Konfigurieren der ASA für redundante oder Backup-ISP-Links

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Cisco Adaptive Security Appliance (ASA) der Serie ASA 5500 für die Verwendung der statischen Route-Tracking-Funktion konfiguriert wird, damit das Gerät redundante oder Backup-Internetverbindungen verwenden kann.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

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

- Cisco Serie ASA 555-X mit Softwareversion 9.x oder höher
- Cisco ASDM Version 7.x 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 Serie ASA 5500 Version 9.1(5) verwenden.

> **Hinweis**: Der Befehl **backup interface** ist erforderlich, um die vierte Schnittstelle der Serie ASA 5505 zu konfigurieren. Weitere Informationen finden Sie im Abschnitt zur Backup-Schnittstelle der *Cisco Security Appliance Command Reference, Version 7.2*.

Hintergrundinformationen

Dieser Abschnitt bietet eine Übersicht über die in diesem Dokument beschriebene Funktion zur statischen Routenverfolgung sowie einige wichtige Empfehlungen, bevor Sie beginnen.

Übersicht über die Funktion für die statische Routenverfolgung

Ein Problem bei der Verwendung statischer Routen besteht darin, dass kein inhärenter Mechanismus vorhanden ist, der feststellen kann, 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. Diese Funktion entfernt die statische Route aus der Routing-Tabelle und ersetzt sie bei einem Ausfall durch eine Backup-Route.

Durch die statische Weiterleitung kann die ASA eine kostengünstige Verbindung zu einem sekundären ISP herstellen, falls die primäre Mietleitung nicht mehr verfügbar ist. Um diese Redundanz zu erreichen, ordnet die ASA eine statische Route einem von Ihnen definierten Überwachungsziel zu. Der Service Level Agreement (SLA)-Vorgang überwacht das Ziel mit periodischen ICMP-Echoanfragen. 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-Monitor 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.

In dem in diesem Dokument verwendeten Beispiel unterhält die ASA 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 Digital Subscriber Line (DSL) mit niedrigerer Geschwindigkeit, auf die über ein DSL-Modem zugegriffen wird, das vom sekundären ISP bereitgestellt wird.

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

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 ASA die Routing-Tabelle, um den Datenverkehr an die DSL-Verbindung weiterzuleiten. Um diese Redundanz zu erreichen, wird die statische Routenverfolgung verwendet.

Die ASA wird mit einer statischen Route konfiguriert, die den gesamten Internetdatenverkehr an den primären ISP weiterleitet. Der SLA-Überwachungsprozess überprüft alle zehn Sekunden, 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 ASA verfügbar bleibt. Wie in diesem Dokument beschrieben, eignet sich diese Konfiguration möglicherweise nicht für den eingehenden Zugriff auf Ressourcen hinter der ASA. Um nahtlose eingehende Verbindungen zu ermöglichen, sind erweiterte Netzwerkkenntnisse erforderlich. Diese Fähigkeiten werden in diesem Dokument nicht behandelt.

Wichtige Empfehlungen

Bevor Sie die in diesem Dokument beschriebene Konfiguration versuchen, müssen Sie ein Überwachungsziel auswählen, das auf ICMP-Echoanfragen (Internet Control Message Protocol) reagieren kann. Das Ziel kann ein beliebiges Netzwerkobjekt sein, das Sie auswählen. Es wird jedoch empfohlen, ein Ziel festzulegen, das eng mit der Internetdienstanbieter-Verbindung verknüpft ist. Hier einige mögliche Überwachungsziele:

- Die ISP-Gateway-Adresse
- Eine andere vom ISP verwaltete Adresse
- Ein Server in einem anderen Netzwerk, z. B. ein AAA-Server (Authentication, Authorization, and Accounting), mit dem die ASA 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 ASA voll betriebsbereit und konfiguriert ist, damit der Cisco Adaptive Security Device Manager (ASDM) Konfigurationsänderungen vornehmen kann.

> **Tipp**: Weitere Informationen zum Konfigurieren des Geräts durch das ASDM finden Sie im Abschnitt Konfigurieren von HTTPS-Zugriff für ASDM im *CLI Book 1: Konfigurationsleitfaden für die CLI der Cisco ASA-Serie für allgemeine Vorgänge, 9.1*.

Konfigurieren

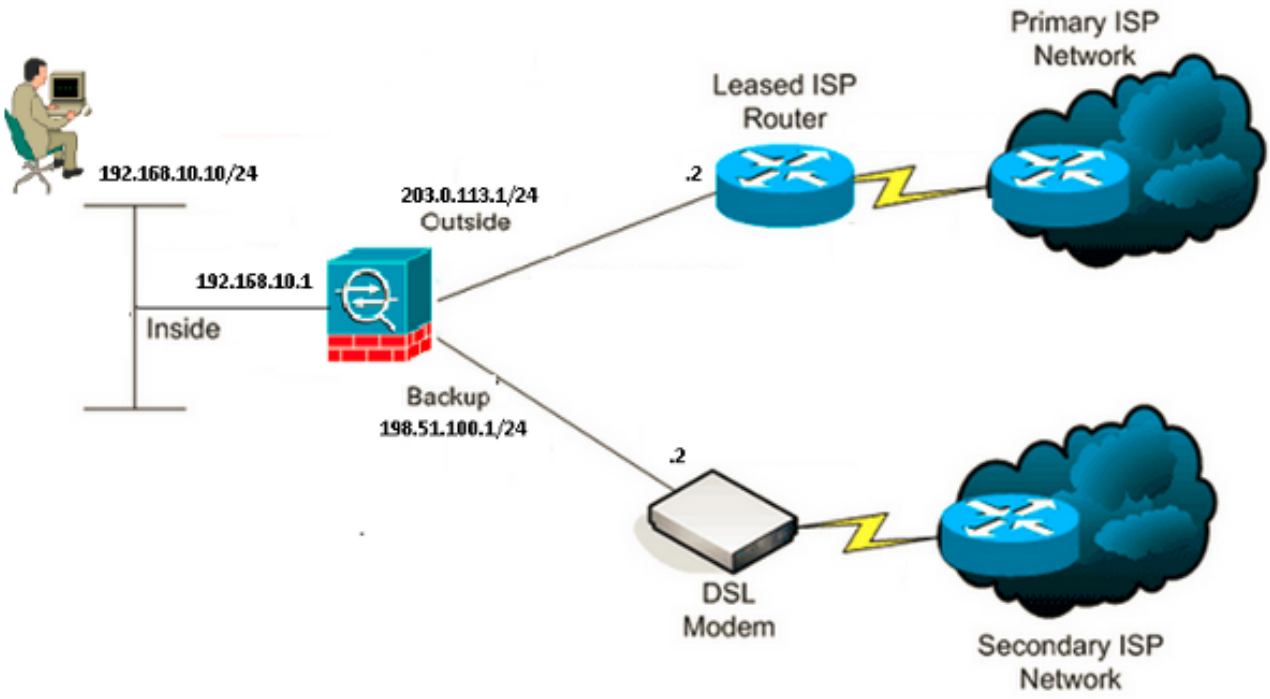
Verwenden Sie die in diesem Abschnitt beschriebenen Informationen, um die ASA für die Verwendung der Funktion zur statischen Routenverfolgung zu konfigurieren.

