PIX/ASA 7.X : Пример конфигурации многоадресности на платформах PIX/ASA с внешним отправителем

Содержание

Введение

Этот документ содержит пример конфигурации для многоадресной передачи на устройстве адаптивной защиты Cisco (ASA) и (или) устройстве защиты PIX с ПО версии 7.x. В данном примере отправитель многоадресного трафика за пределами устройства защиты и хосты на внутренней стороне пытаются получать многоадресный трафик. Хосты передают отчеты IGMP, сообщая о составе группы, а межсетевой экран использует разреженный режим масштабируемого протокола маршрутизации (PIM) в качестве динамического протокола многоадресной маршрутизации на вышестоящий маршрутизатор, за которым находится источник потока.

Примечание: FWSM/ASA не поддерживает 232. x. x. Подсеть x/8 как номер группы, поскольку это зарезервировано для SSM ASA. Таким образом, FWSM/ASA не позволяет этой подсети использоваться или пересекаться, и mroute не становится созданным. Но, можно все еще передать этот многоадресный трафик через ASA/FWSM при инкапсуляции его в Туннеле GRE.

Предварительные условия

Требования

PIX Cisco или Устройство обеспечения безопасности ASA, которое работает под управлением ПО версии 7.0, 7.1, или 7.2.

Используемые компоненты

Сведения в этом документе основываются на PIX Cisco или Межсетевом экране Cisco ASA, который выполняет версию 7. x.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

PIX/ASA 7.x представляет полный разреженный режим многоадресной рассылки (PIM sparse) и двунаправленную поддержку динамической многоадресной маршрутизации через межсетевой экран. Разреженный режим PIM (многоадресная рассылка, независящая от протокола) не поддерживается. 7.x программное обеспечение все еще поддерживает устаревшую групповую адресацию 'тупиковый режим', в котором межсетевым экраном является просто Прокси - сервер IGMP между интерфейсами, как поддерживался в Версии PIX 6. x.

Эти операторы сохраняются для многоадресного трафика через межсетевой экран:

- Если access-list применен к интерфейсу, где многоадресный трафик получен, то список контроля доступа (ACL) должен явно разрешить трафик. Если никакой access-list не применен к интерфейсу, явная запись ACL, которая разрешает, многоадресный трафик не необходим.
- Пакеты групповой адресации всегда подвергаются проверке Пересылки по обратному пути межсетевого экрана, независимо от того, настроена ли **команда reverse-path forward check** на интерфейсе. Поэтому, если нет никакого маршрута на интерфейсе, что пакет был получен на источнике пакета групповой адресации, тогда пакет отброшен.
- Если нет никакого маршрута на интерфейсе назад к источнику пакетов групповой адресации, используйте **команду mroute**, чтобы дать межсетевому экрану команду не отбрасывать пакеты.

