تكوين ZBFW من قالب واجهة سطر الأوامر SD-WAN

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين نهج جدار الحماية المستند إلى المنطقة (ZBFW) باستخدام قالب ميزة واجهة سطر الأوامر (CLI) الإضافية من Cisco Catalyst SD-WAN Manager.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- شبكة منطقة واسعة معرفة ببرنامج Cisco Catalyst (SD-WAN)
- التشغيل الأساسي لجدار الحماية المستند إلى المنطقة (ZBFW)

المكونات المستخدمة

- مدير Cisco Catalyst SD-WAN 20.9.3.2
- Cisco IOS® XE Catalyst SD-WAN Edges 17.6.5a

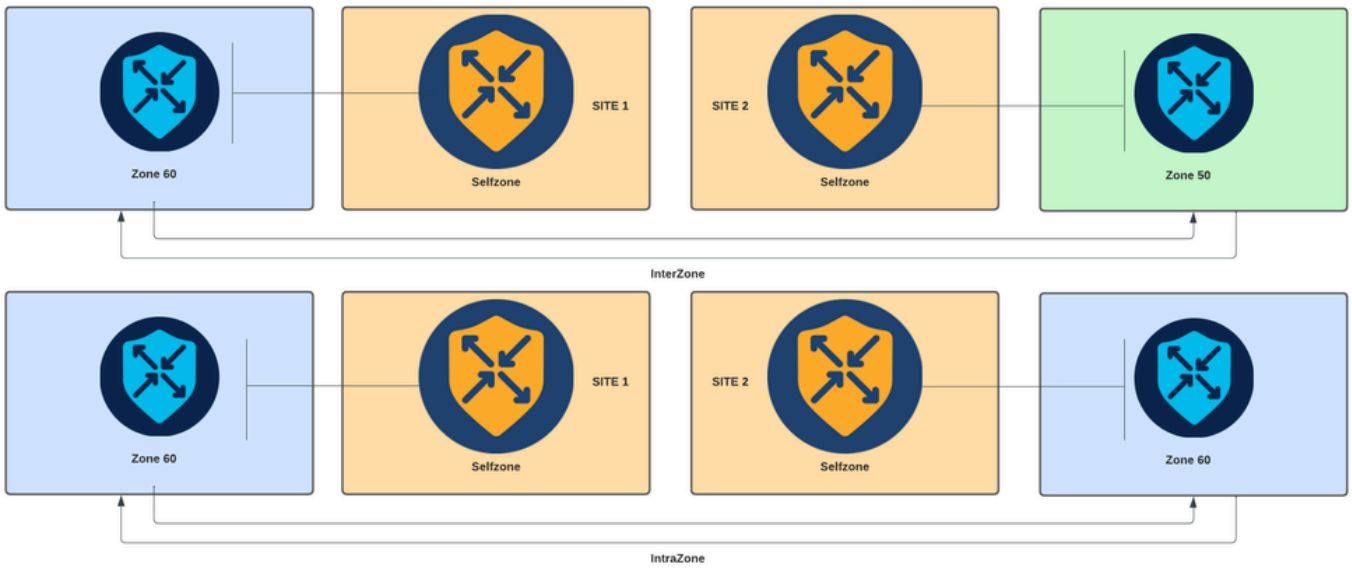
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

سياسة جدار الحماية هي نوع من نهج الأمان المحلي الذي يسمح بفحص حركة مرور بيانات TCP و UDP و ICMP حسب الحالة. وتستخدم مفهوم المناطق؛ وبالتالي، يسمح لتدفقات حركة المرور التي تنشأ في منطقة معينة بالمضي إلى منطقة أخرى استنادا إلى السياسة بين المنطقتين.

