# DHCP-client of -server met configuratie van ZBF-router

## Inhoud



## Inleiding

Dit document beschrijft hoe u een router kunt configureren die fungeert als een Dynamic Host Control Protocol (DHCP)-server of DHCP-client met de functie ZBF (Zone-Based Firewall). Omdat het vrij gebruikelijk is om DHCP en ZBF gelijktijdig ingeschakeld te hebben, helpen deze configuratietips ervoor te zorgen dat deze functies correct op elkaar inwerken.

## Voorwaarden

### Vereisten

Cisco raadt u aan bekend te zijn met de Cisco IOS® op de softwarerelease gebaseerde firewall. Raadpleeg de Zone-Based Policy Firewall Design and Application Guide voor meer informatie.

### Gebruikte componenten

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

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 de potentiële impact van elke opdracht begrijpen.

# Functieinformatie

Wanneer ZBF is ingeschakeld op een IOS-router, wordt elk verkeer naar de zelfzone (dat wil zeggen, verkeer dat bestemd is voor het beheervliegtuig van de router) standaard toegestaan in de IOS 15.x-coderegel.

Als u een beleid voor een zone (zoals 'binnen' of 'buiten') tot de zelfzone (out-to-self-beleid) of het omgekeerde (self-to-out-beleid) hebt gemaakt, moet u expliciet het toelaatbare verkeer definiëren in het beleid dat aan deze zones is gekoppeld. Gebruik de actie Inspect of pass om het toegestane verkeer te definiëren.

# Gegevensanalyse

DHCP gebruikt UDP-pakketten (User Datagram Protocol) om het DHCP-proces te voltooien. Op zone gebaseerde firewallconfiguraties die de actie voor de inspectie van deze UDP-pakketten voor uitzending specificeren, kunnen door de router worden gedropt en het DHCP-proces kan mislukken. Mogelijk ziet u dit logbericht ook:

```
%FW-6-DROP_PKT: Dropping udp session 0.0.0.0:68 255.255.255.255:67 on zone-pair
self-out class dhcp with ip ident 0
```

Raadpleeg het probleem dat in Cisco bug-id CSCso53376 is beschreven, "ZBF-inspectie werkt niet voor uitzendverkeer".

Om dit probleem te voorkomen, wijzigt u de op een zone gebaseerde firewallconfiguratie zodat de wachtactie in plaats van de controleactie wordt toegepast op het DHCP-verkeer.

> **Opmerking**: dit is alleen nodig als er een beleid wordt toegepast op de zelfzone op de router.

# Zone-Based Firewall als DHCP-client met passactie voor UDP-verkeer

## Configureren

Deze voorbeeldconfiguratie gebruikt de reeks van de pasactie in plaats van de controleactie in de beleid-kaart voor al verkeer UDP aan of van de router.

```
zone security outside
zone security inside
```

```
interface Ethernet0/1
zone-member security outside
interface Ethernet0/2
zone-member security inside

class-map type inspect match-all dhcp
match protocol udp

policy-map type inspect out-to-self
class type inspect dhcp
pass
class class-default
drop
policy-map type inspect self-to-out
class type inspect dhcp
pass
class class-default
drop

zone-pair security out-to-self source outside destination self
service-policy type inspect out-to-self
zone-pair security self-to-out source self destination outside
service-policy type inspect self-to-out
```

### Verifiëren

Controleer de systemen om te verifiëren dat de router met succes een DHCP-adres heeft verkregen.

Wanneer zowel het uit-aan-zelf als zelf-aan-uit beleid worden gevormd om verkeer over te gaan UDP, kan de router een IP adres uit DHCP zoals aangetoond in deze syslog verkrijgen:

```
%DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1/0 assigned DHCP address 192.168.1.5,
mask 255.255.255.0
```

Wanneer slechts het uit-aan-zelfzonebeleid wordt gevormd om verkeer over te gaan UDP, kan de router ook een IP adres uit DHCP verkrijgen, en deze syslog wordt gecreëerd:

```
%DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1/0 assigned DHCP address 192.168.1.6,
mask 255.255.255.0
```

Wanneer slechts het zelf-aan-uit zonebeleid wordt gevormd om verkeer over te gaan UDP, kan de router een IP adres uit DHCP verkrijgen, en deze syslog wordt gecreëerd:

```
%DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1/0 assigned DHCP address 192.168.1.7,
mask 255.255.25
```

