PIX/ASA 7.x: البث المتعدد على الأنظمة الأساسية PIX/ASA مع المرسل على مثال التكوين الخارجي

المحتويات

المقدمة

يقدم هذا المستند نموذجا لتكوين البث المتعدد على جهاز الأمان القابل للتكيف (ASA) من Cisco و/أو جهاز الأمان PIX الذي يشغل الإصدار 7.x. في هذا المثال، يتواجد مرسل البث المتعدد في الخارج من جهاز الأمان وتحاول الأجهزة المضيفة الموجودة بالداخل تلقي حركة مرور البث المتعدد. ترسل الأجهزة المضيفة تقارير IGMP للإبلاغ عن عضوية المجموعة، ويستخدم جدار الحماية الوضع المتناثر للبث المتعدد المستقل عن البروتوكول (PIM) كبروتوكول توجيه البث المتعدد الديناميكي إلى موجه البث الأولي، والذي يتواجد خلفه مصدر الدفق.

ملاحظة: لا يدعم FWSM/ASA الشبكة الفرعية x.x.x/8.232 كرقم مجموعة نظرا لأنه محجوز ل ASA SSM. لذلك لا يسمح FWSM/ASA باستخدام هذه الشبكة الفرعية أو تمريرها ولا يتم إنشاء المسار. غير أنه، ما يزال يمكنك تمرير حركة مرور البث المتعدد هذه من خلال ASA/FWSM إذا قمت بتغليفها في نفق GRE.

المتطلبات الأساسية

المتطلبات

جهاز أمان Cisco PIX أو ASA الذي يشغل الإصدار 7.0 أو 7.1 أو 7.2 من البرنامج.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى جدار حماية Cisco PIX أو Cisco ASA يشغل الإصدار x.7.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

يقدم PIX/ASA 7.x وضع PIM المتناثر الكامل والدعم ثنائي الإتجاه للتوجيه الديناميكي للبث المتعدد من خلال جدار الحماية. وضع PIM المكثف غير مدعوم. لا يزال برنامج x.7 يدعم البث المتعدد القديم 'stub-mode' حيث يكون جدار الحماية مجرد وكيل IGMP بين الواجهات كما كان مدعوما في PIX، الإصدار x.6.

هذه الكشوف صحيحة ل multicast حركة مرور من خلال جدار الحماية:

- إذا تم تطبيق قائمة الوصول على الواجهة التي يتم فيها إستلام حركة مرور البث المتعدد، فيجب على قائمة التحكم في الوصول (ACL) السماح بحركة المرور بشكل صريح. إذا لم يتم تطبيق أي قائمة وصول على الواجهة، فإن إدخال قائمة التحكم في الوصول (ACL) الصريح الذي يسمح بحركة مرور البث المتعدد غير ضروري.
- تخضع حزم بيانات البث المتعدد دائما للتحقق من إعادة توجيه المسار العكسي لجدار الحماية، بغض النظر عما إذا كان الأمر **reverse-path forward check** تم تكوينه على الواجهة أم لا. لذلك، إذا لم يكن هناك مسار على الواجهة التي تم إستلام الحزمة عليها إلى مصدر حزمة البث المتعدد، حينئذ يتم إسقاط الحزمة.
- إذا لم يكن هناك مسار على الواجهة مرة أخرى إلى مصدر حزم البث المتعدد، فاستخدم الأمر **mroute** لتوجيه جدار الحماية إلى عدم إسقاط الحزم.

