

ZBFW configureren vanuit SD-WAN CLI-sjabloon

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuratie](#)

[Besturingsplane](#)

[Dataplane](#)

[Verifiëren](#)

Inleiding

Dit document beschrijft hoe u het op Zone-based Firewall (ZBFW) beleid kunt configureren met behulp van een CLI Add-On Feature Template van Cisco Catalyst SD-WAN Manager.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Catalyst softwaregedefinieerde Wide Area Network (SD-WAN)
- Zone-Based Firewall (ZBFW) basisbediening

Gebruikte componenten

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

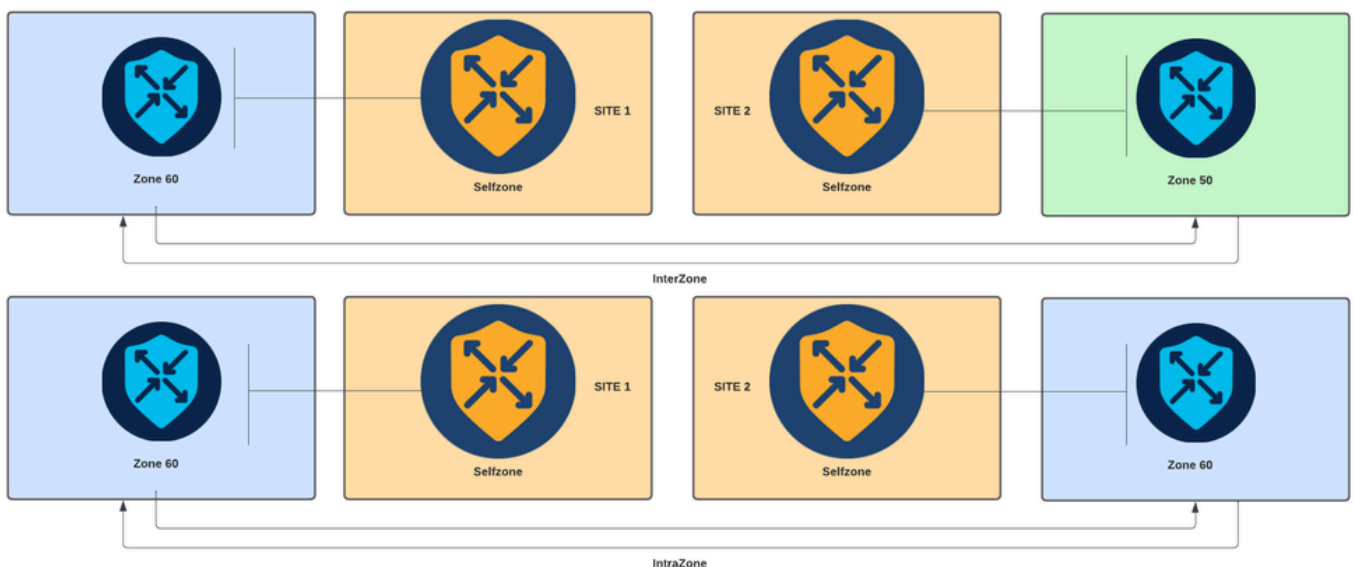
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Een firewallbeleid is een type van gelokaliseerd veiligheidsbeleid dat stateful inspection van TCP-, UDP- en ICMP-gegevensverkeersstromen toestaat. Het begrip zones wordt gebruikt; daarom mogen verkeersstromen die afkomstig zijn uit een bepaalde zone naar een andere zone gaan op basis van het beleid tussen de twee zones.

