# ASA/PIX met RIP-configuratievoorbeeld

## Inhoud



## Inleiding

Dit document legt uit hoe te om de Cisco ASA te configureren om routes door Routing Information Protocol (RIP) te leren, verificatie en herdistributie uit te voeren.

Raadpleeg PIX/ASA 8.X: Het configureren van HTTP op de Cisco adaptieve security applicatie (ASA) voor meer informatie over de configuratie van Ecu.

**Opmerking:** Deze documentconfiguratie is gebaseerd op RIP versie 2.

**Opmerking:** Asymmetrische routing wordt niet ondersteund in ASA/PIX.

## Voorwaarden

### Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Cisco ASA/PIX moet versie 7.x of hoger uitvoeren.
- RIP wordt niet ondersteund in multi-context-modus; het wordt alleen in één modus ondersteund.

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 5500 Series adaptieve security applicatie (ASA) die softwareversie 8.0 en hoger uitvoert.
- Cisco Adaptieve Security Devices Manager (ASDM) softwareversie 6.0 en hoger.

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.

## Verwante producten

De informatie in dit document is ook van toepassing op de Cisco 500 Series PIX-firewall die softwareversie 8.0 en hoger uitvoert.

## Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

# Achtergrondinformatie

RIP is een ver-vectorprotocol dat hoptelling als metriek voor weg selectie gebruikt. Wanneer RIP op een interface wordt geactiveerd, zendt de interface uit RIP uitzendingen met aangrenzende apparaten om dynamisch over routes te leren en te adverteren.

De steun van het veiligheidsapparaat zowel RIP versie 1 als RIP versie 2. RIP versie 1 stuurt het Subnet masker met de routingupdate niet. RIP versie 2 VERSTUURT het SUBNET masker met het routingupdate en steunt veranderlijk-lengtesubnet maskers. Daarnaast ondersteunt RIP versie 2 buren authenticatie wanneer routing updates wordt uitgewisseld. Deze verificatie garandeert dat het beveiligingsapparaat betrouwbare routinginformatie van een vertrouwde bron ontvangt.

**Beperkingen:**

1. Het security apparaat kan geen RIP-updates tussen interfaces doorgeven.
2. RIP versie 1 steunt Subnetmaskers van variabele lengte (VLSM) niet.
3. RIP heeft een maximum aantal van 15 hopcellen. Een route met een hoptelling van meer dan 15 wordt als onbereikbaar beschouwd.
4. De convergentie van RIP is relatief langzaam in vergelijking met andere routeringsprotocollen.
5. U kunt slechts één RIP-proces op het veiligheidsapparaat inschakelen.

**Opmerking:** deze informatie is alleen van toepassing op RIP versie 2:

1. Als u de buurauthenticatie gebruikt, moeten de authenticatiesleutel en de sleutel ID op alle buurapparaten hetzelfde zijn die RIP versie 2 updates aan de interface leveren.
2. Met RIP versie 2, zendt het veiligheidsapparaat en ontvangt standaardrouteupdates met het gebruik van het multicast adres 224.0.0.9. In passieve modus ontvangt het routeupdates op dat adres.
3. Wanneer RIP versie 2 op een interface wordt gevormd, wordt het multicast adres 224.0.0.9 op die interface geregistreerd. Wanneer een configuratie van RIP versie 2 uit een interface wordt verwijderd, is dat multicast adres niet geregistreerd.

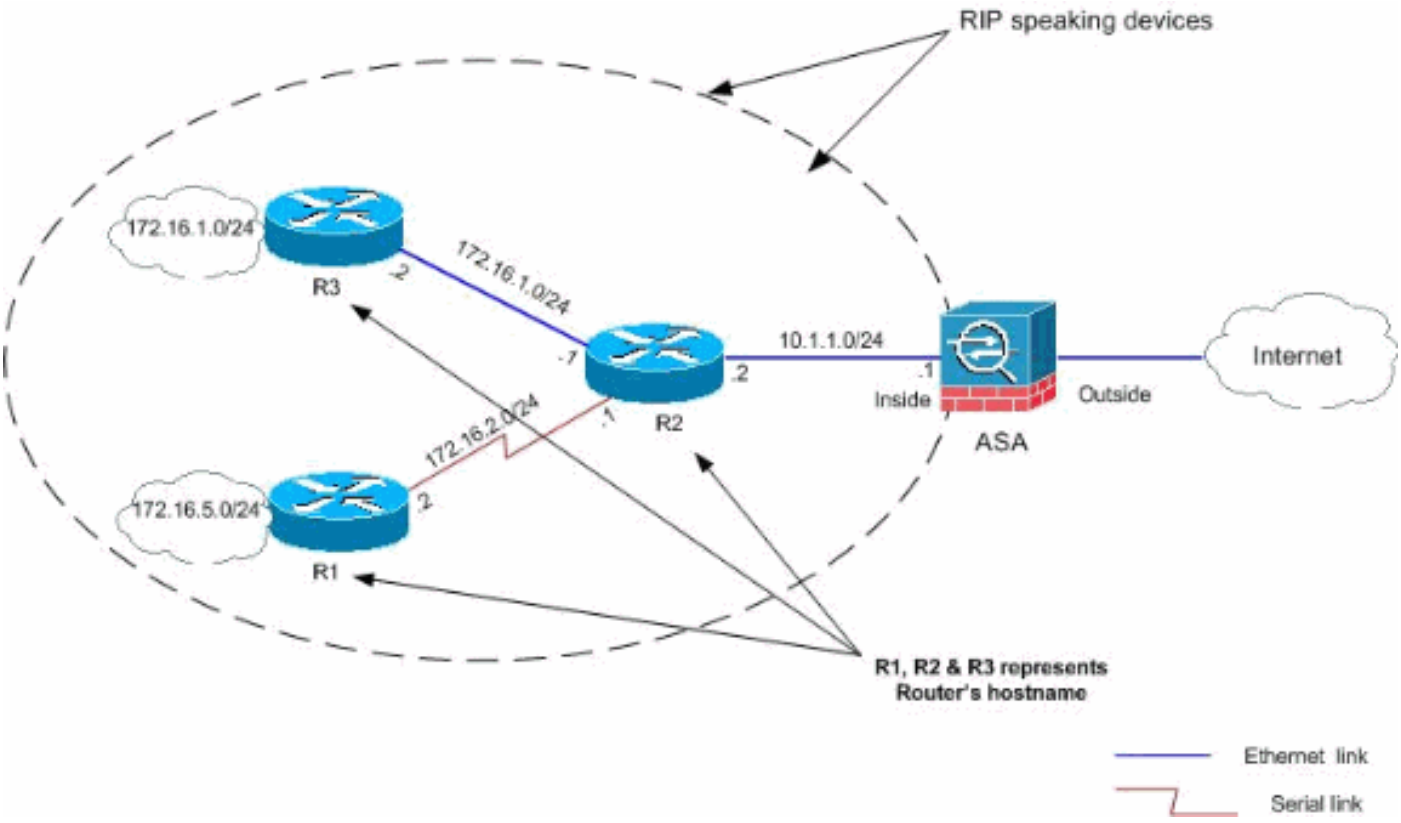
# Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

**Opmerking:** Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

## Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:




## Configuraties

Dit document gebruikt deze configuraties:

- ASDM-configuratie
- RIP-verificatie configureren
- Cisco ASA CLI-configuratie

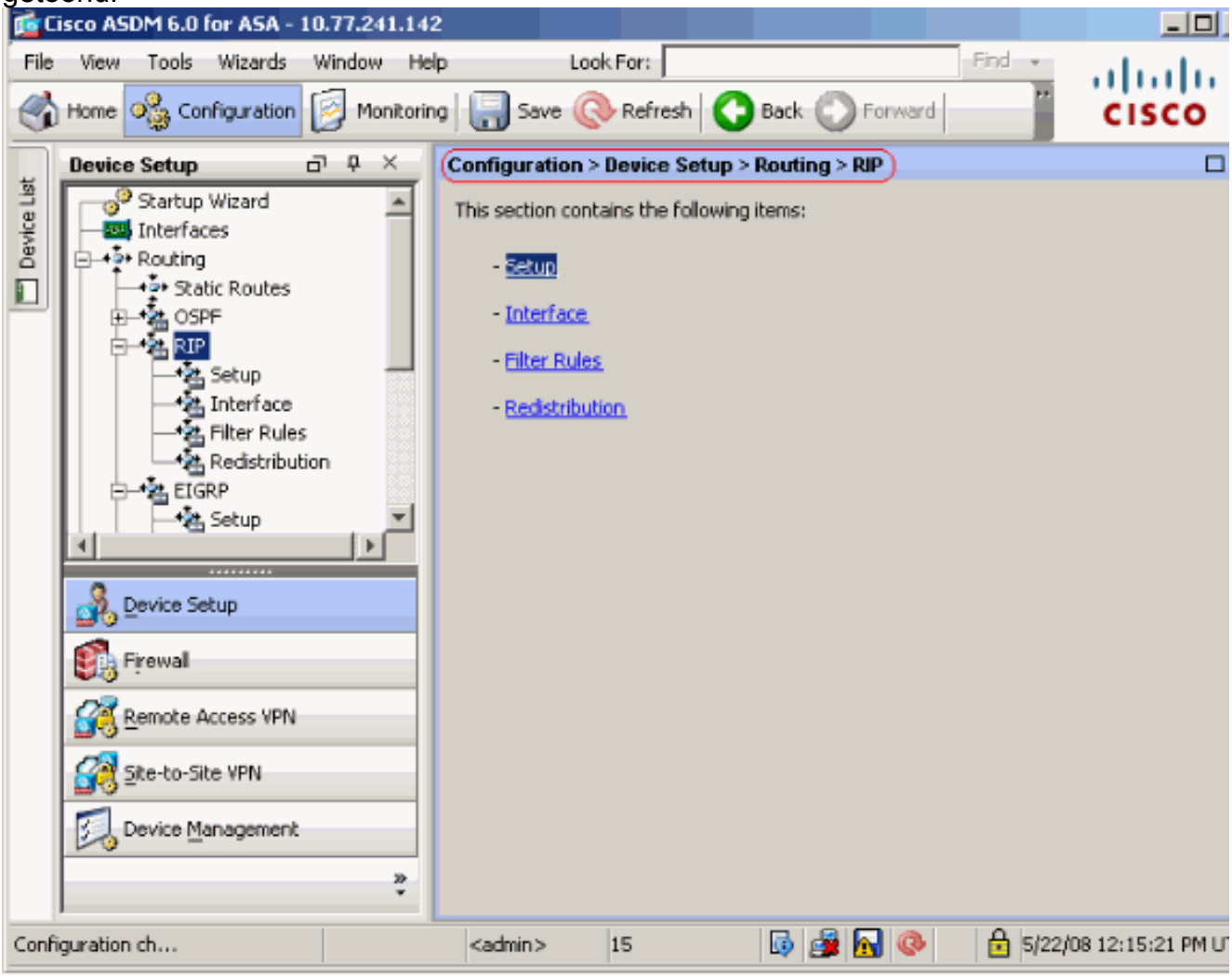
- Cisco IOS-configuratie (R2) CLI-router
- Configuratie van Cisco IOS-router (R1) CLI
- Cisco IOS-routerconfiguratie (R3) CLI

## ASDM-configuratie

Adaptieve Security Devices Manager (ASDM) is een op browser gebaseerde toepassing die wordt gebruikt om de software op security apparaten te configureren en te controleren. ASDM wordt geladen vanaf het security apparaat en gebruikt om het apparaat te configureren, te controleren en te beheren. U kunt de ASDM Launcher (alleen Windows®) ook gebruiken om de ASDM-toepassing sneller te starten dan de Java-applicatie. In dit gedeelte wordt de informatie beschreven die u nodig hebt om de functies te configureren die in dit document worden beschreven met ASDM.

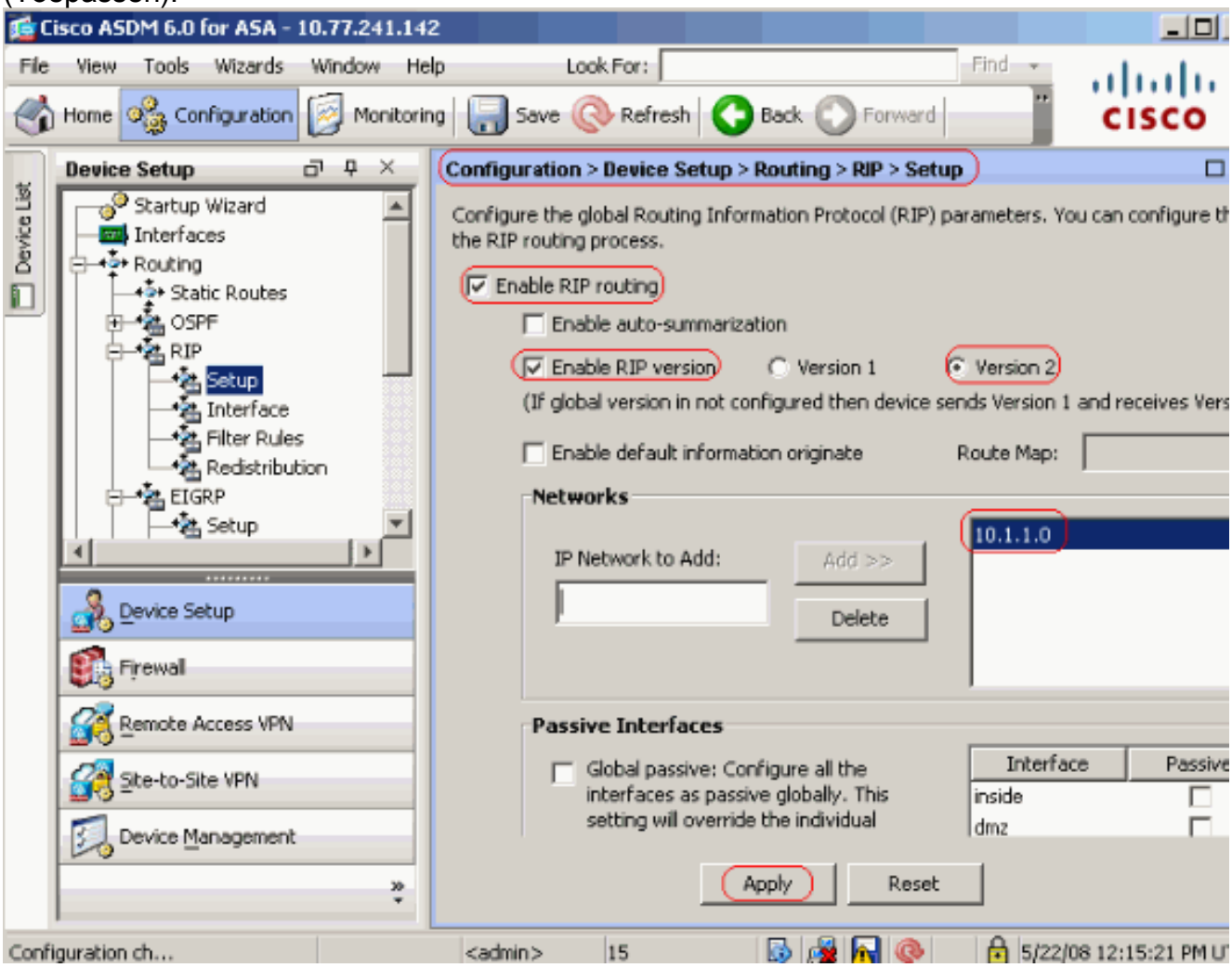
Voltooi deze stappen om RIP in de Cisco ASA te configureren:

1. Meld u aan bij Cisco ASA met ASDM.
2. Kies **Configuratie > de Instellen van het apparaat > het Rijen > RIP** in de ASDM interface, zoals in het schermschot wordt getoond.




3. Kies **Configuratie > de Instellen van het apparaat > het Routing > RIP > Instellen** om de routing van RIP zoals weergegeven **in** te schakelen.Kies het aanvinkvakje **Toegang tot RIP-routing**.Kies het aanvinkvakje **RIP** met radioknop **versie 2 inschakelen**.Voeg onder **het** tabblad **Networks** het netwerk **10.1.1.0 toe**.Klik op **Apply**

(Toepassen).




