debug igmp** te gebruiken.In dit geval worden de debugs ingeschakeld en verstuurt de host 10.0.0.2 een IGMP-rapport voor groep 224.1.2.3.

```
!--- Enable IGMP debugging. ciscoasa#debug igmp
IGMP debugging is on
ciscoasa# IGMP: Received v2 Report on inside from 10.0.0.2 for 224.1.2.3
IGMP: group_db: add new group 224.1.2.3 on inside
IGMP: MRIB updated (*,224.1.2.3) : Success
IGMP: Switching to EXCLUDE mode for 224.1.2.3 on inside
IGMP: Updating EXCLUDE group timer for 224.1.2.3

ciscoasa#
!--- Disable IGMP debugging ciscoasa#un all
```

3. Controleer dat de firewall geldige PIM buren heeft en dat de firewall verbinding verstuurt en informatie ontvangt.

```
ciscoasa#show pim neigh

Neighbor Address  Interface          Uptime    Expires DR pri Bidir

172.16.1.2        outside            04:26:58  00:01:20 1 (DR)

ciscoasa#show pim traffic

PIM Traffic Counters
Elapsed time since counters cleared: 04:27:11

                              Received     Sent
Valid PIM Packets             543          1144
Hello                         543          1079
Join-Prune                    0            65
Register                      0            0
Register Stop                 0            0
Assert                        0            0
Bidir DF Election             0            0

Errors:
Malformed Packets                          0
Bad Checksums                              0
Send Errors                                0
Packet Sent on Loopback Errors             0
Packets Received on PIM-disabled Interface 0
Packets Received with Unknown PIM Version  0
Packets Received with Incorrect Addressing 0
ciscoasa#
```

4. Gebruik de opdracht **opnemen** om te controleren of de buiteninterface de multicast-pakketten voor de groep ontvangt.

```
ciscoasa#configure terminal

!--- Create an access-list that is only used !--- to flag the packets to capture.
ciscoasa(config)#access-list captureacl permit ip any host 224.1.2.3

!--- Define the capture named capout, bind it to the outside interface, and !--- specify to
only capture packets that match the access-list captureacl. ciscoasa(config)#capture capout
interface outside access-list captureacl

!--- Repeat for the inside interface. ciscoasa(config)#capture capin interface inside
access-list captureacl

!--- View the contents of the capture on the outside. This verifies that the !--- packets
are seen on the outside interface ciscoasa(config)#show capture capout
138 packets captured
   1: 02:38:07.639798 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
   2: 02:38:07.696024 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
   3: 02:38:07.752295 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
   4: 02:38:07.808582 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
   5: 02:38:07.864823 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
   6: 02:38:07.921110 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
   7: 02:38:07.977366 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
   8: 02:38:08.033689 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
   9: 02:38:08.089961 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  10: 02:38:08.146247 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  11: 02:38:08.202504 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  12: 02:38:08.258760 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  13: 02:38:08.315047 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  14: 02:38:08.371303 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
```

```
  15: 02:38:08.427574 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  16: 02:38:08.483846 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  17: 02:38:08.540117 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  18: 02:38:08.596374 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  19: 02:38:08.652691 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  20: 02:38:08.708932 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  21: 02:38:08.765188 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  22: 02:38:08.821460 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  23: 02:38:08.877746 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  24: 02:38:08.934018 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316

 !--- Here you see the packets forwarded out the inside !--- interface towards the clients.
ciscoasa(config)#show capture capin
89 packets captured
   1: 02:38:12.873123 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
   2: 02:38:12.929380 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
   3: 02:38:12.985621 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
   4: 02:38:13.041898 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
   5: 02:38:13.098169 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
   6: 02:38:13.154471 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
   7: 02:38:13.210743 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
   8: 02:38:13.266999 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
   9: 02:38:13.323255 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  10: 02:38:13.379542 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  11: 02:38:13.435768 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  12: 02:38:13.492070 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  13: 02:38:13.548342 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  14: 02:38:13.604598 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  15: 02:38:13.660900 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  16: 02:38:13.717141 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  17: 02:38:13.773489 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  18: 02:38:13.829699 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  19: 02:38:13.885986 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  20: 02:38:13.942227 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  21: 02:38:13.998483 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  22: 02:38:14.054852 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  23: 02:38:14.111108 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
  24: 02:38:14.167365 192.168.1.2.52292 > 224.1.2.3.1234:  udp 1316
ciscoasa(config)#

 !--- Remove the capture from the memory of the firewall. ciscoasa(config)#no capture
capout
```

Known Bugs

Cisco bug-ID CSCse81633 (alleen geregistreerde klanten) — ASA 4 GE-SSM Gig-poorten drogen IGMP-verbindingen stilletjes in.

- **Symptoom**-Wanneer een 4GE-SSM module in een ASA is geïnstalleerd en de multicast-routing samen met IGMP op de interfaces wordt gevormd, worden de IGMP-verbindingen op de interfaces van de 4GE-SSM module gedropt.
- **De voorwaarden**-IGMP hoeven niet te worden ingetrokken op de Bord Gig-interfaces van de ASA.
- **Werken**-voor multicast routing, gebruik de geïntegreerde Gig-interfacepoorten.
- **Vast in versies**—7.0(6), 7.1(2)18, 7.2(1)11

Gerelateerde informatie

- Cisco ASA 5500 Series adaptieve security applicatie
- Cisco PIX 500 Series security applicaties
- Technische ondersteuning en documentatie – Cisco Systems