ASA/PIX 7.x: Konfigurationsbeispiel für redundante oder Backup-ISP-Links

Inhalt

Einführung

Ein Problem mit statischen Routen besteht darin, dass kein inhärenter Mechanismus vorhanden ist, um festzustellen, ob die Route aktiv oder inaktiv ist. Die Route bleibt selbst dann in der Routing-Tabelle, wenn das nächste Hop-Gateway nicht mehr verfügbar ist. Statische Routen werden nur dann aus der Routing-Tabelle entfernt, wenn die zugehörige Schnittstelle auf der Sicherheits-Appliance ausfällt. Um dieses Problem zu beheben, wird eine statische Route-Tracking-Funktion verwendet, um die Verfügbarkeit einer statischen Route zu verfolgen. Wenn diese Route fehlschlägt, wird sie aus der Routing-Tabelle entfernt und durch eine Backup-Route ersetzt.

Dieses Dokument enthält ein Beispiel für die Verwendung der statischen Route-Tracking-Funktion auf der Security Appliance der Serie PIX 500 oder der Adaptive Security Appliance der Serie ASA 5500, um dem Gerät die Verwendung redundanter oder Backup-Internetverbindungen zu ermöglichen. In diesem Beispiel ermöglicht die statische Routenverfolgung der Verwendung einer

kostengünstigen Verbindung zu einem sekundären Internetdienstanbieter (ISP), falls die primäre Mietleitung nicht verfügbar ist.

Um diese Redundanz zu erreichen, ordnet die Security Appliance eine statische Route einem von Ihnen definierten Überwachungsziel zu. Der Service Level Agreement (SLA)-Vorgang überwacht das Ziel mithilfe von ICMP-Echoanfragen (Periodensystem Internet Control Message Protocol). Wenn keine Echo-Antwort empfangen wird, wird das Objekt als inaktiv angesehen, und die zugehörige Route wird aus der Routing-Tabelle entfernt. Anstelle der zu entfernenden Route wird eine zuvor konfigurierte Backup-Route verwendet. Während die Backup-Route verwendet wird, versucht der SLA-Überwachungsvorgang weiterhin, das Überwachungsziel zu erreichen. Sobald das Ziel wieder verfügbar ist, wird die erste Route in der Routing-Tabelle ersetzt und die Backup-Route entfernt.

Hinweis: Die in diesem Dokument beschriebene Konfiguration kann nicht für den Lastenausgleich oder die Lastverteilung verwendet werden, da sie von ASA/PIX nicht unterstützt wird. Verwenden Sie diese Konfiguration nur für Redundanz- oder Backup-Zwecke. Beim ausgehenden Datenverkehr werden der primäre und dann der sekundäre ISP verwendet, falls der primäre ausfällt. Der Ausfall des primären ISP verursacht eine temporäre Unterbrechung des Datenverkehrs.

Voraussetzungen

Anforderungen

Wählen Sie ein Überwachungsziel aus, das auf ICMP-Echo-Anfragen reagieren kann. Das Ziel kann ein beliebiges Netzwerkobjekt sein, das Sie auswählen. Es wird jedoch empfohlen, ein Ziel festzulegen, das eng mit Ihrer ISP-Verbindung verknüpft ist. Mögliche Überwachungsziele sind:

- Die ISP-Gateway-Adresse
- Eine andere vom ISP verwaltete Adresse
- Ein Server in einem anderen Netzwerk, z. B. ein AAA-Server, mit dem die Sicherheits-Appliance kommunizieren muss
- Ein persistentes Netzwerkobjekt in einem anderen Netzwerk (ein Desktop- oder Notebook-Computer, den Sie nachts herunterfahren können, ist keine gute Wahl)

In diesem Dokument wird davon ausgegangen, dass die Sicherheits-Appliance vollständig betriebsbereit und konfiguriert ist, damit der Cisco ASDM Konfigurationsänderungen vornehmen kann.

Hinweis: Weitere Informationen darüber, wie der ASDM das Gerät konfigurieren kann, finden Sie unter Zulassen von HTTPS-Zugriff für ASDM.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco PIX Security Appliance 515E mit Softwareversion 7.2(1) oder höher
- Cisco Adaptive Security Device Manager 5.2(1) oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Sie können diese Konfiguration auch mit der Cisco Security Appliance der Serie ASA 5500, Version 7.2(1), verwenden.

Hinweis: Der Befehl **backup interface** ist erforderlich, um die vierte Schnittstelle auf der ASA 5505 zu konfigurieren. Weitere Informationen finden Sie in der Sicherungsschnittstelle.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Hintergrundinformationen

In diesem Beispiel unterhält die Sicherheits-Appliance zwei Verbindungen zum Internet. Die erste Verbindung ist eine Standleitung mit hoher Geschwindigkeit, auf die über einen Router zugegriffen wird, der vom primären ISP bereitgestellt wird. Die zweite Verbindung ist eine DSL-Leitung (Digital Subscriber Line) mit niedrigerer Geschwindigkeit, auf die über ein DSL-Modem zugegriffen wird, das vom sekundären ISP bereitgestellt wird.

Hinweis: Load Balancing tritt in diesem Beispiel nicht auf.

Die DSL-Verbindung ist inaktiv, solange die Mietleitung aktiv ist und das primäre ISP-Gateway erreichbar ist. Fällt jedoch die Verbindung zum primären ISP aus, ändert die Security Appliance die Routing-Tabelle so, dass der Datenverkehr an die DSL-Verbindung geleitet wird. Diese Redundanz wird durch statische Routenverfolgung erreicht.

Die Sicherheits-Appliance ist mit einer statischen Route konfiguriert, die den gesamten Internetdatenverkehr an den primären ISP weiterleitet. Alle 10 Sekunden überprüft der SLA-Überwachungsprozess, ob das primäre ISP-Gateway erreichbar ist. Wenn der SLA-Überwachungsprozess feststellt, dass das primäre ISP-Gateway nicht erreichbar ist, wird die statische Route, die den Datenverkehr an diese Schnittstelle weiterleitet, aus der Routing-Tabelle entfernt. Um diese statische Route zu ersetzen, wird eine alternative statische Route installiert, die den Datenverkehr an den sekundären ISP weiterleitet. Diese alternative statische Route leitet den Datenverkehr über das DSL-Modem an den sekundären ISP weiter, bis die Verbindung zum primären ISP erreichbar ist.

Diese Konfiguration bietet eine relativ kostengünstige Möglichkeit sicherzustellen, dass der ausgehende Internetzugriff für Benutzer hinter der Sicherheits-Appliance verfügbar bleibt. Wie in diesem Dokument beschrieben, eignet sich diese Konfiguration möglicherweise nicht für den eingehenden Zugriff auf Ressourcen hinter der Sicherheits-Appliance. Um nahtlose eingehende Verbindungen zu ermöglichen, sind erweiterte Netzwerkkenntnisse erforderlich. Diese Fähigkeiten werden in diesem Dokument nicht behandelt.

