從SD-WAN CLI模板配置ZBFW

目錄

簡介

本文檔介紹如何使用Cisco Catalyst SD-WAN Manager中的CLI附加功能模板配置基於區域的防火牆(ZBFW)策略。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Catalyst軟體定義廣域網路(SD-WAN)
- 區域型防火牆(ZBFW)基本操作

採用元件

- Cisco Catalyst SD-WAN管理員20.9.3.2
- Cisco IOS® XE Catalyst SD-WAN邊緣17.6.5a

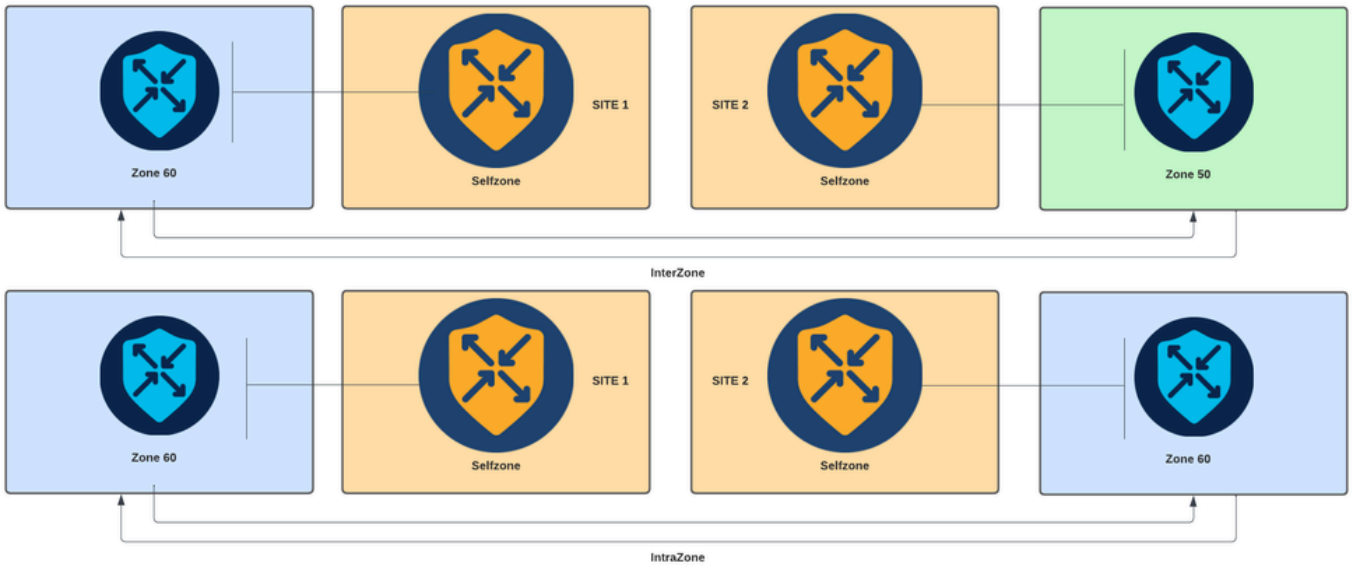
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

防火牆策略是一種本地化的安全策略，允許對TCP、UDP和ICMP資料流進行狀態檢測。它使用區域的概念；因此，根據兩個區域之間的策略，允許來自給定區域的流量進入另一個區域。

