ASA/PIX 7.x: El ISP redundante o de reserva enlaza el ejemplo de configuración

Contenido

Introducción

Un problema con las rutas estáticas es la ausencia de un mecanismo inherente para determinar si la ruta está activa o desactiva. 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 función de seguimiento de la ruta estática se utiliza para seguir la disponibilidad de una ruta estática y, si esa ruta falla, la quita de la tabla de ruteo y la substituye por una ruta de respaldo.

Este documento proporciona un ejemplo de cómo utilizar la función de seguimiento de la ruta estática en el PIX 500 Series Security Appliance o ASA 5500 Series Adaptive Security Appliance para habilitar el dispositivo para utilizar conexiones de Internet redundantes o de respaldo. En este ejemplo, el seguimiento de la ruta estática permite que el dispositivo de seguridad utilice una conexión económica a un Proveedor de servicios de Internet (ISP) secundario en caso de que la

línea arrendada primaria deje de estar disponible.

Para alcanzar esta redundancia, el dispositivo de seguridad se asocia con una ruta estática a un objetivo de monitoreo que defina. La operación de acuerdo de nivel de servicio (SLA) monitorea el objetivo con solicitudes de eco periódicas del Internet Control Message Protocol (ICMP). Si no se recibe respuesta de eco, el objeto se considera desactivado, 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 respaldo esté en funcionando, la operación del monitor SLA continúa intentando alcanzar el objetivo 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.

Nota: La configuración descrita en este documento no se puede utilizar para el Equilibrio de carga o la carga a compartir pues no se soporta encendido ASA/PIX. Use esta configuración para la redundancia o para realizar un un respaldo solamente. El tráfico saliente utiliza el ISP primario y el ISP secundario, si el primario falla. El incidente del ISP primario causa una interrupción temporal del tráfico.

prerrequisitos

Requisitos

Elija una blanco de la supervisión que pueda responder a los pedidos de eco ICMP. El objetivo puede ser cualquier objeto de red que elija, pero se recomienda un objetivo directamente relacionado a su conexión ISP. Algunos objetivos de monitoreo posibles incluyen:

- La dirección del gateway ISP
- Otra dirección administrada por ISP
- Un servidor en otra red, tal como un servidor de AAA, con el cual el dispositivo de seguridad 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 supone que el dispositivo de seguridad está completamente operativo y configurado para permitir que el ASDM de Cisco realice los cambios de configuraciones.

Nota: Para obtener información sobre cómo permitir que el ASDM configure el dispositivo, consulte Cómo permitir Acceso HTTPS para ASDM.

Componentes Utilizados

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

- Cisco PIX Security Appliance 515E con versión de software 7.2(1) o posterior
- Cisco Adaptive Security Device Manager 5.2(1) 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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

También puede usar esta configuración con el Cisco ASA 5500 Series Security Appliance versión 7.2(1).

Nota: El comando **backup interface** se requiere para configurar la cuarta interfaz en el ASA 5505. Refiera a la Interfaz de respaldo para más información.

Convenciones

Para más información sobre las convenciones sobre documentos, consulte Convenciones sobre Consejos Técnicos de Cisco.

Antecedentes

En este ejemplo, el dispositivo de seguridad mantiene dos conexiones al 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 baja velocidad a al que se accede a través de un módem DLS proporcionado por el ISP secundario.

Nota: El balance de carga no ocurre en este ejemplo.

La conexión DSL permanece inactiva mientras la línea arrendada está activa y el gateway del ISP primario es accesible. Sin embargo, si la conexión al ISP primario se desactiva, el dispositivo de seguridad cambia la tabla de ruteo al tráfico directo a la conexión DSL. El seguimiento de la ruta estática se utiliza para alcanzar esta redundancia.

El dispositivo de seguridad se configura con una ruta estática que dirige todo el tráfico de Internet al ISP primario. Cada 10 segundos el proceso de monitoreo confirma que el gateway del ISP primario sea 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 económica de garantizar que el acceso a Internet saliente sigue estando disponible para los usuarios del dispositivo de seguridad. Según lo descrito en este documento, esta disposición quizá no sea conveniente para el acceso de entrada a los recursos del dispositivo de seguridad. Se necesitan habilidades de red avanzadas para alcanzar las conexiones entrantes . Estas habilidades no se abordan en este documento.

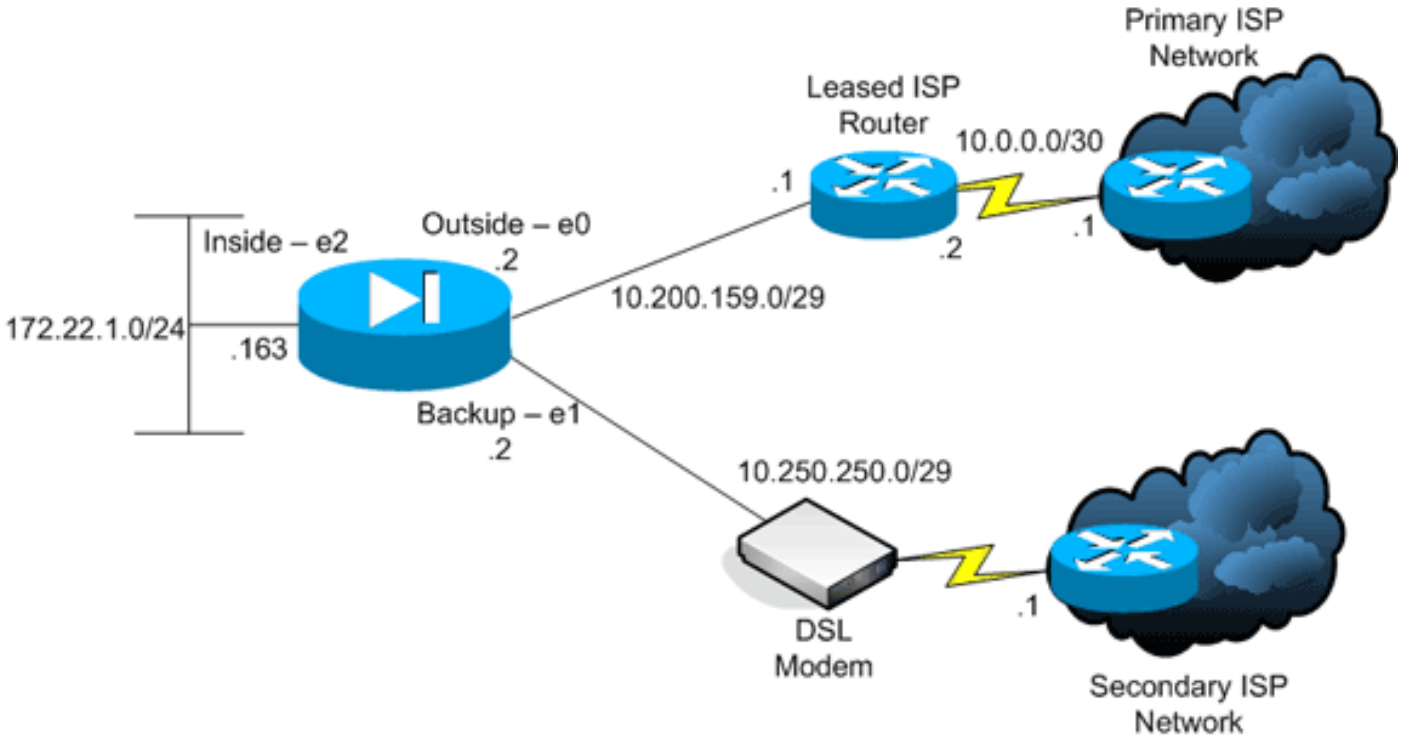
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Las direcciones IP usadas en esta configuración no son legalmente enrutables en Internet. Son direcciones RFC1918 que se utilizan en un ambiente de laboratorio.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