Настройка

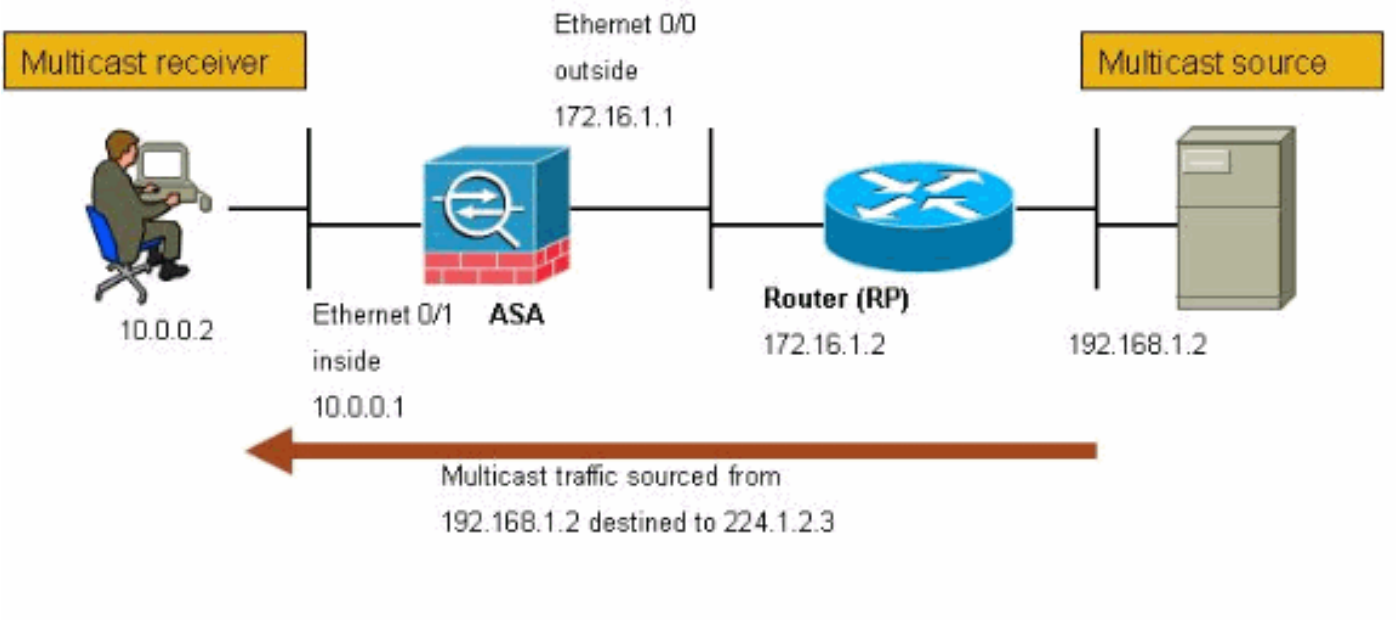
В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети.

Многоадресный трафик получен от 192.168.1.2 и использует пакеты UDP на порту 1234, предназначенном для группировки 224.1.2.3.



!--- конфигурацию

В данном документе используется следующая конфигурация:

PIX Cisco или Межсетевой экран ASA, который выполняет Версию 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
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

- **show mroute** — Отображает таблицу многоадресной маршрутизации IPv4.`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** — Отображает состояние соединения для определяемого типа соединения. `!--- 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** — Записи Показов в таблице соседа PIM. `!--- 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)`

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Процедура устранения неполадок

Следуйте этим инструкциям для устранения проблем конфигурации.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

1. Если получатели групповой адресации напрямую подключаются к внутренней части межсетевого экрана, они передают отчеты IGMP для получения многоадресной рассылки. Используйте **команду show igmp traffic**, чтобы проверить получение отчетов IGMP от внутренней части.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. Межсетевой экран может отобразить более подробную информацию о данных IGMP при помощи **команды debug igmp**.В этом случае отладки включены, и хост 10.0.0.2 передает отчет IGMP за группой 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. Проверьте, что межсетевой экран имеет допустимых соседей PIM и что межсетевой экран передает и получает информацию о соединении/сливе.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. Используйте команду **перехвата**, чтобы проверить, что внешний интерфейс получает пакеты групповой адресации для группы.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
```

Известные ошибки

Идентификатор ошибки Cisco CSCse81633 (только зарегистрированные клиенты) — Порты Концерта 4GE-SSM ASA тихо отбрасывают соединения IGMP.

- **Признак** — Когда модуль 4GE-SSM установлен в ASA и multicast-routing, настроен наряду с IGMP на интерфейсах, соединения IGMP отброшены на интерфейсах модуля 4GE-SSM.
- **Условия** — соединения IGMP не отброшены на встроенных Интерфейсах gig ASA.
- **Обходной путь** — Для многоадресной маршрутизации, используйте встроенные порты Интерфейса gig.
- **Исправленный в версиях** — 7.0 (6), 7.1 (2) 18, 7.2 (1) 11

Дополнительные сведения

- Поддержка многофункционального устройства защиты Cisco ASA серии 5500
- Поддержка Cisco PIX 500 Series Security Appliances
- Cisco Systems – техническая поддержка и документация