ASA/PIX 7.x: Configuratievoorbeeld van redundante of back-up ISP-links

Inhoud

Inleiding

Een probleem met statische routes is dat er geen inherent mechanisme bestaat om te 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 te volgen en, als die route faalt, deze uit de routingtabel te verwijderen en door een back-uproute te vervangen.

Dit document geeft een voorbeeld van hoe de statische route-tracking-functie moet worden gebruikt op de PIX 500 Series security applicatie of de ASA 5500 Series adaptieve security applicatie, om het apparaat in staat te stellen redundante of back-up internetverbindingen te gebruiken. In dit voorbeeld staat statische route volgen het veiligheidsapparaat toe om een goedkope verbinding aan een secundaire dienstverlener van Internet (ISP) te gebruiken als de

primaire huurlijn niet beschikbaar wordt.

Om deze redundantie te bereiken, associeert het veiligheidsapparaat een statische route met een door u gedefinieerd bewakingsdoel. De SLA-operatie (Service Level Agreement) controleert het doel met periodieke verzoeken van ICMP-echo's (Internet Control Message Protocol). Als een antwoord van echo niet wordt ontvangen, wordt het object neerwaarts overwogen en de bijbehorende route wordt 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 proberen het doel te bereiken. Zodra het doel opnieuw beschikbaar is, wordt de eerste route vervangen in de routingtabel, en wordt de reserveroute verwijderd.

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

Voorwaarden

Vereisten

Kies een bewakingsdoel dat kan reageren op verzoeken van de ICMP-echo. Het doel kan elk netwerkobject zijn dat u kiest, maar een doel dat nauw verbonden is met uw ISP-verbinding wordt aanbevolen. Enkele mogelijke controledoelstellingen zijn:

- Het ISP-poortadres
- Een ander ISP-beheerd adres
- Een server op een ander netwerk, zoals een AAA-server, waarmee het beveiligingsapparaat 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 het beveiligingsapparaat volledig gebruiksklaar is en is geconfigureerd om Cisco ASDM in staat te stellen de configuratie te wijzigen.

Opmerking: Raadpleeg voor informatie over hoe u ASDM kunt toestaan om het apparaat te configureren HTTPS-toegang voor ASDM.

Gebruikte componenten

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

- Cisco PIX security applicatie 5150E met softwareversie 7.2(1) of hoger
- Cisco adaptieve security applicatie Manager 5.2(1) 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 security applicatie, versie 7.2(1).

Opmerking: de opdracht **back-upinterface** is vereist om de vierde interface van de ASA 5505 te configureren. Raadpleeg de back-upinterface voor meer informatie.

Conventies

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

Achtergrondinformatie

In dit voorbeeld onderhoudt het beveiligingsapparaat twee verbindingen met 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 digitale abonneelijn (DSL) die door een DSL-modem wordt benaderd die door de secundaire ISP wordt geleverd.

Opmerking: taakverdeling gebeurt in dit voorbeeld niet.

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 wordt verbroken, verandert het security apparaat de routingtabel om het verkeer naar de DSL-verbinding te richten. Statische route tracking wordt gebruikt om deze redundantie te bereiken.

Het veiligheidsapparaat is ingesteld met een statische route die al het internetverkeer naar de primaire ISP leidt. Elke 10 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 uitgaande internettoegang beschikbaar blijft voor gebruikers achter het beveiligingsapparaat. Zoals in dit document wordt beschreven, is deze instelling mogelijk niet geschikt voor inkomende toegang tot bronnen achter het beveiligingsapparaat. Geavanceerde netwerkvaardigheden zijn vereist om naadloze inkomende verbindingen te bereiken. Deze vaardigheden komen niet in dit document aan bod.

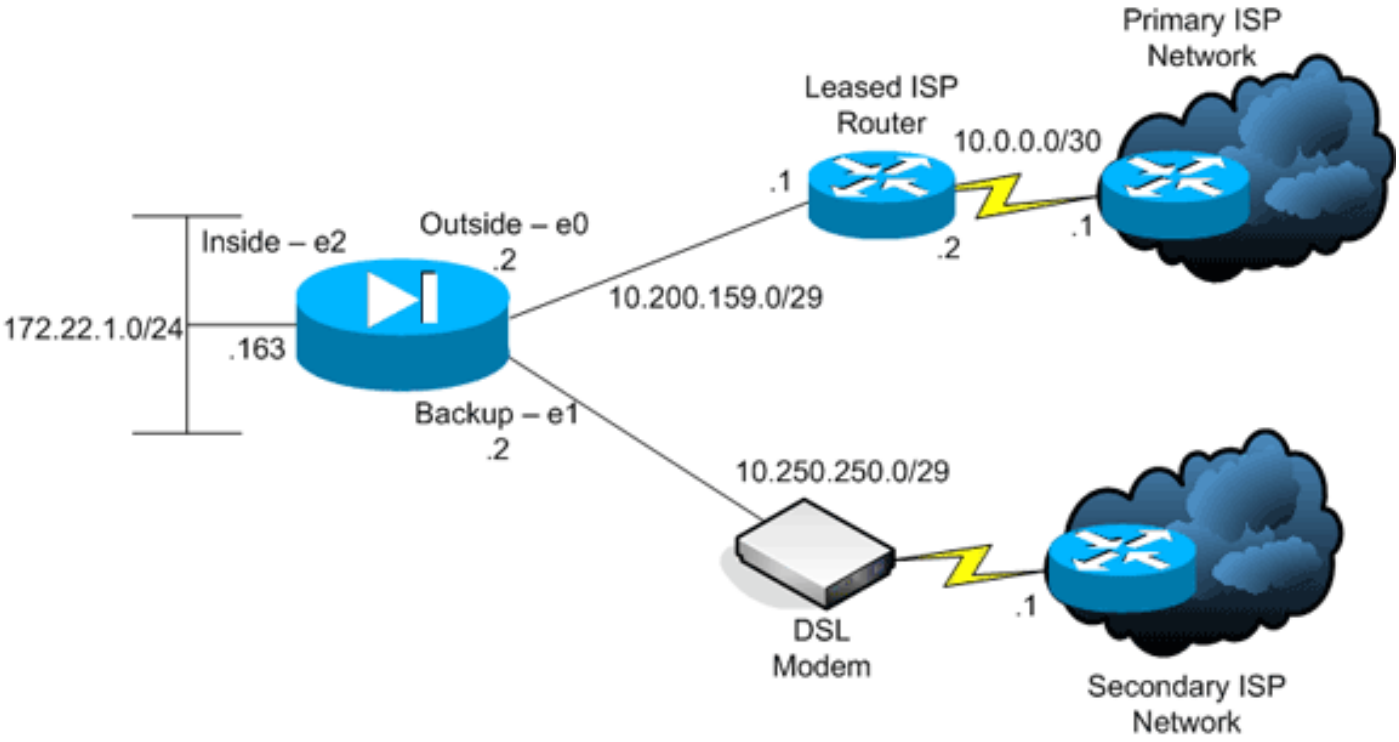
Configureren

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

Opmerking: de IP-adressen die in deze configuratie gebruikt worden, zijn niet wettelijk routeerbaar op internet. Het zijn RFC 1918 adressen die in een labomgeving gebruikt worden.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt deze configuraties:

