

Konfigurieren der ZBFW über die SD-WAN-CLI-Vorlage

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfiguration](#)

[Steuern Sie Fläche](#)

[Daten-Fläche](#)

[Überprüfung](#)

Einleitung

In diesem Dokument wird die Konfiguration einer ZBFW-Richtlinie (Zone-Based Firewall) mithilfe einer Funktionsvorlage für ein CLI-Add-On von Cisco Catalyst SD-WAN Manager beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Catalyst Software-Defined Wide Area Network (SD-WAN)
- ZBFW-Basisbetrieb (Zone-Based Firewall)

Verwendete Komponenten

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

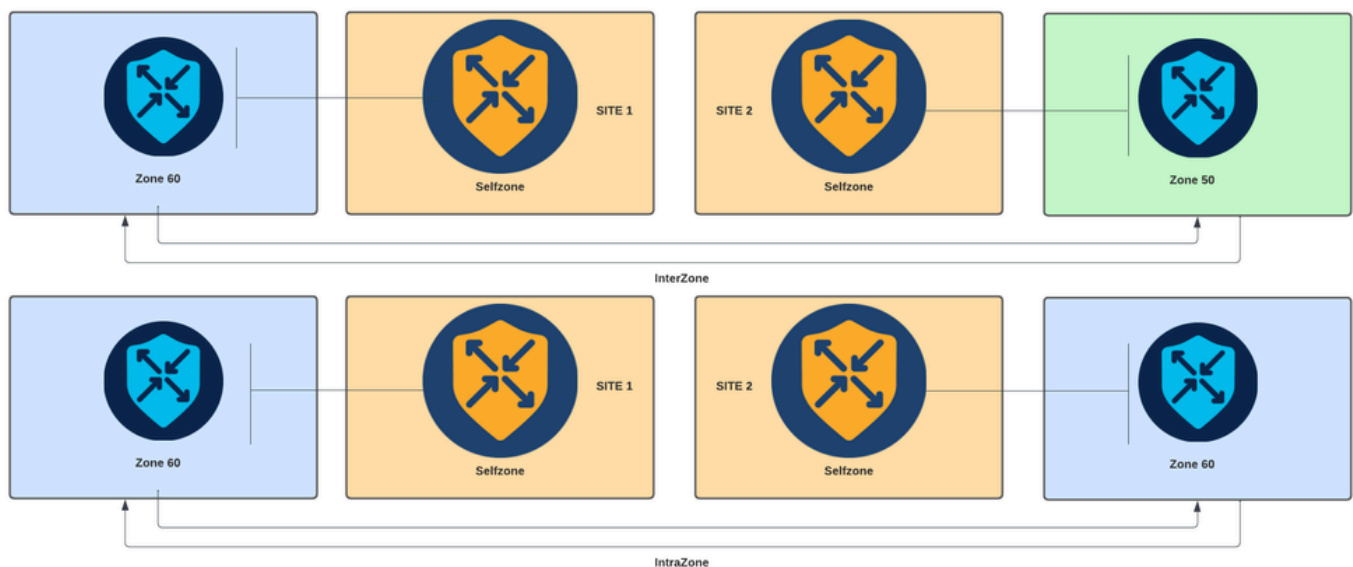
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Eine Firewall-Richtlinie ist eine Art lokalisierter Sicherheitsrichtlinie, die eine Stateful-Inspection des TCP-, UDP- und ICMP-Datenverkehrs ermöglicht. Dabei wird das Konzept der Zonen verwendet. Daher können Datenverkehrsflüsse, die von einer bestimmten Zone ausgehen, auf Basis der Richtlinie zwischen den beiden Zonen zu einer anderen Zone weitergeleitet werden.

