Configurazione di ZBFW dal modello SD-WAN CLI

Sommario

Introduzione

Questo documento descrive come configurare i criteri ZBFW (Zone-Based Firewall) con un modello di funzionalità aggiuntiva CLI di Cisco Catalyst SD-WAN Manager.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Un criterio firewall è un tipo di criterio di sicurezza localizzato che consente l'ispezione con conservazione dello stato dei flussi di traffico dati TCP, UDP e ICMP. Si basa sul concetto di zone; pertanto, i flussi di traffico provenienti da una determinata zona possono passare a un'altra zona in base ai criteri applicati tra le due zone.

Una zona è un gruppo di una o più VPN. I tipi di zone esistenti in ZBFW sono:

- Zona di origine: gruppo di VPN che originano i flussi di traffico dei dati. Una VPN può far parte di una sola zona.
- Zona di destinazione: un gruppo di VPN che termina i flussi di traffico dati. Una VPN può far parte di una sola zona.
- Interzona: è chiamata interzona quando il flusso del traffico tra zone diverse (per impostazione predefinita la comunicazione è negata).
- Intrazona: è chiamata intrazone quando il traffico attraversa la stessa zona (per impostazione predefinita la comunicazione è consentita).
- Selfzone: viene utilizzato per controllare il traffico che proviene dal router o è diretto al router stesso (zona predefinita creata e preconfigurata dal sistema; per impostazione predefinita, la comunicazione è consentita).

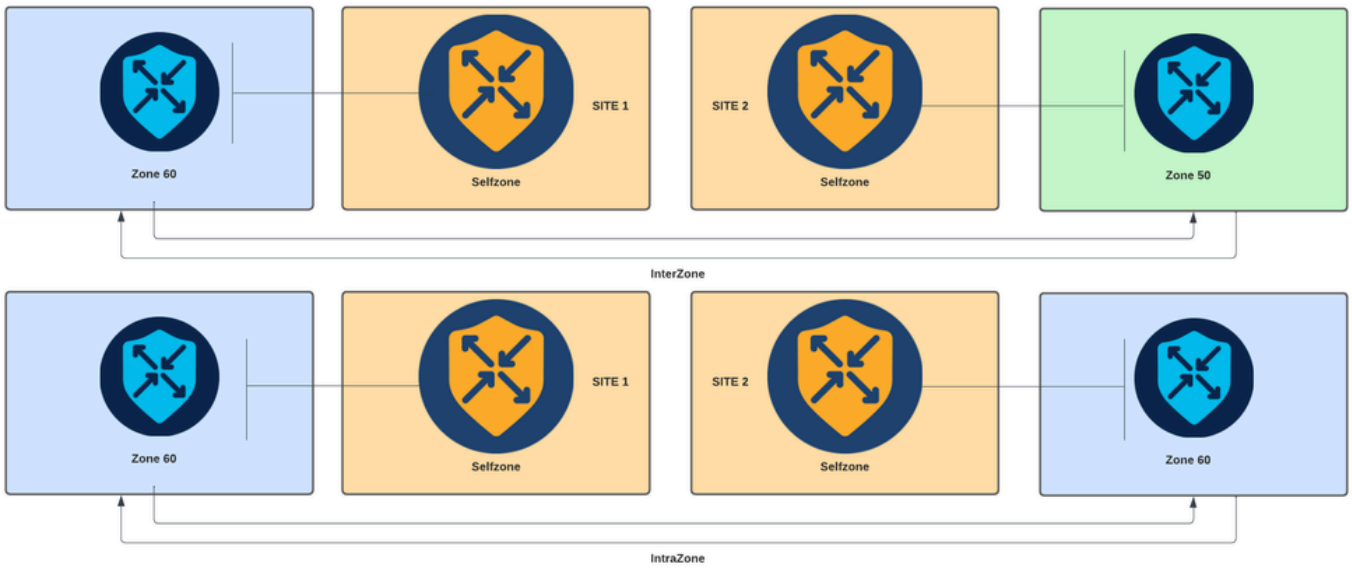
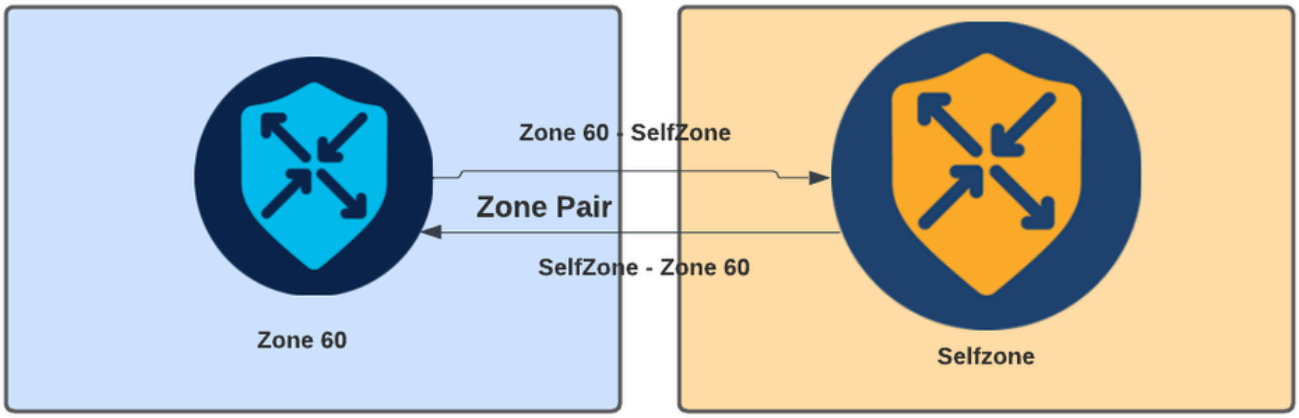