- Opdracht-Line Interface (CLI)
- Adaptieve Security Devices Manager (ASDM)

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

CLI-configuratie

PIX

```
pix# show running-config
: Saved
:
PIX Version 7.2(1)
!
hostname pix
domain-name default.domain.invalid
enable password 9jNfZuG3TC5tCVH0 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.200.159.2 255.255.255.248
!
interface Ethernet1
 nameif backup
!--- The interface attached to the Secondary ISP. !---
"backup" was chosen here, but any name can be assigned.
security-level 0 ip address 10.250.250.2 255.255.255.248
! interface Ethernet2 nameif inside security-level 100
ip address 172.22.1.163 255.255.255.0 ! interface
```

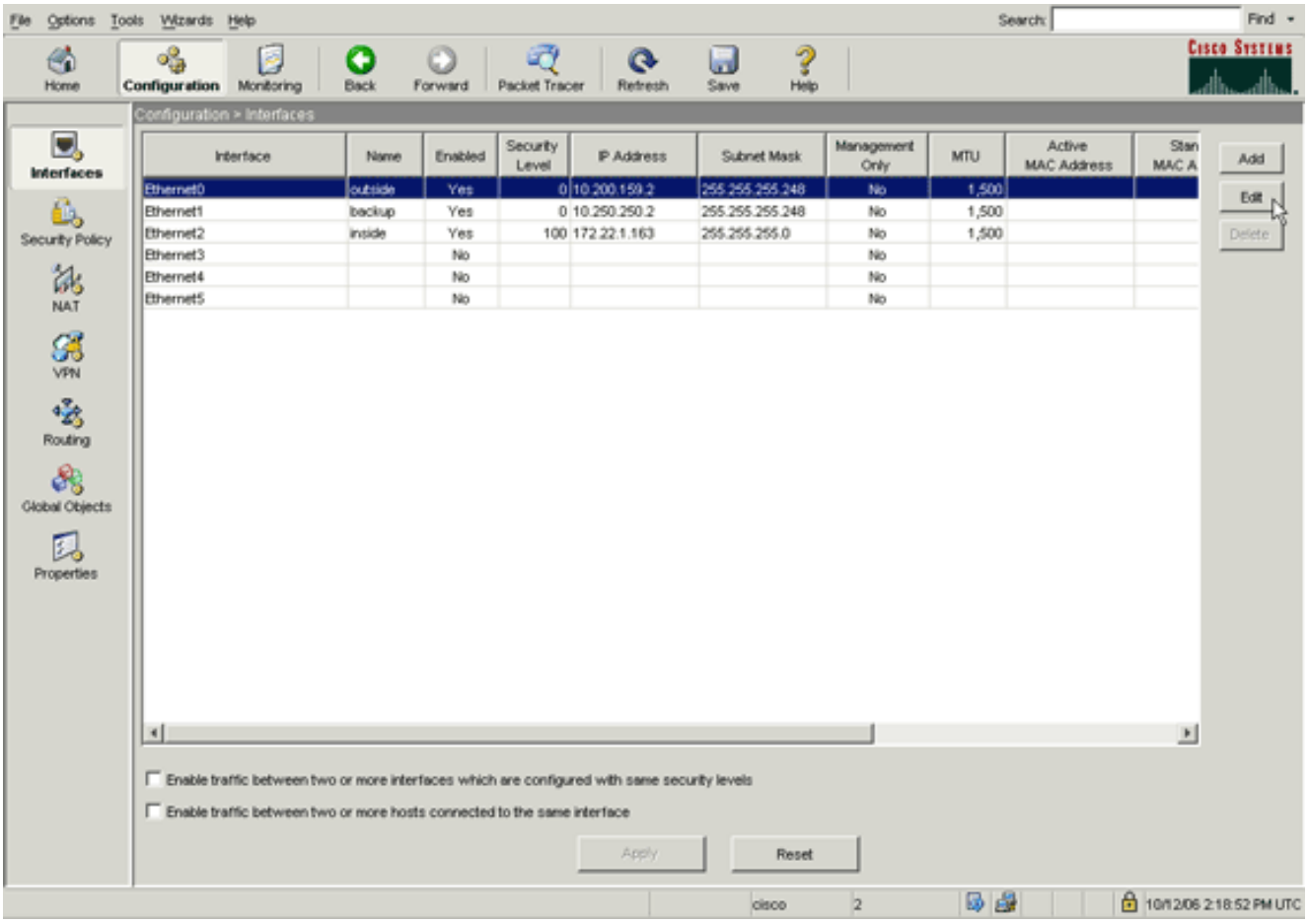
```
Ethernet3 shutdown no nameif no security-level no ip
address ! interface Ethernet4 shutdown no nameif no
security-level no ip address ! interface Ethernet5
shutdown no nameif no security-level no ip address !
passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive dns
server-group DefaultDNS domain-name
default.domain.invalid pager lines 24 logging enable
logging buffered debugging mtu outside 1500 mtu backup
1500 mtu inside 1500 no failover asdm image
flash:/asdm521.bin no asdm history enable arp timeout
14400 global (outside) 1 interface
global (backup) 1 interface
nat (inside) 1 172.16.1.0 255.255.255.0
!--- NAT Configuration for Outside and Backup route
outside 0.0.0.0 0.0.0.0 10.200.159.1 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
10.250.250.1 254
!--- 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 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 uauth 0:05:00 absolute
username cisco password ffIRPGpDSOJh9YLq encrypted http
server enable http 172.22.1.0 255.255.255.0 inside no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart sla monitor 123
 type echo protocol ipIcmpEcho 10.0.0.1 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. !
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 timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  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 netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:a4a0e9be4593ad43bc17a1cc25e32dc2
: end
```

