

ASA configureren voor redundante of back-up ISP-links

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Verwante producten](#)

[Achtergrondinformatie](#)

[Overzicht van statische routekaarten](#)

[Belangrijke aanbevelingen](#)

[Configureren](#)

[Netwerkdigram](#)

[CLI-configuratie](#)

[ASDM-configuratie](#)

[Verifiëren](#)

[Controleer of de configuratie voltooid is](#)

[Bevestig dat de back-uproute is geïnstalleerd \(CLI-methode\)](#)

[Bevestig dat de back-uproute is geïnstalleerd \(ASDM-methode\)](#)

[Problemen oplossen](#)

[Opdrachten debug](#)

[Overtrokken route wordt onnodig verwijderd](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u de Cisco ASA 5500 Series adaptieve security applicatie (ASA) kunt configureren voor het gebruik van de statische route-tracking-functie om het apparaat in staat te stellen redundante of back-up internetverbindingen te gebruiken.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

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

- Cisco ASA 5555-X Series die software versie 9.x of hoger uitvoeren
- Cisco ASDM versie 7.x of 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

U kunt deze configuratie ook gebruiken met Cisco ASA 5500 Series versie 9.1(5).

Opmerking: De opdracht **back-upinterface** is vereist om de vierde interface van de ASA 5505 Series te kunnen configureren. Raadpleeg het [gedeelte](#) van de [back-upinterface](#) van de *Cisco Security Appliance Opdracht Referentie, versie 7.2* voor meer informatie.

Achtergrondinformatie

Deze sectie verschaft een overzicht van de statische route-tracking-functie die in dit document wordt beschreven, evenals een aantal belangrijke aanbevelingen voordat u start.

Overzicht van statische routekaarten

Eén probleem met het gebruik van statische routes is dat er geen inherent mechanisme bestaat dat kan bepalen of de route omhoog of omlaag is. De route blijft in de routingtabel, zelfs als de volgende hopgateway niet beschikbaar wordt. Statische routes worden alleen uit de routingtabel verwijderd als de bijbehorende interface op het security apparaat omlaag gaat. Om dit probleem op te lossen, wordt een statische route-tracking-functie gebruikt om de beschikbaarheid van een statische route op te sporen. De functie verwijdert de statische route uit de routingtabel en vervangt deze door een reserveroute bij een defect.

Statische route tracking stelt de ASA in staat om een goedkope verbinding met een secundaire ISP te gebruiken voor het geval dat de primaire huurlijn niet beschikbaar wordt. Om deze redundantie te bereiken, associeert de ASA een statische route met een controledoel dat u definieert. De SLA-operatie (Service Level Agreement) bewaakt het doel met periodieke ICMP-echo-verzoeken. Als een echo-antwoord niet wordt ontvangen, dan wordt het object neerwaarts overwogen en wordt de bijbehorende route uit de routingtabel verwijderd. Een eerder gevormde back-uproute wordt gebruikt in plaats van de route die wordt verwijderd. Terwijl de back-uproute in gebruik is, blijft de SLA-monitor-handeling de pogingen voortzetten om het doel van de controle te bereiken. Zodra het doel opnieuw beschikbaar is, wordt de eerste route vervangen in de routingtabel, en wordt de reserveroute verwijderd.

In het voorbeeld dat in dit document wordt gebruikt, onderhoudt de ASA twee verbindingen met

het internet. De eerste verbinding is een snelle huurlijn die door een router wordt benaderd die door de primaire ISP wordt verstrekt. De tweede verbinding is een lagere snelheid DSL (Digital Subscriber Line) die door een DSL-modem wordt benaderd die door de secundaire ISP wordt geleverd.

Opmerking: De configuratie die in dit document wordt beschreven, kan niet worden gebruikt voor het taakverdeling of het delen van de lading, aangezien deze niet op de ASA wordt ondersteund. Gebruik deze configuratie alleen voor redundantie of back-up doeleinden. Het uitgaande verkeer gebruikt de primaire ISP, en vervolgens de secundaire ISP als de primaire fout optreedt. Het falen van de primaire ISP veroorzaakt een tijdelijke verstoring van het verkeer.

De DSL-verbinding is leeg zolang de huurlijn actief is en de primaire ISP poort bereikbaar is. Als de verbinding met de primaire ISP echter afneemt, verandert de ASA de routingtabel om het verkeer naar de DSL-verbinding te sturen. Statische route tracking wordt gebruikt om deze redundantie te bereiken.

ASA wordt ingesteld met een statische route die het gehele internetverkeer naar de primaire ISP leidt. Om de tien seconden, controleert het SLA controleproces om te bevestigen dat de primaire ISP poort bereikbaar is. Als het SLA controleproces bepaalt dat de primaire ISP gateway niet bereikbaar is, wordt de statische route die verkeer naar die interface leidt verwijderd van de routingtabel. Om die statische route te vervangen, is een alternatieve statische route die verkeer naar de secundaire ISP leidt geïnstalleerd. Deze alternatieve statische route richt verkeer naar de secundaire ISP door de DSL modem tot de verbinding met de primaire ISP bereikbaar is.

Deze configuratie biedt een relatief goedkope manier om ervoor te zorgen dat de toegang tot het uitgaande internet beschikbaar blijft voor gebruikers achter de ASA. Zoals in dit document beschreven, zou deze opstelling niet geschikt kunnen zijn voor inkomende toegang tot middelen achter de ASA. Geavanceerde netwerkvaardigheden zijn vereist om naadloze inkomende verbindingen te bereiken. Deze vaardigheden komen niet in dit document aan bod.

Belangrijke aanbevelingen

Voordat u de configuratie probeert die in dit document wordt beschreven, moet u een bewakingsdoelmap kiezen die kan reageren op oproepen van de echo-weerslag van het Internet Control Message Protocol (ICMP). Het doel kan een netwerkobject zijn dat u kiest, maar een doel dat nauw verbonden is met de verbinding van uw Internet Service Provider (ISP) wordt aanbevolen. Hier zijn een paar mogelijke monitoringdoelstellingen:

- Het ISP-poortadres
- Een ander ISP-beheerd adres
- Een server op een ander netwerk, zoals een AAA-server (Verificatie, autorisatie en accounting) waarmee de ASA moet communiceren
- Een aanhoudend netwerkobject op een ander netwerk (een desktop of notebook-computer die je 's nachts kunt afsluiten, is geen goede keuze.)

Dit document gaat ervan uit dat de ASA volledig operationeel en geconfigureerd is om Cisco

Adaptieve Security Apparaat Manager (ASDM) in staat te stellen configuratiewijzigingen door te voeren.

