PIX/ASA 7.x: Multicast auf den PIX/ASA-Plattformen mit Absender im externen Konfigurationsbeispiel

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für Multicast auf der Cisco Adaptive Security Appliance (ASA) und/oder der PIX Security Appliance, die Version 7.x ausführt. In diesem Beispiel befindet sich der Multicast-Absender außerhalb der Sicherheits-Appliance, und die Hosts innerhalb versuchen, den Multicast-Datenverkehr zu empfangen. Die Hosts senden IGMP-Berichte, um die Gruppenmitgliedschaft zu melden, und die Firewall verwendet den PIM-Sparse-Modus (Protocol Independent Multicast) als dynamisches Multicast-Routing-Protokoll zum Upstream-Router, hinter dem sich die Quelle des Streams befindet.

Hinweis: FWSM/ASA unterstützt das Subnetz 232.x.x/8 nicht als Gruppennummer, da es für ASA SSM reserviert ist. FWSM/ASA lässt also zu, dass dieses Subnetz nicht verwendet oder durchlaufen wird, und mroute wird nicht erstellt. Sie können diesen Multicast-Datenverkehr jedoch weiterhin über ASA/FWSM leiten, wenn Sie ihn in den GRE-Tunnel einkapseln.

Voraussetzungen

Anforderungen

Eine Cisco PIX- oder ASA Security Appliance, die die Softwareversion 7.0, 7.1 oder 7.2 ausführt.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einer Cisco PIX- oder Cisco ASA-Firewall, die Version 7.x ausführt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

PIX/ASA 7.x bietet einen vollständigen PIM Sparse Mode und bidirektionale Unterstützung für dynamisches Multicast-Routing über die Firewall. Der PIM Dense Mode wird nicht unterstützt. Die 7.x-Software unterstützt weiterhin den Legacy-Multicast-Stubmodus, bei dem die Firewall lediglich ein IGMP-Proxy zwischen den Schnittstellen ist, wie in PIX, Version 6.x, unterstützt.

Diese Anweisungen gelten für Multicast-Datenverkehr durch die Firewall:

- Wenn eine Zugriffsliste auf die Schnittstelle angewendet wird, an der der Multicast-Datenverkehr empfangen wird, muss die Zugriffskontrollliste (ACL) den Datenverkehr explizit zulassen. Wenn auf die Schnittstelle keine Zugriffsliste angewendet wird, ist der explizite ACL-Eintrag, der den Multicast-Datenverkehr zulässt, nicht erforderlich.
- Die Multicast-Datenpakete werden immer der Reverse Path Forwarding-Prüfung der Firewall unterzogen, unabhängig davon, ob der Befehl **Reverse Path Forwarding Check** auf der Schnittstelle konfiguriert ist. Wenn also auf der Schnittstelle keine Route vorhanden ist, über die das Paket an die Quelle des Multicast-Pakets empfangen wurde, wird das Paket verworfen.
- Wenn auf der Schnittstelle keine Route zurück zur Quelle der Multicast-Pakete vorhanden ist, weisen Sie die Firewall mithilfe des Befehls **mroute** an, die Pakete nicht zu verwerfen.

