Understand RST Packets Sent by Secure Firewall (Inzicht in RST-pakketten verzonden via beveiligde firewall)

Inhoud

Inleiding

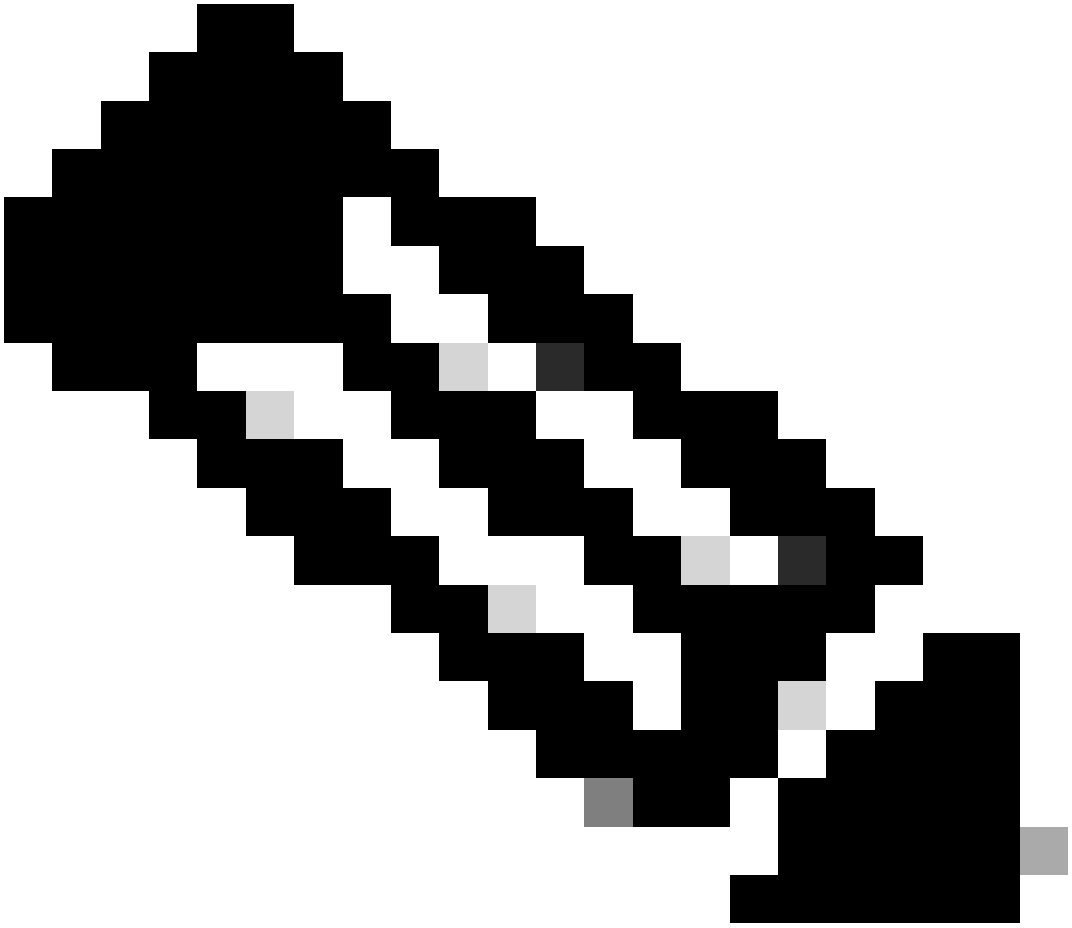
In dit document wordt het gedrag van een Cisco-firewall beschreven wanneer TCP-resets worden verzonden voor TCP-sessies die proberen de firewall over te dragen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ASA-pakketstroom
- FTD-pakketstroom
- ASA/FTD-pakketvastlegging



Opmerking: dit beschreven gedrag is van toepassing op ASA en Secure Firewall Threat Defence.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze software:

- ASA
- Secure Firewall Threat Defence (FTD)