Tip: Voor informatie over hoe u ASDM kunt toestaan om het apparaat te configureren raadpleegt u het [instellen](#) van [HTTPS Access voor ASDM](#) gedeelte van *CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.1*.

Configureren

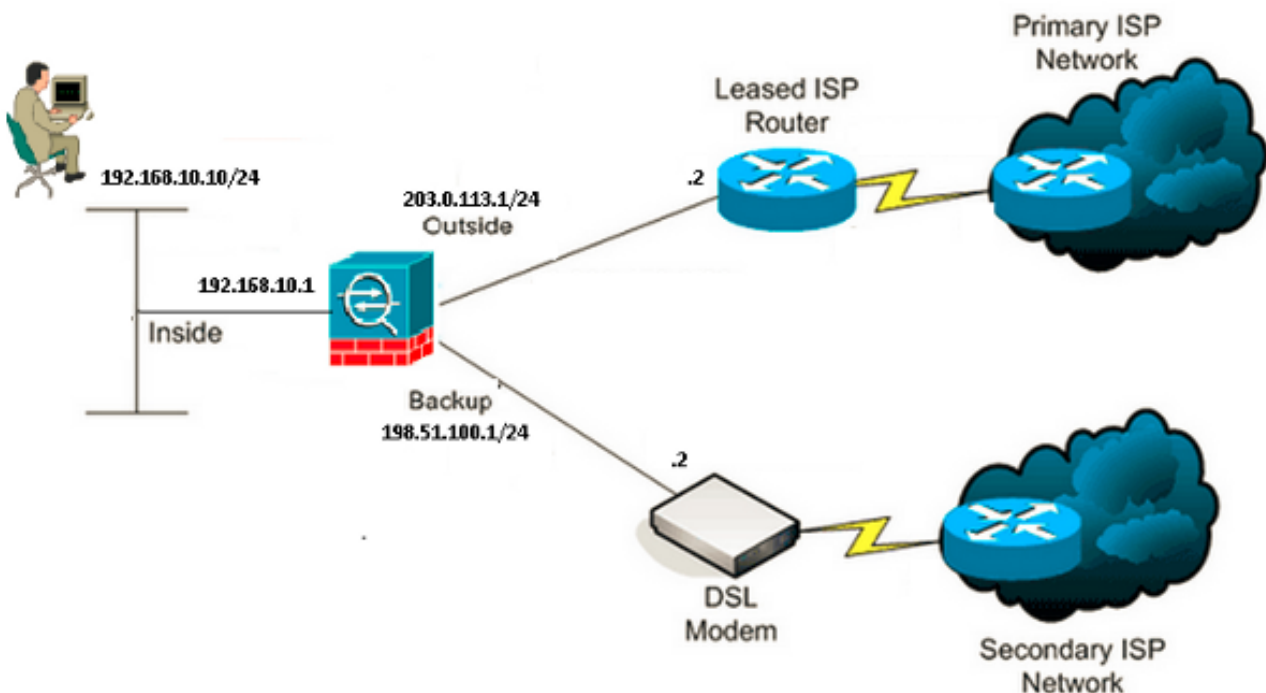
Gebruik de informatie die in deze sectie wordt beschreven om de ASA te configureren voor het gebruik van de statische route-tracking-functie.

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

Opmerking: De IP-adressen die in deze configuratie worden gebruikt zijn niet wettelijk routeerbaar op het internet. Ze zijn [RFC 1918](#) adressen, die in een labomgeving gebruikt worden.

Netwerkdigram

Het voorbeeld in deze sectie gebruikt deze netwerkinstellingen:



CLI-configuratie

Gebruik deze informatie om de ASA via de [CLI](#) te configureren:

ASA# **show running-config**

```
ASA Version 9.1(5)
!
hostname ASA
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 203.0.113.1 255.255.255.0
!
interface GigabitEthernet0/2
 nameif backup
 security-level 0
 ip address 198.51.100.1 255.255.255.0

!--- The interface attached to the Secondary ISP.
!--- "backup" was chosen here, but any name can be assigned.

!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 no nameif
 no security-level
 no ip address
!
boot system disk0:/asa915-smp-k8.bin
ftp mode passive
clock timezone IND 5 30
object network Inside_Network
 subnet 192.168.10.0 255.255.255.0
object network inside_network
 subnet 192.168.10.0 255.255.255.0
pager lines 24
logging enable
mtu inside 1500
mtu outside 1500
mtu backup 1500
icmp unreachable rate-limit 1 burst-size 1
```

```

no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
object network Inside_Network
  nat (inside,outside) dynamic interface
object network inside_network
  nat (inside,backup) dynamic interface

!--- NAT Configuration for Outside and Backup

route outside 0.0.0.0 0.0.0.0 203.0.113.2 1 track 1

!--- Enter this command in order to track a static route.
!--- This is the static route to be installed in the routing
!--- table while the tracked object is reachable. The value after
!--- the keyword "track" is a tracking ID you specify.

route backup 0.0.0.0 0.0.0.0 198.51.100.2 254

!--- Define the backup route to use when the tracked object is unavailable.
!--- The administrative distance of the backup route must be greater than
!--- the administrative distance of the tracked route.
!--- If the primary gateway is unreachable, that route is removed
!--- and the backup route is installed in the routing table
!--- instead of the tracked route.

timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00

sla monitor 123
  type echo protocol ipIcmpEcho 4.2.2.2 interface outside
  num-packets 3
  frequency 10

!--- Configure a new monitoring process with the ID 123. Specify the
!--- monitoring protocol and the target network object whose availability the tracking
!--- process monitors. Specify the number of packets to be sent with each poll.
!--- Specify the rate at which the monitor process repeats (in seconds).

sla monitor schedule 123 life forever start-time now

!--- Schedule the monitoring process. In this case the lifetime
!--- of the process is specified to be forever. The process is scheduled to begin
!--- at the time this command is entered. As configured, this command allows the
!--- monitoring configuration specified above to determine how often the testing
!--- occurs. However, you can schedule this monitoring process to begin in the
!--- future and to only occur at specified times.

crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
!
track 1 rtr 123 reachability

!--- Associate a tracked static route with the SLA monitoring process.
!--- The track ID corresponds to the track ID given to the static route to monitor:
!--- route outside 0.0.0.0 0.0.0.0 10.0.0.2 1 track 1
!--- "rtr" = Response Time Reporter entry. 123 is the ID of the SLA process