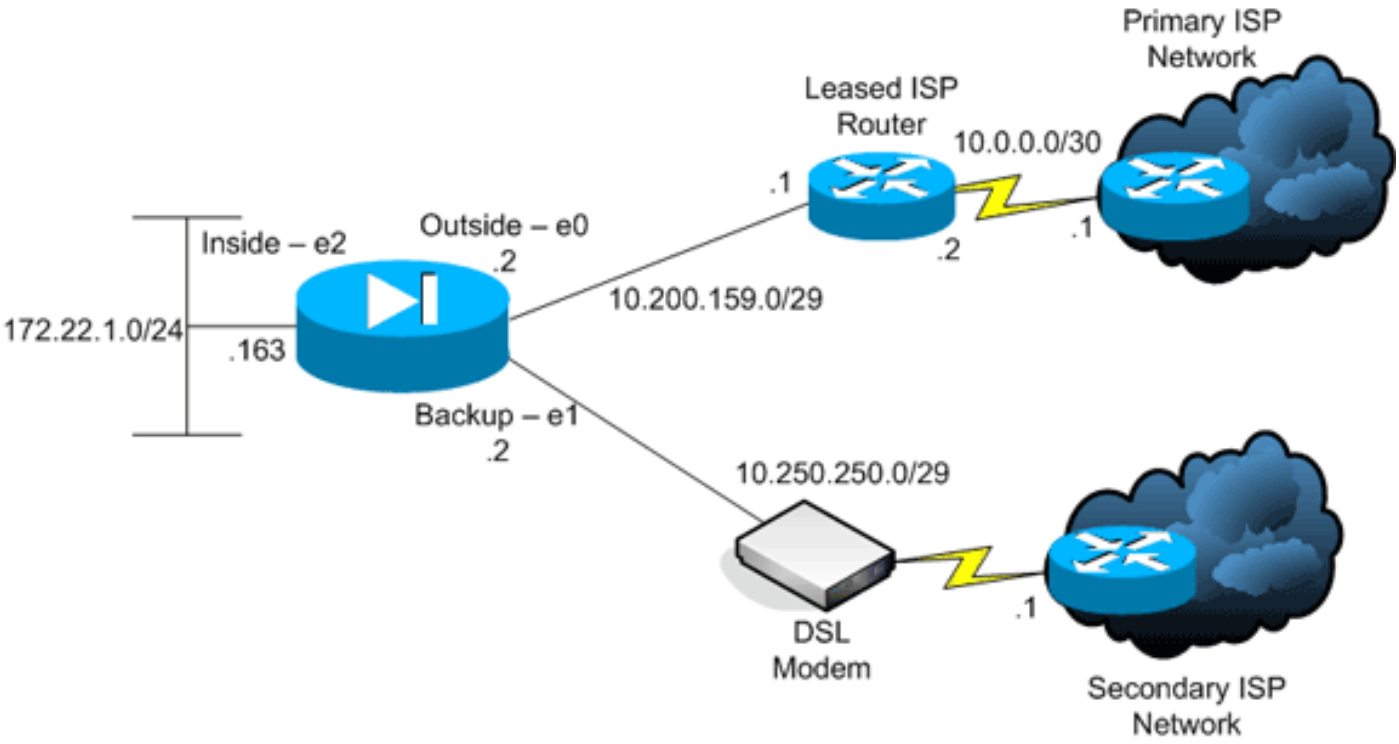
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Die in dieser Konfiguration verwendeten IP-Adressen können nicht legal im Internet geroutet werden. Sie sind RFC 1918 -Adressen, die in einer Laborumgebung verwendet werden.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- Befehlszeilenschnittstelle (CLI)
- Adaptive Security Device Manager (ASDM)

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

CLI-Konfiguration

PIX

```
pix# show running-config
: Saved
:
PIX Version 7.2(1)
!
hostname pix
domain-name default.domain.invalid
enable password 9jNfZuG3TC5tCVH0 encrypted
names
```

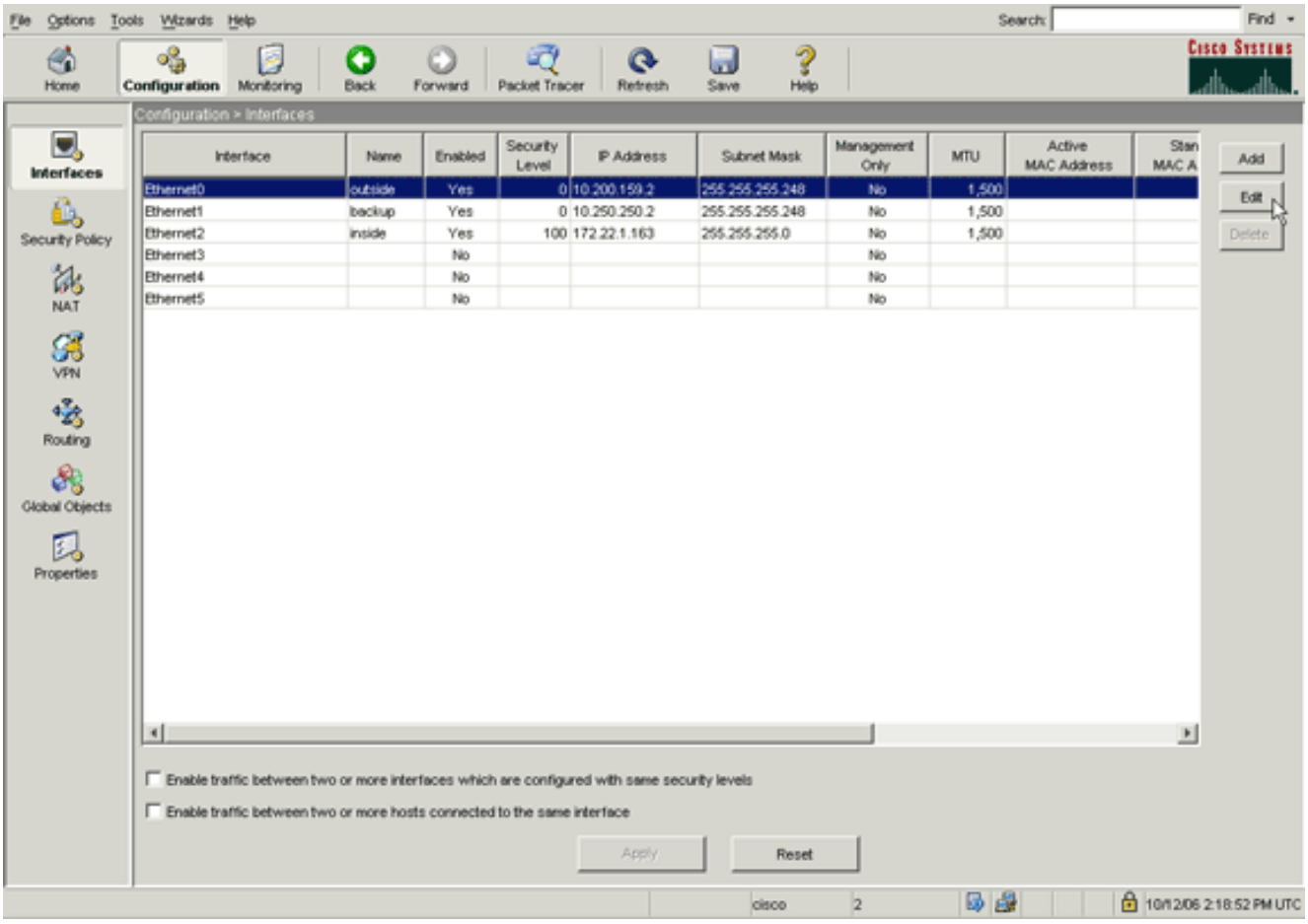
```
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.200.159.2 255.255.255.248
!
interface Ethernet1
 nameif backup
!--- The interface attached to the Secondary ISP. !---
"backup" was chosen here, but any name can be assigned.
security-level 0 ip address 10.250.250.2 255.255.255.248
! 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
```