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen über die Befehle zu erhalten, die in diesem Abschnitt verwendet werden.

> **Hinweis**: Die in dieser Konfiguration verwendeten IP-Adressen sind im Internet nicht rechtlich routbar. Sie sind RFC 1918-Adressen, die in einer Laborumgebung verwendet werden.

Netzwerkdiagramm

Im Beispiel in diesem Abschnitt wird die folgende Netzwerkeinrichtung verwendet:



CLI-Konfiguration

Verwenden Sie diese Informationen, um die ASA über die CLI zu konfigurieren:

```
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
```

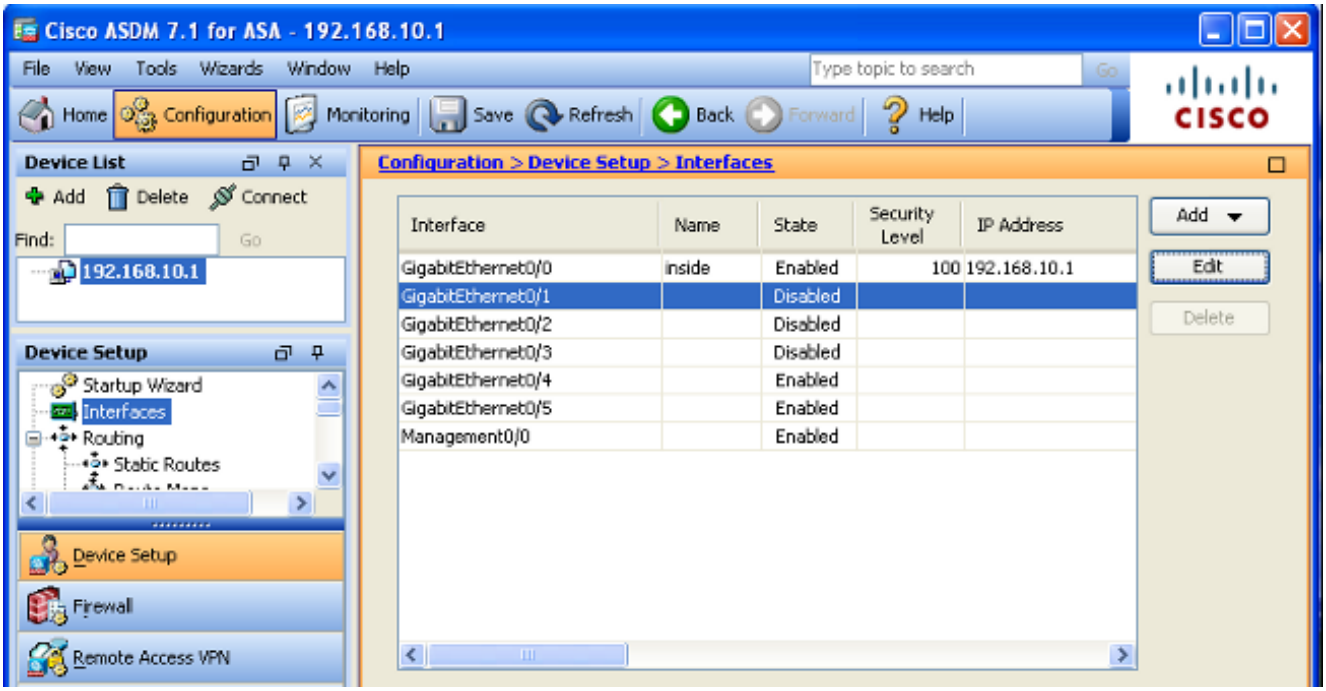
```
mtu outside 1500
mtu backup 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
object network Inside_Network
 nat (inside,outside) dynamic interface
object network inside_network
 nat (inside,backup) dynamic interface

!--- 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
```

