تكوين جدار الحماية المستند إلى المنطقة (ZBFW) في موقع مشترك مع مؤسسة عنصر الحدود الموحد (CUBE) من Cisco

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين جدار الحماية المستند إلى المنطقة (ZBFW) في موقع مشترك مع مؤسسة عنصر الحدود الموحد (CUBE) من Cisco.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

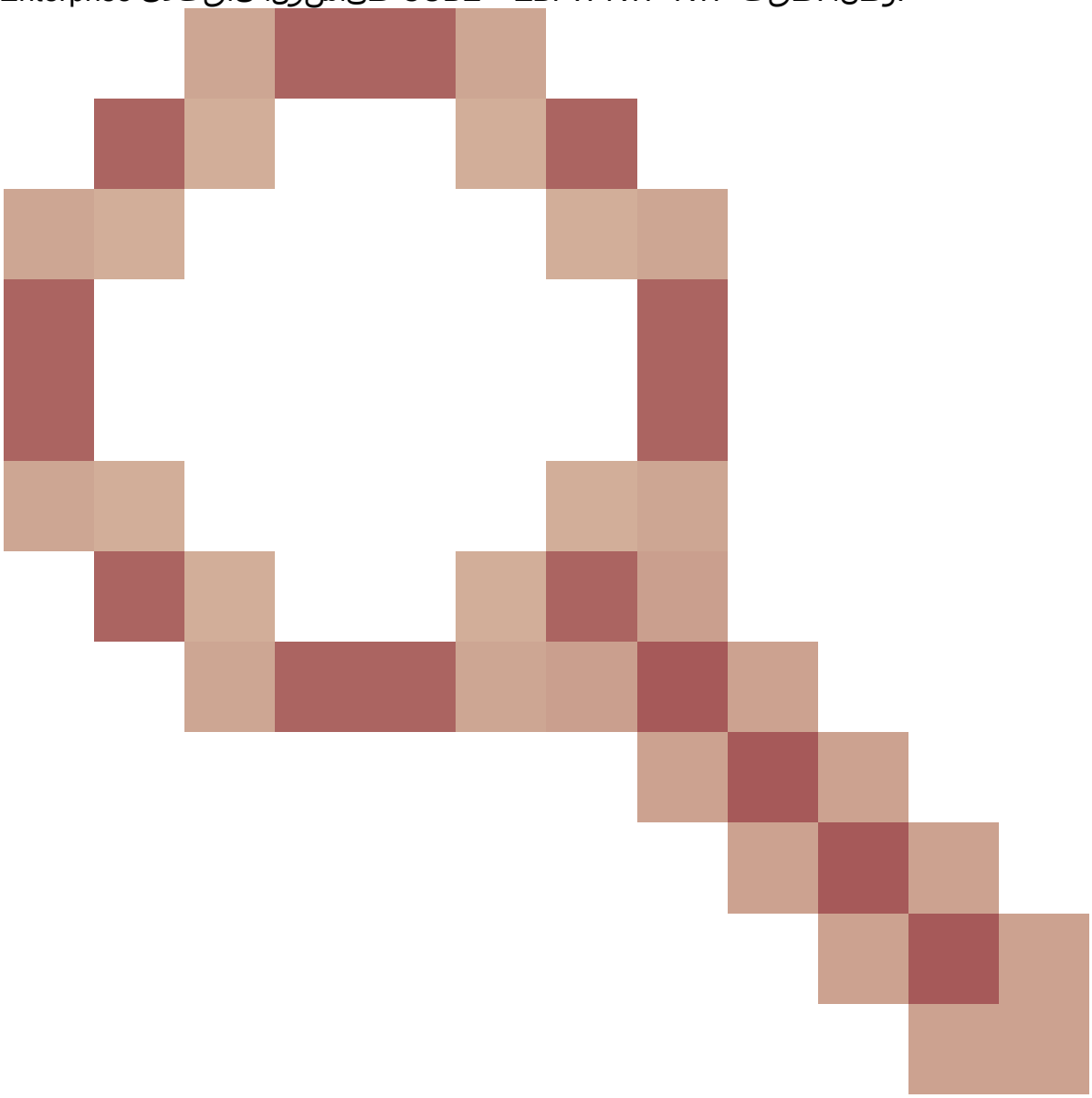
- موجه Cisco الذي يشغل برنامج Cisco IOS® XE 17.10.1a