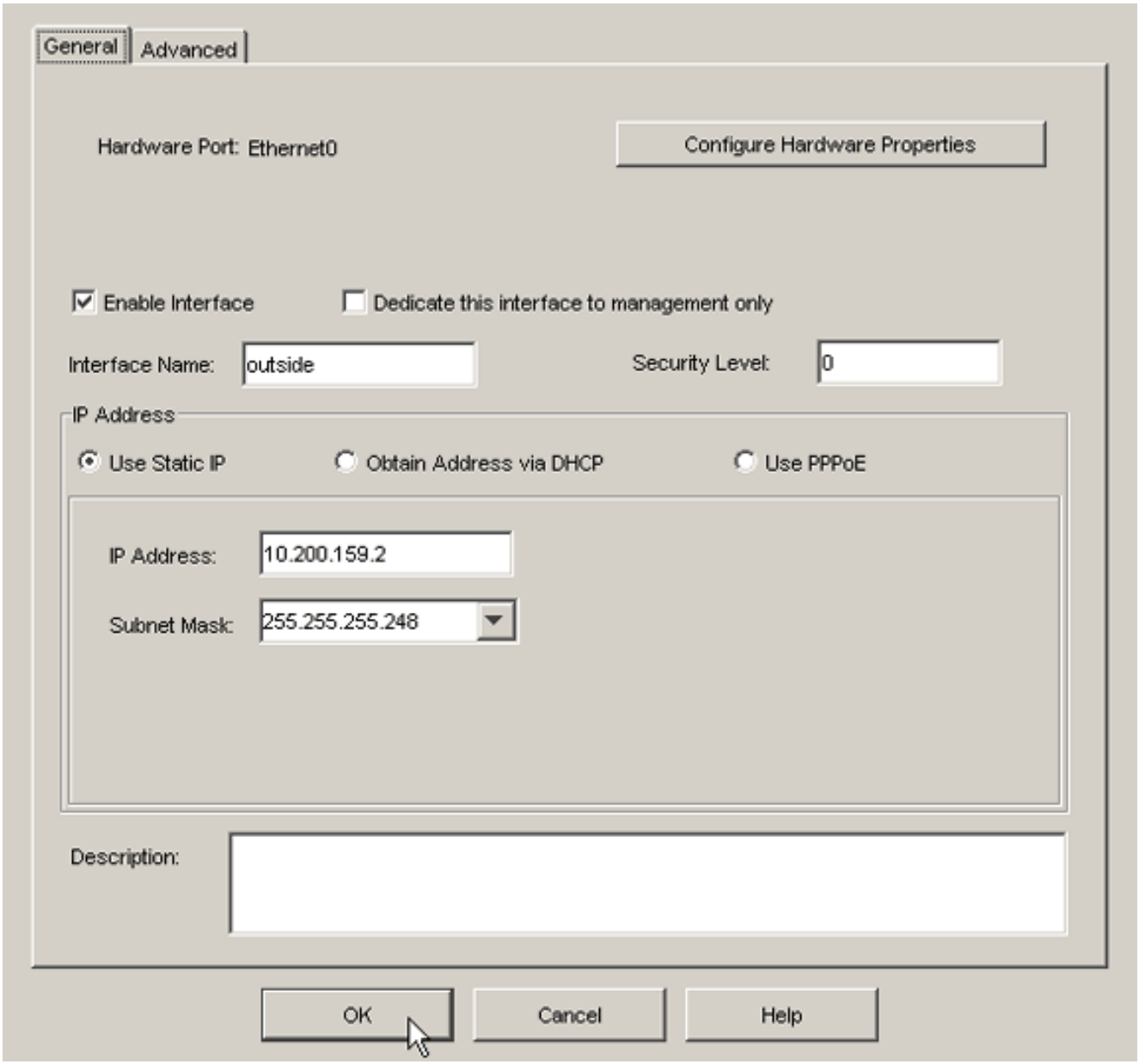
ASDM-Konfiguration

Gehen Sie wie folgt vor, um die redundante oder Backup-ISP-Unterstützung mit der ASDM-Anwendung zu konfigurieren:

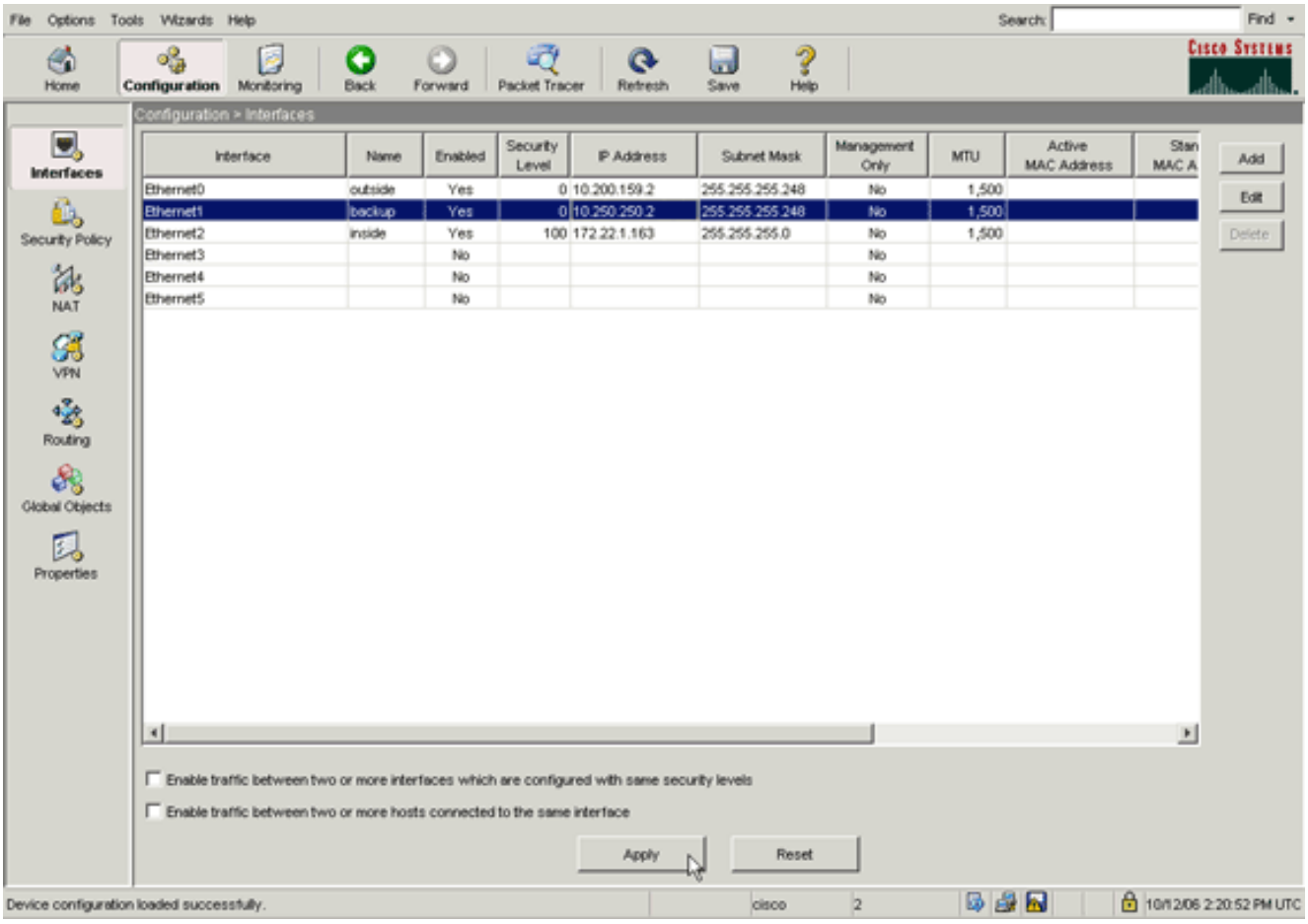
1. Klicken Sie in der ASDM-Anwendung auf **Konfiguration** und dann auf **Schnittstellen**.



