

Configurazione dell'ASA per i collegamenti ISP ridondanti o di backup

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Prodotti correlati](#)

[Premesse](#)

[Panoramica della funzione Tracciamento route statica](#)

[Suggerimenti importanti](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione CLI](#)

[Configurazione ASDM](#)

[Verifica](#)

[Confermare il completamento della configurazione](#)

[Confermare che la route di backup sia installata \(metodo CLI\)](#)

[Confermare che la route di backup sia installata \(metodo ASDM\)](#)

[Risoluzione dei problemi](#)

[Comandi debug](#)

[Route rilevata rimossa inutilmente](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare Cisco ASA serie 5500 Adaptive Security Appliance (ASA) per l'utilizzo della funzione di tracciamento statico del percorso in modo da consentire al dispositivo di utilizzare connessioni Internet ridondanti o di backup.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ASA serie 5555-X con software versione 9.x o successive
- Cisco ASDM versione 7.x o successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco ASA serie 5500 versione 9.1(5).

Nota: Per configurare la quarta interfaccia sull'appliance ASA serie 5505, è necessario usare il comando **backup interface**. Per ulteriori informazioni, consultare la sezione [backup interface](#) della *guida di riferimento dei comandi di Cisco Security Appliance, versione 7.2*.

Premesse

In questa sezione viene fornita una panoramica della funzione di tracciamento statico delle route descritta in questo documento, oltre a suggerimenti importanti prima di iniziare.

Panoramica della funzione Tracciamento route statica

Un problema relativo all'utilizzo delle route statiche è rappresentato dal fatto che non esiste alcun meccanismo intrinseco in grado di determinare se la route è verso l'alto o verso il basso. Il percorso rimane nella tabella di routing anche se il gateway dell'hop successivo non è più disponibile. Gli instradamenti statici vengono rimossi dalla tabella di routing solo se l'interfaccia associata sull'appliance di sicurezza non è attiva. Per risolvere questo problema, viene utilizzata una funzione di rilevamento statico della route per tenere traccia della disponibilità di una route statica. La feature rimuove la route statica dalla tabella di routing e la sostituisce con una route di backup in caso di errore.

Il rilevamento statico del percorso consente all'ASA di utilizzare una connessione a un ISP secondario a basso costo nel caso in cui la linea leasing principale non sia più disponibile. Per ottenere questa ridondanza, l'ASA associa una route statica a una destinazione di monitoraggio definita dall'utente. L'operazione SLA (Service Level Agreement) controlla la destinazione con richieste echo ICMP periodiche. Se non si riceve una risposta echo, l'oggetto viene considerato inattivo e la route associata viene rimossa dalla tabella di routing. Al posto della route rimossa viene utilizzata una route di backup configurata in precedenza. Mentre il percorso di backup è in uso, l'operazione di monitoraggio SLA continua i tentativi di raggiungere la destinazione di monitoraggio. Quando la destinazione è nuovamente disponibile, la prima route viene sostituita nella tabella di routing e la route di backup viene rimossa.

Nell'esempio riportato nel documento, l'appliance ASA mantiene due connessioni a Internet. La prima connessione è una linea affittata ad alta velocità a cui si accede tramite un router fornito dall'ISP primario. La seconda connessione è una DSL (Digital Subscriber Line) a velocità inferiore a cui si accede tramite un modem DSL fornito dall'ISP secondario.

Nota: La configurazione descritta in questo documento non può essere usata per il bilanciamento del carico o la condivisione del carico, in quanto non è supportata sull'appliance ASA. Utilizzare questa configurazione solo a scopo di backup o ridondanza. Il traffico in uscita utilizza l'ISP primario e quindi l'ISP secondario in caso di errore del primario. Il guasto dell'ISP primario causa un'interruzione temporanea del traffico.

La connessione DSL è inattiva finché la linea in leasing è attiva e il gateway ISP primario è raggiungibile. Tuttavia, se la connessione all'ISP primario non è attiva, l'ASA modifica la tabella di routing in modo da indirizzare il traffico alla connessione DSL. Per ottenere questa ridondanza, viene utilizzato il tracciamento statico del percorso.

L'ASA è configurata con una route statica che indirizza tutto il traffico Internet all'ISP primario. Ogni dieci secondi, il processo di monitoraggio degli SLA verifica che il gateway ISP primario sia raggiungibile. Se il processo di monitoraggio dello SLA determina che il gateway ISP primario non è raggiungibile, la route statica che indirizza il traffico a tale interfaccia viene rimossa dalla tabella di routing. Per sostituire la route statica, viene installata una route statica alternativa che indirizza il traffico all'ISP secondario. Questa route statica alternativa indirizza il traffico all'ISP secondario tramite il modem DSL finché non è raggiungibile il collegamento all'ISP primario.

Questa configurazione rappresenta un modo relativamente economico per garantire che l'accesso a Internet in uscita resti disponibile per gli utenti che usano l'ASA. Come descritto in questo documento, la configurazione potrebbe non essere adatta per l'accesso in entrata alle risorse dietro l'appliance ASA. Per ottenere connessioni in entrata senza problemi sono necessarie competenze di rete avanzate. Queste competenze non sono descritte nel presente documento.

Suggerimenti importanti

Prima di provare la configurazione descritta in questo documento, è necessario scegliere una destinazione di monitoraggio in grado di rispondere alle richieste echo ICMP (Internet Control Message Protocol). La destinazione può essere qualsiasi oggetto di rete scelto dall'utente, ma è consigliabile utilizzare una destinazione strettamente collegata al provider di servizi Internet (ISP). Di seguito sono riportati alcuni possibili obiettivi di monitoraggio:

- Indirizzo gateway ISP
- Altro indirizzo gestito da ISP
- Un server su un'altra rete, ad esempio un server di autenticazione, autorizzazione e accounting (AAA) con cui l'appliance ASA deve comunicare
- Un oggetto di rete permanente in un'altra rete (un computer desktop o notebook che è possibile arrestare di notte non è una buona scelta)

In questo documento si presume che l'ASA sia completamente operativa e configurata in modo da consentire a Cisco Adaptive Security Device Manager (ASDM) di apportare modifiche alla

configurazione.