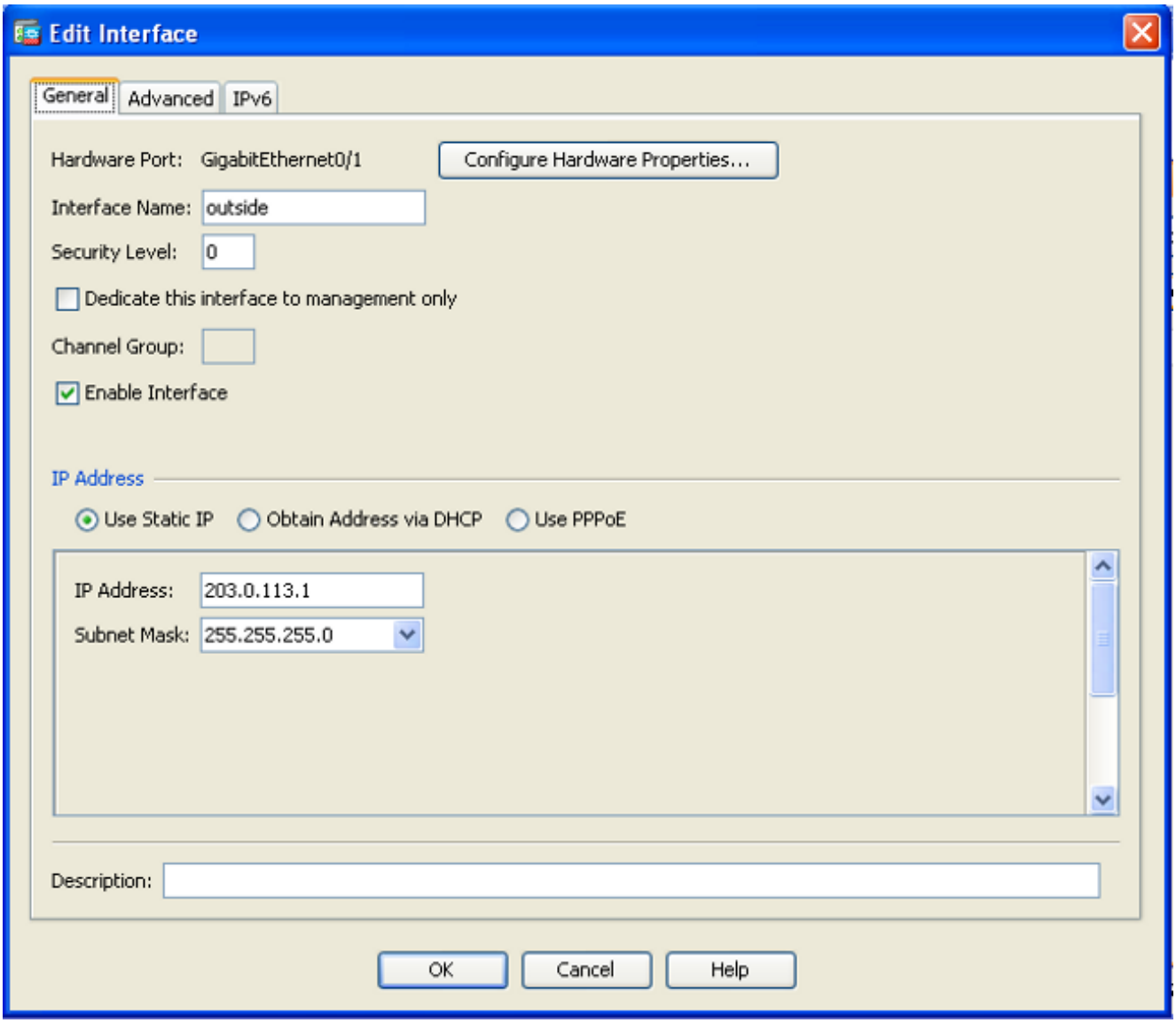
ASDM-Konfiguration

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

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



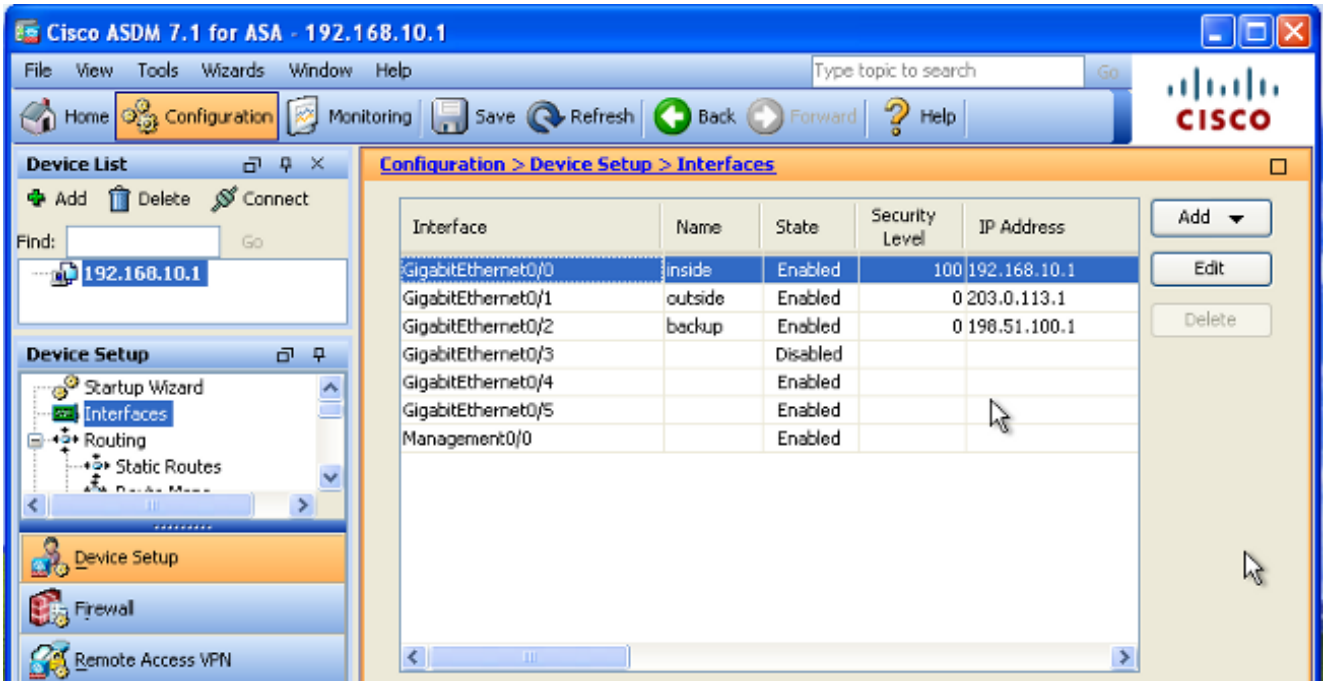
2. Wählen Sie **GigabitEthernet0/1** aus der Liste Schnittstellen aus, und klicken Sie dann auf **Bearbeiten**. Dieses Dialogfeld wird angezeigt:



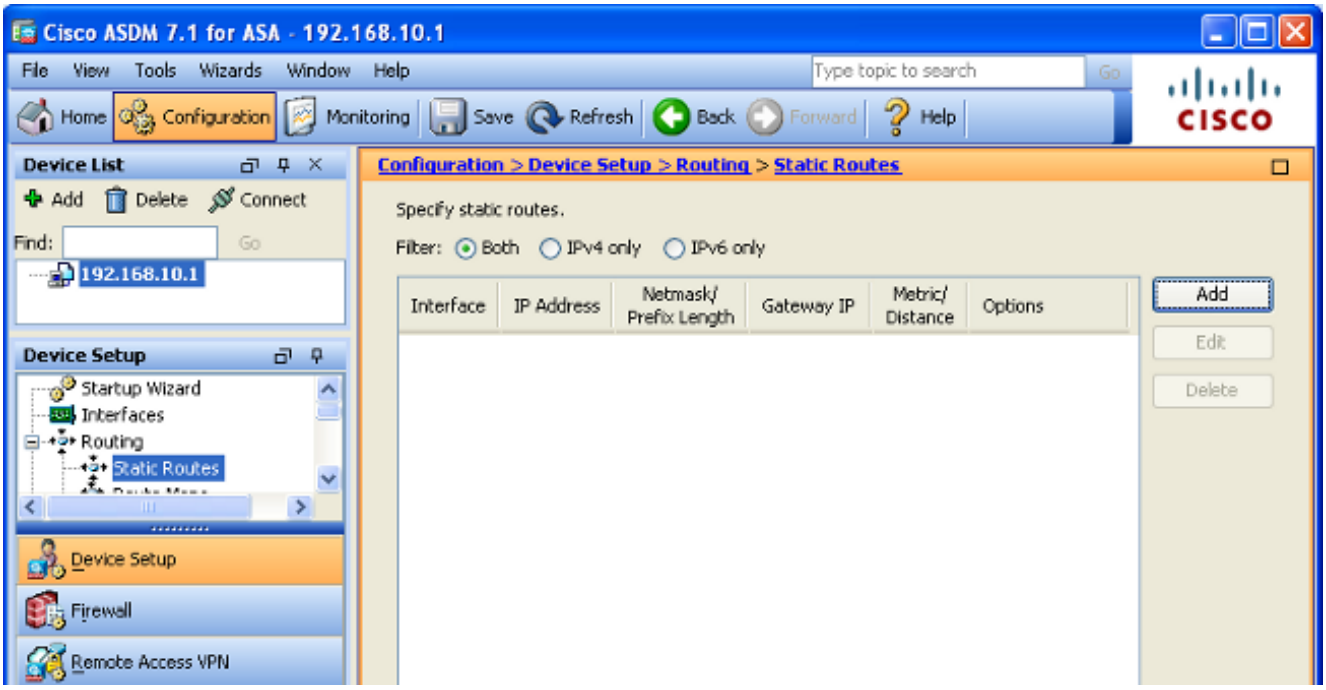
3. Aktivieren Sie das Kontrollkästchen **Enable Interface (Schnittstelle aktivieren)**, und geben Sie die entsprechenden Werte in den Feldern *Interface Name (Schnittstellenname)*, *Security Level (Sicherheitsstufe)*, *IP Address (IP-Adresse)* und *Subnet Mask (Subnetzmaske) ein.*

4. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

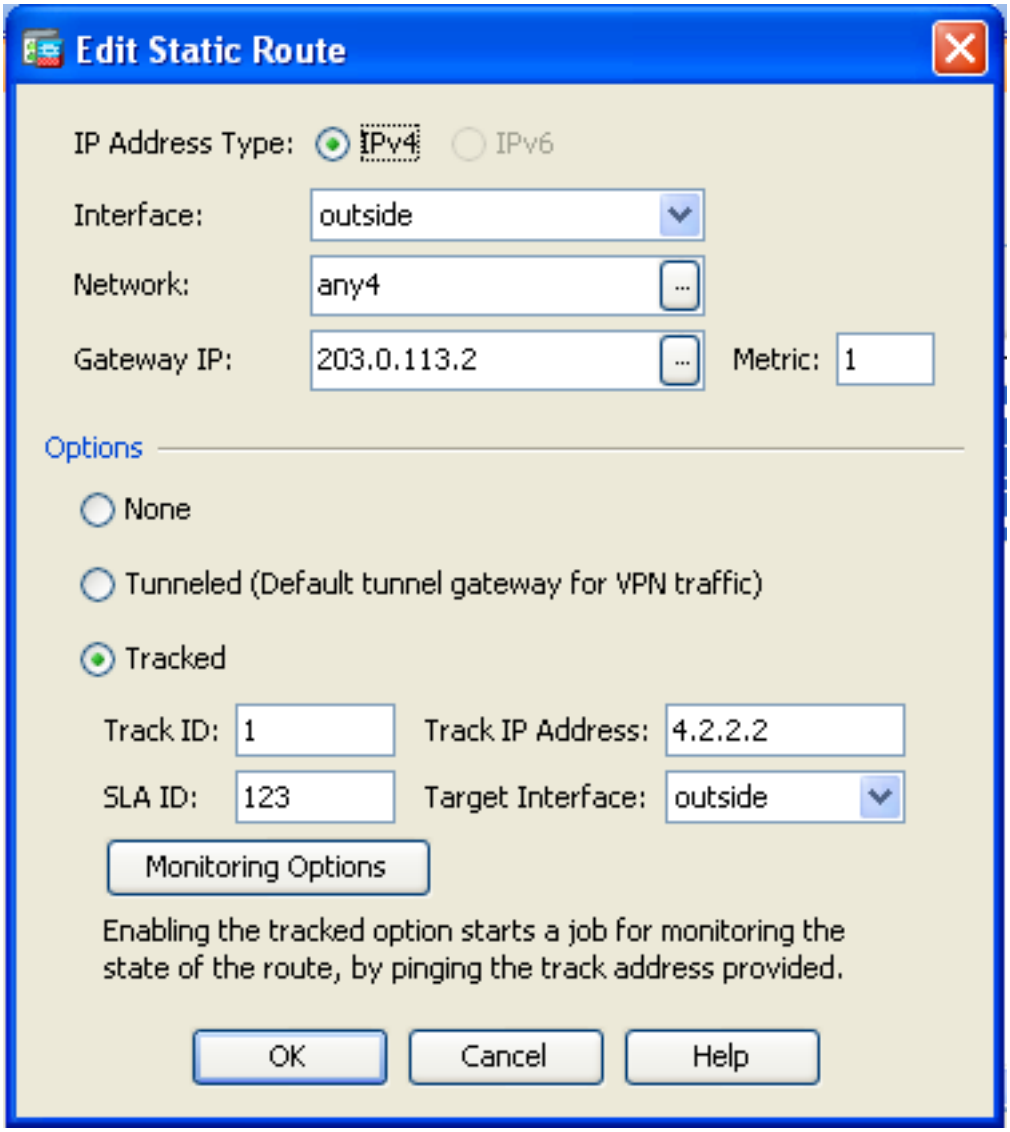
5. Konfigurieren Sie die anderen Schnittstellen nach Bedarf, und klicken Sie dann auf **Apply**, um die ASA-Konfiguration zu aktualisieren:



6. Wählen Sie **Routing** aus, und klicken Sie links neben der ASDM-Anwendung auf **Statische Routen**:



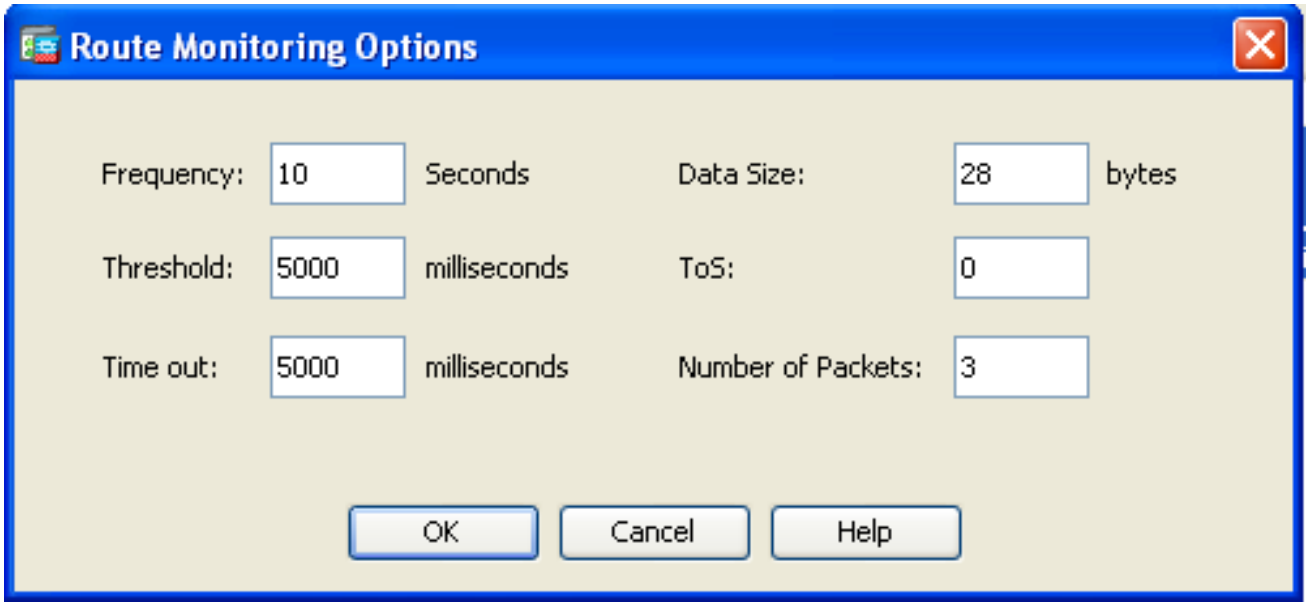
7. Klicken Sie auf **Hinzufügen**, um die neuen statischen Routen hinzuzufügen. Dieses Dialogfeld wird angezeigt:



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 **203.0.113.2** das primäre ISP-Gateway und **4.2.2.2** das zu überwachende Objekt mit ICMP-Echos.

9. Klicken Sie im Bereich Options (Optionen) auf das Optionsfeld **Tracked (Nachverfolgt)**, und geben Sie die entsprechenden Werte in die Felder *Track-ID*, *SLA-ID* und *Track-IP-Adresse ein*.