- Interfaz de línea de comandos (CLI)
- Adaptive Security Device Manager (ASDM)

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Configuración de CLI

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.
```

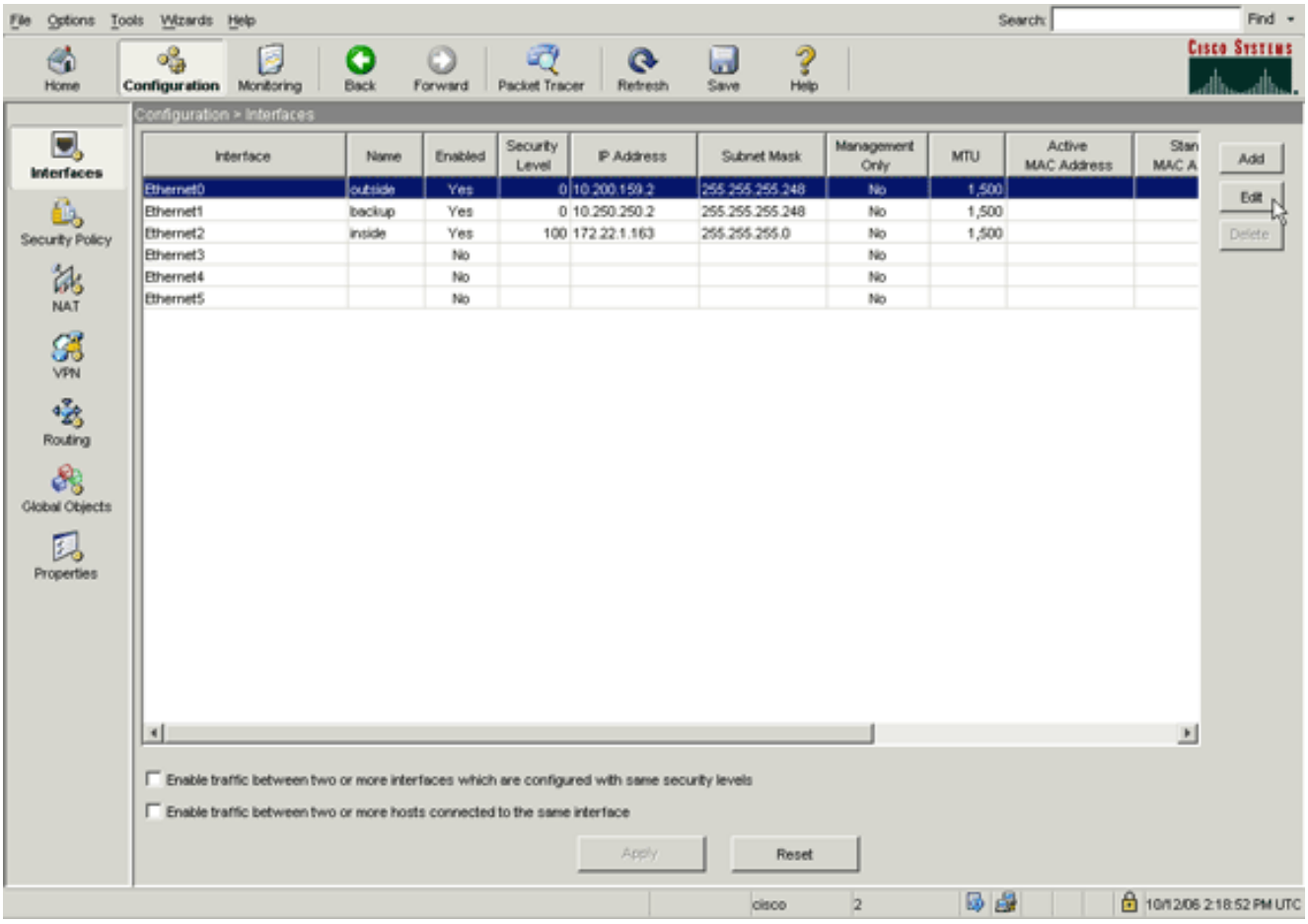
```
security-level 0 ip address 10.250.250.2 255.255.255.248
! interface Ethernet2 nameif inside security-level 100
ip address 172.22.1.163 255.255.255.0 ! interface
Ethernet3 shutdown no nameif no security-level no ip
address ! interface Ethernet4 shutdown no nameif no
security-level no ip address ! 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