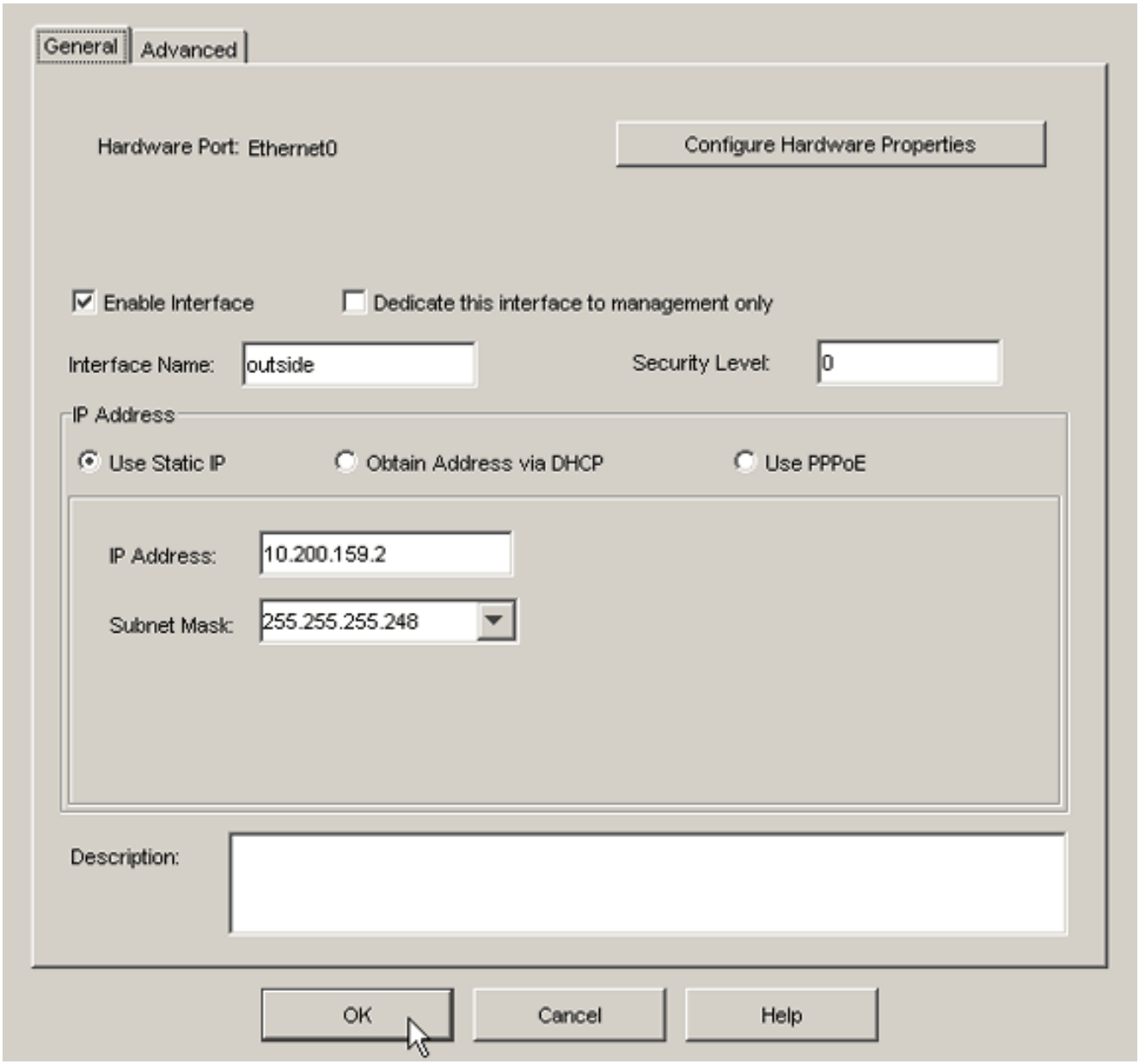
ASDM-configuratie

Voltooi de volgende stappen om redundante of back-up ISP-ondersteuning met de ASDM-toepassing te configureren:

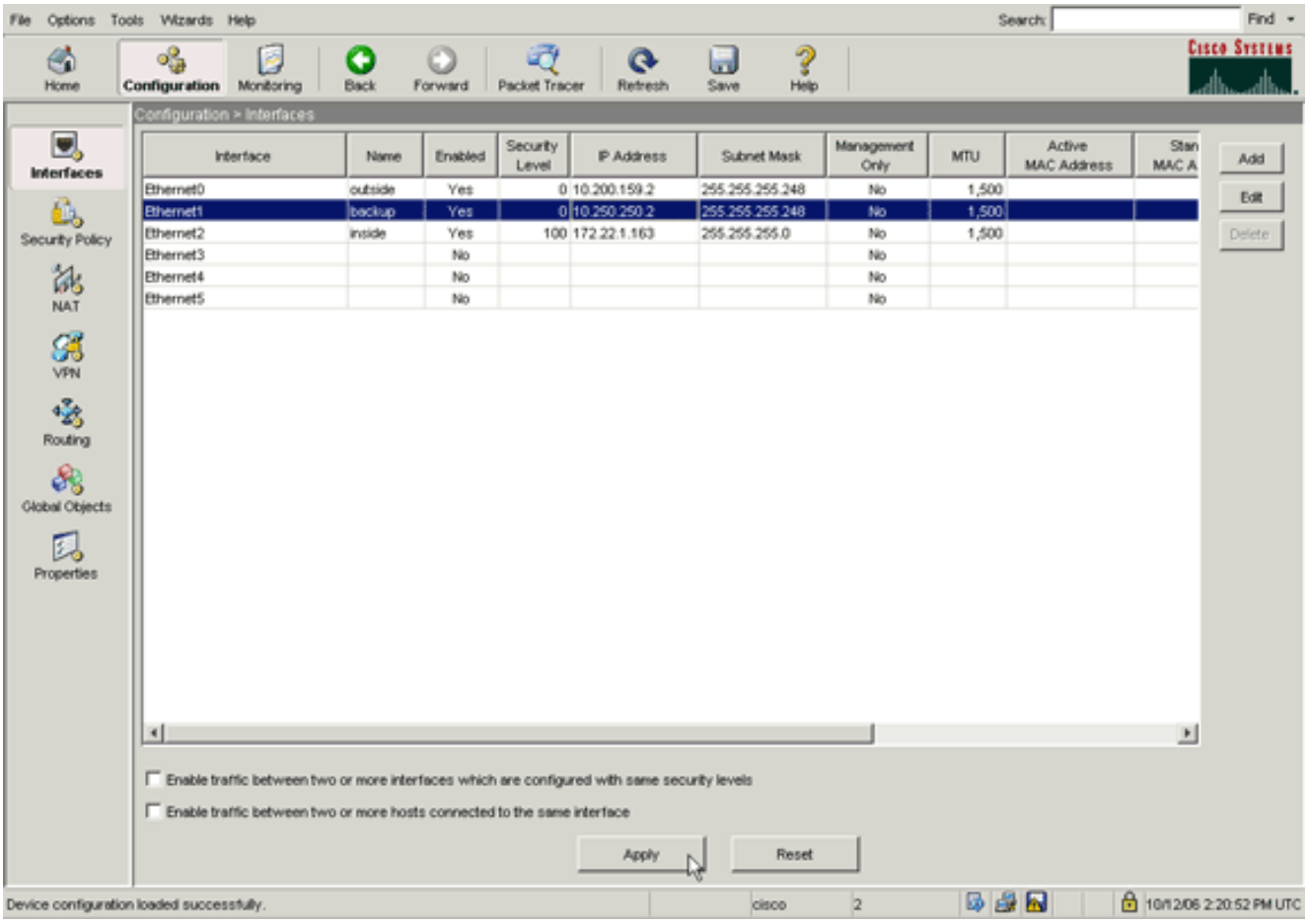
1. Klik in de ASDM-toepassing op **Configuration** en vervolgens op **Interfaces**.



