Informazioni sui pacchetti RST inviati da Secure Firewall

Sommario

Introduzione

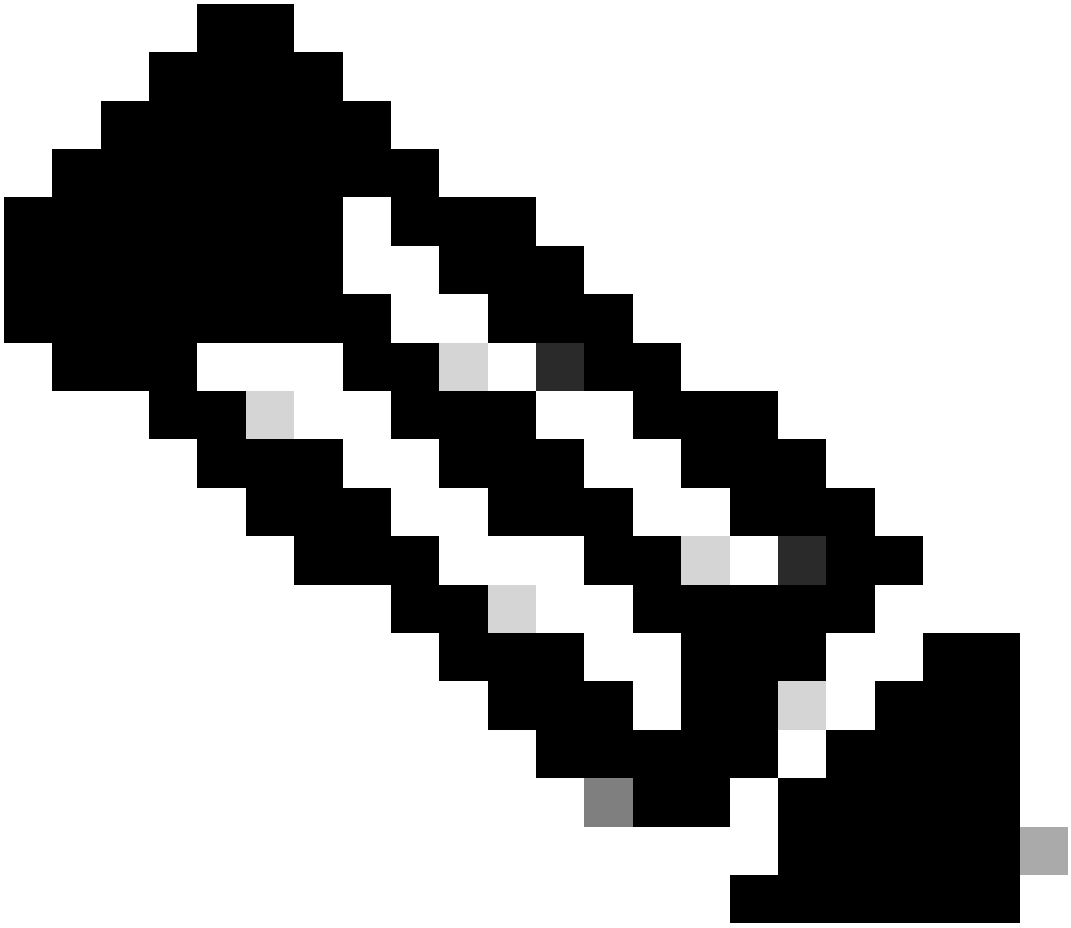
In questo documento viene spiegato come il dispositivo Cisco Firewall invia pacchetti di tipo reset TCP alle sessioni TCP che cercano di attraversare il firewall.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Flusso di pacchetti ASA
- Flusso pacchetto FTD
- Acquisizioni pacchetti ASA/FTD



Nota: questo comportamento descritto si applica alle appliance ASA e Secure Firewall Threat Defense.