```

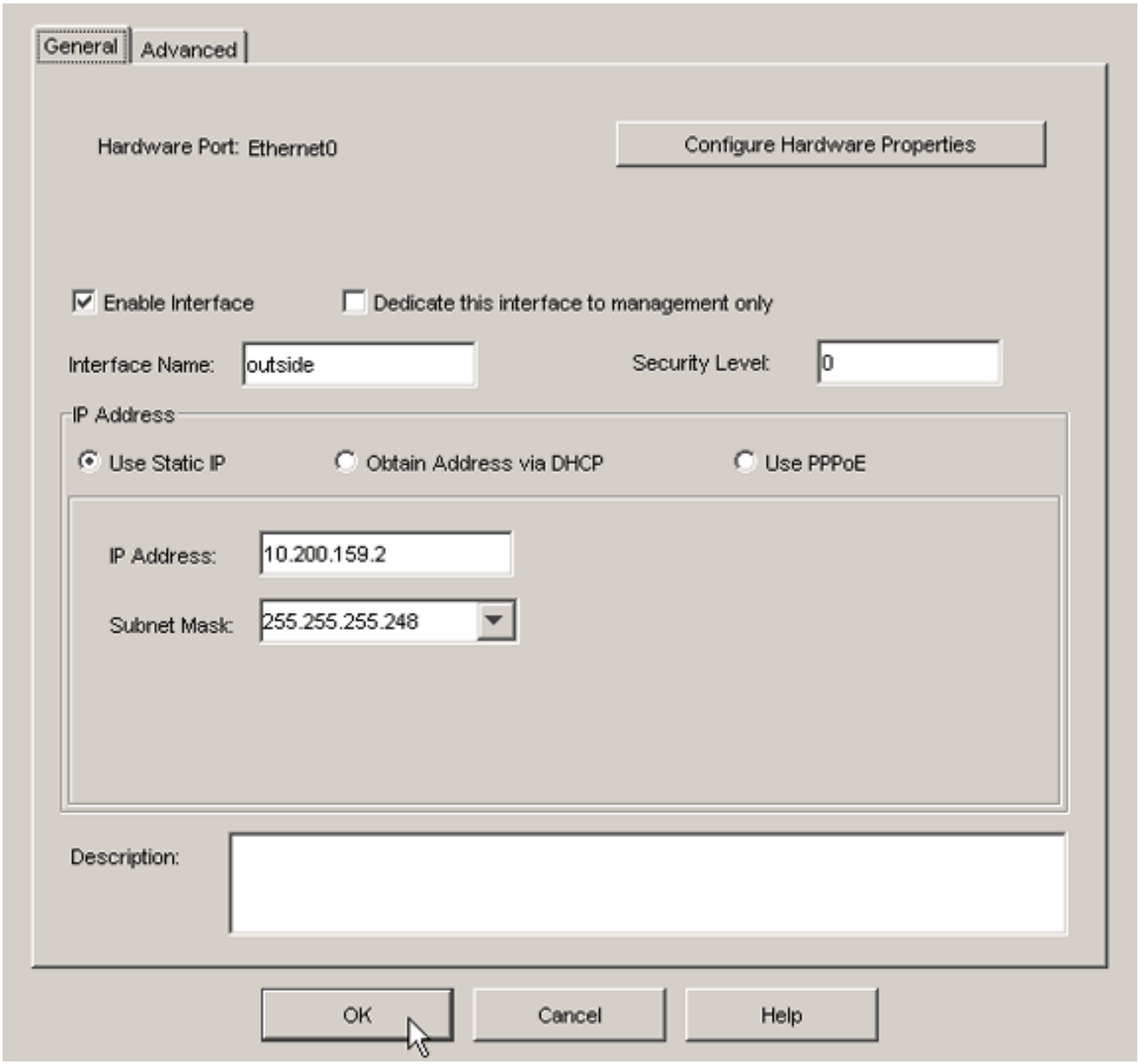
Configuración de ASDM

Para configurar el soporte redundante o de respaldo ISP con la aplicación ASDM, complete estos pasos:

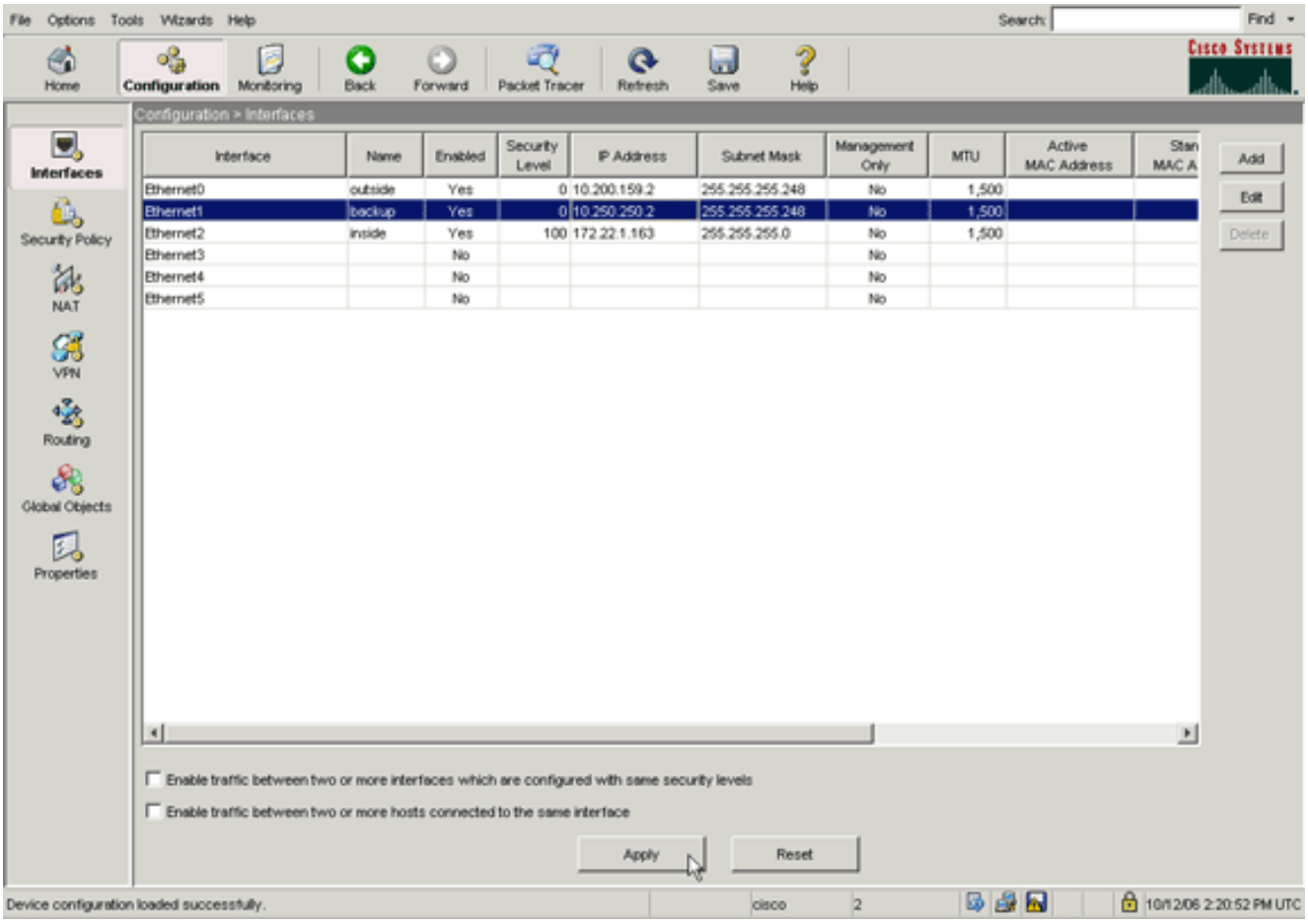
1. En la aplicación ASDM, haga clic en **Configuración**, y después haga clic en **Interfaces**



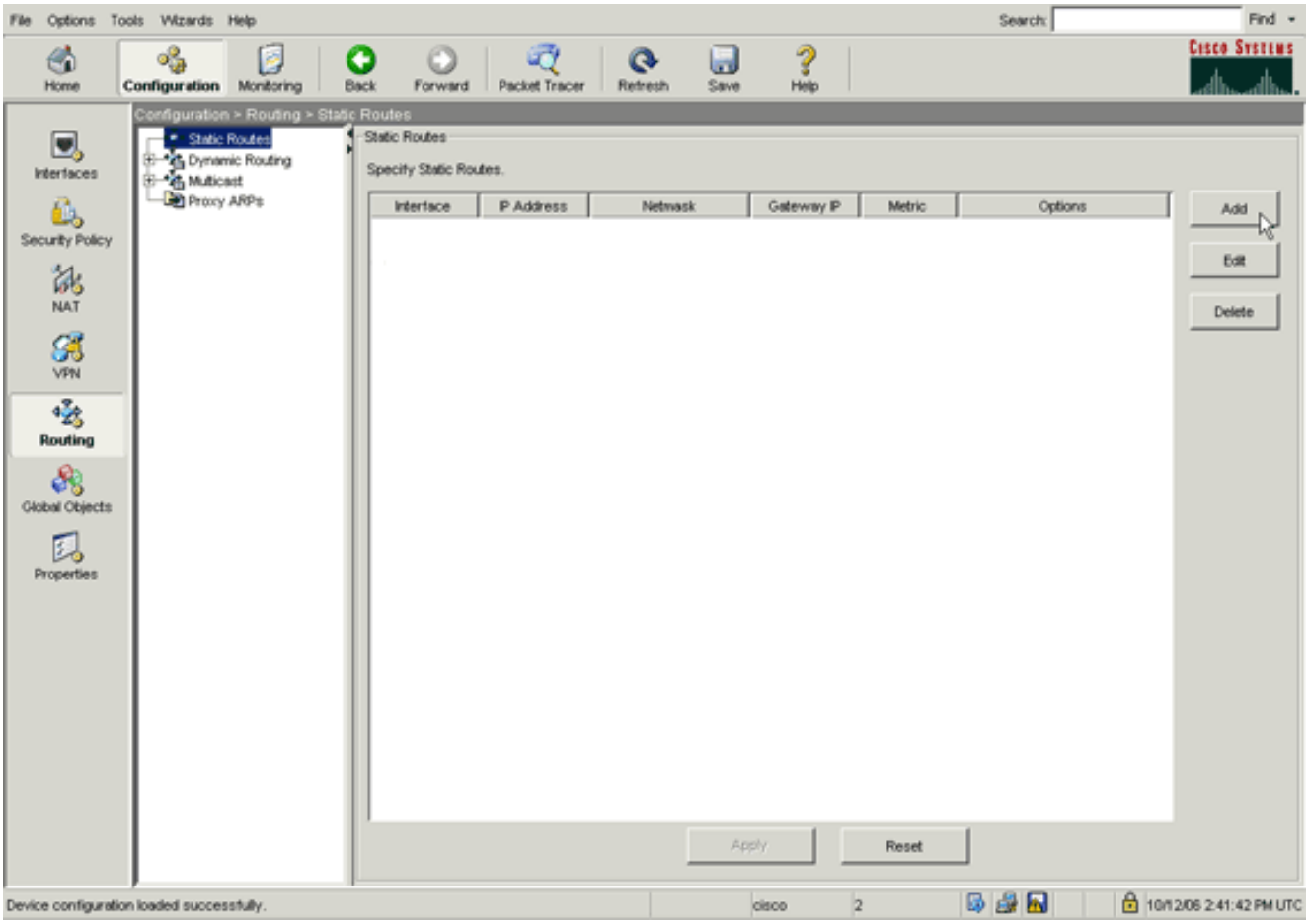
2. Desde la lista Interfaces, seleccione **Ethernet0** , y haga en **Editar**.Este cuadro de diálogo aparece.



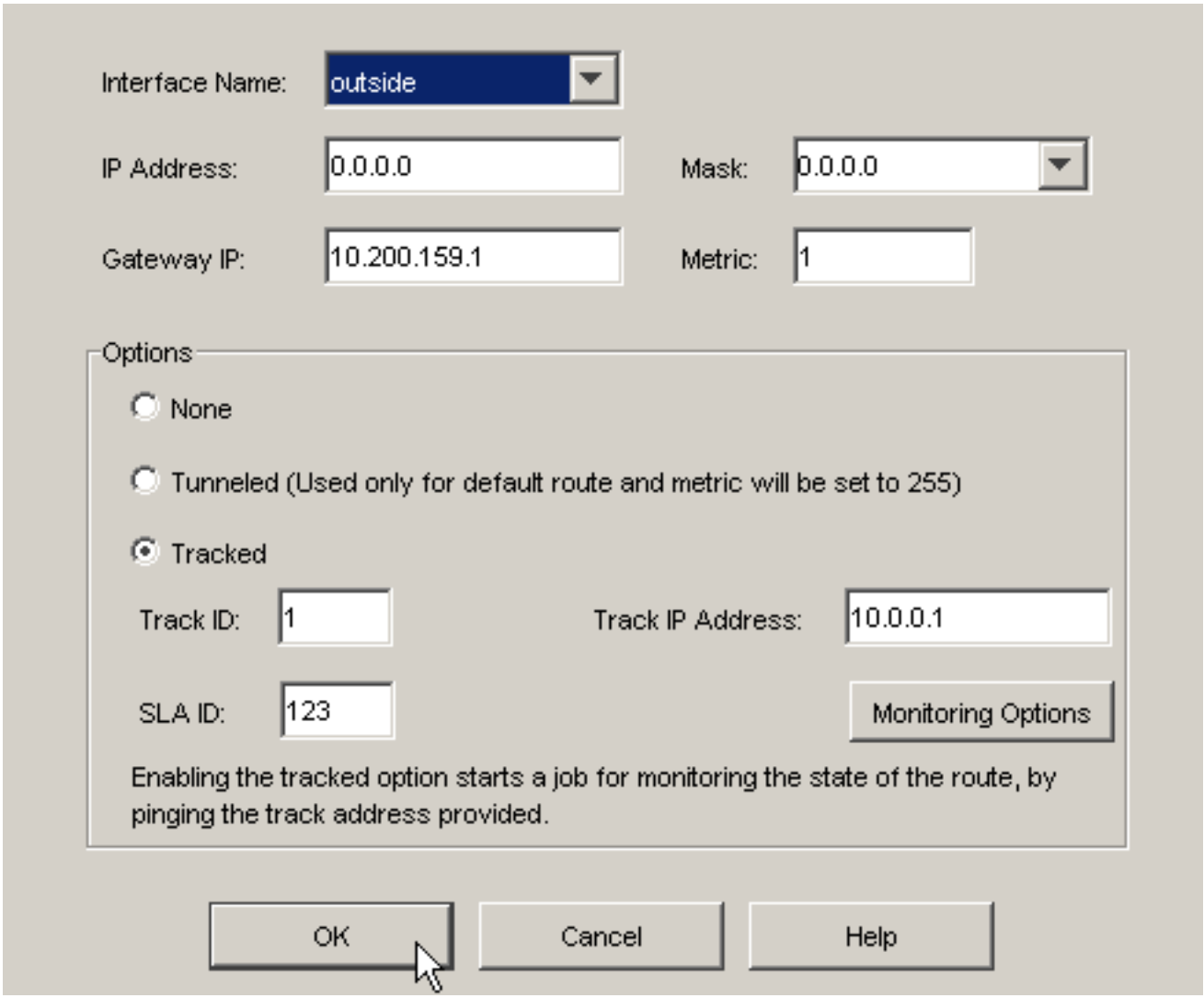
