PIX/ASA 7.x: Esempio di multicast su piattaforme PIX/ASA con mittente su configurazione esterna

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Convenzioni](#)
[Premesse](#)
[Configurazione](#)
[Esempio di rete](#)
[Configurazione](#)
[Verifica](#)
[Risoluzione dei problemi](#)
[Procedura di risoluzione dei problemi](#)
[Bug noti](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene fornita una configurazione di esempio per il multicast su Cisco Adaptive Security Appliance (ASA) e/o PIX Security Appliance con versione 7.x. Nell'esempio, il mittente multicast si trova all'esterno dell'appliance di sicurezza e gli host all'interno stanno tentando di ricevere il traffico multicast. Gli host inviano report IGMP per segnalare l'appartenenza ai gruppi e il firewall utilizza la modalità sparse Protocol Independent Multicast (PIM) come protocollo di routing multicast dinamico per il router upstream, dietro il quale risiede l'origine del flusso.

Nota: FWSM/ASA non supporta la subnet 232.x.x.x/8 come numero di gruppo perché è riservata per ASA SSM. Pertanto, il modulo FWSM/ASA non consente di utilizzare o attraversare questa subnet e il percorso non viene creato. Tuttavia, è ancora possibile passare il traffico multicast tramite ASA/FWSM se lo si incapsula nel tunnel GRE.

Prerequisiti

Requisiti

Appliance di sicurezza Cisco PIX o ASA con software versione 7.0, 7.1 o 7.2.

Componenti usati

Le informazioni di questo documento si basano su un firewall Cisco PIX o Cisco ASA con versione 7.x.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

PIX/ASA 7.x introduce la modalità sparse PIM completa e il supporto bidirezionale per il routing multicast dinamico attraverso il firewall. La modalità PIM dense non è supportata. Il software 7.x supporta ancora la "modalità stub" multicast legacy in cui il firewall è semplicemente un proxy IGMP tra le interfacce come supportato in PIX versione 6.x.

Queste istruzioni sono valide per il traffico multicast attraverso il firewall:

- Se all'interfaccia che riceve il traffico multicast viene applicato un elenco degli accessi, l'elenco di controllo di accesso (ACL) deve consentire esplicitamente il traffico. Se all'interfaccia non viene applicato alcun elenco degli accessi, non è necessaria la voce ACL esplicita che autorizza il traffico multicast.
- I pacchetti di dati multicast sono sempre soggetti al controllo Reverse Path Forwarding del firewall, indipendentemente dal fatto che il comando **reverse-path forward check** sia configurato sull'interfaccia. Pertanto, se sull'interfaccia non è presente alcun percorso su cui il pacchetto è stato ricevuto per l'origine del pacchetto multicast, il pacchetto viene scartato.
- Se sull'interfaccia non è presente alcun percorso verso l'origine dei pacchetti multicast, usare il comando **mroute** per indicare al firewall di non rilasciare i pacchetti.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