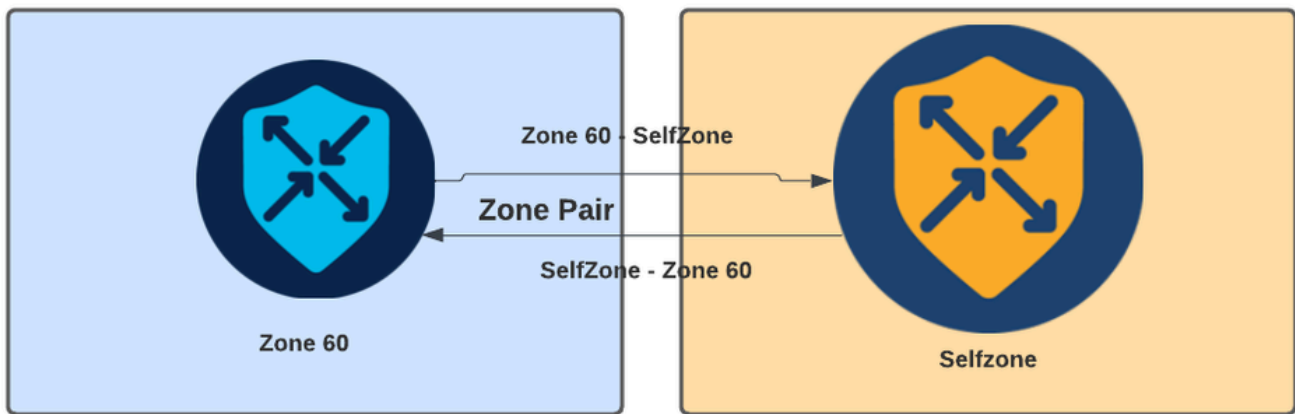
Een zone is een groep van een of meer VPN's. Het type van zones dat op ZBFW bestaat zijn:

- Bronzone: een groep VPN's die de stromen van het dataverkeer voortbrengt. Een VPN kan slechts deel uitmaken van één zone.
- Doelgebied: een groep VPN's die de stromen van het gegevensverkeer beëindigt. Een VPN kan slechts deel uitmaken van één zone.
- Interzone: het wordt interzone genoemd wanneer de verkeersstroom tussen verschillende zones (standaard wordt de communicatie ontkend).
- Intrazone: het wordt intrazone genoemd wanneer het verkeer door dezelfde zone stroomt (standaard is communicatie toegestaan).
- Selfzone: het wordt gebruikt voor het controleren van verkeer dat afkomstig is van of geleid naar de router zelf (Standaardzone die door systeem wordt gecreëerd en vooraf geconfigureerd, door gebrek is de communicatie toegestaan).



Op zone gebaseerde firewalldiagram

Een ander concept dat in ZBFW wordt gebruikt is het zonepaar, dat een container is die een bronzone associeert met een bestemmingszone. Zone-paren passen een firewallbeleid toe op het verkeer dat tussen de twee zones stroomt.