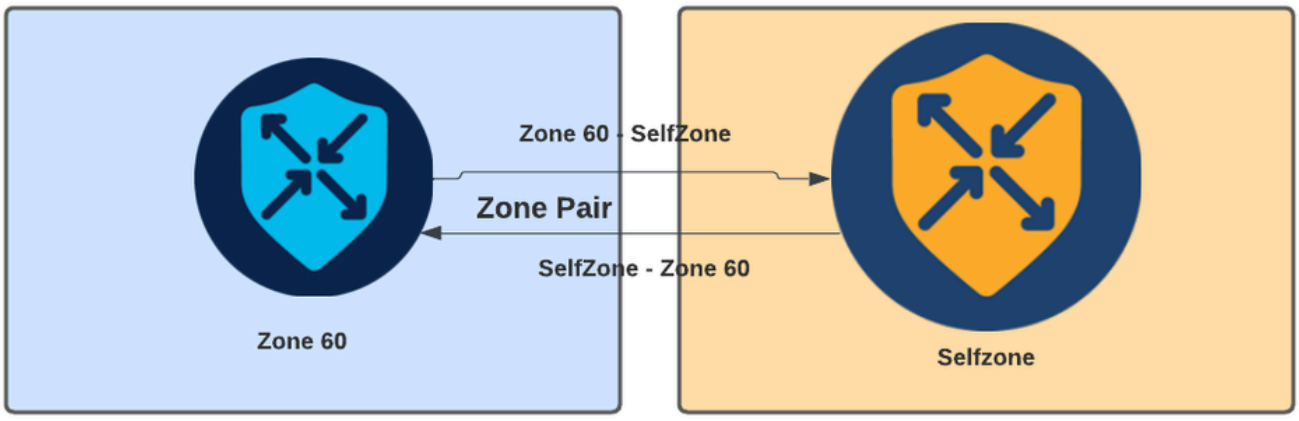
區域是一個或多個VPN的組。ZBFW上存在的區域型別為：

- 源區：一組發起資料流量流的VPN。VPN只能是一個區域的一部分。
- 目標區域:一組VPN，用於終止資料流量。VPN只能是一個區域的一部分。
- Interzone:當流量在不同的區域之間流動時，它稱為區域間通訊（預設情況下，通訊被拒絕）。
- Intrazone:當流量流經同一區域時，它稱為區域內網路（預設情況下允許通訊）。
- Selfzone：用於控制源自或定向到路由器本身的流量（系統建立和預配置的預設區域，預設情況下允許通訊）。