**Velden**Laat RIP routing-Controleer dit aankruisvakje in om RIP routing op het security apparaat toe te laten. Wanneer u RIP toelaat, wordt het op alle interfaces geactiveerd. Als u dit aankruisvakje controleert, stelt u ook de andere velden in dit venster in. Schakel dit vakje uit om RIP-routing op het security apparaat uit te schakelen.Schakel deze optie in en schakel deze optie uit om automatische routesamenvatting uit te schakelen. Controleer dit aanvinkvakje om automatische routinematige samenvatting opnieuw in te schakelen. RIP versie 1 gebruikt altijd automatische samenvatting. U kunt automatische samenvatting niet uitschakelen voor RIP versie 1. Als u RIP versie 2 gebruikt, kunt u automatische samenvatting uitschakelen als u dit aankruisvakje verwijdert. Schakel automatische samenvatting uit als u routing tussen losstaande subnetten moet uitvoeren. Wanneer automatische samenvatting wordt uitgeschakeld, worden subnetten geadverteerd.Toegang tot RIP versie - Controleer dit aanvinkvakje om de versie van RIP te specificeren die door het veiligheidsapparaat wordt gebruikt. Als dit aankruisvakje wordt gewist, verstuurt het beveiligingsapparaat RIP versie 1 updates en accepteert u RIP versie 1 en versie 2 updates. Deze instelling kan per interface in het interfacevenster worden overschreven.Versie 1-Specificeert dat het security apparaat alleen updates 1 van RIP stuurt en ontvangt. Alle ontvangen versies 2 worden ingetrokken.Versie 2-Specificeert dat het security apparaat alleen RIP versie 2 updates stuurt en ontvangt. Alle ontvangen updates van versie 1 worden ingetrokken.Laat standaardinformatie van begin tot begin toe deze controledoos om een standaardroute in het eind van RIP te genereren. U kunt een routekaart configureren die u moet voltooien voordat de standaardroute kan worden gegenereerd.Route-map-Voer de naam van de routekaart in om van toepassing te zijn. Het routingproces genereert de

standaardroute als de routekaart is tevreden.IP-netwerk om toe te voegen-definieert een netwerk voor het RIP-routingproces. Het opgegeven netwerknummer moet geen subnetinformatie bevatten. Er is geen limiet aan het aantal netwerken dat u kunt toevoegen aan de configuratie van het security apparaat. RIP die updates routeert wordt verzonden en slechts door interfaces op de gespecificeerde netwerken ontvangen. Als het netwerk van een interface niet wordt gespecificeerd, wordt de interface niet in om het even welke updates van RIP geadverteerd.Add-klik deze knop om het gespecificeerde netwerk aan de lijst met netwerken toe te voegen.Verwijderen: klik op deze knop om het geselecteerde netwerk uit de lijst met netwerken te verwijderenConfigureer interfaces mondiaal als passief — Controleer dit aankruisvakje om alle interfaces op het beveiligingsapparaat in te stellen op passieve RIP-modus. Het beveiligingstoestel luistert naar RIP routinguitzendingen op alle interfaces en gebruikt die informatie om de routingtabellen te bevolken maar zendt geen routingupdates uit. Gebruik de tabel Passive Interfaces om specifieke interfaces in te stellen voor passieve RIP.Passive interfaces tabel—Toont de geconfigureerde interfaces op het beveiligingsapparaat. Controleer het aankruisvakje in de passieve kolom voor de interfaces die u in passieve modus wilt uitvoeren. De andere interfaces zenden en ontvangen nog steeds RIP-uitzendingen.

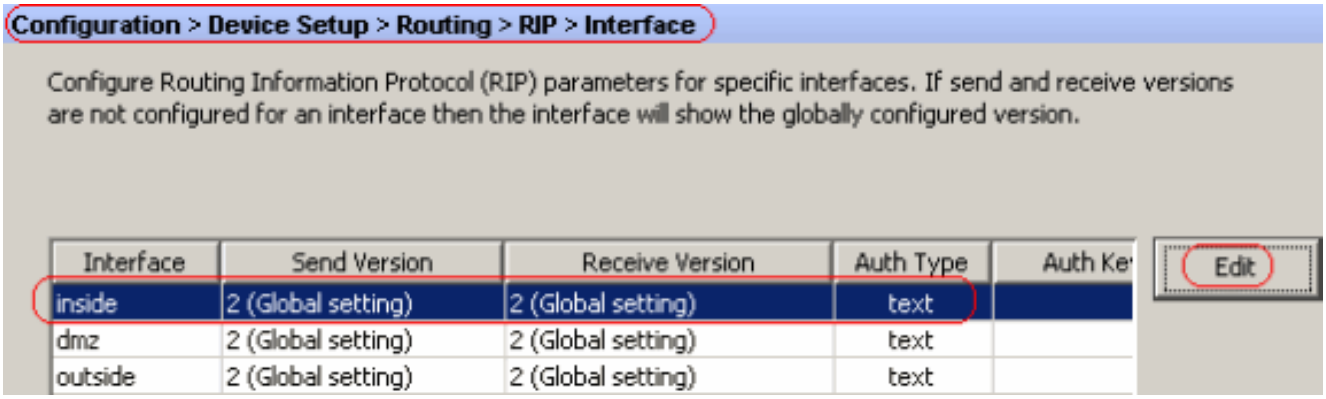
## RIP-verificatie configureren

Cisco ASA ondersteunt MD5 verificatie van routing updates van het RIP v2-routingprotocol. De MD5 keyed digest in elk RIP-pakket voorkomt de introductie van onbevoegde of valse routingberichten uit niet-goedgekeurde bronnen. De toevoeging van authenticatie aan uw berichten van RIP waarborgt dat uw routers en Cisco ASA slechts routingberichten van andere routingapparaten accepteren die met de zelfde pre-gedeelde sleutel worden gevormd. Zonder deze authenticatie ingesteld, als u een ander routeapparaat met andere of tegenovergestelde routeinformatie op het netwerk introduceert, kunnen de routingtabellen op uw routers of Cisco ASA corrupt worden, en kan een ontkenning van de dienstaanval optreden. Wanneer u authenticatie aan de RIP berichten toevoegt die tussen uw routingapparaten, die de ASA omvatten, het voorkomt de doelgerichte of toevallige toevoeging van een andere router aan het netwerk en om het even welk probleem.

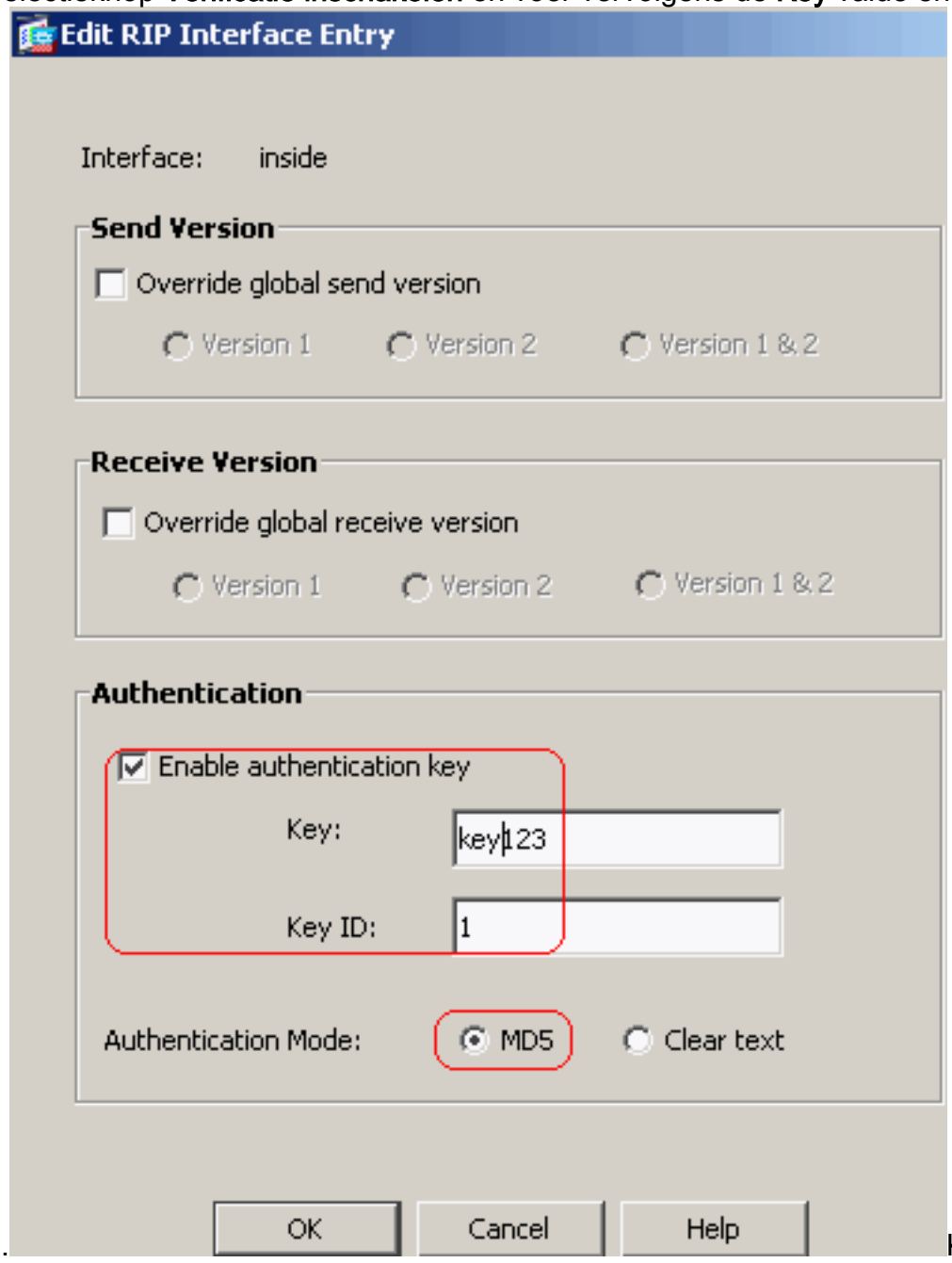
RIP routeverificatie wordt ingesteld per interface. Alle RIP buren op interfaces die voor de authenticatie van het bericht van het RIP worden gevormd moeten met de zelfde authentificatiemodus en de sleutel worden gevormd.