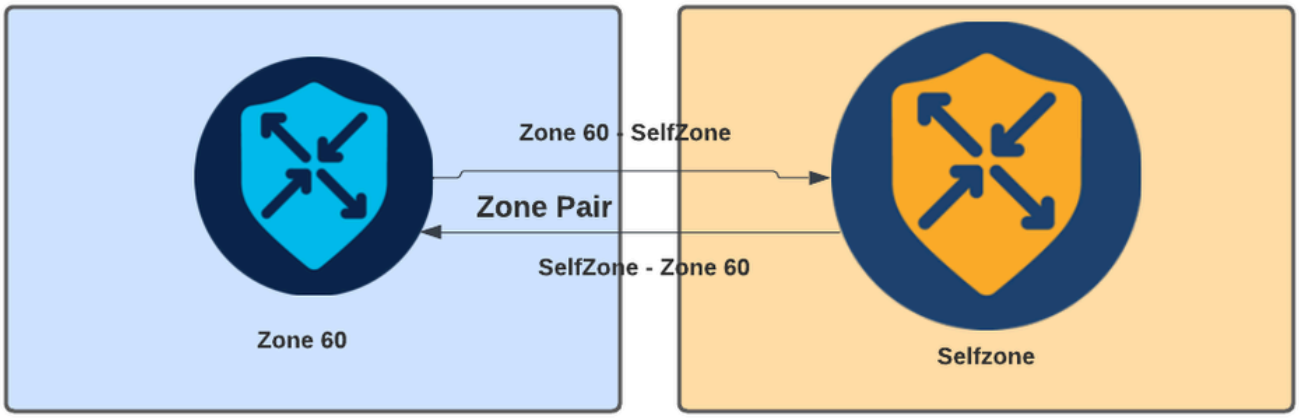
المنطقة هي مجموعة من واحدة أو أكثر من شبكات VPN. نوع المناطق الموجودة على ZBFW هي:

- منطقة المصدر: مجموعة من شبكات VPN تقوم بإنشاء تدفقات حركة مرور البيانات. يمكن أن تكون شبكة VPN جزءا من منطقة واحدة فقط.
- منطقة الوجهة: مجموعة من شبكات VPN التي تنهي تدفقات حركة مرور البيانات. يمكن أن تكون شبكة VPN جزءا من منطقة واحدة فقط.
- Interzone: ويطلق عليها اسم Interzone عند تدفق حركة المرور بين المناطق المختلفة (يتم رفض الاتصال بشكل افتراضي).
- داخل المنطقة: ويتم استدعاؤها ضمن المنطقة عندما تتدفق حركة المرور عبر نفس المنطقة (بشكل افتراضي، يتم السماح بالاتصالات).
- Selfzone: يتم إستخدامها للتحكم في حركة المرور التي يتم الحصول عليها من الموجه نفسه أو توجيهها إليه (المنطقة الافتراضية التي تم إنشاؤها وتكوينها مسبقا بواسطة النظام، ويتم السماح بالاتصالات بشكل افتراضي).



الرسم التخطيطي لجدار الحماية المستند إلى المنطقة

هناك مفهوم آخر مستخدم في ZBFW وهو زوج المنطقة، وهو حاوية تربط منطقة مصدر بمنطقة الوجهة. تطبق أزواج المناطق سياسة جدار حماية على حركة المرور التي تتدفق بين المنطقتين.