Konfigurieren

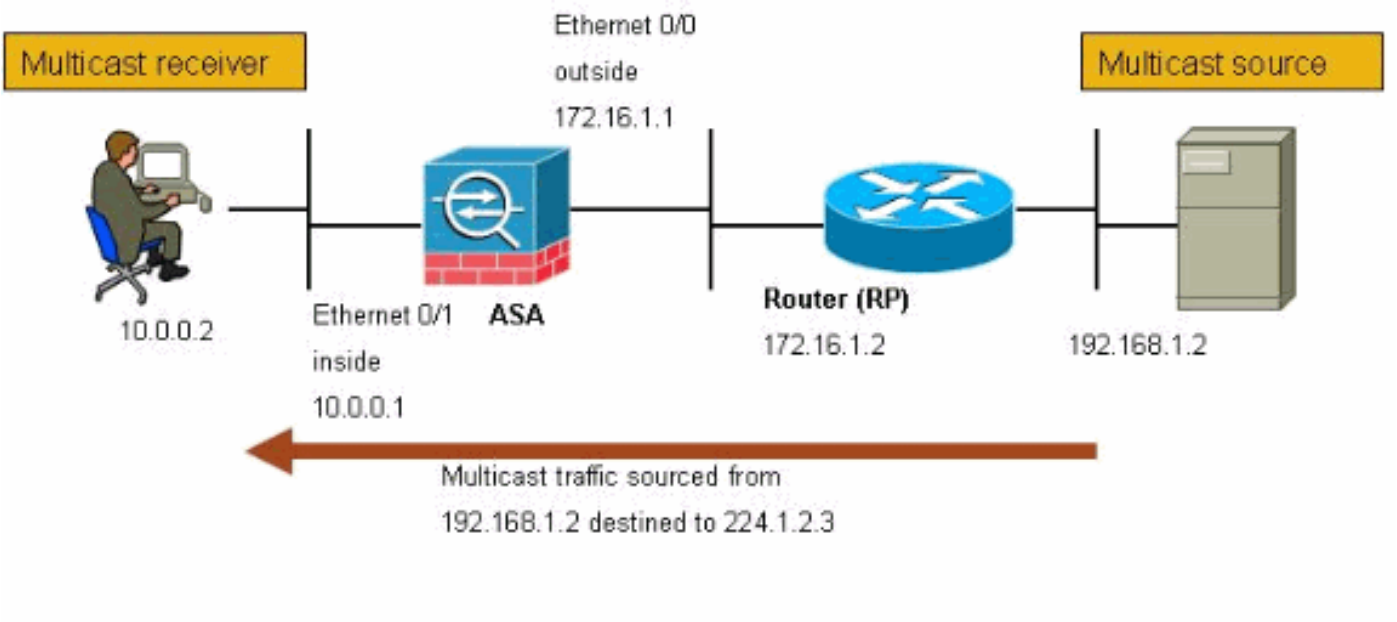
In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird diese Netzwerkeinrichtung verwendet.

Der Multicast-Datenverkehr stammt von 192.168.1.2 und verwendet UDP-Pakete an Port 1234, die für die Gruppe 224.1.2.3 bestimmt sind.



Konfiguration

In diesem Dokument wird diese Konfiguration verwendet:

Cisco PIX- oder ASA-Firewall mit Version 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
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show mroute**: Zeigt die IPv4-Multicast-Routing-Tabelle an.

```
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
```

- **show conn**: Zeigt den Verbindungsstatus für den festgelegten Verbindungstyp an.

```
!--- 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#
```

- **show pim neighbor**: Zeigt Einträge in der Tabelle für den PIM-Nachbarn an.

```
!--- 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)
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Fehlerbehebungsverfahren

Befolgen Sie diese Anweisungen, um eine Fehlerbehebung für Ihre Konfiguration durchzuführen.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

1. Wenn die Multicast-Empfänger direkt mit der Firewall verbunden sind, senden sie IGMP-Berichte, um den Multicast-Stream zu empfangen. Verwenden Sie den Befehl **show igmp traffic** (IGMP-Datenverkehr anzeigen), um zu überprüfen, ob Sie von innen IGMP-Berichte erhalten.

```
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. Die Firewall kann mithilfe des Befehls **debug igmp** detailliertere Informationen zu den IGMP-Daten anzeigen.In diesem Fall sind die Debug-Dateien aktiviert, und der Host 10.0.0.2 sendet einen IGMP-Bericht für die Gruppe 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. Überprüfen Sie, ob die Firewall über gültige PIM-Nachbarn verfügt und dass die Firewall Informationen zum Verbinden/Löschen sendet und empfängt.

```
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. Verwenden Sie den Befehl **capture**, um zu überprüfen, ob die externe Schnittstelle die Multicast-Pakete für die Gruppe empfängt.

```
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
```

Bekannte Fehler

Cisco Bug ID CSCse81633 (nur registrierte Kunden) - ASA 4GE-SSM Gig-Ports für leises Verwerfen von IGMP-Joins.

- **Symptom** - Wenn ein 4GE-SSM-Modul in einer ASA installiert wird und Multicast-Routing zusammen mit IGMP an den Schnittstellen konfiguriert wird, werden IGMP-Joins an den Schnittstellen des 4GE-SSM-Moduls verworfen.
- **Bedingungen** - IGMP-Joins werden nicht an den integrierten Gig-Schnittstellen der ASA verworfen.
- **Problemumgehung** - Verwenden Sie für Multicast-Routing die integrierten Gig-Schnittstellenports.
- **Fest in Versionen**: 7.0(6), 7.1(2)18, 7.2(1)11

Zugehörige Informationen

- Unterstützung für Cisco Adaptive Security Appliances der Serie ASA 5500
- Unterstützung von Cisco PIX Security Appliances der Serie 500
- Technischer Support und Dokumentation - Cisco Systems