Configure el ASA para los links redundantes o de reserva ISP

Contenido

Introducción

Este documento describe cómo configurar el dispositivo de seguridad adaptante de las 5500 Series de Cisco ASA (ASA) para el uso de la característica de seguimiento de la Static ruta para permitir al dispositivo para utilizar las conexiones de Internet redundantes o de reserva.

Prerequisites

Requisitos

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.

- 5555-X Series de Cisco ASA que funciona con la versión de software 9.x o más adelante
- Cisco ASDM versión 7.x o más adelante

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Usted puede también utilizar esta configuración con la versión 9.1(5) de las 5500 Series de Cisco ASA.

> **Note**: Requieren al **comando backup interface** para configurar la cuarta interfaz en las 5505 Series ASA. Refiera a la sección de la Interfaz de respaldo de la *referencia de comandos del dispositivo del Cisco Security, versión 7.2* para más información.

Antecedentes

Esta sección proporciona una descripción de la característica de seguimiento de la Static ruta que se describe en este documento, así como algunas recomendaciones importantes antes de que usted comience.

Descripción de la característica de seguimiento de la Static ruta

Un problema con el uso de las Static rutas es que existe ningún mecanismo inherente que puede determinar si la ruta está hacia arriba o hacia abajo. 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 solucionar este problema, una característica de seguimiento de la Static ruta se utiliza para seguir la Disponibilidad de una Static ruta. La característica quita la Static ruta de la tabla de ruteo y la substituye por una ruta de seguridad sobre el error.

El seguimiento de la Static ruta permite que el ASA utilice una conexión barata a un ISP secundario en caso que la línea arrendada primaria llegue a ser inasequible. Para alcanzar esta Redundancia, el ASA asocia una Static ruta a una blanco de la supervisión que usted defina. La operación del Acuerdo de nivel de servicio (SLA) monitorea la blanco con los pedidos de eco ICMP periódicos. Si una Respuesta de eco no se recibe, después el objeto se considera abajo, y la ruta asociada se quita de la tabla de ruteo. Una ruta de respaldo previamente configurada se utiliza en lugar de la ruta que se quita. Mientras que la ruta de seguridad es funcionando, la operación del monitor de SLA continúa sus tentativas de alcanzar la blanco de la supervisión. 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, el 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 un Digital Subscriber Line (DSL) más de poca velocidad que se accede a través de un módem DLS proporcionado por el ISP secundario.

> **Note**: La configuración que se describe en este documento no se puede utilizar para el Equilibrio de carga o la carga a compartir, pues no se soporta en el ASA. Use esta configuración para la redundancia o para realizar un un respaldo solamente. El tráfico saliente utiliza el ISP primario, y entonces el ISP secundario si el primario falla. 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 va la conexión al ISP primario abajo, el ASA cambia el tráfico directo de la tabla de ruteo para a la conexión DSL. El seguimiento de la Static ruta se utiliza para alcanzar esta Redundancia.

El ASA se configura con una Static ruta que dirija todo el tráfico de Internet al ISP primario. Cada diez segundos, las pruebas del proceso del monitor de SLA para confirmar que el gateway del ISP primario es accesible. 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 manera relativamente barata de asegurarse de que el acceso a internet saliente sigue siendo disponible para los usuarios detrás del ASA. Según lo descrito en este documento, esta configuración no pudo ser conveniente para el acceso entrante a los recursos detrás del ASA. Las habilidades avanzadas del establecimiento de una red se requieren para alcanzar las conexiones hacia adentro inconsútiles. Estas habilidades no se abordan en este documento.

Recomendaciones importantes

Antes de que usted intente la configuración que se describe en este documento, usted debe elegir una blanco de la supervisión que pueda responder a los pedidos de eco del Internet Control Message Protocol (ICMP). La blanco puede ser cualquier objeto de red que usted elija, pero se recomienda una blanco que se ata de cerca a su conexión de Proveedor de servicios de Internet (ISP). Aquí están algunas blancos posibles de la supervisión:

- La dirección del gateway ISP
- Otra dirección administrada por ISP
- Un servidor en otra red, tal como un servidor del Authentication, Authorization, and Accounting (AAA) con el cual el ASA debe comunicar
- 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 el ASA está completamente - operativo y configurado para permitir que el Cisco Adaptive Security Device Manager (ASDM) realice los cambios de configuración.

> **Tip**: Para la información sobre cómo permitir que el ASDM configure el dispositivo, refiera al acceso HTTPS que configura para la sección del ASDM del *libro 1 CLI: Guía de configuración CLI de los funcionamientos generales de la serie de Cisco ASA, 9.1*.

