

# Configurer ZBFW à partir du modèle de CLI SD-WAN

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configuration](#)

[Plan de contrôle](#)

[Plan de données](#)

[Vérifier](#)

---

## Introduction

Ce document décrit comment configurer une politique de pare-feu basée sur les zones (ZBFW) à l'aide d'un modèle de fonctionnalité complémentaire CLI de Cisco Catalyst SD-WAN Manager.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Réseau étendu défini par logiciel (SD-WAN) Cisco Catalyst
- Fonctionnement de base du pare-feu basé sur les zones (ZBFW)

### Composants utilisés

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

Une politique de pare-feu est un type de politique de sécurité localisée qui permet l'inspection avec état des flux de trafic de données TCP, UDP et ICMP. Il utilise le concept de zones ; par conséquent, les flux de trafic qui proviennent d'une zone donnée sont autorisés à passer à une autre zone en fonction de la politique entre les deux zones.

Une zone est un groupe d'un ou plusieurs VPN. Les types de zones qui existent sur ZBFW sont les suivants :

- Zone source : groupe de réseaux privés virtuels qui génère les flux de trafic de données. Un VPN ne peut faire partie que d'une seule zone.
- Zone de destination : Groupe de VPN qui termine les flux de trafic de données. Un VPN ne peut faire partie que d'une seule zone.
- Interzone : il est appelé interzone lorsque le trafic circule entre différentes zones (par défaut, la communication est refusée).
- Intrazone : il est appelé intrazone lorsque le trafic traverse la même zone (par défaut, la communication est autorisée).
- Selfzone : elle est utilisée pour contrôler le trafic provenant du routeur ou dirigé vers celui-ci (zone par défaut créée et préconfigurée par le système ; par défaut, la communication est autorisée).

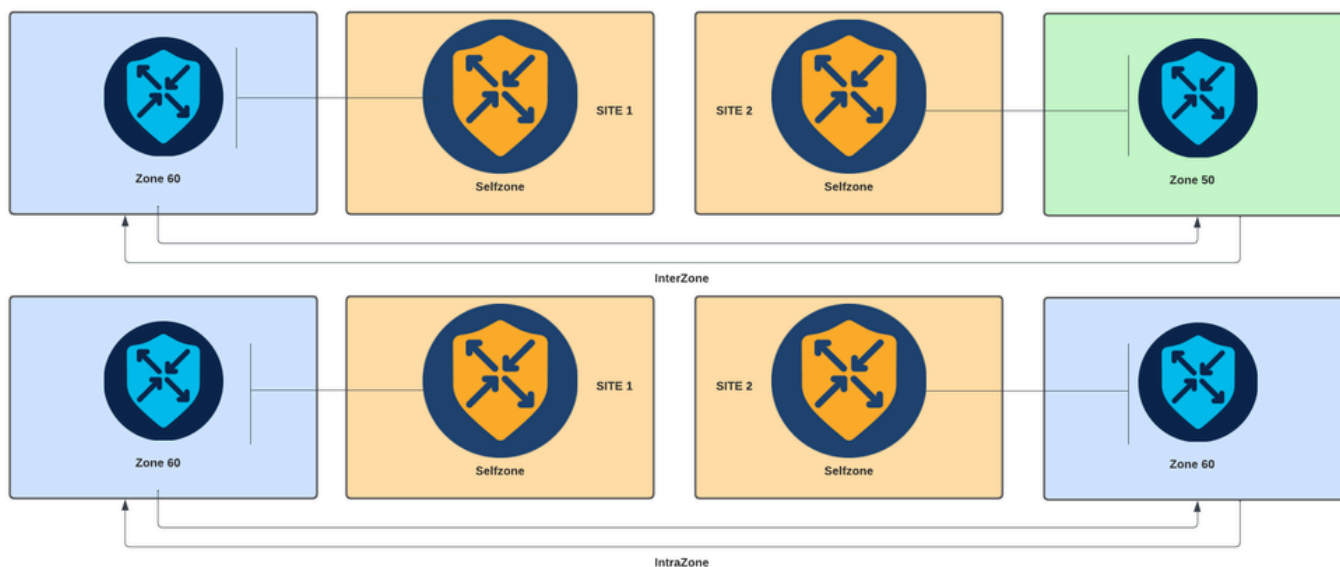
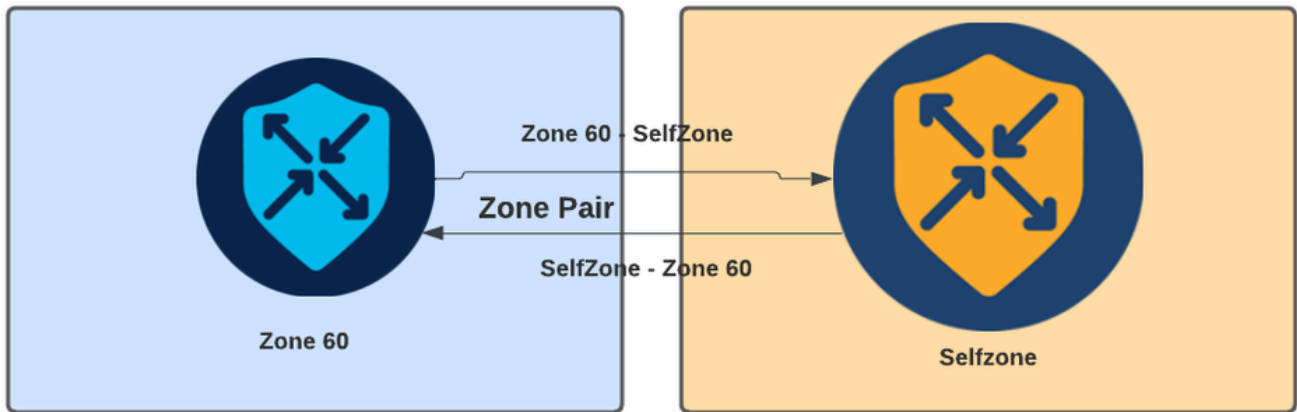