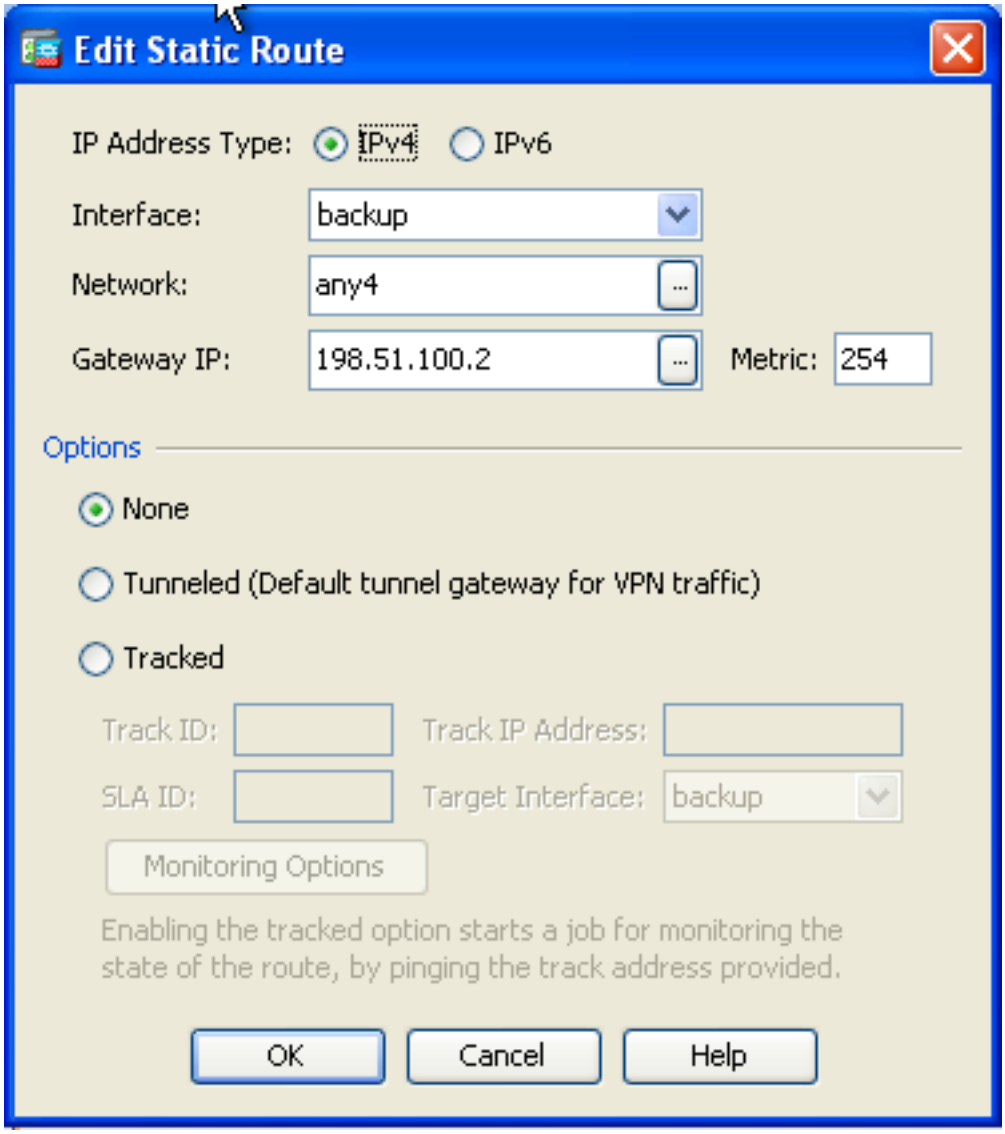
10. Klicken Sie auf **Überwachungsoptionen**. Dieses Dialogfeld wird angezeigt:



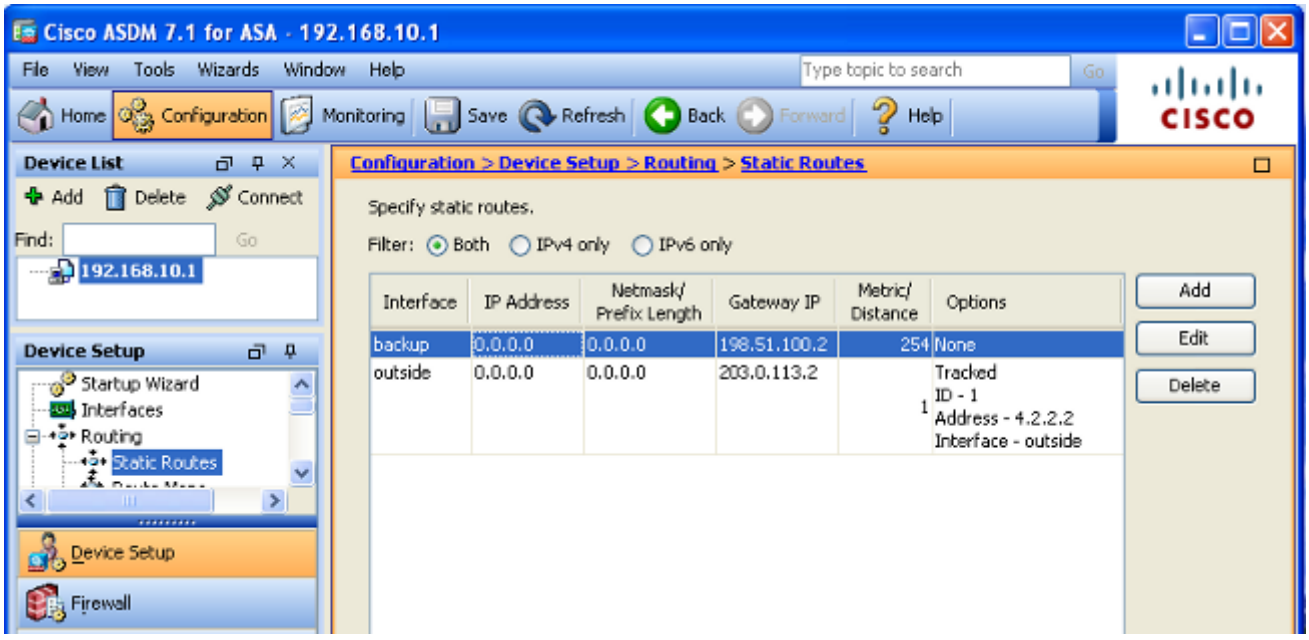
11. Geben Sie die entsprechenden Werte für die Frequenz und andere Überwachungsoptionen ein, und klicken Sie dann auf **OK**.