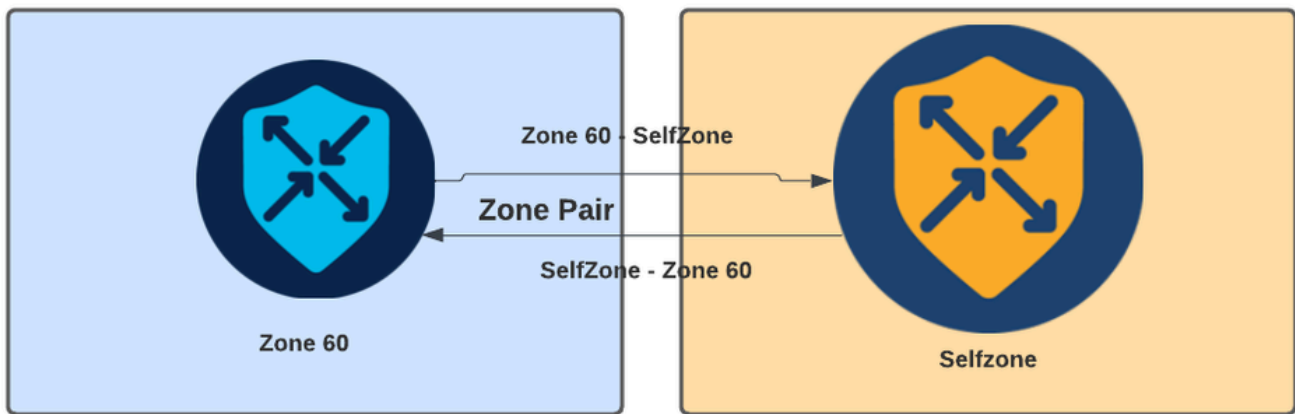
Eine Zone ist eine Gruppe aus einem oder mehreren VPNs. Folgende Zonentypen sind in ZBFW verfügbar:

- Quellzone: Eine Gruppe von VPNs, die den Datenverkehrsfluss anstoßen. Ein VPN kann nur Teil einer Zone sein.
- Zielzone: Eine Gruppe von VPNs, die den Datenverkehrsfluss terminiert. Ein VPN kann nur Teil einer Zone sein.
- Interzone: Wenn der Datenverkehr zwischen verschiedenen Zonen stattfindet, wird er Interzone genannt (standardmäßig wird die Kommunikation verweigert).
- Intrazone: Sie wird als Intrazone bezeichnet, wenn der Datenverkehr durch dieselbe Zone fließt (standardmäßig ist die Kommunikation zulässig).
- Selfzone: Sie wird zur Steuerung des Datenverkehrs verwendet, der vom Router selbst stammt oder an diesen weitergeleitet wird (Standardzone wird vom System erstellt und vorkonfiguriert, standardmäßig ist die Kommunikation zulässig).



Zonenbasiertes Firewall-Diagramm

Ein weiteres Konzept, das in ZBFW verwendet wird, ist das Zonenpaar. Hierbei handelt es sich um einen Container, der eine Quellzone mit einer Zielzone verknüpft. Zonenpaare wenden eine Firewall-Richtlinie auf den Datenverkehr an, der zwischen den beiden Zonen übertragen wird.