Diagramme de pare-feu basé sur les zones

Un autre concept utilisé dans ZBFW est la paire de zones, qui est un conteneur qui associe une zone source à une zone de destination. Les paires de zones appliquent une politique de pare-feu au trafic qui circule entre les deux zones.



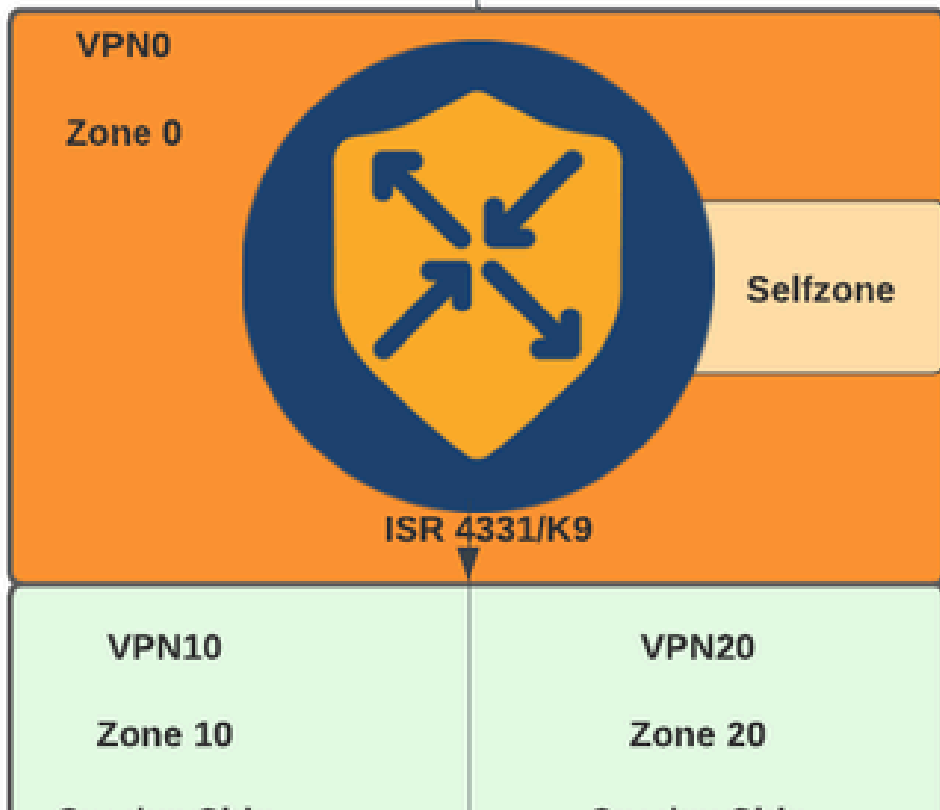
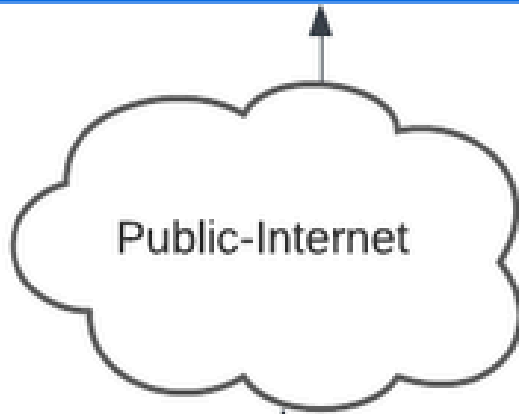
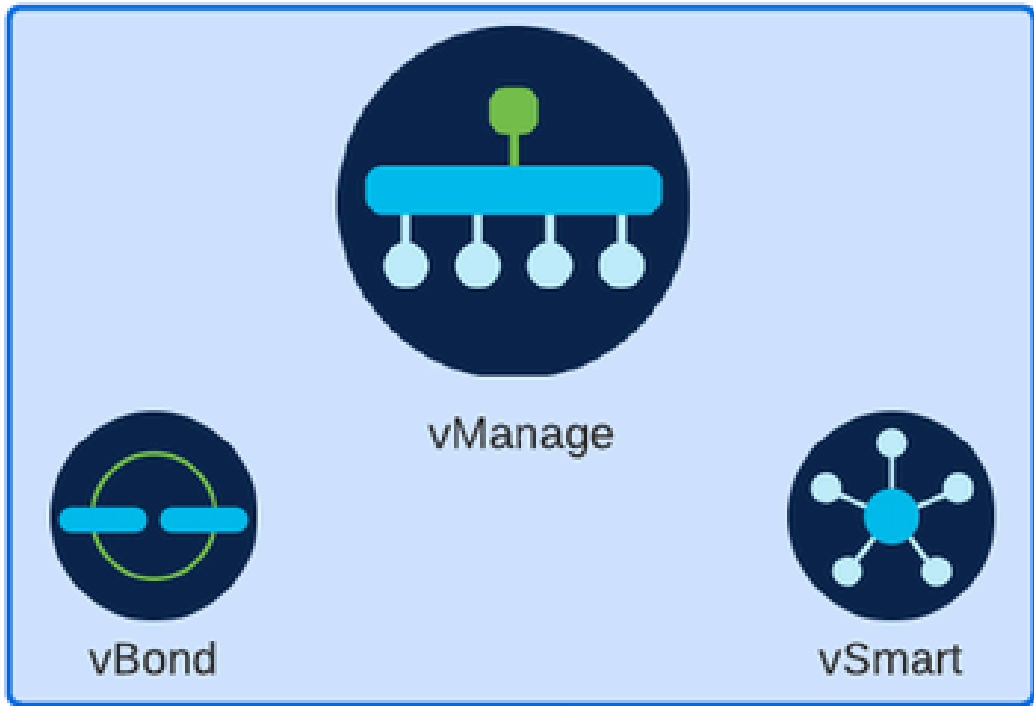
Exemple de zone-paire

Une fois la paire de zones définie, les actions suivantes s'appliquent aux flux :


- Drop : rejette simplement le flux de correspondance.
- Pass : autorise le flux de paquets sans inspection avec état, comme l'action permit dans les listes d'accès. Si une action pass est définie dans un flux, une passe de retour est nécessaire pour ce flux.
- Inspecter : permet l'inspection avec état du trafic qui circule de la source à la zone de destination, et autorise automatiquement le retour des flux de trafic.