Diagramma del firewall basato su zone

Un altro concetto utilizzato in ZBFW è la coppia di zone, ovvero un contenitore che associa una zona di origine a una zona di destinazione. Le coppie di zone applicano un criterio firewall al traffico che scorre tra le due zone.



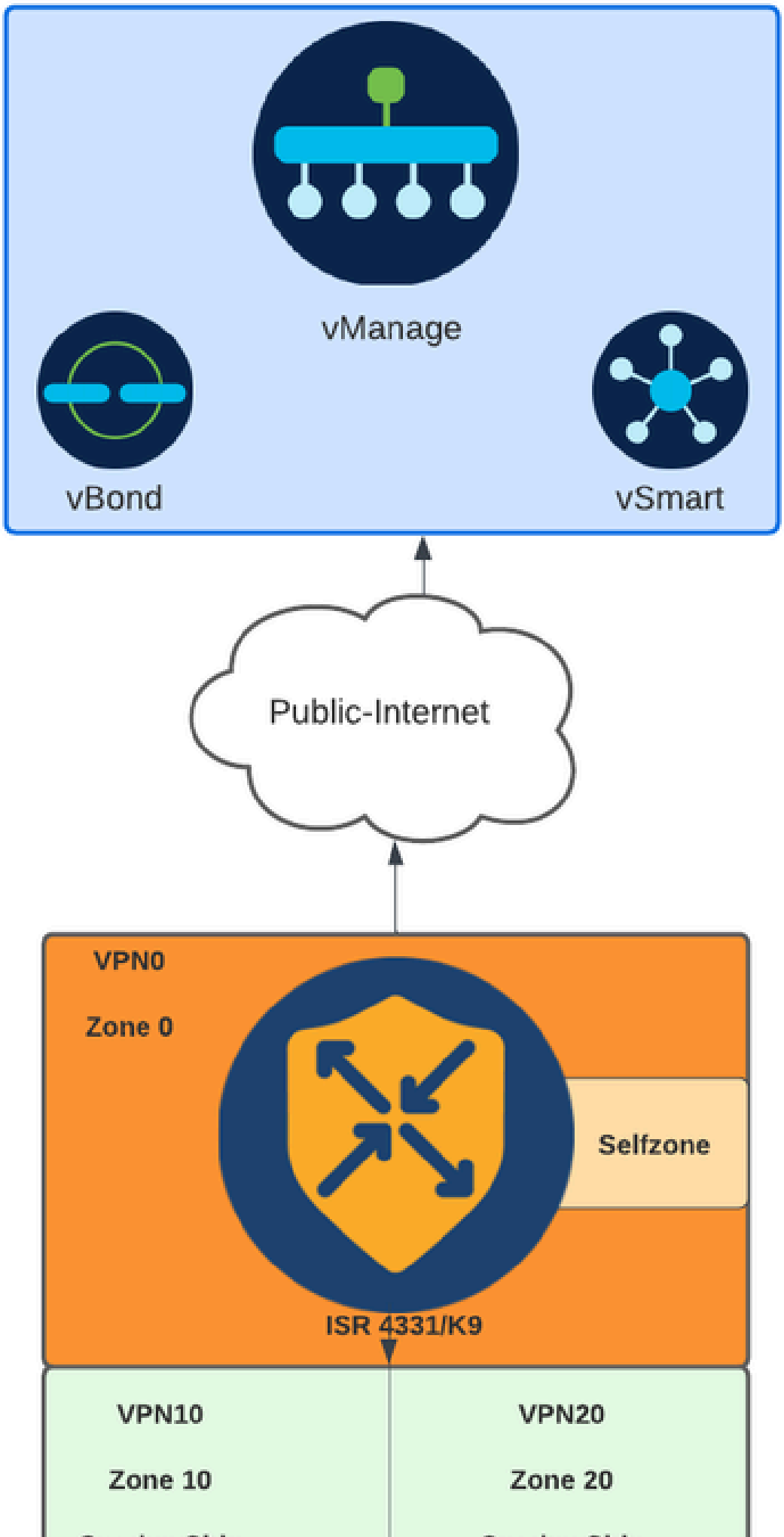
Esempio di coppia di zone

Dopo aver definito la coppia di zone, le azioni applicabili ai flussi sono le seguenti:

- Caduta: elimina semplicemente il flusso di corrispondenza.
- Accetta: consente il flusso di pacchetti senza ispezione con conservazione dello stato, in modo simile all'azione di autorizzazione negli elenchi degli accessi. Se in un flusso viene impostata un'azione di accettazione, è necessario un passaggio di ritorno per tale flusso.
- Ispeziona: permette l'ispezione con conservazione dello stato del traffico che scorre da una zona di origine a una di destinazione e permette automaticamente la restituzione dei flussi di traffico.

Configurazione

Esempio di rete


vManage
vBond
vSmart
Public-Internet
VPN0
Zone 0
Selfzone
ISR 4331/K9
VPN10
Zone 10
VPN20
Zone 20

Se l'interfaccia WAN è configurata tramite DHCP, è necessario creare una regola che consenta alla zona autonoma (interfaccia) di raggiungere l'indirizzo IP dell'hop successivo nel caso in cui il dispositivo di ricaricamento e il router abbiano bisogno di ottenere un nuovo indirizzo IP.

Piano di controllo

1. Creare la mappa dei parametri di ispezione:

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

Il comando max-incomplete tcp configuration viene utilizzato per specificare il numero massimo di connessioni incomplete prima che la sessione TCP venga interrotta.

Il comando **multi-tenancy** configuration è un parametro globale richiesto nella configurazione ZBFW. Quando ZBFW è configurato tramite l'interfaccia utente di SD-WAN Manager, la linea viene aggiunta per impostazione predefinita. Quando ZBFW è configurato tramite l'interfaccia della riga di comando (CLI), questa riga deve essere aggiunta.

2. Creare una zona WAN:

```
zone security wan
vpn 0
```

Nota: L'area autonoma viene creata per impostazione predefinita e non è necessario configurarla.

3. Configurare il gruppo di oggetti per gli indirizzi di origine e di destinazione:

```
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. Creare l'elenco degli accessi 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. Creare la mappa delle classi:

```
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. Creare la mappa dei criteri da aggiungere alla coppia di zone:

```
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. Creare la coppia di zone e collegarvi la mappa dei criteri:

```
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 volta che i flussi del piano di controllo sono consentiti, è possibile applicare la configurazione del piano dati.

Per convalidare le connessioni di controllo, utilizzare il comando EXEC:

<#root>

```
Device#
```

show sdwan control connections

Se ZBFW per self-zone e wan-zone non è configurato correttamente, i dispositivi perdono le connessioni di controllo e ottengono un errore della console simile al seguente:

<#root>

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

Piano dati

1. Creare una zona di sicurezza per ogni VRF (Virtual Routing and Forwarding) necessario:

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

3. Configurare il gruppo di oggetti per gli indirizzi di origine e di destinazione:

```
 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. Creare l'elenco degli accessi 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. Creare la mappa delle classi:

```
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. Creare la mappa dei criteri da aggiungere alla coppia di zone:

```
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. Creare la coppia di zone e collegarvi la mappa dei criteri:

```
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: Per ulteriori informazioni sull'utilizzo dei modelli CLI, vedere Modelli delle funzionalità aggiuntive e modelli CLI di CLI.

Verifica

Per convalidare la mappa-classi di ispezione configurata, utilizzare il comando EXEC:

<#root>

Device#

show class-map type inspect

Per convalidare la mappa-criteri di ispezione configurata, utilizzare il comando EXEC:

<#root>

Device#

show policy-map type inspect

Per convalidare la coppia di zone configurata, utilizzare il comando EXEC:

<#root>

Device#

show zone-pair security

Per convalidare l'elenco degli accessi configurato, usare il comando EXEC:

<#root>

Device#

show ip access-list

Per convalidare l'object group configurato, utilizzare il comando EXEC:

<#root>

Device#

show object-group

Per visualizzare lo stato della sessione ZBFW, usare il comando EXEC:

<#root>

Device#

show sdwan zonebfwdp 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 - 
```

Per visualizzare le statistiche sulla coppia di zone, utilizzare il 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

Per visualizzare le statistiche di rilascio ZBFW, usare il comando EXEC:

<#root>

```
Device#
```

show sdwan zbfw drop-statistics

```
zbfw drop-statistics catch-all                          0
```

```
zbfw drop-statistics l4-max-halfsession                0
zbfw drop-statistics l4-session-limit                  0
zbfw drop-statistics l4-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 l4-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
```

Per visualizzare le statistiche di rilascio di QuantumFlow Processor (QFP), utilizzare il 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
```

Per visualizzare le perdite del firewall QFP, utilizzare il 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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).