Suggerimento: Per informazioni su come consentire all'ASDM di configurare il dispositivo, fare riferimento alla sezione [Configurazione dell'accesso HTTPS per ASDM](#) del *registro CLI 1: Guida alla configurazione della CLI per le operazioni generali della serie Cisco ASA, 9.1.*

Configurazione

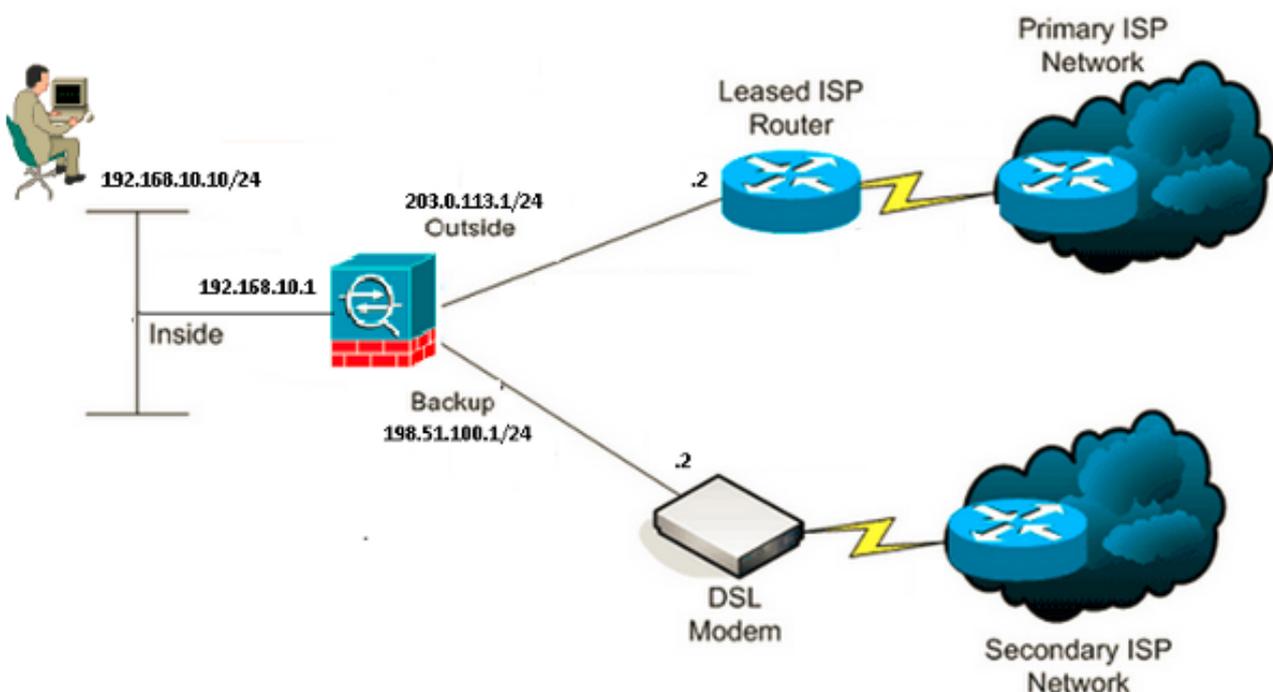
Usare le informazioni descritte in questa sezione per configurare l'ASA per l'uso della funzione di tracciamento statico della route.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca dei comandi](#) (solo utenti [registrati](#)).

Nota: Gli indirizzi IP utilizzati in questa configurazione non sono legalmente indirizzabili su Internet. Si tratta degli indirizzi [RFC 1918](#) utilizzati in un ambiente lab.

Esempio di rete

L'esempio fornito in questa sezione utilizza la seguente configurazione della rete:



Configurazione CLI

Per configurare l'ASA dalla [CLI](#), usare queste informazioni:

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.