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 (Private Internet Exchange) installiert.

13. Klicken Sie auf **OK**, um das Dialogfeld zu schließen:



Die Konfigurationen werden in der Schnittstellenliste angezeigt:



14. Wählen Sie die Routing-Konfiguration aus, und klicken Sie dann auf **Apply** (Übernehmen), um die ASA-Konfiguration zu aktualisieren.

Überprüfen

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

Bestätigen Sie, dass die Konfiguration abgeschlossen ist.

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

Verwenden Sie die folgenden **show**-Befehle, um sicherzustellen, dass die Konfiguration abgeschlossen ist:

- **show running-config sla monitor** - In der Ausgabe dieses Befehls werden die SLA-Befehle in der Konfiguration angezeigt.

```
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
```

- **show sla monitor configuration** - In der Ausgabe dieses Befehls werden die aktuellen Konfigurationseinstellungen des Vorgangs angezeigt.

```
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:
```

- **show sla monitor Operational State** - Die Ausgabe dieses Befehls zeigt die Betriebsstatistiken des SLA-Vorgangs an.

  Bevor der primäre ISP ausfällt, ist dies der Betriebsstatus:

```
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
```

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

```
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
```

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

Geben Sie den Befehl **show route** ein, um zu bestätigen, dass die Backup-Route installiert ist.

Bevor der primäre ISP ausfällt, sieht die Routing-Tabelle ähnlich aus:

```
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
```

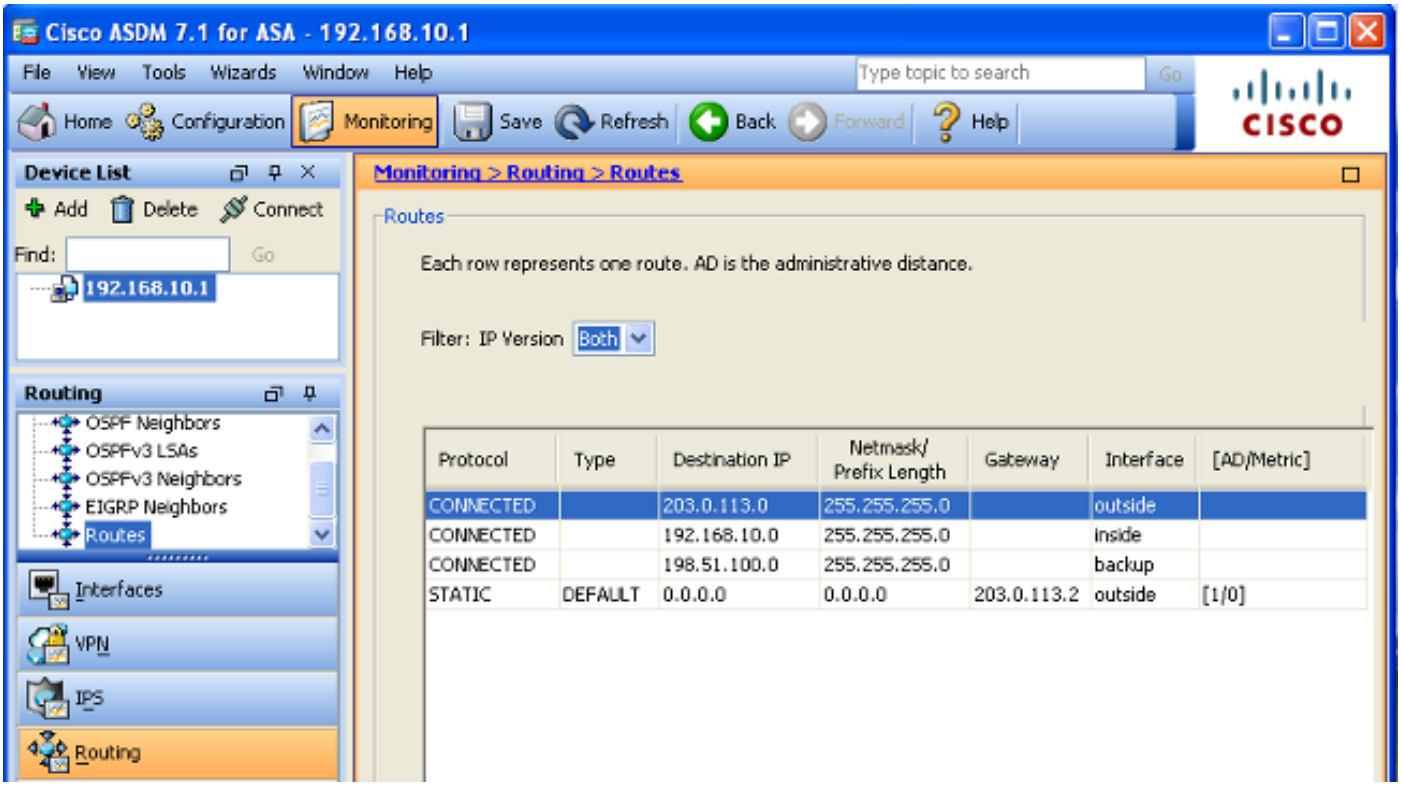
Wenn der primäre ISP ausfällt, wird die statische Route entfernt und die Backup-Route installiert. Die Routing-Tabelle sieht der folgenden ähnlich aus:

```
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
```