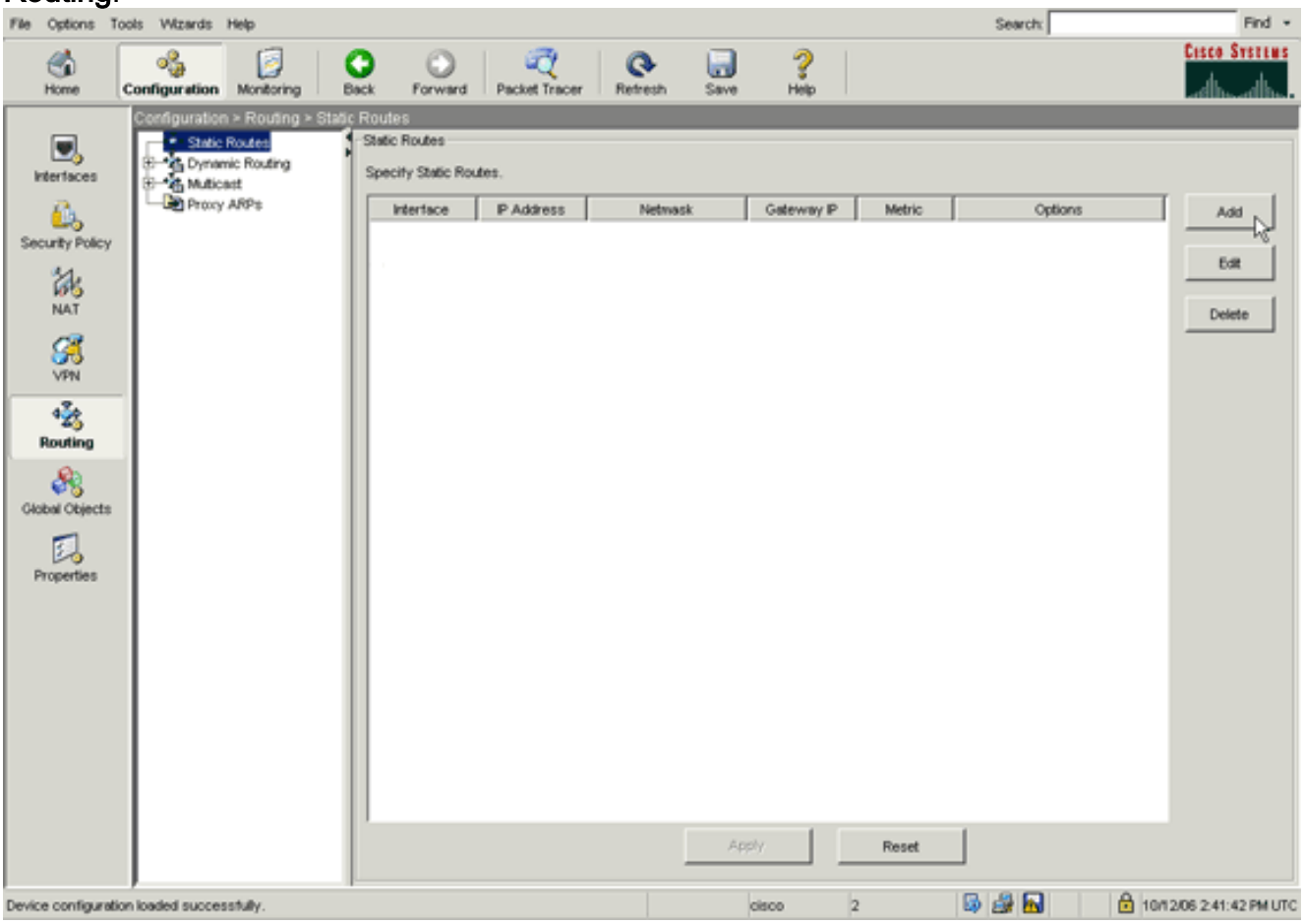
2. Wählen Sie in der Liste Schnittstellen die Option **Ethernet0 aus**, und klicken Sie dann auf **Bearbeiten**.Dieses Dialogfeld wird angezeigt.



3. Aktivieren Sie das Kontrollkästchen **Enable Interface** (Schnittstelle aktivieren), und geben Sie Werte in die Felder Interface Name (Schnittstellenname), Security Level (Sicherheitsstufe), IP Address (IP-Adresse) und Subnet Mask (Subnetzmaske) ein.
4. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.
5. Konfigurieren Sie ggf. andere Schnittstellen, und klicken Sie auf **Apply**, um die Konfiguration der Sicherheits-Appliance zu aktualisieren.