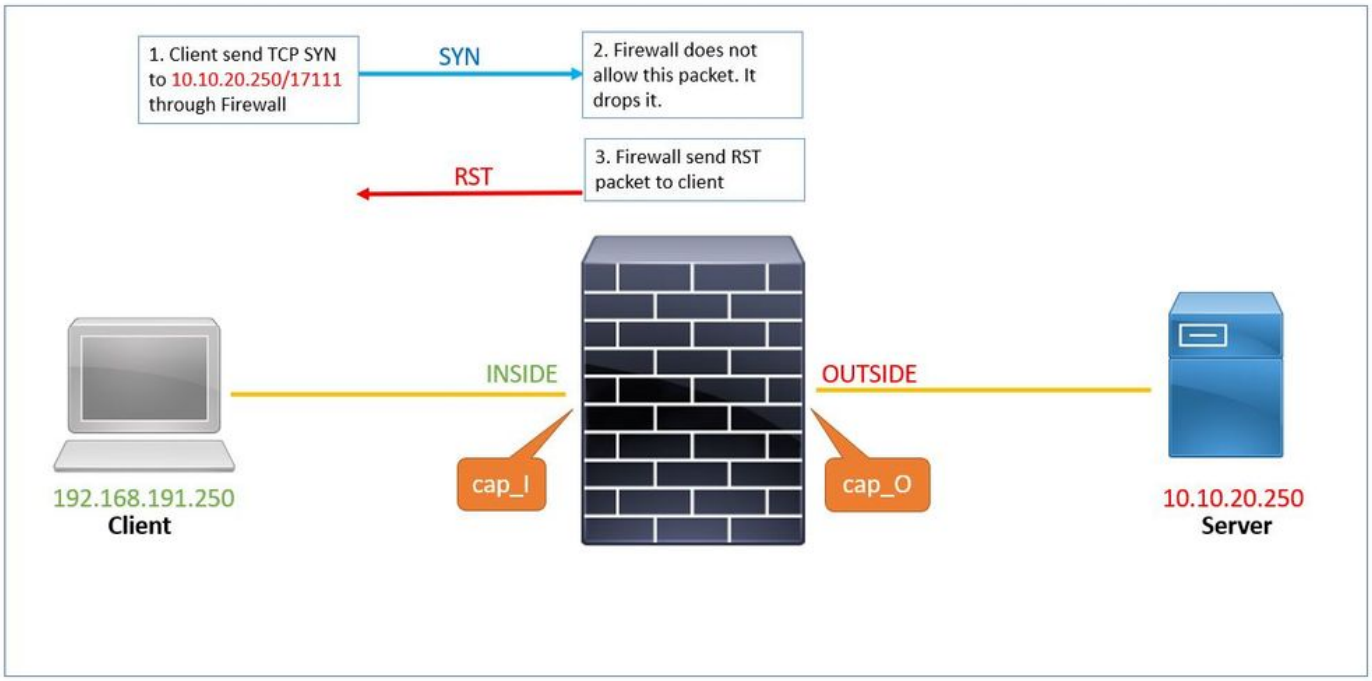
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Problemen oplossen

De firewall verzendt TCP-reset voor TCP-sessies die proberen de firewall te doorsturen en die worden geweigerd door de firewall op basis van toegangslijsten. De firewall verzendt ook resets voor pakketten die zijn toegestaan door een toegangslijst, maar die niet behoren tot een verbinding die bestaat in de firewall en daarom wordt ontkend door de stateful optie.

Case Study 1: De service resetoutbound is ingeschakeld en de traffic client-to-server wordt geweigerd.

Door gebrek, wordt de dienst **terugkomend** toegelaten voor alle interfaces. In deze casestudy is er geen regel om client-to-server verkeer toe te staan.



Dit zijn de opnamen die in de firewall zijn geconfigureerd:

```
# 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
```

Service reset is standaard ingeschakeld. Daarom, als de output van het show run service bevel niets toont, betekent dat het wordt toegelaten:

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

1. De client verzendt TCP/SYN via Firewall naar server 10.10.20.250/17111. Packet nummer 1 in deze opname:

```
# 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. Aangezien er geen ACL is om dit verkeer toe te staan, laat de Veilige Firewall dit pakket met redenacl-drop vallen. Dit pakket wordt opgenomen in de asp-drop-opname.