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

معلومات أساسية

- لم يتم دعم الموقع المشترك ل Cube Enterprise و ZBFW على Cisco IOS XE حتى 16.7.1+

- يدعم CUBE Enterprise تدفقات الوسائط CUBE + ZBFW RTP-RTP فقط. انظر:



CSCwe66293

- ال ينطبق هذا المستند على وكيل الوسائط CUBE أو مزود خدمة CUBE أو بوابات MGCP أو SCCP أو بوابات Cisco SRST أو ESRST أو بوابات H323 أو البوابات الصوتية التناظرية/TDM الأخرى.

- للاطلاع على بوابات الصوت TDM/التناظرية و ZBFW، راجع المستند التالي: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/213550-troubleshoot-one-way-audio-problems-in-f.html

الرسم التخطيطي للشبكة

سيوضح تكوين النموذج وحدتي تقسيم منطقتين للشبكة مسماتين داخل الشبكة وخارجها.

يحتوي الداخل على شبكة IP واحدة ويتضمن الخارج شبكتين IP.

مخطط شبكة الطبقة 3

```
Endpoint_A - Network A - Gig1 - CUBE - Gig3 - Network B - CUCM
                                          \_ Network C - Endpoint_B
```

تدفق المكالمات من المستوى 7

```
Call Direction ======================================>
Endpoint_A > SIP > CUBE > SIP > CUCM > SIP > Endpoint_B
```

تدفق وسائط من المستوى السابع

```
Endpoint_A <> RTP <> CUBE <> RTP <> Endpoint_B
```

مفاهيم مسار اصطدام ZBFW

- عند تكوين ZBFW، تقوم بتكوين اسم منطقة أمان يتم تعريفه بعد ذلك على واجهة. بعد هذا كله حركة مرور إلى/من أن قارن يقترن مع ذلك منطقة إسم.
  - يسمح دائما بحركة المرور من/إلى نفس المنطقة.
  - يتم إسقاط حركة المرور إلى/من مناطق مختلفة ما لم يسمح بها تكوين المسؤول.
- لتحديد تدفقات حركة المرور المسموح بها، يجب إنشاء تعيين منطقة عبر تكوين زوج منطقة أحادي الإتجاه الذي يحدد أسماء مناطق المصدر والوجهة.
  - وبعد ذلك يرتبط تعيين زوج المنطقة هذا بنهج خدمة يستخدم لتوفير تحكم متعدد المستويات لأنواع حركة المرور التي تم فحصها والسماح بها وغير المسموح بها.
- تعمل CUBE Enterprise في المنطقة الذاتية الخاصة. تتضمن المنطقة الذاتية حركة مرور أخرى إلى الموجه/منه مثل ICMP و SSH و NTP و DNS، وما إلى ذلك.
  - لا يوجد PVDM الخاص بالجهاز للاستخدام مع CUBE LTI في المنطقة الذاتية ويجب

تعيينه إلى منطقة تم تكوينها إدارياً.

- يسمح ZBFW بحركة المرور العائدة تلقائياً لذلك يجب على المسؤول تكوين أزواج المناطق لتعريف حركة المرور العائدة.

مع وضع النقاط الثلاث التالية في الاعتبار، يمكن إضافة المناطق التالية بشكل مبهج على شبكة L3 الخاصة بنا حيث:

- الشبكة a، gig1 هي المنطقة الخارجية
- توجد الشبكة B والشبكة C و Gig3 داخل المنطقة
- المكعب هو جزء من المنطقة الذاتية

```
      _______OUTSIDE_______                 ______INSIDE______
     |                      |              |                  |
Endpoint_A - Network A - Gig1 - CUBE - Gig3 - Network B - CUCM
                                 |         \_ Network C - Endpoint_B
                               SELF
```

بعد ذلك يمكننا إنشاء أربع تعيينات لزوج مناطق أحادي الإتجاه نحتاج إليها لحركة مرور البيانات عبر CUBE+ZBFW:

المصدر	الوجهة	الاستخدام
خارج	ذاتي	وسائط SIP و RTP الواردة من نقطة النهاية A
ذاتي	داخل	وسائط SIP و RTP الصادرة من CUBE إلى CUCM ونقطة النهاية B.
داخل	ذاتي	وسائط SIP و RTP الواردة من CUCM ونقطة النهاية B.
ذاتي	خارج	وسائط SIP و RTP الصادرة من CUBE إلى نقطة النهاية A.