Configurar

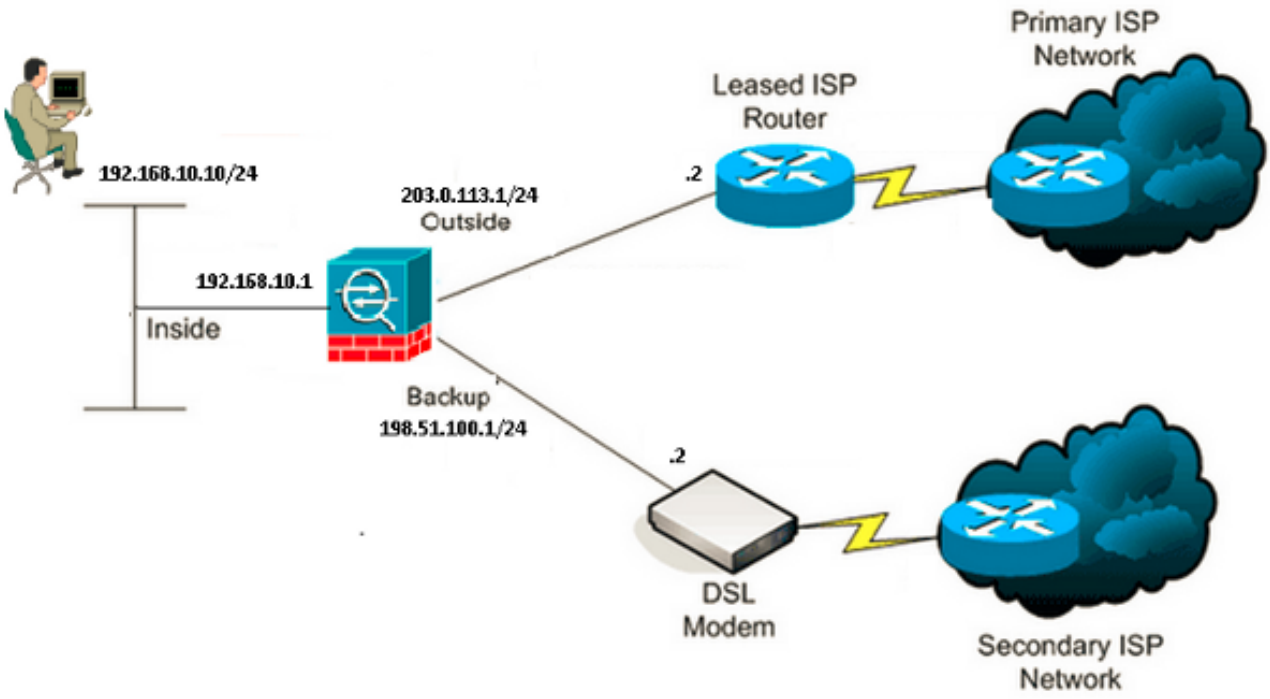
Utilice la información que se describe en esta sección para configurar el ASA para el uso de la característica de seguimiento de la Static ruta.

> **Note**: Utilice la herramienta de búsqueda de comandos (clientes registrados solamente) para obtener más información sobre los comandos que se utilizan en esta sección.

> **Note**: Los IP Addresses que se utiliza en esta configuración no son legalmente routable en Internet. Son los direccionamientos del RFC 1918, que se utilizan en un ambiente de laboratorio.

Diagrama de la red

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



Configuración de CLI

Utilice esta información para configurar el ASA vía el CLI:

```
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
```

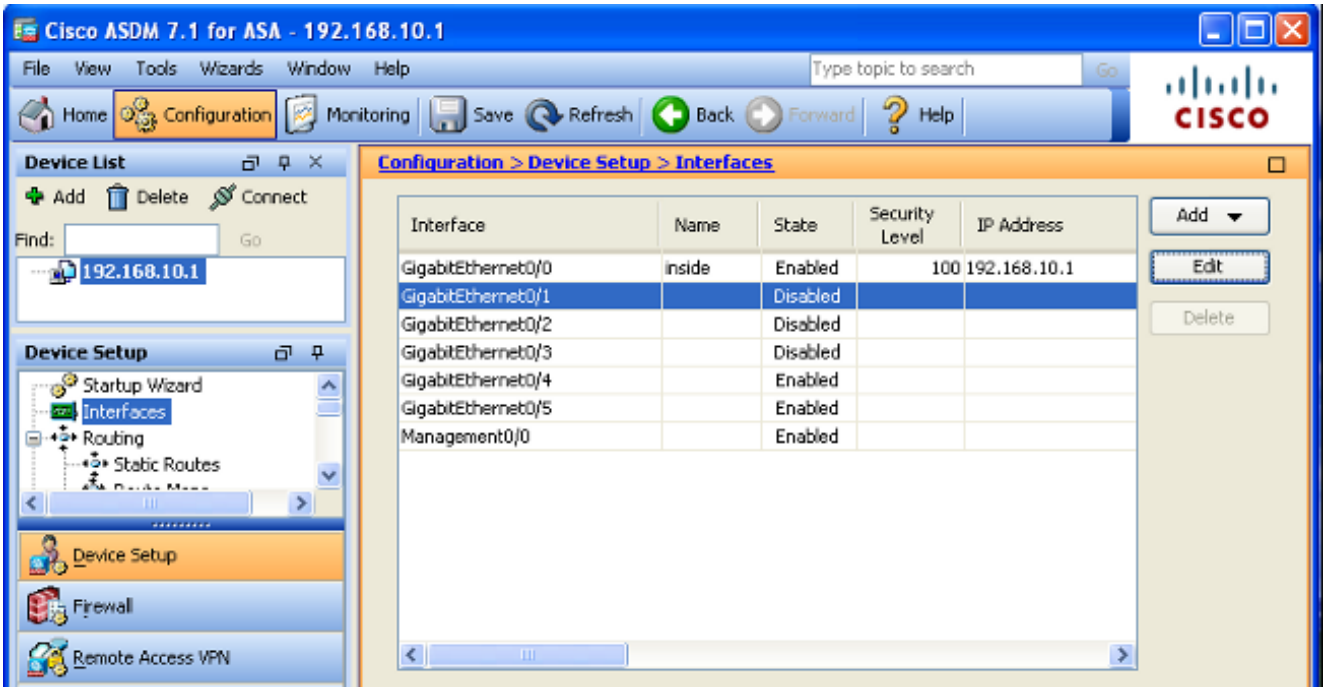
```
mtu outside 1500
mtu backup 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
object network Inside_Network
 nat (inside,outside) dynamic interface
object network inside_network
 nat (inside,backup) dynamic interface

!--- 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
```

