Configuración de ASA para links ISP redundantes o de respaldo

Contenido

Introducción

Este documento describe cómo configurar la función de seguimiento de ruta estática de Cisco ASA serie 5500 para utilizar conexiones redundantes o de respaldo de Internet.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ASA serie 5555-X que ejecuta la versión de software 9.x o posterior
- Cisco ASDM versión 7.x o posterior

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Productos Relacionados

También puede utilizar esta configuración con Cisco ASA serie 5500 versión 9.1(5).

> **Nota**: se requiere el comando **backup interface** para configurar la cuarta interfaz en la serie ASA 5505. Consulte la sección interfaz de respaldo de la *Referencia de Comandos de Dispositivos de Seguridad de Cisco, Versión 7.2* para obtener más información.

Antecedentes

Esta sección proporciona una descripción general de la función de seguimiento de rutas estáticas que se describe en este documento, así como algunas recomendaciones importantes antes de comenzar.

Descripción General de la Función Static Route Tracking

Un problema con el uso de rutas estáticas es que no existe ningún mecanismo inherente que pueda determinar si la ruta está activa o no.

La ruta permanece en la tabla de ruteo incluso si el gateway de salto siguiente deja de estar disponible.

Las rutas estáticas se quitan de la tabla de ruteo solamente si la interfaz asociada en el dispositivo de seguridad deja de funcionar.

Para resolver este problema, se utiliza una función de seguimiento de ruta estática para realizar un seguimiento de la disponibilidad de una ruta estática.

La función quita la ruta estática de la tabla de ruteo y la reemplaza con una ruta de respaldo en caso de falla.

El seguimiento de ruta estática permite que ASA utilice una conexión económica con un ISP secundario en el caso de que la línea arrendada principal deje de estar disponible.

Para lograr esta redundancia, ASA asocia una ruta estática con un destino de monitoreo que usted define.

La operación del acuerdo de nivel de servicio (SLA) supervisa el destino con solicitudes de eco ICMP periódicas.

Si no se recibe una respuesta de eco, el objeto se considera desactivado y la ruta asociada se elimina de la tabla de routing.

Una ruta de respaldo previamente configurada se utiliza en lugar de la ruta que se quita.

Mientras la ruta de respaldo está en uso, la operación de monitoreo de SLA continúa con sus intentos de alcanzar el destino de monitoreo.

Una vez que el objetivo esté disponible otra vez, la primera ruta se substituye en la tabla de ruteo, y se quita la ruta de respaldo.

En el ejemplo que se utiliza en este documento, ASA mantiene dos conexiones a Internet.

La primera conexión es una línea arrendada de alta velocidad a la que se accede con un router proporcionado por el ISP primario.

La segunda conexión es una línea de suscriptor digital (DSL) de menor velocidad a la que se accede a través

de un módem DSL proporcionado por el ISP secundario.

> **Nota**: La configuración que se describe en este documento no se puede utilizar para el balanceo de carga o el uso compartido de carga, ya que no es compatible con ASA. Use esta configuración para la redundancia o para realizar un un respaldo solamente. El tráfico saliente utiliza el ISP primario y, a continuación, el secundario si falla el primario. El incidente del ISP primario causa una interrupción temporal del tráfico.

La conexión DSL permanece inactiva mientras la línea arrendada está activa y el gateway del ISP primario es accesible.

Sin embargo, si la conexión con el ISP primario deja de funcionar, el ASA cambia la tabla de ruteo para dirigir el tráfico a la conexión DSL.

El seguimiento de ruta estática se utiliza para lograr esta redundancia.

El ASA se configura con una ruta estática que dirige todo el tráfico de Internet al ISP primario.

Cada diez segundos, el proceso de monitoreo de SLA verifica para confirmar que el gateway ISP primario es alcanzable.

Si el proceso de monitoreo SLA determina que el gateway del ISP primario no es accesible, la ruta estática que dirige tráfico a esa interfaz se quita de la tabla de ruteo.

Para substituir que la ruta estática, una ruta estática alterna que dirige el tráfico al ISP secundario está instalada.

Esta ruta estática dirige el tráfico al ISP secundario a través del módem DLS hasta que la conexión al ISP primario sea accesible.

Esta configuración proporciona una forma relativamente económica de garantizar que el acceso saliente a Internet siga estando disponible para los usuarios detrás del ASA.

Como se describe en este documento, esta configuración no siempre es adecuada para el acceso entrante a los recursos detrás del ASA. Se requieren conocimientos avanzados de redes para lograr conexiones entrantes sin problemas.

Estas habilidades no se abordan en este documento.

Recomendaciones importantes

Antes de intentar la configuración que se describe en este documento, debe elegir un destino de supervisión que pueda responder a las solicitudes de eco ICMP (Internet Control Message Protocol, Protocolo de mensajes de control de Internet).

El destino puede ser cualquier objeto de red que elija, pero se recomienda un destino estrechamente vinculado a la conexión del proveedor de servicios de Internet (ISP).

Estos son algunos de los posibles objetivos de supervisión:

- La dirección del gateway ISP
- Otra dirección administrada por ISP
- Un servidor en otra red, como un servidor de Autenticación, Autorización y Contabilización (AAA) con el cual el ASA debe comunicarse

- Un objeto de red persistente en otra red (un equipo de escritorio o portátil que puede apagar por la noche no es una buena opción)

Este documento asume que ASA está completamente operativo y configurado para permitir que el Cisco Adaptive Security Device Manager (ASDM) realice cambios de configuración.