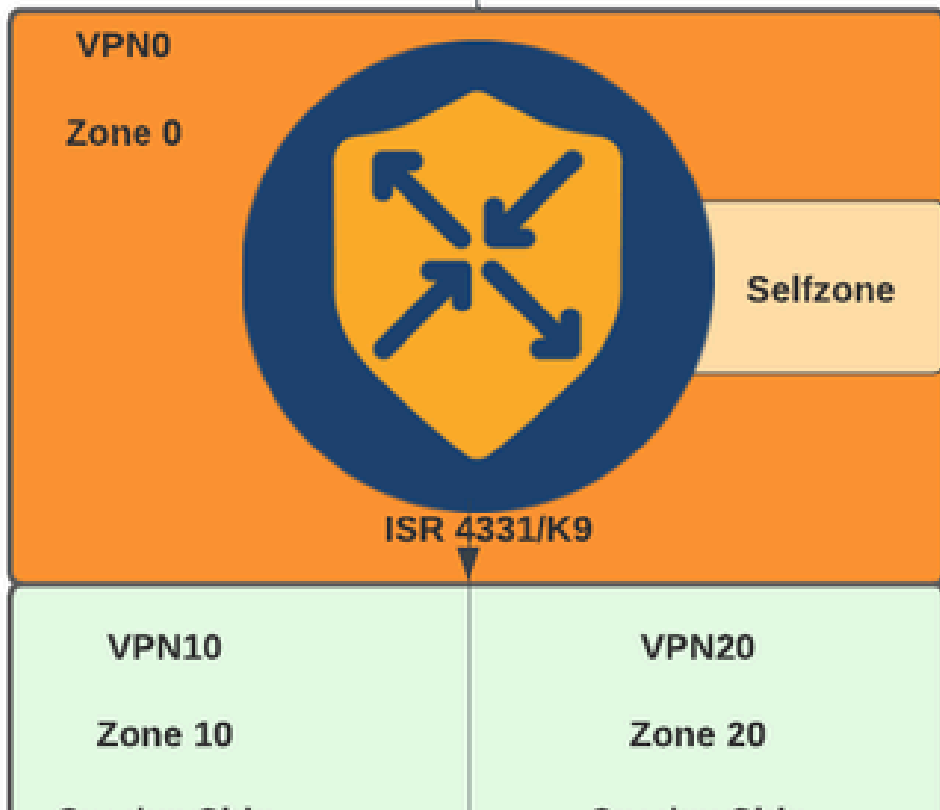
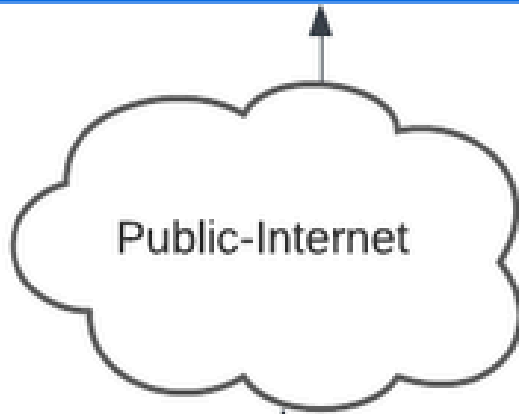
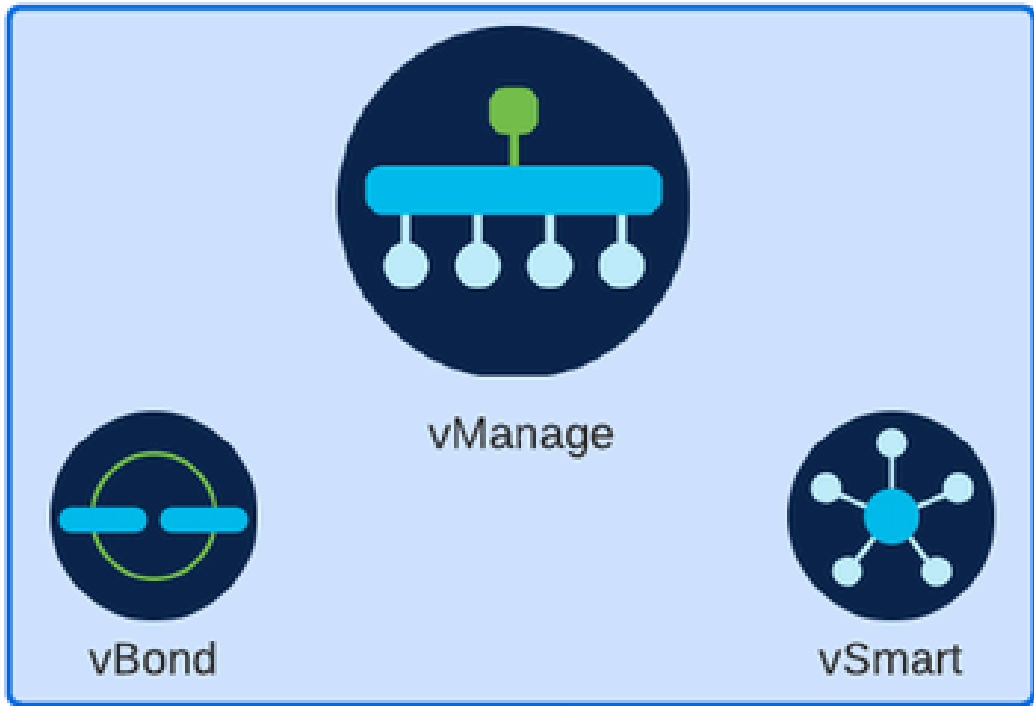
Voorbeeld van zone-paar


Nadat het zonepaar is gedefinieerd, zijn de acties die van toepassing zijn op de stromen:

- Drop: gewoon afgedankte overeenkomende stroom.
- Pass: laat pakketstroom toe zonder stateful inspection, gelijkend op de vergunningsactie in toegangslijsten. Of een pasactie in een stroom wordt ingesteld, is een terugkeerpas voor die stroom nodig.
- Inspecteren: staat voor stateful inspection van verkeer toe dat van bron naar bestemmingszone stroomt, en laat automatisch verkeersstromen toe om terug te keren.