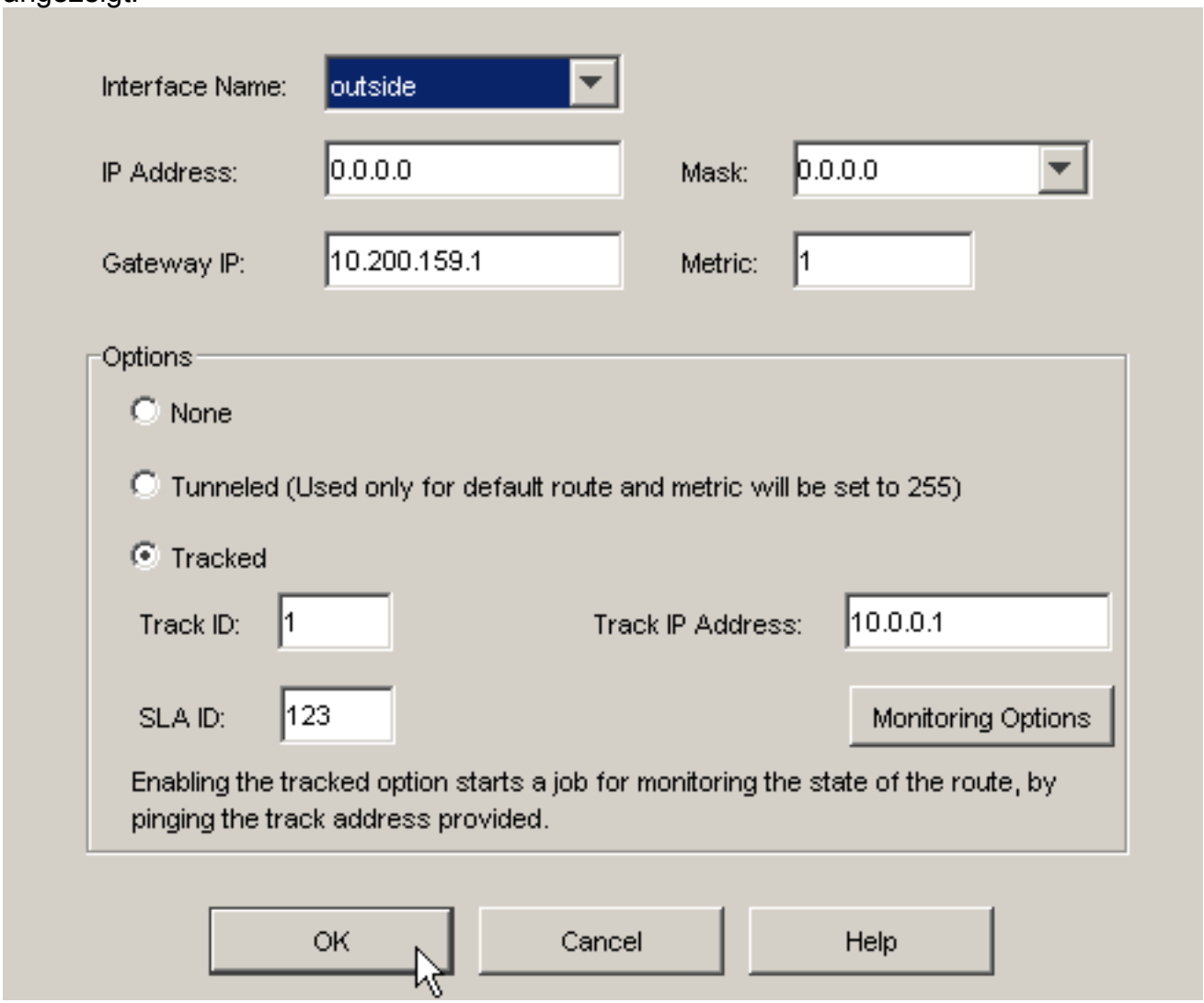


6. Klicken Sie links neben der ASDM-Anwendung auf **Routing**.

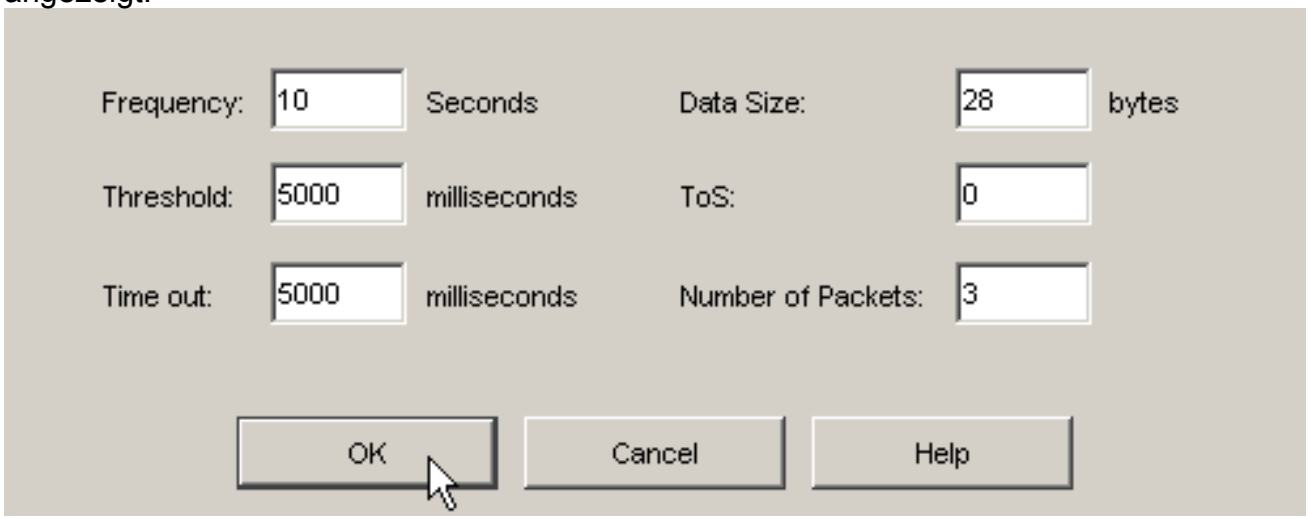


7. Klicken Sie auf **Hinzufügen**, um die neuen statischen Routen hinzuzufügen.Dieses Dialogfeld wird

angezeigt.