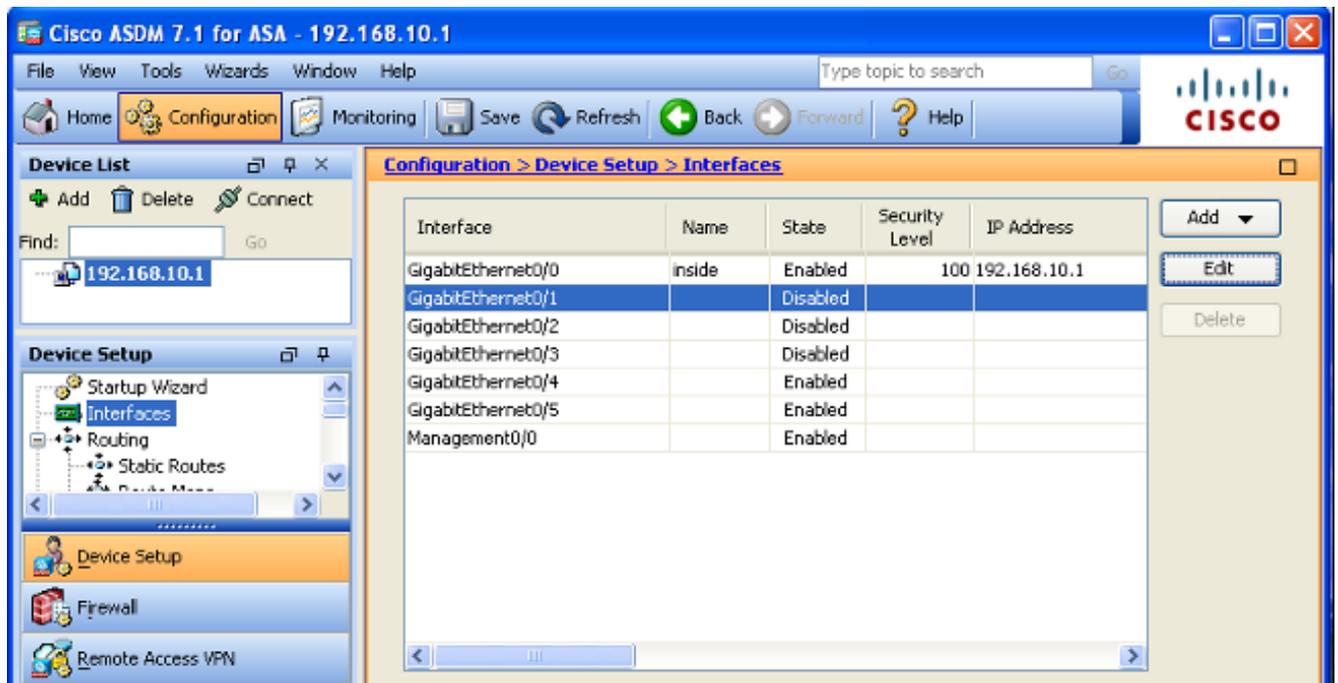
```

```
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
```

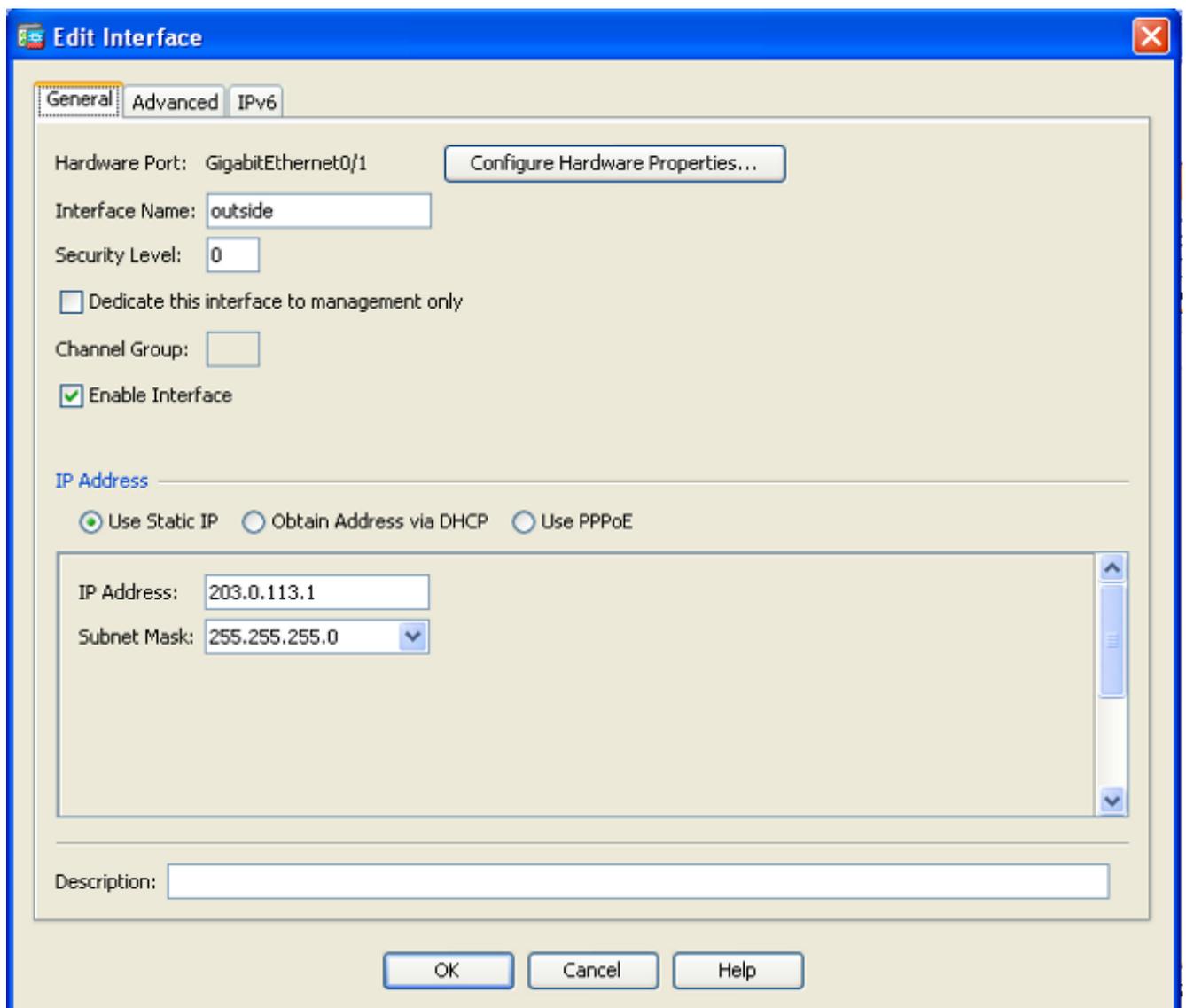
Configurazione ASDM

Completare questa procedura per configurare il supporto di ISP ridondanti o di backup con l'applicazione [ASDM](#):

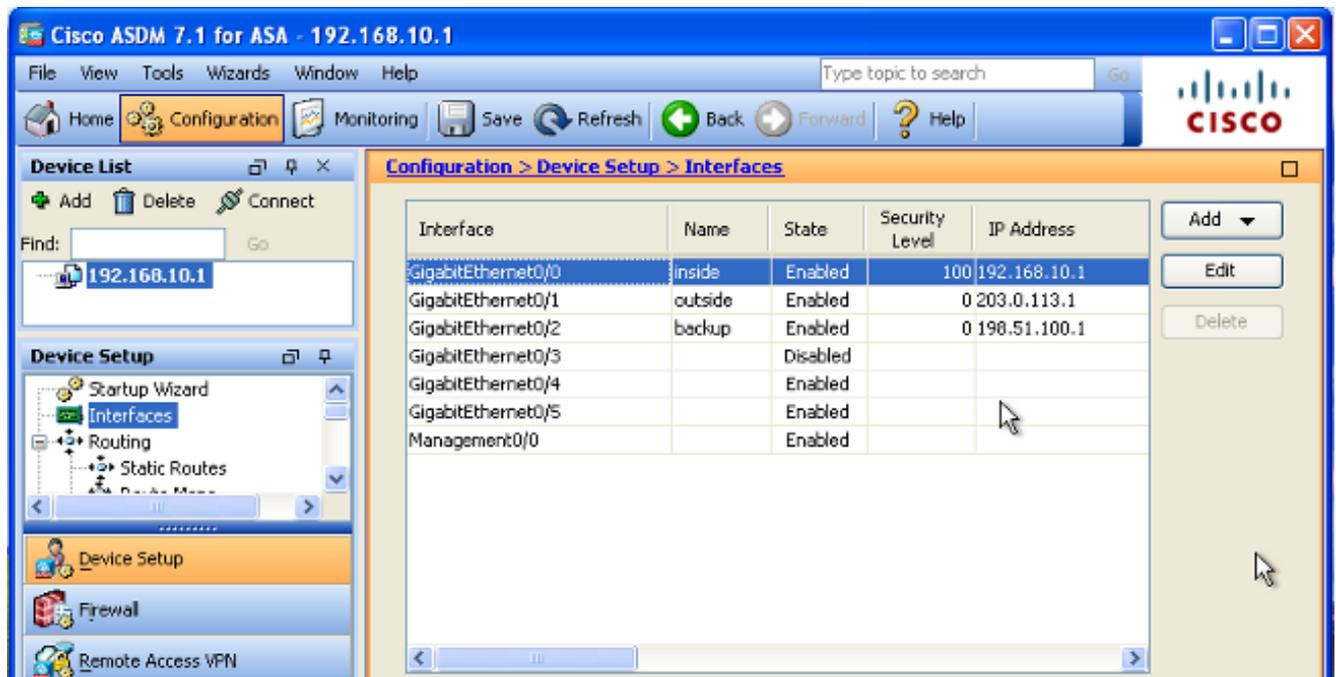
1. Nell'applicazione ASDM, fare clic su **Configurazione**, quindi su **Interfacce**.



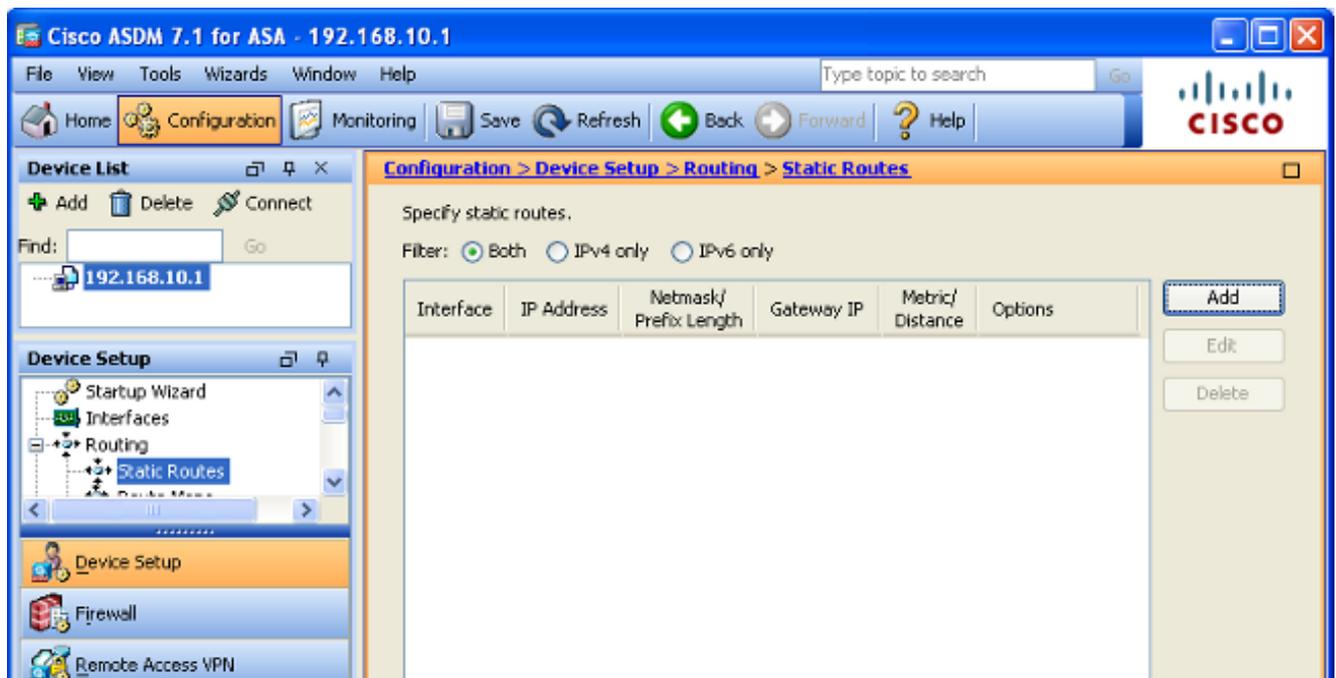
2. Selezionare **Gigabit Ethernet0/1** dall'elenco Interfacce, quindi fare clic su **Modifica**. Viene visualizzata la seguente finestra di dialogo:



3. Selezionare la casella di controllo **Abilita interfaccia** e immettere i valori appropriati nei campi *Nome interfaccia*, *Livello di protezione*, *Indirizzo IP* e *Subnet mask*.
4. Per chiudere la finestra di dialogo, fare clic su **OK**.