> **Sugerencia**: para obtener información sobre cómo permitir que el ASDM configure el dispositivo, refiérase a la sección Configuración del Acceso HTTPS para ASDM del *Manual de Configuración CLI Book 1: Cisco ASA Series General Operations, 9.1*.

Configurar

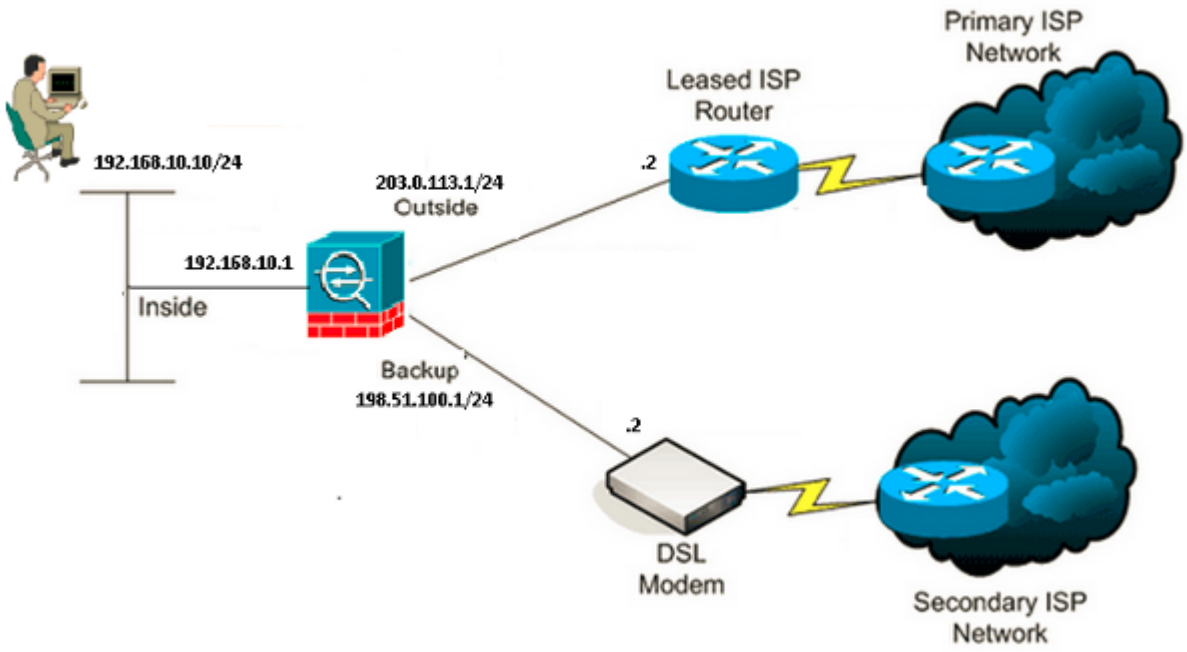
Utilice la información que se describe en esta sección para configurar el ASA para el uso de la función de seguimiento de ruta estática.

> **Nota**: Utilice la Command Lookup Tool (registered customers solamente) para obtener más información sobre los comandos que se utilizan en esta sección.

> **Nota**: Las direcciones IP que se utilizan en esta configuración no son legalmente enrutables en Internet. Son direcciones RFC 1918 , que se utilizan en un entorno de laboratorio.

Diagrama de la red

El ejemplo que se proporciona en esta sección utiliza esta configuración de red:



Configuración de CLI

Utilice esta información para configurar el ASA a través de la CLI :

