

Configuración de ZBFW desde una plantilla CLI de SD-WAN

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración](#)

[Plano de Control](#)

[Plano de Datos](#)

[Verificación](#)

Introducción

Este documento describe cómo configurar la política de firewall basado en zonas (ZBFW) mediante una plantilla de función complementaria CLI de Cisco Catalyst SD-WAN Manager.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Red de área extensa definida por software (SD-WAN) Cisco Catalyst
- Funcionamiento básico del firewall basado en zonas (ZBFW)

Componentes Utilizados

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Una política de firewall es un tipo de política de seguridad localizada que permite la inspección con estado de los flujos de tráfico de datos TCP, UDP e ICMP. Utiliza el concepto de zonas; por lo tanto, los flujos de tráfico que se originan en una zona determinada pueden continuar a otra zona en función de la política entre las dos zonas.

Una zona es un grupo de una o más VPN. El tipo de zonas que existe en ZBFW son:

- Zona de origen: grupo de VPN que origina los flujos de tráfico de datos. Una VPN puede ser parte de una sola zona.
- Zona de destino: grupo de VPN que finaliza los flujos de tráfico de datos. Una VPN puede ser parte de una sola zona.
- Interzona: se denomina interzona cuando el tráfico fluye entre diferentes zonas (de forma predeterminada, la comunicación es denegada).
- Intrazona: se denomina intrazona cuando el tráfico fluye a través de la misma zona (de forma predeterminada se permite la comunicación).
- Selfzone: se utiliza para controlar el tráfico que se origina o se dirige al propio router (zona predeterminada creada y preconfigurada por el sistema; de forma predeterminada, se permite la comunicación).

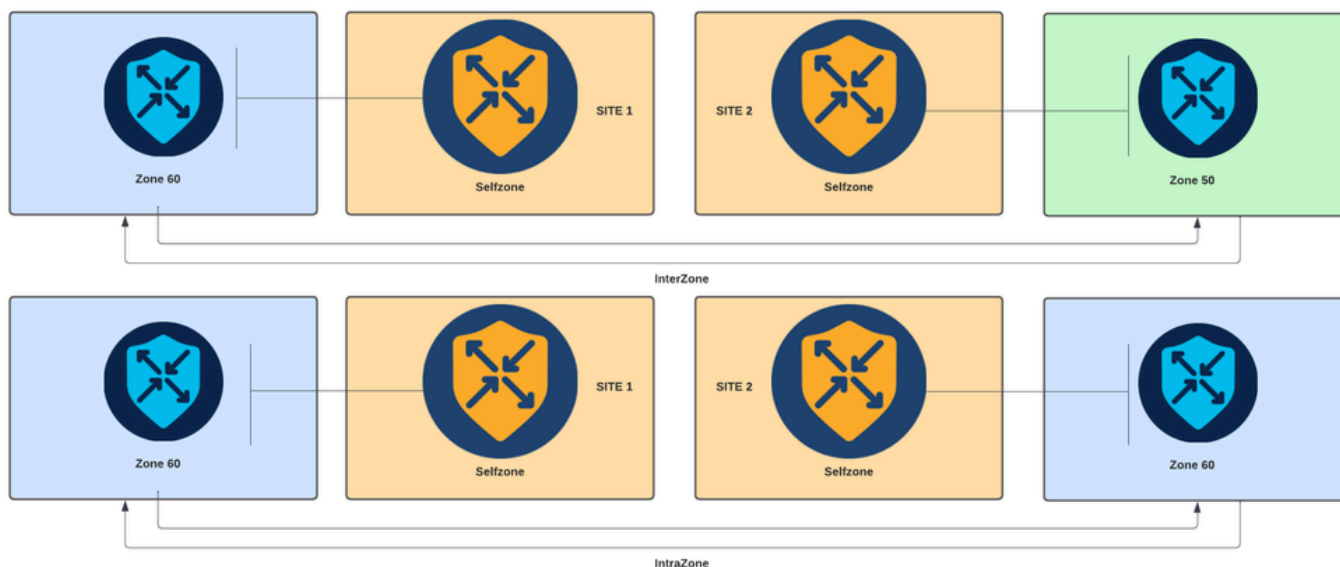
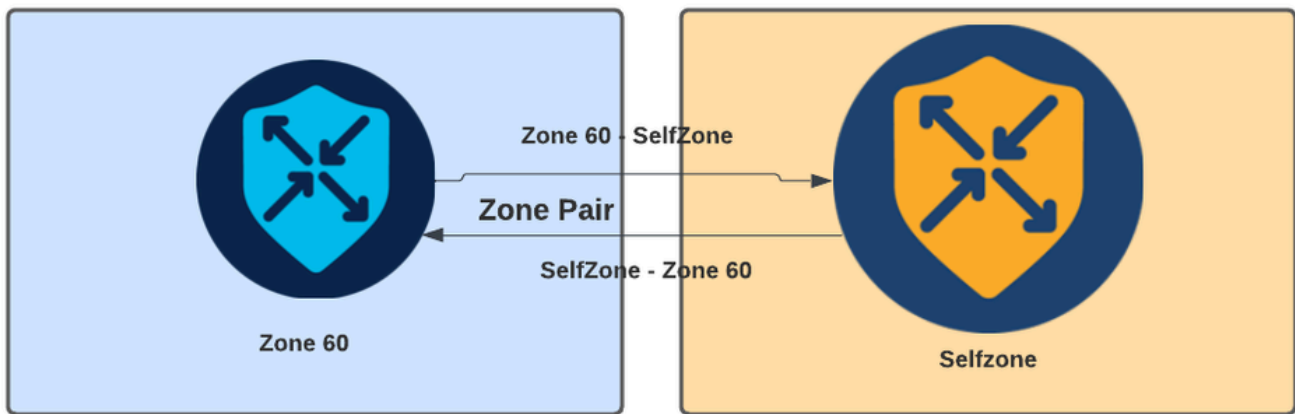