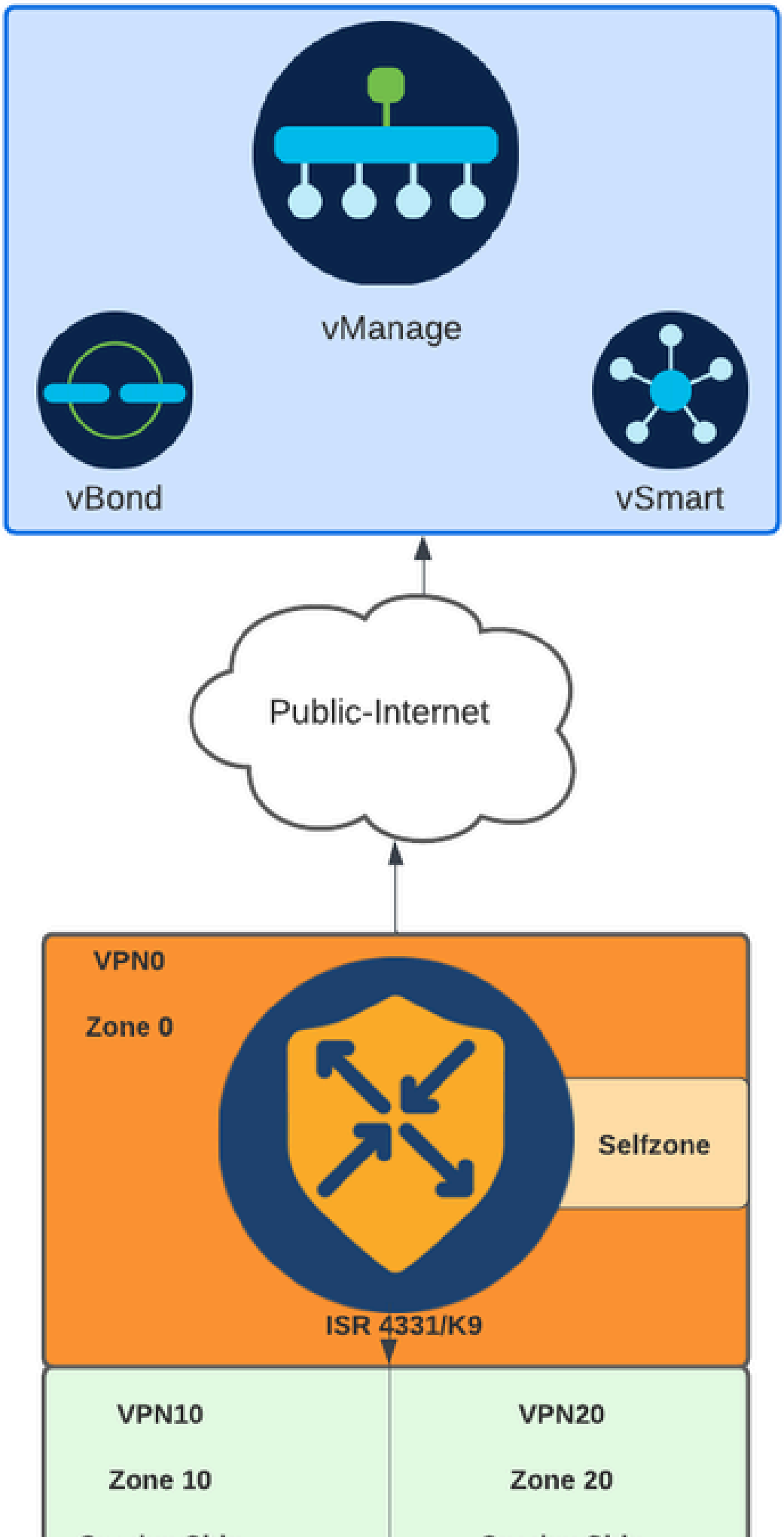
مثال زوج مناطق

بعد تعريف زوج المنطقة، تكون الإجراءات التي تنطبق على التدفقات هي:

- إسقاط: ببساطة يتجاهل تدفق المطابقة.
- Pass: يسمح بتدفق الحزمة بدون فحص الحالة، مماثل للإجراء المسموح به في قوائم الوصول. سواء تم تعيين إجراء تمرير في التدفق، يلزم تمرير إرجاع لذلك التدفق.
- فحص: يسمح بالتفحص الذي يحدد حالة حركة المرور التي تتدفق من منطقة المصدر إلى منطقة الوجهة، ويسمح تلقائيا بتدفقات حركة المرور بالرجوع.

التكوين

الرسم التخطيطي للشبكة


vManage
vBond
vSmart
Public-Internet
VPN0
Zone 0
Selfzone
ISR 4331/K9
VPN10
Zone 10
VPN20
Zone 20

ليتم تطبيقه في مستوى البيانات. ومع ذلك، يلزم التأكد من تكوين مستوى التحكم والسماح للجهاز بالاتصال بوحدات التحكم في SD-WAN لبناء إتصالات التحكم.