Voltooi deze stappen om RIP MD5 verificatie op de Cisco ASA mogelijk te maken.

1. Kies op ASDM **Configuration > Devices Setup > Routing > RIP > Interface** en kies de interne interface met muis. Klik op **Edit**
(Bewerken).




2. Kies het selectieknop **Verificatie inschakelen** en voer vervolgens de **Key** value en **Key ID** waarde in.




Klik op **OK** en vervolgens **op Toepassen**.

## Cisco ASA CLI-configuratie

| Cisco ASA |
| --- |
| |

```
ciscoasa#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!

!--- Inside interface configuration interface
Ethernet0/1 nameif inside security-level 100 ip address
10.1.1.1 255.255.255.0 !--- RIP authentication is
configured on the inside interface. rip authentication
mode md5
 rip authentication key




!

!--- Output Suppressed !--- Outside interface
configuration interface Ethernet0/2 nameif outside
security-level 0 ip address 192.168.1.2 255.255.255.0 !-
-- RIP Configuration router rip
 network 10.0.0.0
 version 2

!--- This is the static default gateway configuration in
!--- order to reach the Internet. route outside 0.0.0.0
0.0.0.0 192.168.1.1 1
```

## Cisco IOS-configuratie (R2) CLI-router

**Cisco IOS-router (R2)**

```
interface Ethernet0
 ip address 10.1.1.2 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain 1

!
router rip
 version 2
 network 10.0.0.0
 network 172.16.0.0
 no auto-summary
```

## Configuratie van Cisco IOS-router (R1) CLI

**Cisco IOS-router (R1)**

```
router rip
 version 2
 network 172.16.0.0
 no auto-summary
```

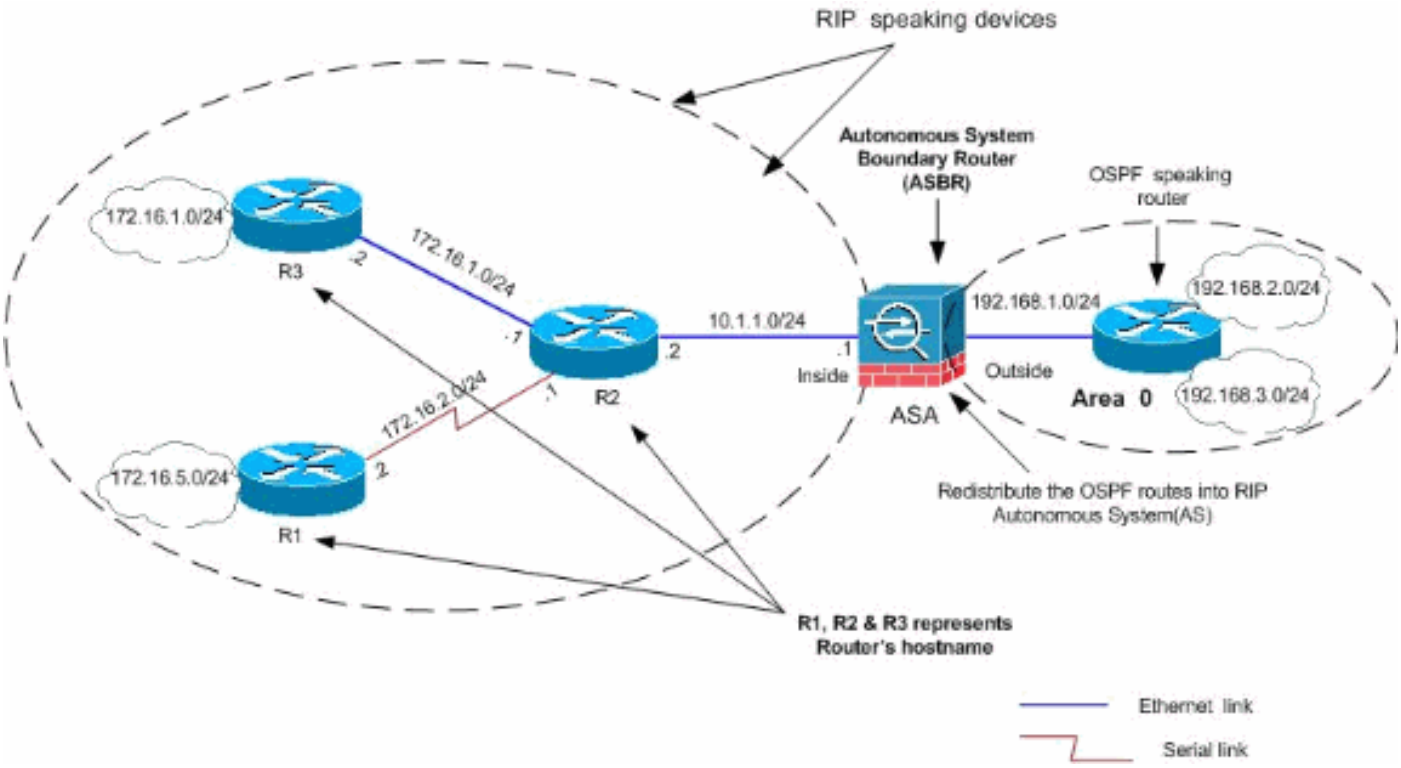
## Cisco IOS-routerconfiguratie (R3) CLI

| Cisco IOS-router (R3) |
| --- |
| router rip<br>version 2<br>network 172.16.0.0<br>no auto-summary |

## Verdeel dit opnieuw in RIP met ASA

U kunt routes van de OSPF, de EHBO, de statische, en verbonden routingprocessen in het het routingproces van RIP opnieuw verdelen.

