

从SD-WAN CLI模板配置ZBFW

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

[配置](#)

[控制层面](#)

[数据层面](#)

[验证](#)

简介

本文档介绍如何使用Cisco Catalyst SD-WAN Manager中的CLI附加功能模板配置基于区域的防火墙(ZBFW)策略。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Catalyst软件定义的广域网(SD-WAN)
- 基于区域的防火墙(ZBFW)基本操作

使用的组件

- 思科Catalyst SD-WAN管理器20.9.3.2
- 思科IOS® XE Catalyst SD-WAN边缘17.6.5a

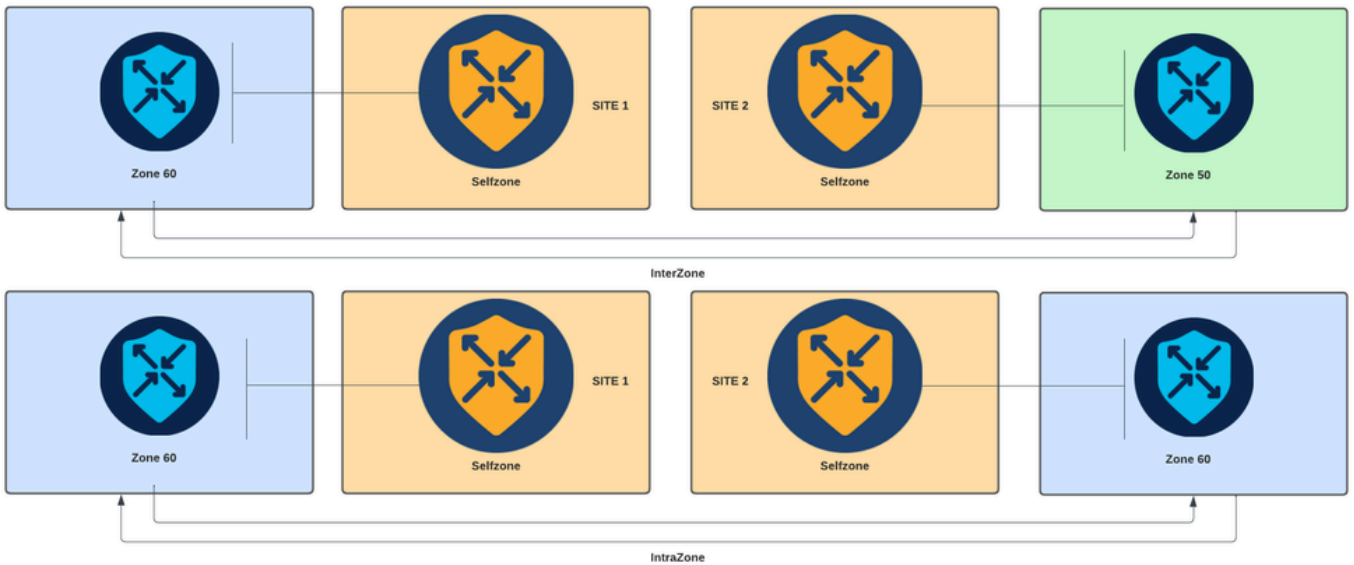
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

防火墙策略是一种本地化的安全策略，允许对TCP、UDP和ICMP数据流进行状态检查。它使用区域的概念；因此，允许来自给定区域的流量根据两个区域之间的策略进入另一个区域。

