أستكشاف أخطاء حزم البث المتعدد وإصلاحها PIM الخاص عبر جدار الحماية باستخدام تكوين Bidir

المحتويات

مسألة

تتم ملاحظة هذه الأعراض على برنامج Secure Firewall Threat Defense (المعروف سابقا باسم Dual-FTD) الذي يشارك كميزة وسيطة في مجال التوجيه متعدد البث آنذاك مع برنامج BIDIR-PIM)، وهو عبارة عن Directional Protocol Independent Multicast (المعروف سابقا باسم PIM-SM):

1. المسار الخاص بمجموعة البث المتعدد المحددة 232.4.4.4 غير موجود:

```
<#root>

device#

show mroute 232.4.4.4

No mroute entries found.
```

2. يزداد عداد "عمليات السقوط الأخرى" لنطاق المجموعة 232.0.0.0/8 في إخراج الأمر show mfib count:

```
<#root>

device#

show mfib count
```

IP Multicast Statistics
6 routes, 3 groups, 0.00 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Other counts: Total

/RPF failed/

Other drops(OIF-null, rate-limit etc)

Group: 224.0.1.39
RP-tree:
Forwarding: 0/0/0/0, Other: 0/0/0
Group: 224.0.1.40
RP-tree:
Forwarding: 0/0/0/0, Other: 0/0/0

Group: 232.0.0.0/8

RP-tree:
Forwarding: 0/0/0/0,

Other: 2551

/0/

2551 <----

device#

show mfib count

IP Multicast Statistics
6 routes, 3 groups, 0.00 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Other counts: Total

/RPF failed/

Other drops(OIF-null, rate-limit etc)

Group: 224.0.1.39
RP-tree:
Forwarding: 0/0/0/0, Other: 0/0/0
Group: 224.0.1.40
RP-tree:

```
Forwarding: 0/0/0/0, Other: 0/0/0

Group: 232.0.0.0/8


RP-tree:
Forwarding: 0/0/0/0,

Other: 2864

/0/

2864

<----
```

3. يتم إسقاط حزم البث المتعدد باستخدام سبب إسقاط حد معدل التداخل (حد معدل التداخل) لإسقاط باستمرار: يزداد عداد الإسقاط في مسار الأمان السريع (ASP).

```
<#root>

device#

cap capi trace interface inside match udp any host 232.4.4.4


device#

show cap capi trace


2: 19:36:08.509205

192.168.1.2.12345 > 232.4.4.4.12345

:  udp 0
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 13056 ns
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
```

Elapsed time: 13056 ns
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Elapsed time: 2560 ns
Config:
Additional Information:
Found flow with id 4876, using existing flow

Result:
input-interface: inside
input-status: up
input-line-status: up
Action: drop
Time Taken: 28672 ns

Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (NA

device#

show asp drop

Frame drop:

Punt rate limit exceeded (punt-rate-limit) 142

FP L2 rule drop (l2_acl) 6

Last clearing: 19:38:00 UTC Apr 29 2026 by admin

Flow drop:

Last clearing: 19:38:00 UTC Apr 29 2026 by admin

…

device#

show asp drop

Frame drop:

Punt rate limit exceeded (punt-rate-limit) 780

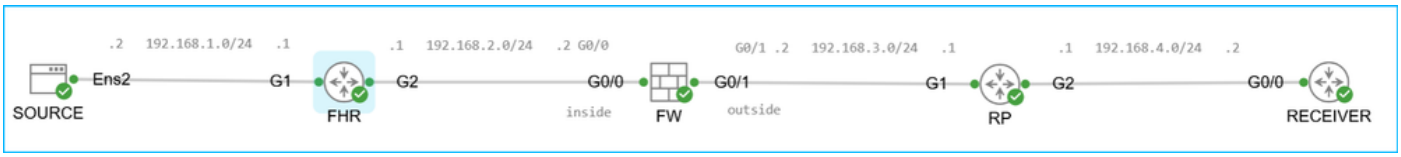
FP L2 rule drop (l2_acl) 37

4. ال تعرض صور الواجهة الخارجية أي حزم بث متعدد لمخرج:

```
<#root>

device#

capture capo type raw-data interface outside match udp any host 232.4.4.4

device#

show cap capo

0 packet captured

0 packet shown
```

البيئة

المخطط:



طوبولوجيا.png

النقاط الرئيسية:

- يستخدم النظراء في مجال البث المتعدد BIDIR-PIM.
- يشير "الموجه" في هذه المقالة إلى موجه Cisco مثل CSR أو ASR.