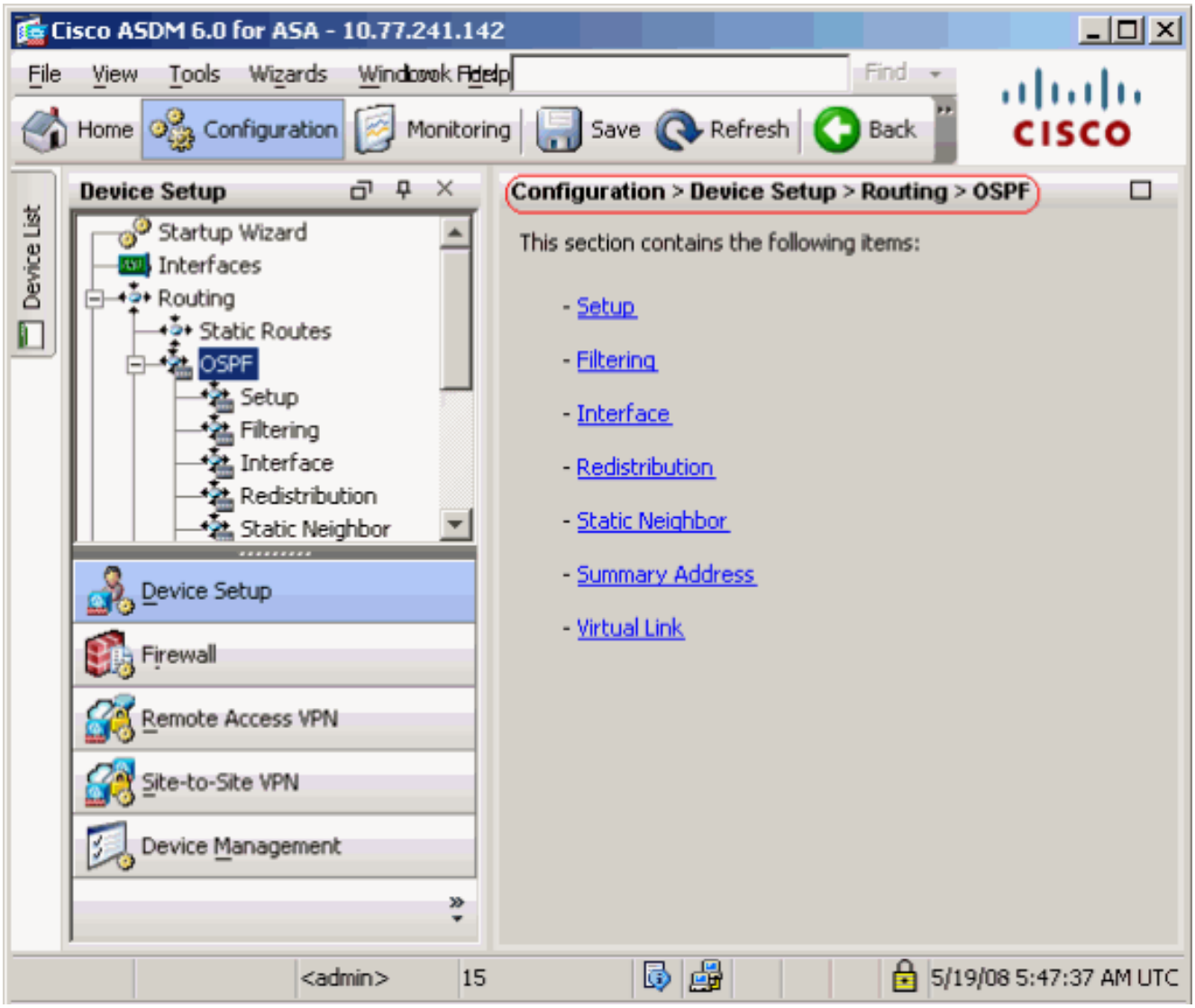
In dit voorbeeld, wordt de herverdeling van de OSPF-routes in RIP met het netwerkdiagram getoond:



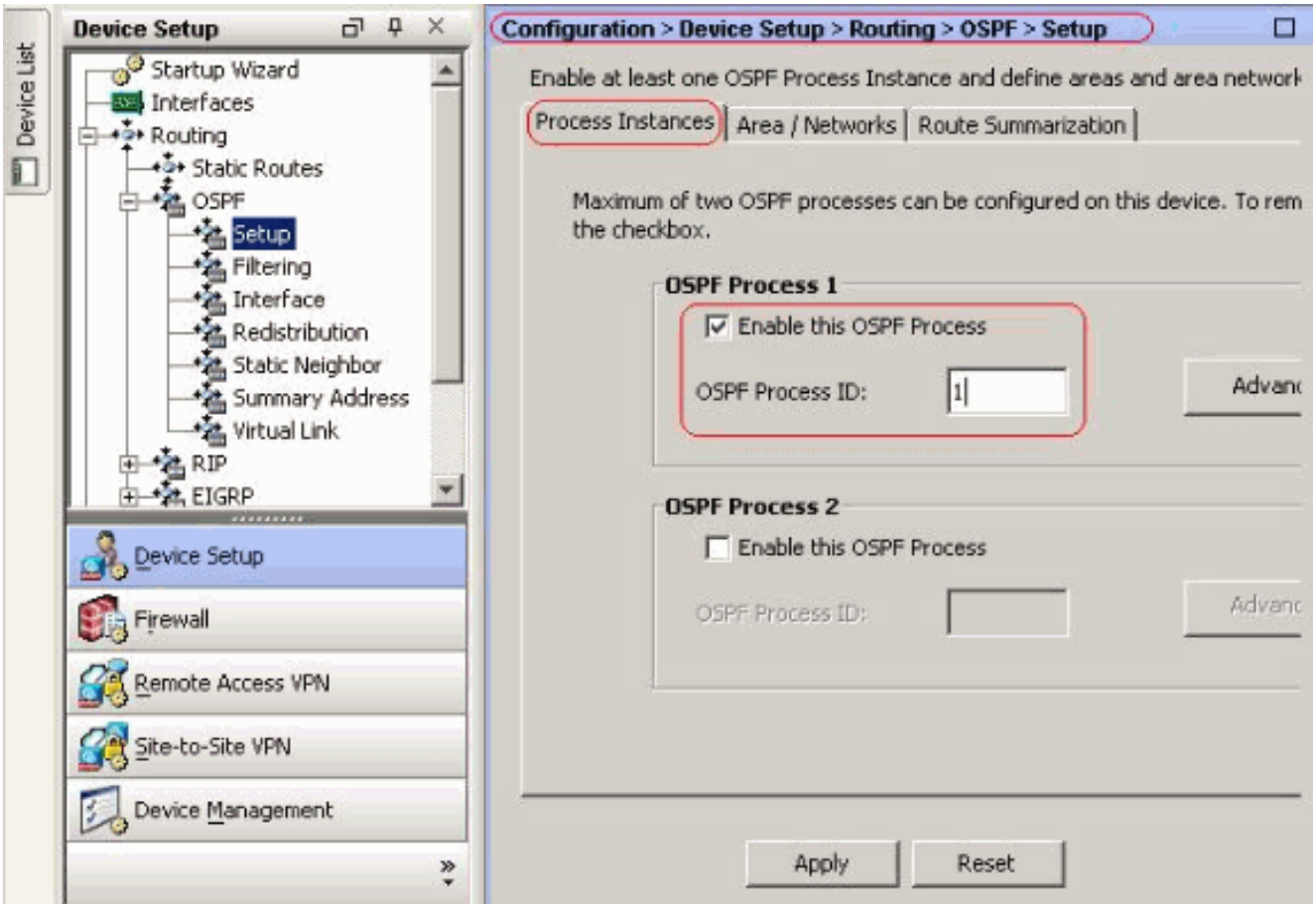

## ASDM-configuratie

Voer de volgende stappen uit:

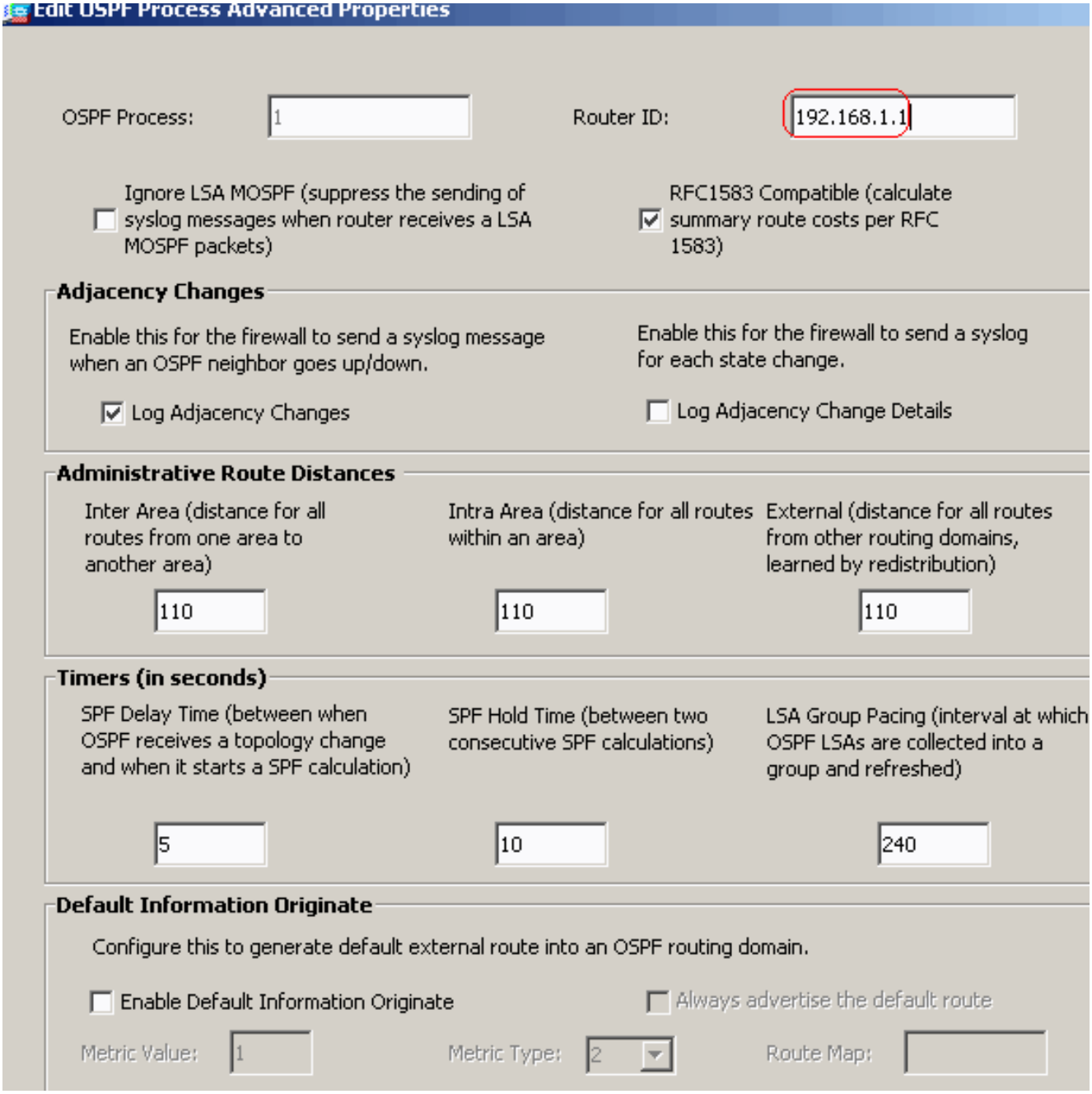
1. **OSPF-configuratie**Kies **Configuratie > de Instellen van het apparaat > Routing > OSPF** in de ASDM-interface, zoals in de screenshot wordt getoond.