3. Marque la **casilla de verificación Interfaz**, e ingrese los valores en los campos Nombre de Interfaz, Nivel de Seguridad, Dirección IP, y Máscara de Subred.
4. Haga Click en OK para cerrar el cuadro de diálogo.
5. Configure otras interfaces según se requiera, y haga clic en **Aplicar** para actualizar la configuración de dispositivo de
seguridad.



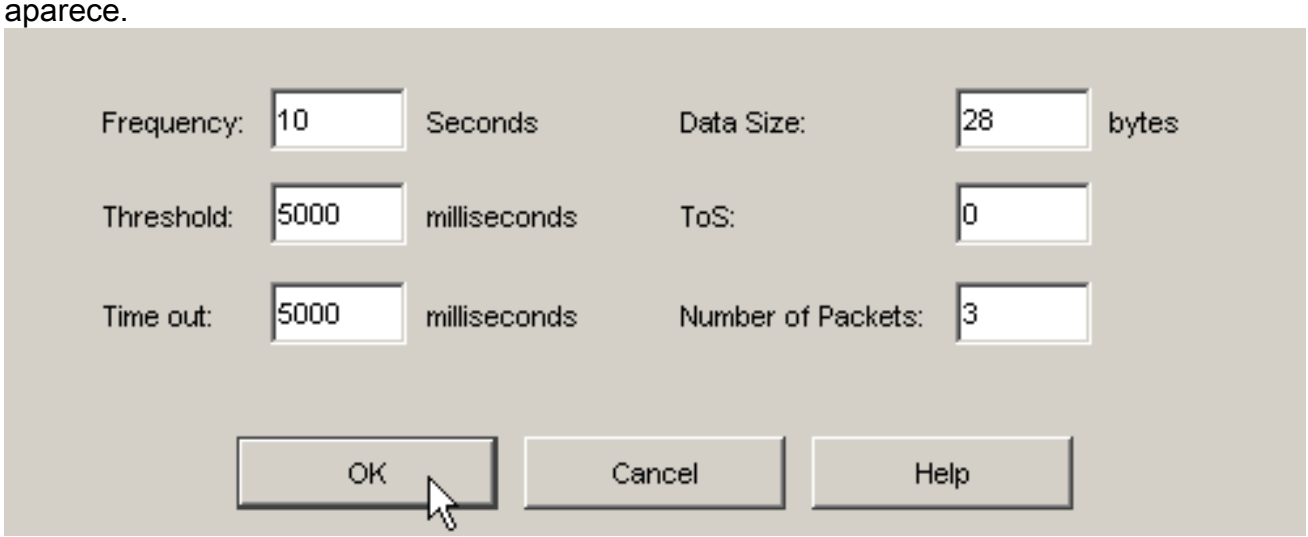
6. Haga clic en **Ruteo** ubicado en el lado izquierdo de la aplicación de ASDM.



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



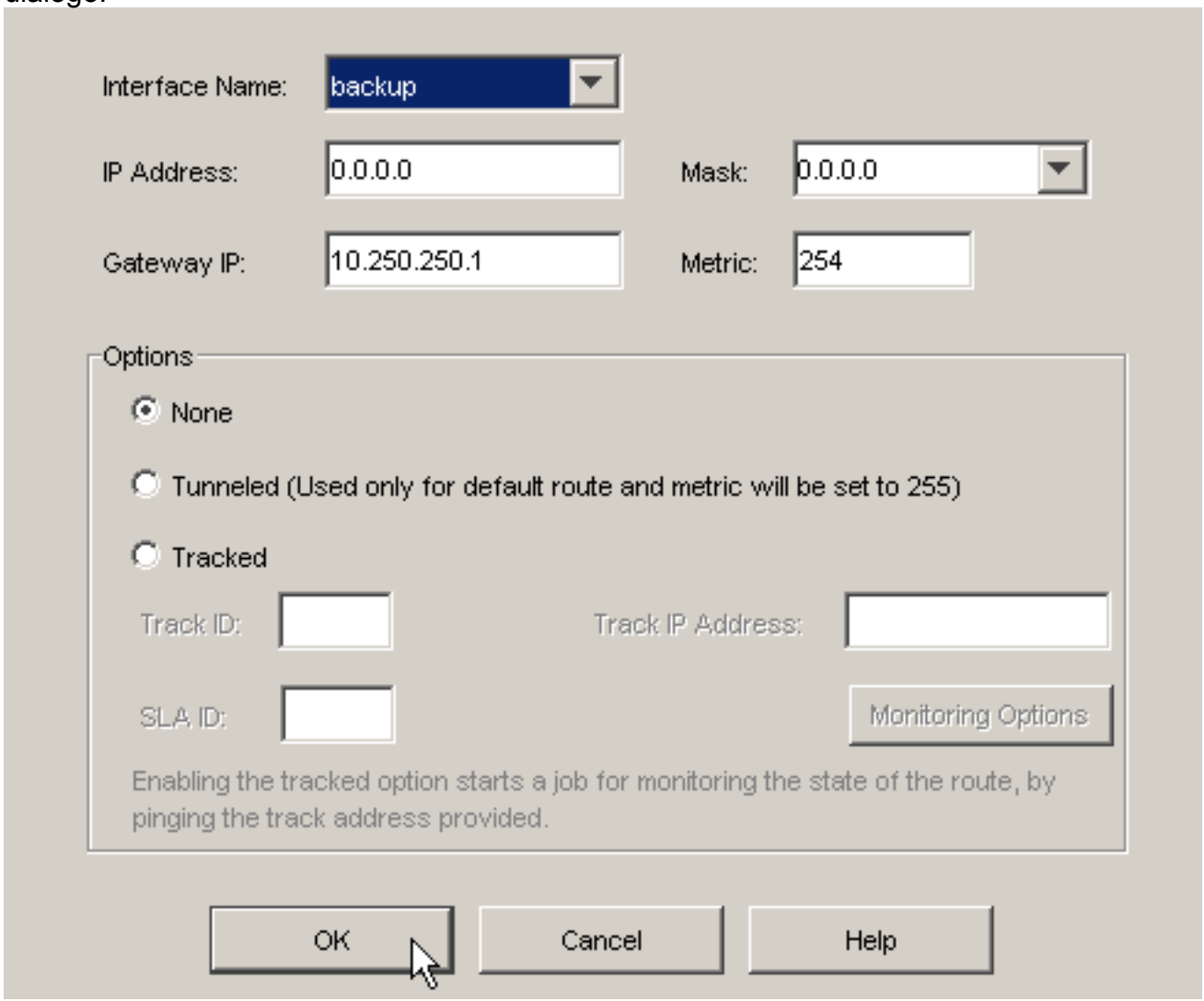
8. De la lista desplegable Nombre de la Interfaz, elija la interfaz en la cual la ruta reside, y