

# Probleemoplossing voor Cisco IOS-firewallconfiguraties

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document bevat informatie die u kunt gebruiken om problemen op te lossen met configuraties van Cisco IOS®-firewalls.

## Voorwaarden

### Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

### Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

### Conventies

Raadpleeg [Cisco Technical Tips Conventions](#) (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

## Problemen oplossen

Opmerking: Raadpleeg [Important Information on Debug Commands](#) (Belangrijke informatie over opdrachten met debug) voordat u debug -opdrachten opgeeft.

- Om een toegangslijst om te keren (te verwijderen), zet een "nee" voor het bevel van de toegangsgroep in de wijze van de interfaceconfiguratie:

```
<#root>
```

```
int
```

```
no ip access-group # in|out
```

- Als te veel verkeer wordt ontkend, bestudeer de logica van uw lijst of probeer om een extra bredere lijst te bepalen, en pas het in plaats daarvan toe. Voorbeeld:

```
<#root>
```

```
access-list # permit tcp any any  
access-list # permit udp any any  
access-list # permit icmp any any  
int
```

```
ip access-group # in|out
```

- De opdracht IP-toegangslijsten tonen toont welke toegangslijsten worden toegepast en welk verkeer door deze lijsten wordt geweigerd. Als u de pakkettelling bekijkt die voor en na de mislukte handeling met het bron- en bestemmingsIP-adres wordt ontkend, wordt dit nummer verhoogd als de toegangslijst verkeer blokkeert.
- Als de router niet zwaar wordt geladen, kan het zuiveren op een pakketniveau op de uitgebreide of IP inspecteren toegangslijst worden gedaan. Als de router zwaar wordt geladen, wordt het verkeer vertraagd door de router. Gebruik discretie met debugging opdrachten.

Voeg tijdelijk de opdracht zonder ip route-cache aan de interface toe:

```
<#root>
```

```
int
```

```
no ip route-cache
```

In de modus Inschakelen (maar niet configureren):

```
<#root>
```

```
term mon
```

```
debug ip packet # det
```

levert een soortgelijke output op:

```
*Mar 1 04:38:28.078: IP: s=10.31.1.161 (Serial0), d=171.68.118.100 (Ethernet0),  
g=10.31.1.21, len 100, forward
```

```
*Mar 1 04:38:28.086: IP: s=171.68.118.100 (Ethernet0), d=9.9.9.9 (Serial0), g=9.9.9.9,  
len 100, forward
```

- Uitgebreide toegangslijsten kunnen ook worden gebruikt met de optie "log" aan het einde van de verschillende instructies:

```
<#root>
```

```
access-list 101 deny ip host 171.68.118.100 host 10.31.1.161 log
```

```
access-list 101 permit ip any any
```

Daarom ziet u berichten op het scherm voor toegestaan en geweigerd verkeer:

```
*Mar 1 04:44:19.446: %SEC-6-IPACCESSLOGDP: list 111 permitted icmp 171.68.118.100  
-> 10.31.1.161 (0/0), 15 packets
```

```
*Mar 1 03:27:13.295: %SEC-6-IPACCESSLOGP: list 118 denied tcp 171.68.118.100(0)
-> 10.31.1.161(0), 1 packet
```

- Als de lijst van IP-inspecties verdacht is, wordt met de opdracht debug ip inspect <type\_of\_traffic> output geproduceerd zoals deze uitvoer:

```
Feb 14 12:41:17 10.31.1.52 56: 3d05h: CBAC* sis 258488 pak 16D0DC TCP P ack 3195751223
seq 3659219376(2) (10.31.1.5:11109) => (12.34.56.79:23)
Feb 14 12:41:17 10.31.1.52 57: 3d05h: CBAC* sis 258488 pak 17CE30 TCP P ack 3659219378
seq 3195751223(12) (10.31.1.5:11109) <= (12.34.56.79:23)
```

Raadpleeg voor deze opdrachten en andere informatie over probleemoplossing de [Proxy voor probleemoplossing](#).

## Gerelateerde informatie

- [Productondersteuning voor Cisco IOS-firewall](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

## 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.