ASA/PIX 7.x: Esempio di configurazione dei collegamenti ISP ridondanti o di backup

Sommario

Introduzione

Un problema con le route statiche è che non esiste alcun meccanismo intrinseco per 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 funzionalità di rilevamento statico della route per tenere traccia della disponibilità di una route statica e, se la route ha esito negativo, rimuoverla dalla tabella di routing e sostituirla con una route di backup.

In questo documento viene illustrato come usare la funzione di tracciamento statico del percorso su un'appliance di sicurezza PIX serie 5500 o su un'appliance di sicurezza adattiva ASA serie 5500 per abilitare il dispositivo a usare connessioni Internet ridondanti o di backup. Nell'esempio, il rilevamento statico dei percorsi consente all'accessorio di protezione di utilizzare una connessione a basso costo a un provider di servizi Internet (ISP) secondario nel caso in cui la linea principale

non sia più disponibile.

Per ottenere questa ridondanza, l'accessorio di sicurezza associa un percorso statico a una destinazione di monitoraggio definita dall'utente. L'operazione SLA (Service Level Agreement) monitora la destinazione con richieste echo periodiche ICMP (Internet Control Message Protocol). 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 a tentare 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.

Nota: la configurazione descritta in questo documento non può essere usata per il bilanciamento del carico o la condivisione del carico perché non è supportata su ASA/PIX. 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.

Prerequisiti

Requisiti

Scegliere una destinazione di monitoraggio in grado di rispondere alle richieste echo ICMP. La destinazione può essere qualsiasi oggetto di rete scelto dall'utente, ma è consigliabile utilizzare una destinazione strettamente collegata alla connessione ISP. Alcuni possibili obiettivi di monitoraggio includono:

- Indirizzo gateway ISP
- Altro indirizzo gestito da ISP
- Un server su un'altra rete, ad esempio un server AAA, con cui l'appliance di sicurezza 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'appliance di sicurezza sia completamente operativa e configurata per consentire a Cisco ASDM di apportare modifiche alla configurazione.

Nota: per informazioni su come consentire all'ASDM di configurare il dispositivo, fare riferimento a Consenti accesso HTTPS per ASDM.

Componenti usati

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

- Cisco PIX Security Appliance 515E con software versione 7.2(1) o successive
- Cisco Adaptive Security Device Manager 5.2(1) o versioni 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 Security Appliance versione 7.2(1).

Nota: per configurare la quarta interfaccia sull'appliance ASA 5505, è necessario usare il comando **backup interface**. Per ulteriori informazioni, fare riferimento a interfaccia di backup.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

In questo esempio l'accessorio di protezione 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 linea DSL (Digital Subscriber Line) a velocità inferiore a cui si accede tramite un modem DSL fornito dall'ISP secondario.

Nota: in questo esempio il bilanciamento del carico non viene eseguito.

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 principale non è attiva, l'appliance di sicurezza modifica la tabella di routing in modo da indirizzare il traffico alla connessione DSL. Per ottenere questa ridondanza, viene utilizzato il tracciamento statico delle route.

L'appliance di sicurezza è configurata con un percorso statico che indirizza tutto il traffico Internet all'ISP primario. Ogni 10 secondi il processo di monitoraggio dello 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 rimanga disponibile per gli utenti che si trovano dietro l'appliance di sicurezza. Come descritto in questo documento, questa impostazione potrebbe non essere adatta per l'accesso in entrata alle risorse dietro l'appliance di sicurezza. Per ottenere connessioni in entrata senza problemi sono necessarie competenze di rete avanzate. Queste competenze non sono descritte nel presente documento.

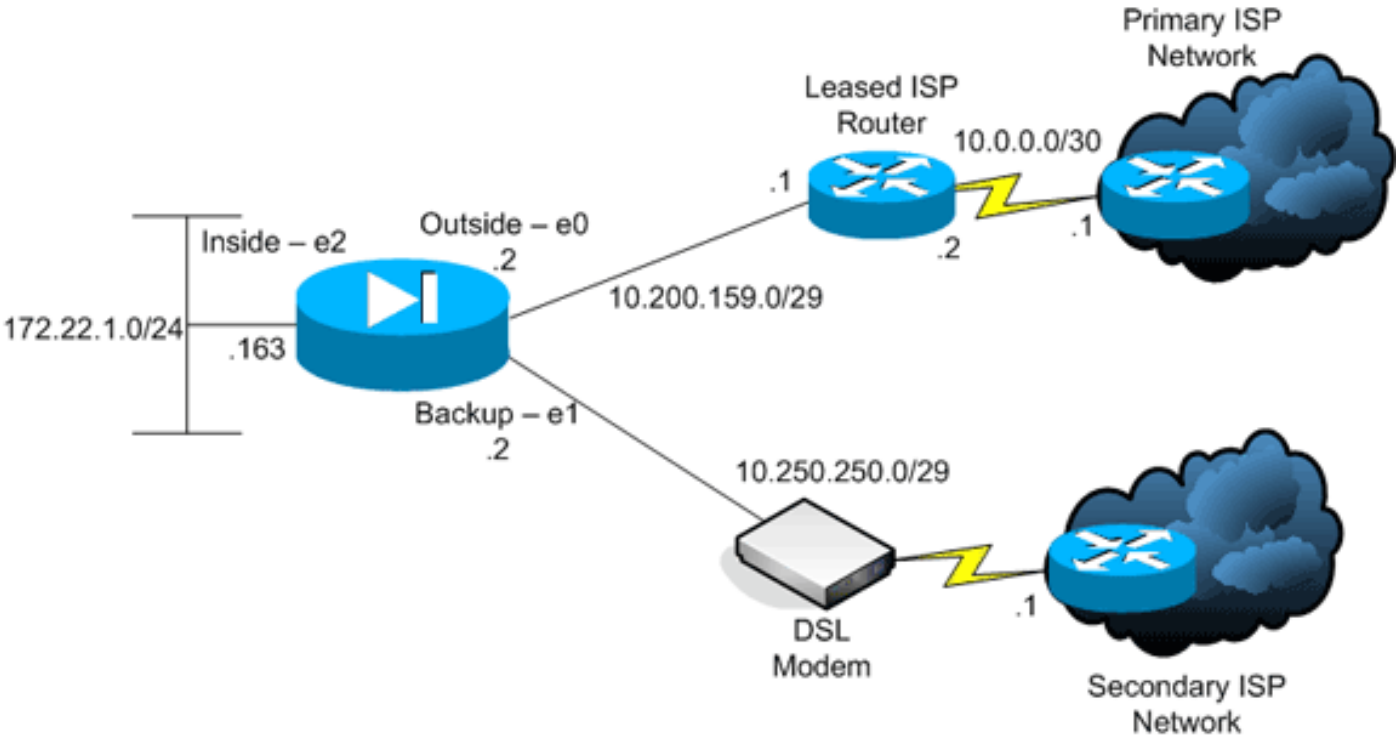
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: gli indirizzi IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Nel documento vengono usate queste configurazioni:

- CLI (Command-Line Interface)
- Adaptive Security Device Manager (ASDM)

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

Configurazione 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
```

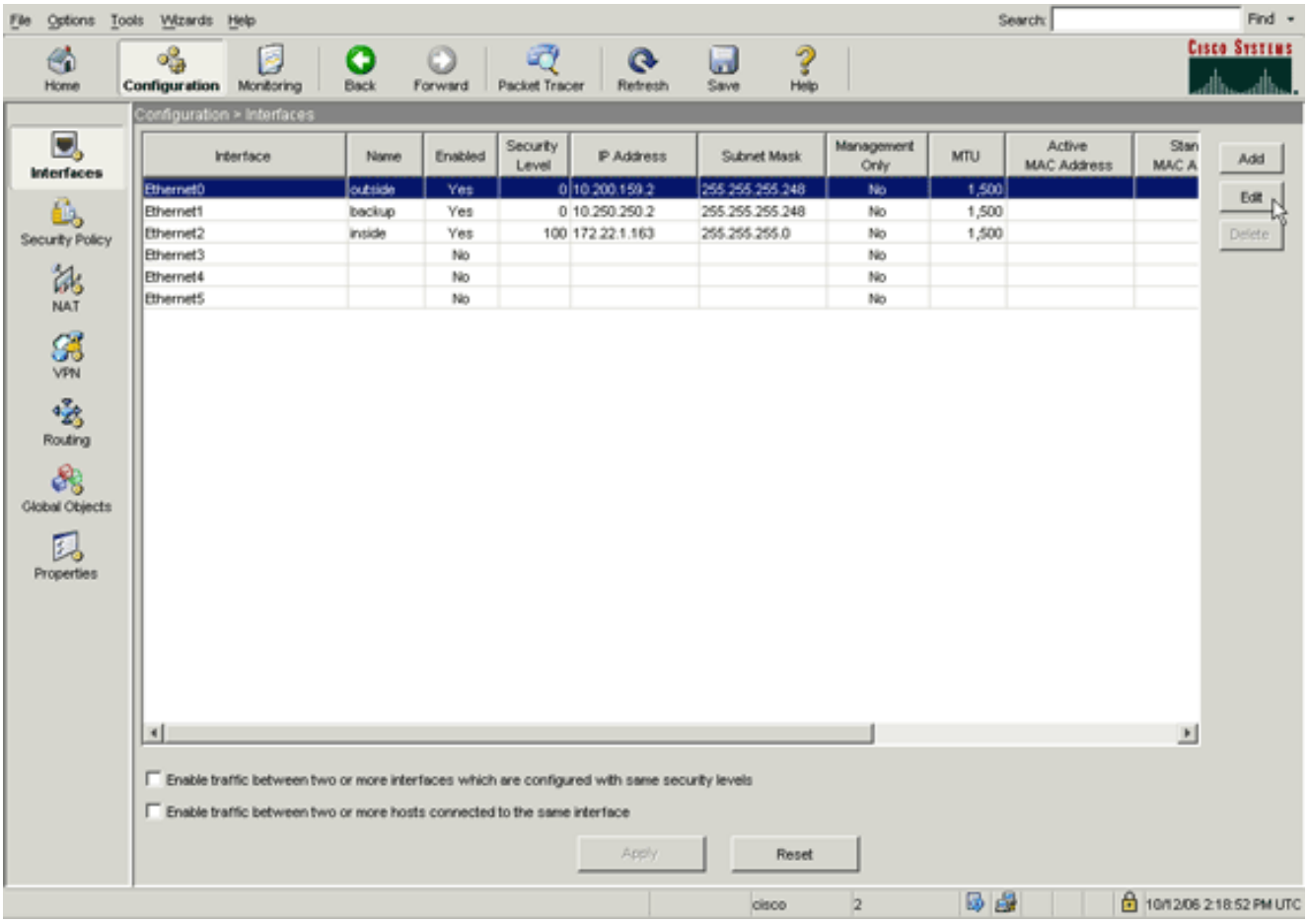
```
 nameif backup
!--- The interface attached to the Secondary ISP. !---
"backup" was chosen here, but any name can be assigned.
security-level 0 ip address 10.250.250.2 255.255.255.248
! interface Ethernet2 nameif inside security-level 100
ip address 172.22.1.163 255.255.255.0 ! interface
Ethernet3 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
```