ملاحظة: ما إذا شكلت قارن WAN يكون عبر DHCP، وه ضروري أن يخلق قاعدة أن يسمح المنطقة الذاتية (قارن) أن يبلغ الخطوة التالي عنوان في حالة ما إذا أداة إعادة تحميل والموجه يحتاج أن يحصل عنوان جديد.

مستوى التحكم

1. قم بإنشاء خريطة معلمة الفحص:

```
parameter-map type inspect-global
multi-tenancy
vpn zone security
 alert on
 log dropped-packets
 max-incomplete tcp timeout
```

يتم إستخدام max-incomplete tcp
أمر التكوين لتحديد الحد الأقصى لعدد الاتصالات غير المكتملة قبل إسقاط جلسة عمل TCP.

أمر **multi-tenancy** التكوين عبارة عن معلمة عامة مطلوبة في تكوين ZBFW. عند تكوين ZBFW عبر واجهة المستخدم الرسومية SD-WAN Manager، تتم إضافة الخط بشكل افتراضي. عندما يتم تكوين ZBFW عبر واجهة سطر الأوامر (CLI)، يلزم إضافة هذا السطر.

2. إنشاء منطقة شبكة WAN:

```
zone security wan
vpn 0
```

ملاحظة: يتم إنشاء المنطقة الذاتية بشكل افتراضي، وليس من الضروري تكوينها.

---

3. قم بتكوين مجموعة الكائنات لعناوين المصدر والوجهة:

```
object-group network CONTROLLERS
 host 172.18.121.103
 host 172.18.121.106
 host 192.168.20.152
 host 192.168.22.203
object-group network WAN_IPs
 host 10.122.163.207
```

4. إنشاء قائمة الوصول إلى IP:

```
ip access-list extended self-to-wan-acl
 10 permit tcp object-group WAN_IPs object-group CONTROLLERS
 20 permit udp object-group WAN_IPs object-group CONTROLLERS
 30 permit ip object-group WAN_IPs object-group CONTROLLERS
ip access-list extended wan-to-self-acl
 10 permit tcp object-group CONTROLLERS object-group WAN_IPs
 20 permit udp object-group CONTROLLERS object-group WAN_IPs
 30 permit ip object-group CONTROLLERS object-group WAN_IPs
```

5. قم بإنشاء خريطة الفئة:

```
class-map type inspect match-all self-to-wan-cm
 match access-group name self-to-wan-acl
class-map type inspect match-all wan-to-self-cm
 match access-group name wan-to-self-acl
```

6. قم بإنشاء خريطة السياسة لإضافتها إلى زوج المناطق:

```
policy-map type inspect wan-to-self-pm
 class type inspect wan-to-self-cm
  inspect
 class class-default
policy-map type inspect self-to-wan-pm
 class type inspect self-to-wan-cm
  inspect
 class class-default
```

7. قم بإنشاء زوج المنطقة وربط خريطة السياسة به:

```
zone-pair security self-to-wan source self destination wan
 service-policy type inspect self-to-wan-pm
zone-pair security wan-to-self source wan destination self
 service-policy type inspect wan-to-self-pm
```

بمجرد السماح بتدفق مستوى التحكم، يمكن تطبيق تكوين مستوى البيانات.