Configureren

Netwerkdigram



 Of WAN-interface via DHCP is geconfigureerd, het is nodig om een regel te maken om zelf-zone (interface) toe te staan om het volgende-hop IP-adres te bereiken voor het geval dat het herlaadapparaat en de router een nieuw IP-adres moeten krijgen.

Besturingsplane

1. Maak de geïnspecteerde parameterkaart:

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


Het `max-incomplete tcp`

configuratiebevel wordt gebruikt om het maximumaantal onvolledige verbindingen te specificeren alvorens de zitting van TCP daling is.

Het `multi-tenancy` configuratiebevel is een globale parameter die in de configuratie ZBFW wordt vereist. Wanneer ZBFW is geconfigureerd via SD-WAN Manager GUI, wordt de regel standaard toegevoegd. Wanneer ZBFW is geconfigureerd via Command Line Interface (CLI), moet deze regel worden toegevoegd.

2. Een WAN-zone maken:

```
zone security wan
vpn 0
```

 Opmerking: Zelfzone wordt standaard gecreëerd, het is niet nodig om deze te configureren.

3. Configureer de objectgroep voor de bron- en doeladressen:

```
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. Maak de IP-toegangslijst aan:

```
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. Maak de klassenkaart:

```
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. Maak de beleidskaart om aan het zonepaar toe te voegen:

```
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. Maak het zonepaar en koppel de beleidskaart eraan:

```
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
```

Zodra de besturingsplane-stromen zijn toegestaan, kan de configuratie van het gegevensvlak worden toegepast.

Om de controle-aansluitingen te valideren, gebruikt u de opdracht EXEC:

<#root>

Device#

```
show sdwan control connections
```

Of ZBFW voor zelf-zone en wan-zone niet correct wordt geconfigureerd, de apparaten verliezen de controle verbindingen en krijgen een console fout gelijkend de volgende:

<#root>

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

Dataplane

1. Maak een security zone aan voor elke Virtual Routing and Forwarding (VRF) die nodig is:

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

3. Configureer de objectgroep voor de bron- en doeladressen:

```
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. Maak de IP-toegangslijst aan:

```
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. Maak de klassenkaart:

```
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. Maak de beleidskaart om aan het zonepaar toe te voegen:

```
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. Maak het zonepaar en koppel de beleidskaart eraan:

```
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
```

 Opmerking: Zie [CLI-functiesjablonen](#) en [CLI-sjablonen voor](#) meer informatie over het gebruik van [CLI-sjablonen](#).

Verifiëren

Om de geconfigureerde inspectie van class-map te valideren, gebruikt u de opdracht EXEC:

```
<#root>
```

```
Device#
```

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

Om de geconfigureerd te controleren, gebruikt u de opdracht EXEC:

<#root>

Device#

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

Om het geconfigureerde zonepaar te valideren, gebruikt u de opdracht EXEC:

<#root>

Device#

```
show zone-pair security
```

Om de geconfigureerde toegangslijst te valideren, gebruikt u de opdracht EXEC:

<#root>

Device#

```
show ip access-list
```

Om de geconfigureerde objectgroep te valideren, gebruikt u de opdracht EXEC:

<#root>

Device#

```
show object-group
```

Om de ZBFW-sessiestatus weer te geven, gebruikt u de opdracht 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 -
```

Om de zone-paar statistieken weer te geven, gebruikt u de opdracht 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
```

Gebruik de opdracht EXEC om de ZBFW-vervolgstatistieken weer te geven:

```
<#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

```

Gebruik de opdracht EXEC om de QFP-drop-statistieken (QuantumFlow Processor) weer te geven:

```
<#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

Gebruik de opdracht EXEC om de QFP firewall-druppels weer te geven:

<#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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.