PIX/ASA 7.x: Multicast on the PIX/ASA Platforms with Sender on Outside Configuration Example

Contents

Introduction

This document provides a sample configuration for multicast on the Cisco Adaptive Security Appliance (ASA) and/or PIX Security Appliance that runs version 7.x. In this example, the multicast sender is on the outside of the security appliance and hosts on the inside are attempting to receive the multicast traffic. The hosts send IGMP reports to report group membership, and the firewall uses Protocol Independent Multicast (PIM) sparse mode as the dynamic multicast routing protocol to the upstream router, behind which the source of the stream resides.

Note: FWSM/ASA does not support 232.x.x.x/8 subnet as a group number as it is reserved for ASA SSM. So FWSM/ASA does not allow this subnet to be used or traversed and mroute does not get created. But, you can still pass this multicast traffic through ASA/FWSM if you encapsulate it in GRE tunnel.

Prerequisites

Requirements

A Cisco PIX or ASA Security Appliance that runs software version 7.0, 7.1, or 7.2.

Components Used

The information in this document is based on a Cisco PIX or Cisco ASA Firewall that runs version 7.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

PIX/ASA 7.x introduces full PIM sparse mode and bi-directional support for dynamic multicast routing through the firewall. PIM dense mode is not supported. The 7.x software still supports legacy multicast 'stub-mode' in which the firewall is simply an IGMP proxy between interfaces as was supported in PIX version 6.x.

These statements hold true for multicast traffic through the firewall:

- If an access-list is applied to the interface where the multicast traffic is received, then the access control list (ACL) must explicitly permit the traffic. If no access-list is applied to the interface, the explicit ACL entry that permits the multicast traffic is not necessary.
- The multicast data packets are always subjected to the Reverse Path Forwarding check of the firewall, regardless of whether the **reverse-path forward check** command is configured on the interface. Therefore, if there is no route on the interface that the packet was received on to the source of the multicast packet, then the packet is dropped.
- If there is no route on the interface back to the source of the multicast packets, use the **mroute** command to instruct the firewall not to drop the packets.
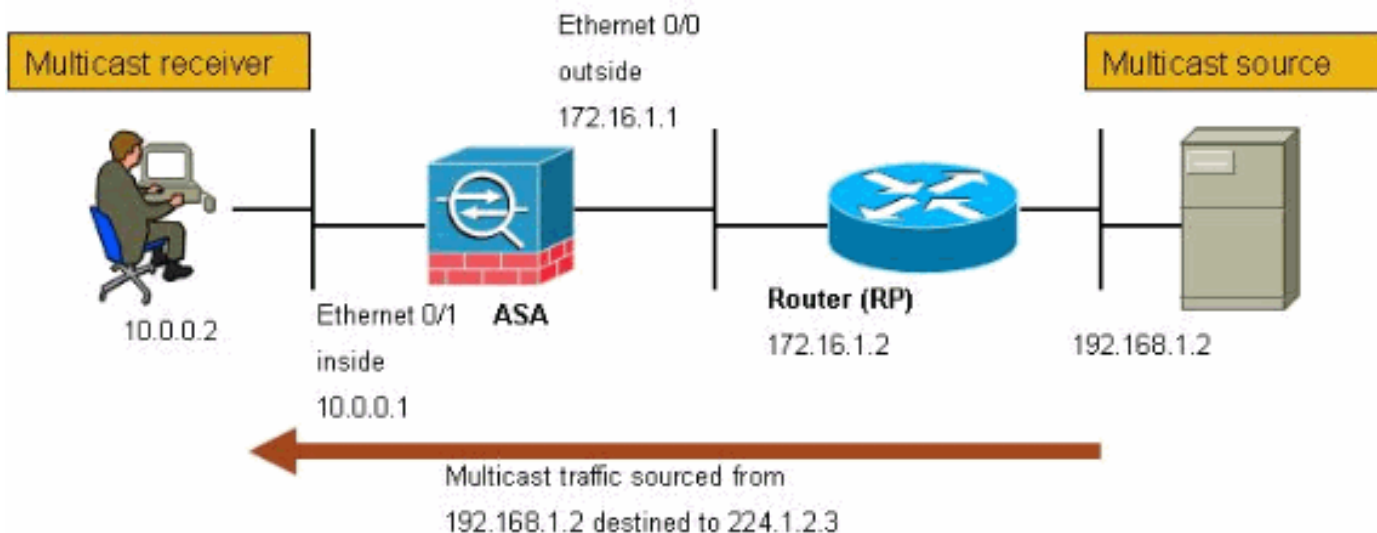
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup.

The multicast traffic is sourced from 192.168.1.2 and uses UDP packets on port 1234 destined to group 224.1.2.3.

Multicast traffic sourced from 192.168.1.2 destined to 224.1.2.3

Configuration

This document uses this configuration:

Cisco PIX or ASA Firewall that runs 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
```

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show mroute**—Displays the IPv4 multicast routing table.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**—Displays the connection state for the designated connection type.
  !--- 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**—Displays entries in the PIM neighbor table.
  !--- 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)

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Procedure

Follow these instructions in order to troubleshoot your configuration.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

1. If the multicast receivers are directly connected to the inside of the firewall, they send IGMP reports to receive the multicast stream. Use the **show igmp traffic** command in order to verify that you receive IGMP reports from the inside.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. The firewall can display more detailed information about the IGMP data by using the **debug**

igmp command.In this case, the debugs are enabled and the host 10.0.0.2 sends an IGMP report for the group 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. Verify that the firewall has valid PIM neighbors and that the firewall sends and receives join/prune information.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. Use the **capture** command in order to verify that the outside interface receives the multicast packets for the group.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 (registered customers only) —ASA 4GE-SSM Gig ports silently drop IGMP joins.

- **Symptom**—When a 4GE-SSM module is installed into an ASA and multicast-routing is configured along with IGMP on the interfaces, IGMP joins are dropped on the interfaces of the 4GE-SSM module.
- **Conditions**—IGMP joins are not dropped on the onboard Gig interfaces of the ASA.
- **Workaround**—For multicast routing, use the onboard Gig interface ports.
- **Fixed in versions**—7.0(6), 7.1(2)18, 7.2(1)11

Related Information

- **Cisco ASA 5500 Series Adaptive Security Appliance Support**
- **Cisco PIX 500 Series Security Appliances Support**
- **Technical Support & Documentation - Cisco Systems**