## Configurer

Diagramme du réseau



---

 Si l'interface WAN est configurée via DHCP, il est nécessaire de créer une règle pour permettre à la zone auto (interface) d'atteindre l'adresse IP du tronçon suivant au cas où le périphérique et le routeur de rechargement auraient besoin d'obtenir une nouvelle adresse IP.

---

## Plan de contrôle

### 1. Créez la correspondance des paramètres de contrôle :

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

La commande `max-incomplete tcp`


configuration permet de spécifier le nombre maximal de connexions incomplètes avant la suppression de la session TCP.

La `multi-tenancy` commande de configuration est un paramètre global requis dans la configuration ZBFW. Lorsque ZBFW est configuré via l'interface utilisateur graphique du gestionnaire SD-WAN, la ligne est ajoutée par défaut. Lorsque ZBFW est configuré via l'interface de ligne de commande (CLI), cette ligne doit être ajoutée.

### 2. Créez une zone WAN :

```
zone security wan
vpn 0
```

---

 Remarque : La zone Self est créée par défaut, il n'est pas nécessaire de la configurer.

---

### 3. Configurez le groupe d'objets pour les adresses source et de destination :

```
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. Créez la liste de contrôle d'accès 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. Créez la carte de classe :

```
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. Créez le mappage de stratégie à ajouter à la paire de zones :

```
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. Créez la paire de zones et liez la carte de stratégie à celle-ci :

```
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
```

Une fois que les flux du plan de contrôle sont autorisés, la configuration du plan de données peut être appliquée.

Pour valider les connexions de contrôle, utilisez la commande EXEC :

<#root>

Device#

```
show sdwan control connections
```

Si ZBFW pour self-zone et wan-zone n'est pas correctement configuré, les périphériques perdent les connexions de contrôle et obtiennent une erreur de console similaire à la suivante :

```
<#root>
```

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

## Plan de données

1. Créez une zone de sécurité pour chaque VRF (Virtual Routing and Forwarding) nécessaire :

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

3. Configurez le groupe d'objets pour les adresses source et de destination :

```
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. Créez la liste de contrôle d'accès 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. Créez la carte de classe :

```
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. Créez le mappage de stratégie à ajouter à la paire de zones :

```
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. Créez la paire de zones et liez la carte de stratégie à celle-ci :

```
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
```

---

 Remarque : Pour plus d'informations sur l'utilisation des modèles CLI, consultez [Modèles de fonctions complémentaires CLI](#) et [Modèles CLI](#).

---

## Vérifier

Pour valider le class-map inspecté configuré, utilisez la commande EXEC :

```
<#root>
```

```
Device#
```

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

Pour valider le policy-map inspect configuré, utilisez la commande EXEC :



```
<#root>
```

```
Device#
```

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

Pour valider la zone-pair configurée, utilisez la commande EXEC :

```
<#root>
```

```
Device#
```

```
show zone-pair security
```

Pour valider la liste de contrôle d'accès configurée, utilisez la commande EXEC :

```
<#root>
```

```
Device#
```

```
show ip access-list
```

Pour valider le groupe d'objets configuré, utilisez la commande EXEC :

```
<#root>
```

```
Device#
```

```
show object-group
```

Pour afficher l'état de la session ZBFW, utilisez la commande EXEC :

```
<#root>
```

```
Device#
```

```
show sdwan zonebfpw 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 -
```

Pour afficher les statistiques de zone-pair, utilisez la commande 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
```

Pour afficher les statistiques de dépôt ZBFW, utilisez la commande 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

```

Pour afficher les statistiques d'abandon de QuantumFlow Processor (QFP), utilisez la commande 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      |

Pour afficher les abandons du pare-feu QFP, utilisez la commande 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 |

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.