5. Configurare le altre interfacce come necessario, quindi fare clic su **Apply** per aggiornare la configurazione dell'ASA:



6. Selezionare **Routing** e fare clic su **Static Routing** sul lato sinistro dell'applicazione ASDM:



7. Per aggiungere le nuove route statiche, fare clic su **Add** (Aggiungi). Viene visualizzata la seguente finestra di dialogo:

Edit Static Route

IP Address Type: IPv4 IPv6

Interface:

Network:

Gateway IP: Metric:

Options

None

Tunneled (Default tunnel gateway for VPN traffic)

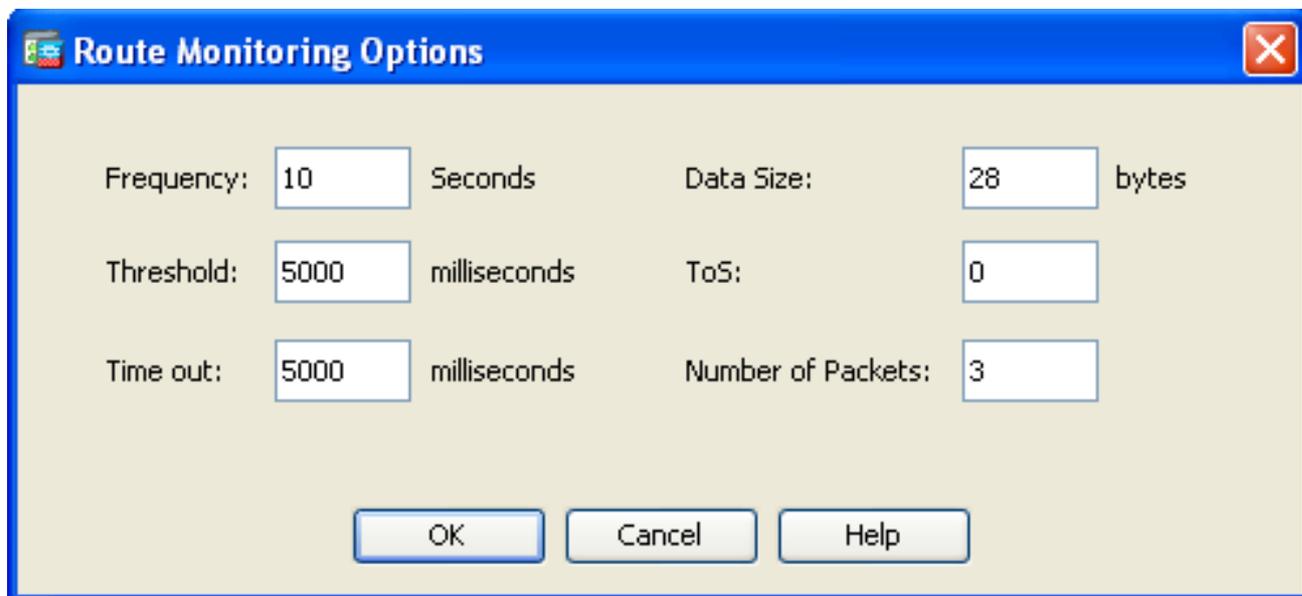
Tracked

Track ID: Track IP Address:

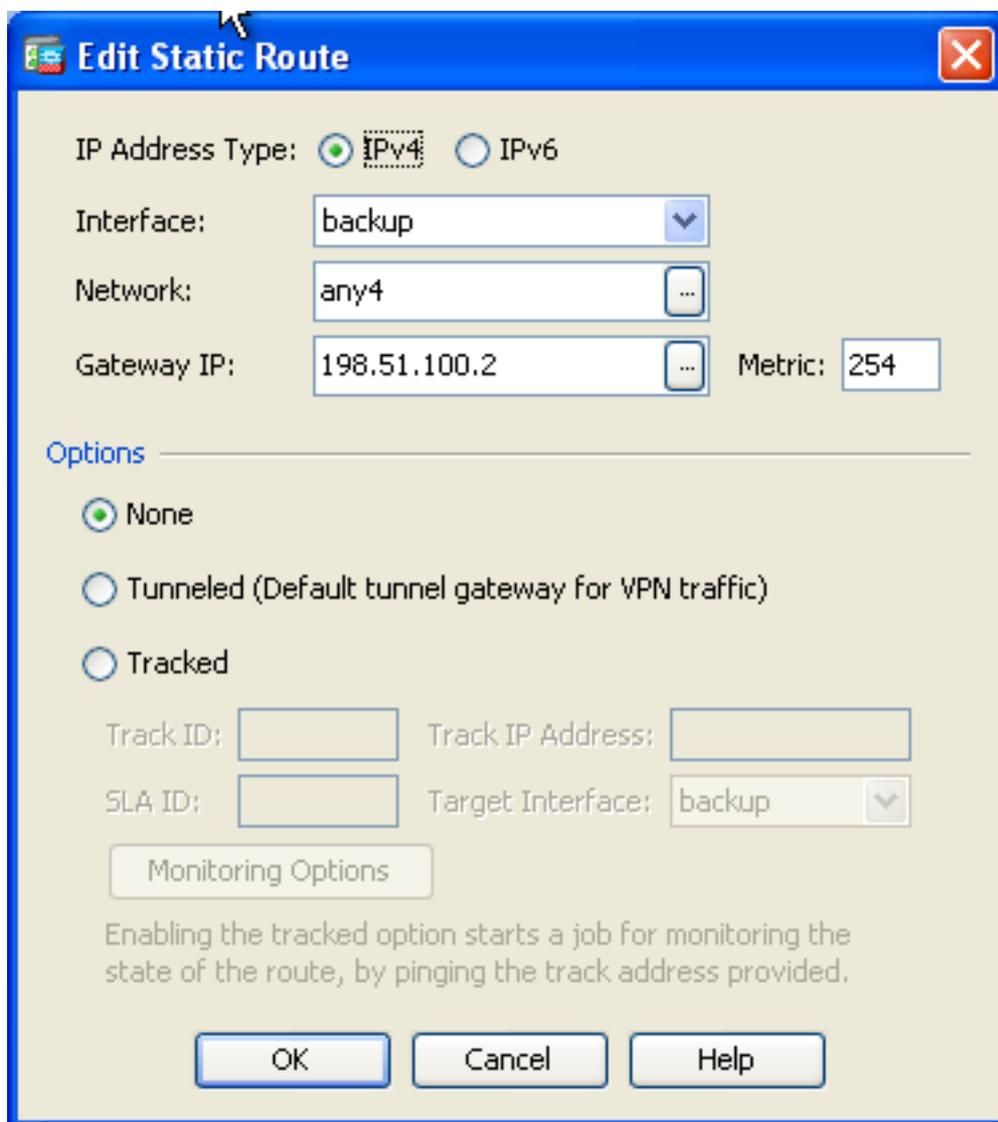
SLA ID: Target Interface:

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

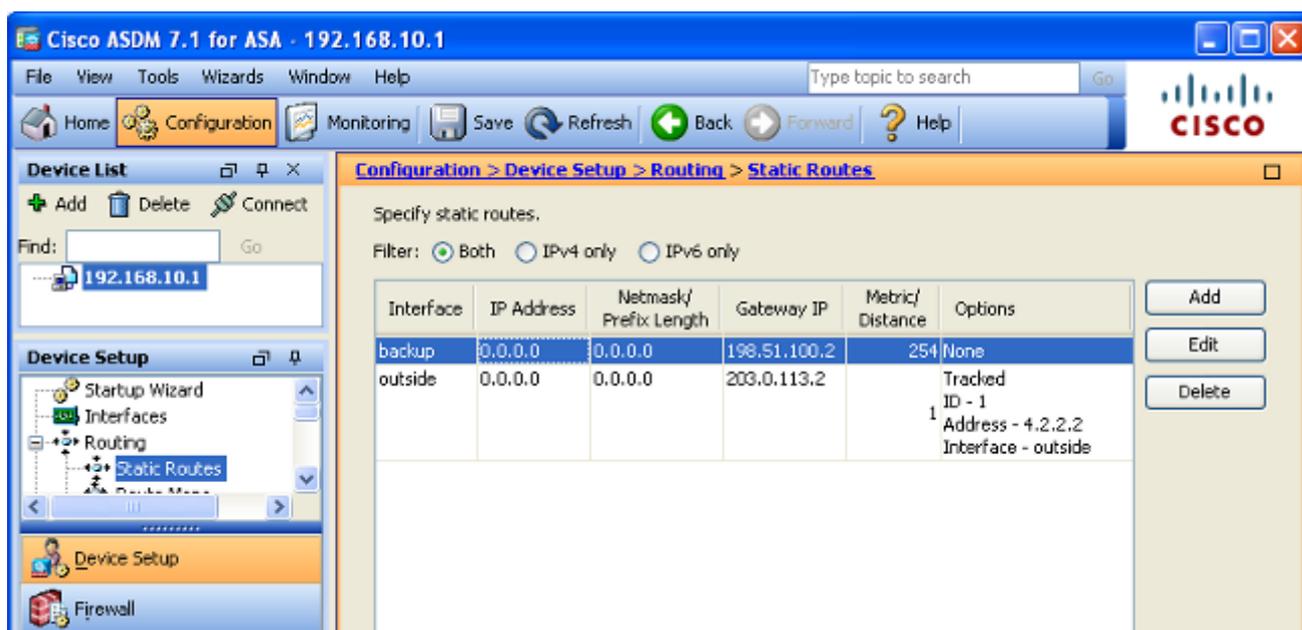