التكوين

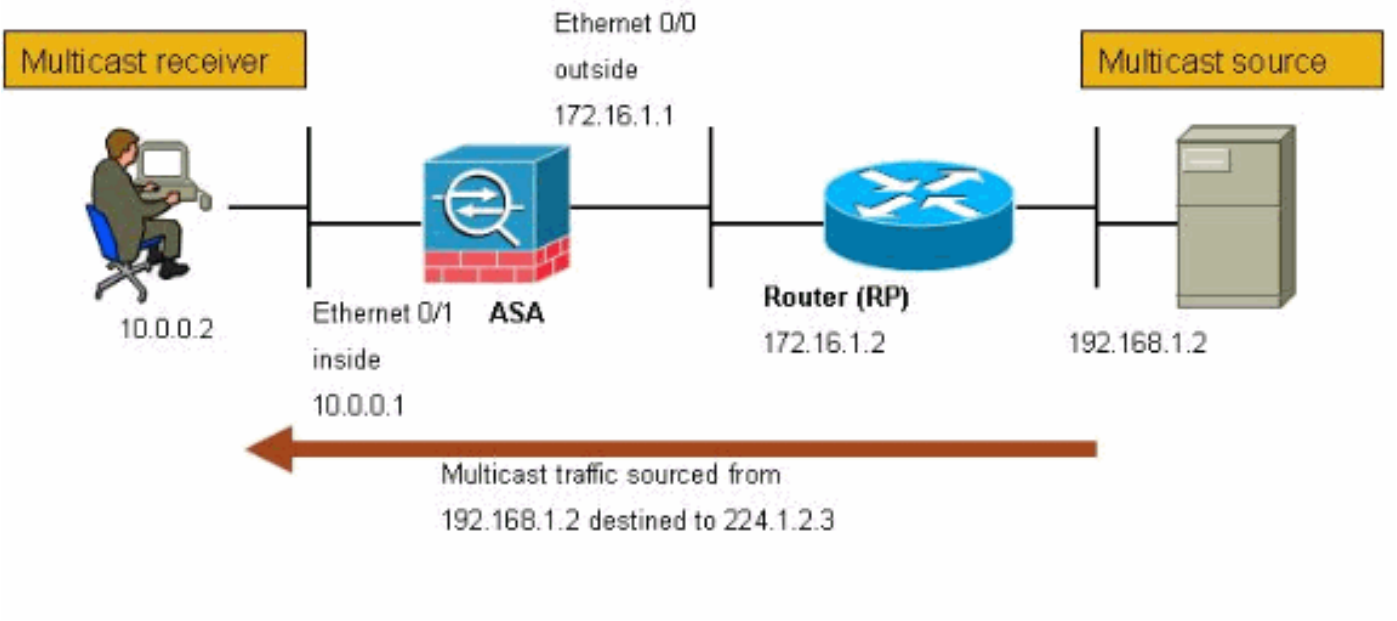
في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي.

يتم مصدر حركة مرور البث المتعدد من 192.168.1.2 ويستخدم حزم UDP على المنفذ 1234 الموجهة إلى المجموعة 224.1.2.3.



التكوين

يستعمل هذا وثيقة هذا تشكيل:

جدار حماية Cisco PIX أو ASA الذي يشغل الإصدار x.7

```
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
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

- **show mroute**— يعرض جدول توجيه البث المتعدد ل 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

never, RP 172.16.1.2, flags: SCJ/00:00:12 ,(224.1.2.3 ,*)
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 ---!

flags: SJ ,00:00:12/00:03:17 ,(224.1.2.3 ,192.168.1.2)
Incoming interface: outside
RPF nbr: 0.0.0.0
Immediate Outgoing interface list: Null
```

- **show conn**— يعرض حالة الاتصال لنوع الاتصال المعين.

```
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
in use, 12 most used 10
- UDP out 192.168.1.2:51882 in 224.1.2.3:1234 idle 0:00:00 flags
#ciscoasa
```

- **إظهار جار PIM**—يعرض الإدخالات في جدول PIM المجاور.

```
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
```

```
(outside            04:06:37  00:01:27 1 (DR       172.16.1.2
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

إجراء استكشاف الأخطاء وإصلاحها

اتبع هذه التعليمات لاستكشاف أخطاء عملية التكوين لديك وإصلاحها.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

1. إذا كانت أجهزة إستقبال البث المتعدد متصلة مباشرة بداخل جدار الحماية، فإنها ترسل تقارير IGMP لتلقي تدفق البث المتعدد. أستخدم الأمر **show igmp traffic** للتحقق من إستلامك تقارير IGMP من الداخل.