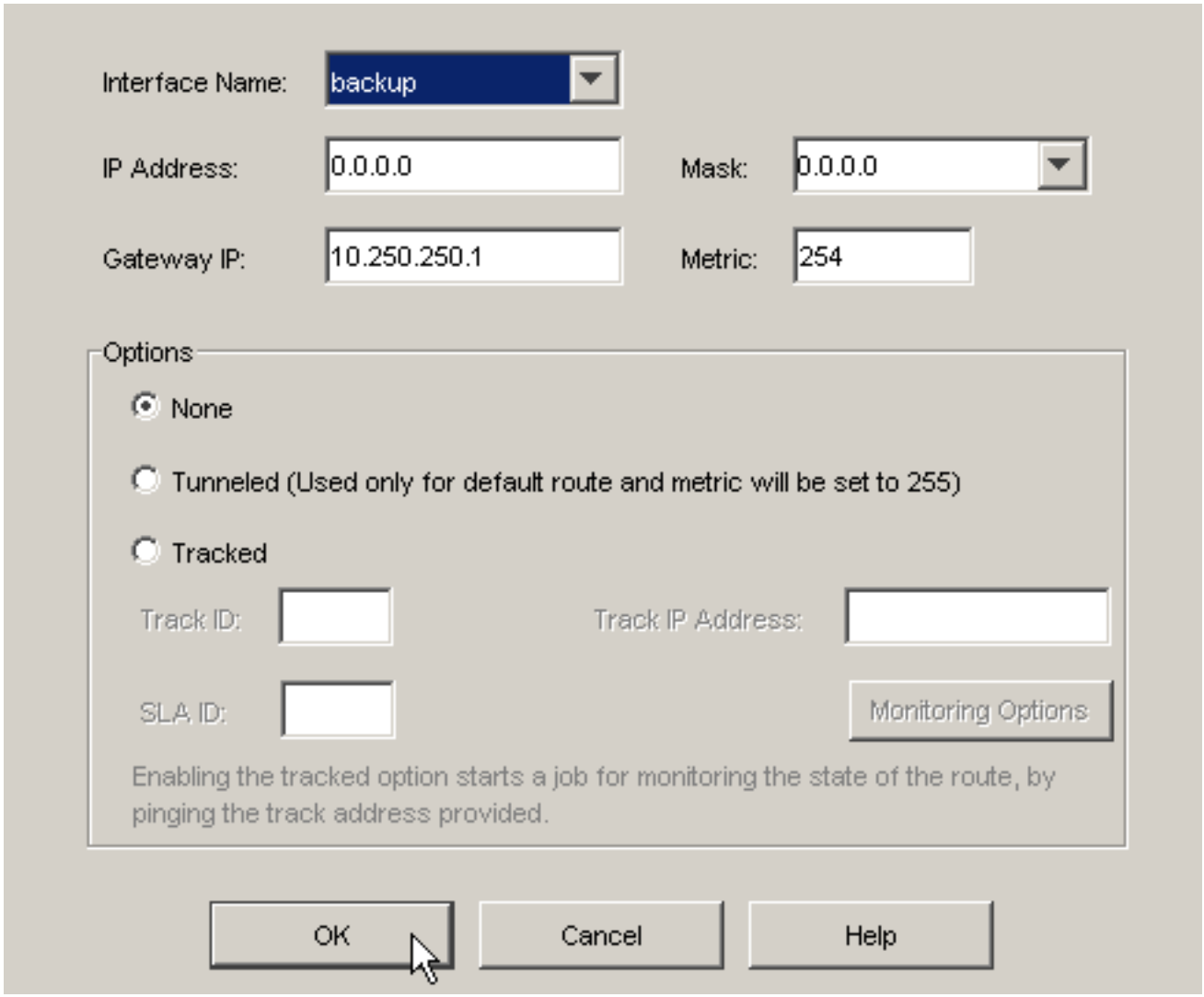
8. Wählen Sie in der Dropdown-Liste Interface Name (Schnittstellenname) die Schnittstelle aus, auf der die Route gespeichert ist, und konfigurieren Sie die Standardroute für die Verbindung zum Gateway. In diesem Beispiel ist 10.0.0.1 das primäre ISP-Gateway und das mit ICMP-Echos zu überwachende Objekt.
9. Klicken Sie im Bereich Options (Optionen) auf das Optionsfeld **Tracked (Verfolgung)**, und geben Sie Werte in die Felder Track-ID, SLA-ID und Track-IP-Adresse ein.
10. Klicken Sie auf **Überwachungsoptionen**.Dieses Dialogfeld wird angezeigt.



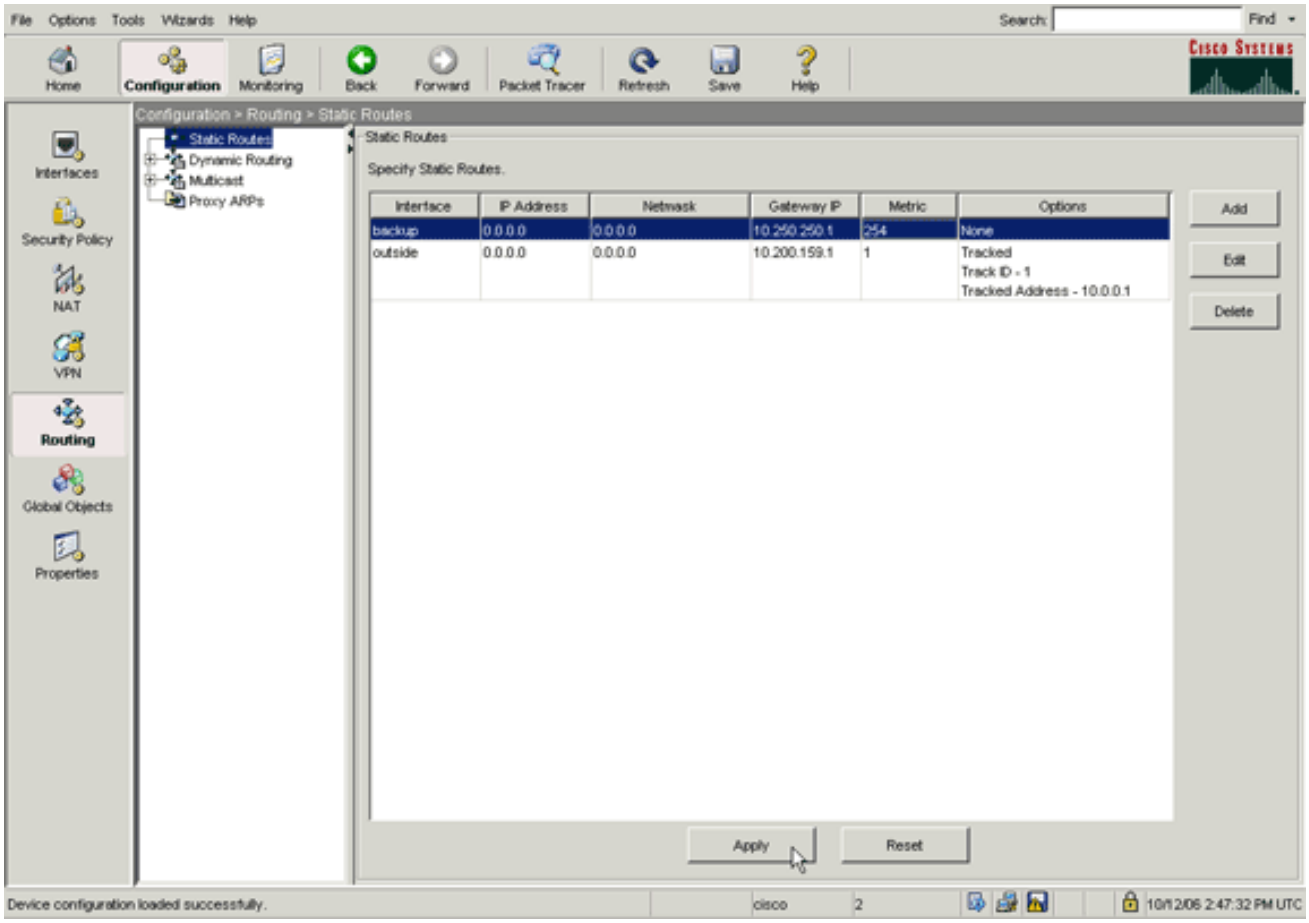
11. Geben Sie Werte für die Frequenz und andere Überwachungsoptionen ein, und klicken Sie

auf **OK**.