- رادصإلا ،Cisco IOS XE جمانرب لغشت يتلا ASR1001-X يه (RP) ءاقتلالا ةطقن 17.09.08. يكمن أن تتأثر الأنظمة الأساسية الأخرى وإصدارات البرامج أيضا.
- رادصإلا ،Cisco IOS XE جمانرب لغشي يذلا C9200L-48T-4G وه (FHR) ىلوألا ةوطخلا هجوم 16.12.04. يكمن أن تتأثر الأنظمة الأساسية الأخرى وإصدارات البرامج أيضا.
- ثبلا قاطنل ةهجاو Loopback0 ىلع 10.4.4.4 (RP) ءاقتلالا ةطقن ناونع رشن متي لماكلاب ددعتملا ثبلا لاجم يف يكيمانيد لكشب 224.0.0.0/8 مادختساب هجوم نيوكت نمضتت يتلا رشنلا تايلمع رثأتت نأ نكمي امك .PIM Bootstrap (BSR) جمانرب ناونع PIM RP الثابت.

:RP ىلع PIM نيوكت

<#root>

device#

show run interface loopback0

```
interface Loopback0
 description LO0
 ip address 10.4.4.4 255.255.255.255
 ip pim sparse-mode
```

device(config)#

ip pim bidir-enable

device(config)#

ip pim bsr-candidate Loopback0 0 1

device(config)#

ip pim rp-candidate Loopback0 interval 10 priority 1 bidir

- هنأ ،يأ ،لبقتسملاب لصتم هنأ ىلع RP ضرع متي ،ةلاحلا هذه يف ،ةطاسبلا لجأ نم أيضا آخر هجوم ةوطخ (LHR). اذه إختياري.
- اضيأ رثأتت نأ نكمي .7.6.4 رادصإلا لغشي يذلا Secure Firewall 3110 وه ةيامحلا رادج ةلدعملا نامألا ةزهجأ جماربو جماربلا تارادصإو ىرخألا ةيساسألا ةيامحلا رادج ةمظنأ (ASA).
- ةوطخلا هجوم عم PIM رواجت كانهو ددعتملا ثبلا هيجوت نيكمت متي ،ةيامحلا رادج ىلع ىلوألا (FHR) و RP عم ةيناكمإ PIM BIDIR:

<#root>

device#

show run multicast-routing

```
multicast-routing

device#
show pim neighbor

Neighbor Address  Interface          Uptime    Expires DR pri Bidir
     192.168.2.1       inside             1d12h     00:01:40 1
                                                                  B
     192.168.3.1       outside            1d12h     00:01:35 1
                                                                  B
```

- على جدار الحماية، وعلى الرغم من إستخدام PIM BSR، يتم تكوين عنوان RP ل PIM يدويا. هذا تكوين متكرر. ونتيجة لذلك، يوجد تعيينان لبروتوكول rp-to-group بين المجموعة 224.0.0.0/4 وعنوان RP 10.4.4.4:

<#root>

```
device#
show run pim

pim rp-address 10.4.4.4 bidir

device#
show pim group-map

Group Range         Proto    Client    Groups RP address      Info
     224.0.1.39/32*      DM      static   0      0.0.0.0
     224.0.1.40/32*      DM      static   0      0.0.0.0
     224.0.0.0/24*       L-Local static   1      0.0.0.0
     232.0.0.0/8*        SSM     config   0      0.0.0.0
224.0.0.0/4*        BD      BSR      0      10.4.4.4   RPF: outside,192.168.3.1 <-- * means the mapping

     224.0.0.0/4         BD      config   0      10.4.4.4   RPF: outside,192.168.3.1
```

```
224.0.0.0/4          SM      static   0      0.0.0.0          RPF: ,0.0.0.0
```

قرار

قبل المتابعة تأكد من مراجعة قسم السبب.

من المتوقع أن يتم إسقاط الحزمة على جدار الحماية بسبب عدم التوافق بين التكوين المقصود (BIDIR-PIM) وحركة المرور التي تحتاج إلى المعالجة باستخدام PIM SSM.

إذا كانت التهيئة المقصودة هي BIDIR-PIM، فعليك وضع الخيارات التالية في الاعتبار:

- إستخدام مجموعات SSM غير PIM فقط.
- إذا كان يجب إستخدام مجموعات PIM SSM، فتأكد من معالجة جدار الحماية لمجموعات البث المتعدد من نطاق PIM SSM كعناوين مجموعات غير SSM. راجع قسم الأسئلة والأجوبة للحصول على مزيد من المعلومات.
- تأمل في معرف تصحيح الأخطاء من Cisco CSCwt9960.