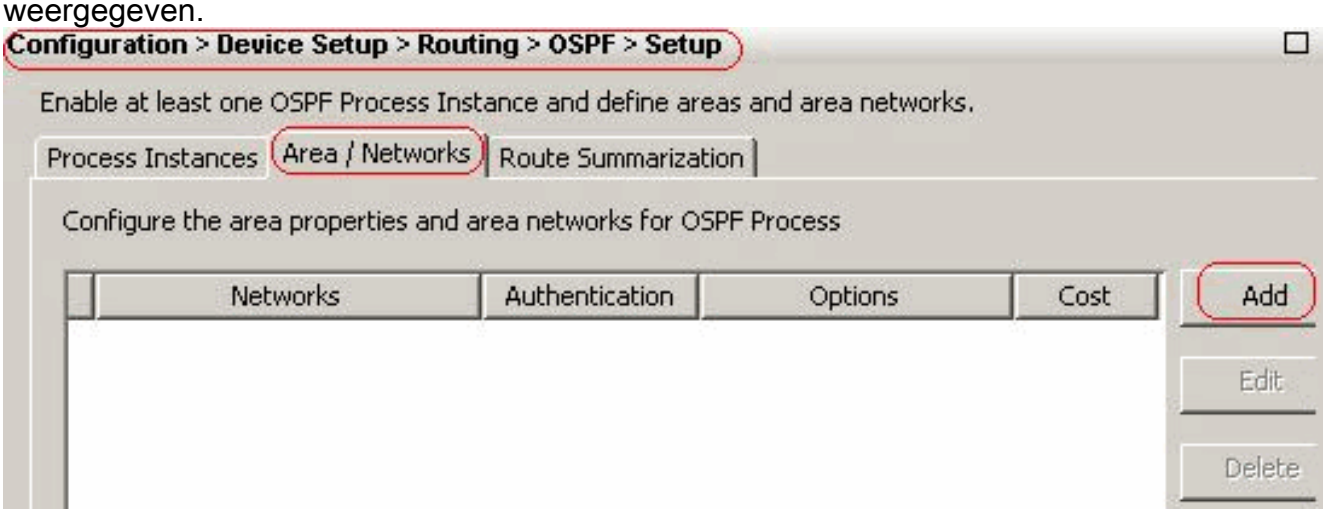

Schakel het OSPF-routingproces in op het tabblad **Setup > Procesorganen**, zoals in het screenshot. In dit voorbeeld, is het OSPF ID-proces
**1**.




Klik op **Geavanceerd** in het **tabblad Instellen >** tabblad **Procesorganen** om optionele geavanceerde OSPF-routingparameters te configureren. U kunt processpecifieke instellingen bewerken, zoals de instellingen van de router-ID, de veranderingen in de nabijheid, de administratieve routeafstanden, de timers en de standaardinstellingen van de Informatie.

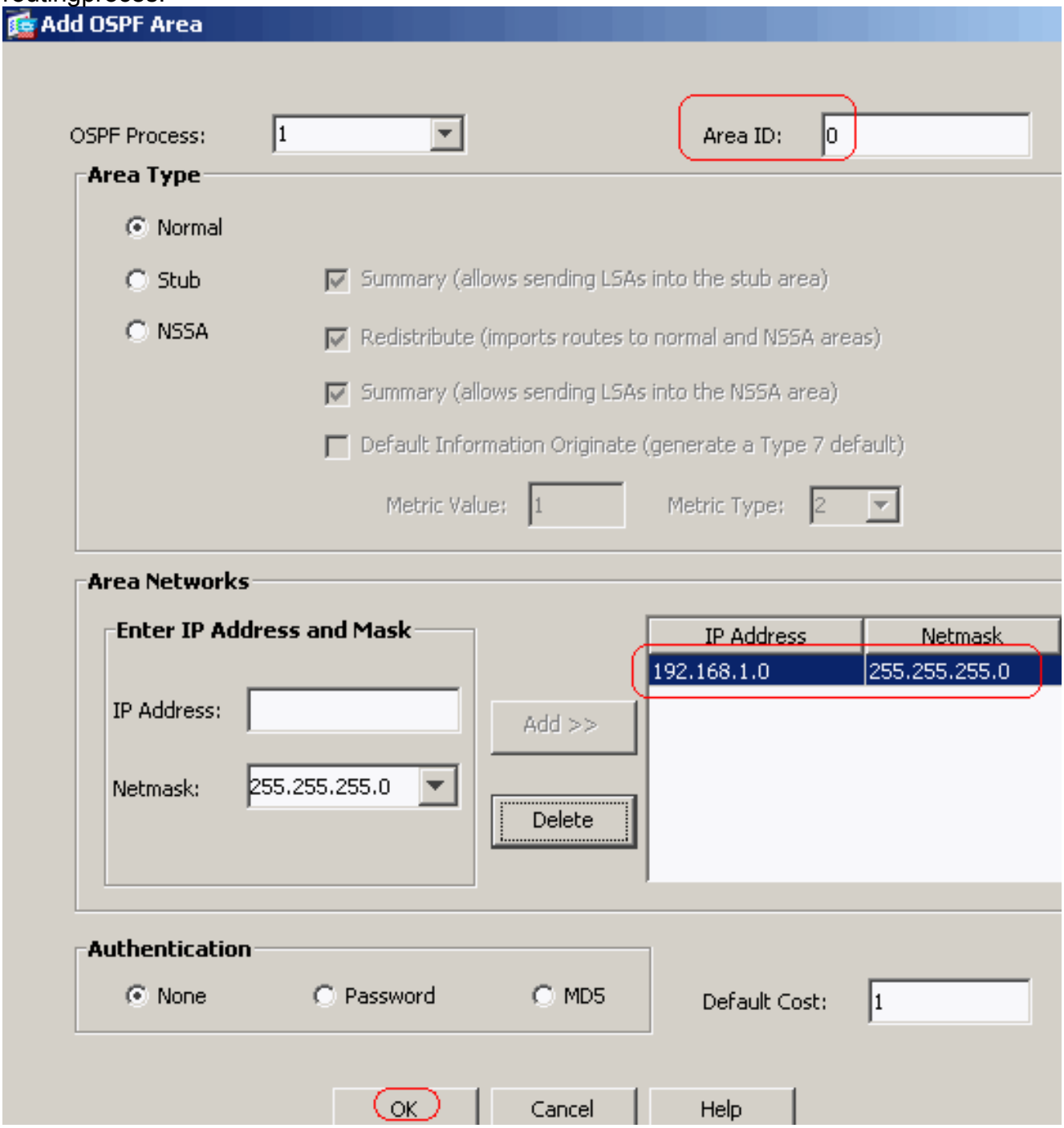



Klik op **OK**.Nadat u de vorige stappen hebt voltooid, definieert u de netwerken en interfaces die deelnemen aan OSPF-routing in het tabblad **Setup > Gebied/netwerken**. Klik op **Toevoegen** zoals in deze screenshot wordt weergegeven.

