PIX/ASA 7.x: Exemplo de configuração de multicast nas plataformas PIX/ASA com remetente fora da empresa

Contents

Introduction
Prerequisites
Requirements
Componentes Utilizados
Conventions
Informações de Apoio
Configurar
Diagrama de Rede
Configuração
Verificar
Troubleshoot
Procedimento de Troubleshooting
Erros conhecidos
Informações Relacionadas

Introduction

Este documento fornece uma configuração de exemplo para o multicast no Cisco Adaptive Security Appliance (ASA) e/ou no PIX Security Appliance que executa a versão 7.x. Neste exemplo, o remetente do multicast está na parte externa do mecanismo de segurança e os hosts dentro tentam receber o tráfego multicast. Os hosts enviam relatórios IGMP à associação do grupo de relatórios e o firewall usa o modo de difusão Protocol Independent Multicast (PIM) como o protocolo de roteamento multicast dinâmico para o roteador de upstream, por trás do qual a origem da stream reside.

Observação: o FWSM/ASA não suporta a sub-rede 232.x.x.x/8 como um número de grupo, pois está reservado para o ASA SSM. Portanto, o FWSM/ASA não permite que essa sub-rede seja usada ou atravessada e o mroute não é criado. No entanto, você ainda pode passar esse tráfego multicast pelo ASA/FWSM se encapsulá-lo no túnel GRE.

Prerequisites

Requirements

Um Cisco PIX ou ASA Security Appliance que executa o software versão 7.0, 7.1 ou 7.2.

Componentes Utilizados

As informações neste documento são baseadas em um Cisco PIX ou Cisco ASA Firewall que executa a versão 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

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

O PIX/ASA 7.x apresenta o modo escasso de PIM completo e o suporte bidirecional para roteamento multicast dinâmico através do firewall. O modo denso de PIM não é suportado. O software 7.x ainda suporta o 'modo stub' multicast legado no qual o firewall é simplesmente um proxy IGMP entre interfaces como era suportado no PIX versão 6.x.

Estas afirmações são verdadeiras para o tráfego multicast através do firewall:

- Se uma lista de acesso for aplicada à interface onde o tráfego multicast é recebido, a lista de controle de acesso (ACL) deve permitir explicitamente o tráfego. Se nenhuma lista de acesso for aplicada à interface, a entrada explícita da ACL que permite o tráfego multicast não será necessária.
- Os pacotes de dados multicast são sempre submetidos à verificação de Reverse Path Forwarding do firewall, independentemente de o comando **reverse-path forward check** estar configurado na interface. Portanto, se não houver rota na interface na qual o pacote foi recebido para a origem do pacote multicast, o pacote será descartado.
- Se não houver nenhuma rota na interface de volta à origem dos pacotes multicast, use o comando **mroute** para instruir o firewall a não descartar os pacotes.

Configurar

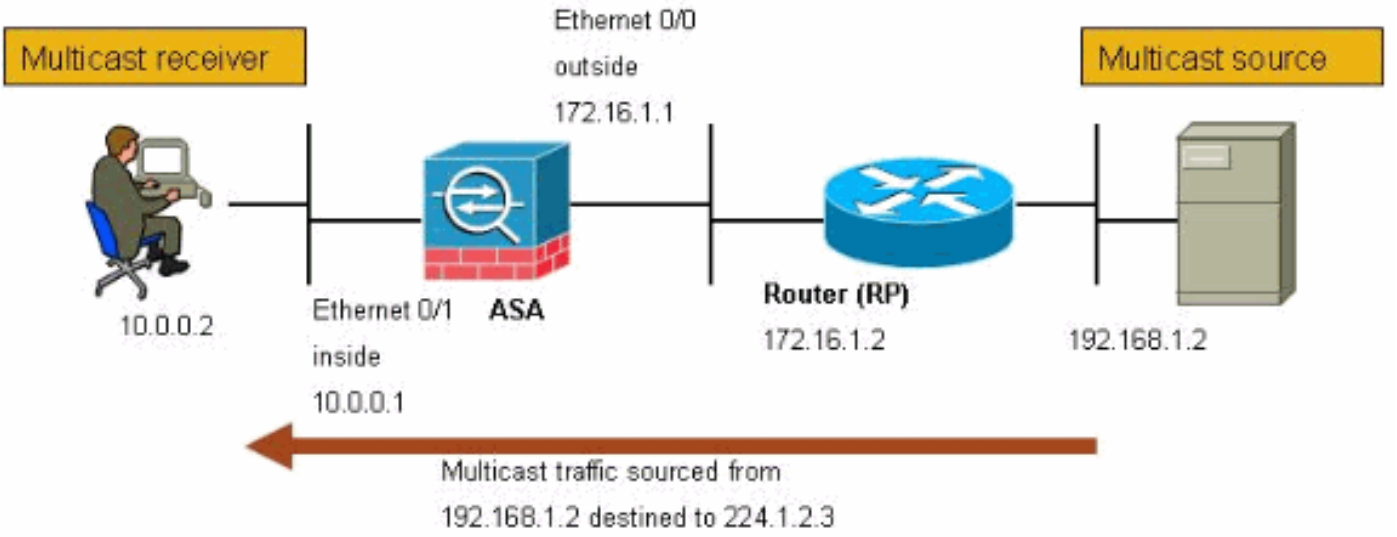
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede.

O tráfego multicast é originado de 192.168.1.2 e usa pacotes UDP na porta 1234 destinados ao grupo 224.1.2.3.



Configuração

Este documento utiliza esta configuração:

Cisco PIX ou ASA Firewall com versão 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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **show mroute** — Exibe a tabela de roteamento 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** — Exibe o estado da conexão para o tipo de conexão designado.

```
!--- 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** —Exibe entradas na tabela de vizinhos 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)
```

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Procedimento de Troubleshooting

Siga estas instruções para solucionar problemas de sua configuração.

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

1. Se os receptores multicast estiverem diretamente conectados ao interior do firewall, eles enviarão relatórios IGMP para receber o fluxo multicast. Use o comando **show igmp traffic** para verificar se você recebe relatórios IGMP de dentro.
```
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. O firewall pode exibir informações mais detalhadas sobre os dados IGMP usando o comando **debug igmp**.Nesse caso, as depurações são ativadas e o host 10.0.0.2 envia um relatório IGMP para o grupo 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. Verifique se o firewall tem vizinhos PIM válidos e se o firewall envia e recebe informações de

junção/remoção.

```
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 o comando **capture** para verificar se a interface externa recebe os pacotes multicast para o grupo.

```
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
```

Erros conhecidos

ID de bug da Cisco CSCse81633 (somente clientes registrados) — as portas ASA 4GE-SSM Gig descartam silenciosamente junções IGMP.

- **Sintoma** —Quando um módulo 4GE-SSM é instalado em um ASA e o roteamento multicast é configurado juntamente com o IGMP nas interfaces, as junções IGMP são descartadas nas interfaces do módulo 4GE-SSM.
- **Condições**—as junções IGMP não são descartadas nas interfaces Gig onboard do ASA.
- **Solução alternativa** — para o roteamento multicast, use as portas de interface Gig onboard.
- **Fixo em versões**—7.0(6), 7.1(2)18, 7.2(1)11

Informações Relacionadas

- Suporte do Cisco ASA 5500 Series Adaptive Security Appliance

- Suporte aos dispositivos de segurança Cisco PIX 500 Series
- Suporte Técnico e Documentação - Cisco Systems