السبب

ينتمي العنوان 232.4.4.4 إلى نطاق مجموعة البث المتعدد محدد المصدر (SSM) المحجوزة بواسطة سلطة الأرقام المعينة عبر الإنترنت (IANA). يحتفظ جدار الحماية تلقائيا بنطاق PIM SSM ل 232.0.0.0/8:

<#root>

```
device#
```

show pim group-map

```
Group Range          Proto   Client   Groups RP address      Info

     224.0.1.39/32*      DM      static   0      0.0.0.0
     224.0.1.40/32*      DM      static   0      0.0.0.0
     224.0.0.0/24*       L-Local static   1      0.0.0.0
```

```
232.0.0.0/8*        SSM     config   0      0.0.0.0

224.0.0.0/4*        BD      BSR      0      10.4.4.4   RPF: outside,192.168.3.1
224.0.0.0/4         BD      config   0      10.4.4.4   RPF: outside,192.168.3.1
      224.0.0.0/4         SM      static   0      0.0.0.0         RPF: ,0.0.0.0
```

النقاط الأساسية حول PIM SSM:

- (S، G). وهو يبني أشجارا مستندة إلى المصدر ويستعمل مسارات
- البنية الأساسية للشجرة المشتركة المستندة إلى RP لبروتوكول PIM-SM غير مطلوب. وبمعنى آخر، لا يتم إستخدام موجهات RP وأ (*، G).
- ينضم المستلمون عادة إلى شجرة البث المتعدد باستخدام بروتوكول إدارة مجموعة الإنترنت الإصدار 3 (IGMPv3) مع "تصفية المصدر"، أي قدرة النظام على الإبلاغ عن الاهتمام بتلقي الحزم فقط من عناوين مصدر محددة، أو من جميع عناوين المصدر باستثناء عناوين المصدر المحددة، التي يتم إرسالها إلى عنوان بث متعدد محدد.

النقاط الأساسية حول BIDIR-PIM:

- وهو يبني أشجارا مشتركة ثنائية الإتجاه تربط مصادر البث المتعدد وأجهزة الاستقبال.
- الأشجار ثنائية الإتجاه يتم بناؤها باستخدام آلية إختيار مرشدة محددة تعمل على كل رابط في طوبولوجيا البث المتعدد.
- بمساعدة DF، يتم إعادة توجيه بيانات البث المتعدد بشكل طبيعي من المصادر إلى المتلقين دون طلب حالة خاصة من RP وبالتالي على طول الشجرة المشتركة إلى المصدر.
- (S، G). لا يستخدم بروتوكول BIDIR-PIM أقصر مسار لأشجار المسار (SPT) وإدخالات
- يقوم أقران BIDIR-PIM ببناء أشجار مشتركة باستخدام إدخالات (*، g). يجب أن يكون هذا الإدخال لمجموعة بث متعدد معينة موجودا في جدول المسار.

BIDIR-PIM و PIM SSM من الكم أن BIDIR-PIM و PIM SSM لكل من النقاط الرئيسية لمقارنة مظهر مهام وظائف حصرية لكل منهما PIM.

في هذه الحالة، يتم تكوين مجال البث المتعدد لاستخدام BIDIR-PIM، بينما تنتمي مجموعة البث المتعدد إلى النطاق المحجوز بواسطة ANA وجدار الحماية ل PIM SSM. انظر أن مجال البث المتعدد يستخدم BIDIR-PIM، (S، G) فإن المسارات المطلوبة ل PIM SSM غير متوفرة على جدار الحماية. بسبب نقص المسارات، لا تتوفر واجهة الخروج/الصادر لحركة مرور البث المتعدد. ينتج عن غياب واجهة الخروج/الصادر عمليات إسقاط حزم في قاعدة معلومات إعادة

وأ show mfib رماوأ مادختساب طاقسإلا تايلمع نم ققحتلا نكمي .(MFIB) ددعتملا ثبلا هيجوت
show mfib count:

<#root>

```
device#

show mfib count


IP Multicast Statistics
6 routes, 3 groups, 0.00 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Other counts: Total

/RPF failed/

Other drops(OIF-null, rate-limit etc)


Group: 224.0.1.39
RP-tree:
Forwarding: 0/0/0/0, Other: 0/0/0
Group: 224.0.1.40
RP-tree:
Forwarding: 0/0/0/0, Other: 0/0/0

Group: 232.0.0.0/8


RP-tree:
Forwarding: 0/0/0/0, Other:

333797

/0/

333797
```

رادج نوكم وه اذه .(CP) مكحتلا ةطقن كارشإ لالخ نم رداصلا/جورخلا ةهجاو لح ةيامحلا رادج لواحي لثم ،مكحتلا ىوتسمو ةرادإلا فئاظو نع يسيئر لكشب لوؤسملا يويحلا ةيامحلا ةجلاعمو تاعومجملا ةرادإ/لاطعألا ىلع بلغتلاو ةرادإلا ىلإ لوصولاو هيجوتلا تالوكوتورب مزحلا ةهجوملا ىلإ ةهجاو رادج ةيامحلا ةيوانعو IP ثبلل ددعتملا امو ىلإ كلذ.

