

# Configurar ZBFW a partir do modelo SD-WAN CLI

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração](#)

[Controle o plano](#)

[Plano dos dados](#)

[Verificar](#)

---

## Introdução

Este documento descreve como configurar a política de firewall baseado em zona (ZBFW) usando um modelo de recurso complementar de CLI do Cisco Catalyst SD-WAN Manager.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Rede de longa distância definida pelo software Cisco Catalyst (SD-WAN)
- Operação básica do Zone-Based Firewall (ZBFW)

### Componentes Utilizados

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

Uma política de firewall é um tipo de política de segurança localizada que permite a inspeção stateful de fluxos de tráfego de dados TCP, UDP e ICMP. Usa o conceito de zonas; portanto, os fluxos de tráfego que se originam em uma determinada zona têm permissão para ir para outra zona com base na política entre as duas zonas.

Uma zona é um grupo de uma ou mais VPNs. Os tipos de zonas que existem no ZBFW são:

- Zona de origem: um grupo de VPNs que origina os fluxos de tráfego de dados. Uma VPN pode fazer parte de apenas uma zona.
- Zona de destino: um grupo de VPNs que encerra os fluxos de tráfego de dados. Uma VPN pode fazer parte de apenas uma zona.
- Interzona: ela é chamada de interzone quando o tráfego flui entre zonas diferentes (por padrão, a comunicação é negada).
- Intrazona: é chamada intrazona quando o tráfego flui através da mesma zona (Por padrão a comunicação é permitida).
- Selfzone: é usado para controlar o tráfego que é originado ou direcionado para o próprio roteador (zona padrão criada e pré-configurada pelo sistema; por padrão, a comunicação é permitida).

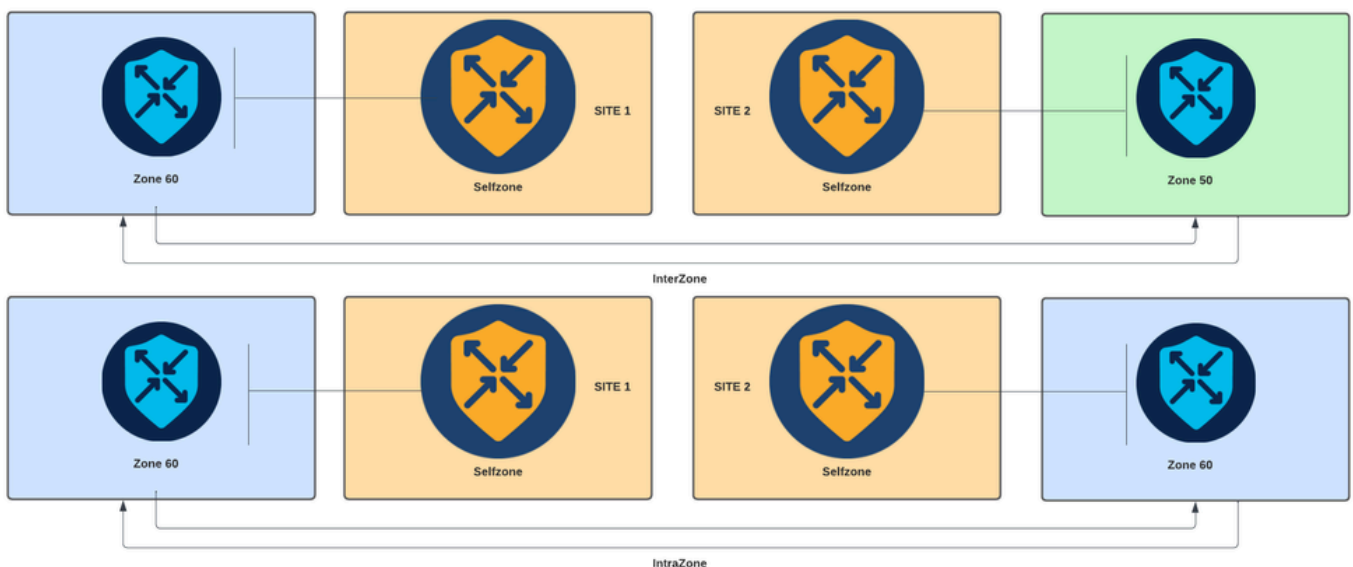
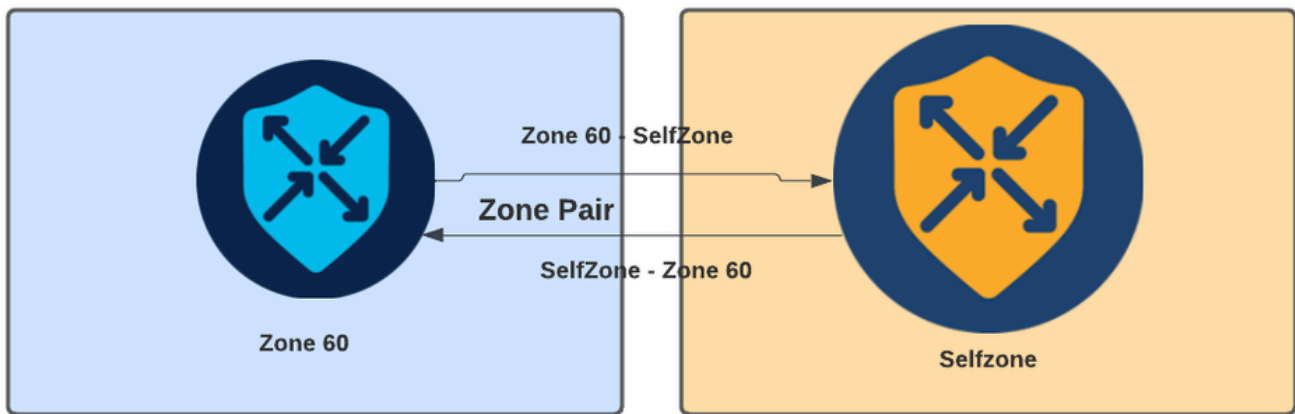