```
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. يمكن لجدار الحماية عرض معلومات أكثر تفصيلا حول بيانات IGMP باستخدام الأمر **debug igmp**.في هذه الحالة، يتم تمكين تصحيح الأخطاء ويرسل المضيف 10.0.0.2 تقرير IGMP للمجموعة 224.1.2.3.

```
ciscoasa#debug igmp ---! Enable IGMP debugging.
                                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
ciscoasa#un all ---! Disable IGMP debugging
```

3. تحقق من أن جدار الحماية يحتوي على جيران PIM صالحين ومن أن جدار الحماية يرسل ويستلم معلومات الانضمام/النسخ.

```
ciscoasa#show pim neigh

Neighbor Address  Interface          Uptime    Expires DR pri Bidir
```

```
(outside            04:26:58  00:01:20 1 (DR        172.16.1.2

                                                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
                                  Packet Sent on PIM-disabled Interface       0
                                  Packet Received on PIM-disabled Interface   0
                                  Packet Received with Unknown PIM Version    0
                                  Packet Received with Incorrect Addressing   0
                                                                      #ciscoasa
```

4. أستخدم الأمر **capture** للتحقق من أن الواجهة الخارجية تتلقى حزم البث المتعدد للمجموعة.

```
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
                                                                packets captured 138
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:07.639798 :1
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:07.696024 :2
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:07.752295 :3
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:07.808582 :4
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:07.864823 :5
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:07.921110 :6
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:07.977366 :7
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:08.033689 :8
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:08.089961 :9
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:08.146247 :10
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:08.202504 :11
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:08.258760 :12
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:08.315047 :13
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:08.371303 :14
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:08.427574 :15
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:08.483846 :16
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:08.540117 :17
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:08.596374 :18
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:08.652691 :19
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:08.708932 :20
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:08.765188 :21
      udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:08.821460 :22
```

```
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:08.877746 :23
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:08.934018 :24

Here you see the packets forwarded out the inside !--- interface towards the clients. ---!
                                        ciscoasa(config)#show capture capin
                                                  packets captured 89
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:12.873123 :1
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:12.929380 :2
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:12.985621 :3
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:13.041898 :4
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:13.098169 :5
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:13.154471 :6
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:13.210743 :7
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:13.266999 :8
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:13.323255 :9
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:13.379542 :10
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:13.435768 :11
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:13.492070 :12
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:13.548342 :13
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:13.604598 :14
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:13.660900 :15
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:13.717141 :16
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:13.773489 :17
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:13.829699 :18
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:13.885986 :19
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:13.942227 :20
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:13.998483 :21
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:14.054852 :22
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:14.111108 :23
udp 1316  :224.1.2.3.1234 < 192.168.1.2.52292 02:38:14.167365 :24
                                                    #(ciscoasa(config

Remove the capture from the memory of the firewall. ciscoasa(config)#no capture ---!
                                                                  capout
```

أخطاء معروفة

معرف تصحيح الأخطاء من CSCse81633 Cisco (العملاء المسجلون فقط) — منافذ ASA 4GE-SSM Gig تقوم بإسقاط وصلات IGMP بصمت.

- **العرض**— عند تثبيت وحدة 4GE-SSM في ASA وتكوين التوجيه متعدد البث مع IGMP على الواجهات، يتم إسقاط وصلات IGMP على واجهات وحدة 4GE-SSM.
- **الشروط**—لا يتم إسقاط وصلات IGMP على واجهات Gig المدمجة ل ASA.
- **الحل البديل**—لتوجيه البث المتعدد، أستخدم منافذ واجهة Gig المدمجة.
- **ثابتة في الإصدارات** - 7.0(6) و 7.1(2)18 و 7.2(1)11

معلومات ذات صلة

- دعم جهاز الأمان القابل للتكيف ASA 5500 Series من Cisco
- دعم أجهزة الأمان Cisco PIX 500 Series Security Appliances
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).