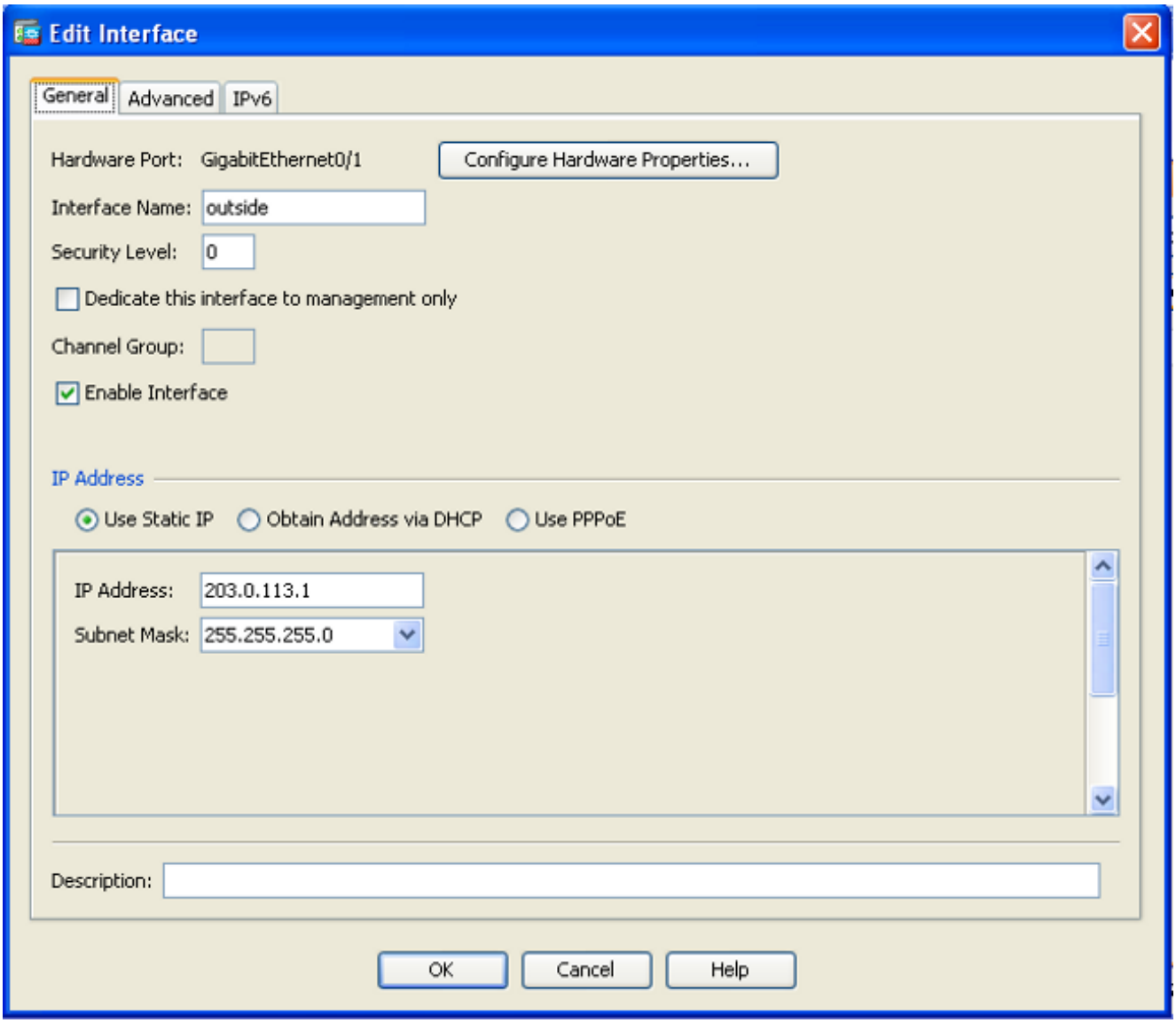
Configuración de ASDM

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

1. Dentro de la aplicación ASDM, haga clic la **configuración**, y después haga clic las **interfaces**.



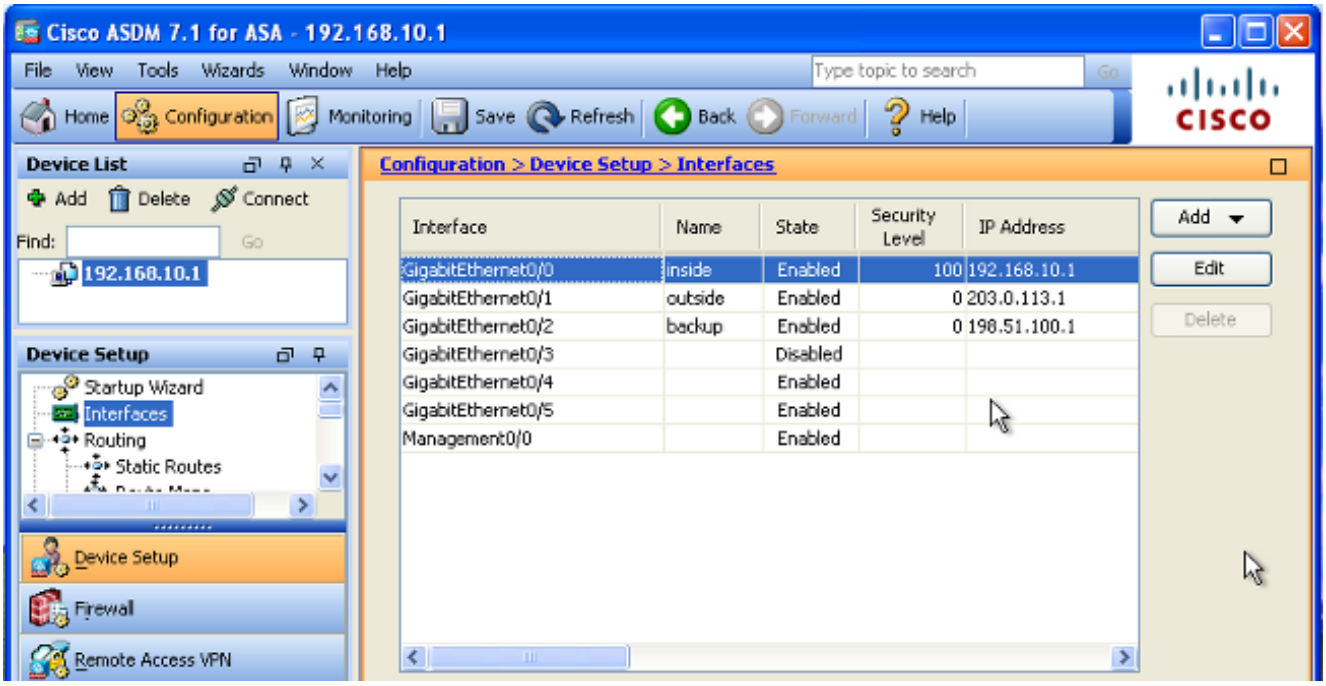
2. Seleccione **GigabitEthernet0/1 de la** lista de las interfaces, y después haga clic **editan**. Este cuadro de diálogo aparece:



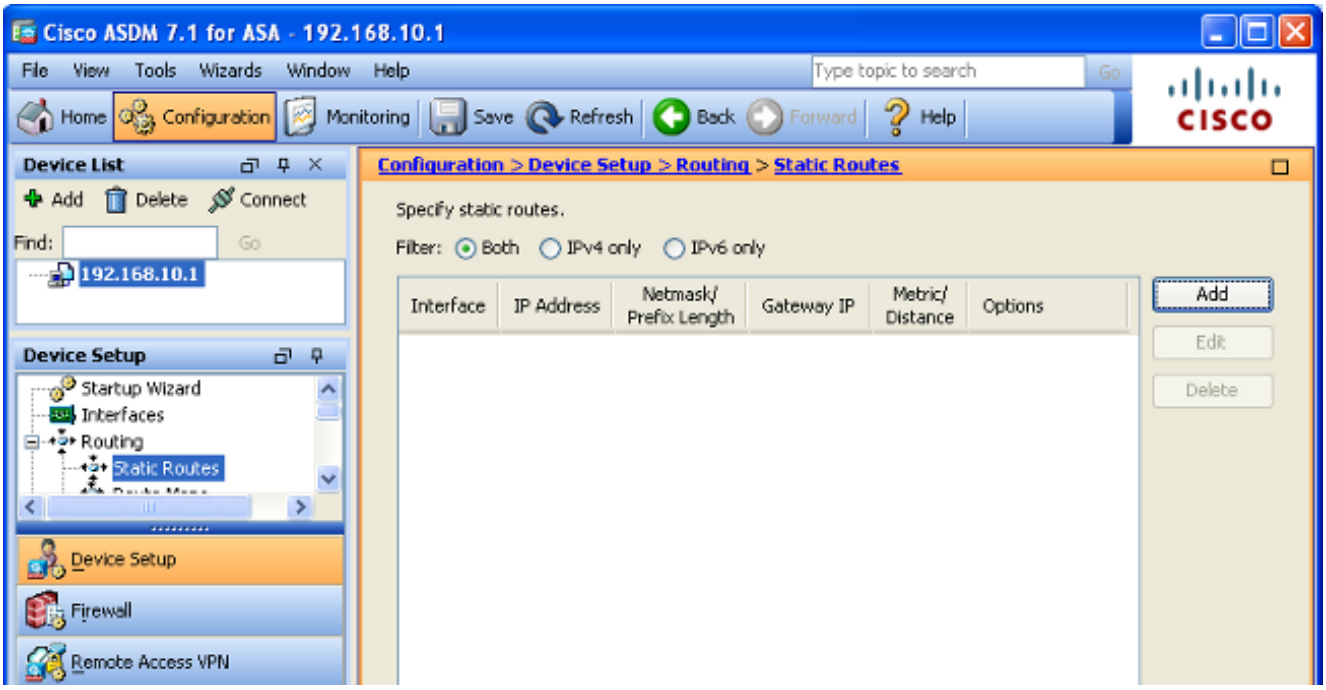
3. Marque el rectángulo de **comprobaciones de interfaz del habilitar**, y ingrese los valores apropiados en los campos del *nombre*, del *nivel de seguridad*, del *IP Address*, y de la *máscara de subred de la interfaz*.