Diagrama de firewall baseado em zona

Outro conceito usado no ZBFW é o par de zonas, que é um contêiner que associa uma zona de origem a uma zona de destino. Os pares de zonas aplicam uma política de firewall ao tráfego que flui entre as duas zonas.



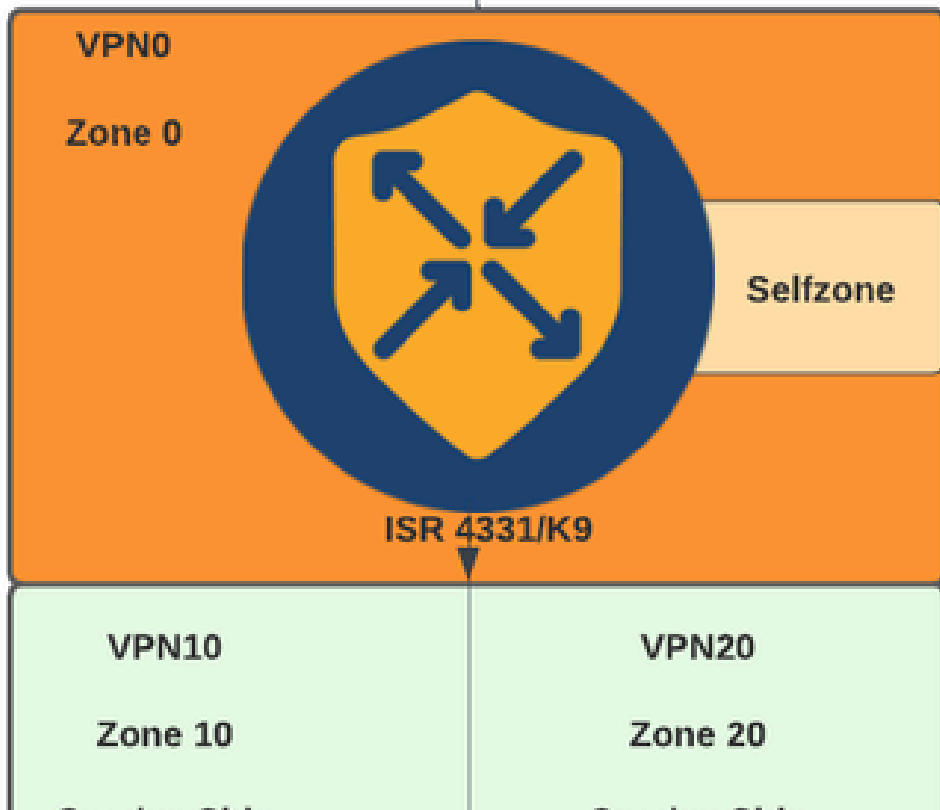
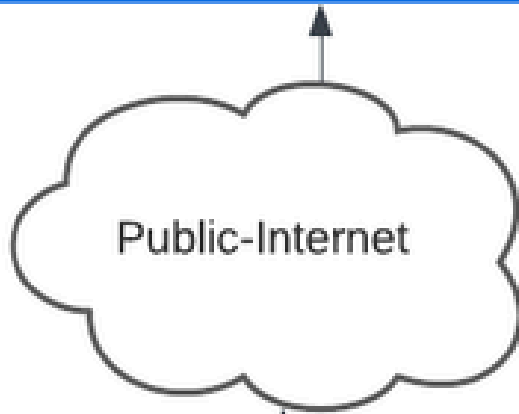
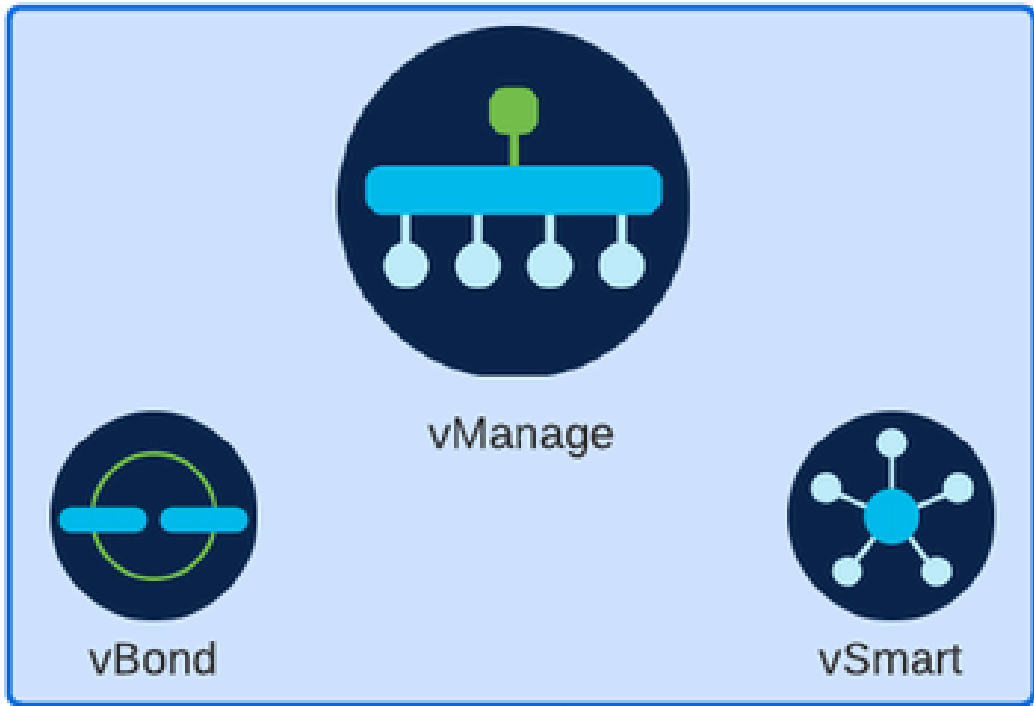
Exemplo de par de zona