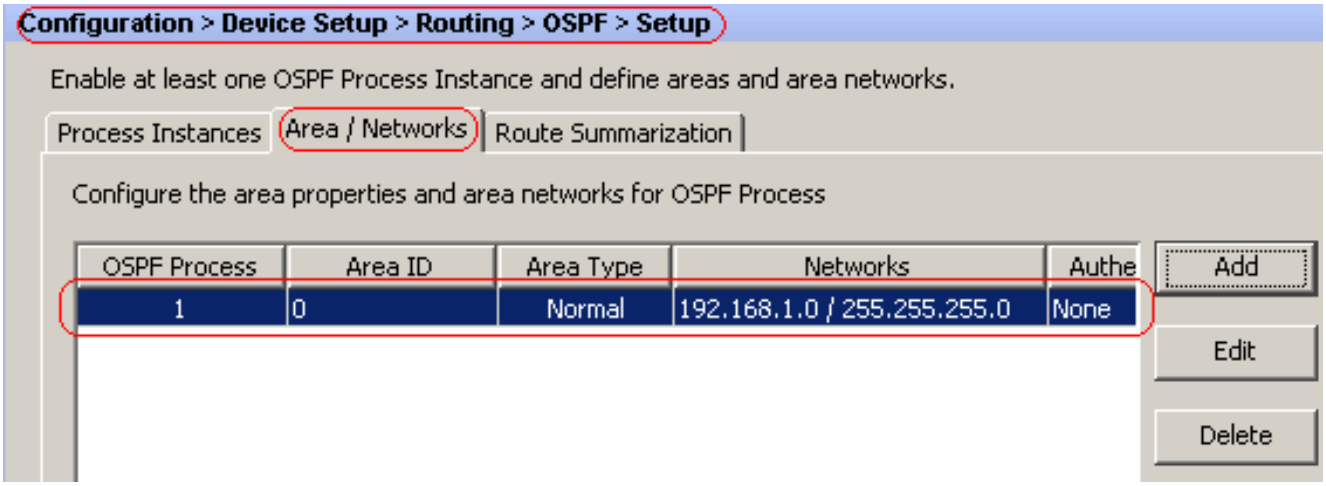



Dit scherm verschijnt. In dit voorbeeld, is het enige netwerk dat wij toevoegen het

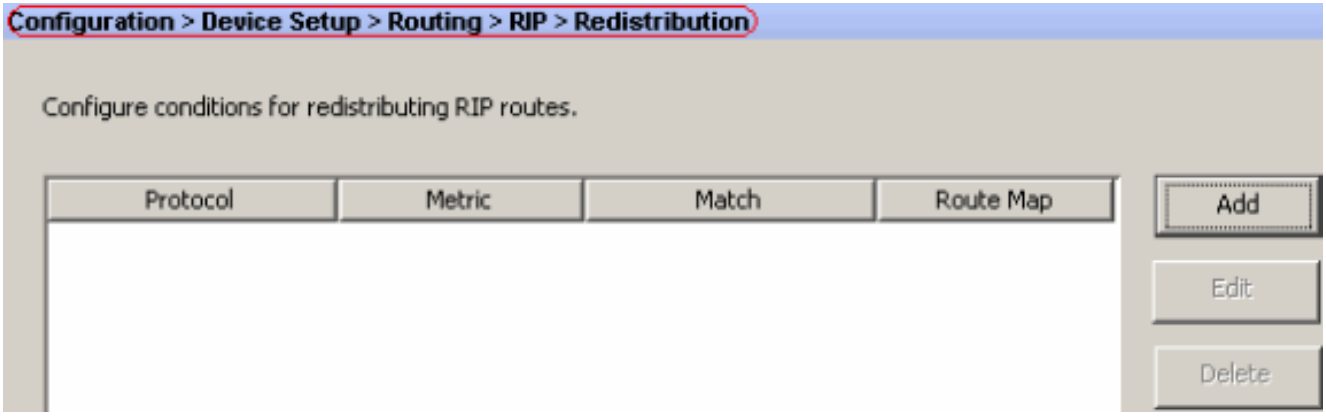
buitennetwerk (192.168.1.0/24) aangezien OSPF slechts op de buiteninterface wordt toegelaten.**Opmerking:** Alleen interfaces met een IP-adres die binnen de gedefinieerde netwerken vallen, nemen deel aan het OSPF-routingproces.




Klik op **OK**.Klik op **Apply** (Toepassen).

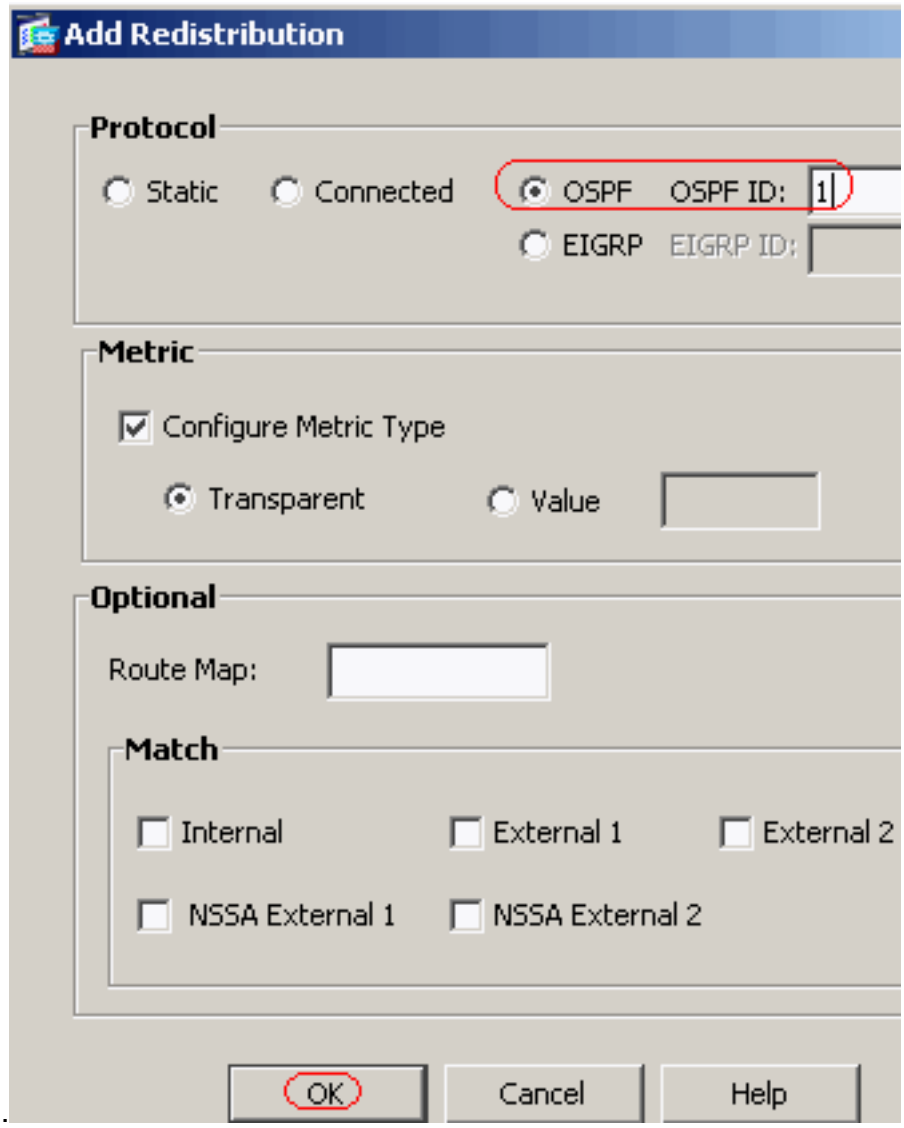



2. Kies **Configuratie > de Instellen van het apparaat > het Verspreiden > RIP > Herdistributie > Toevoegen** om OSPF routes in RIP te herverdelen.




3. Klik op **OK** en vervolgens **op**

Toepassen.




## Compatibele CLI-configuratie

| CLI-configuratie van ASA voor opnieuw distribueren van OSPF in RIP AS |
| --- |
| router rip<br> network 10.0.0.0<br> **redistribute ospf 1 metric transparent**<br> version 2<br>!<br>router ospf 1<br> router-id 192.168.1.1<br> network 192.168.1.0 255.255.255.0 area 0<br> area 0<br> log-adj-changes |

U kunt de routingtabel van de aangrenzende Cisco IOS router (R2) zien na het opnieuw verdelen van OSPF-routes in RIP AS.