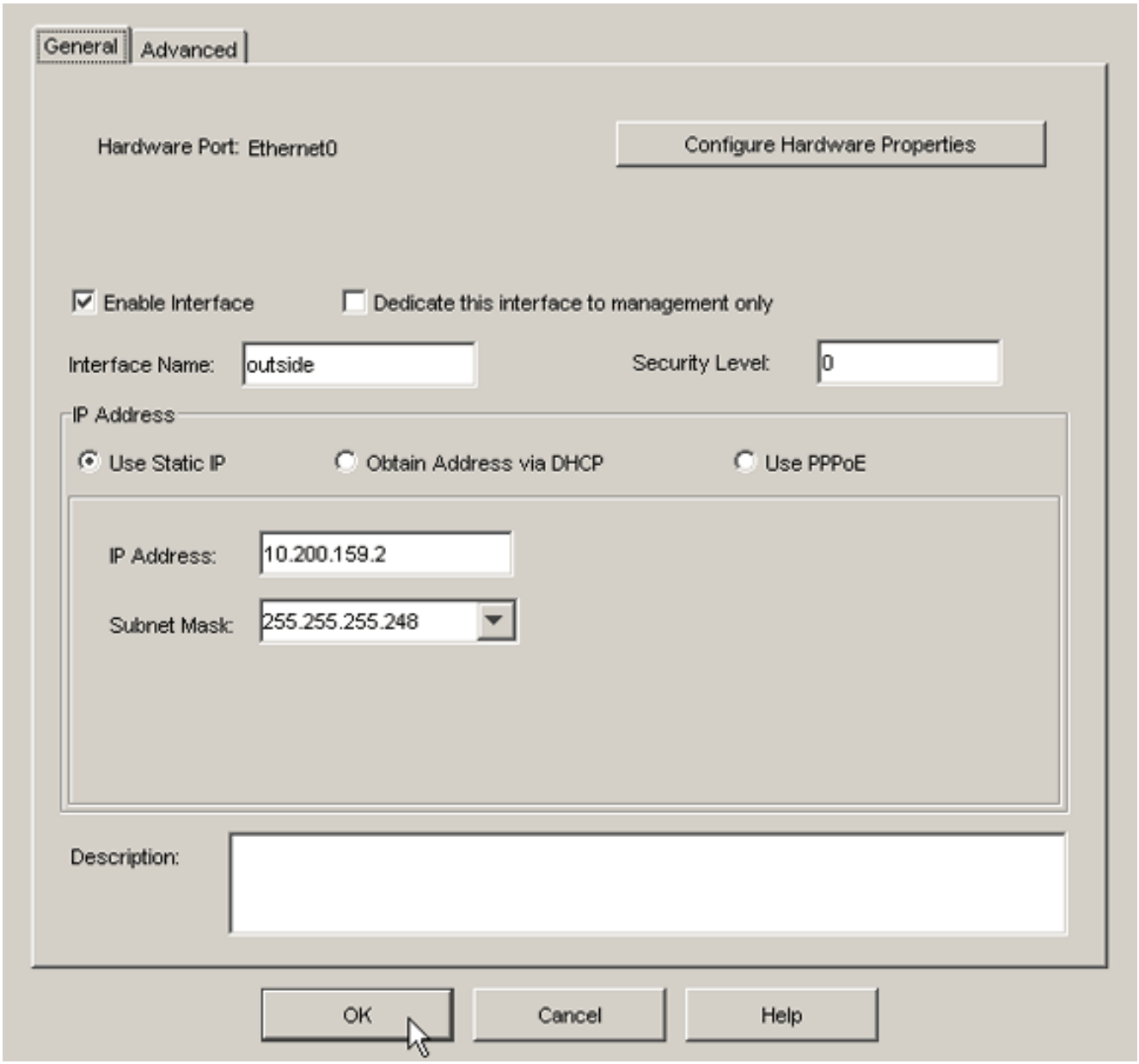
Configurazione ASDM

Per configurare il supporto di ISP ridondanti o di backup con l'applicazione ASDM, attenersi alla seguente procedura:

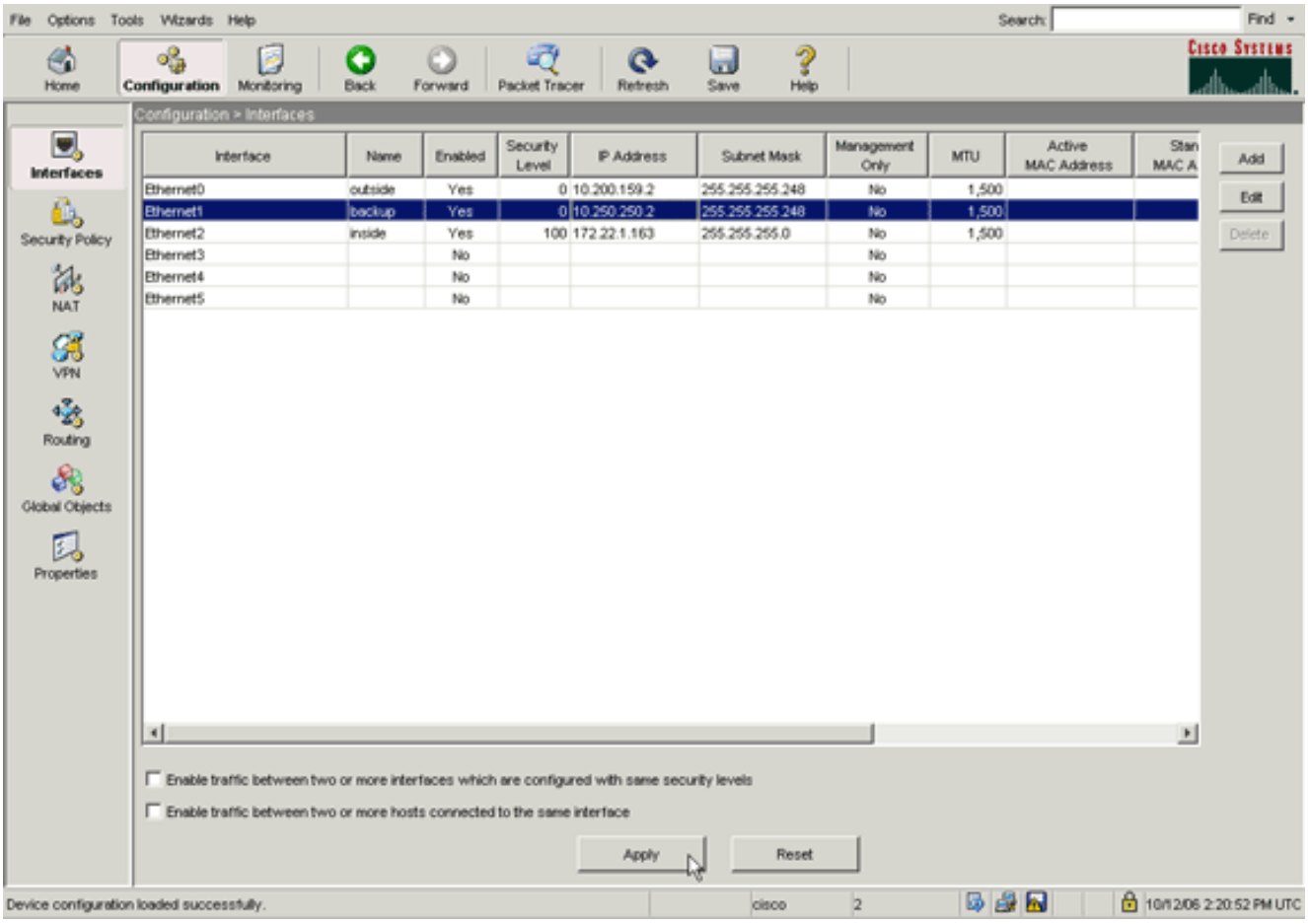
1. Nell'applicazione ASDM, fare clic su **Configurazione**, quindi su **Interfacce**.



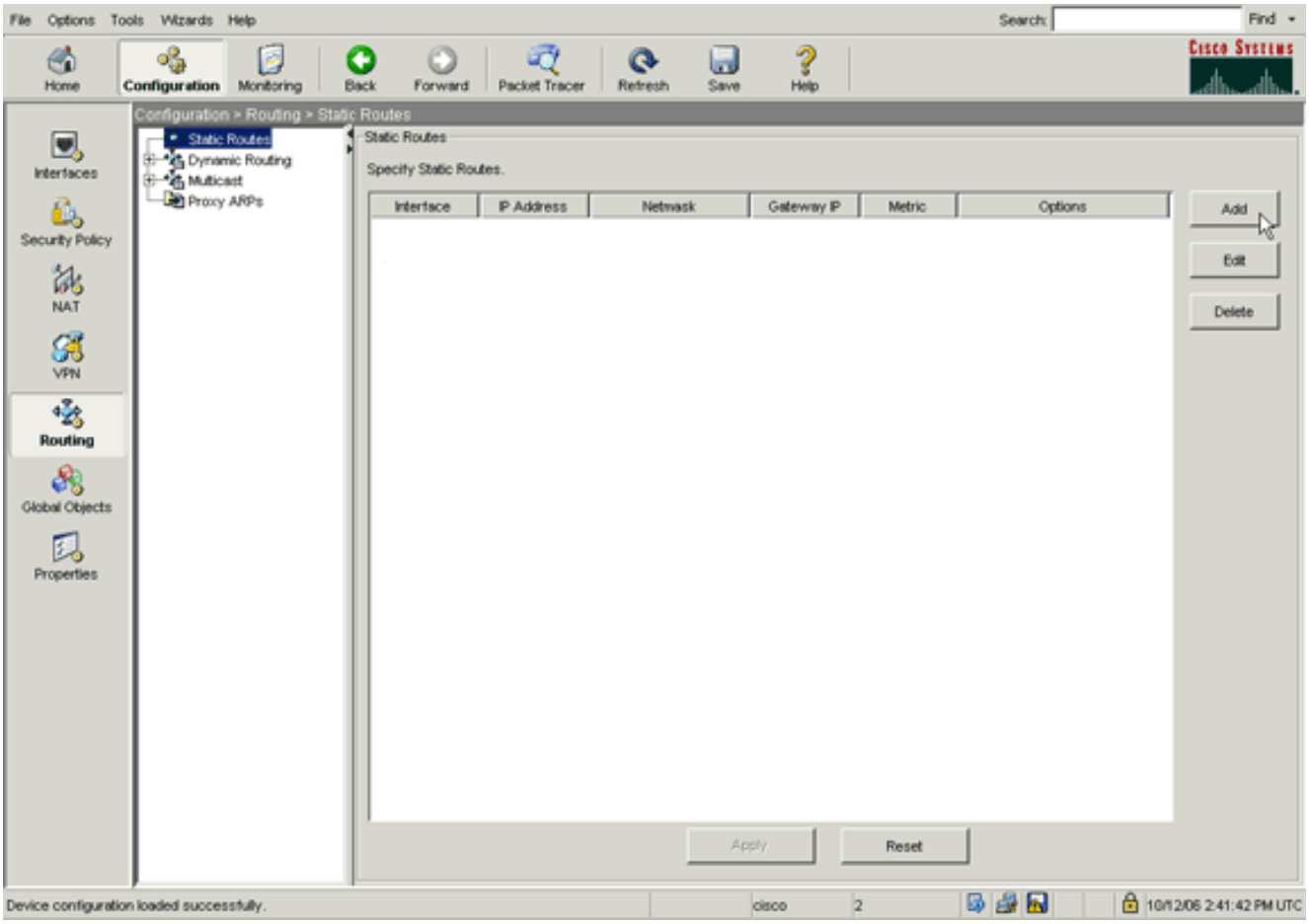
2. Dall'elenco Interfacce selezionare **Ethernet0**, quindi fare clic su **Modifica**.Viene visualizzata questa finestra di
dialogo.



3. Selezionare la casella di controllo **Abilita interfaccia** e immettere i valori 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 altre