4. Haga Click en OK para cerrar el cuadro de diálogo.

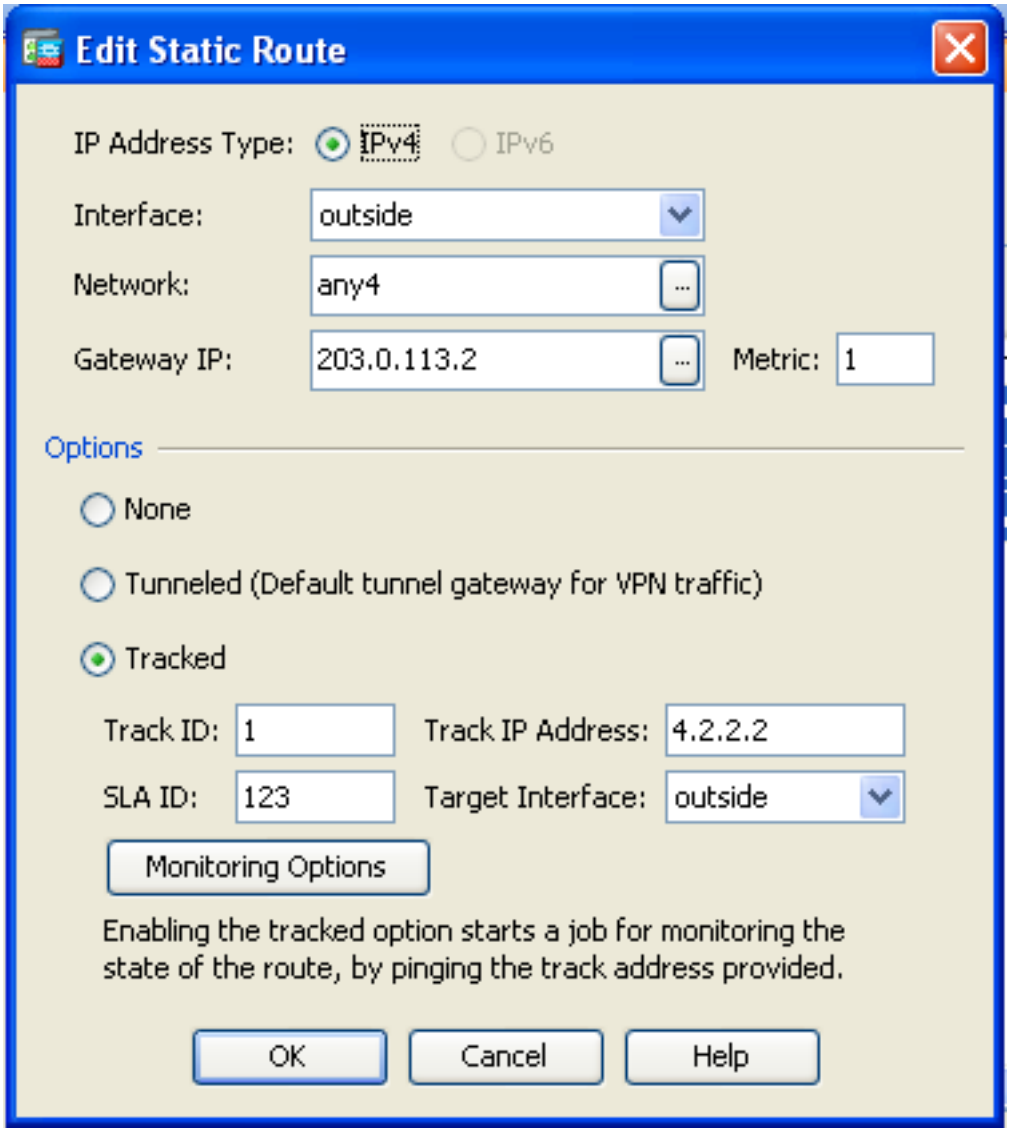
5. Configure las otras interfaces según las necesidades, y después haga clic **se aplican** para poner al día la configuración ASA:



6. Seleccione la **encaminamiento** y haga clic las **Static rutas** situadas en el lado izquierdo de la aplicación ASDM:



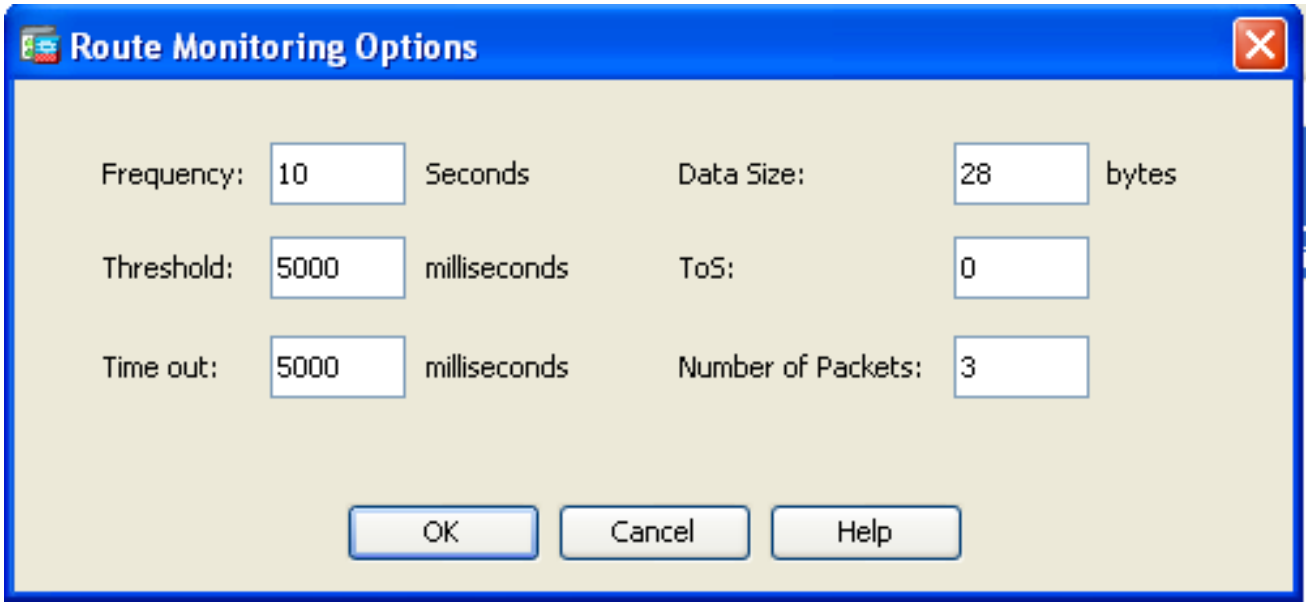
7. Haga clic en **Agregar** para agregar las nuevas rutas estáticas. Este cuadro de diálogo aparece:



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 del ISP primario y **4.2.2.2** es el objeto a monitorear con los ecos ICMP.

9. En el área de las opciones, haga clic el botón de radio **seguido** y ingrese los valores apropiados en la *pista ID*, *SLA ID*, y campos del *IP Address de la pista*.