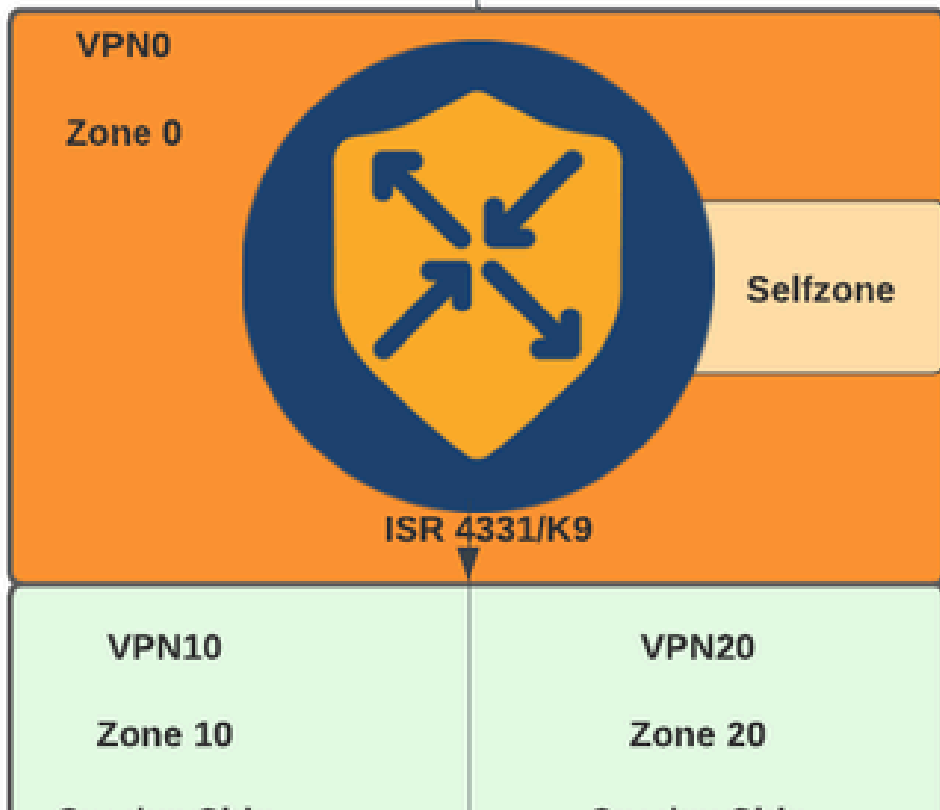
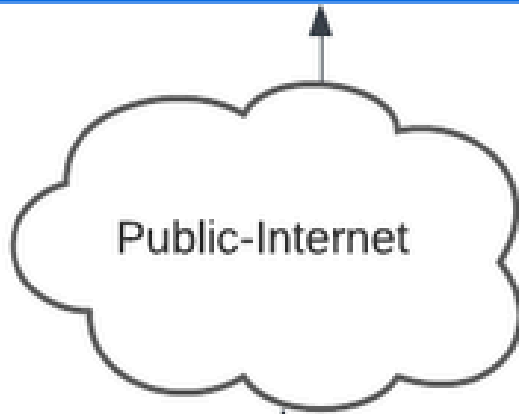
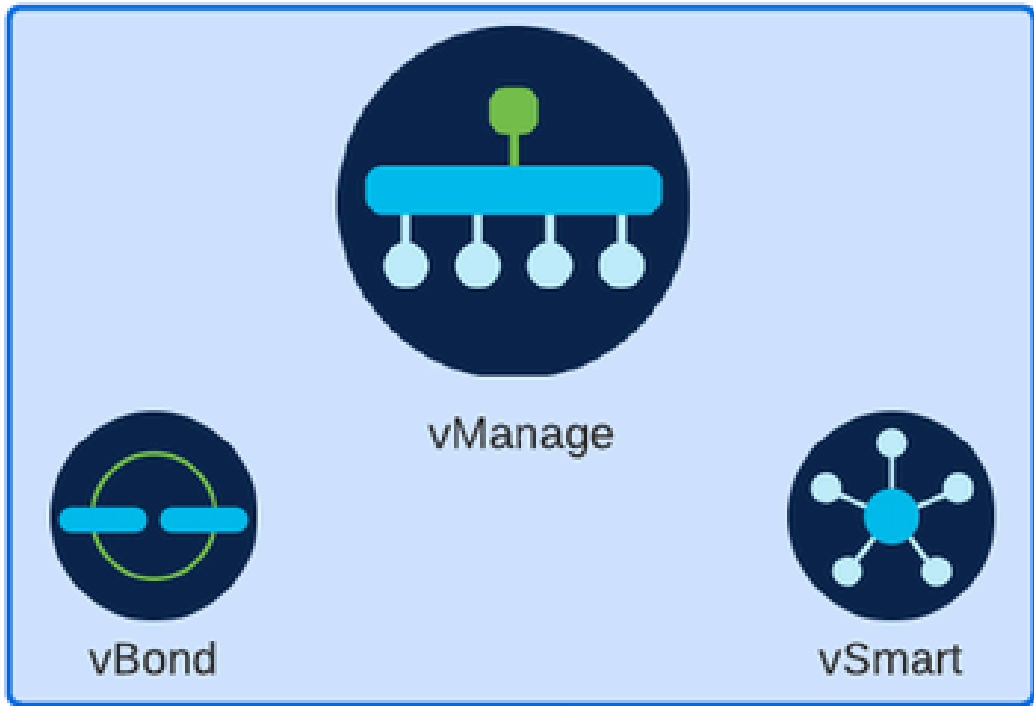
Beispiel für ein Zonenpaar


Nach der Definition des Zonenpaars gelten folgende Aktionen für die Flows:

- Drop: verwirft einfach den Matchflow.
- Bestanden: lässt den Paketfluss ohne statusbehaftete Prüfung zu, ähnlich der Genehmigungsaktion in Zugriffslisten. Unabhängig davon, ob eine Bestanden-Aktion in einem Fluss festgelegt wird, ist ein Rücklauf für diesen Fluss erforderlich.
- Inspizierung: ermöglicht die Stateful-Inspection des Datenverkehrs, der von der Quell- zur Zielzone fließt, und die automatische Rückführung des Datenverkehrs.

