

# ASA/PIX 7.x:冗餘或備份ISP鏈路配置示例

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[相關產品](#)

[慣例](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[組態](#)

[CLI組態](#)

[ASDM配置](#)

[驗證](#)

[確認配置已完成](#)

[確認備份路由已安裝 \( CLI方法 \)](#)

[確認已安裝備份路由 \( ASDM方法 \)](#)

[疑難排解](#)

[Debug指令](#)

[不必要地刪除跟蹤的路由](#)

[ASA上的SLA監控](#)

[相關資訊](#)

## 簡介

靜態路由的問題在於不存在用於確定路由是開啟還是關閉的固有機制。即使下一跳網關不可用，該路由仍保留在路由表中。僅當安全裝置上的關聯介面關閉時，才會從路由表中刪除靜態路由。為了解決此問題，靜態路由跟蹤功能用於跟蹤靜態路由的可用性，如果該路由失敗，則將其從路由表中刪除並替換為備份路由。

本文檔提供了有關如何使用PIX 500系列安全裝置或ASA 5500系列自適應安全裝置上的靜態路由跟蹤功能以使裝置能夠使用冗餘或備份網際網路連線的示例。在此示例中，靜態路由跟蹤允許安全裝置在主租用線路不可用時使用到輔助網際網路服務提供商(ISP)的廉價連線。

為了實現此冗餘，安全裝置將靜態路由與您定義的監控目標相關聯。服務級別協定(SLA)操作使用定期的網際網路控制消息協定(ICMP)回應請求來監控目標。如果沒有收到回應，對象將被視為關閉，並從路由表中刪除關聯的路由。使用先前配置的備份路由來代替已移除的路由。使用備份路由時，SLA監控操作將繼續嘗試到達監控目標。目標再次可用後，第一個路由將替換在路由表中，備份路由將被刪除。

**注意：**本文檔中介紹的配置不能用於負載平衡或負載共用，因為ASA/PIX不支援此配置。此配置僅用於冗餘或備份目的。如果主交換機發生故障，則傳出流量使用主ISP，然後使用輔助ISP。主ISP故障會導致流量暫時中斷。

## [必要條件](#)

### [需求](#)

選擇可以響應ICMP回應請求的監控目標。目標可以是您選擇的任何網路對象，但推薦的目標與您的ISP連線密切相關。一些可能的監測目標包括：

- ISP網關地址
- 另一個ISP管理的地址
- 安全裝置需要與之通訊的另一網路上的伺服器，如AAA伺服器
- 另一個網路上的永續性網路對象（夜間可以關閉的台式機或筆記型電腦不是很好的選擇）

本文檔假設安全裝置完全可以運行並配置為允許Cisco ASDM更改配置。

**注意：**有關如何允許ASDM配置裝置的資訊，請參閱[允許ASDM的HTTPS訪問](#)。

### [採用元件](#)

本文中的資訊係根據以下軟體和硬體版本：

- Cisco PIX安全裝置515E，軟體版本7.2(1)或更高版本
- 思科自適應安全裝置管理器5.2(1)或更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

### [相關產品](#)

您還可以將此配置與Cisco ASA 5500系列安全裝置版本7.2(1)配合使用。

**注意：**在ASA 5505上配置第四個介面時需要**backup interface**命令。有關詳細資訊，請參閱[備份介面](#)。

### [慣例](#)

如需檔案慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

## [背景資訊](#)

在本示例中，安全裝置維護兩個與Internet的連線。第一個連線是通過主ISP提供的路由器訪問的高速租用線路。第二連線是通過輔助ISP提供的DSL數據機訪問的低速數字使用者線路(DSL)。

**注意：**本示例中未發生負載均衡。

只要租用線路處於活動狀態且主要ISP網關可訪問，DSL連線即處於空閒狀態。但是，如果與主ISP的連線中斷，安全裝置會更改路由表，將流量定向到DSL連線。靜態路由跟蹤用於實現此冗餘。

安全裝置配置了一條靜態路由，該路由將所有網際網路流量定向到主ISP。SLA監控程式每10秒檢查一次，確認主ISP網關可訪問。如果SLA監控過程確定無法到達主ISP網關，則從路由表中刪除將流量定向到該介面的靜態路由。為了替換該靜態路由，安裝了將流量定向到輔助ISP的備用靜態路由。此備用靜態路由通過DSL數據機將流量定向到輔助ISP，直到通向主要ISP的鏈路可訪問。