<#root>

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.
```

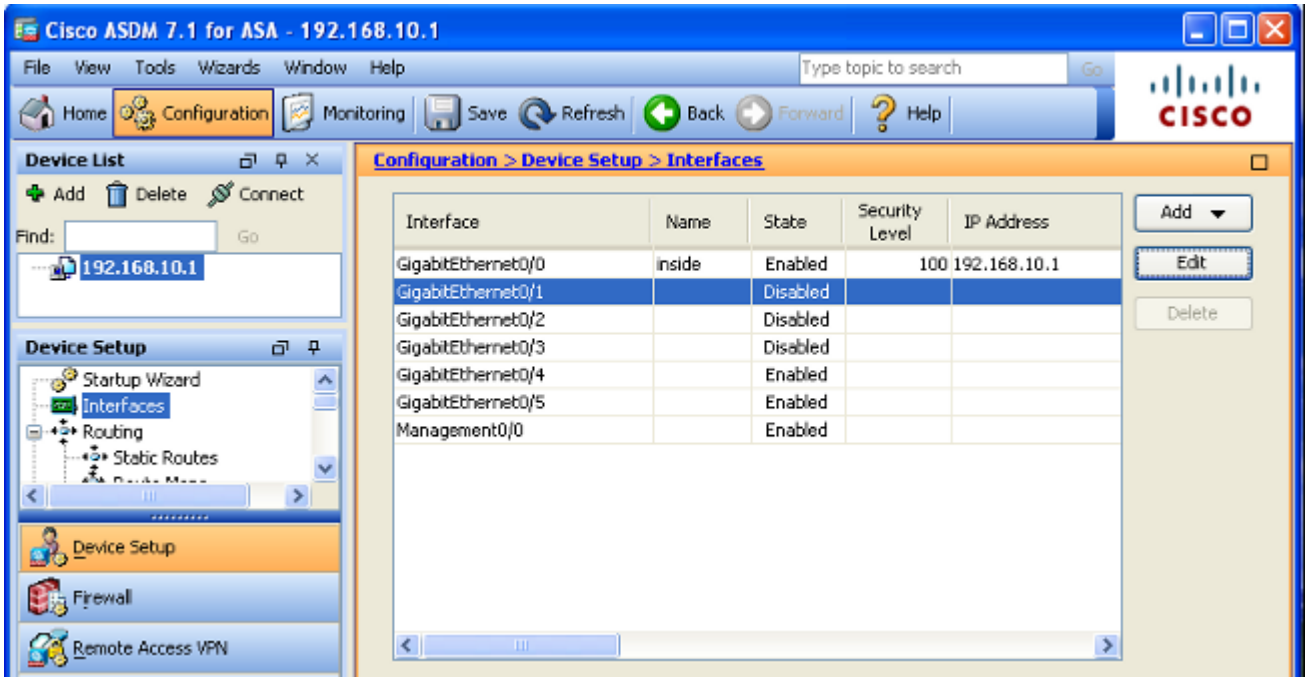
```
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 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
```

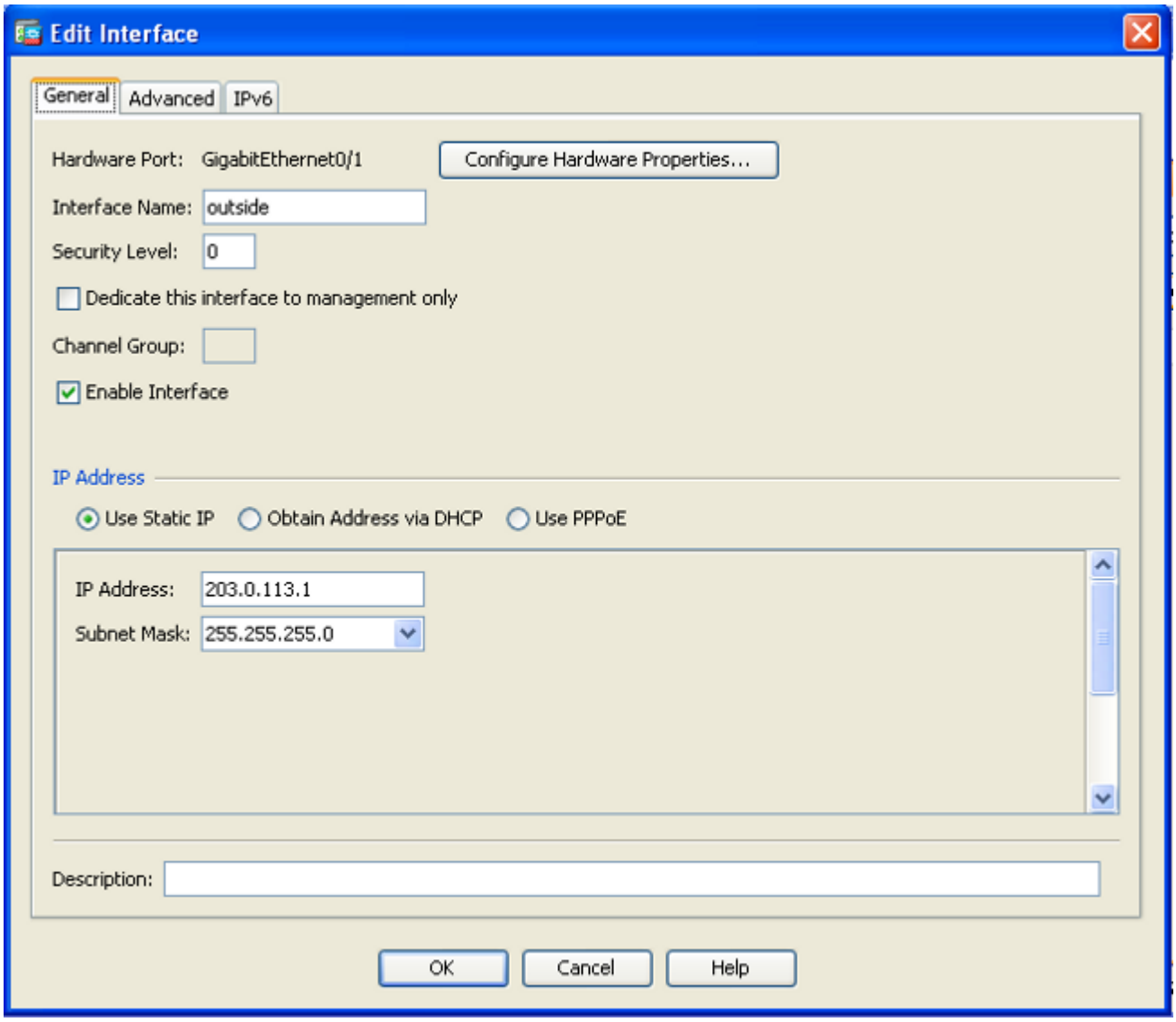
Configuración de ASDM

Complete estos pasos para configurar el soporte ISP redundante o de respaldo con la aplicación ASDM:

1. Dentro de la aplicación ASDM, haga clic en **Configuration**, y luego haga clic en **Interfaces**.



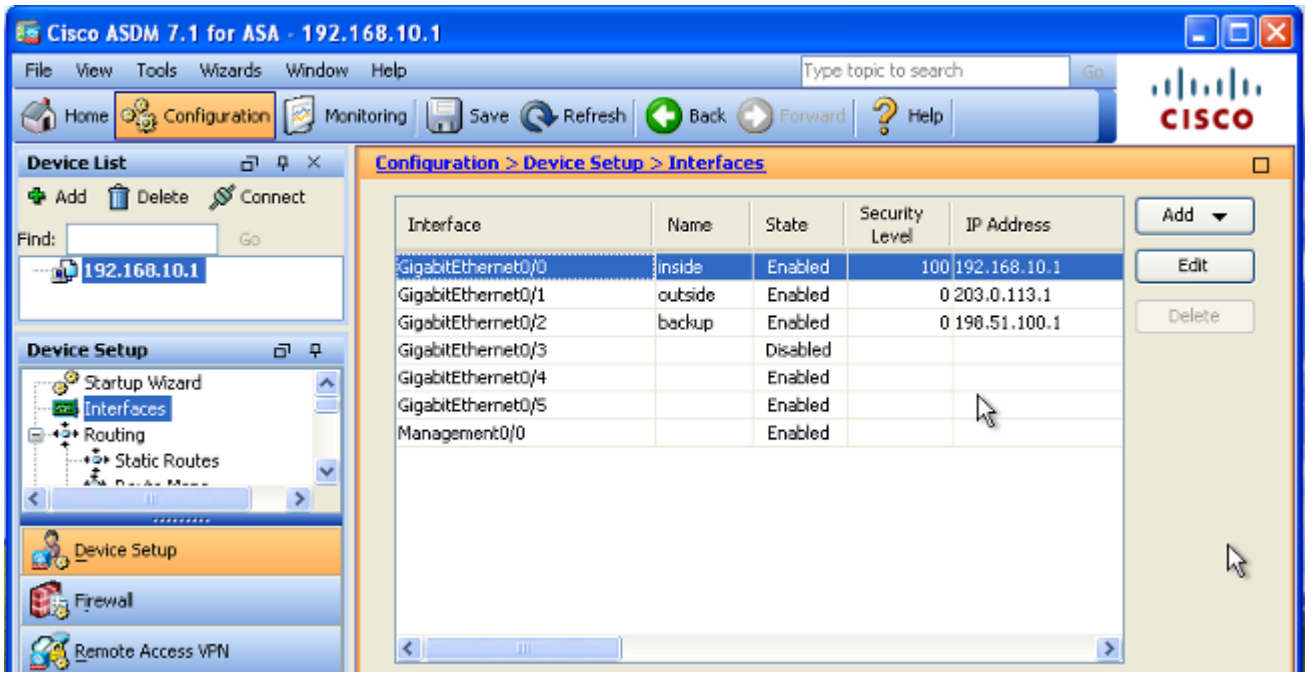
2. Seleccione **GigabitEthernet0/1** en la lista Interfaces y, a continuación, haga clic en **Edit**. Este cuadro de diálogo aparece:



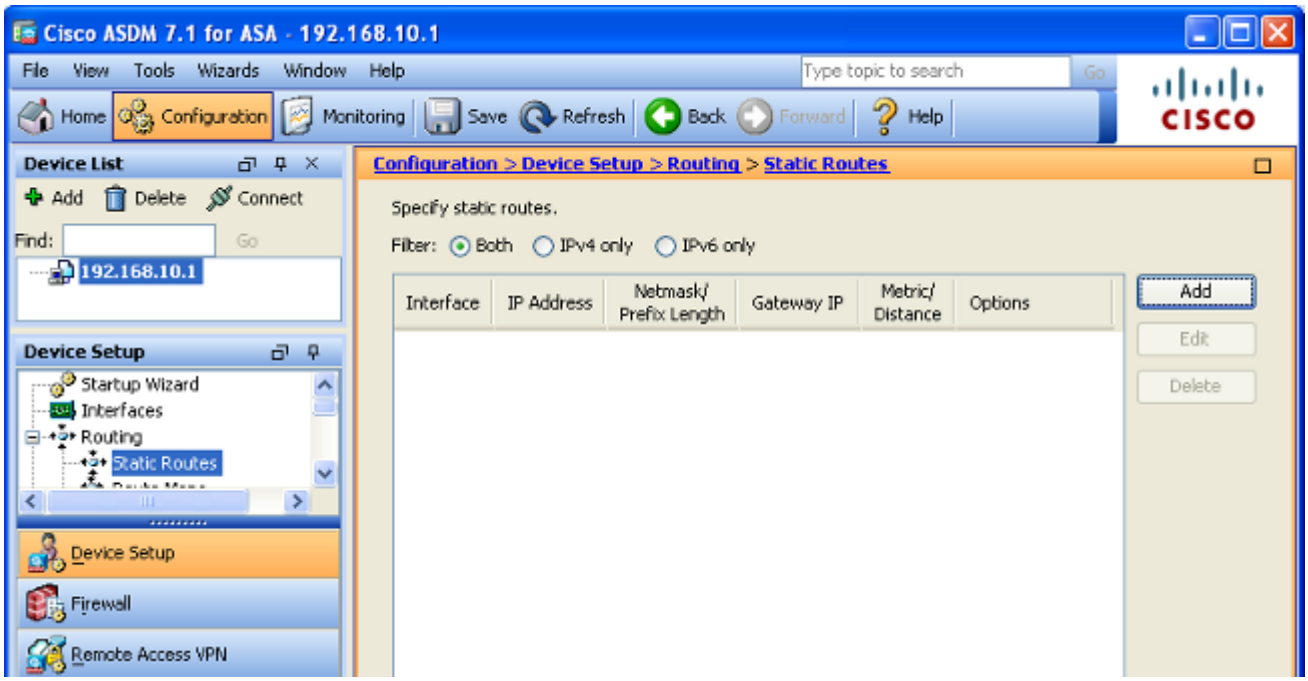
3. Marque la casilla de verificación Enable Interface e introduzca los valores adecuados en los campos *Interface Name*, *Security Level*, IP Address y *Subnet Mask.*

4. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.

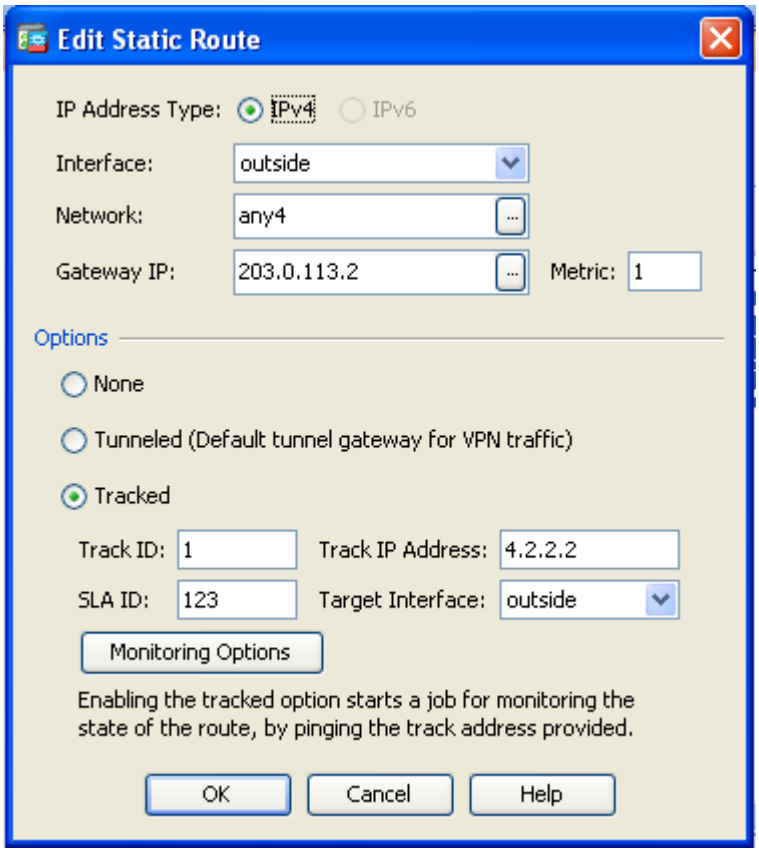
5. Configure las otras interfaces según sea necesario y luego haga clic en **Apply** para actualizar la configuración de ASA:



6. Seleccione **Routing** y haga clic en **Rutas estáticas** ubicadas en el lado izquierdo de la aplicación ASDM:



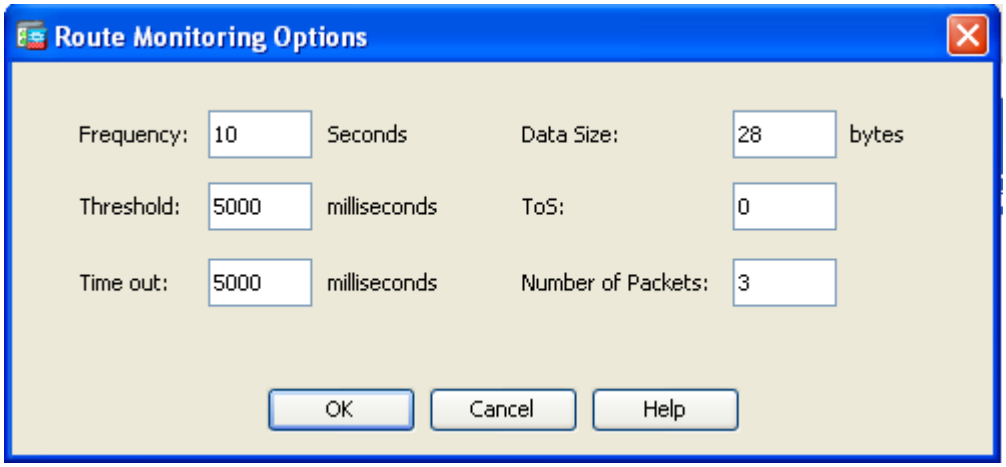
7. Haga clic en **Agregar para agregar las nuevas rutas estáticas.** Este cuadro de diálogo aparece:



8. De la lista desplegable Nombre de la Interfaz, elija la interfaz en la cual la ruta reside, y configure la ruta predeterminada para alcanzar el gateway. En este ejemplo, **203.0.113.2** es el gateway ISP primario y **4.2.2.2** es el objeto a monitorear con ecos ICMP.