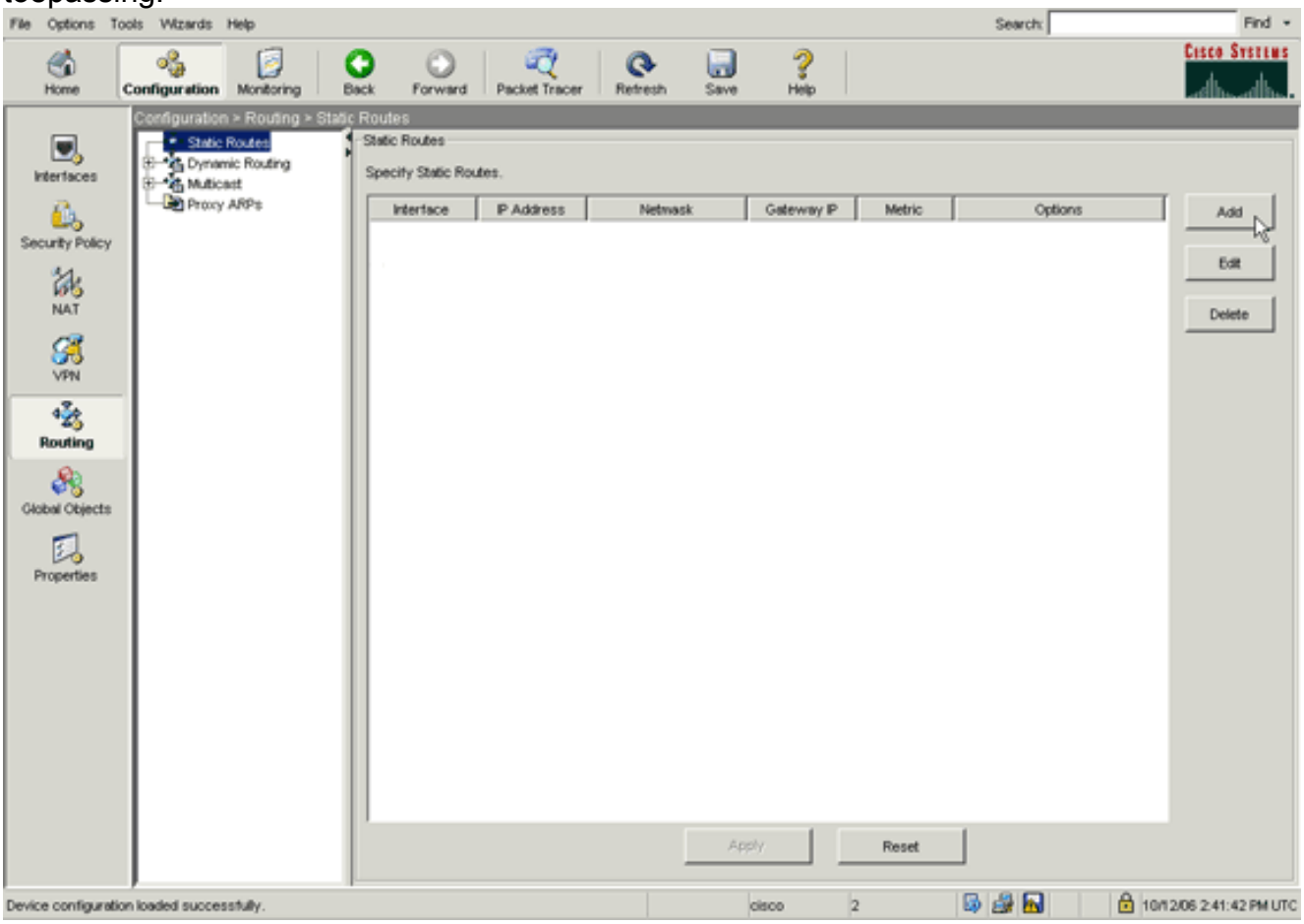
2. Selecteer in de lijst Interfaces de optie **Ethernet0** en klik vervolgens op **Bewerken**.Dit dialoogvenster
verschijnt.



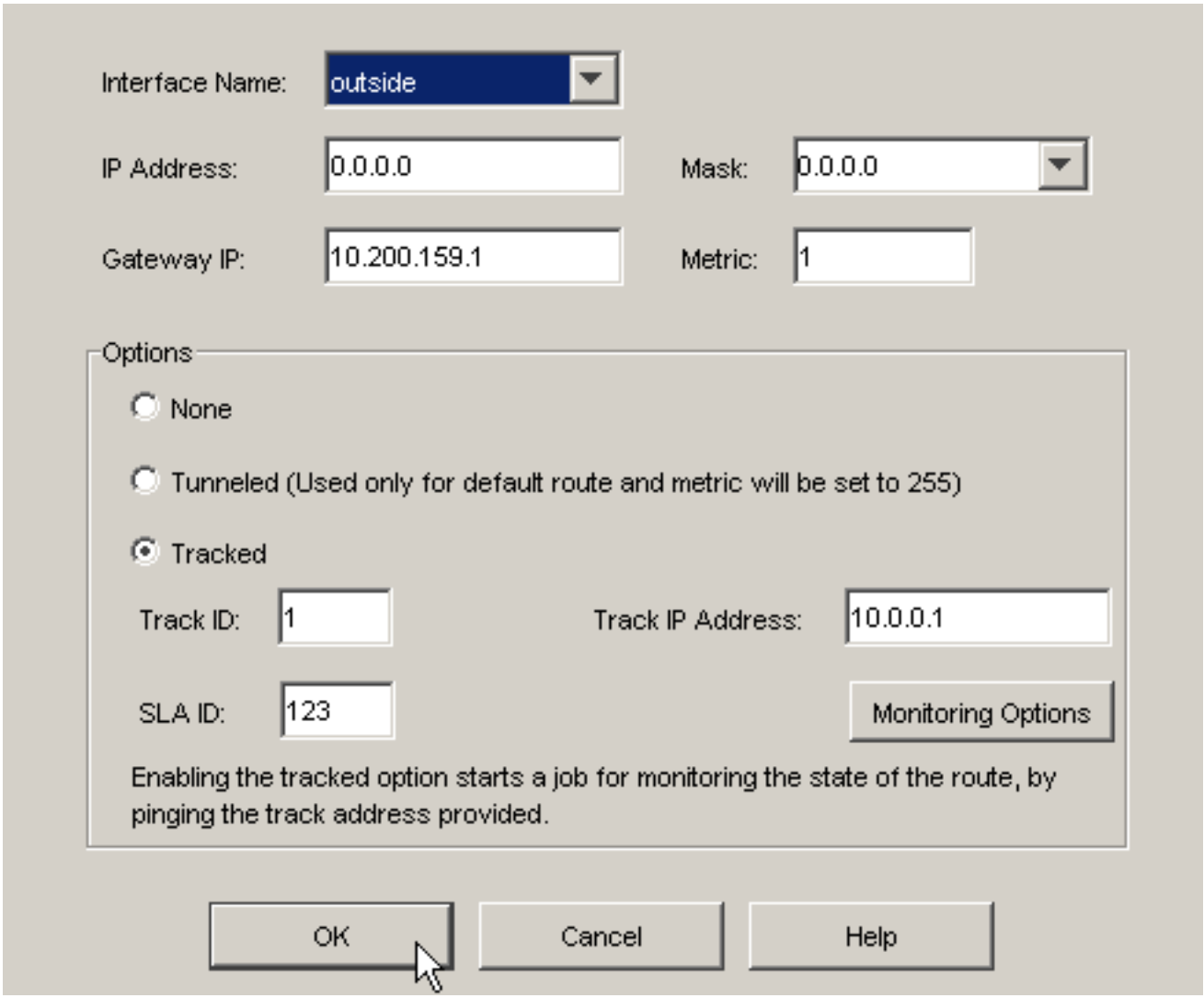
3. Controleer het dialoogvenster **Interface inschakelen** en voer waarden in de velden Interfacenaam, Beveiligingsniveau, IP-adres en Subnetmasker in.
4. Klik op **OK** om het dialoogvenster te sluiten.
5. Configureer andere interfaces zoals nodig en klik op **Toepassen** om de configuratie van het beveiligingsapparaat bij te
werken.