12. Fügen Sie eine weitere statische Route für den sekundären ISP hinzu, um eine Route zum Internet bereitzustellen.Um eine sekundäre Route zu erstellen, konfigurieren Sie diese Route mit einer höheren Metrik, z. B. 254. Wenn die primäre Route (primärer ISP) ausfällt, wird diese Route aus der Routing-Tabelle entfernt. Diese sekundäre Route (sekundärer ISP) wird stattdessen in der PIX-Routing-Tabelle installiert.
13. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.



Die Konfigurationen werden in der Liste Schnittstelle angezeigt.



14. Wählen Sie die Routing-Konfiguration aus, und klicken Sie auf **Apply**, um die Konfiguration der Sicherheits-Appliance zu aktualisieren.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Bestätigen Sie, dass die Konfiguration abgeschlossen ist.

Verwenden Sie diese **show**-Befehle, um zu überprüfen, ob die Konfiguration abgeschlossen ist.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show running-config sla monitor**: Zeigt die SLA-Befehle in der Konfiguration an.

```
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
```

- **show sla monitor configuration** (Konfiguration für **Einzelmonitor anzeigen**): Zeigt die aktuellen Konfigurationseinstellungen des Vorgangs an.

```
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:
```

- **show sla monitor Operational State (Betriebsstatus anzeigen)** - Zeigt die Betriebsstatistiken des SLA-Vorgangs an.Bevor der primäre ISP ausfällt, ist dies der Betriebsstatus:

```
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
```

  Wenn der primäre ISP ausfällt (und der ICMP die Zeitüberschreitung wiederholt), ist dies der Betriebsstatus:

```
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
```

Bestätigen Sie, dass die Backup-Route installiert ist (CLI-Methode).

Mit dem Befehl **show route** können Sie bestimmen, wann die Backup-Route installiert ist.

- Bevor der primäre ISP ausfällt, folgt die Routing-Tabelle:

```
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
```

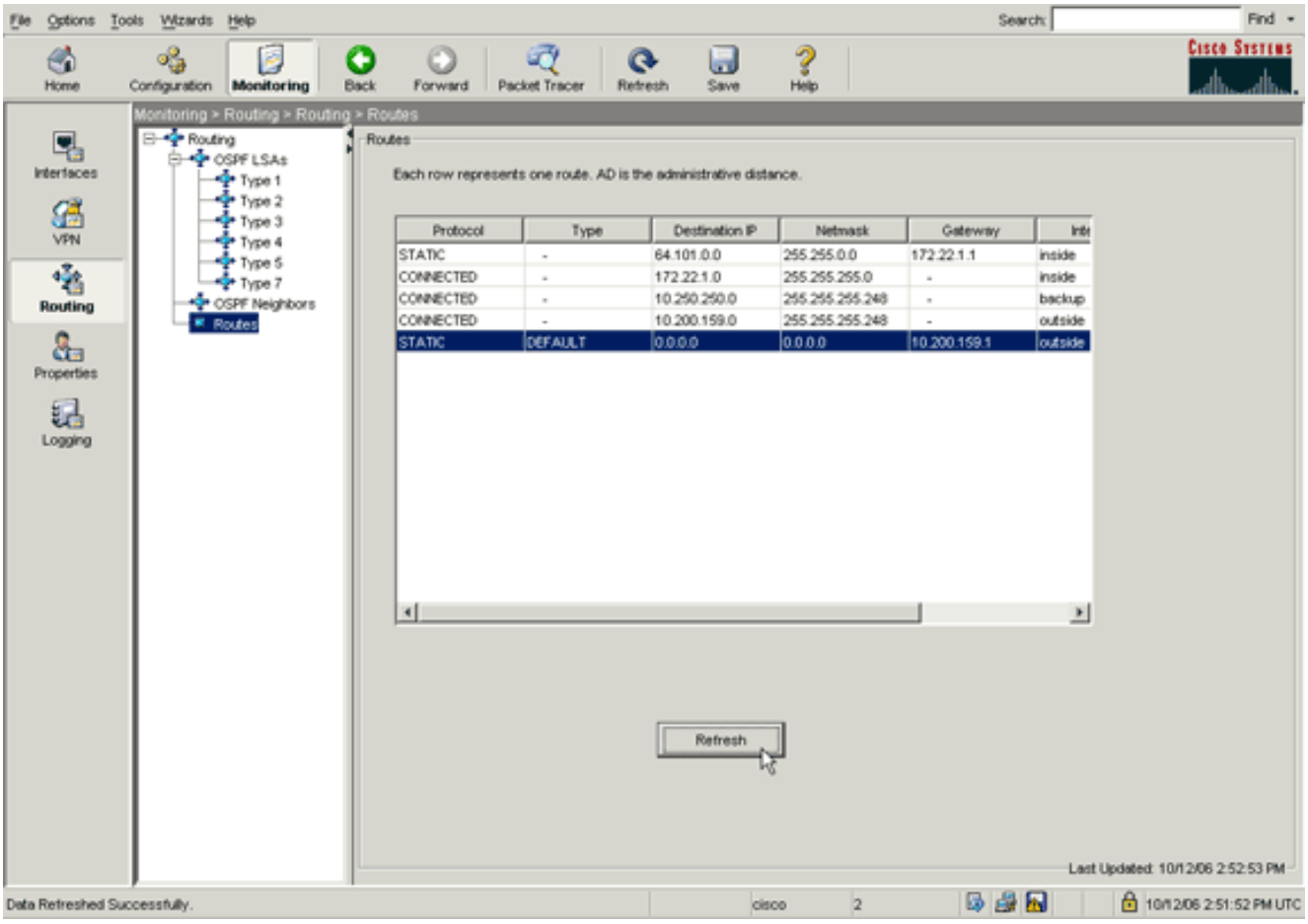
- Wenn der primäre ISP ausfällt, wird die statische Route entfernt und die Backup-Route installiert. Dies ist die Routing-Tabelle:

```
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
```