Componenti usati

Le informazioni fornite in questo documento si basano sul seguente software:

- ASA
- Secure Firewall Threat Defense FTD

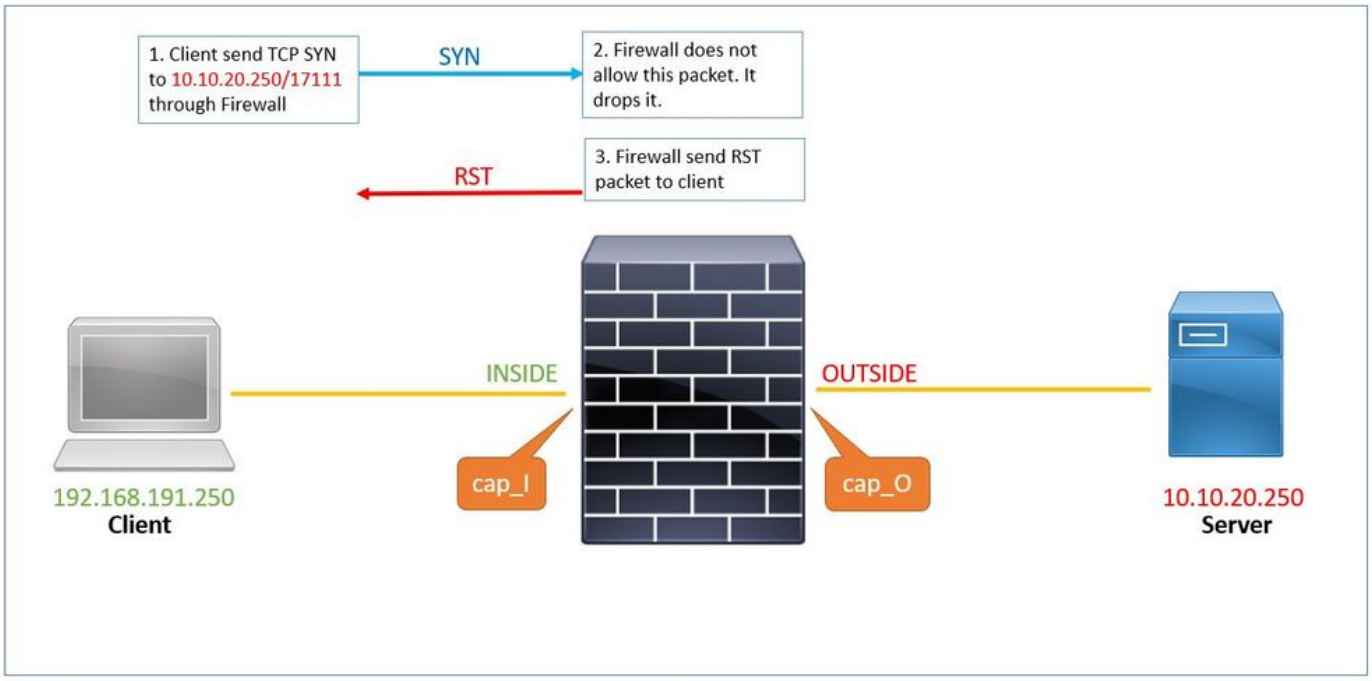
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Risoluzione dei problemi

Il firewall invia reimpostazioni TCP per le sessioni TCP che tentano di attraversare il firewall e che vengono negate dal firewall in base agli elenchi degli accessi. Il firewall invia inoltre reimpostazioni per i pacchetti consentiti da un elenco degli accessi, ma che non appartengono a una connessione esistente nel firewall e che pertanto viene negata dalla funzionalità di conservazione dello stato.

Caso di studio 1: il servizio resetoutbound è abilitato e il traffico da client a server è negato.

Per impostazione predefinita, il servizio **resetoutbound** è abilitato per tutte le interfacce. In questo caso di studio non esiste una regola per consentire il traffico da client a server.