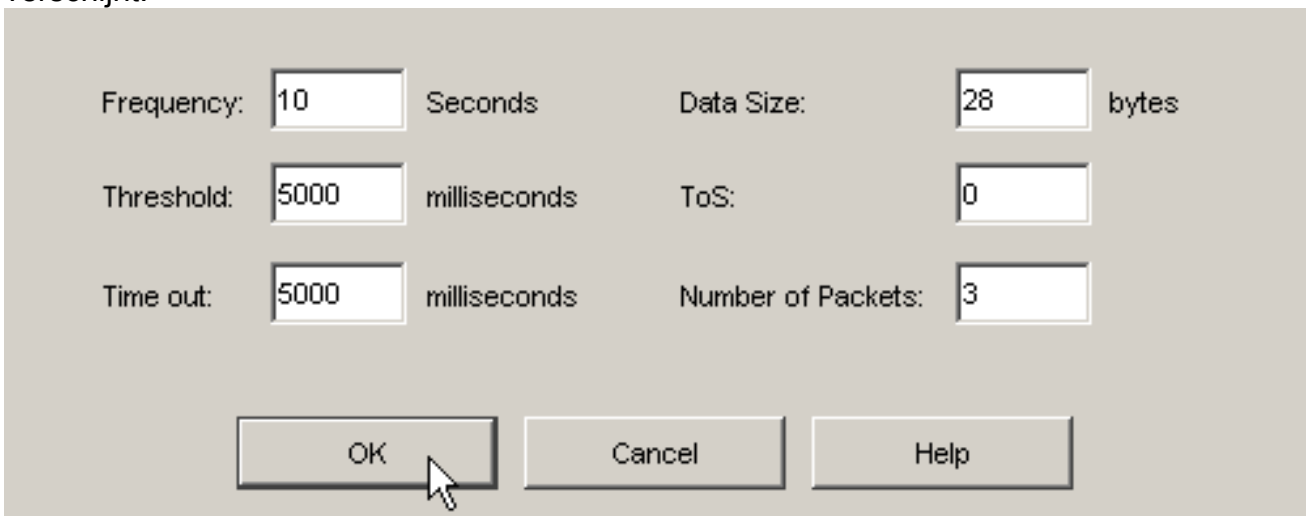
6. Klik op **Routing** aan de linkerkant van de ASDM-toepassing.



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



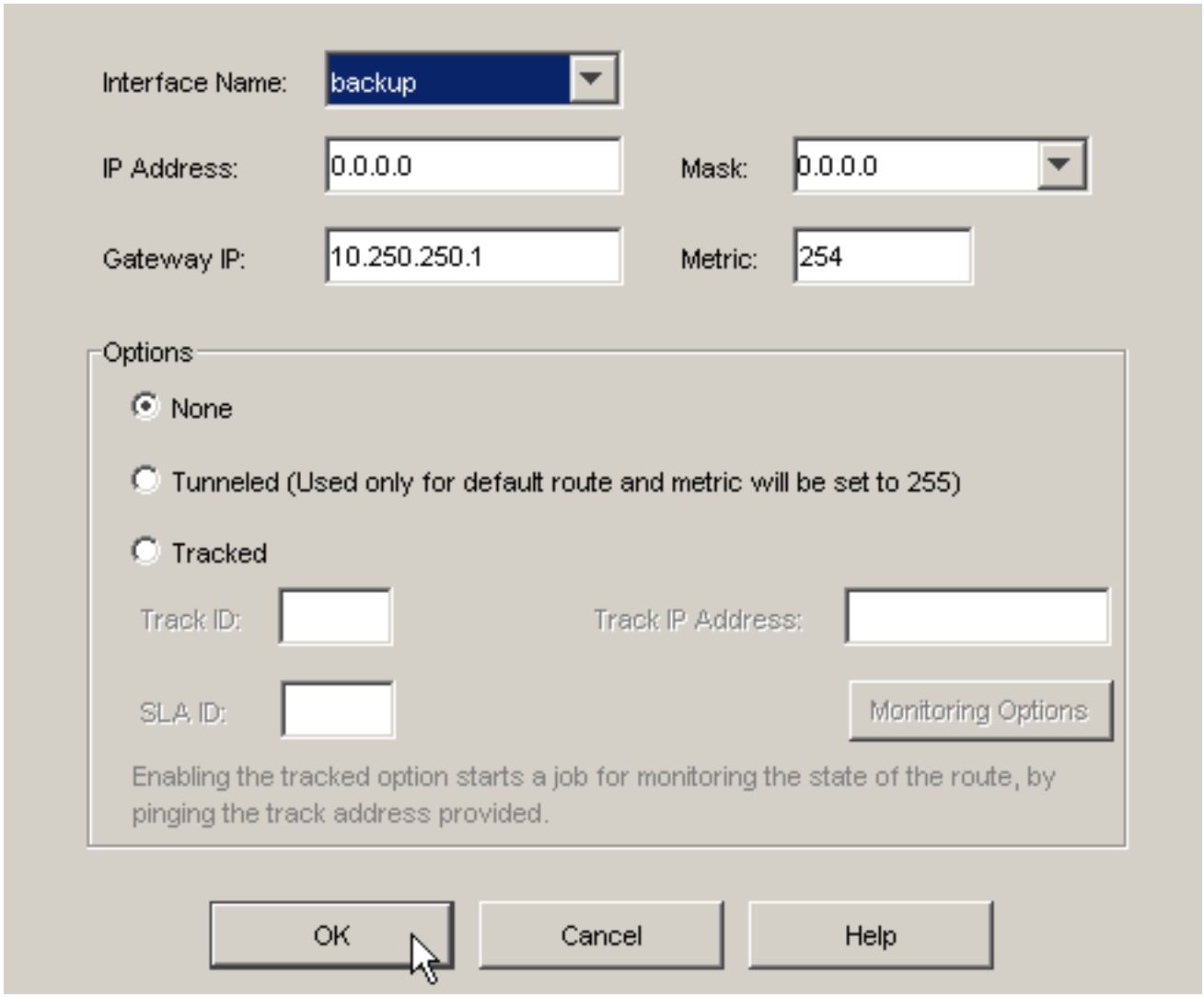
8. Kies de interface waarop de route zich bevindt in de vervolgkeuzelijst Interfacenaam en stel de standaardroute in om de poort te bereiken. In dit voorbeeld, is 10.0.0.1 de primaire ISP gateway, zowel als het object om met de echo's van ICMP te controleren.
9. In het gebied Opties, klik de radioknop **Tracked**, en voer waarden in in de velden TrainingID, SLA ID en IP-adres.
10. Klik op **bewakingsopties**.Dit dialoogvenster verschijnt.



