PIX/ASA 7.x:PIX/ASA 플랫폼에서 Sender on Outside 컨피그레이션 예

목차

소개

이 문서에서는 버전 7.x를 실행하는 Cisco ASA(Adaptive Security Appliance) 및/또는 PIX Security Appliance의 멀티캐스트에 대한 샘플 컨피그레이션을 제공합니다.이 예에서는 멀티캐스트 발신자가 보안 어플라이언스의 외부에 있으며, 내부의 호스트가 멀티캐스트 트래픽을 수신하려고 시도합니다.호스트는 IGMP 보고서를 보고서 그룹 멤버쉽으로 전송하며, 방화벽은 PIM(Protocol Independent Multicast) 스파스 모드를 동적 멀티캐스트 라우팅 프로토콜로 사용하여 스트림의 소스가 상주하는 업스트림 라우터에 연결합니다.

참고: FWSM/ASA는 ASA SSM용으로 예약되어 있으므로 232.x.x.x/8 서브넷을 그룹 번호로 지원하지 않습니다.따라서 FWSM/ASA는 이 서브넷을 사용하거나 통과하는 것을 허용하지 않으며, mroute는 생성되지 않습니다.그러나 GRE 터널에 캡슐화하더라도 ASA/FWSM을 통해 이 멀티캐스트 트래픽을 전달할 수 있습니다.

사전 요구 사항

요구 사항

소프트웨어 버전 7.0, 7.1 또는 7.2를 실행하는 Cisco PIX 또는 ASA Security Appliance

사용되는 구성 요소

이 문서의 정보는 버전 7.x를 실행하는 Cisco PIX 또는 Cisco ASA 방화벽을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

PIX/ASA 7.x는 방화벽을 통한 동적 멀티캐스트 라우팅을 위한 전체 PIM 스파스 모드 및 양방향 지원을 제공합니다.PIM 덴스 모드는 지원되지 않습니다.7.x 소프트웨어는 PIX 버전 6.x에서 지원되었던 것과 같이 방화벽이 인터페이스 간의 IGMP 프록시일 뿐인 레거시 멀티캐스트 'stub-mode'를 계속 지원합니다.

이러한 설명은 방화벽을 통과하는 멀티캐스트 트래픽에 대해 참입니다.

- 액세스 목록이 멀티캐스트 트래픽이 수신되는 인터페이스에 적용되는 경우 ACL(Access Control List)에서 트래픽을 명시적으로 허용해야 합니다.인터페이스에 액세스 목록이 적용되지 않은 경우 멀티캐스트 트래픽을 허용하는 명시적 ACL 항목은 필요하지 않습니다.
- 멀티캐스트 데이터 패킷은 인터페이스에서 reverse-**path forward check** 명령이 구성되었는지 여부에 관계없이 항상 방화벽의 Reverse Path Forwarding 검사를 받습니다.따라서 패킷이 멀티캐스트 패킷의 소스로 수신된 인터페이스에 경로가 없으면 패킷이 삭제됩니다.
- 인터페이스에 멀티캐스트 패킷의 소스로 돌아가는 경로가 없는 경우 mroute 명령을 사용하여 방화벽에서 패킷을 삭제하지 않도록 **지시합니다**.