Di seguito sono riportate le clip configurate nel firewall:

```
# show capture
capture cap_I type raw-data trace trace-count 50 interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.191.250 host 10.10.20.250
capture cap_O type raw-data trace trace-count 50 interface OUTSIDE [Capturing - 0 bytes]
match tcp host 192.168.191.250 host 10.10.20.250
capture asp type asp-drop all [Capturing - 0 bytes]
match tcp host 192.168.191.250 host 10.10.20.250
```

Il servizio resetoutbound è abilitato per impostazione predefinita. Pertanto, se l'output del show run service comando non visualizza nulla, significa che è abilitato:

```
# show run service ...
```

1. Il client invia TCP SYN al server 10.10.20.250/17111 tramite il firewall. Numero pacchetto 1 nell'acquisizione:

```
# show capture cap_I
1: 19:48:55.512500 192.168.191.250.46118 > 10.10.20.250.17111: S 3490277958:3490277958(0) win 29200 <ms
```

2. Poiché non è disponibile un ACL per consentire il traffico, il firewall sicuro scarta il pacchetto con il acl-drop motivo. Questo pacchetto viene acquisito nell'acquisizione asp-drop.

```
# show capture cap_I packet-number 1 trace det

1: 19:48:55.512500 a2c7.1e00.0004 0050.56b3.05b1 0x0800 Length: 74
192.168.191.250.46118 > 10.10.20.250.17111: S [tcp sum ok] 3490277958:3490277958(0) win 29200 <mss 1380
    (DF) (ttl 49, id 60335)

<output removed>

Subtype: log
Result: DROP
Config:
access-group allow_all global
access-list allow_all extended deny ip any any
Additional Information:

<output removed>

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
```

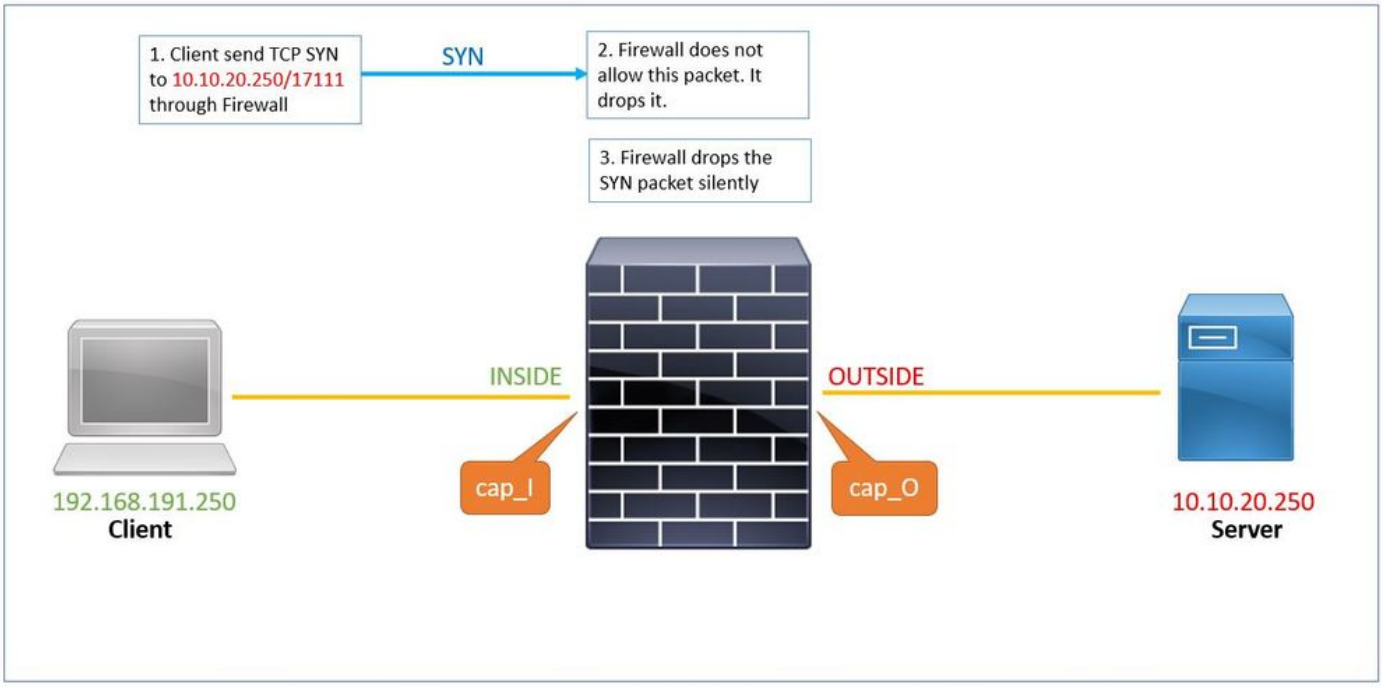
```
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x0000561961c8333f flow
```