ىلع .ةجمدم ةيامح تايلآ ىلع ةيامحلا رادج يوتحي ،مكحتلا ةطقنل دئازلا ليمحتلا بنجتل ةطقن ىلإ (DP) تانايبلا ىوتسم نم ةلسرملا مزحلا لدعم ةيامحلا رادج دحي ،لاثملا ليبس لدعم دح زواجتي يذلا ASP طاقسإ ببسب لدعملا زواجتت يتلا ةمزحلا طاقسإ متي .مكحتلا.

التخفيض (Punt-rate-limit). يمكن التحقق من معدل البت في إخراج عرض asp event dp-cp punt | بدء الأمر type event:

<#root>

```
device#

show asp event dp-cp punt | begin EVENT-TYPE

EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE

punt              1264746          0  1264746        0  1264746         44

                                                  <-- 15-second punt rate

  multicast       1250020          0  1250020        0  1250020         44



  pim               14726          0    14726        0    14726          0
```

للتلخيص، يكون الاستنتاج هو أنه من المتوقع إسقاط الحزمة على جدار الحماية بسبب الحاجة إلى المعالجة التي تحتاج إلى حركة المرور (BIDIR-PIM) المقصود بين التكوين توافق عدم باستخدام PIM SSM.

أسئلة وأجوبة

في هذا القسم، يشير "الموجه" إلى موجه Cisco مثل CSR و"جدار الحماية" إلى جدران الحماية من Cisco التي تشغل ASA أو FTD.

1. س: هل يتم تلقائيا حجز جدار الحماية 232.0.0.0/8 ل PIM SSM؟

ج: نعم. على عكس الموجهات مثل CSR، على سبيل المثال، لا يتطلب تكوين محدد. على الموجهات، يحتاج نطاق PIM SSM إلى تكوين صريح:

<#root>

```
device(config)#
```

```
ip pim ssm ?

default  Use 232/8 group range for SSM

range    ACL for group range to be used for SSM
```

2. س: هل العداد "عمليات الإسقاط الأخرى" في MFIB خاص بجدار الحماية؟

ج: لا. يتواجد عداد مماثل على موجهات Cisco مع توجيه البث المتعدد.

3. س: هل سيقوم جهاز آخر مثل موجه في مكان جدار الحماية أيضا بإسقاط الحزم المرسلة إلى المجموعة 232.4.4.4؟

ج: يعتمد على كيفية معالجة الموجه للعنوان 232.4.4.4. على عكس جدران الحماية، لا تقوم الموجهات بشكل افتراضي بحجز النطاق 232.0.0.0/8 ل PIM SSM. ومع ذلك، إذا تم تمكين كل من PIM SSM و BIDIR-PIM، وكان الموجه إما RP الخاص ب BIDIR-PIM أو يتلقى تعيين RP إلى PIM SSM باستخدام عامة BIDIR ويستلم حزم البث المتعدد التي يتم إرسالها إلى نطاق مجموعة SSM، يتم إسقاط الحزم وزيادة عداد MFIB "آخر":

<#root>

```
device#

show run | i pim

ip pim bidir-enable

no ip pim autorp

ip pim ssm default

device#
```

show ip pim rp mapping

Auto-RP is not enabled
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4
RP 10.4.4.4 (?), v2,

bidir <-- mapping has the bidir flag

Info source: 10.4.4.4 (?), via bootstrap, priority 1, holdtime 150
Uptime: 17:32:39, expires: 00:02:05

device#

show ip mfib count

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Other counts: Total/RPF failed

/Other drops(OIF-null, rate-limit etc)
Default
9 routes, 6 (*,G)s, 3 (*,G/m)s
Group: 224.0.0.0/4
RP-tree,
SW Forwarding: 1/0/28/0, Other: 41037/41037/0
HW Forwarding: 3428217/0/64/0, Other: 0/0/0

Group: 232.0.0.0/8

RP-tree,

SW Forwarding: 0/0/0/0, Other: 97/97

/0 <----
HW Forwarding: 0/0/0/0, Other: 0/0/0

device#

show ip mfib count

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Other counts: Total/RPF failed