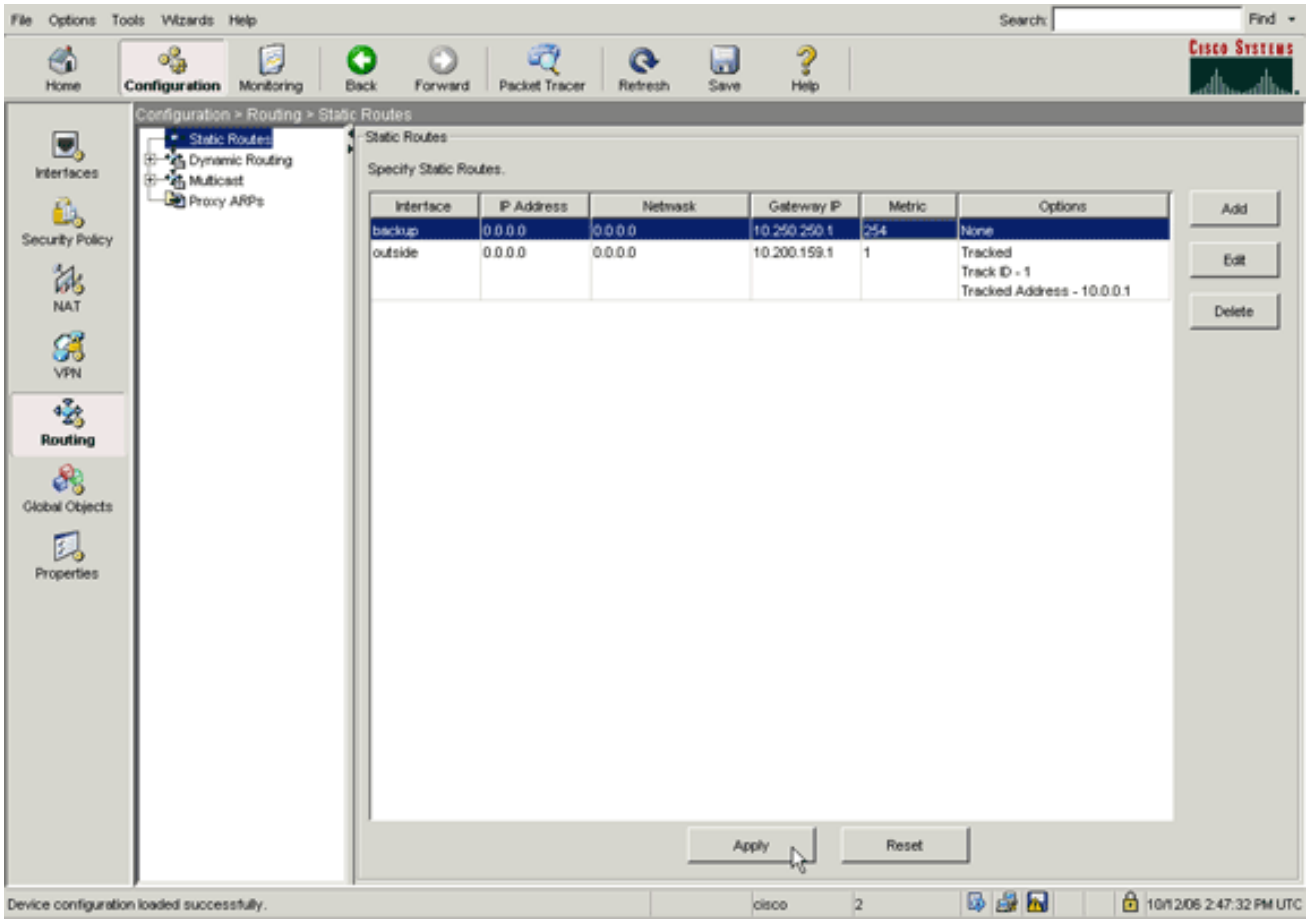
11. Voer waarden in voor frequentie en andere opties voor controle en klik op **OK**.
12. Voeg een andere statische route voor de secundaire ISP toe om een route te verstrekken om het internet te bereiken.Om het een secundaire route te maken, moet u deze route met

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.

13. Klik op **OK** om het dialoogvenster te sluiten.



De configuraties verschijnen in de lijst Interface.



14. Selecteer de routerconfiguratie en klik op **Toepassen** om de configuratie van het beveiligingsapparaat bij te werken.

Verifiëren

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

Controleer of de configuratie is voltooid

Gebruik deze opdrachten **om** te controleren of de configuratie is voltooid.