基於區域的防火牆圖

ZBFW中使用的另一個概念是區域對，它是將源區域與目標區域關聯的容器。區域對將防火牆策略應用於在兩個區域之間流動的流量。



區域對示例

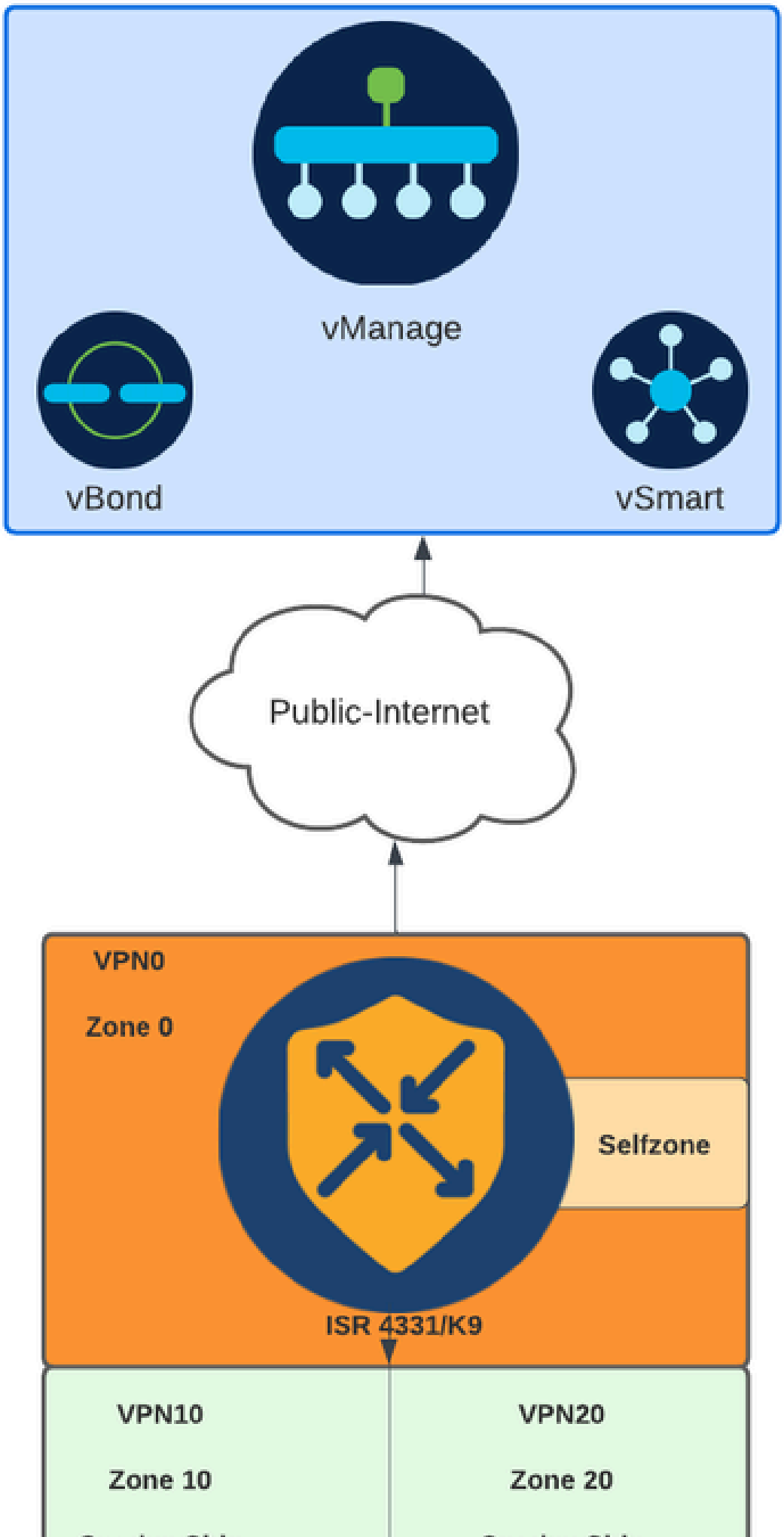
定義區域對後，適用於流的操作為：

- Drop：只是丟棄匹配流。
- 通過：允許資料包流而不進行狀態檢查，類似於訪問清單中的允許操作。無論在流中設定通過

操作，都需要該流的返回通過。
- 檢查：允許對從源區域流向目標區域的流量進行狀態檢查，並自動允許流量返回。

設定

網路圖表


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

```
 multi-tenancy
 vpn zone security
  alert on
  log dropped-packets
  max-incomplete tcp timeout
```

max-incomplete tcp

configuration命令用於指定TCP會話丟棄之前未完成連線的最大數量。

配置**multi-tenancy**命令是ZBFW配置中所需的全域性引數。當通過SD-WAN管理器GUI配置ZBFW時，預設情況下會新增線路。通過命令列介面(CLI)配置ZBFW時，需要新增此行。

2.建立WAN區域:

```
zone security wan
vpn 0
```

附註：預設情況下會建立自區域，無需對其進行配置。

3.為源地址和目的地地址配置對象組：

```
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.建立IP access-list:

```
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.建立類對映:

```
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.建立要新增到區域對中的策略對映:

```
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.建立區域對並將策略對映鏈接到它：

```
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
```

一旦允許控制平面流，就可以應用資料平面配置。

要驗證control-connections，請使用EXEC命令：

<#root>

Device#

show sdwan control connections

無論是否正確配置了自帶區和wan區的ZBFW，裝置都會失去控制連線，並會遇到類似以下情況的控制檯錯誤：

<#root>

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

資料平面

1.為所需的每個虛擬路由和轉送(VRF)建立安全區域：

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

3.為源地址和目的地地址配置對象組：

```
 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.建立IP access-list:

```
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.建立類對映:

```
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.建立要新增到區域對中的策略對映:

```
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.建立區域對並將策略對映鏈接到它：

```
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
```

附註：有關使用CLI模板的詳細資訊，請參閱CLI附加功能模板和CLI模板。

驗證

要驗證配置的inspect class-map，請使用EXEC命令：

<#root>

Device#

show class-map type inspect

要驗證配置的inspect policy-map，請使用EXEC命令：

<#root>

Device#

show policy-map type inspect

要驗證已配置的區域對，請使用EXEC命令：

<#root>

Device#

show zone-pair security

要驗證配置的access-list，請使用EXEC命令：

```
<#root>

Device#

show ip access-list
```

要驗證已配置的對象組，請使用EXEC命令：

```
<#root>

Device#

show object-group
```

要顯示ZBFW會話狀態，請使用EXEC命令：

```
<#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 - 0
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 - 0
```

要顯示區域對統計資訊，請使用EXEC命令：

```
<#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
```

要顯示ZBFW丟棄統計資訊，請使用EXEC命令：

<#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
```

要顯示QuantumFlow處理器(QFP)丟棄統計資訊，請使用EXEC命令：

<#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
```

要顯示QFP防火牆丟棄，請使用EXEC命令：

<#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
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。