```
# 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
```

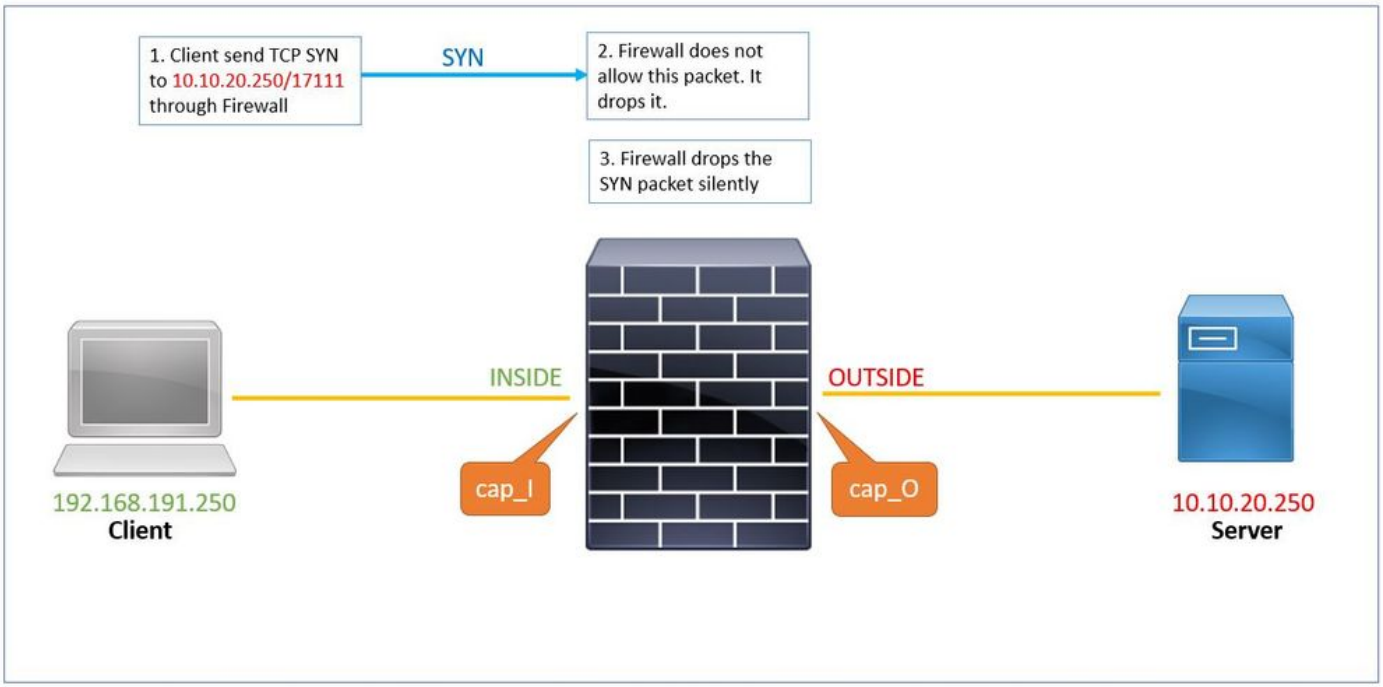
```
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x0000561961c8333f flow
```

3. De firewall stuurt een RST-pakket met het IP-adres van de server als het IP-adres van de bron. Packet nummer 2 in deze opname:

```
# 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
```

Case Study 2: Service reset niet ingeschakeld en traffic client-to-server wordt geweigerd.

In Case Study 2 is er geen regel om client-to-server verkeer toe te staan en is de **terugzetten** van de service uitgeschakeld.



Het show run service bevel toont dat de dienst **terugkomend** gehandicapt is.

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

1. De client stuurt TCP via Firewall naar server 10.10.20.250/17111. Packet nummer 1 in deze opname:

```
# 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. Aangezien er geen ACL is om dit verkeer toe te staan, laat de beveiligde firewall dit pakket met acl-drop reden vallen. Dit pakket wordt opgenomen in de **asp-drop capture**.