بوضع هذه المفاهيم في الاعتبار، يمكننا بدء تكوين ZBFW على عمل الموجه Cisco IOS XE كمكعب.

التكوينات

تحديد مناطق الأمان

تذكر أنك بحاجة إلى تكوين منطقتين للأمان: داخل وخارج. الواجهات التي لا يلزم تعريفها على أنها افتراضية.

```
!
zone security INSIDE
zone security OUTSIDE
!
```

إنشاء قائمة وصول وخريطة فئة وخريطة سياسة لحركة المرور الموثوق بها

للتحكم في حركة المرور التي يجب علينا تكوين الأسلوب للموجه لمطابقتها والسماح بها.

للقيام بذلك، سنقوم بإنشاء قائمة وصول موسعة وخريطة فئة ومخطط سياسة لفحص حركة المرور الخاصة بنا.

من أجل التبسيط سننشئ سياسة لكل منطقة توقع بتعييني كل من حركة المرور الواردة والصادرة.

لاحظ أنه قد يتم إستخدام التكوينات مثل SIP لبروتوكول المطابقة وSIP-TLS لبروتوكول المطابقة ولكن ألأغراض توضيحية، تم تكوين IP/Ports

خارج قائمة الوصول الموسعة، خريطة الفئة، خريطة السياسة

<#root>

```
! Define Access List with ACLs for OUTSIDE interface


ip access-list extended TRUSTED-ACL-OUT
 10 remark Match SIP TCP/UDP 5060 and TCP TLS 5061
 11 permit tcp 192.168.1.0 0.0.0.255 any range 5060 5061
 12 permit tcp any 192.168.1.0 0.0.0.255 range 5060 5061
 13 permit udp 192.168.1.0 0.0.0.255 any eq 5060
 14 permit udp any 192.168.1.0 0.0.0.255 eq 5060
 !
 20 remark Match RTP Port Range, IOS-XE and Remote Endpoints
 21 permit udp 192.168.1.0 0.0.0.255 any range 8000 48198
 22 permit udp any 192.168.1.0 0.0.0.255 range 8000 48198
!

! Tie ACL with Class Map


class-map type inspect match-any TRUSTED-CLASS-OUT
 match access-group name TRUSTED-ACL-OUT
!

! Tie Class Map with Policy and inspect


policy-map type inspect TRUSTED-POLICY-OUT
 class type inspect TRUSTED-CLASS-OUT
```

```
  inspect
 class class-default
  drop log
!
```

داخل قائمة الوصول الموسعة، خريطة الفئة، خريطة السياسة

```
!
ip access-list extended TRUSTED-ACL-IN
 1 remark SSH, NTP, DNS
 2 permit tcp any any eq 22
 3 permit udp any any eq 123
 4 permit udp any any eq 53
 !
 10 remark Match SIP TCP/UDP 5060 and TCP TLS 5061
 11 permit tcp 192.168.2.0 0.0.0.255 any range 5060 5061
 12 permit tcp any 192.168.2.0 0.0.0.255 range 5060 5061
 13 permit udp 192.168.2.0 0.0.0.255 any eq 5060
 14 permit udp any 192.168.2.0 0.0.0.255 eq 5060
 !
 20 remark Match RTP Port Range, IOS-XE and Remote Endpoints
 21 permit udp 192.168.2.0 0.0.0.255 any range 8000 48198
 22 permit udp any 192.168.2.0 0.0.0.255 range 8000 48198
 23 permit udp 192.168.3.0 0.0.0.31 any range 8000 48198
 24 permit udp any 192.168.3.0 0.0.0.31 range 8000 48198
!
class-map type inspect match-any TRUSTED-CLASS-IN
 match access-group name TRUSTED-ACL-IN
!
policy-map type inspect TRUSTED-POLICY-IN
 class type inspect TRUSTED-CLASS-IN
  inspect
 class class-default
  drop log
!
```

إنشاء تعييناتزوج منطق

بعد ذلك يجب إنشاء تعييناتزوج منطق الأربعة التي تمت مناقشتها مسبقا في الجدول.