9. En el área Opciones, haga clic en el botón de opción **Seguimiento** e ingrese los valores apropiados en los campos *Track ID*, *SLA ID* y *Track IP Address*.

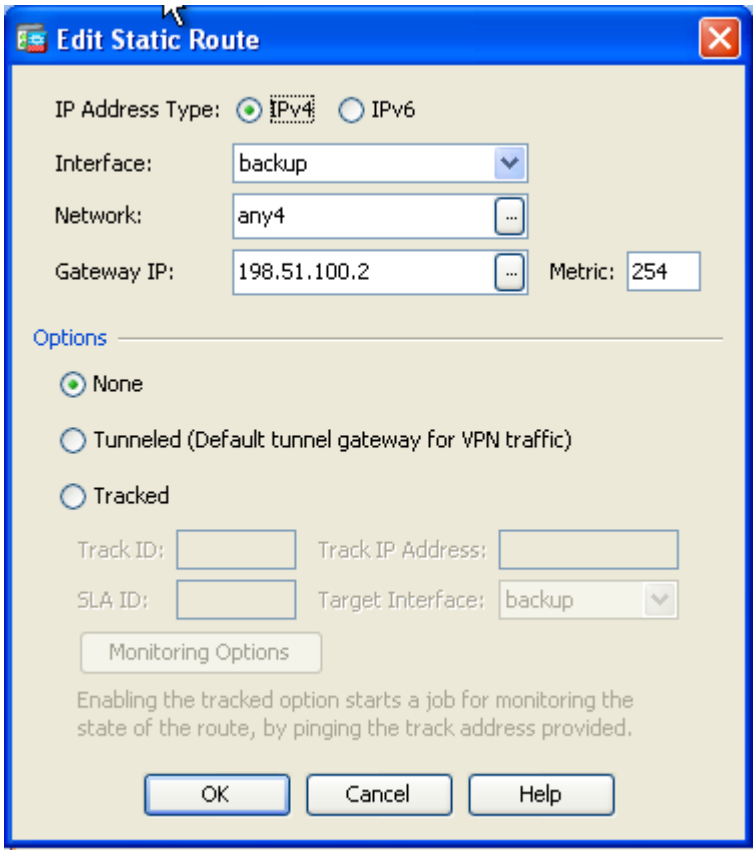
10. Haga clic en **Opciones de Monitoreo**. Este cuadro de diálogo aparece:



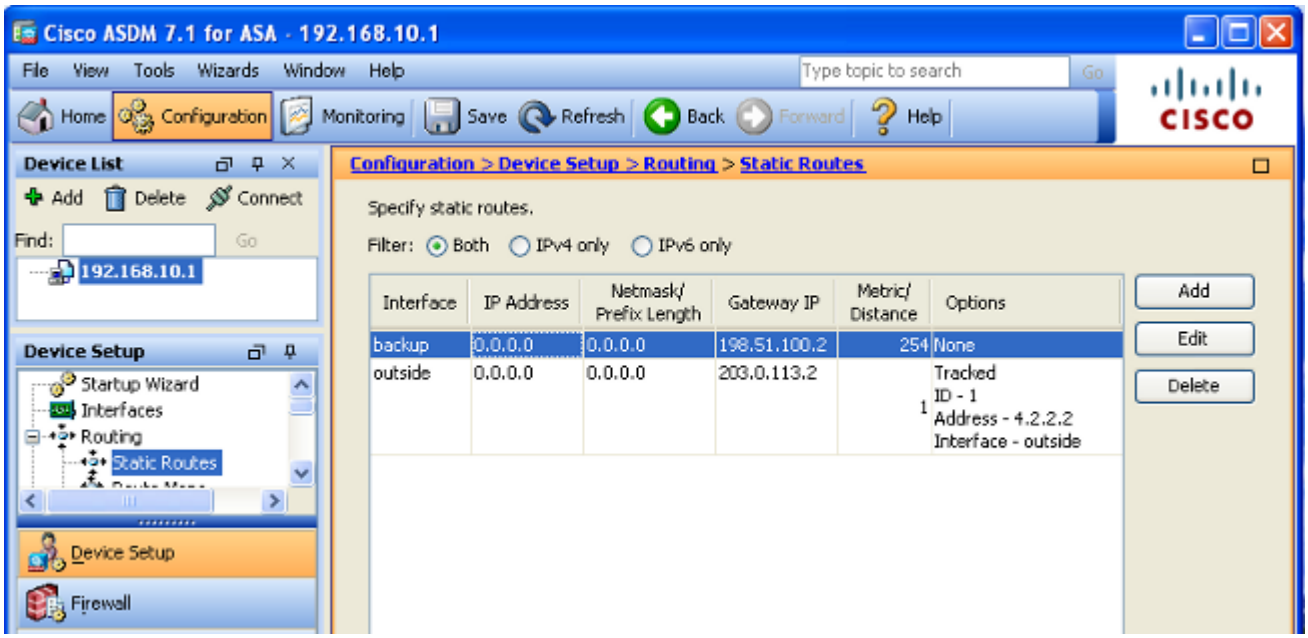
11. Introduzca los valores adecuados para la frecuencia y otras opciones de supervisión y, a continuación, haga clic en **Aceptar**.

12. Agregue otra ruta estática para el ISP secundario para proporcionar una ruta y conectarse con Internet. Para que sea una ruta secundaria, configure esta ruta con una métrica más alto, tal como 254. Si la ruta principal (ISP primario) falla, esa ruta se quita de la tabla de ruteo. Esta ruta secundaria (ISP secundario) se instala en su lugar en la tabla de enrutamiento de Private Internet Exchange (PIX).

13. Haga clic en **Aceptar** para cerrar el cuadro de diálogo:



Las configuraciones aparecen en la lista de interfaz:



14. Seleccione la configuración de ruteo y luego haga clic en **Apply** para actualizar la configuración de ASA.

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Confirme que la configuración ha finalizado

> **Nota**: la herramienta Output Interpreter Tool (sólo clientes registrados) admite ciertos comandos **show**. Utilice la herramienta para ver una análisis de información de salida del comando show.

Utilice estos comandos **show** para verificar que su configuración esté completa:

- **show running-config sla monitor** - La salida de este comando muestra los comandos SLA en la configuración.

  <#root>