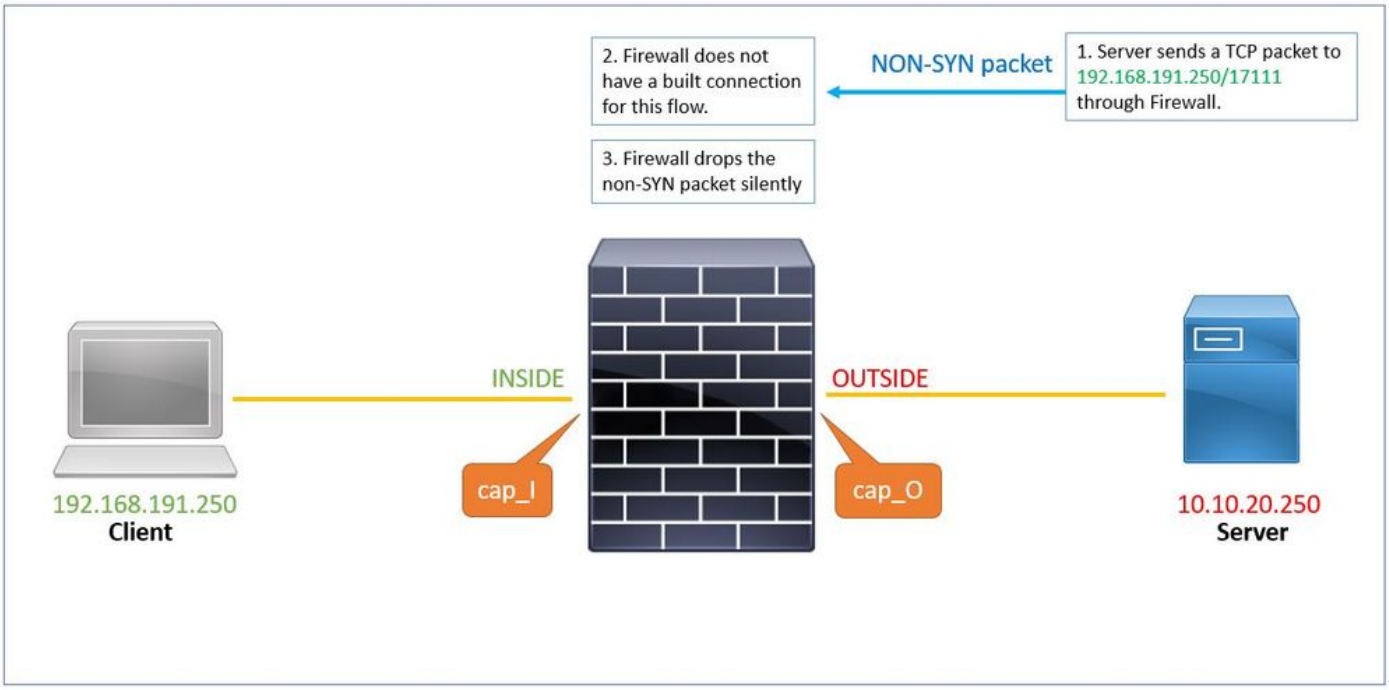
```
# show capture cap_I packet-number 1 trace det

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

3. De **asp-drop capture** projector toont het SYN-pakket maar er is geen RST-pakket teruggestuurd cap_I capture via de interne interface:

```
# 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
```

Case Study 3: Service reset-uitgaande uitgeschakeld (standaard): service-reset uitgeschakeld (standaard)

Door gebrek, de dienst **resetoutbound** wordt toegelaten voor alle interfaces en de dienst **resetbound** is gehandicapt.



1. De server verzendt een TCP-pakket (SYN/ACK) naar de client via de firewall. De firewall heeft geen ingebouwde verbinding voor deze stroom.