ستشير أزواج المنطق هذه إلى سياسة خدمة تم إنشاؤها سابقا في خريطة السياسة.

<#root>

```
! INSIDE <> SELF


zone-pair security IN-SELF source INSIDE destination self
 service-policy type inspect TRUSTED-POLICY-IN
zone-pair security SELF-IN source self destination INSIDE
 service-policy type inspect TRUSTED-POLICY-IN
!
```

```
! OUTSIDE <> SELF


zone-pair security OUT-SELF source OUTSIDE destination self
 service-policy type inspect TRUSTED-POLICY-OUT
zone-pair security SELF-OUT source self destination OUTSIDE
 service-policy type inspect TRUSTED-POLICY-OUT
!
```

تعيين مناطق للواجهات

<#root>

```
! Assign Zones to interfaces


int gig1
 zone-member security INSIDE
!
int gig3
 zone-member security OUTSIDE
!
```

التحقق من الصحة

نموذج تدفق حزم البيانات - الاتصال

عند هذه النقطة، ستقوم مكالمة من نقطة النهاية B إلى CUBE موجهة ل CUCM باستدعاء التسلسل التالي:

1. سوف تدخل حزمة TCP SIP الواردة إلى المكعب على 5060 gig 1 ويتم تعيينها إلى منطقة مصدر خارجية
2. يعمل المكعب في المنطقة الذاتية وبالتالي سيتم إستخدام زوج المناطق من الخارج إلى المنطقة الذاتية (خارج-self)
3. سيتم إستخدام خرج السياسة الموثوق بها ل service-policy/map لفحص حركة المرور استنادا إلى قائمة الوصول الموثوق بها للفئة out وقائمة الوصول للخرج الموثوق بها
4. سيستخدم CUBE بعد ذلك منطق توجيه المكالمات المحلي لتحديد مكان إرسال المكالمة وواجهة الخروج التي سيتم إستخدامها. في هذا مثال مخرج قارن يكون gig 3 ل CUCM.
    1. ارجع إلى هذا المستند للحصول على نظرة عامة على توجيه المكالمات عبر المكعب: https://www.cisco.com/c/en/us/support/docs/voice/ip-telephony-voice-over-ip-voip/211306-In-Depth-Explanation-of-Cisco-IOS-and-IO.html
5. سيقوم المكعب بإنشاء مأخذ توصيل TCP جديد ودعوة SIP الكاملة المصادر من Gig 3 (في الداخل). يعمل المكعب في المنطقة الذاتية لذلك سوف يستخدم زوج مناطق الإخراج الذاتي
6. سيتم إستخدام قائمة الوصول الموثوق بها ل نهج الخدمة/تعيين السياسة الموثوق

بها لفحص حركة المرور استنادا إلى قائمة الوصول الموثوق بها من الفئة Class-Map وقائمة الوصول إلى قائمة التحكم في الوصول (ACL) الموثوق بها
7. لحركة المرور العائدة في منطقة الدخول والمخرج الذاتي هذا لإرسال استجابات للاستدعاء.

إظهار الأوامر

show zone-pair security

- سيظهر هذا الأمر جميع تعيينات زوج المنطقة ونهج الخدمة المطبق.
- المصدر، غاية الكلمة المفتاح يستطيع كنت استعملت أن يعين خاص منطقة-زوج، تعيين أن يتحقق إن يتواجد كثير.

<#root>

Router#

show zone-pair security

```
Zone-pair name IN-SELF 2
    Source-Zone INSIDE Destination-Zone self
    service-policy TRUSTED-POLICY-IN
Zone-pair name OUT-SELF 4
    Source-Zone OUTSIDE Destination-Zone self
    service-policy TRUSTED-POLICY-OUT
Zone-pair name SELF-IN 5
    Source-Zone self Destination-Zone INSIDE
    service-policy TRUSTED-POLICY-IN
Zone-pair name SELF-OUT 6
    Source-Zone self Destination-Zone OUTSIDE
    service-policy TRUSTED-POLICY-OUT
```