/Other drops(OIF-null, rate-limit etc)
Default
9 routes, 6 (*,G)s, 3 (*,G/m)s

```
Group: 224.0.0.0/4
RP-tree,
SW Forwarding: 1/0/28/0, Other: 41037/41037/0
HW Forwarding:   3428217/0/64/0, Other: 0/0/0
```

Group: 232.0.0.0/8

```
RP-tree,
```

```
SW Forwarding: 0/0/0/0,
```

Other: 106/106

```
/0 <----
HW Forwarding:   0/0/0/0, Other: 0/0/0
```

لاحظ أن عكس جدار الحماية مع عداد "عمليات الإسقاط الأخرى" المتزايد على الموجه، فإن العداد المتزايد هو "فشل RPF".

4. س: كيف يتم فرض جدران الحماية لمعالجة مجموعة من نطاق PIM SSM كمجموعة عناوين ليس SSM؟

ج: تأكد من أن RP يعلن عن تعيين RP إلى مجموعة للمجموعات الأكثر تحديدا من 232.0.0.0/8 (البادئة الأطول) وأن جدار الحماية قم بتكوين عنوان RP يدويا للمجموعات المحددة.

الخيار 1. التكوين على RP:

<#root>

```
device(config)#
```

access-list 1 permit host 232.4.4.4

```
device(config)#
```

ip pim rp-candidate Loopback0 group 1 interval 10 priority 1 bidir

```
<-- group refers to the access-list
```

التحقق من جدار الحماية:

```
<#root>

device#

show pim group-map 232.4.4.4

Group Range         Proto   Client   Groups RP address      Info

232.4.4.4/32*       BD

BSR      0       10.4.4.4   RPF: outside,192.168.3.1 <-- Proto is BD, not SSM
```

الخيار 2. التكوين على جدار الحماية:

```
<#root>

device(config)#

access-list mcast standard permit 232.4.4.4 255.255.255.254

device(config)#

pim rp-address 10.4.4.4 mcast bidir

device(config)#

show pim group-map 232.4.4.4

Group Range         Proto   Client   Groups RP address      Info

232.4.4.4/31*

BD

config   0       10.4.4.4   RPF: outside,192.168.3.1 <-- Proto is BD, not SSM
```

لاحظ أن قائمة الوصول يجب ألا تستخدم إدخالات المضيف أو الإدخالات ذات القناع 255.255.255.255.255.

5. س: ماذا يحدث إذا كان جدار الحماية يعالج مجموعة من نطاق PIM SSM كعنوان مجموعة غير SSM؟

ج: افترض أنه يتم التعامل مع المجموعة 232.4.4 كعنوان غير SSM (ارجع إلى السؤال 4):

```
<#root>

device#

show pim group-map 232.4.4.4

Group Range          Proto   Client   Groups RP address      Info

232.4.4.4/32*        BD

BSR      0      10.4.4.4    RPF: outside,192.168.3.1
```

إذا كان إصدار البرنامج يتأثر بمعرف تصحيح الأخطاء من Cisco [CSCwt99960](), فإن مسار (*، G) مفقود، وتتدفق ثبل المتعدد محدد المعدل بنحو 50 حزمة في الثانية. يتم إسقاط الحزم الزائدة بسبب تجاوز حد معدل النفاد (Punt-rate-limit) ASP للإفلات:

```
<#root>

device#

show mroute 232.4.4.4

No mroute entries found.

device#

show mfib 232.4.4.4 count

IP Multicast Statistics
7 routes, 4 groups, 0.00 average sources per group

Forwarding Counts
```

: Pkt Count/

Pkts per second

/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group: 232.4.4.4
RP-tree:
Forwarding: 23317/

50

/28/10, Other: 0/0/0

device#

show mfib 232.4.4.4 count

IP Multicast Statistics
7 routes, 4 groups, 0.00 average sources per group

Forwarding Counts:

Pkt Count/

Pkts per second

/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group: 232.4.4.4
RP-tree:
Forwarding: 23540/

49

/28/10, Other: 0/0/0

device#

capture capi interface inside trace match udp any host 232.4.4.4

device#

show capture capi trace | i Drop-reason

```
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (NA
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (NA
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (NA
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (NA
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (NA
```

```
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (NA
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (NA
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (NA
                                                                                                      …
```

أحلت ل كثير معلومة ال cisco بق id CSCwt9960.

المحتوى ذي الصلة

- كتلة البث المتعدد الخاصة بالمصدر
- معرف تصحيح الأخطاء من Cisco CSCwt99960

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).