3. Il firewall invia un pacchetto RST con l'indirizzo IP del server come indirizzo IP di origine. Numero pacchetto 2 nell'acquisizione:

```
# show capture cap_I
1: 19:48:55.512500 192.168.191.250.46118 > 10.10.20.250.17111: S 3490277958:3490277958(0) win 29200 <ms
        timestamp 2096884214 0,nop,wscale 7>
2: 19:48:55.512806 10.10.20.250.17111 > 192.168.191.250.46118: R 0:0(0) ack 3490277959 win 29200
```

Caso di studio 2: reimpostazione del servizio in uscita non abilitata e traffico da client a server negato.

Nel caso studio 2, non esiste alcuna regola per consentire il traffico da client a server e il servizio **reset outbound** è disabilitato.



Il comandoshow run service visualizza che il servizio **resetoutbound** è disabilitato.

```
# show run service
no service resetoutbound
```

1. Il client invia TCP al server 10.10.20.250/17111 attraverso il firewall. Numero pacchetto 1 nell'acquisizione:

```
# show capture cap_I

1: 19:48:55.512500 192.168.191.250.46118 > 10.10.20.250.17111: S 3490277958:3490277958(0) win 29200
<mss 1380,sackOK,timestamp 2096884214 0,nop,wscale 7>
```

2. Poiché non è disponibile un ACL per consentire il traffico, il firewall sicuro scarta il pacchetto acl-drop con motivo. Questo pacchetto viene acquisito in **asp-drop capture**.

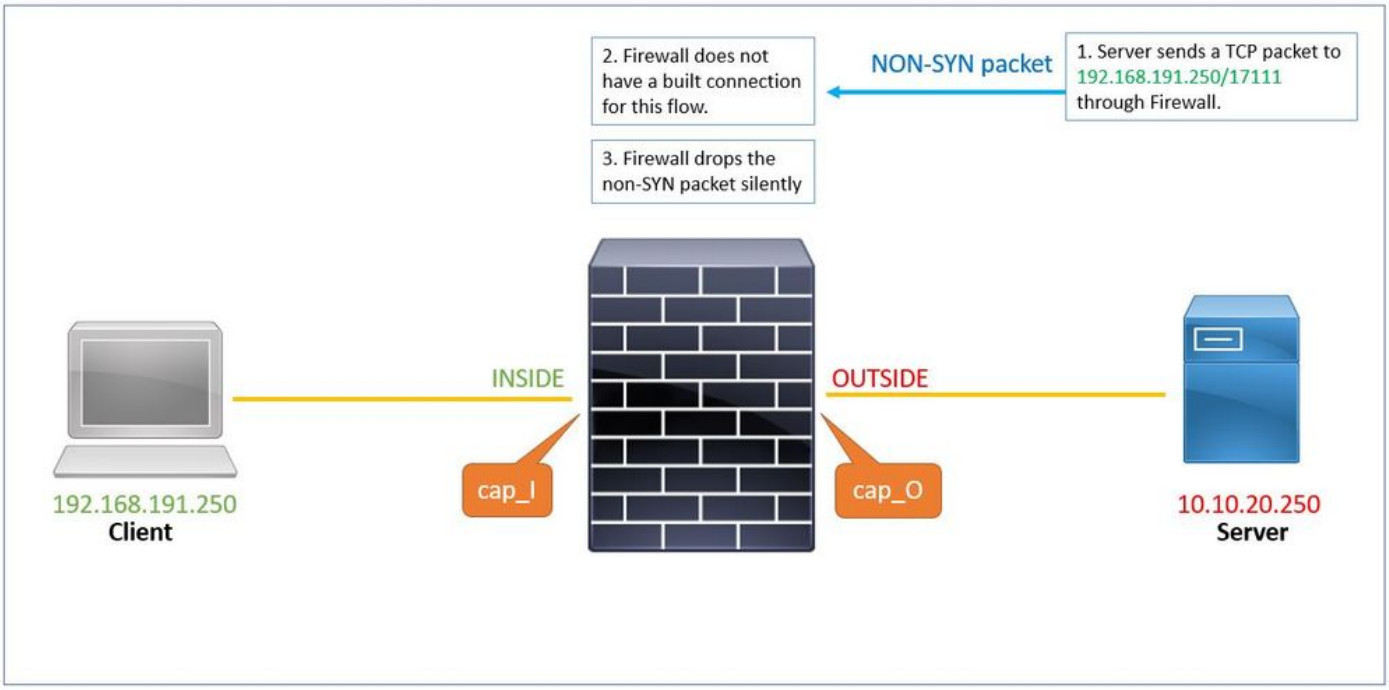
```
# show capture cap_I packet-number 1 trace det

1: 19:48:55.512500 a2c7.1e00.0004 0050.56b3.05b1 0x0800 Length: 74 192.168.191.250.46118 > 10.10.20.250
```