Konfigurieren

Netzwerkdiagramm



 Unabhängig davon, ob die WAN-Schnittstelle über DHCP konfiguriert wird, muss eine Regel erstellt werden, damit die Kernzone (Schnittstelle) die Next-Hop-IP-Adresse erreichen kann, falls das Gerät und der Router eine neue IP-Adresse erhalten müssen.

Steuern Sie Fläche

1. Erstellen Sie die Parameterzuordnung inspect:

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


Der `max-incomplete tcp`

Konfigurationsbefehl gibt die maximale Anzahl unvollständiger Verbindungen an, bevor die TCP-Sitzung beendet wird.

Der `multi-tenancy` Konfigurationsbefehl ist ein globaler Parameter, der in der ZBFW-Konfiguration erforderlich ist. Wenn ZBFW über die Benutzeroberfläche des SD-WAN-Managers konfiguriert wird, wird die Leitung standardmäßig hinzugefügt. Wenn ZBFW über eine Befehlszeilenschnittstelle (CLI) konfiguriert wird, muss diese Zeile hinzugefügt werden.

2. Erstellen Sie eine WAN-Zone:

```
zone security wan
vpn 0
```

 Anmerkung: Die Kernzone wird standardmäßig erstellt, eine Konfiguration ist nicht erforderlich.

3. Konfigurieren Sie die Objektgruppe für die Quell- und Zieladressen:

```
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. Erstellen Sie die IP-Zugriffsliste:

```
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. Erstellen Sie die Klassenzuordnung:

```
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. Erstellen Sie die Richtlinienzuordnung, um sie dem Zonenpaar hinzuzufügen:

```
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. Erstellen Sie das Zonenpaar und verknüpfen Sie die Richtlinienzuordnung damit:

```
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
```

Sobald die Datenflüsse auf der Kontrollebene zulässig sind, kann die Konfiguration der Datenebene angewendet werden.

Verwenden Sie den Befehl EXEC, um Steuerverbindungen zu validieren:

<#root>

Device#

```
show sdwan control connections
```

Unabhängig davon, ob ZBFW für die Kernzone und die WAN-Zone nicht richtig konfiguriert ist, gehen die Steuerverbindungen für die Geräte verloren, und es tritt ein Konsolenfehler auf, ähnlich dem nächsten:

<#root>

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

Daten-Fläche

1. Erstellen Sie eine Sicherheitszone für jede erforderliche Virtual Routing and Forwarding (VRF):

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

3. Konfigurieren Sie die Objektgruppe für die Quell- und Zieladressen:

```
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. Erstellen Sie die IP-Zugriffsliste:

```
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. Erstellen Sie die Klassenzuordnung:


```
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. Erstellen Sie die Richtlinienzuordnung, um sie dem Zonenpaar hinzuzufügen:

```
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. Erstellen Sie das Zonenpaar und verknüpfen Sie die Richtlinienzuordnung damit:

```
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
```

 Anmerkung: Weitere Informationen zur Verwendung von CLI-Vorlagen finden Sie unter [CLI-Add-On-Funktionsvorlagen](#) und [CLI-Vorlagen](#).

Überprüfung

Um die konfigurierte Klassenzuordnung für inspect zu validieren, verwenden Sie den Befehl EXEC:

```
<#root>
```

```
Device#
```

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

Um die konfigurierte inspect policy-map zu validieren, verwenden Sie den Befehl EXEC:

<#root>

Device#

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

Um das konfigurierte Zonenpaar zu validieren, verwenden Sie den Befehl EXEC:

<#root>

Device#

```
show zone-pair security
```

Um die konfigurierte Zugriffsliste zu validieren, verwenden Sie den Befehl EXEC:

<#root>

Device#

```
show ip access-list
```

Um die konfigurierte Objektgruppe zu validieren, verwenden Sie den EXEC-Befehl:

<#root>

Device#

```
show object-group
```

Um den ZBFW-Sitzungsstatus anzuzeigen, verwenden Sie den EXEC-Befehl:

<#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 - C
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 - C
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 - C
```

```
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 -
```

Um die Zonenpaarstatistik anzuzeigen, verwenden Sie den Befehl 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
```

Um die ZBFW-Löschstatistik anzuzeigen, verwenden Sie den EXEC-Befehl:

```
<#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

```

Verwenden Sie den EXEC-Befehl, um die Statistiken zum Ablegen von QuantumFlow Processor (QFP) anzuzeigen:

```
<#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

Um die QFP-Firewall-Drops anzuzeigen, verwenden Sie den EXEC-Befehl:

```
<#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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.