```

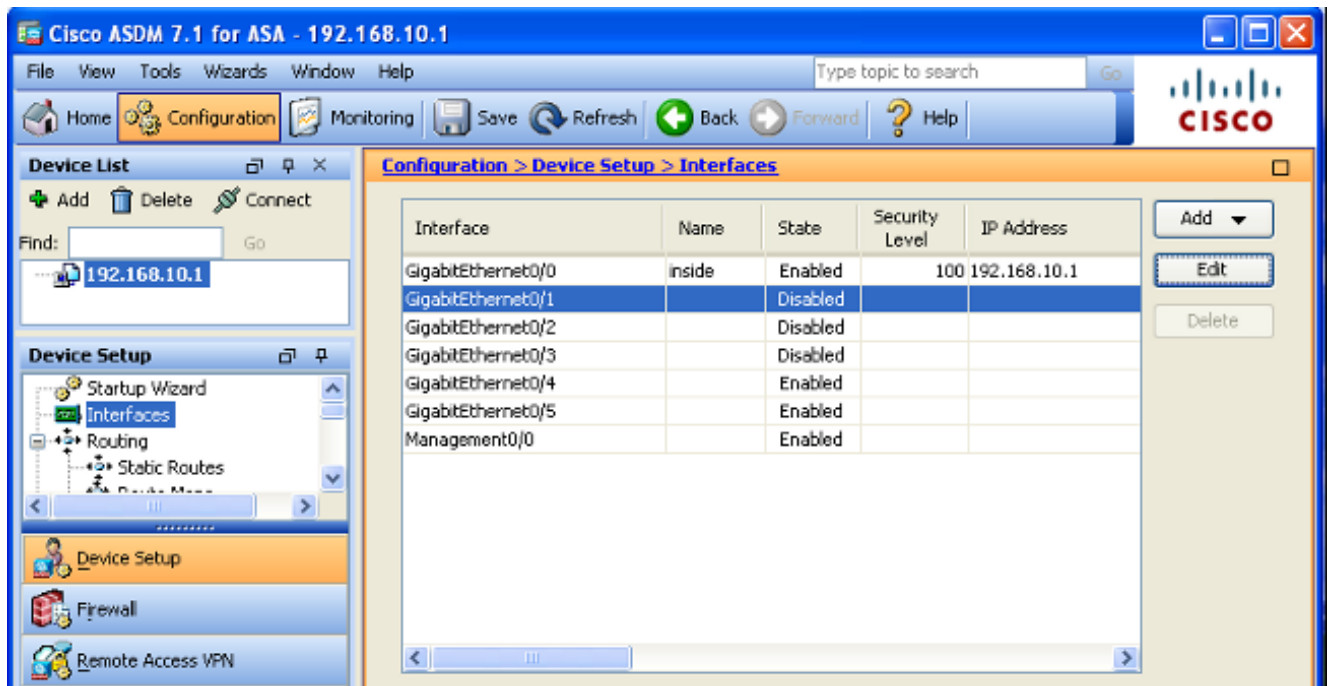
!--- defined above.

```
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
priority-queue inside
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect rsh
    inspect rtsp
    inspect esmtp
    inspect sqlnet
    inspect skinny
    inspect sunrpc
    inspect xdmcp
    inspect sip
    inspect netbios
    inspect tftp
    inspect ip-options
    inspect icmp
!
service-policy global_policy global
```

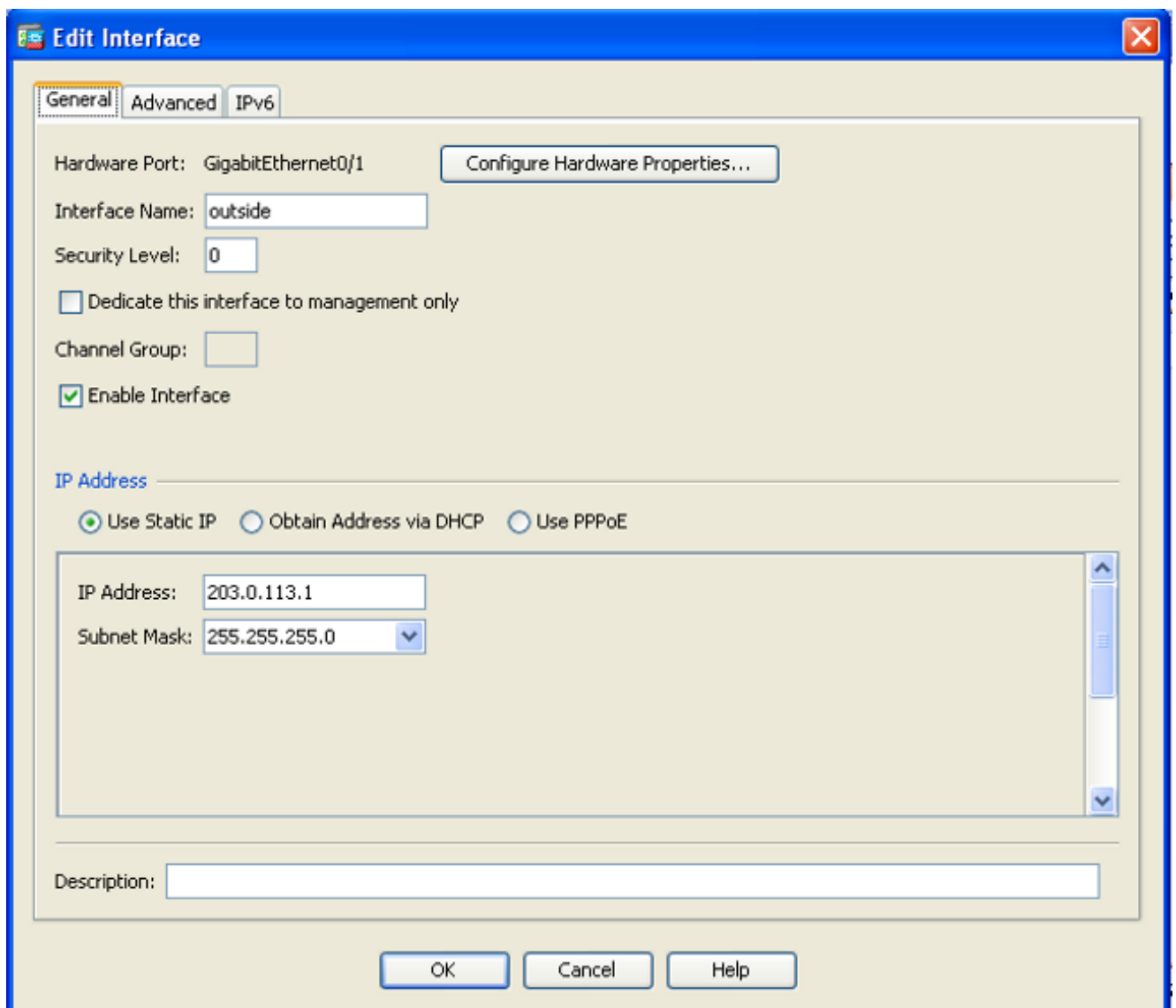
ASDM-configuratie

Voltooi deze stappen om redundante of back-up ISP ondersteuning te configureren met de [ASDM-toepassing](#):