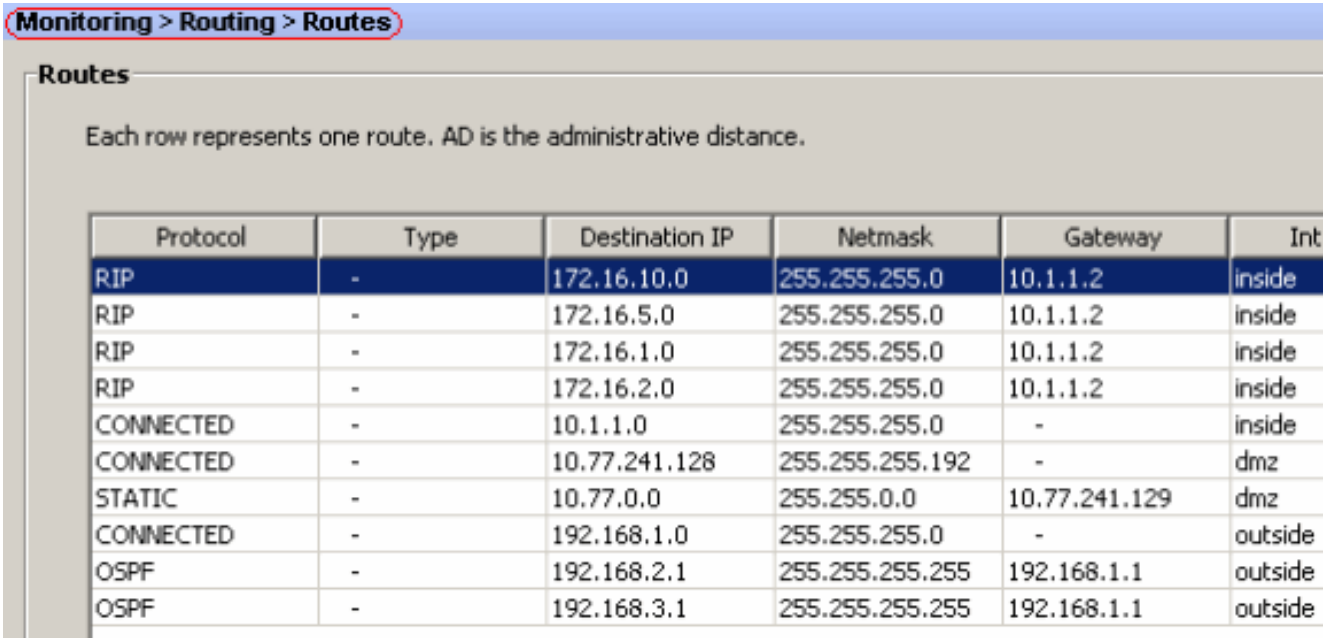
```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 4 subnets
R       172.16.10.0 [120/1] via 172.16.1.2, 00:00:25, Ethernet1
R       172.16.5.0 [120/1] via 172.16.2.2, 00:00:20, Serial1
C       172.16.1.0 is directly connected, Ethernet1
C       172.16.2.0 is directly connected, Serial1
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Ethernet0
R       10.77.241.128/26 [120/1] via 10.1.1.1, 00:00:06, Ethernet0
R    192.168.1.0/24 [120/1] via 10.1.1.1, 00:00:05, Ethernet0
     192.168.2.0/32 is subnetted, 1 subnets
R       192.168.2.1 [120/12] via 10.1.1.1, 00:00:05, Ethernet0
     192.168.3.0/32 is subnetted, 1 subnets
R       192.168.3.1 [120/12] via 10.1.1.1, 00:00:05, Ethernet0
!--- Redistributed route advertised by Cisco ASA
```

# Verifiëren

Volg deze stappen om de configuratie van uw computer te controleren:

1. U kunt de routingtabel controleren als u navigeert aan **Monitoring > Routing > Routes**. In dit screenshot kunt u zien dat de netwerken 172.16.1.0/24, 172.16.2.0/24, 172.16.5.0/24 en 172.16.10.0/24 worden geleerd via R2 (10.1.1.2) met RIP.




| Protocol | Type | Destination IP | Netmask | Gateway | Int |
|---|---|---|---|---|---|
| RIP | - | 172.16.10.0 | 255.255.255.0 | 10.1.1.2 | inside |
| RIP | - | 172.16.5.0 | 255.255.255.0 | 10.1.1.2 | inside |
| RIP | - | 172.16.1.0 | 255.255.255.0 | 10.1.1.2 | inside |
| RIP | - | 172.16.2.0 | 255.255.255.0 | 10.1.1.2 | inside |
| CONNECTED | - | 10.1.1.0 | 255.255.255.0 | - | inside |
| CONNECTED | - | 10.77.241.128 | 255.255.255.192 | - | dmz |
| STATIC | - | 10.77.0.0 | 255.255.0.0 | 10.77.241.129 | dmz |
| CONNECTED | - | 192.168.1.0 | 255.255.255.0 | - | outside |
| OSPF | - | 192.168.2.1 | 255.255.255.255 | 192.168.1.1 | outside |
| OSPF | - | 192.168.3.1 | 255.255.255.255 | 192.168.1.1 | outside |

2. Vanaf de CLI kunt u de opdracht **Show route** gebruiken om dezelfde output te krijgen.

```
ciscoasa#show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is not set

R    172.16.10.0 255.255.255.0 [120/2] via 10.1.1.2, 0:00:10, inside
R    172.16.5.0 255.255.255.0 [120/2] via 10.1.1.2, 0:00:10, inside
R    172.16.1.0 255.255.255.0 [120/1] via 10.1.1.2, 0:00:10, inside
R    172.16.2.0 255.255.255.0 [120/1] via 10.1.1.2, 0:00:10, inside
C    10.1.1.0 255.255.255.0 is directly connected, inside
C    10.77.241.128 255.255.255.192 is directly connected, dmz
S    10.77.0.0 255.255.0.0 [1/0] via 10.77.241.129, dmz
C    192.168.1.0 255.255.255.0 is directly connected, outside
O    192.168.2.1 255.255.255.255 [110/11] via 192.168.1.1, 0:34:46, outside
O    192.168.3.1 255.255.255.255 [110/11] via 192.168.1.1, 0:34:46, outside
ciscoasa#
```

# Problemen oplossen

Deze sectie omvat informatie over debug opdrachten die nuttig kunnen zijn voor het oplossen van OSPF-problemen.

## Opdrachten voor troubleshooting

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

**Opmerking:** Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

- **debug rip gebeurtenissen**—hiermee kan worden gezeten van RIP gebeurtenissen

```
ciscoasa#debug rip events
rip_route_adjust for inside coming up
RIP: sending request on inside to 224.0.0.9
RIP: received v2 update from 10.1.1.2 on inside
     172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops
     172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops
RIP: Update contains 4 routes
RIP: received v2 update from 10.1.1.2 on inside
     172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops
     172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops
RIP: Update contains 4 routes
RIP: sending v2 flash update to 224.0.0.9 via dmz (10.77.241.142)
RIP: build flash update entries
        10.1.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
        172.16.1.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
        172.16.2.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
        172.16.5.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
        172.16.10.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
RIP: Update contains 5 routes
RIP: Update queued
RIP: sending v2 flash update to 224.0.0.9 via inside (10.1.1.1)
RIP: build flash update entries - suppressing null update
RIP: Update sent via dmz rip-len:112
RIP: sending v2 update to 224.0.0.9 via dmz (10.77.241.142)
RIP: build update entries
        10.1.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
        172.16.1.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
```

```
        172.16.2.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
        172.16.5.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
        172.16.10.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
        192.168.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
        192.168.2.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0
        192.168.3.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0
RIP: Update contains 8 routes
RIP: Update queued
RIP: sending v2 update to 224.0.0.9 via inside (10.1.1.1)
RIP: build update entries
        10.77.241.128 255.255.255.192 via 0.0.0.0, metric 1, tag 0
        192.168.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
        192.168.2.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0
        192.168.3.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0
RIP: Update contains 4 routes
RIP: Update queued
RIP: Update sent via dmz rip-len:172
RIP: Update sent via inside rip-len:92
RIP: received v2 update from 10.1.1.2 on inside
     172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops
     172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops
RIP: Update contains 4 routes
```

# Gerelateerde informatie

- Cisco 5500 Series ondersteuningspagina voor adaptieve security applicatie
- Cisco 500 Series PIX-ondersteuningspagina
- PIX/ASA 8.X: Het configureren van HTTP op de Cisco adaptieve security applicatie (ASA)
- Technische ondersteuning en documentatie – Cisco Systems