

PIX/ASA 7.x : Exemple de configuration de multicast sur les plates-formes PIX/ASA avec l'expéditeur à l'extérieur

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configuration](#)

[Vérification](#)

[Dépannage](#)

[Procédure de dépannage](#)

[Bogues connus](#)

[Informations connexes](#)

[Introduction](#)

Ce document propose un exemple de configuration de multidiffusion sur la gamme ASA (Adaptive Security Appliance) de Cisco et/ou sur la gamme PIX qui exécute la version 7.x. Dans cet exemple, l'expéditeur de la multidiffusion est à l'extérieur des appareils de sécurité et les hôtes à l'intérieur tentent de recevoir le trafic de la multidiffusion. Les hôtes envoient des rapports IGMP pour signaler l'appartenance au groupe et le pare-feu utilise le mode clairsemé du protocole de multidiffusion indépendante (PIM) pour le routage dynamique de la multidiffusion vers le routeur en amont, derrière lequel réside la source du flux.

Remarque : FWSM/ASA ne prend pas en charge le sous-réseau 232.x.x.x/8 en tant que numéro de groupe, car il est réservé à ASA SSM. Par conséquent, FWSM/ASA n'autorise pas l'utilisation ou la traversée de ce sous-réseau et mroute n'est pas créée. Mais vous pouvez toujours transmettre ce trafic de multidiffusion via ASA/FWSM si vous l'encapsulez dans un tunnel GRE.

[Conditions préalables](#)

[Conditions requises](#)

Dispositif de sécurité Cisco PIX ou ASA qui exécute les versions 7.0, 7.1 ou 7.2 du logiciel.

Components Used

Les informations de ce document sont basées sur un pare-feu Cisco PIX ou Cisco ASA qui exécute la 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

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Informations générales

PIX/ASA 7.x introduit le mode intermédiaire PIM complet et la prise en charge bidirectionnelle pour le routage de multidiffusion dynamique via le pare-feu. Le mode dense PIM n'est pas pris en charge. Le logiciel 7.x prend toujours en charge le 'mode stub' de multidiffusion hérité dans lequel le pare-feu est simplement un proxy IGMP entre les interfaces comme pris en charge dans PIX version 6.x.

Ces instructions s'appliquent au trafic de multidiffusion via le pare-feu :

- Si une liste d'accès est appliquée à l'interface où le trafic de multidiffusion est reçu, alors la liste de contrôle d'accès (ACL) doit explicitement autoriser le trafic. Si aucune liste d'accès n'est appliquée à l'interface, l'entrée ACL explicite qui autorise le trafic de multidiffusion n'est pas nécessaire.
- Les paquets de données de multidiffusion sont toujours soumis au contrôle Reverse Path Forwarding du pare-feu, que la commande **inverpath Forwarding Check** soit configurée sur l'interface. Par conséquent, s'il n'y a aucune route sur l'interface sur laquelle le paquet a été reçu vers la source du paquet de multidiffusion, alors le paquet est abandonné.
- S'il n'y a aucune route sur l'interface vers la source des paquets de multidiffusion, utilisez la commande **mroute** pour demander au pare-feu de ne pas abandonner les paquets.

Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

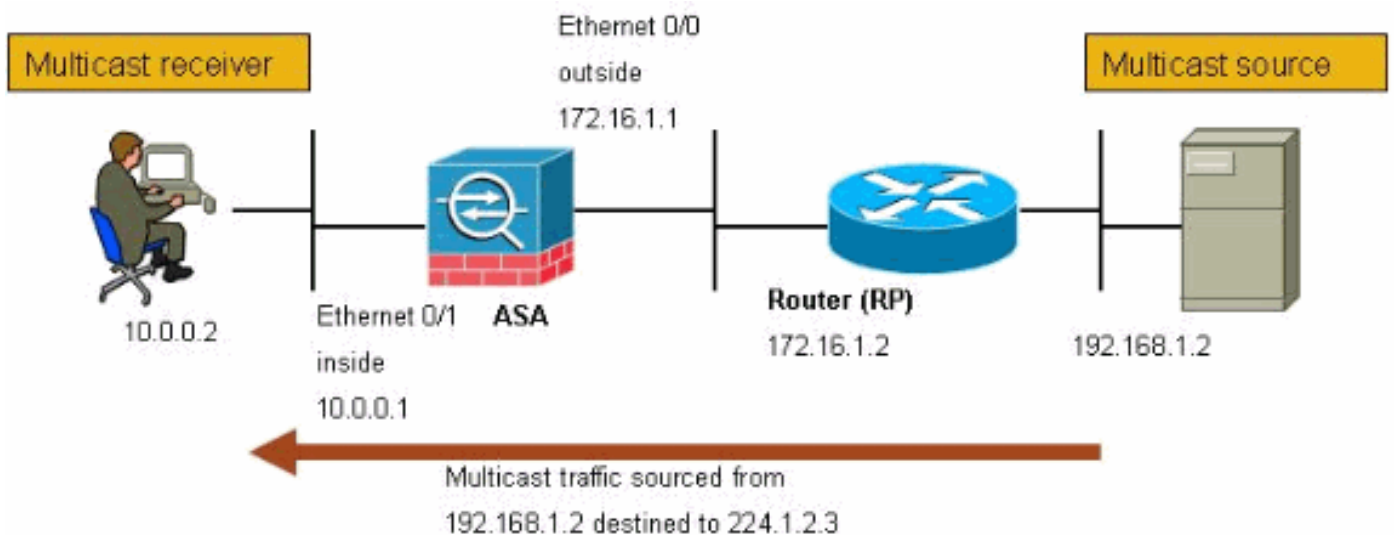
Remarque : utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise cette configuration du réseau.

Le trafic de multidiffusion provient de 192.168.1.2 et utilise des paquets UDP sur le port 1234

destinés au groupe 224.1.2.3.



[Configuration](#)

Ce document utilise la configuration suivante :

Pare-feu Cisco PIX ou ASA qui exécute la 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
```

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'[Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\) prend en charge certaines commandes show](#). Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

- **show mroute** : affiche la table de routage de multidiffusion 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** : affiche l'état de la connexion pour le type de connexion désigné.

!--- 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** : affiche les entrées de la table de voisinage 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)	

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Procédure de dépannage

Suivez ces instructions afin de faire le dépannage de votre configuration .

L'[Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\)](#) prend en charge certaines [commandes show](#). Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Remarque : Consulter les [renseignements importants sur les commandes de débogage](#) avant d'utiliser les commandes de **débogage**.

1. Si les récepteurs de multidiffusion sont directement connectés à l'intérieur du pare-feu, ils envoient des rapports IGMP pour recevoir le flux de multidiffusion. Utilisez la commande **show igmp traffic** afin de vérifier que vous recevez des rapports IGMP de l'intérieur.

```
ciscoasa#show igmp traffic
```

```
IGMP Traffic Counters
Elapsed time since counters cleared: 04:11:08

Valid IGMP Packets          Received      Sent
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. Le pare-feu peut afficher des informations plus détaillées sur les données IGMP à l'aide de la commande **debug igmp**. Dans ce cas, les débogages sont activés et l'hôte 10.0.0.2 envoie un rapport IGMP pour le groupe 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. Vérifiez que le pare-feu a des voisins PIM valides et que le pare-feu envoie et reçoit des informations de jointure/élingue.

```
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. Utilisez la commande **capture** afin de vérifier que l'interface externe reçoit les paquets de multidiffusion pour le groupe.

```
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
```

Bogues connus

ID de bogue Cisco [CSCse81633](#) (clients [enregistrés](#) uniquement) —Les ports Gig ASA 4GE-SSM abandonnent silencieusement les jointures IGMP.

- **Symptom** - Lorsqu'un module 4GE-SSM est installé dans un ASA et que le routage multidiffusion est configuré avec IGMP sur les interfaces, les jointures IGMP sont abandonnées sur les interfaces du module 4GE-SSM.
- **Conditions** : les jointures IGMP ne sont pas abandonnées sur les interfaces Gig embarquées de l'ASA.
- **Solution** : pour le routage de multidiffusion, utilisez les ports d'interface Gig intégrés.
- **Correction dans les versions** - 7.0(6), 7.1(2)18, 7.2(1)11

Informations connexes

- [Prise en charge des appareils de sécurité adaptatifs de la gamme Cisco ASA 5500](#)
- [Assistance des dispositifs de sécurité de la gamme Cisco PIX 500](#)
- [Support et documentation techniques - Cisco Systems](#)