configure la ruta predeterminada para alcanzar el gateway. En este ejemplo, 10.0.0.1 es el gateway de ISP primario, y el objeto de monitoreo con ecos ICMP.
9. En el área Opciones, Haga clic en el botón de opción **Localizado**, e ingrese los valores en los campos Seguimiento ID, SLA ID, y Dirección IP Seguimiento.
10. Haga clic en **Opciones de Monitoreo**.Este cuadro de diálogo aparece.



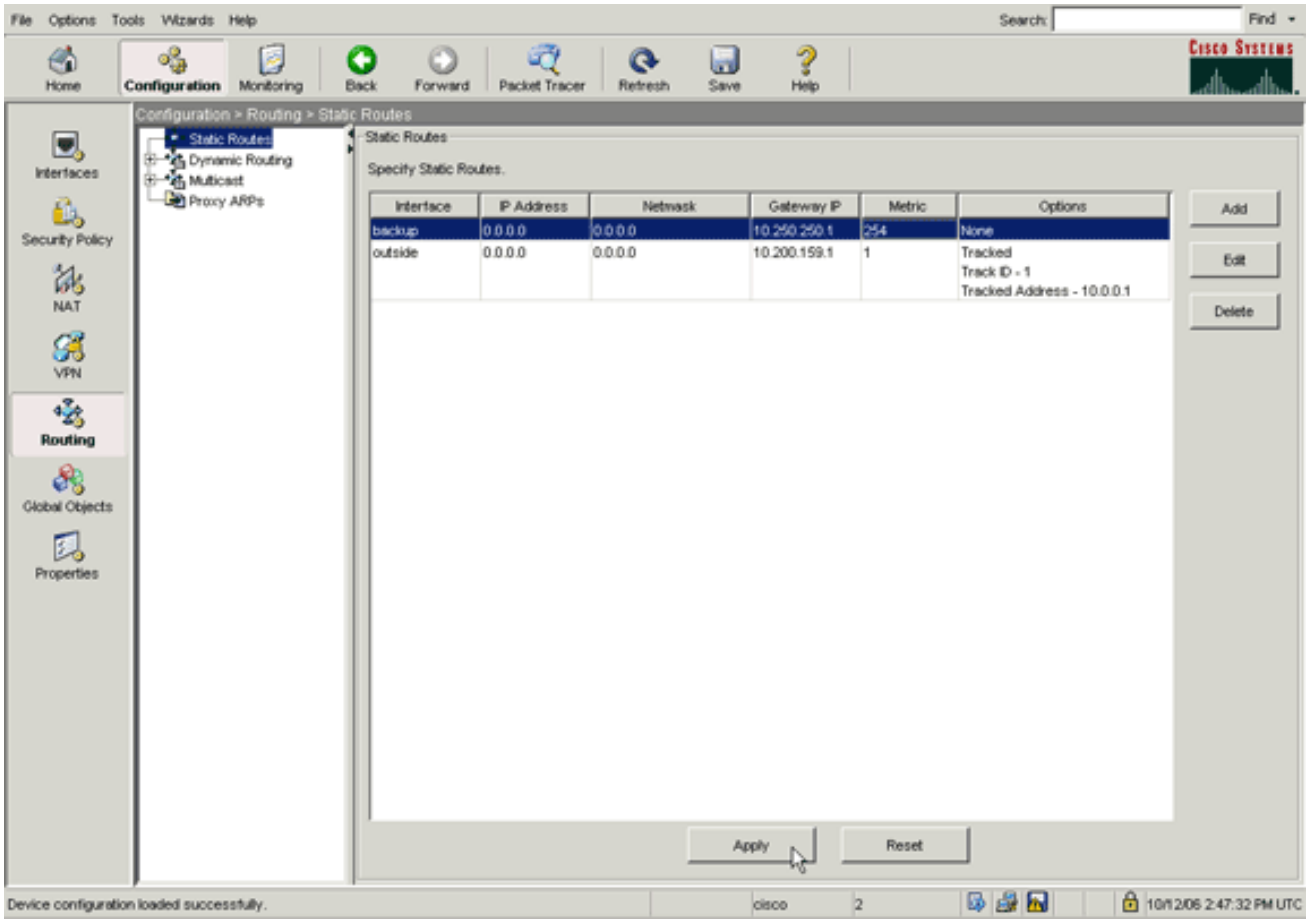
11. Ingrese los valores para la frecuencia y otras opciones de monitoreo, y haga clic en la **AUTORIZACIÓN**.
12. Agregue otra ruta estática para el ISP secundario para proporcionar una ruta y conectarse

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) en cambio, está instalada en la tabla de ruteo 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 haga clic en **Aplicar** para actualizar la configuración del dispositivo de seguridad.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Confirme que la Configuración esté Completo

Use estos comandos de **show** para verificar que su configuración esté completa.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **show running-config sla monitor** — Muestra los comandos SLA en la configuración.