구성

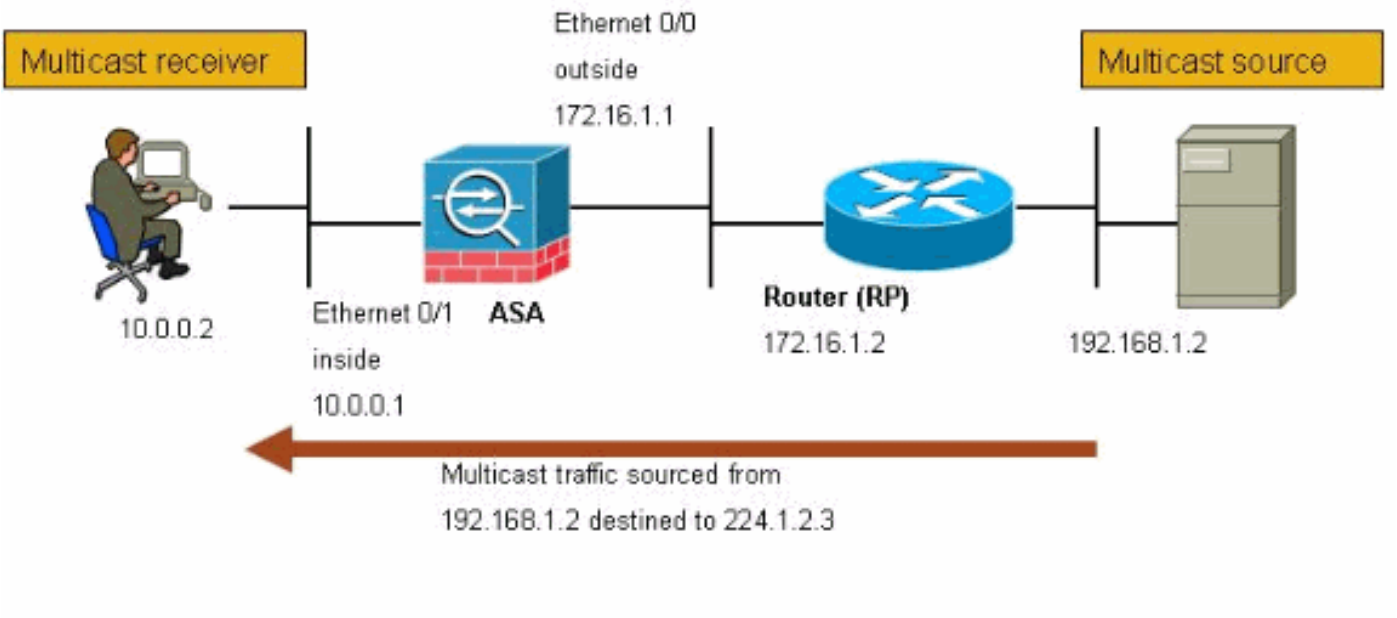
이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.

멀티캐스트 트래픽은 192.168.1.2에서 소싱되며 224.1.2.3을 그룹화할 포트 1234에서 UDP 패킷을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

버전 7.x를 실행하는 Cisco PIX 또는 ASA 방화벽

```
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
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show mroute** - IPv4 멀티캐스트 라우팅 테이블을 표시합니다.

```
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** - 지정된 연결 유형의 연결 상태를 표시합니다.

```
!--- 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** - PIM 네이버 테이블의 항목을 표시합니다.

```
!--- 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)
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 절차

컨피그레이션 문제를 해결하려면 다음 지침을 따르십시오.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

1. 멀티캐스트 수신기가 방화벽 내부에 직접 연결되어 있으면 멀티캐스트 스트림을 수신하기 위해 IGMP 보고서를 전송합니다.내부에서 IGMP 보고서를 수신하는지 확인하려면 **show igmp traffic** 명령을 사용합니다.

```
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. 방화벽은 debug igmp 명령을 사용하여 IGMP 데이터에 대한 자세한 정보를 표시할 수 **있습니다**.이 경우 디버그가 활성화되고 호스트 10.0.0.2이 그룹 224.1.2.3에 대한 IGMP 보고서를 전송합니다.

```
!--- 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. 방화벽에 유효한 PIM 인접 디바이스가 있고 방화벽에서 가입/정리 정보를 보내고 수신하는지 확인합니다.

```
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. 외부 인터페이스가 그룹의 멀티캐스트 패킷을 수신하는지 확인하려면 capture 명령을 사용합니다.

```
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
```

알려진 버그

Cisco 버그 ID CSCse81633(등록된 고객만 해당) —ASA 4GE-SSM Gig 포트는 IGMP 조인을 자동으로 삭제합니다.

- **증상** - 4GE-SSM 모듈이 ASA에 설치되고 인터페이스에서 IGMP와 함께 멀티캐스트 라우팅이 구성되면 4GE-SSM 모듈의 인터페이스에서 IGMP 조인이 삭제됩니다.
- **조건** - ASA의 온보드 Gig 인터페이스에서 IGMP 조인이 삭제되지 않습니다.
- **해결** 방법 - 멀티캐스트 라우팅의 경우 온보드 Gig 인터페이스 포트를 사용합니다.
- **버전 고정**—7.0(6), 7.1(2)18, 7.2(1)11

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliance 지원
- Cisco PIX 500 Series 보안 어플라이언스 지원
- 기술 지원 및 문서 – Cisco Systems