## Zone-Based Firewall met Pass Action voor DHCP-verkeer

### Configureren

Deze voorbeeldconfiguratie laat zien hoe u al het UDP-verkeer uit een zone in de zelfzone van uw router voorkomt, met uitzondering van DHCP-pakketten. Gebruik een toegangslijst met specifieke

poorten om alleen DHCP-verkeer toe te staan; in dit voorbeeld is UDP-poort 67 en UDP-poort 68 gespecificeerd om aan te passen. Een klasse-kaart die verwijzingen de toegang-lijst heeft de toegepaste pasactie.

```
access-list extended 111
 10 permit udp any any eq 67

access-list extended 112
 10 permit udp any any eq 68

class-map type inspect match-any self-to-out
match access-group 111
class-map type inspect match-any out-to-self
match access-group 112

zone security outside
zone security inside

interface Ethernet0/1
zone-member security outside
interface Ethernet0/2
zone-member security inside

policy-map type inspect out-to-self
class type inspect out-to-self
pass
class class-default
drop
policy-map type inspect self-to-out
class type inspect self-to-out
pass
class class-default
drop

zone-pair security out-to-self source outside destination self
service-policy type inspect out-to-self
zone-pair security self-to-out source self destination outside
service-policy type inspect self-to-out
```

## Verifiëren

De output van het overzicht **beleid-kaart type inspecteert streek-paar sessies** bevel om te bevestigen dat de router het verkeer van DHCP door de streek firewall toelaat. In deze voorbeelduitvoer geven de gemarkeerde tellers aan dat pakketten door de zone-firewall worden doorgegeven. Als deze tellers nul zijn, is er een probleem met de configuratie, of de pakketten komen niet aan de router voor verwerking.

```
router#show policy-map type inspect zone-pair sessions

policy exists on zp out-to-self
Zone-pair: out-to-self
Service-policy inspect : out-to-self
Class-map: out-to-self (match-any)
Match: access-group 112
3 packets, 924 bytes
30 second rate 0 bps
Pass
6 packets, 1848 bytes
```

```
Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes

policy exists on zp self-to-out
Zone-pair: self-to-out
Service-policy inspect : self-to-out
Class-map: self-to-out (match-any)
Match: access-group 111
6 packets, 3504 bytes
30 second rate 0 bps
Pass
6 packets, 3504 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes
```

# Scenario voor onjuiste configuraties

Dit steekproefscenario toont wat gebeurt wanneer de router verkeerd wordt gevormd om de inspecteactie voor DHCP-verkeer te specificeren. In dit scenario wordt de router geconfigureerd als DHCP-client. De router stuurt een DHCP-detectiebericht om een IP-adres te verkrijgen. De op een zone gebaseerde firewall is ingesteld om dit DHCP-verkeer te inspecteren. Dit is een voorbeeld van de ZBF-configuratie:

```
zone security outside
zone security inside

interface Ethernet0/1
zone-member security outside

interface Ethernet0/2
zone-member security inside

class-map type inspect match-all dhcp
match protocol udp

policy-map type inspect out-to-self
class type inspect dhcp
inspect
class class-default
drop
policy-map type inspect self-to-out
class type inspect dhcp
inspect
class class-default
drop

zone-pair securiy out-to-self source outside destination self
service-policy type inspect out-to-self
zone-pair security self-to-out source self destination outside
service-policy type inspect self-to-out
```

Wanneer het zelf-aan-uitbeleid met de inspect actie voor UDP verkeer wordt gevormd, wordt het DHCP-detectiepakket gelaten vallen, en deze syslog wordt gemaakt:

```
%FW-6-DROP_PKT: Dropping udp session 0.0.0.0:68 255.255.255.255:67 on zone-pair
self-out class dhcp with ip ident 0
```

Wanneer zowel het zelf-aan-uit als het uit-aan-zelf beleid met de Inspect actie voor UDP verkeer worden gevormd, wordt het DHCP-detectiepakket gelaten vallen, en deze syslog wordt gemaakt:

```
%FW-6-DROP_PKT: Dropping udp session 0.0.0.0:68 255.255.255.255:67 on zone-pair
self-out class dhcp with ip ident 0
```

Wanneer het out-to-self-beleid de ingeschakelde actie inspecteren heeft en het self-to-out beleid de pass-actie voor UDP-verkeer heeft ingeschakeld, wordt het DHCP-aanbodpakket verwijderd nadat het DHCP-detectiepakket is verzonden en wordt deze syslog gemaakt:

```
%FW-6-DROP_PKT: Dropping udp session 192.168.1.1:67 255.255.255.255:68 on zone-pair
out-self class dhcp with ip ident 0
```

# Router als DHCP-server

Als de interne interface van de routers fungeert als een DHCP-server en als de clients die verbinding maken met de interne interface de DHCP-clients zijn, is dit DHCP-verkeer standaard toegestaan als er geen interne-to-zelf of zelf-naar-interne zone beleid is.

Als een van deze beleidsregels echter bestaat, moet u een pass-actie configureren voor het verkeer van belang (UDP-poort 67 of UDP-poort 68) in het servicebeleid voor het zonepaar.

# Problemen oplossen

Er is momenteel geen specifieke informatie over probleemoplossing beschikbaar voor deze configuraties.

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.