```
# 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
```

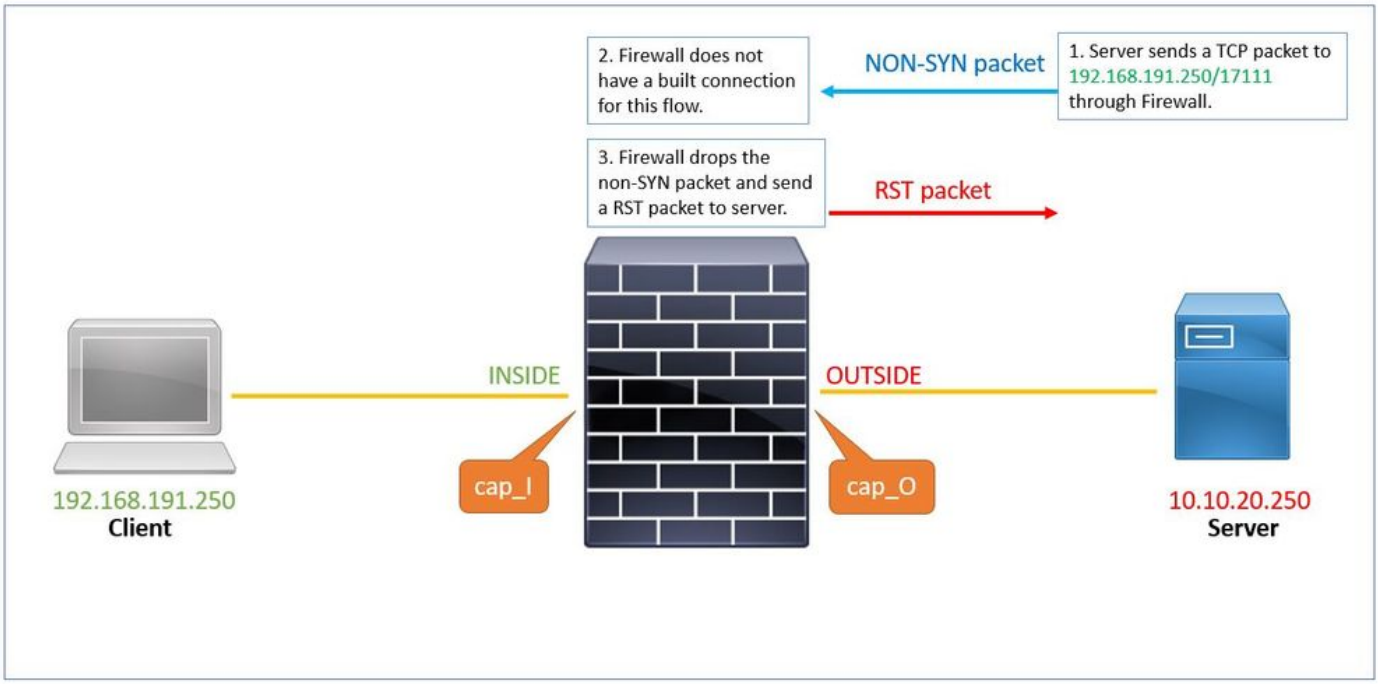
2. Reset wordt niet verzonden van Firewall naar server. Dit SYN/ACK pakket wordt in stilte met reden tcp-not-syn gevallen. Het is ook in asp-drop capture gevangengenomen.

```
# 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
```

Case Study 4: Service reset-uitgaande uitgeschakeld (standaard)-service resetten uitgeschakeld.

Door gebrek, de dienst **teruggaand** is gehandicapt voor alle interfaces en de dienst **terugstellen** is gehandicapt ook met configuratiebevel.



De output van het show run service bevel toont dat de dienst **teruggaand** (door gebrek) gehandicapt is en de dienst **terugkomend** door configuratiebevel gehandicapt is.

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

1. De server verzendt een TCP-pakket (SYN/ACK) naar de client via de 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. De firewall heeft geen ingebouwde verbinding voor deze stroom en laat deze vallen. Het asp-drop captures pakket wordt getoond:

```
# 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. Aangezien de service is **hersteld**, stuurt de firewall een RST-pakket naar de server met het bronip-adres van de 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
```

Gerelateerde informatie

- **Cisco Technical Support en downloads**

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.