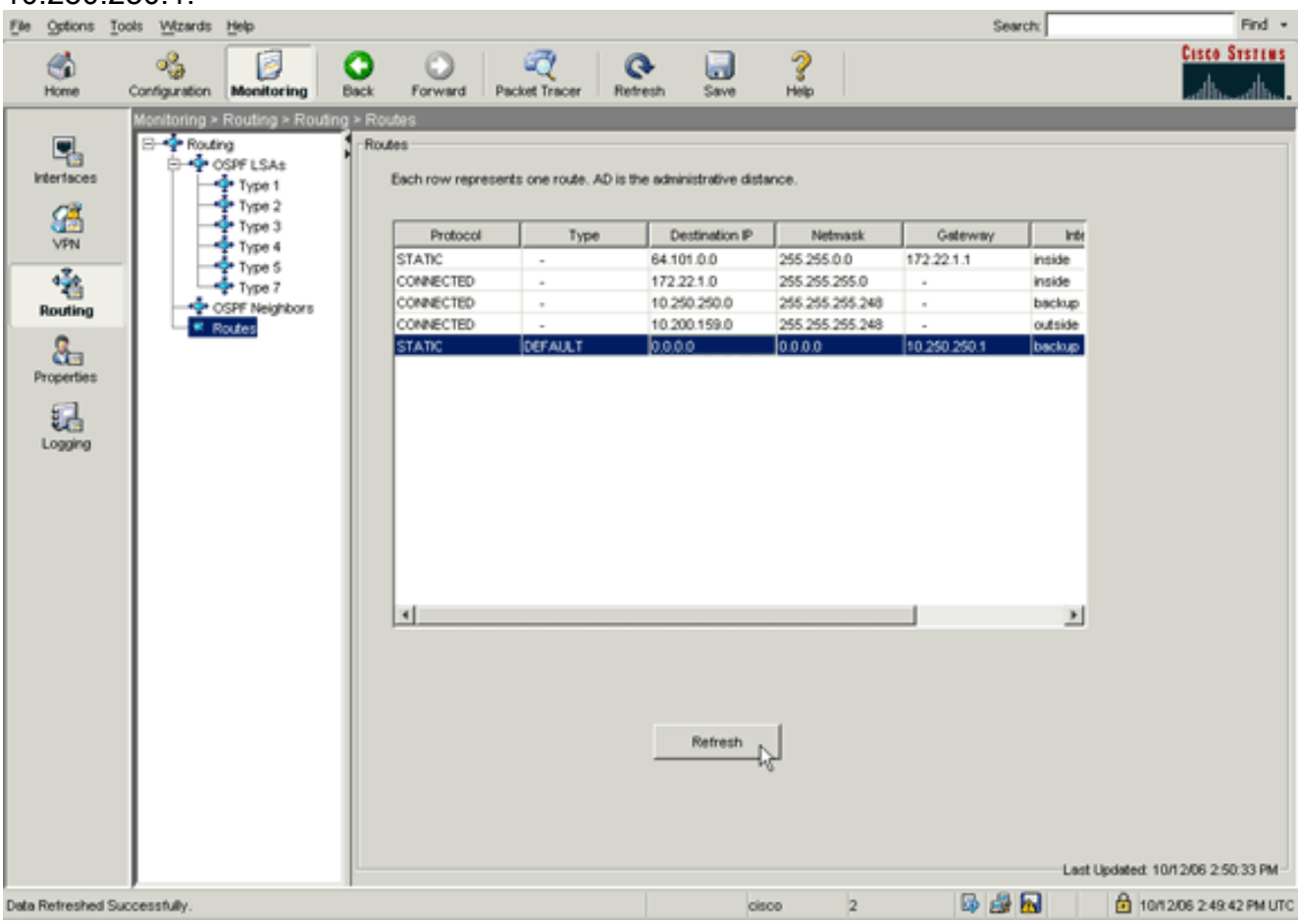
Bestätigen Sie, dass die Backup-Route installiert ist (ASDM-Methode).

Gehen Sie wie folgt vor, um gemeinsam mit dem ASDM zu überprüfen, ob die Backup-Route installiert ist:

1. Klicken Sie auf **Monitoring** und dann auf **Routing**.
2. Wählen Sie in der Routing-Struktur **Routen aus**.Bevor der primäre ISP ausfällt, folgt die Routing-
   Tabelle:



Die STANDARD-Route zeigt über die externe Schnittstelle auf 10.0.0.2.Wenn der primäre ISP ausfällt, wird die Route entfernt und die Backup-Route installiert. Die STANDARD-Route zeigt nun über die Sicherungsschnittstelle auf 10.250.250.1.



Fehlerbehebung

Debugbefehle

- **debug sla monitor trace**: Zeigt den Fortschritt des Echo-Vorgangs an.Das verfolgte Objekt (primäres ISP-Gateway) ist aktiv, und ICMP-Echos sind erfolgreich.

```
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
```

  Das verfolgte Objekt (primäres ISP-Gateway) ist ausgefallen, und ICMP-Echos schlagen fehl.

```
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 sla monitor error (SLA-Überwachungsfehler debug)**: Zeigt Fehler an, die beim SLA-Überwachungsprozess auftreten.Das verfolgte Objekt (primäres ISP-Gateway) ist aktiv, und ICMP ist erfolgreich.

```
%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
```

  Das verfolgte Objekt (primäres ISP-Gateway) ist ausgefallen, und die verfolgte Route wird entfernt.

```
%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.
```

Nachverfolgte Route wird unnötigerweise entfernt

Wenn die verfolgte Route unnötigerweise entfernt wird, stellen Sie sicher, dass das Überwachungsziel immer für den Empfang von Echoanfragen verfügbar ist. Stellen Sie außerdem sicher, dass der Zustand Ihres Überwachungsziels (d. h. ob das Ziel erreichbar ist oder nicht) eng mit dem Zustand der primären ISP-Verbindung verknüpft ist.

Wenn Sie ein Überwachungsziel auswählen, das weiter entfernt ist als das ISP-Gateway, schlägt möglicherweise eine andere Verbindung entlang dieser Route fehl, oder ein anderes Gerät kann sich stören. Diese Konfiguration kann dazu führen, dass der SLA-Monitor zu dem Schluss gelangt, dass die Verbindung zum primären ISP fehlgeschlagen ist, und dass die Sicherheits-Appliance unnötig zum sekundären ISP-Link übergeht.

Wenn Sie beispielsweise einen Zweigstellen-Router als Überwachungsziel auswählen, kann die ISP-Verbindung mit Ihrer Zweigstelle sowie eine andere Verbindung unterwegs fehlschlagen. Wenn die ICMP-Echos, die von der Überwachung gesendet werden, fehlschlagen, wird die primäre verfolgte Route entfernt, obwohl die primäre ISP-Verbindung noch aktiv ist.

In diesem Beispiel wird das primäre ISP-Gateway, das als Überwachungsziel verwendet wird, vom ISP verwaltet und befindet sich auf der anderen Seite der ISP-Verbindung. Diese Konfiguration stellt sicher, dass die ISP-Verbindung fast sicher ausfällt, wenn die ICMP-Echos, die von der Überwachung gesendet werden, ausfallen.

SLA-Überwachung auf ASA

Problem:

Die SLA-Überwachung funktioniert nicht, nachdem die ASA auf Version 8.0 aktualisiert wurde.

Lösung:

Das Problem ist möglicherweise auf den in der **OUTSIDE-**Schnittstelle konfigurierten Befehl **IP Reverse-Path** zurückzuführen. Entfernen Sie den Befehl in ASA, und versuchen Sie, die SLA-Überwachung zu überprüfen.

Zugehörige Informationen

- Konfigurieren der statischen Routen-Nachverfolgung
- Befehlsreferenz für PIX/ASA 7.2
- Cisco Security Appliances der Serie ASA 5500
- Cisco Security Appliances der Serie PIX 500
- Technischer Support und Dokumentation - Cisco Systems