للتحقق من صحة إتصالات التحكم، أستخدم أمر EXEC:

<#root>

```
Device#
```

show sdwan control connections

سواء لم يتم تكوين ZBFW للمنطقة الذاتية ومنطقة wan-zone بشكل صحيح، تفقد الأجهزة إتصالات التحكم وتحصل على خطأ وحدة تحكم مماثل للخطأ التالي:

<#root>

Oct 30 19:44:17.731: %IOSXE-6-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000 TS:00000004865486441431 %FW-6-

مستوى البيانات

1. إنشاء منطقة أمان لكل عملية توجيه وإعادة توجيه ظاهرية (VRF) مطلوبة:

```
zone security user
vpn 10
zone security server
vpn 20
```

3. قم بتكوين مجموعة الكائنات لعناوين المصدر والوجهة:

```
 object-group network USER
 host 10.10.10.1
 host 10.10.10.2
 host 10.10.10.3
object-group network SERVER
 host 10.20.20.1
 host 10.20.20.2
```

4. إنشاء قائمة الوصول إلى IP:

```
ip access-list extended user-to-server-acl
 10 permit tcp object-group USER object-group SERVER
 20 permit udp object-group USER object-group SERVER
 30 permit ip object-group USER object-group SERVER
ip access-list extended server-to-user-acl
 10 permit tcp object-group SERVER object-group USER
 20 permit udp object-group SERVER object-group USER
 30 permit ip object-group SERVER object-group USER
```

5. قم بإنشاء خريطة الفئة:

```
class-map type inspect match-all user-to-server-cm
 match access-group name user-to-server-acl
class-map type inspect match-all server-to-wan-cm
 match access-group name server-to-user-acl
```

6. قم بإنشاء خريطة السياسة لإضافتها إلى زوج المناطق:

```
policy-map type inspect user-to-server-pm
 class type inspect user-to-server-cm
  inspect
 class class-default
policy-map type inspect server-to-user-pm
 class type inspect server-to-user-cm
  inspect
 class class-default
```

7. قم بإنشاء زوج المنطقة وربط خريطة السياسة به:

```
zone-pair security user-to-server source user destination server
 service-policy type inspect user-to-server-pm
zone-pair security server-to-user source server destination user
 service-policy type inspect server-to-user-pm
```

ملاحظة: للحصول على مزيد من المعلومات حول إستخدام قوالب واجهة سطر الأوامر، راجع قوالب ميزة الوظيفة الإضافية ل CLI وقوالب واجهة سطر الأوامر.

التحقق من الصحة

للتحقق من صحة خريطة الفئة التي تم تكوينها، أستخدم أمر EXEC:

<#root>

Device#

show class-map type inspect

للتحقق من صحة خريطة السياسة التي تم تكوينها، أستخدم أمر EXEC:

```
<#root>

Device#

show policy-map type inspect
```

للتحقق من صحة زوج المناطق الذي تم تكوينه، أستخدم أمر EXEC:

```
<#root>

Device#

show zone-pair security
```

للتحقق من صحة قائمة الوصول التي تم تكوينها، أستخدم أمر EXEC:

```
<#root>

Device#

show ip access-list
```

للتحقق من صحة مجموعة الكائنات التي تم تكوينها، أستخدم أمر EXEC:

```
<#root>

Device#

show object-group
```

لعرض حالة جلسة عمل ZBFW، أستخدم أمر EXEC:

```
<#root>

Device#

show sdwan zonebfwdp sessions

 SRC DST TOTAL TOTAL UTD
SESSION SRC DST SRC DST VPN VPN NAT INTERNAL INITIATOR RESPONDER APPLICATION POLICY
ID STATE SRC IP DST IP PORT PORT PROTOCOL VRF VRF ID ID ZP NAME CLASSMAP NAME FLAGS FLAGS BYTES BYTES T
----------------------------------------------------------------------------------------------------

8 open 172.18.121.106 10.122.163.207 48960 32168 PROTO_L4_UDP 0 0 0 65534 wan-to-self wan-to-self-cm - 0


5 open 10.122.163.207 172.18.121.106 32168 32644 PROTO_L4_UDP 0 0 65534 0 self-to-wan self-to-wan-cm - 0

7 open 10.122.163.207 172.18.121.103 32168 32168 PROTO_L4_UDP 0 0 65534 0 self-to-wan self-to-wan-cm - 0
```

```
6 open 172.18.121.106 10.122.163.207 60896 32168 PROTO_L4_UDP 0 0 0 65534 wan-to-self wan-to-self-cm - 
9 open 10.122.163.207 172.18.121.106 32168 34178 PROTO_L4_UDP 0 0 65534 0 self-to-wan self-to-wan-cm - 
```