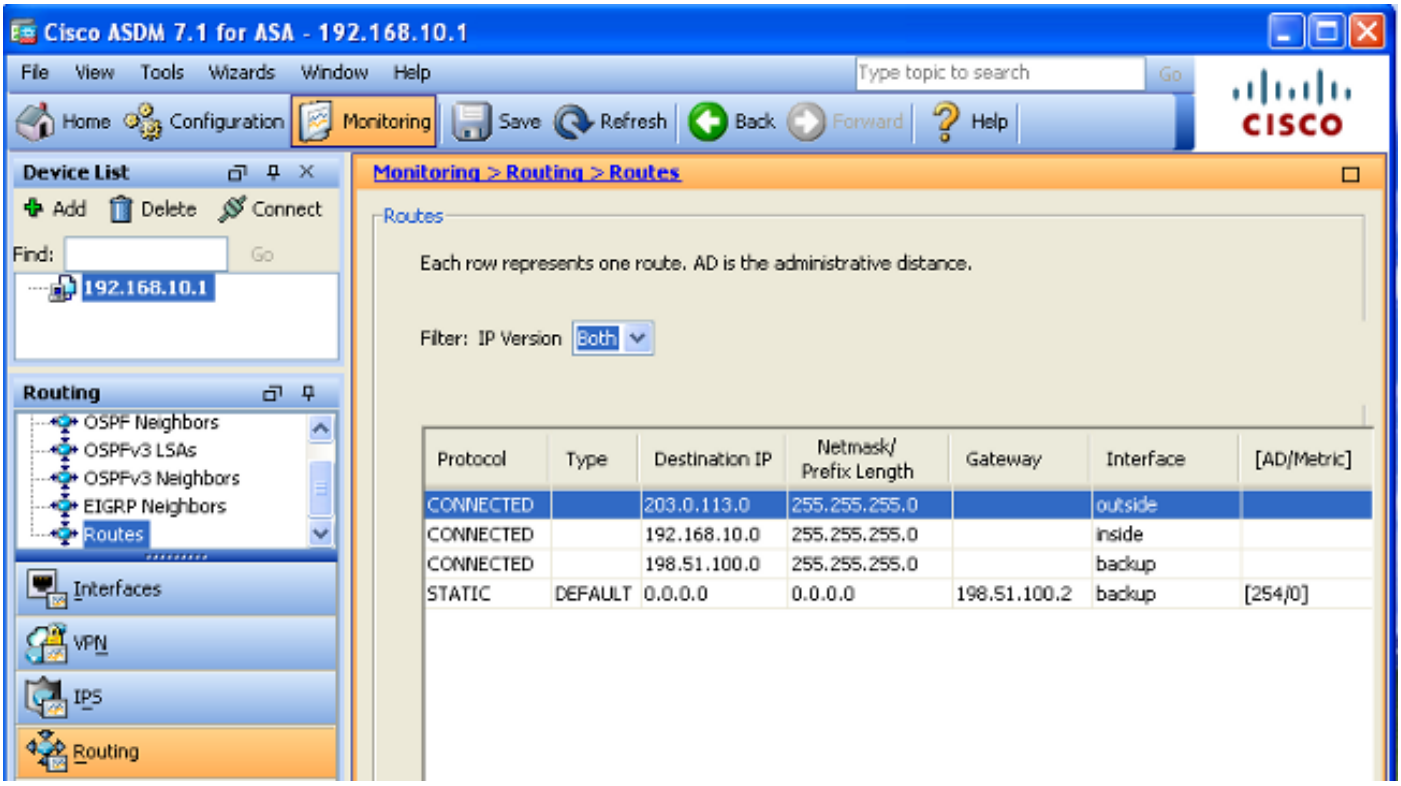
Bestätigen Sie, dass die Backup-Route installiert ist (ASDM-Methode).

Um zu bestätigen, dass die Backup-Route über das ASDM installiert wird, navigieren Sie zu **Monitoring > Routing**, und wählen Sie dann **Routen** aus der Routing-Struktur aus.

Bevor der primäre ISP ausfällt, erscheint die Routing-Tabelle ähnlich der im nächsten Image angezeigten. Beachten Sie, dass die **STANDARD-**Route über die **externe** Schnittstelle auf **203.0.113.2** verweist:



Wenn der primäre ISP ausfällt, wird die Route entfernt und die Backup-Route installiert. Die **STANDARD-**Route zeigt nun über die **Backup-**Schnittstelle auf **198.51.100.2**:



Fehlerbehebung

Dieser Abschnitt enthält einige nützliche Debugbefehle und beschreibt, wie ein Problem behoben wird, bei dem die verfolgte Route unnötigerweise entfernt wird.

Debugbefehle

Sie können diese Debugbefehle verwenden, um Konfigurationsprobleme zu beheben:

- **debug sla monitor trace** - In der Ausgabe dieses Befehls wird der Fortschritt des Echo-Vorgangs angezeigt.

  Wenn das verfolgte Objekt (primäres ISP-Gateway) aktiv ist und der ICMP-Echos erfolgreich ist, sieht die Ausgabe ähnlich aus wie folgt:

```
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
```

  Wenn das verfolgte Objekt (primäres ISP-Gateway) ausgefallen ist und die ICMP-Echos fehlschlagen, erscheint die Ausgabe ähnlich wie folgt:

```
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)** - In der Ausgabe dieses Befehls werden alle Fehler angezeigt, die beim SLA-Überwachungsprozess auftreten.

  Wenn das verfolgte Objekt (primäres ISP-Gateway) aktiv ist und der ICMP erfolgreich ist, wird die Ausgabe ähnlich wie folgt angezeigt:

```
%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
```

  Wenn das verfolgte Objekt (primäres ISP-Gateway) ausgefallen ist und die verfolgte Route entfernt wird, wird die Ausgabe ähnlich wie folgt angezeigt:

```
%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.
```

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, kann eine andere Verbindung entlang dieser Route fehlschlagen oder ein anderes Gerät 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 ASA 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, fehlschlagen.

Zugehörige Informationen

- Cisco Firewalls der nächsten Generation der Serie ASA 5500-X
- Technischer Support und Dokumentation - Cisco Systems