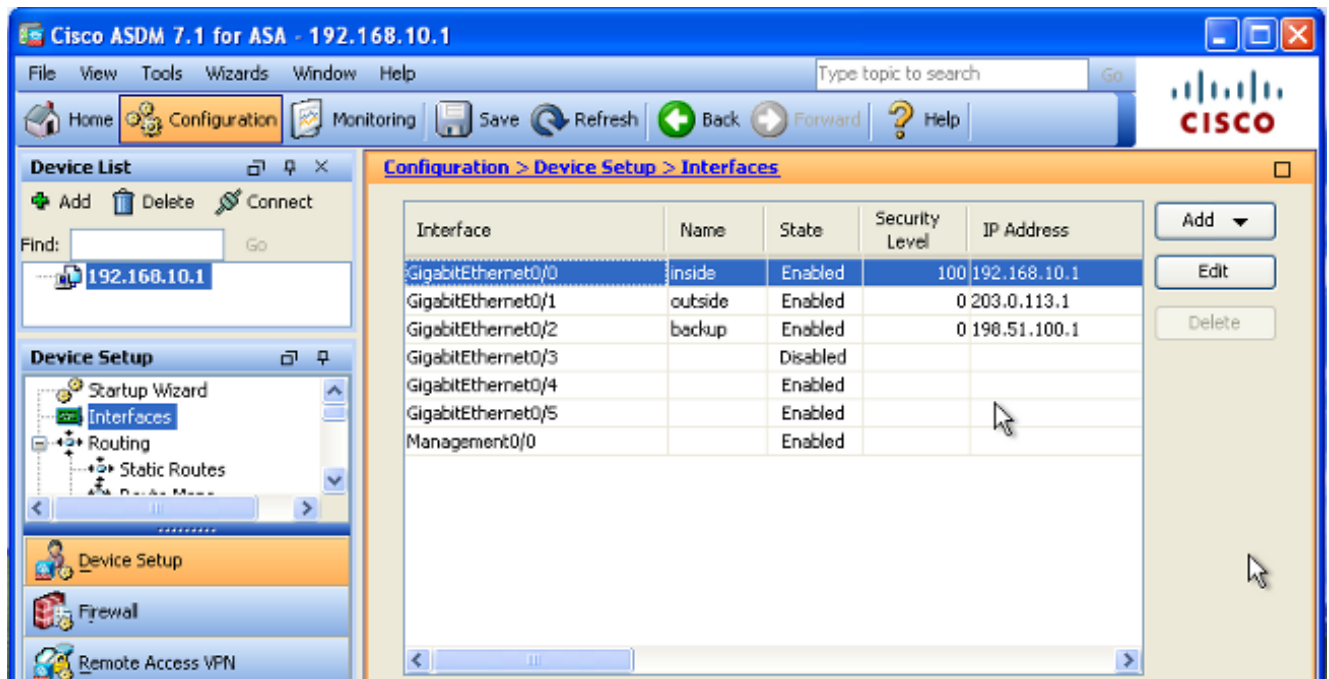
1. Klik in de ASDM-toepassing op **Configuration** en vervolgens op **Interfaces**.



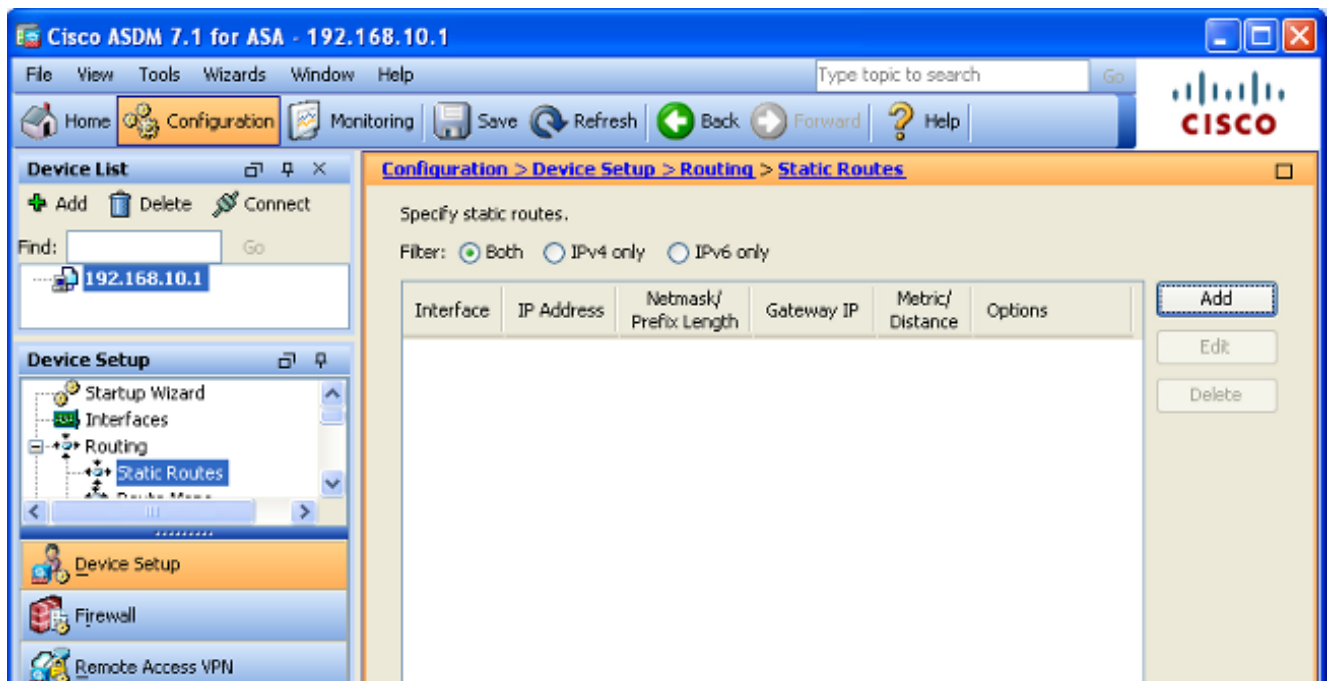
2. Selecteer **Gigabit Ethernet0/1** in de lijst Interfaces en klik vervolgens op **Bewerken**. Dit dialoogvenster verschijnt:



- Controleer het aankruisvakje **Interface inschakelen** en voer de juiste waarden in de velden *Interfacenaam*, *Beveiligingsniveau*, *IP-adres* en *Subnetmasker* in.
- Klik op **OK** om het dialoogvenster te sluiten.
- Configureer de andere interfaces zoals nodig en klik vervolgens op **Toepassen** om de ASA configuratie bij te werken:



- Selecteer **Routing** en klik op **statische routers** aan de linkerkant van de ASDM-toepassing:



- Klik op **Add** om de nieuwe statische routes toe te voegen. Dit dialoogvenster verschijnt:

Edit Static Route

IP Address Type: IPv4 IPv6

Interface:

Network:

Gateway IP: Metric:

Options

None

Tunneled (Default tunnel gateway for VPN traffic)

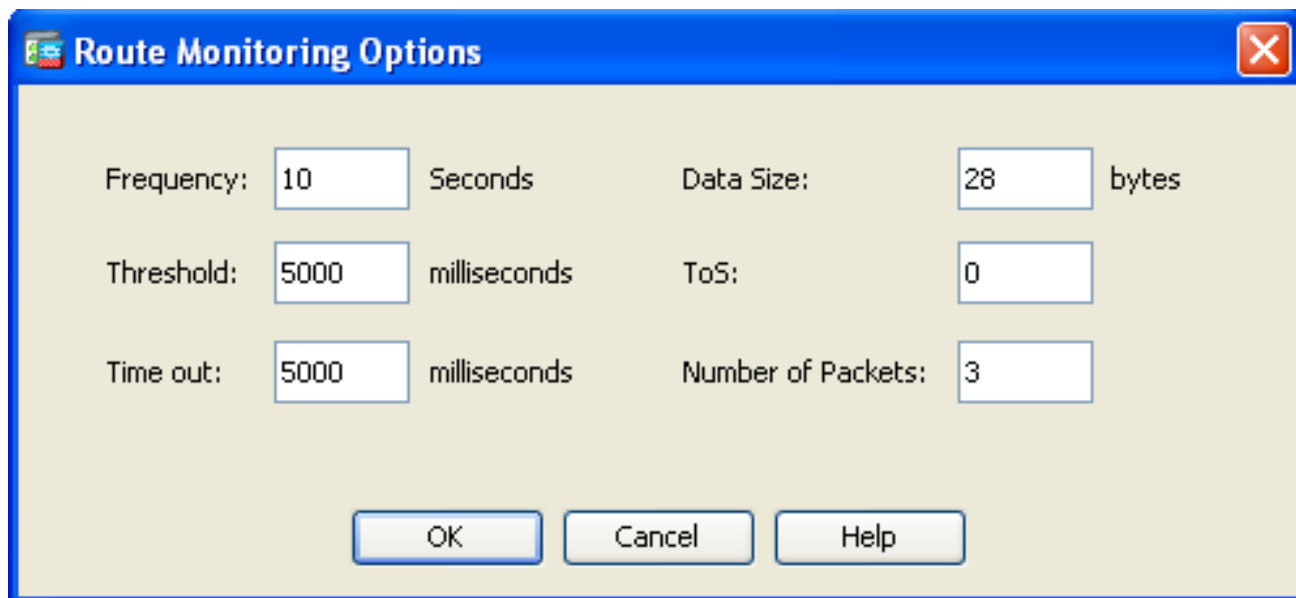
Tracked

Track ID: Track IP Address:

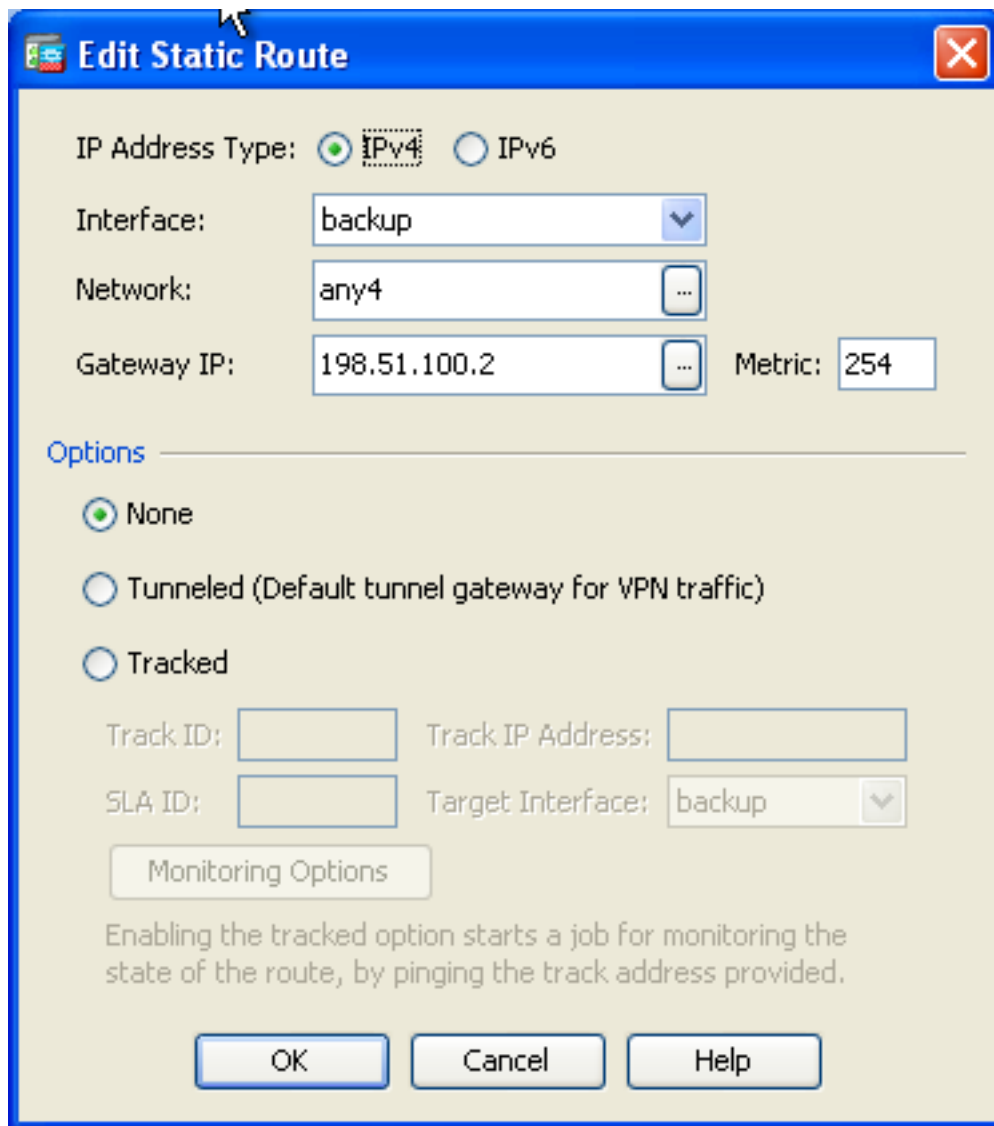
SLA ID: Target Interface:

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

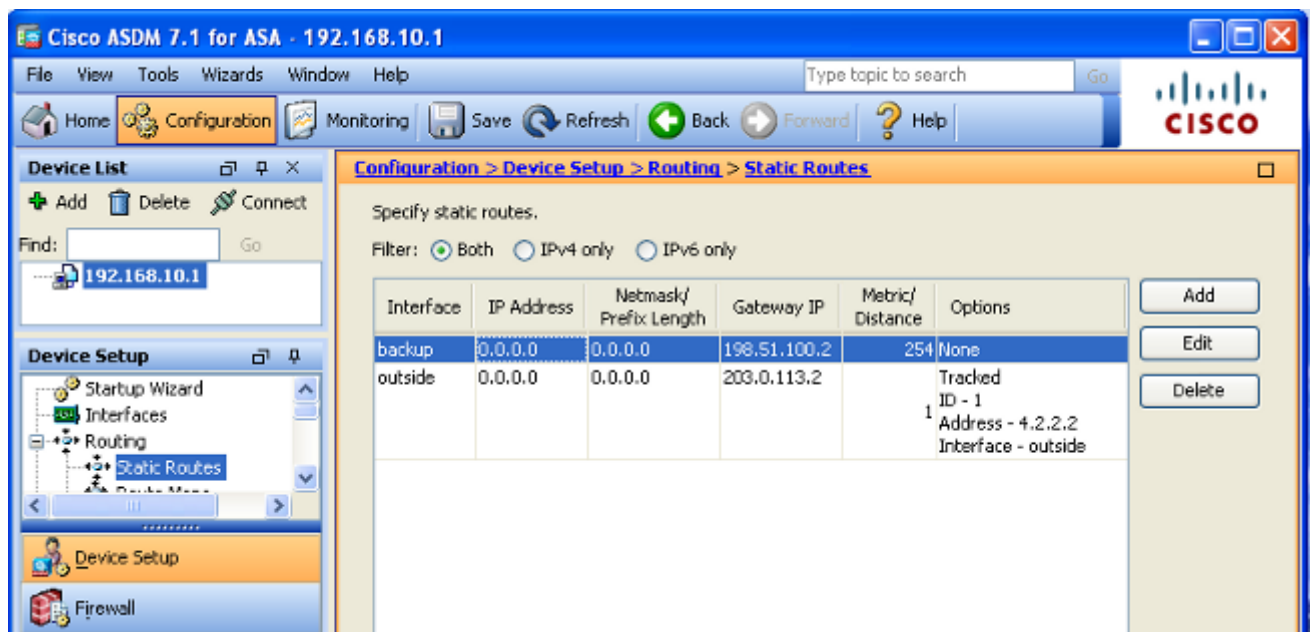
8. Kies de interface waarop de route zich bevindt in de vervolgkeuzelijst Interfacenaam en stel de standaardroute in om de poort te bereiken. In dit voorbeeld, **203.0.113.2** is de primaire ISP gateway en **4.2.2.2** is het object om met de ICMP echo's te controleren.
9. In het gebied Opties, klik op de radioknop **Tracked** en voer de juiste waarden in in de velden SLA-ID, *SLA-ID* en *IP-adres*.
10. Klik op **bewakingsopties**. Dit dialoogvenster verschijnt:



11. Voer de gewenste waarden in voor de frequentie en andere opties voor controle en klik vervolgens op **OK**.
12. Voeg een andere statische route voor de secundaire ISP toe om een route te verstrekken om het internet te bereiken. Om het een secundaire route te maken, moet u deze route met een hogere statistiek configureren, zoals 254. Als de primaire route (primaire ISP) faalt, wordt die route verwijderd van de routingtabel. Deze secundaire route (secondaire ISP) is in plaats daarvan geïnstalleerd in de PIX-routingtabel (Private Internet Exchange).
13. Klik op **OK** om het dialoogvenster te sluiten:



De configuraties verschijnen in de interfacelijst.



14. Selecteer de routerconfiguratie en klik vervolgens op **Toepassen** om de ASA-configuratie bij te werken.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Controleer of de configuratie voltooid is

Opmerking: De [Output Interpreter Tool \(alleen voor geregistreeerde klanten\) ondersteunt bepaalde opdrachten met show](#). Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show**.

Gebruik deze opdrachten om te controleren of de configuratie is voltooid:

- **toon in werking stellen-beslist monitor** - De uitvoer van deze opdracht toont de SLA opdrachten in de configuratie.

```
ASA# show running-config sla monitor
sla monitor 123
  type echo protocol ipIcmpEcho 4.2.2.2 interface outside
  num-packets 3
  frequency 10
sla monitor schedule 123 life forever start-time now
```

- **Toon de configuratie van de monitor** - De uitvoer van deze opdracht toont de huidige configuratie instellingen van de verrichting.

```
ASA# show sla monitor configuration 123
IP SLA Monitor, Infrastructure Engine-II.
Entry number: 123
Owner:
Tag:
Type of operation to perform: echo
Target address: 4.2.2.2
Interface: outside
Number of packets: 3
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data&colon; No
Operation frequency (seconds): 10
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

- **Laat de operationele toestand zien** - De uitvoer van deze opdracht geeft de operationele statistieken van de SLA-operatie weer.

Voordat de primaire ISP failliet gaat, is dit de operationele staat:

```
ASA# show sla monitor operational-state 123
Entry number: 123
Modification time: 13:30:40.672 IND Sun Jan 4 2015
Number of Octets Used by this Entry: 2056
```

```
Number of operations attempted: 46
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 13:38:10.672 IND Sun Jan 4 2015
Latest operation return code: OK
RTT Values:
RTTAvg: 1          RTTMin: 1          RTTMax: 1
NumOfRTT: 3       RTTSum: 3          RTTSum2: 3
```

Nadat de primaire ISP faalt (en het ICMP bevestigt de time-out), is dit de operationele status:

```
ASA# show sla monitor operational-state
Entry number: 123
Modification time: 13:30:40.671 IND Sun Jan 4 2015
Number of Octets Used by this Entry: 2056
Number of operations attempted: 57
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 13:40:00.672 IND Sun Jan 4 2015
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0          RTTMin: 0          RTTMax: 0
NumOfRTT: 0       RTTSum: 0          RTTSum2: 0
```

Bevestig dat de back-uproute is geïnstalleerd (CLI-methode)

Typ de opdracht route **tonen** om te bevestigen dat de back-uproute is geïnstalleerd.

Voordat de primaire ISP faalt, lijkt de routingtabel op dit punt:

```
ASA# 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 203.0.113.2 to network 0.0.0.0
```

```
C    203.0.113.0 255.255.255.0 is directly connected, outside
C    192.168.10.0 255.255.255.0 is directly connected, inside
C    198.51.100.0 255.255.255.0 is directly connected, backup
S*  0.0.0.0 0.0.0.0 [1/0] via 203.0.113.2, outside
```

Nadat de primaire ISP faalt, wordt de statische route verwijderd, en de reserveroute wordt geïnstalleerd, lijkt de routingtabel op dit:

ASA# **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

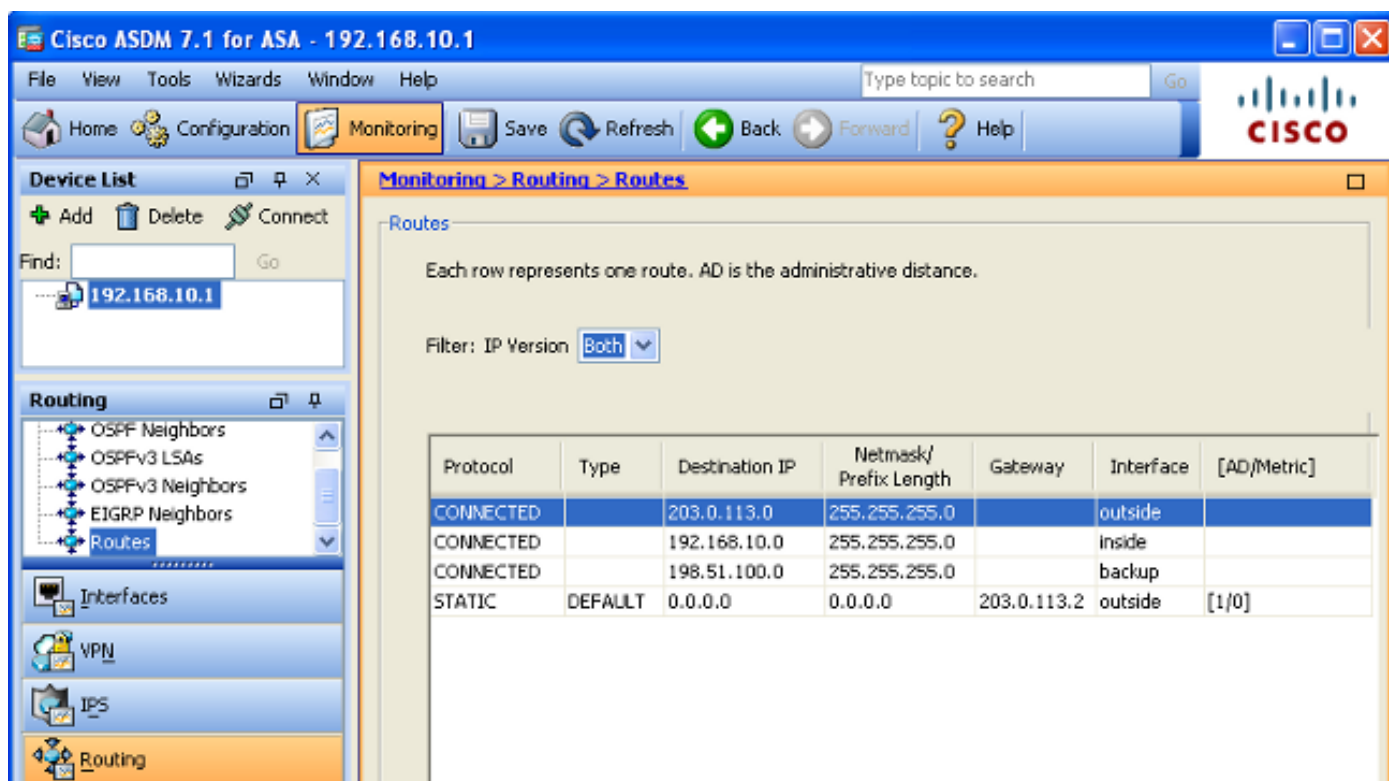
Gateway of last resort is 198.51.100.2 to network 0.0.0.0