لعرض إحصائيات زوج المناطق، أستخدم أمر EXEC:

```
<#root>

Device#

show sdwan zbfw zonepair-statistics

zbfw zonepair-statistics user-to-server
src-zone-name user
dst-zone-name server
policy-name user-to-server-pm
fw-traffic-class-entry user-to-server-cm
zonepair-name user-to-server

class-action Inspect


pkts-counter 0
bytes-counter 0
attempted-conn 0

current-active-conn 0


max-active-conn 0
current-halfopen-conn 0
max-halfopen-conn 0
current-terminating-conn 0
max-terminating-conn 0

time-since-last-session-create 0
```

لعرض إحصائيات إسقاط ZBFW، أستخدم أمر EXEC:

```
<#root>

Device#

show sdwan zbfw drop-statistics

zbfw drop-statistics catch-all                          0
```

```
zbfw drop-statistics l4-max-halfsession                0
zbfw drop-statistics l4-session-limit                  0
zbfw drop-statistics l4-scb-close                      0
```

```
zbfw drop-statistics insp-policy-not-present           0
```

```
zbfw drop-statistics insp-sess-miss-policy-not-present 0
```

```
zbfw drop-statistics insp-classification-fail          0
zbfw drop-statistics insp-class-action-drop            0
zbfw drop-statistics insp-policy-misconfigure          0
```

```
zbfw drop-statistics l4-icmp-err-policy-not-present    0
```

```
zbfw drop-statistics invalid-zone                      0
```

```
zbfw drop-statistics ha-ar-standby                     0
zbfw drop-statistics no-forwarding-zone                0
```

```
zbfw drop-statistics no-zone-pair-present            105 <<< If no zone-pair configured
```

لعرض إحصائيات إسقاط معالج QuantumFlow (QFP)، أستخدم أمر EXEC:

<#root>

```
Device#
```

```
show platform hardware qfp active statistic drop
```

```
Last clearing of QFP drops statistics: never
------------------------------------------------------------------------
Global Drop Stats                          Packets               Octets
------------------------------------------------------------------------
```

```
BFDoffload                                  194                14388

FirewallBackpressure                          0                    0
FirewallInvalidZone                           0                    0
FirewallL4                                    1                   74
FirewallL4Insp                              372                40957
FirewallL7                                    0                    0
FirewallNoForwardingZone                      0                    0
FirewallNoNewSession                          0                    0
FirewallNonsession                            0                    0
FirewallNotFromInit                           0                    0
FirewallNotInitiator                      11898                885244
FirewallPolicy                                0                    0
```

لعرض عملياتإسقاط جدار حماية QFP، أستخدم أمر EXEC:

<#root>

```
Device#
show platform hardware qfp active feature firewall drop all
```

```
-----------------------------------------------------------------------------
Drop Reason                                                          Packets
-----------------------------------------------------------------------------
TCP out of window                                                          0
TCP window overflow                                                        0
<snipped>
TCP - Half-open session limit exceed                                       0
Too many packet per flow                                                   0
<snipped>
ICMP ERR PKT:no IP or ICMP                                                 0
ICMP ERR Pkt:exceed burst lmt                                              0
ICMP Unreach pkt exceeds lmt                                               0
ICMP Error Pkt invalid sequence                                            0
ICMP Error Pkt invalid ACK                                                 0
ICMP Error Pkt too short                                                   0
Exceed session limit                                                       0
Packet rcvd in SCB close state                                             0
Pkt rcvd after CX req teardown                                             0
CXSC not running                                                           0
```

Zone-pair without policy 0 <<< Existing zone-pair, but not

Same zone without Policy 0 <<< Zone without policy configu

<snipped>

No Zone-pair found 105 <<< If no zone-pair configured

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).