3. Il comando **asp-drop capture** mostra il pacchetto SYN, ma non il pacchetto RST inviato nuovamente cap_I capture tramite l'interfaccia interna:

```
# show cap cap_I
1: 23:58:32.850755 192.168.191.250.46118 > 10.10.20.250.17111: S 3490277958:3490277958(0) win 29200 <ms

# show cap asp
1: 23:58:32.850999 192.168.191.250.46118 > 10.10.20.250.17111: S 3490277958:3490277958(0) win 29200 <ms
```

Caso aziendale 3: Resetoutbound del servizio disabilitato (impostazione predefinita) Resetinbound del servizio disabilitato (impostazione predefinita)

Per impostazione predefinita, il **reimpostazione del servizio in uscita** è abilitato per tutte le interfacce e il servizio **reimpostazione in entrata** è disabilitato.



1. Il server invia un pacchetto TCP (SYN/ACK) al client attraverso il firewall. Il firewall non dispone di una connessione predefinita per questo flusso.

```
# show capture cap_O

1: 00:22:35.111993 10.10.20.250.17111 > 192.168.191.250.46118: S 3475024584:3475024584(0) ack 349027795
```

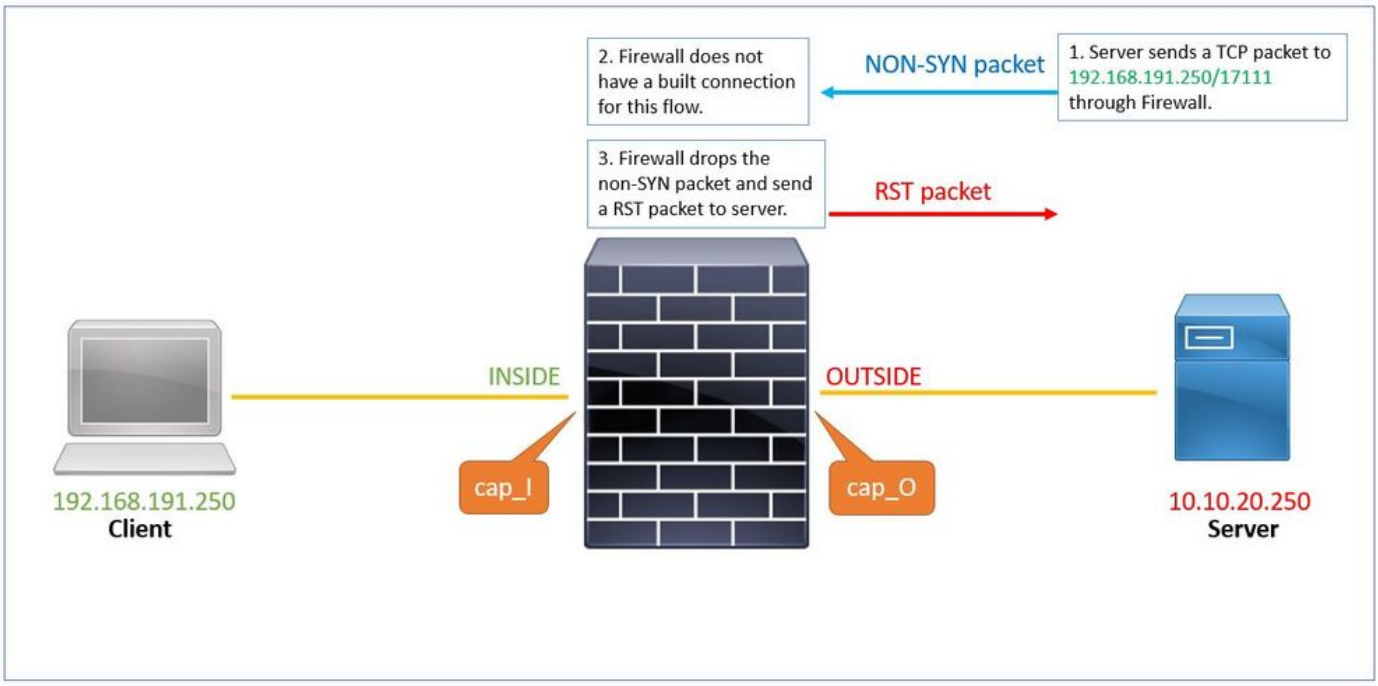
2. La reimpostazione non viene inviata dal firewall al server. Questo pacchetto SYN/ACK viene scartato in modo invisibile all'utente con il motivo tcp-not-syn. Viene catturato anche in asp-drop capture.

```
# show capture cap_O packet-number 1 trace detail
1: 00:22:35.111993 a2c7.1e00.003e 0050.56b3.1ef5 0x0800 Length: 70
10.10.20.250.17111 > 192.168.191.250.46118: S [tcp sum ok] 3475024584:3475024584(0) ack 3490277959 win
   (DF) (ttl 255, id 62104)

<output removed>

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
output-interface: INSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (tcp-not-syn) First TCP packet not SYN, Drop-location: frame 0x0000561961c89aaa flow (NA)/
</pre
```

```
# show capture asp

1: 00:22:35.112176 10.10.20.250.17111 > 192.168.191.250.46118: S 3475024584:3475024584(0) ack 349027795
```