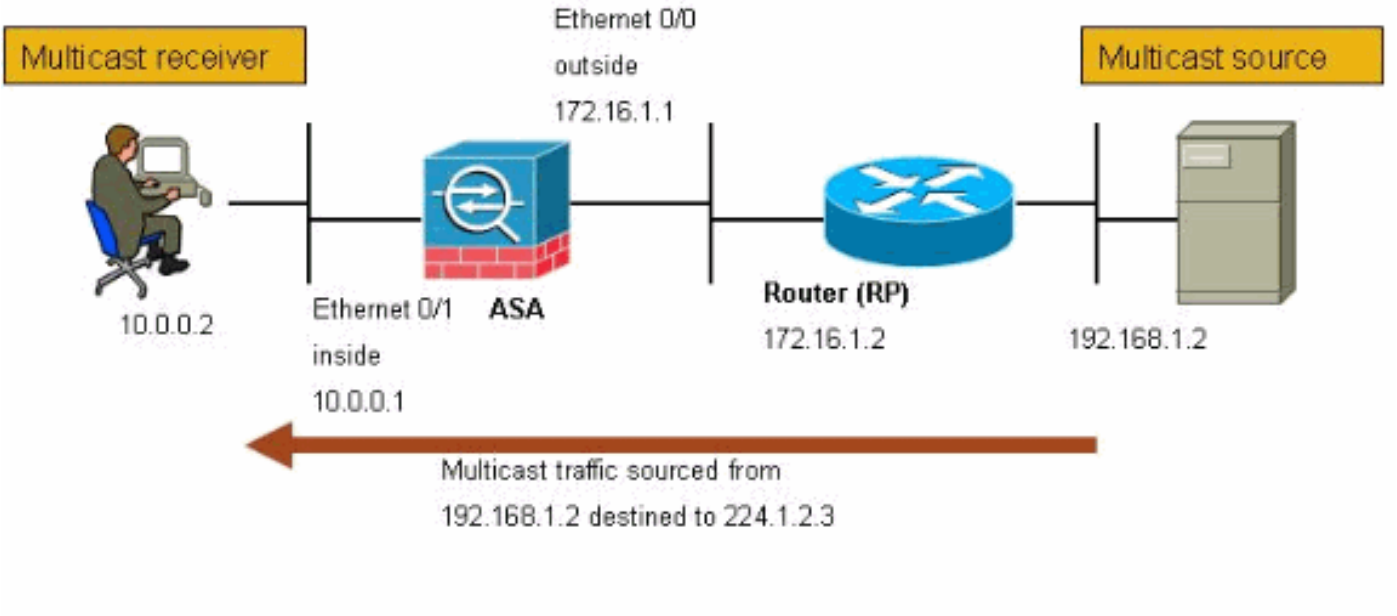
Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete.

Il traffico multicast ha origine da 192.168.1.2 e utilizza pacchetti UDP sulla porta 1234 destinata al

gruppo 224.1.2.3.



Configurazione

Nel documento viene usata questa configurazione:

Cisco PIX o ASA Firewall con versione 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
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show mroute**: visualizza la tabella di routing multicast 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** - Visualizza lo stato della connessione per il tipo di connessione designato.

```
!--- 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 neighbors** - Visualizza le voci della tabella PIM neighbors.

```
!--- 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)
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Procedura di risoluzione dei problemi

Seguire queste istruzioni.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

1. Se i ricevitori multicast sono collegati direttamente all'interno del firewall, inviano rapporti IGMP per ricevere il flusso multicast. Per verificare di aver ricevuto report IGMP dall'interno, usare il comando **show igmp traffic**.

```
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. Il firewall può visualizzare informazioni più dettagliate sui dati IGMP utilizzando il comando **debug igmp**.In questo caso, i debug sono abilitati e l'host 10.0.0.2 invia un report IGMP per il gruppo 24.1.2.3.

```
!--- 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. Verificare che il firewall disponga di vicini PIM validi e che il firewall invii e riceva informazioni di join/eliminazione.

```
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. Per verificare che l'interfaccia esterna riceva i pacchetti multicast per il gruppo, usare il comando **capture**.

```
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
```

Bug noti

Cisco bug ID CSCse81633 (solo utenti registrati) —Le porte ASA 4GE-SSM Gig eliminano automaticamente i join IGMP.

- **Sintomo**: quando un modulo 4GE-SSM viene installato in un'ASA e il routing multicast viene configurato insieme a IGMP sulle interfacce, i join IGMP vengono scartati sulle interfacce del modulo 4GE-SSM.
- **Condizioni**: i join IGMP non vengono scartati sulle interfacce Gig integrate dell'appliance ASA.
- **Soluzione**. Per il routing multicast, utilizzare le porte di interfaccia Gig integrate.
- **Fisso nelle versioni**—7.0(6), 7.1(2)18, 7.2(1)11

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance Support
- Cisco PIX serie 500 Security Appliance Support
- Documentazione e supporto tecnico – Cisco Systems