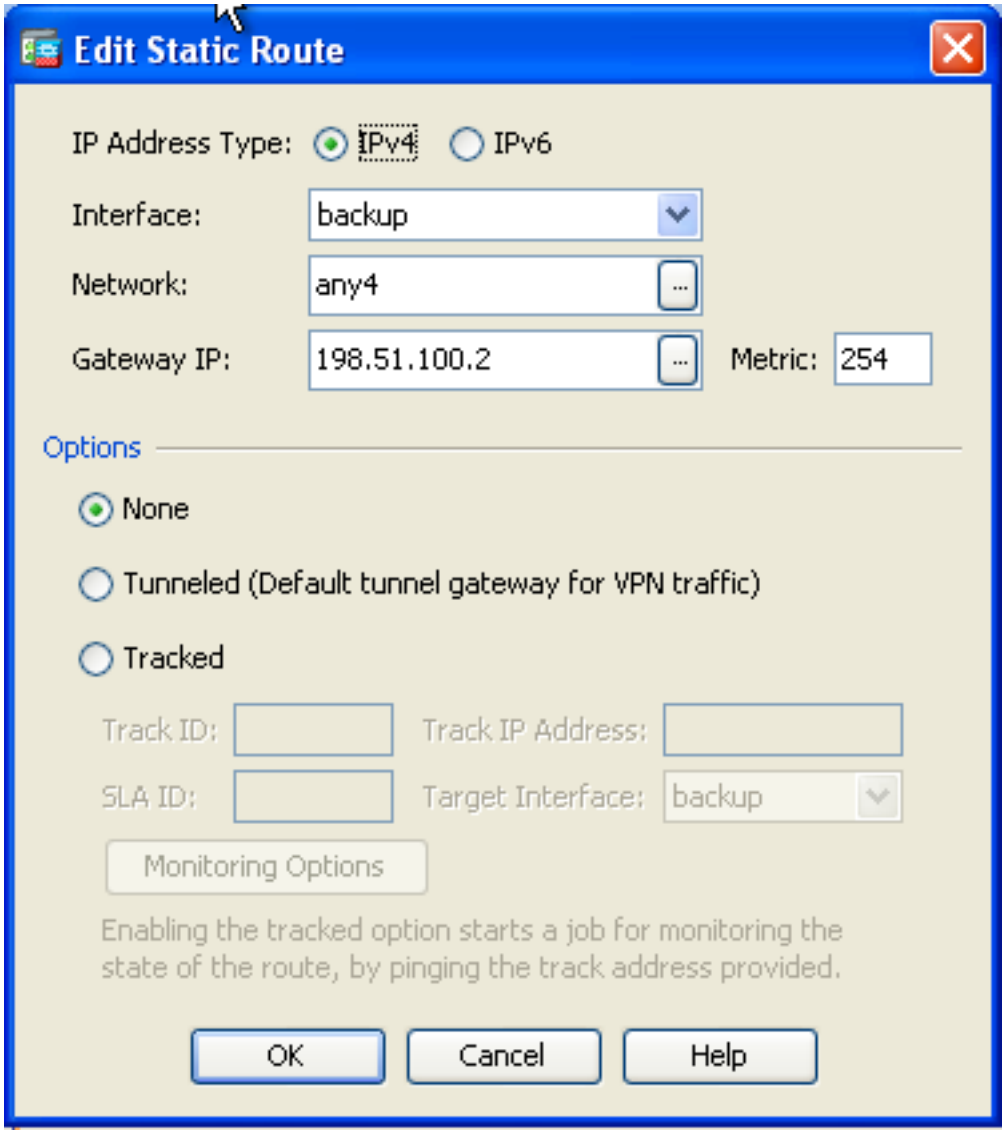
10. Haga clic en **Opciones de Monitoreo**. Este cuadro de diálogo aparece:



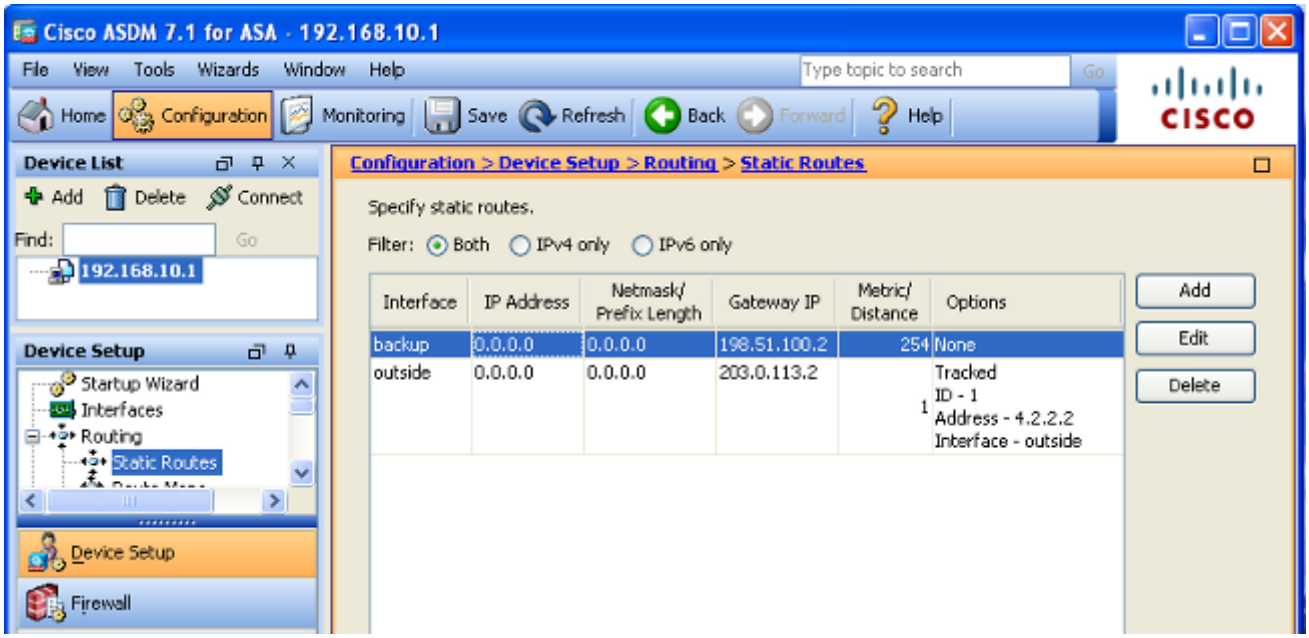
11. Ingrese los valores apropiados para la frecuencia y otras opciones de la supervisión, y después haga clic la **AUTORIZACIÓN**.