Diagrama de firewall basado en zonas

Otro concepto utilizado en ZBFW es el par de zonas, que es un contenedor que asocia una zona de origen con una zona de destino. Los pares de zonas aplican una política de firewall al tráfico que fluye entre las dos zonas.



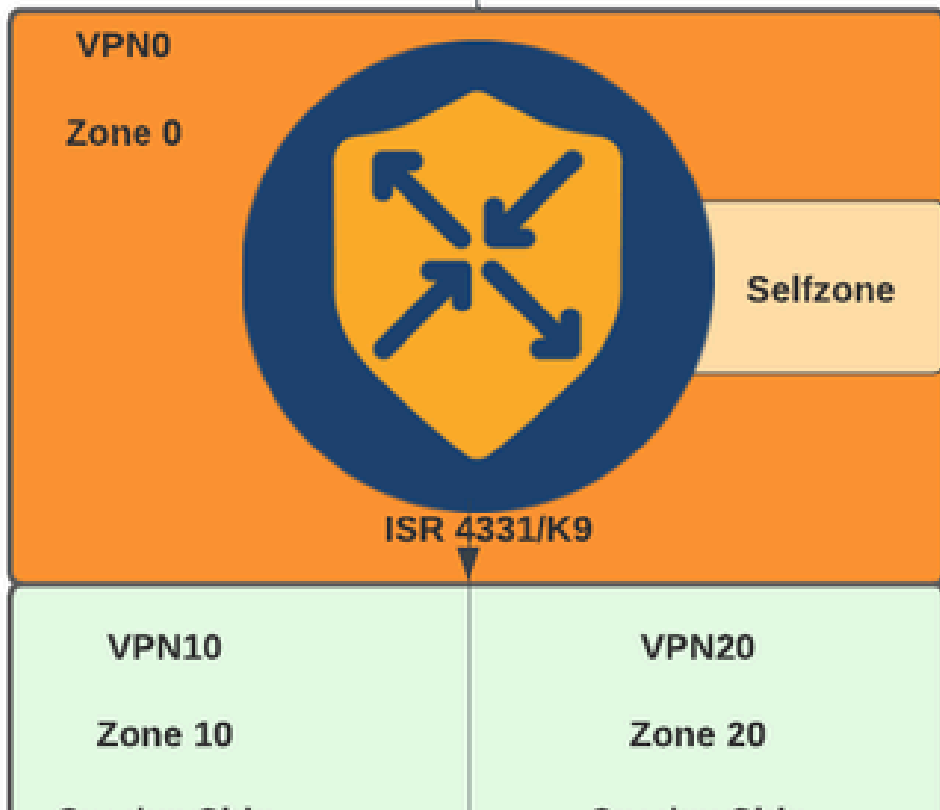
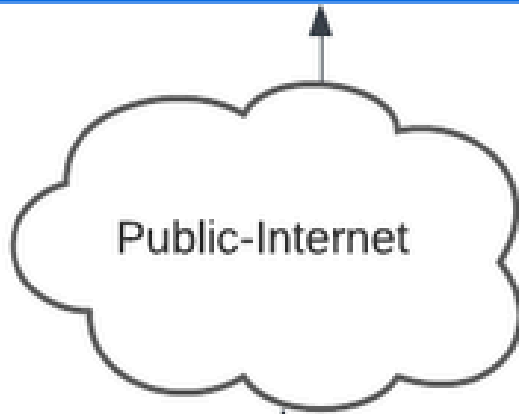
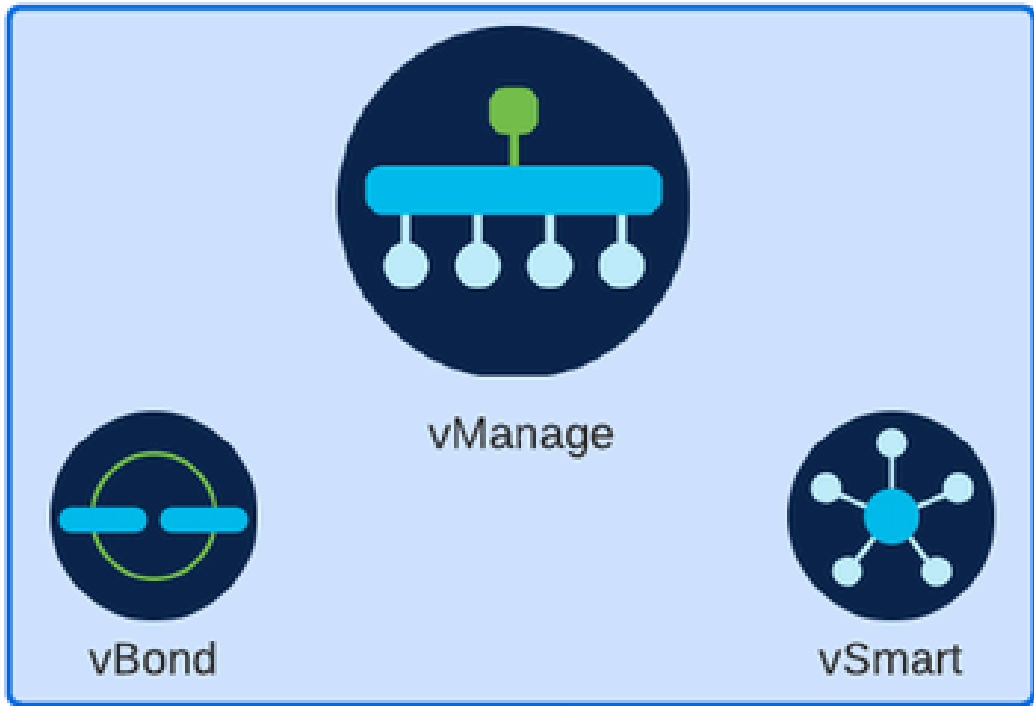
Ejemplo de Zone-Pair


Una vez definido el par de zonas, las acciones que se aplican a los flujos son:

- Descartar: simplemente descarta el flujo de coincidencia.
- Pass: permite el flujo de paquetes sin inspección stateful, similar a la acción permit en las listas de acceso. Si una acción pass se establece en un flujo, se necesita una pasada de retorno para ese flujo.
- Inspeccionar: permite la inspección stateful del tráfico que fluye desde el origen a la zona de destino, y permite automáticamente que los flujos de tráfico regresen.