```
C 203.0.113.0 255.255.255.0 is directly connected, outside
C 192.168.10.0 255.255.255.0 is directly connected, inside
C 198.51.100.0 255.255.255.0 is directly connected, backup
S* 0.0.0.0 0.0.0.0 [254/0] via 198.51.100.2, backup
```

Bevestig dat de back-uproute is geïnstalleerd (ASDM-methode)

Om te bevestigen dat de backup route via ASDM geïnstalleerd is, navigeer naar **Monitoring > Routing** en kies vervolgens **Routes** uit de routingboom.

Voordat de primaire ISP faalt, lijkt de routingtabel gelijk aan de tabel die in de volgende afbeelding wordt weergegeven. Merk op dat de **DEFAULT**-route naar **203.0.113.2** wijst via de **externe** interface:



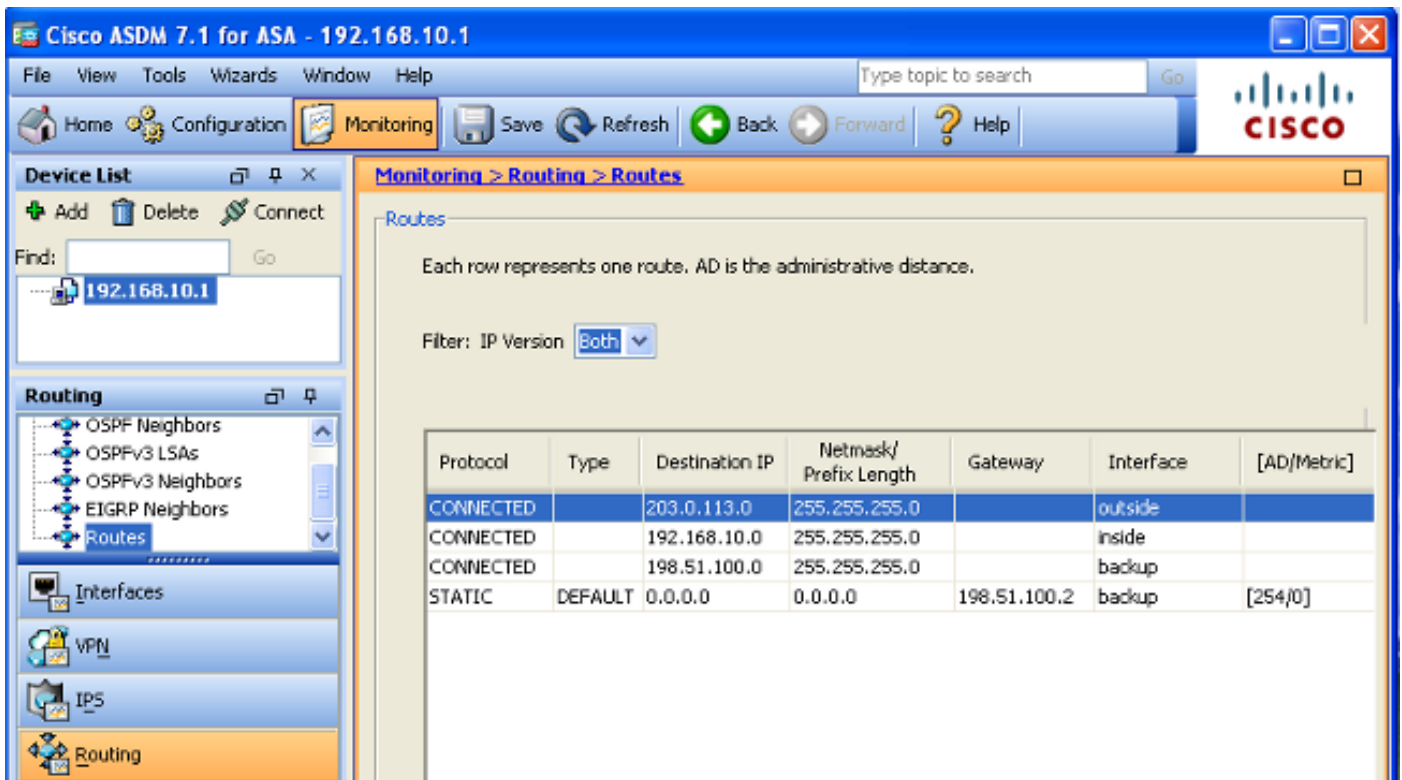
Monitoring > Routing > Routes

Each row represents one route. AD is the administrative distance.

Filter: IP Version

Protocol	Type	Destination IP	Netmask/ Prefix Length	Gateway	Interface	[AD/Metric]
CONNECTED		203.0.113.0	255.255.255.0		outside	
CONNECTED		192.168.10.0	255.255.255.0		inside	
CONNECTED		198.51.100.0	255.255.255.0		backup	
STATIC	DEFAULT	0.0.0.0	0.0.0.0	203.0.113.2	outside	[1/0]

Nadat de primaire ISP faalt, wordt de route verwijderd en wordt de back-uproute geïnstalleerd. De **STANDAARD**route wijst nu op **198.51.100.2** via de **back-up**interface:



Problemen oplossen

Deze sectie verschaft een aantal nuttige debug opdrachten en beschrijft hoe u problemen kunt oplossen bij een probleem waar de getraceerde route onnodig wordt verwijderd.

Opdrachten debug

U kunt deze debug-opdrachten gebruiken om problemen met uw configuratie op te lossen:

- **debug slo monitor trace** - De uitvoer van deze opdracht geeft de voortgang van de echo-bewerking weer.

Als het getraceerde object (primaire ISP poort) omhoog is en de ICMP echo's slagen, verschijnt de output gelijkend op dit:

```
IP SLA Monitor(123) Scheduler: Starting an operation
IP SLA Monitor(123) echo operation: Sending an echo operation
IP SLA Monitor(123) echo operation: RTT=0 OK
IP SLA Monitor(123) echo operation: RTT=0 OK
IP SLA Monitor(123) echo operation: RTT=1 OK
IP SLA Monitor(123) Scheduler: Updating result
```

Als het getraceerde object (primaire ISP poort) is ingedrukt en het ICMP echo's faalt, lijkt de output vergelijkbaar met dit:

```
IP SLA Monitor(123) Scheduler: Starting an operation
IP SLA Monitor(123) echo operation: Sending an echo operation
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) Scheduler: Updating result
```


- **debug van een fout in de monitor** - De uitvoer van deze opdracht toont fouten die het SLA-monitorproces tegenkomt.

Als het getraceerde object (primaire ISP poort) omhoog is en het ICMP slaagt, verschijnt de output gelijkend op dit:

```
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:4.2.2.2
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/39878 laddr 203.0.113.1/39878
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/39878 laddr 203.0.113.1/39878
%ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:00
%ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:00
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:4.2.2.2
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/39879 laddr 203.0.113.1/39879
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/39879 laddr 203.0.113.1/39879
%ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:00
%ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:00
```

Als het getraceerde object (primaire ISP-poort) omlaag is en de getraceerde route wordt verwijderd, verschijnt de output precies zo:

```
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:4.2.2.2
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/59003 laddr 203.0.113.1/59003
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/59004 laddr 203.0.113.1/59004
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/59005 laddr 203.0.113.1/59005
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/59003 laddr 203.0.113.1/59003
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/59004 laddr 203.0.113.1/59004
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/59005 laddr 203.0.113.1/59005
%ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:02
%ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:02
%ASA-6-622001: Removing tracked route 0.0.0.0 0.0.0.0 203.0.113.2,
distance 1, table Default-IP-Routing-Table, on interface outside

!--- 4.2.2.2 is unreachable, so the route to the Primary ISP is removed.
```

Overtrokken route wordt onnodig verwijderd

Als de trackroute onnodig wordt verwijderd, zorg er dan voor dat uw controledoel altijd beschikbaar is om echo-verzoeken te ontvangen. Zorg er bovendien voor dat de status van uw bewakingsdoel (dwz, of het doel al dan niet bereikbaar is) nauw verbonden is met de staat van de primaire ISP-verbinding.

Als u een controledoel kiest dat verder weg dan de ISP gateway is, zou een andere verbinding langs die route kunnen mislukken of een ander apparaat kan interfereren. Deze configuratie kan de SLA monitor veroorzaken om te concluderen dat de verbinding met de primaire ISP heeft gefaald en de ASA onnodig laten falen over de secundaire ISP verbinding.

Bijvoorbeeld, als u een router van het bijkantoor als uw controledoel kiest zou de verbinding van ISP met uw bijkantoor, evenals een andere verbinding onderweg kunnen mislukken. Zodra het ICMP echoën die door de controleoperatie worden verzonden, wordt de primaire getraceerde route verwijderd, alhoewel de primaire ISP verbinding nog actief is.

In dit voorbeeld, de primaire ISP gateway die als het controledoel wordt gebruikt wordt door de ISP beheerd en bevindt zich aan de andere kant van de ISP verbinding. Deze configuratie waarborgt dat als het ICMP echo's weergeeft die door de controle operatie worden verzonden, de ISP verbinding vrijwel zeker is omlaag.

Gerelateerde informatie

- [Cisco ASA 5500-X Series Next-generation firewalls](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)