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) está instalada en la tabla de ruteo del private internet exchange (PIX) en lugar de otro.

13. Haga Click en OK para cerrar el cuadro de diálogo:



Las configuraciones aparecen en la lista de interfaz:



14. Seleccione la configuración de ruteo, y después haga clic **se aplican** para poner al día la configuración ASA.

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Confirme que la configuración es completa

> **Note**: La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

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

- **muestre el monitor del sla de los ejecutar-config** – La salida de este comando visualiza los comandos de SLA en la configuración.

```
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
```

- **muestre la configuración del monitor del sla** – La salida de este comando visualiza las configuraciones de la configuración actual de la operación.

```
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:
```

- **muestre al estado operacional del monitor del sla** – La salida de este comando visualiza las estadísticas operativas de la operación de SLA.

  Antes de que el ISP primario falle, éste es el estado operacional:

```
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 falle (y el descanso de los ecos ICMP), éste es el estado operacional:

```
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
```

Confirme que la ruta de seguridad está instalada (método CLI)

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

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

```
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 quita la Static ruta, y la ruta de seguridad está instalada,

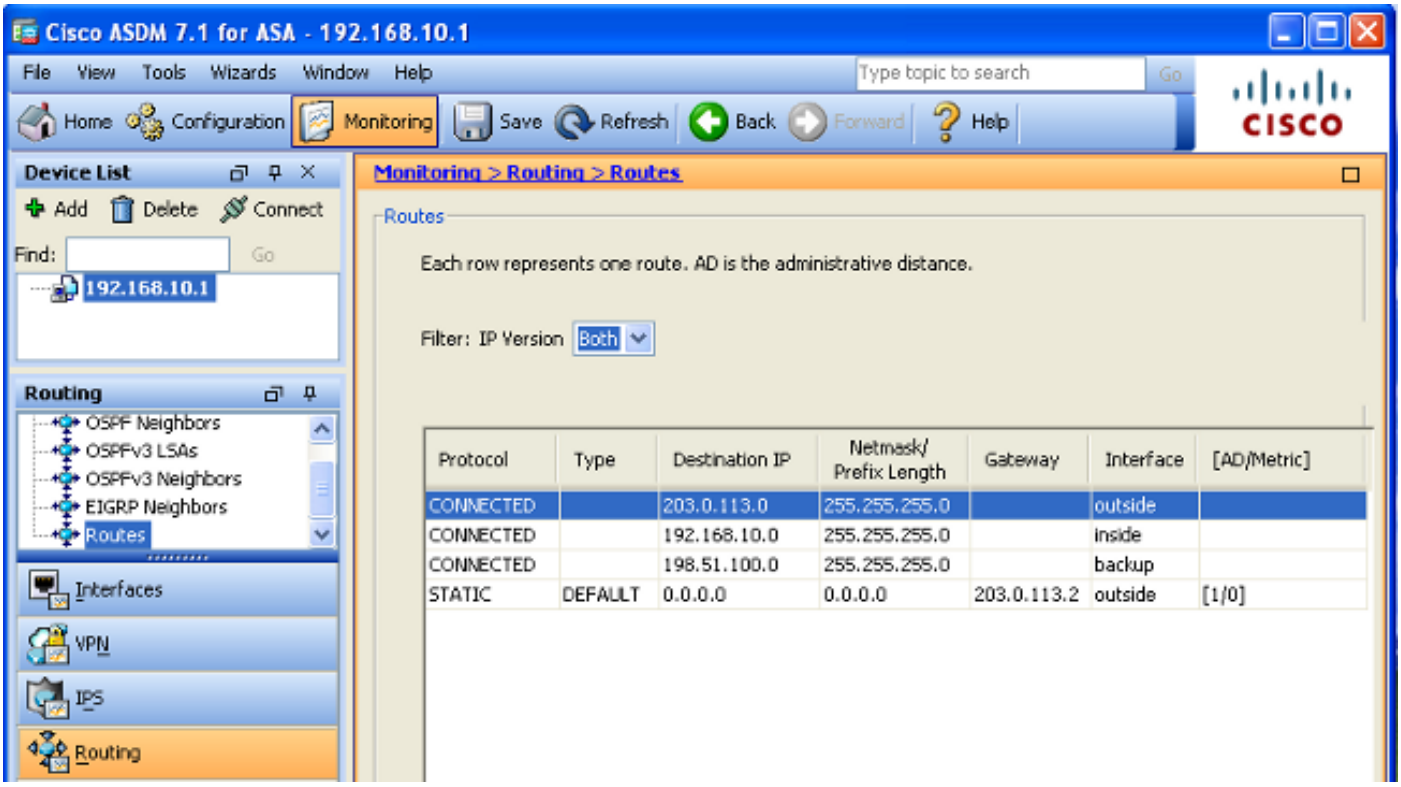
la tabla de ruteo aparece similar a esto:

```
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
```