Configurar

Diagrama de la red



 Tanto si la interfaz WAN se configura mediante DHCP, es necesario crear una regla para permitir que la zona automática (interfaz) alcance la dirección IP del siguiente salto en caso de que el dispositivo de recarga y el router necesiten obtener una nueva dirección IP.

Plano de Control

1. Cree el mapa de parámetro de inspección:

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


El `max-incomplete tcp`

comando de configuración se utiliza para especificar el número máximo de conexiones incompletas antes de que se descarte la sesión TCP.

El `multi-tenancy` comando de configuración es un parámetro global necesario en la configuración de ZBFW. Cuando ZBFW se configura a través de la GUI de SD-WAN Manager, la línea se agrega de forma predeterminada. Cuando ZBFW se configura a través de la interfaz de línea de comandos (CLI), es necesario agregar esta línea.

2. Cree una zona WAN:

```
zone security wan
vpn 0
```

 Nota: La zona automática se crea de forma predeterminada, no es necesario configurarla.

3. Configure el grupo de objetos para las direcciones de origen y destino:

```
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. Cree la lista de acceso 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. Cree el mapa de clase:

```
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. Cree el mapa de política para agregarlo al par de zonas:

```
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. Cree el par de zonas y vincule el mapa de políticas a él:

```
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
```

Una vez que se permiten los flujos del plano de control, se puede aplicar la configuración del plano de datos.

Para validar control-connections, utilice el comando EXEC:

<#root>

Device#

```
show sdwan control connections
```

Si ZBFW para la zona automática y la zona wan no está correctamente configurado, los dispositivos pierden las conexiones de control y obtienen un error de consola similar al siguiente:

```
<#root>
```

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

Plano de Datos

1. Cree una zona de seguridad para cada routing y reenvío virtual (VRF) necesario:

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

3. Configure el grupo de objetos para las direcciones de origen y destino:

```
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. Cree la lista de acceso 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. Cree el mapa de clase:

```
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. Cree el mapa de política para agregarlo al par de zonas:

```
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. Cree el par de zonas y vincule el mapa de políticas a él:

```
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
```



Nota: Para obtener más información sobre el uso de plantillas CLI, consulte [Plantillas de funciones de complementos CLI](#) y [Plantillas CLI](#).

Verificación

Para validar el mapa de clase de inspección configurado, utilice el comando EXEC:

```
<#root>
```

```
Device#
```

```
show class-map type inspect
```

Para validar el policy-map de inspección configurado, utilice el comando EXEC:


```
<#root>
```

```
Device#
```

```
show policy-map type inspect
```

Para validar el par de zonas configurado, utilice el comando EXEC:

```
<#root>
```

```
Device#
```

```
show zone-pair security
```

Para validar la lista de acceso configurada, utilice el comando EXEC:

```
<#root>
```

```
Device#
```

```
show ip access-list
```

Para validar el grupo de objetos configurado, utilice el comando EXEC:

```
<#root>
```

```
Device#
```

```
show object-group
```

Para mostrar el estado de sesión de ZBFW, utilice el comando EXEC:

```
<#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 -
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 -
```

Para mostrar las estadísticas de par de zonas, utilice el comando 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
```

Para mostrar las estadísticas de descarte de ZBFW, utilice el comando EXEC:

```
<#root>
```

```
Device#
```

```
show sdwan zbfw drop-statistics
```

```
zbfw drop-statistics catch-all
```

```
0
```

```

zbfw drop-statistics 14-max-halfsession 0
zbfw drop-statistics 14-session-limit 0
zbfw drop-statistics 14-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 14-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

```

Para mostrar las estadísticas de caídas del procesador QuantumFlow (QFP), utilice el comando 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 |

Para mostrar las caídas del firewall QFP, utilice el comando 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 |

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).