  ```
  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** : La salida de este comando muestra los valores de configuración actuales de la operación.

  <#root>

  ```
  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** - La salida de este comando muestra las estadísticas operativas de la operación SLA.
    - Antes de que el ISP primario falle, éste es el estado operacional:

<#root>

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

    - Después de que el ISP primario falla (y el ICMP hace eco del tiempo de espera), éste es el estado operacional:

<#root>

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
```

Confirmar que la ruta de copia de seguridad está instalada (método CLI)

Ingrese el comando **show route** para confirmar que la ruta de respaldo está instalada.

Antes de que el ISP primario falle, la tabla de ruteo aparece similar a esta:

```
<#root>

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
```

Después de que el ISP primario falle, se quite la ruta estática y se instale la ruta de respaldo, la tabla de ruteo aparece de manera similar a esta:

<#root>

ASA#

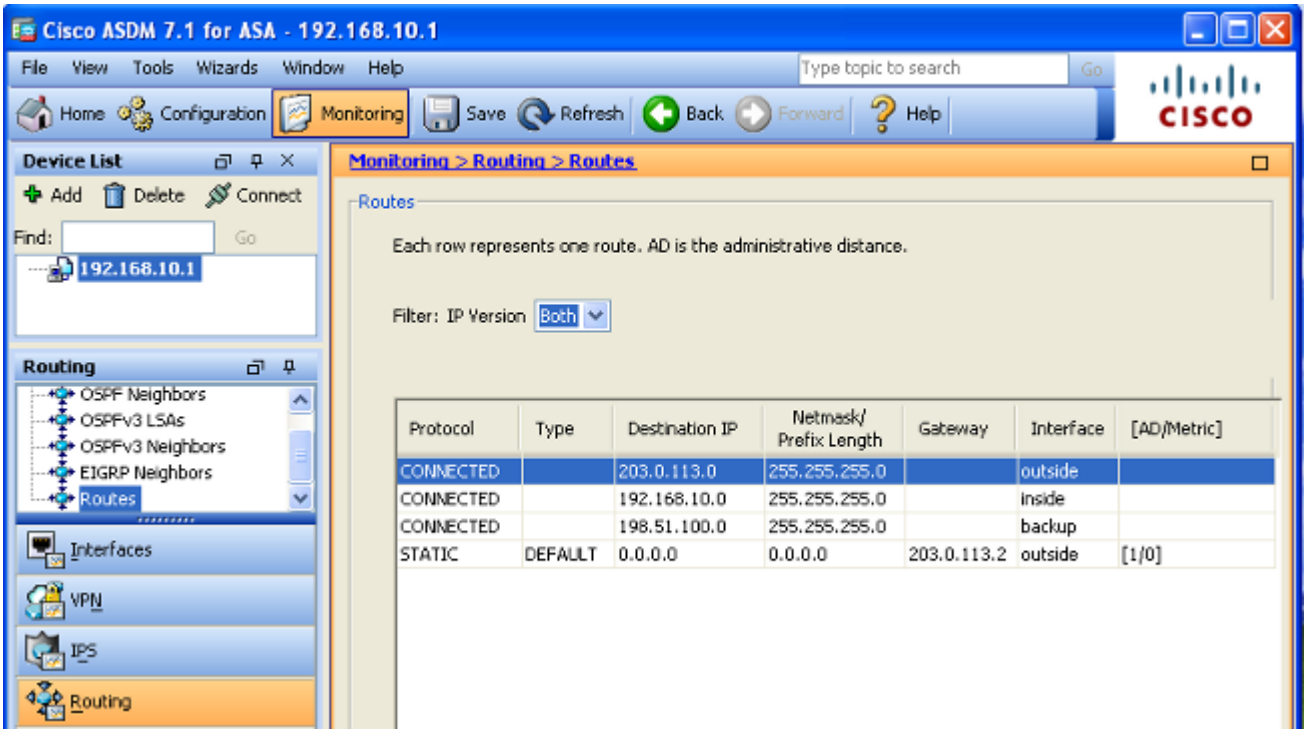
show route

```
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
```