interfacce in base alle esigenze e fare clic su **Apply** (Applica) per aggiornare la configurazione dell'appliance di sicurezza.

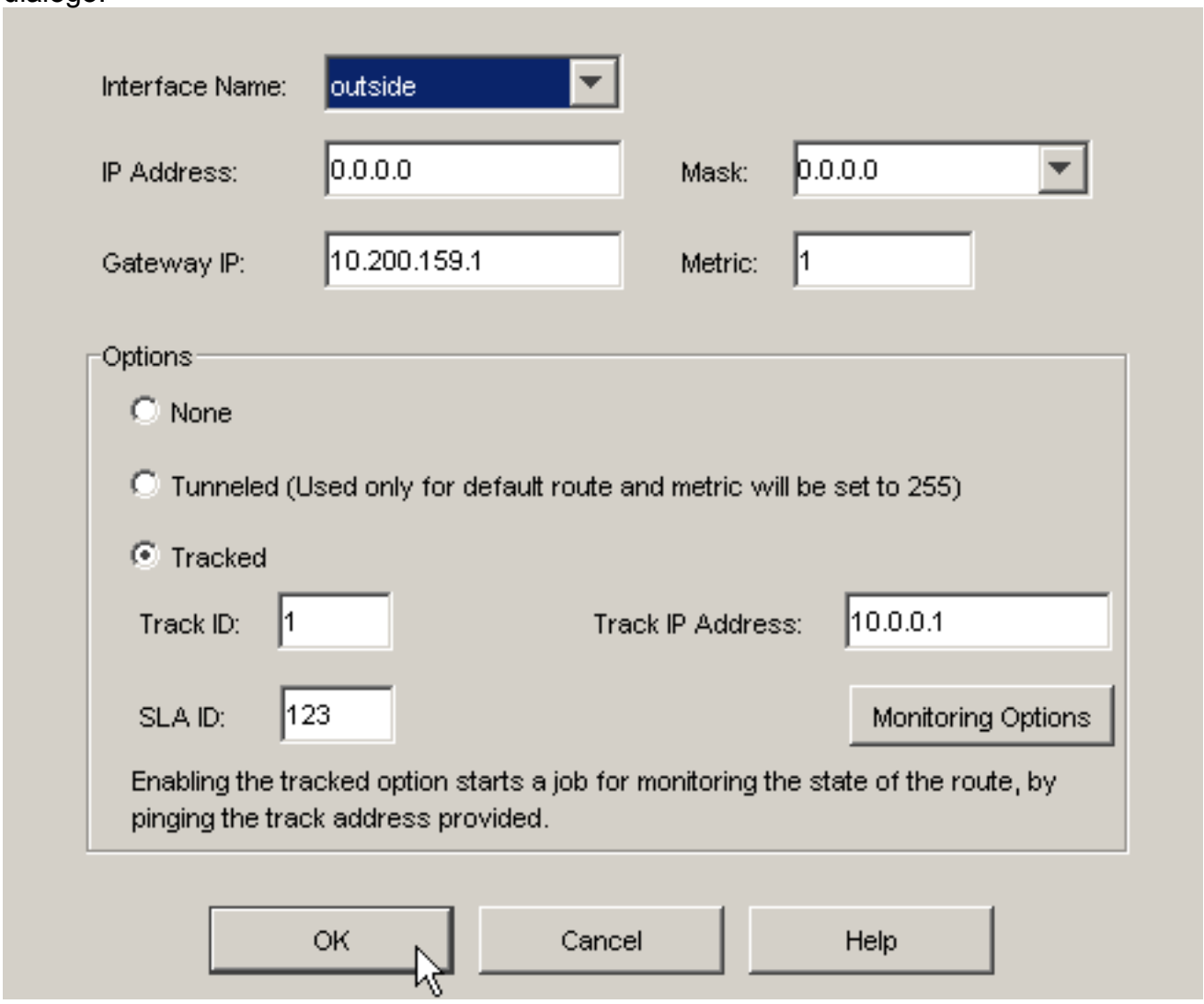


6. Fare clic su **Routing** sul lato sinistro dell'applicazione ASDM.

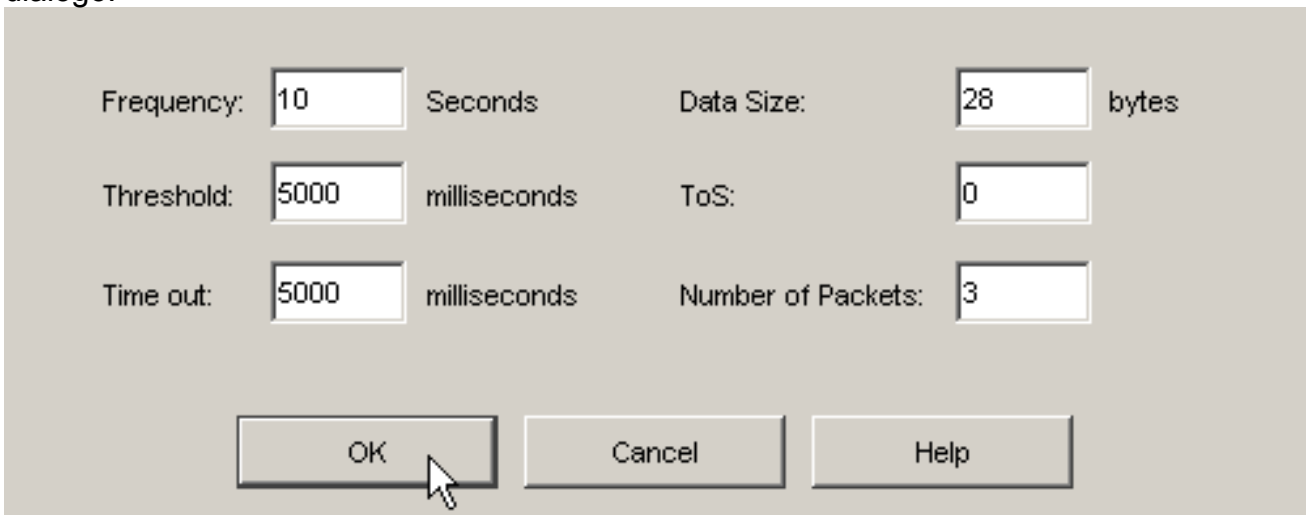


7. Per aggiungere le nuove route statiche, fare clic su **Add** (Aggiungi).Viene visualizzata questa finestra di

dialogo.



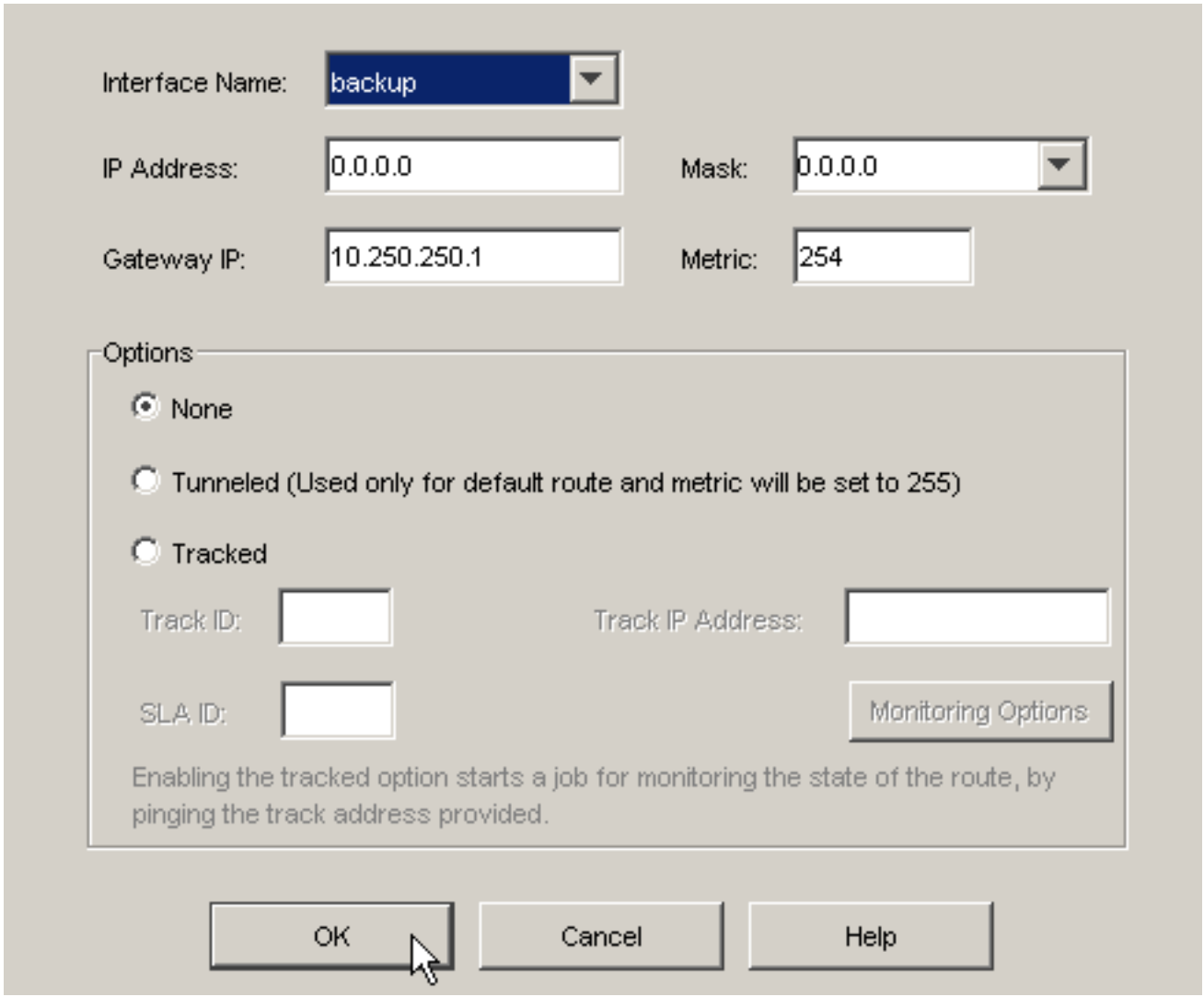
8. Dall'elenco a discesa Interface Name (Nome interfaccia), scegliere l'interfaccia su cui risiede la route e configurare la route predefinita per raggiungere il