Studio del caso 4: il servizio resetoutbound è disabilitato (per impostazione predefinita). Il servizio resetinbound è disabilitato.

per impostazione predefinita, service **resetoutbound** è disabilitato per tutte le interfacce e service **resetinbound** è disabilitato anche con il comando di configurazione.



Nell'output del show run service comando viene visualizzato che il comando **resetoutbound** è disabilitato (per impostazione predefinita) e il comando di configurazione **resetinbound** lo disabilita.

```
# show run service
service resetinbound
```

1. Il server invia un pacchetto TCP (SYN/ACK) al client attraverso il firewall.

```
# show cap cap_O

1: 00:32:26.434395 10.10.20.250.17111 > 192.168.191.250.46118: S 3475024584:3475024584(0) ack 349027795
```

2. Il firewall non dispone di una connessione predefinita per questo flusso e la scarta. Il comandoasp-drop captures mostra il pacchetto:

```
# show capture cap_O packet-number 1 trace detail
1: OO:32:26.434395 a2c7.1eOO.003e 0050.56b3.1ef5 0x0800 Length: 70
10.10.20.250.17111 > 192.168.191.250.46118: S [tcp sum ok] 3475024584:3475024584(0) ack 3490277959 win
   (DF) (ttl 255, id 62104)

<output removed>

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
output-interface: INSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (tcp-not-syn) First TCP packet not SYN, Drop-location: frame 0x0000561961c89aaa flow (NA)/
```

3. Poiché il servizio **viene reimpostato in entrata**, il firewall invia un pacchetto RST al server con l'indirizzo IP di origine del client.

```
# show capture cap_O
1: OO:32:26.434395 10.10.20.250.17111 > 192.168.191.250.46118: S 3475024584:3475024584(0) ack 349027795
2: OO:32:26.434608 192.168.191.250.46118 > 10.10.20.250.17111: R 3490277959:3490277959(0) ack 347502458
```

Informazioni correlate

- **Supporto tecnico Cisco e download**

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).