Depois que o par de zonas é definido, as ações que se aplicam aos fluxos são:


- Drop: simplesmente descarta o fluxo de correspondência.
- Aprovado: permite o fluxo de pacotes sem inspeção stateful, semelhante à ação de permissão nas listas de acesso. Se uma ação de aprovação for definida em um fluxo, será necessária uma aprovação de retorno para esse fluxo.
- Inspeccionar: permite a inspeção stateful do tráfego que flui da zona de origem para a de destino e permite automaticamente o retorno dos fluxos de tráfego.

## Configurar

### Diagrama de Rede



---

 : Se a interface da WAN estiver configurada via DHCP, é necessário criar uma regra para permitir que a autozona (interface) atinja o endereço IP do próximo salto, caso o dispositivo de recarregamento e o roteador precisem obter um novo endereço IP.

---

## Controle o plano

### 1. Crie o mapa de parâmetros de inspeção:

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

O comando `max-incomplete tcp` configuration é usado para especificar o número máximo de conexões incompletas antes que a sessão TCP seja descartada.

O comando `multi-tenancy` configuration é um parâmetro global necessário na configuração ZBFW. Quando o ZBFW é configurado através da GUI do gerenciador de SD-WAN, a linha é adicionada por padrão. Quando o ZBFW é configurado via Interface de Linha de Comando (CLI), essa linha precisa ser adicionada.

### 2. Criar uma zona WAN:

```
zone security wan
vpn 0
```

---

 Note: A autozona é criada por padrão, não é necessário configurá-la.

---

### 3. Configure o grupo de objetos para os endereços de origem e 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. Crie a lista de acesso 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. Crie o mapa de classes:

```
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. Crie o mapa de política para adicionar ao 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. Crie o par de zonas e vincule o mapa de políticas a ele:

```
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
```

Quando os fluxos do plano de controle forem permitidos, a configuração do plano de dados poderá ser aplicada.

Para validar conexões de controle, use o comando EXEC:

<#root>

Device#

```
show sdwan control connections
```

Se o ZBFW para autozona e zona de WAN não estiver configurado corretamente, os dispositivos perderão as conexões de controle e obterão um erro de console semelhante ao seguinte:

```
<#root>
```

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

## Plano dos dados

1. Crie uma zona de segurança para cada Virtual Routing and Forwarding (VRF) necessário:

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

3. Configure o grupo de objetos para os endereços de origem e 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. Crie a lista de acesso 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. Crie o mapa de classes:

```
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. Crie o mapa de política para adicionar ao 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. Crie o par de zonas e vincule o mapa de políticas a ele:

```
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
```



Note: Para obter mais informações sobre o uso de modelos CLI, consulte [Modelos de recurso de complemento CLI](#) e [Modelos CLI](#).

---

## Verificar

Para validar o inspect class-map configurado, use o comando EXEC:

```
<#root>
```

```
Device#
```

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

Para validar o inspect policy-map configurado, use o comando EXEC:



<#root>

Device#

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

Para validar o par de zonas configurado, use o comando EXEC:

<#root>

Device#

```
show zone-pair security
```

Para validar a lista de acesso configurada, use o comando EXEC:

<#root>

Device#

```
show ip access-list
```

Para validar o grupo de objetos configurado, use o comando EXEC:

<#root>

Device#

```
show object-group
```

Para exibir o status da sessão ZBFW, use o 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 exhibir as estatísticas de par de zonas, use o 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 exhibir as estatísticas de queda de ZBFW, use o 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 exibir as estatísticas de queda do processador QuantumFlow (QFP), use o 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 exibir as quedas de firewall QFP, use o 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 cclose 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

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.