8. Dall'elenco a discesa Interface Name (Nome interfaccia), scegliere l'interfaccia su cui risiede la route e configurare la route predefinita per raggiungere il gateway. Nell'esempio, **203.0.113.2** è il gateway ISP primario e **4.2.2.2** è l'oggetto da monitorare con gli echi ICMP.
9. Nell'area Opzioni, fare clic sul pulsante di scelta **Tracciato** e immettere i valori appropriati nei campi *Track ID*, *SLA ID* e *Track IP Address*.
10. Fare clic su **Opzioni di monitoraggio**. Viene visualizzata la seguente finestra di dialogo:



11. Immettere i valori appropriati per la frequenza e le altre opzioni di controllo, quindi fare clic su **OK**.
12. Aggiungere un'altra route statica per l'ISP secondario in modo da fornire una route per raggiungere Internet. Per renderla una route secondaria, configurarla con una metrica più alta, ad esempio 254. Se la route primaria (ISP primario) ha esito negativo, verrà rimossa dalla tabella di routing. Questo percorso secondario (ISP secondario) viene invece installato nella tabella di routing di Private Internet Exchange (PIX).
13. Per chiudere la finestra di dialogo, fare clic su **OK**:



Le configurazioni vengono visualizzate nell'elenco Interfaccia:



14. Selezionare la configurazione di routing e fare clic su **Apply** per aggiornare la configurazione dell'ASA.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Confermare il completamento della configurazione

Nota: Lo [strumento Output Interpreter \(solo utenti registrati\)](#) supporta alcuni comandi `show`. Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando `show`.

Per verificare che la configurazione sia stata completata, usare i seguenti comandi `show`:

- **show running-config sla monitor:** l'output di questo comando visualizza i comandi SLA nella configurazione.