gateway. Nell'esempio, 10.0.0.1 è il gateway ISP primario, nonché l'oggetto da monitorare con echo ICMP.
9. Nell'area Opzioni, fare clic sul pulsante di opzione **Tracciato** e immettere i valori nei campi ID traccia, ID contratto di servizio e Indirizzo IP traccia.
10. Fare clic su **Opzioni di monitoraggio**.Viene visualizzata questa finestra di dialogo.



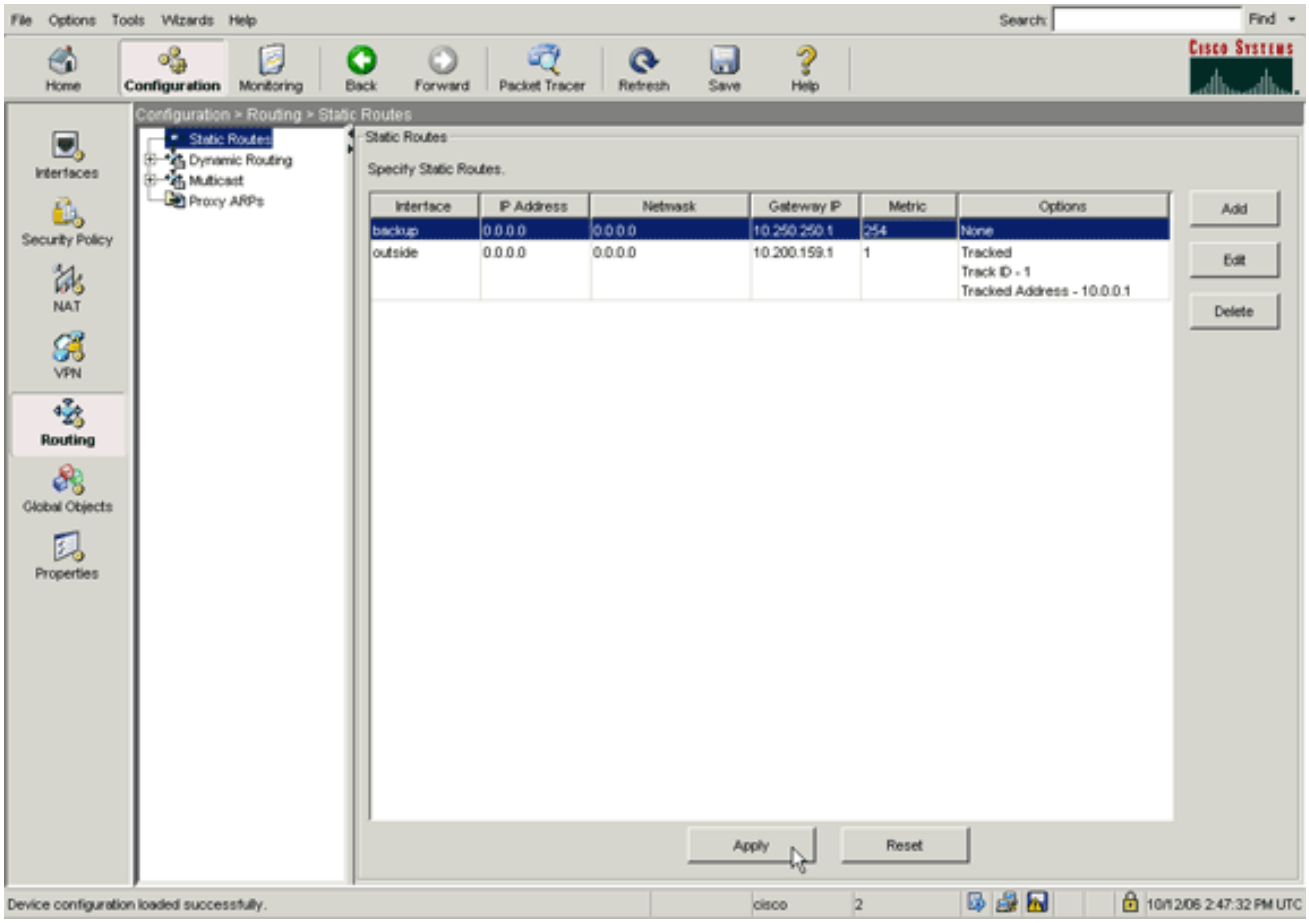
11. Immettere i valori per la frequenza e altre opzioni di controllo e fare clic su **OK**.
12. Aggiungere un'altra route statica per l'ISP secondario in modo da fornire una route per

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 PIX.

13. Per chiudere la finestra di dialogo, fare clic su **OK**.



Le configurazioni vengono visualizzate nell'elenco Interfaccia.



14. Per aggiornare la configurazione dell'appliance di sicurezza, selezionare la configurazione del routing e fare clic su **Applica**.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Confermare il completamento della configurazione

Per verificare che la configurazione sia stata completata, usare i comandi **show**.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show running-config sla monitor**: visualizza i comandi SLA nella configurazione.