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

- **toon in werking stellen-beslist monitor**-Toont de SLA opdrachten in de configuratie.

```
pix# show running-config sla monitor
sla monitor 123
 type echo protocol ipIcmpEcho 10.0.0.1 interface outside
 num-packets 3
 frequency 10
sla monitor schedule 123 life forever start-time now
```

- **toon de configuratie van de monitor** - Hiermee geeft u de huidige configuratie-instellingen van de handeling weer.

```
pix# show sla monitor configuration 123
IP SLA Monitor, Infrastructure Engine-II.
Entry number: 123
Owner:
Tag:
```

```
Type of operation to perform: echo
Target address: 10.0.0.1
Interface: outside
Number of packets: 3
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: 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 monitor operationele-staat**-displays de operationele statistieken van de SLA werking zien.Voordat de primaire ISP failliet gaat, is dit de operationele staat:

```
pix# show sla monitor operational-state 123
Entry number: 123
Modification time: 13:59:37.824 UTC Thu Oct 12 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 367
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: 15:00:37.825 UTC Thu Oct 12 2006
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 verklaart de tijd uit), is dit de operationele staat:

```
pix# show sla monitor operational-state
Entry number: 123
Modification time: 13:59:37.825 UTC Thu Oct 12 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 385
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: 15:03:27.825 UTC Thu Oct 12 2006
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)

Gebruik de opdracht route **tonen** om te bepalen wanneer de back-uproute is geïnstalleerd.

- Voordat de primaire ISP faalt, is dit de routingtabel:

```
pix# 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 10.200.159.1 to network 0.0.0.0

S    64.101.0.0 255.255.0.0 [1/0] via 172.22.1.1, inside
C    172.22.1.0 255.255.255.0 is directly connected, inside
C    10.250.250.0 255.255.255.248 is directly connected, backup
C    10.200.159.0 255.255.255.248 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.200.159.1, outside
```

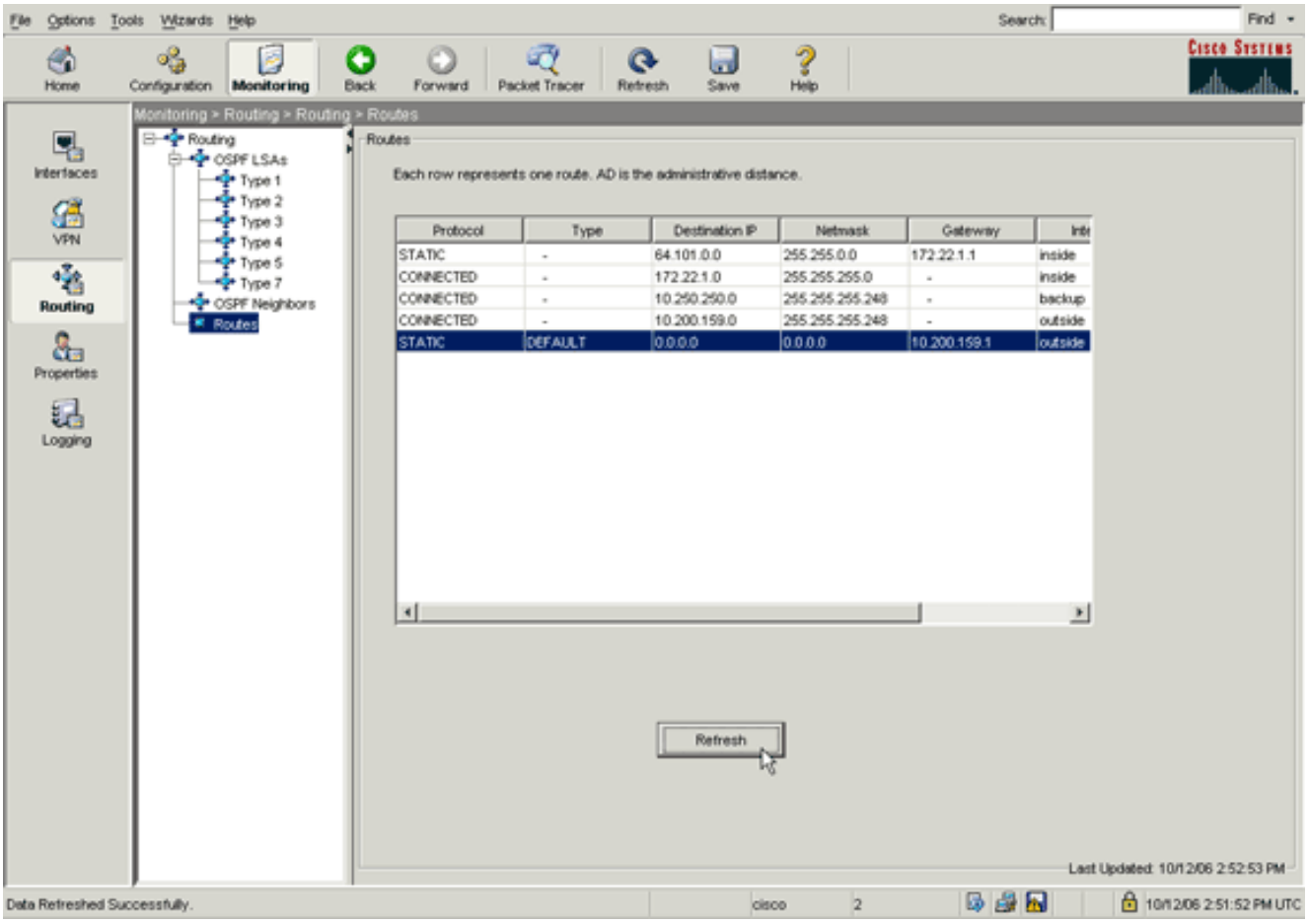
- Nadat de primaire ISP faalt, wordt de statische route verwijderd, en de reserveroute wordt geïnstalleerd, is dit de Routing Tabel:

```
pix(config)# 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 10.250.250.1 to network 0.0.0.0