```
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:** l'output di questo comando visualizza le impostazioni di configurazione correnti dell'operazione.

```
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 operating-state:** l'output di questo comando visualizza le statistiche operative dell'operazione SLA.

Prima che l'ISP primario abbia esito negativo, questo è lo stato operativo:

```
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
```

Quando l'ISP primario ha esito negativo (e l'ICMP indica un timeout), lo stato operativo è il seguente:

```
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
```

Confermare che la route di backup sia installata (metodo CLI)

Immettere il comando **show route** per confermare che la route di backup sia installata.

Prima che l'ISP principale abbia esito negativo, la tabella di routing è simile alla seguente:

```
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
```

Se si verifica un errore nell'ISP primario, la route statica viene rimossa e la route di backup viene

installata, la tabella di routing sarà simile alla seguente:

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

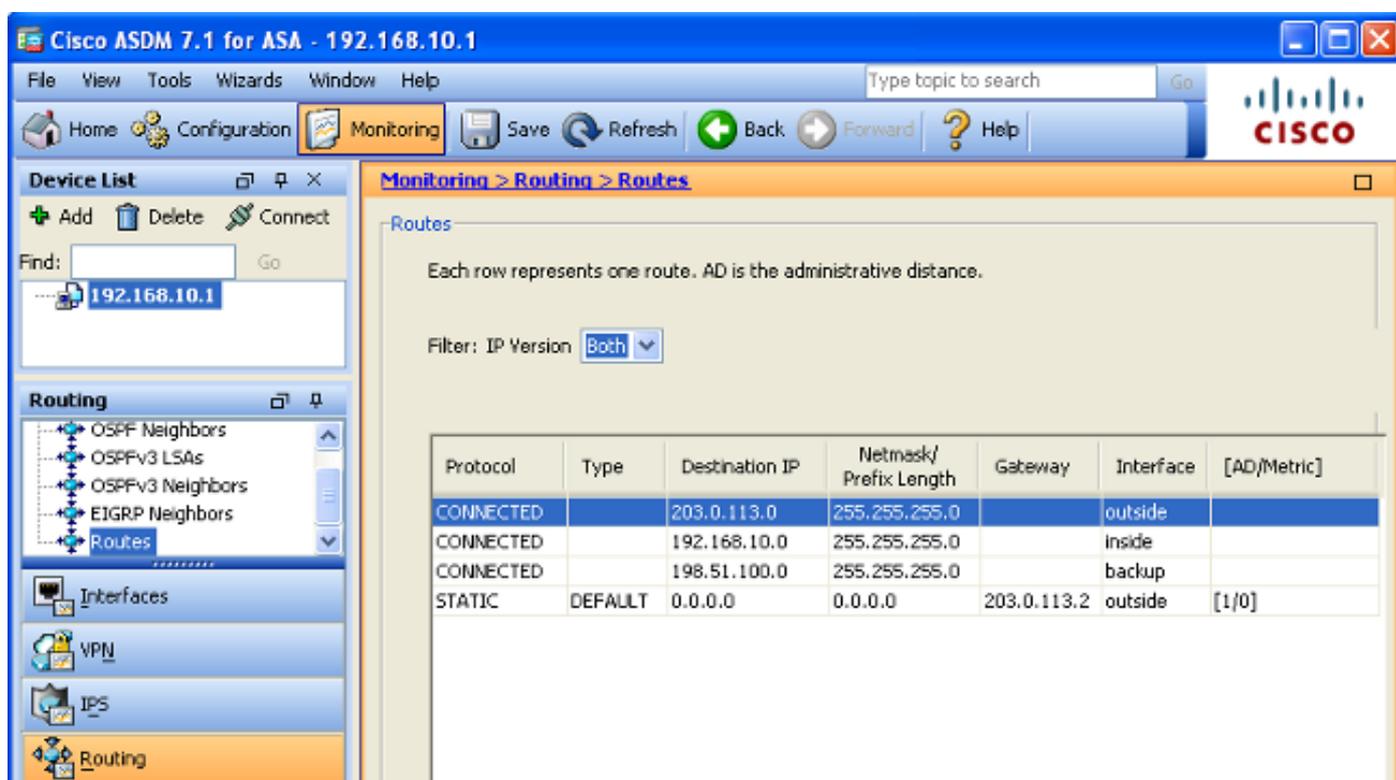
Gateway of last resort is 198.51.100.2 to network 0.0.0.0