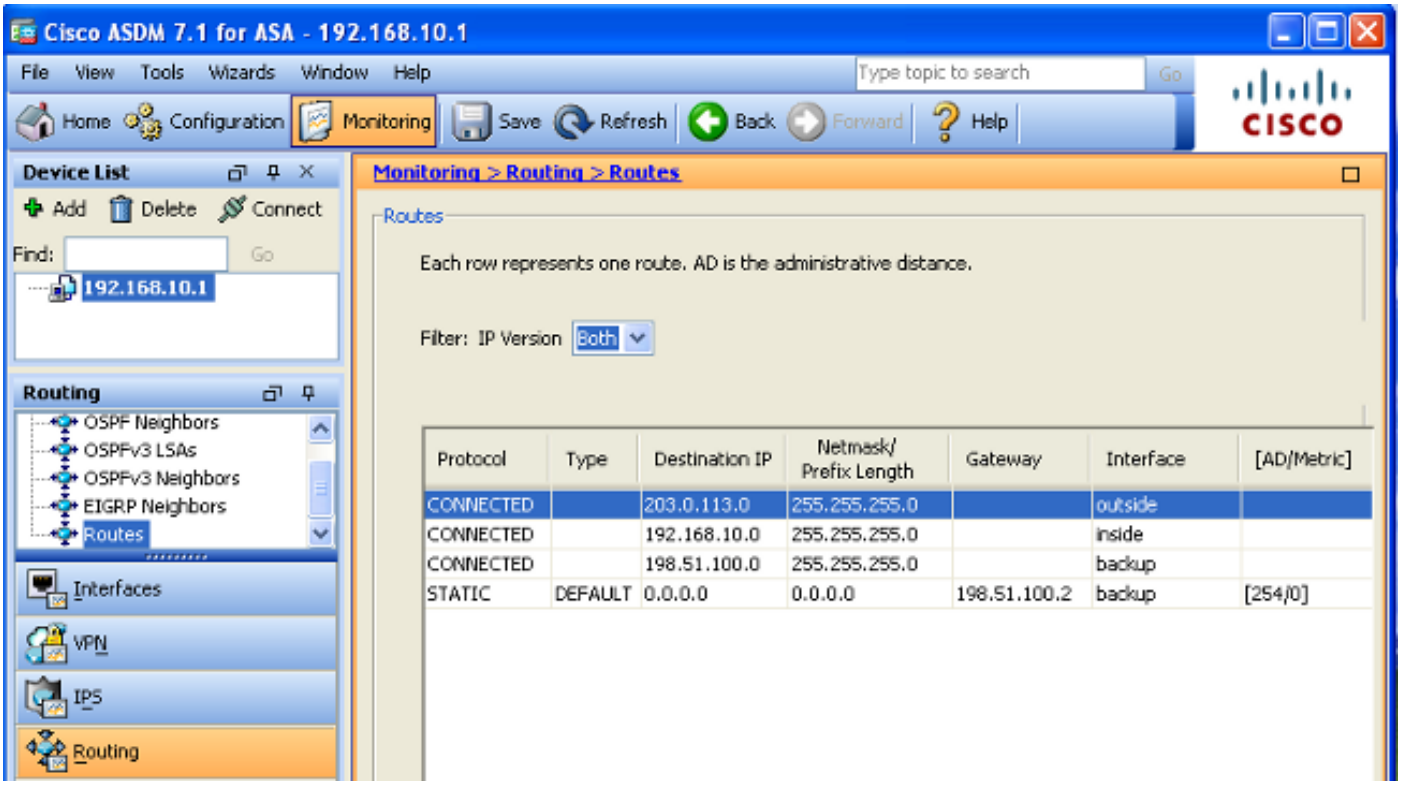
Confirme que la ruta de seguridad está instalada (método del ASDM)

Para confirmar que la ruta de seguridad está instalada vía el ASDM, navegue a **monitorear > encaminamiento**, y después elija las **rutas del** árbol de ruteo.

Antes de que el ISP primario falle, la tabla de ruteo aparece similar a ésa mostrada en la imagen siguiente. Observe que la **ruta predeterminado** señala a **203.0.113.2** a través de la **interfaz exterior**:



Después de que el ISP primario falle, se quita la ruta y la ruta de seguridad está instalada. **La ruta predeterminado** ahora señala a **198.51.100.2** a través de la **Interfaz de respaldo**:



Troubleshooting

Esta sección proporciona algunos comandos debug útiles y describe cómo resolver problemas un problema donde la ruta seguida se quita innecesariamente.

Comandos de Debug

Usted puede utilizar estos comandos debug para resolver problemas sus problemas de configuración:

- **traza del monitor del sla del debug** – La salida de este comando visualiza el progreso de la operación de la generación de eco.

  Si el objeto seguido (gateway del ISP primario) es ascendente y los ecos ICMP tiene éxito, la salida aparece similar a esto:

```
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
```

Si el objeto seguido (gateway del ISP primario) está abajo y los ecos ICMP falla, la salida aparece similar a esto:

```
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
```

- error del monitor del sla del debug – La salida de este comando visualiza cualquier error que los encuentros del proceso del monitor de SLA.

Si el objeto seguido (gateway del ISP primario) es ascendente y el ICMP tiene éxito, la salida aparece similar a esto:

```
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
```

Si se quita el objeto seguido (gateway del ISP primario) está abajo y la ruta seguida, la salida aparece similar a esto:

```
%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 usted elige una blanco de la supervisión que esté más lejos ausente que el gateway ISP, otro link a lo largo de esa ruta pudo fallar u otro dispositivo pudo interferir. Esta configuración pudo hacer al monitor de SLA concluir que la conexión al ISP primario ha fallado y hacer el ASA fallar innecesariamente encima al link secundario ISP.

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 se quitan los ecos ICMP que son enviados por el fall de la operación de monitoreo, la ruta seguida primaria, aunque el link del ISP primario es todavía 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 se asegura de que si los ecos ICMP que son enviados por el fall de la operación de monitoreo, el link ISP están casi seguramente abajo.

Información Relacionada

- Firewall de la última generación de las 5500-X Series de Cisco ASA
- Soporte Técnico y Documentación - Cisco Systems