```
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** — Muestra ajustes de configuración actual de la operación.

```
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** — Muestra las estadísticas operacionales de la operación SLA.Antes de que el ISP primario falle, éste es el estado operacional:

```
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
```

Después de que el ISP primario falle (y se agote el tiempo de espera de los ecos ICMP), éste es el estado operacional:

```
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
```

Confirme que la Ruta de Respaldo esté Instalada (el método CLI)

Use el comando **show route** para determinar cuando está instalada la ruta de respaldo.

- Antes de que el ISP primario falle, ésta es la tabla de ruteo:

```
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
```

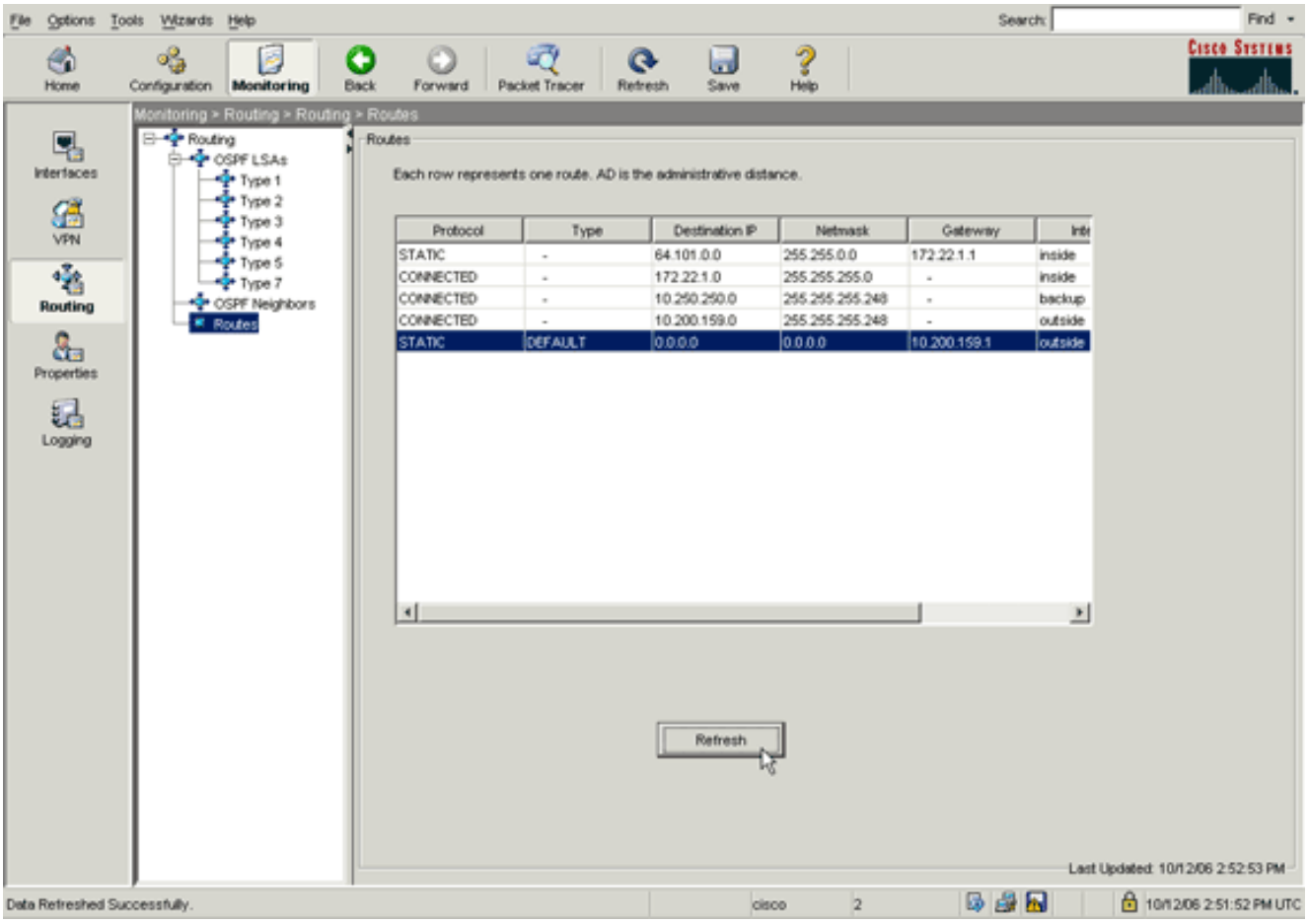
- Después de que el ISP primario falle, se quita la ruta estadística, y la ruta de seguridad está instalada, la siguiente es la tabla de ruteo:

```
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
```

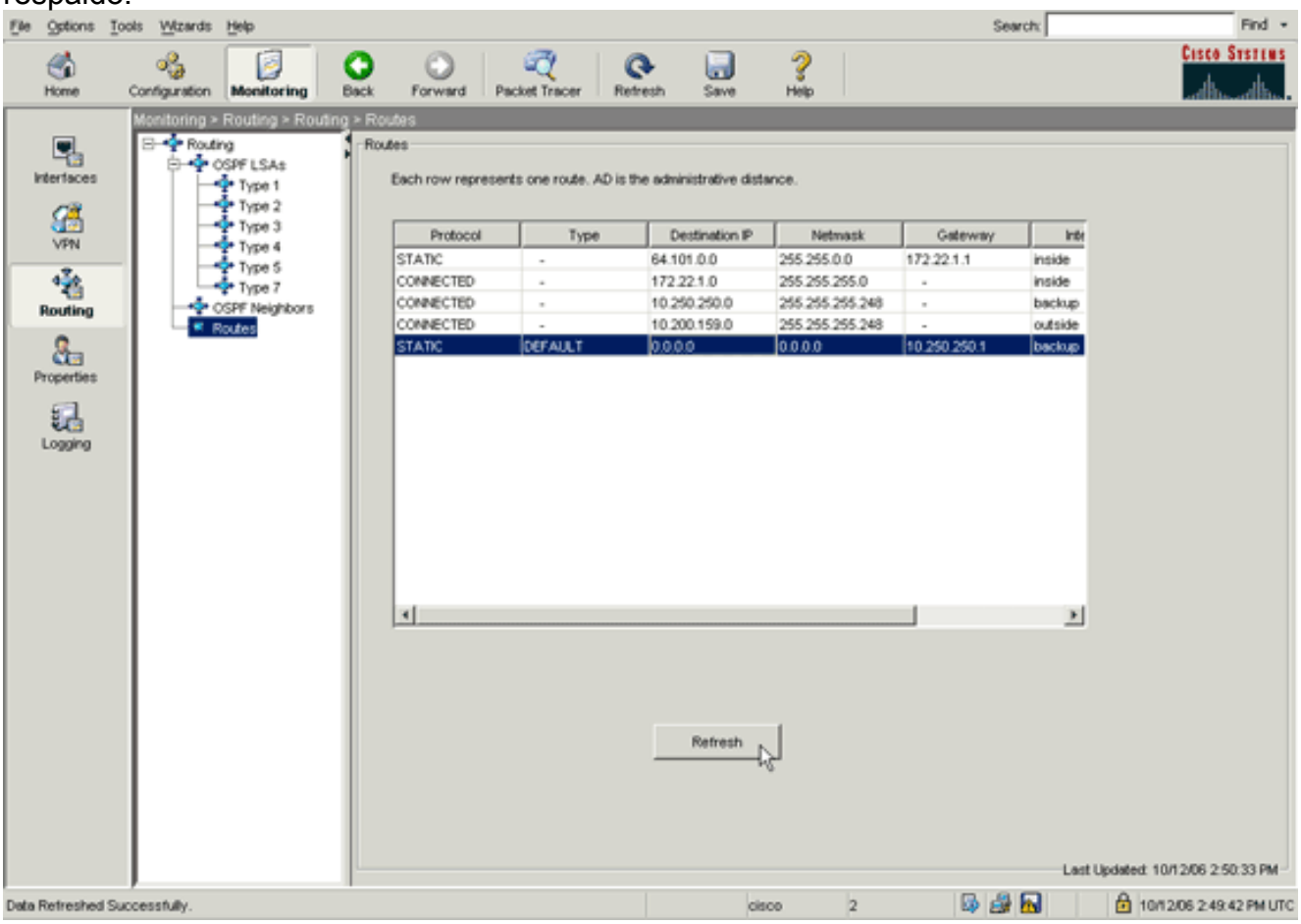
Confirme que la Ruta de Respaldo esté Instalada (el método del ASDM)

Para confirmar con el ASDM que la ruta de seguridad está instalada, complete estos pasos :

1. Haga clic en **Monitorear**, y después haga clic en la **Ruteo**.
2. Del Árbol de ruteo, elija **Rutas**.Antes de que el ISP primario falle, ésta es la tabla de ruteo:



La ruta PREDETERMINADA señala a 10.0.0.2 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 PREDETERMINADA ahora indica 10.250.250.1 a través de la interfaz de respaldo.



Troubleshooting

Comandos de Debug

- **debug sla monitor trace** — Muestra el progreso de la operación de eco.El objeto localizado (gateway del ISP primario) está activado, y los ecos ICMP tienen éxito.

```
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
```

  El objeto localizado (gateway del ISP primario) está desactivado, y los ecos ICMP fallan.

```
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** — Muestra los errores que el proceso de monitoreo SLA detecta.El objeto localizado (gateway del ISP primario) está activado, y ICMP tiene éxito.

```
%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
```

  Se quita el objeto localizado (gateway del ISP primario) está desactivado, y se quita la ruta localizada.

```
%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.
```

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 objetivo de monitoreo que esté más lejos que el gateway ISP, otra conexión en esa ruta puede fallar u otro dispositivo puede interferir. Esta configuración puede hacer que el monitoreo SLA indique que la la conexión al ISP primario ha fallado y hacer que dispositivo de seguridad falle innecesariamente en el 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 que son enviados por laoperación de monitoreo fallan, la ruta localizada primaria se quita, aunque el link ISP primario sigue estando 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 seguramente se interrumpirá.

SLA que monitorea en el ASA

Problema:

El monitorear de SLA no trabaja después de que el ASA sea actualización a la versión 8.0.

Solución:

El problema es sea posiblemente debido al comando del **trayecto inverso IP** configurado en la **interfaz exterior**. Quite el comando en el ASA e intente marcar monitorear de SLA.

Información Relacionada

- Configuración de Seguimiento de la Ruta Estática
- Referencia de Comandos de PIX/ASA 7.2
- Cisco ASA 5500 Series Security Appliances
- Dispositivos de seguridad Cisco PIX de la serie 500
- Soporte Técnico y Documentación - Cisco Systems