```
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
```

Confermare che la route di backup sia installata (metodo ASDM)

Per verificare che il percorso di backup sia installato tramite ASDM, selezionare **Monitoraggio > Instradamento**, quindi scegliere **Instradamenti** dalla struttura Instradamento.

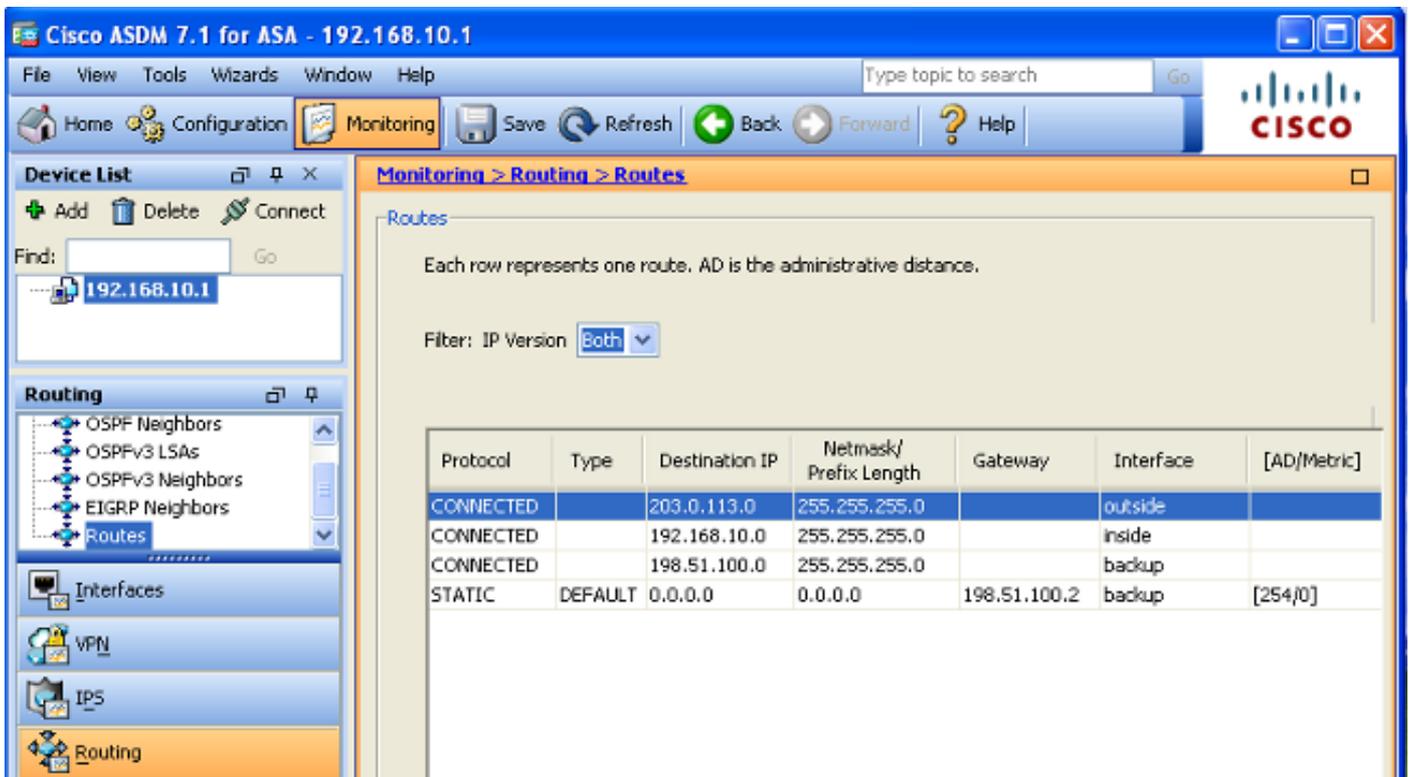
Prima che l'ISP primario abbia esito negativo, la tabella di routing è simile a quella illustrata nell'immagine seguente. Il percorso **DEFAULT** punta a **203.0.113.2** attraverso l'interfaccia **esterna**:



The screenshot shows the Cisco ASDM 7.1 for ASA interface. The 'Monitoring > Routing > Routes' window is open, displaying a table of routes. The table has the following columns: Protocol, Type, Destination IP, Netmask/Prefix Length, Gateway, Interface, and [AD/Metric].

Protocol	Type	Destination IP	Netmask/Prefix Length	Gateway	Interface	[AD/Metric]
CONNECTED		203.0.113.0	255.255.255.0		outside	
CONNECTED		192.168.10.0	255.255.255.0		inside	
CONNECTED		198.51.100.0	255.255.255.0		backup	
STATIC	DEFAULT	0.0.0.0	0.0.0.0	203.0.113.2	outside	[1/0]

Se si verifica un errore nell'ISP primario, la route viene rimossa e viene installata la route di backup. Il percorso **PREDEFINITO** punta ora a **198.51.100.2** tramite l'interfaccia **di backup**:



Risoluzione dei problemi

In questa sezione vengono forniti alcuni utili comandi di debug e viene descritto come risolvere un problema quando la route rilevata viene rimossa inutilmente.

Comandi debug

È possibile usare questi comandi di debug per risolvere i problemi di configurazione:

- **debug sla monitor trace:** l'output di questo comando visualizza lo stato dell'operazione echo.

Se l'oggetto rilevato (gateway ISP primario) è attivo e gli echi ICMP hanno esito positivo, l'output sarà simile al seguente:

```
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
```

Se l'oggetto rilevato (gateway ISP primario) è inattivo e gli echi ICMP hanno esito negativo, l'output sarà simile al seguente:

```
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:** l'output di questo comando visualizza gli errori rilevati dal processo di

monitoraggio SLA.

Se l'oggetto rilevato (gateway ISP primario) è attivo e l'ICMP ha esito positivo, l'output sarà simile al seguente:

```
%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
```

Se l'oggetto rilevato (gateway ISP primario) è inattivo e la route rilevata viene rimossa, l'output sarà simile al seguente:

```
%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.

Route rilevata rimossa inutilmente

Se la route rilevata viene rimossa inutilmente, verificare che la destinazione di monitoraggio sia sempre disponibile per la ricezione di richieste echo. Verificare inoltre che lo stato della destinazione di monitoraggio, ovvero se la destinazione è raggiungibile o meno, sia strettamente correlato allo stato della connessione all'ISP primario.

Se si sceglie una destinazione di monitoraggio più lontana del gateway ISP, è possibile che un altro collegamento lungo tale percorso non riesca o che un altro dispositivo interferisca. Questa configurazione potrebbe causare la conclusione da parte del monitoraggio dello SLA che la connessione all'ISP primario non è riuscita e causare il failover inutilmente dell'ASA sul collegamento dell'ISP secondario.

Ad esempio, se si sceglie un router per filiali come destinazione di monitoraggio, la connessione dell'ISP alla filiale potrebbe non riuscire, così come qualsiasi altro collegamento. Se gli echi ICMP inviati dall'operazione di monitoraggio hanno esito negativo, il percorso principale tracciato viene rimosso, anche se il collegamento all'ISP primario è ancora attivo.

Nell'esempio, il gateway ISP primario utilizzato come destinazione di monitoraggio è gestito dall'ISP e si trova sull'altro lato del collegamento dell'ISP. Questa configurazione garantisce che se gli echi ICMP inviati dall'operazione di monitoraggio hanno esito negativo, il collegamento all'ISP è quasi sicuramente inattivo.

Informazioni correlate

- [Cisco ASA serie 5500-X Next-Generation Firewall](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)