Router#

show zone-pair security source INSIDE destination self

```
Zone-pair name IN-SELF 2
    Source-Zone INSIDE Destination-Zone self
    service-policy TRUSTED-POLICY-IN
```

show call active voice compact

- سيظهر هذا الأمر إتصالات الوسائط البعيدة من منظور CUBE>

<#root>

Router#

show call active voice com | i NA|VRF

```
       <callID> A/O FAX   T<sec>  Codec       type        Peer Address   IP R:<ip>:<udp>
```

```
      467      ANS      T2       g711ulaw    VOIP        Psipp          192.168.1.48:16384
      468      ORG      T2       g711ulaw    VOIP        P8675309       192.168.3.59:16386           NA
```

إظهار إتصالات voip rtp

- يعرض هذا الأمر معلومات اتصال الوسائط البعيدة والمحلية من منظور CUBE

<#root>

```
Router#
```

show voip rtp con | i NA|VRF

```
No. CallId     dstCallId  LocalRTP RmtRTP   LocalIP                                    RemoteIP
1     467        468        8120     16384    192.168.1.12                                192.168.1.48
2     468        467        8122     16386    192.168.2.58                               192.168.3.59
```

إظهار ملخص الصوت النشط

- هذا الأمر، بالاقتران مع أمر "حالات السواد للوسائط" الذي تم تكوينه عبر خدمة الصوت VoIP، سيظهر إحصائيات الإرسال (TX) والتلقي (RX) لأرجل الاتصال.
- إذا كانت الوسائط تتدفق من خلال المكعب و ZBFW، يجب أن يطابق TX مع RX على ساق إستدعاء النظير. على سبيل المثال، 109 TX و 109 RX

<#root>

```
Router#
```

show call active voice br | i dur

```
 dur 00:00:03 tx:107/24156 rx:109/24592 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 dur 00:00:03 tx:109/24592 rx:107/24156 dscp:0 media:0 audio tos:0xB8 video tos:0x0
```

عرض تفاصيل TCP لاتصالات SIP-UA

- يعرض هذا الأمر تفاصيل اتصال SIP TCP النشط من خلال CUBE
- يمكن إستخدام رموز مثل show sip-ua connections udp detail أو show sip-ua connections tcp tls detail لإظهار نفس التفاصيل ل UDP SIP و TCP-TLS

<#root>

```
Router#
```

show sip-ua connections tcp detail

```
Total active connections      : 2
[..truncated..]
Remote-Agent:192.168.3.52, Connections-Count:1
```

```
  Remote-Port Conn-Id Conn-State  WriteQ-Size            Local-Address                Tenant
  =========== ======= =========== =========== ======================================= ======
         5060      51 Established           0 192.168.2.58:51875                         0

Remote-Agent:192.168.1.48, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size            Local-Address                Tenant
  =========== ======= =========== =========== ======================================= ======
        33821      50 Established           0 192.168.1.12:5060                          0
[..truncated..]
```

إظهار النظام الأساسي لجلسات جدار الحماية الخاص بالسياسات

- سيظهر هذا الأمر المكلمة من منظور ZBFW.
- ستكون هناك جلسات عمل SIP والتدفقات الفرعية لـ RTP و RTCP.
- يمكن إستخدام معرف جلسة العمل من هذا الإخراج عند تصحيح أخطاء ZBFW لاحقا.
- يمكن إستخدام تفاصيل النظام الأساسي لجلسات عمل جدار الحماية الخاصة بالسياسات لعرض مزيد من البيانات.