```
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**: visualizza le impostazioni di configurazione correnti dell'operazione.

```
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 operating-state**: visualizza le statistiche operative dell'operazione SLA.Prima che l'ISP primario abbia esito negativo, questo è lo stato operativo:

```
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
```

Dopo il guasto dell'ISP primario (e il timeout dell'eco ICMP), questo è lo stato operativo:

```
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
```

Conferma installazione route di backup (metodo CLI)

Utilizzare il comando **show route** per determinare quando installare la route di backup.

- Prima che l'ISP principale abbia esito negativo, viene visualizzata la tabella di routing:

```
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
```

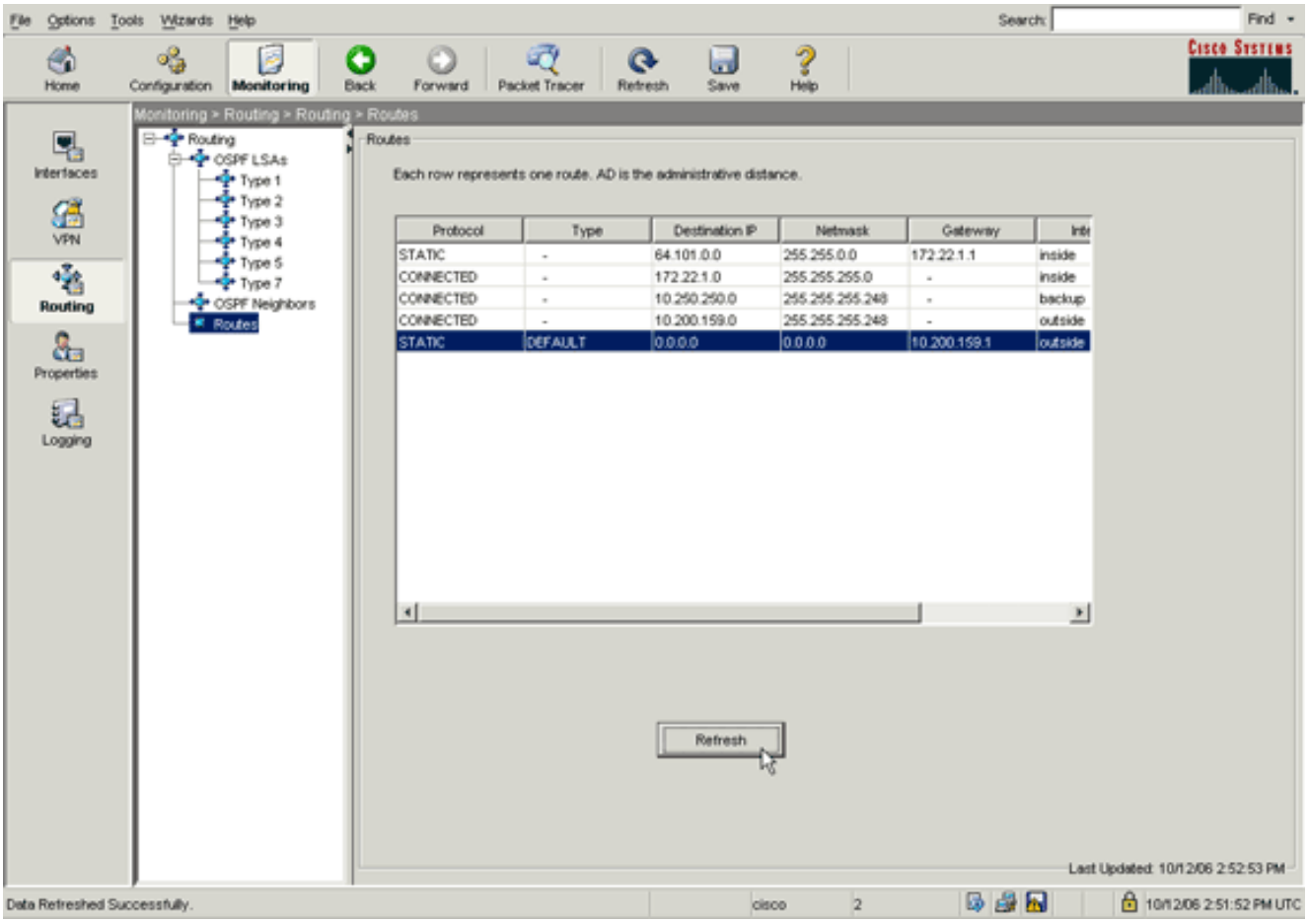
- Se si verifica un errore nell'ISP primario, la route statica viene rimossa e la route di backup viene installata, ovvero la tabella di routing:

```
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
```

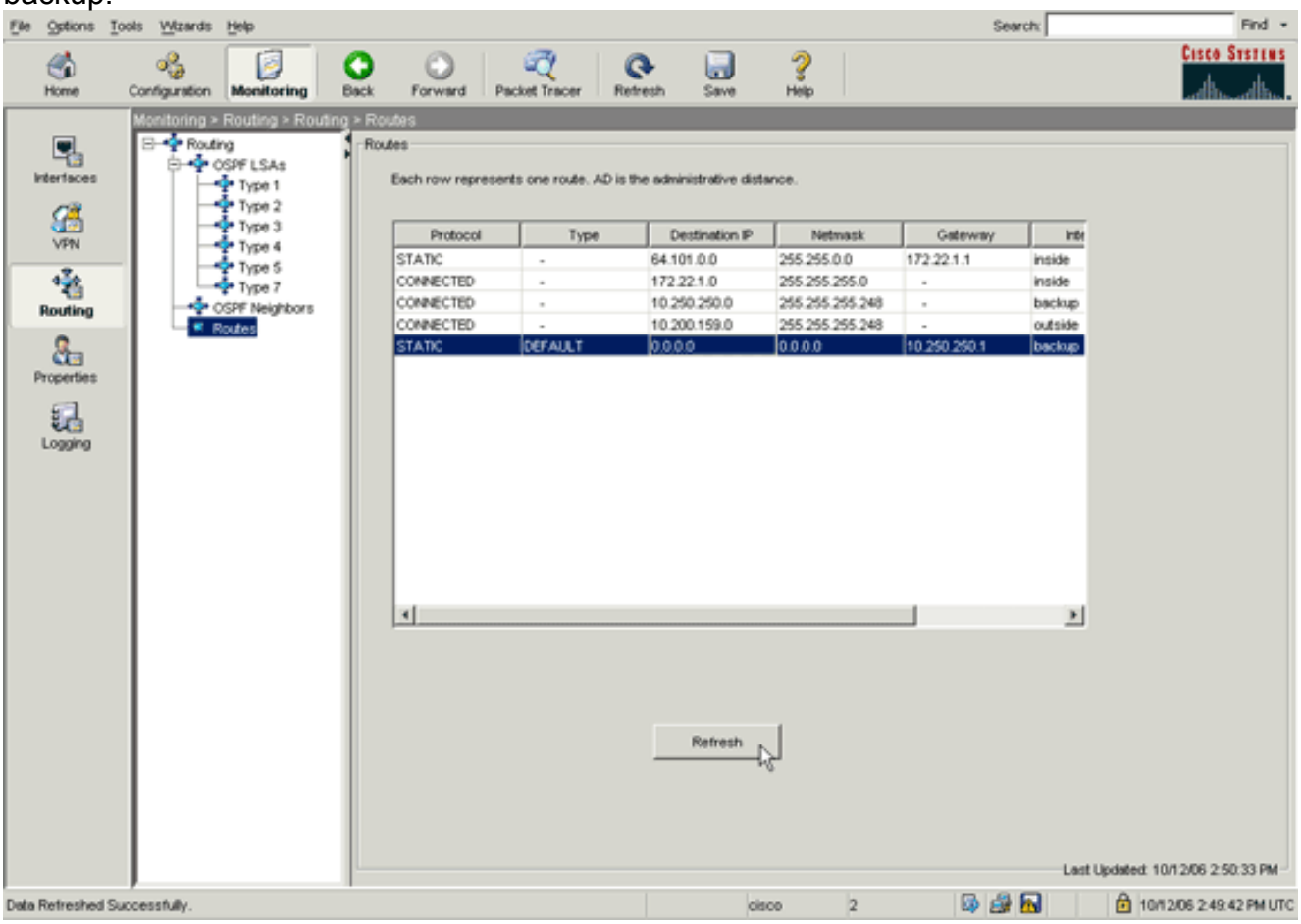
Conferma installazione route di backup (metodo ASDM)

Per verificare con ASDM che il percorso di backup è installato, attenersi alla seguente procedura:

1. Fare clic su **Monitoraggio** e quindi su **Instradamento**.
2. Dalla struttura Ciclo di produzione scegliere **Cicli di produzione**.Prima che l'ISP principale abbia esito negativo, viene visualizzata la tabella di routing:



Il percorso PREDEFINITO punta a 10.0.0.2 attraverso l'interfaccia esterna.Se si verifica un errore nell'ISP primario, la route viene rimossa e la route di backup viene installata. Il percorso PREDEFINITO ora punta a 10.250.250.1 tramite l'interfaccia di backup.



Risoluzione dei problemi

Comandi debug

- **debug sla monitor trace**: visualizza lo stato dell'operazione echo.L'oggetto rilevato (gateway ISP primario) è attivo e l'eco ICMP ha esito positivo.

```
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
```

  L'oggetto rilevato (gateway ISP primario) è inattivo e l'eco ICMP ha esito negativo.

```
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**: visualizza gli errori rilevati dal processo SLA monitor.L'oggetto rilevato (gateway ISP primario) è attivo e ICMP ha esito positivo.

```
%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
```

  L'oggetto rilevato (gateway ISP primario) è inattivo e la route rilevata viene rimossa.

```
%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.
```

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 si verifichi un errore in un altro collegamento lungo il percorso oppure che un altro dispositivo interferisca. Questa configurazione può indurre il monitoraggio dello SLA a concludere che la connessione all'ISP primario ha avuto esito negativo e che l'appliance di sicurezza ha eseguito inutilmente il failover 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 l'eco ICMP inviato dall'operazione di monitoraggio ha esito negativo, il percorso primario 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 l'eco ICMP inviata dall'operazione di monitoraggio ha esito negativo, il collegamento all'ISP è quasi sicuramente inattivo.

Monitoraggio degli SLA sull'appliance ASA

Problema:

Il monitoraggio degli SLA non funziona dopo l'aggiornamento dell'ASA alla versione 8.0.

Soluzione:

Il problema potrebbe essere dovuto al comando **IP Reverse-Path** configurato nell'interfaccia **ESTERNA**. Rimuovere il comando in ASA e provare a controllare il monitoraggio dello SLA.

Informazioni correlate

- Configurazione della traccia delle route statiche
- Guida di riferimento ai comandi di PIX/ASA 7.2
- Cisco ASA serie 5500 Security Appliance
- Cisco PIX serie 500 Security Appliance
- Documentazione e supporto tecnico – Cisco Systems