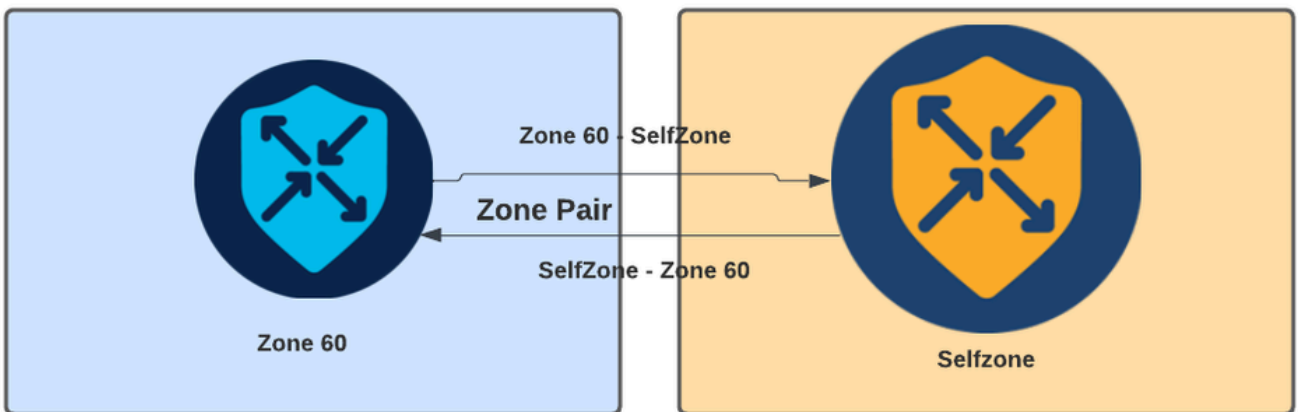
区域是一个或多个VPN的组。ZBFW上存在的区域类型为：

- 源区：发起数据流量流的一组VPN。VPN只能是一个区域的一部分。
- 目标区域:终止数据流量的一组VPN。VPN只能是一个区域的一部分。
- 区域间:当流量在不同区域之间流动时，它称为区域间流量（默认情况下，通信被拒绝）。
- 区域内:当流量流经同一区域时，它称为区域内网络（默认情况下允许通信）。
- Selfzone：用于控制源自或定向到路由器本身的流量（由系统创建和预配置的默认区域，默认情况下允许通信）。



基于区域的防火墙图

ZBFW中使用的另一个概念是区域对，它是将源区域与目标区域关联的容器。区域对将防火墙策略应用于在两个区域之间流动的流量。



区域对示例

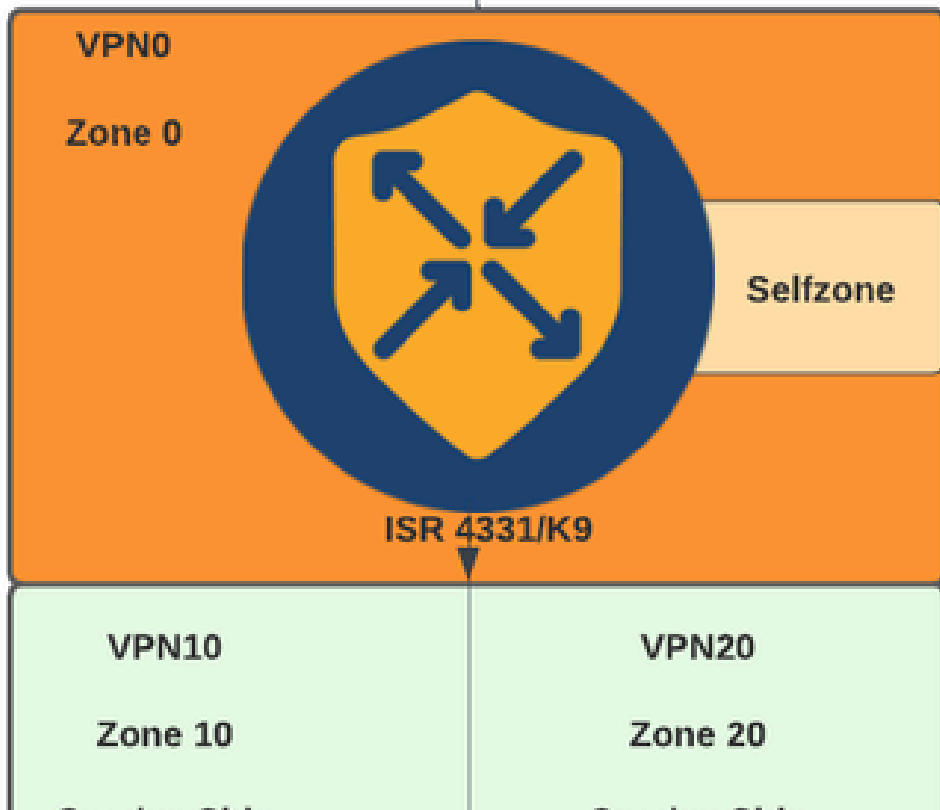
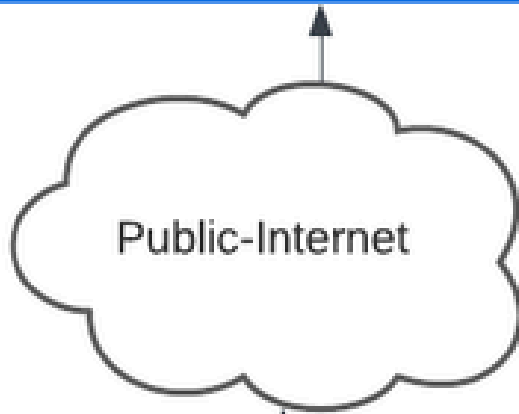
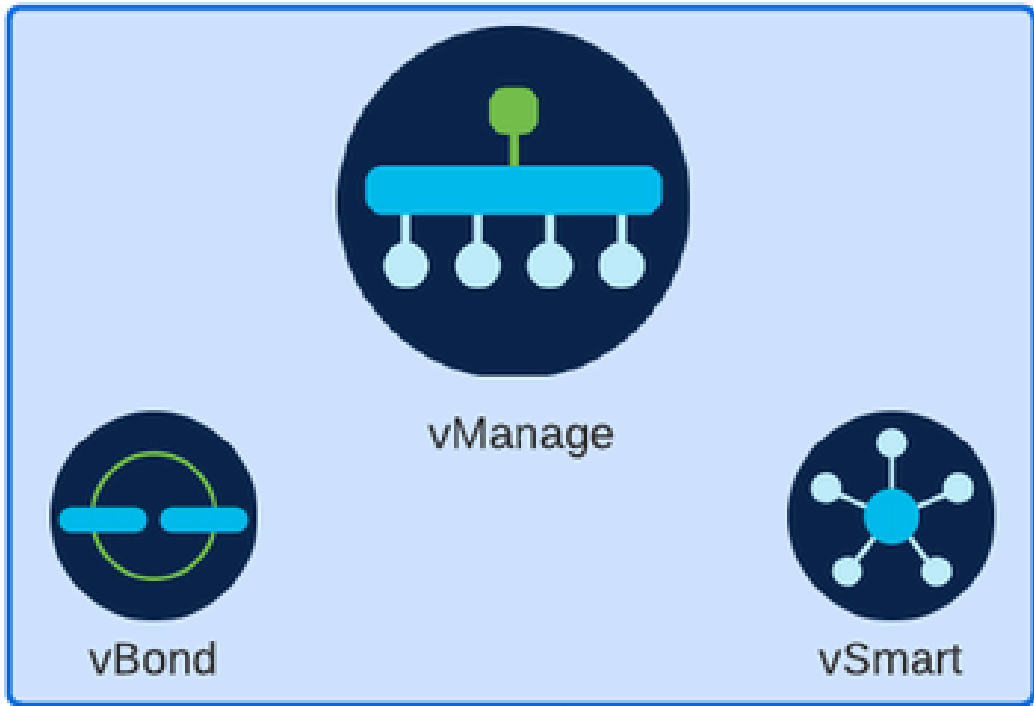
定义区域对后，适用于流的操作为：