<#root>

```
Router#
```

show policy-firewall sessions platform

```
--show platform hardware qfp active feature firewall datapath scb any any any any any all any --
[s=session  i=imprecise channel c=control channel  d=data channel u=utd inspect A/D=appfw action allow/
Session ID:0x000000A8 192.168.2.58 51875 192.168.3.52 5060 proto 6 (-global-:0:-global-:0) (0x16:sip) [
 +-Session ID:0x000000AA 192.168.2.58 0 192.168.3.52 5060 proto 6 (-global-:0:-global-:0) (0x16:sip)  [
 +-Session ID:0x000000A9 192.168.3.52 0 192.168.2.58 5060 proto 6 (-global-:0:-global-:0) (0x16:sip)  [
Session ID:0x000000AC 192.168.3.59 16386 192.168.2.58 8122 proto 17 (-global-:0:-global-:0) (0x2:udp) [
Session ID:0x000000AD 192.168.1.48 16384 192.168.1.12 8120 proto 17 (-global-:0:-global-:0) (0x3a:sip r
Session ID:0x000000A6 192.168.1.48 33821 192.168.1.12 5060 proto 6 (-global-:0:-global-:0) (0x16:sip)
 +-Session ID:0x000000AE 192.168.1.48 16385 192.168.1.12 8121 proto 17 (-global-:0:-global-:0) (0x3a:si
 +-Session ID:0x000000AD 192.168.1.48 16384 192.168.1.12 8120 proto 17 (-global-:0:-global-:0) (0x3a:si
 +-Session ID:0x000000AB 192.168.1.48 0 192.168.1.12 5060 proto 6 (-global-:0:-global-:0) (0x16:sip)
 +-Session ID:0x000000A7 192.168.1.12 0 192.168.1.48 5060 proto 6 (-global-:0:-global-:0) (0x16:sip)
```

show policy-map type فحص جلسات زوج المنطقة

- يعرض هذا الأمر بيانات مماثلة مثل النظام الأساسي لجلسات جدار حماية السياسة ومع ذلك يتم تضمين تعيين زوج المناطق أيضا في الإخراج الذي يكون مفيدا لتصحيح الأخطاء.

```
Router# show policy-map type inspect zone-pair sessions | i Zone-pair|Session ID
  Zone-pair: IN-SELF
        Session ID 0x000000AD (192.168.1.48:16384)=>(192.168.1.12:8120) sip-RTP-data SIS_OPEN
        Session ID 0x000000A6 (192.168.1.48:33821)=>(192.168.1.12:5060) sip SIS_OPEN
        Session ID 0x000000A7 (192.168.1.12:0)=>(192.168.1.48:5060) sip SIS_PREGEN
        Session ID 0x000000AE (192.168.1.48:16385)=>(192.168.1.12:8121) sip-RTP-data SIS_PREGEN
        Session ID 0x000000AB (192.168.1.48:0)=>(192.168.1.12:5060) sip SIS_PREGEN
```

```
Zone-pair: OUT-SELF
       Session ID 0x000000AC (192.168.3.59:16386)=>(192.168.2.58:8122) udp SIS_OPEN
Zone-pair: SELF-IN
Zone-pair: SELF-OUT
       Session ID 0x000000A8 (192.168.2.58:51875)=>(192.168.3.52:5060) sip SIS_OPEN
       Session ID 0x000000AA (192.168.2.58:0)=>(192.168.3.52:5060) sip SIS_PREGEN
       Session ID 0x000000A9 (192.168.3.52:0)=>(192.168.2.58:5060) sip SIS_PREGEN
```

استكشاف الأخطاء وإصلاحها

يمكن العثور على جدار الحماية المستند إلى منطقة Cisco IOS XE لاستكشاف الأخطاء وإصلاحها في هذا المستند:

https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/117721-technote-iosfirewall-00.html

واجهة الترميز المحلي للمكعب (LTI) + ZBFW

- عند تكوين CUBE باستخدام موارد PVDM الخاصة بالأجهزة على اللوحة الأم أو وحدة واجهة الشبكة (NIM)، يمكن إستخدامها لأغراض CUBE LTI.
- تحتوي واجهة اللوحة الخلفية لـ PVDM على محرك خدمة ثابت فئة x/y/z يتوافق مع وضع PVDM. على سبيل المثال، محرك الخدمة 0/4 هو فتحة PVDM/DSP باللوحة الأم.
- يجب تكوين محرك الخدمة هذا باستخدام منطقة والا يوجد في المنطقة الذاتية.

سيقوم التكوين التالي بتعيين محرك الخدمة المستخدم بواسطة CUBE LTI إلى المنطقة الداخلية لأغراض ZBFW.

```
!
interface Service-Engine0/4/0
 zone-member security INSIDE
!
```

يمكن إستخدام منطق مماثل لتعيين زوج منطقة محرك الخدمة لموارد وسائط SCCP المستندة إلى PVDM/DSP للأجهزة وواجهة ربط SCCP ومع ذلك فإن هذا الموضوع يقع خارج نطاق هذا المستند.

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).