S    64.101.0.0 255.255.0.0 [1/0] via 172.22.1.1, inside
C    172.22.1.0 255.255.255.0 is directly connected, inside
C    10.250.250.0 255.255.255.248 is directly connected, backup
C    10.200.159.0 255.255.255.248 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [254/0] via 10.250.250.1, backup
```

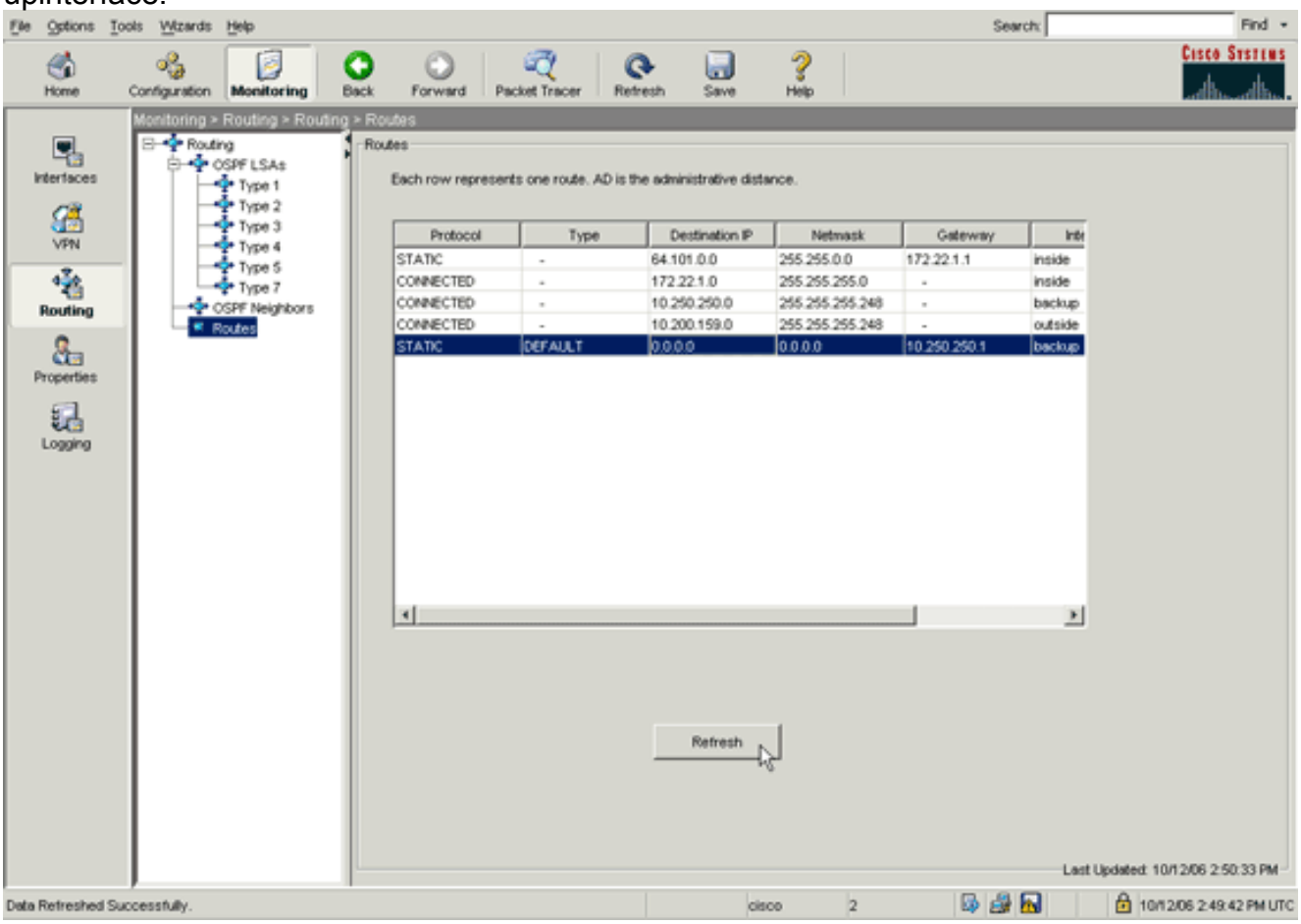
Bevestig dat de back-uproute is geïnstalleerd (ASDM-methode)

Voltooi de volgende stappen om met ASDM te bevestigen dat de back-uproute is geïnstalleerd:

1. Klik op **Monitoring** en klik vervolgens op **Routing**.
2. Kies in de routingboom **Routes**.Voordat de primaire ISP faalt, is dit de routingtabel:



De STANDAARDroute wijst naar 10.0.0.2 via de externe interface.Nadat de primaire ISP faalt, wordt de route verwijderd en wordt de back-uproute geïnstalleerd. De DEFAULT-route wijst nu naar 10.250.250.1 via de back-upinterface.



Problemen oplossen

Opdrachten debug

- **debug van de monitor spoor**-displays de voortgang van de echo-handeling.Het getraceerde object (primaire ISP poort) is omhoog, en de echo's van ICMP slagen.

```
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=3 OK
IP SLA Monitor(123) echo operation: RTT=3 OK
IP SLA Monitor(123) echo operation: RTT=4 OK
IP SLA Monitor(123) Scheduler: Updating result
```

  Het getraceerde object (primaire ISP poort) is omlaag en ICMP echo's falen.

```
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 fout**-displays die de SLA monitor processen tegenkomt.Het getraceerde object (primaire ISP poort) is omhoog, en ICMP slaagt erin.

```
%PIX-7-609001: Built local-host NP Identity Ifc:10.200.159.2
%PIX-7-609001: Built local-host outside:10.0.0.1
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/52696 laddr 10.200.159.2/52696
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/52696 laddr 10.200.159.2/52696
%PIX-7-609002: Teardown local-host NP Identity Ifc:10.200.159.2 duration
               0:00:00
%PIX-7-609002: Teardown local-host outside:10.0.0.1 duration 0:00:00
%PIX-7-609001: Built local-host NP Identity Ifc:10.200.159.2
%PIX-7-609001: Built local-host outside:10.0.0.1
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
               0.200.159.2/52697 laddr 10.200.159.2/52697
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/52697 laddr 10.200.159.2/52697
%PIX-7-609002: Teardown local-host NP Identity Ifc:10.200.159.2
               duration 0:00:00
%PIX-7-609002: Teardown local-host outside:10.0.0.1 duration 0:00:00
```

  Het getraceerde object (primaire ISP poort) is omlaag en de getraceerde route wordt verwijderd.

```
%PIX-7-609001: Built local-host NP Identity Ifc:10.200.159.2
%PIX-7-609001: Built local-host outside:10.0.0.1
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6405 laddr 10.200.159.2/6405
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6406 laddr 10.200.159.2/6406
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6407 laddr 10.200.159.2/6407
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6405 laddr 10.200.159.2/6405
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6406 laddr 10.200.159.2/6406
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6407 laddr 10.200.159.2/6407
%PIX-7-609002: Teardown local-host NP Identity Ifc:10.200.159.2
               duration 0:00:02
%PIX-7-609002: Teardown local-host outside:10.0.0.1 duration 0:00:02
%PIX-6-622001: Removing tracked route 0.0.0.0 0.0.0.0 10.200.159.1,
```

```
                distance 1, table Default-IP-Routing-Table, on interface
                outside
!--- 10.0.0.1 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, kan een andere verbinding langs die route mislukken of een ander apparaat kan interfereren. Door deze configuratie kan de SLA-monitor concluderen dat de verbinding met de primaire ISP heeft gefaald en dat het beveiligingsapparaat onnodig faalt via de secundaire ISP-link.

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 echos heeft die door de controles operatie 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.

SLA-bewaking op ASA

Probleem:

SLA-bewaking werkt niet nadat de ASA is bijgewerkt naar versie 8.0.

Oplossing:

Het probleem is mogelijk veroorzaakt door de opdracht **IP omgekeerd pad** die in de **BUITENKANT** is ingesteld. Verwijder de opdracht in ASA en probeer de SLA bewaking te controleren.

Gerelateerde informatie

- Statische routetracering configureren
- PIX/ASA 7.2 opdrachtreferentie
- Cisco ASA 5500 Series security applicaties
- Cisco PIX 500 Series security applicaties
- Technische ondersteuning en documentatie – Cisco Systems