- 丢弃：仅丢弃匹配流。
- 通过：允许数据包流而不进行状态检查，类似于访问列表中的允许操作。无论在流中设置通过操作，都需要该流的返回通过。

- 检查：允许对从源区域流向目标区域的流量进行状态检查，并自动允许流量返回。

配置

网络图



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


配置命令用于指定TCP会话丢弃之前未完成连接的最大数量 `max-incomplete tcp`

。

配置 `multi-tenancy` 命令是ZBFW配置中所需的全局参数。当通过SD-WAN Manager GUI配置ZBFW时，默认情况下会添加线路。通过命令行界面(CLI)配置ZBFW时，需要添加此行。

2.创建WAN区域:

```
zone security wan
vpn 0
```

 注意：默认情况下会创建自区域，无需对其进行配置。

3.为源地址和目标地址配置对象组：

```
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.创建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.创建类映射:

```
class-map type inspect match-all self-to-wan-cm
  match access-group name self-to-wan-ac1
class-map type inspect match-all wan-to-self-cm
  match access-group name wan-to-self-ac1
```

6. 创建要添加到区域对的策略映射:

```
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. 创建区域对并将策略映射链接到它 :

```
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
```

一旦允许控制平面流，即可应用数据平面配置。

要验证control-connections，请使用EXEC命令：

```
<#root>
```

```
Device#
```

```
show sdwan control connections
```

如果自区域和wan区域的ZBFW配置不正确，设备将失去控制连接，并出现类似下例的控制台错误：

```
<#root>
```

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

数据层面

1.为所需的每个虚拟路由和转发(VRF)创建安全区域：

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

3.为源地址和目标地址配置对象组：

```
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.创建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.创建类映射:

```
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.创建要添加到区域对的策略映射:

```
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.创建区域对并将策略映射链接到它：

```
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
```



注意：有关使用CLI模板的详细信息，请参阅[CLI附加功能模板](#)和[CLI模板](#)。

验证

要验证已配置的inspect class-map，请使用EXEC命令：

```
<#root>
Device#
show class-map type inspect
```

要验证已配置的inspect policy-map，请使用EXEC命令：

```
<#root>
Device#
show policy-map type inspect
```

要验证已配置的区域对，请使用EXEC命令：

```
<#root>
Device#
show zone-pair security
```


要验证已配置的access-list，请使用EXEC命令：

```
<#root>
Device#
show ip access-list
```

要验证已配置的对象组，请使用EXEC命令：

```
<#root>
Device#
show object-group
```

要显示ZBFW会话状态，请使用EXEC命令：

```
<#root>
Device#
show sdwan zonebfpwdp 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
```

要显示区域对统计信息，请使用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
```

要显示ZBFW丢弃统计信息，请使用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

```

要显示QuantumFlow处理器(QFP)丢弃统计信息，请使用EXEC命令：

```
<#root>
```

```
Device#
```

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

```
Last clearing of QFP drops statistics: never
```

```

-----
Global Drop Stats                Packets                Octets
-----
BFDooffload                      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

要显示QFP防火墙丢弃，请使用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

```

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。