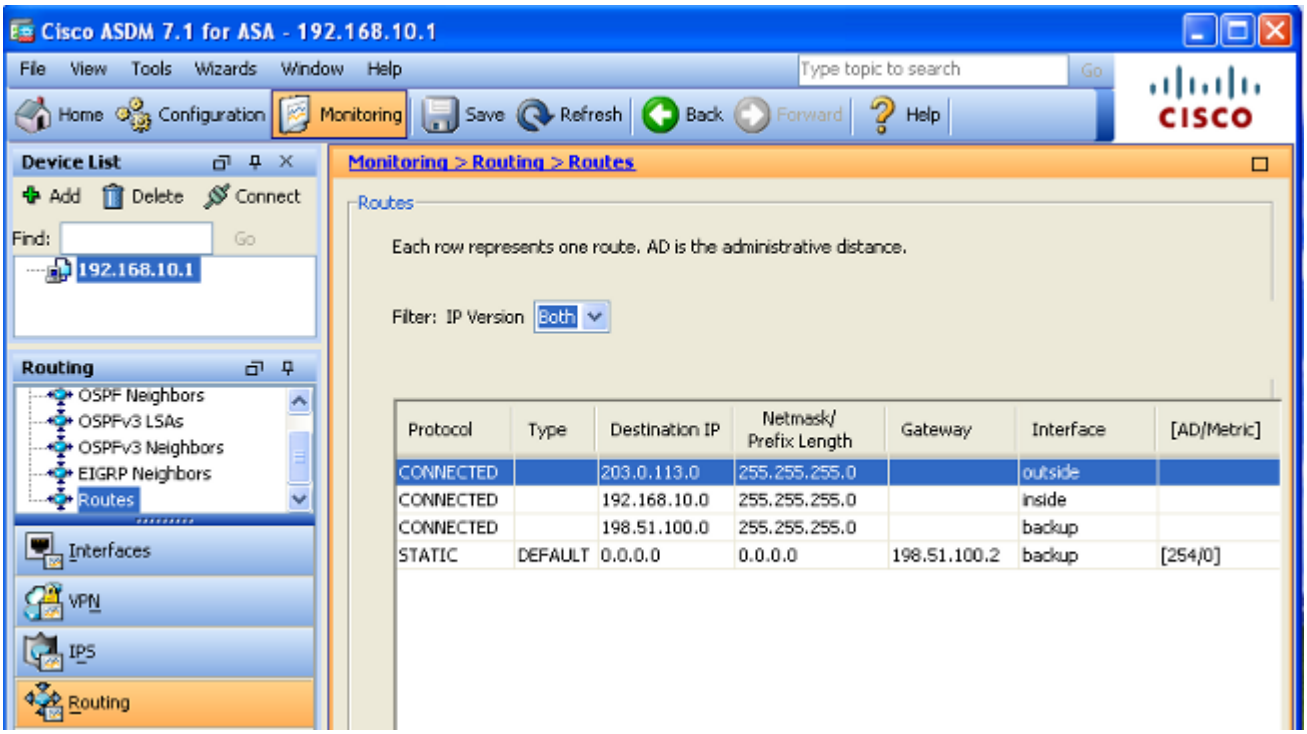
Confirme que la Ruta de Respaldo está Instalada (Método ASDM)

Para confirmar que la ruta de respaldo se instala a través del ASDM, navegue hasta **Monitoring > Routing**, y luego elija **Routes** en el árbol de ruteo.

Antes de que el ISP primario falle, la tabla de ruteo aparece similar a la que se muestra en la siguiente imagen. Observe que la ruta **DEFAULT** apunta a **203.0.113.2** a través de la interfaz **externa**:



Después de que el ISP primario falle, se quita la ruta y se instala la ruta de respaldo. La ruta PREDETERMINADA ahora indica 198.51.100.2 a través de la interfaz de respaldo:



Troubleshoot

Esta sección proporciona algunos comandos de depuración útiles y describe cómo resolver un problema en el que la ruta de seguimiento se elimina innecesariamente.

Comandos de Debug

Puede utilizar estos comandos debug para resolver sus problemas de configuración:

- **debug sla monitor trace -** La salida de este comando muestra el progreso de la operación de eco.
    - Si el objeto rastreado (gateway ISP primario) está activo y el ICMP resuena correctamente, el resultado aparece de manera similar a la siguiente:

```
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
```

    - Si el objeto sometido a seguimiento (gateway ISP primario) está inactivo y los ecos ICMP fallan, el resultado es similar a lo siguiente:

```
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 -** La salida de este comando muestra cualquier error que el proceso de monitoreo SLA encuentre.
    - Si el objeto seguido (gateway ISP primario) está activo y el ICMP funciona correctamente, el resultado es similar a este:

```
%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
```

    - Si el objeto sometido a seguimiento (gateway ISP primario) está inactivo y se elimina la ruta objeto de seguimiento, el resultado es similar al siguiente:

<#root>

```
%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.

La Ruta Localizada se Quitó Innecesariamente

Si la ruta localizada se quita innecesariamente, asegúrese de que su objetivo de monitoreo esté siempre disponible para recibir las solicitudes de eco.

Además, asegúrese de que el estado de su objetivo de monitoreo (es decir, independientemente de si el objetivo es accesible) esté estrechamente relacionado con el estado de conexión de ISP primario.

Si elige un destino de monitoreo que esté más lejos que el gateway del ISP, es posible que otro link a lo largo de esa ruta falle o que otro dispositivo interfiera.

Por lo tanto, esta configuración potencialmente hace que el monitor SLA concluya que la conexión con el ISP primario ha fallado y haga que el ASA conmute por error innecesariamente al link ISP secundario.

Por ejemplo, si elige un router de la sucursal como objetivo de monitoreo, la conexión ISP a su sucursal podría fallar, así como cualquier otro link en ese trayecto.

Una vez que los ecos ICMP enviados por la operación de monitoreo fallan, se elimina la ruta de seguimiento principal, aunque el link ISP primario aún esté activo.

En este ejemplo, el gateway del ISP primario que se utiliza como objetivo de monitoreo es administrado por el ISP y se localiza en el otro lado del link ISP.

Esta configuración garantiza que si los ecos ICMP que se envían por la operación de monitoreo fallan, el link ISP está casi con seguridad inactivo.

Información Relacionada

- **Firewalls de próxima generación Cisco ASA Serie 5500-X**
- **Soporte Técnico y Documentación - Cisco Systems**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).