此配置提供了一種相對便宜的方法，可確保安全裝置後面的使用者仍可訪問出站Internet。如本文檔所述，此設定可能不適用於對安全裝置後資源的入站訪問。需要具備高級網路技能才能實現無縫入站連線。本檔案沒有說明這些技能。

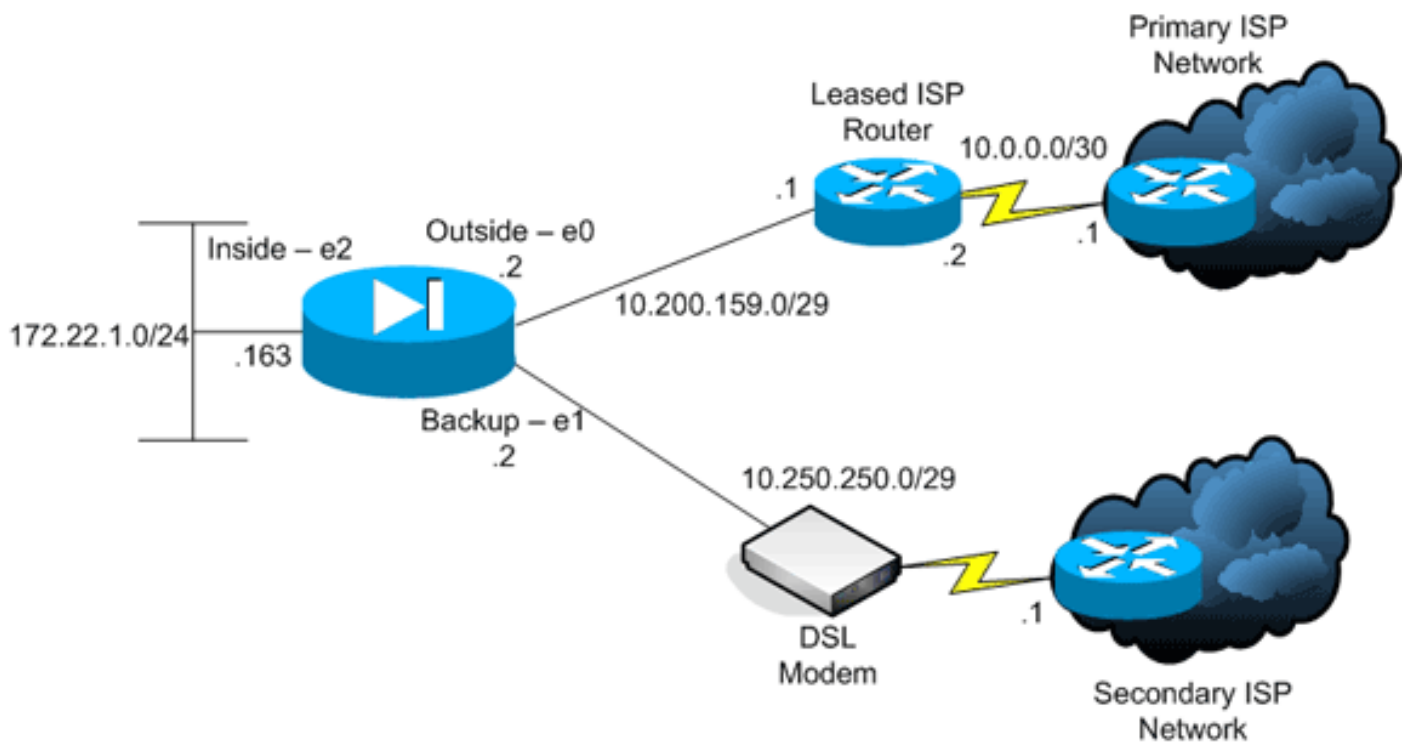
## 設定

本節提供用於設定本文件中所述功能的資訊。

注意：此配置中使用的IP地址不能在Internet上合法路由。它們是[RFC 1918](#)，在實驗室環境中使用。

## 網路圖表

本檔案會使用以下網路設定：



## 組態

本檔案會使用以下設定：

- [命令列介面\(CLI\)](#)
- [調適型安全裝置管理員\(ASDM\)](#)

註：使用[Command Lookup Tool](#)([僅供已註冊客戶使用](#))可獲取本節中使用的命令的詳細資訊。

## CLI組態

## 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.

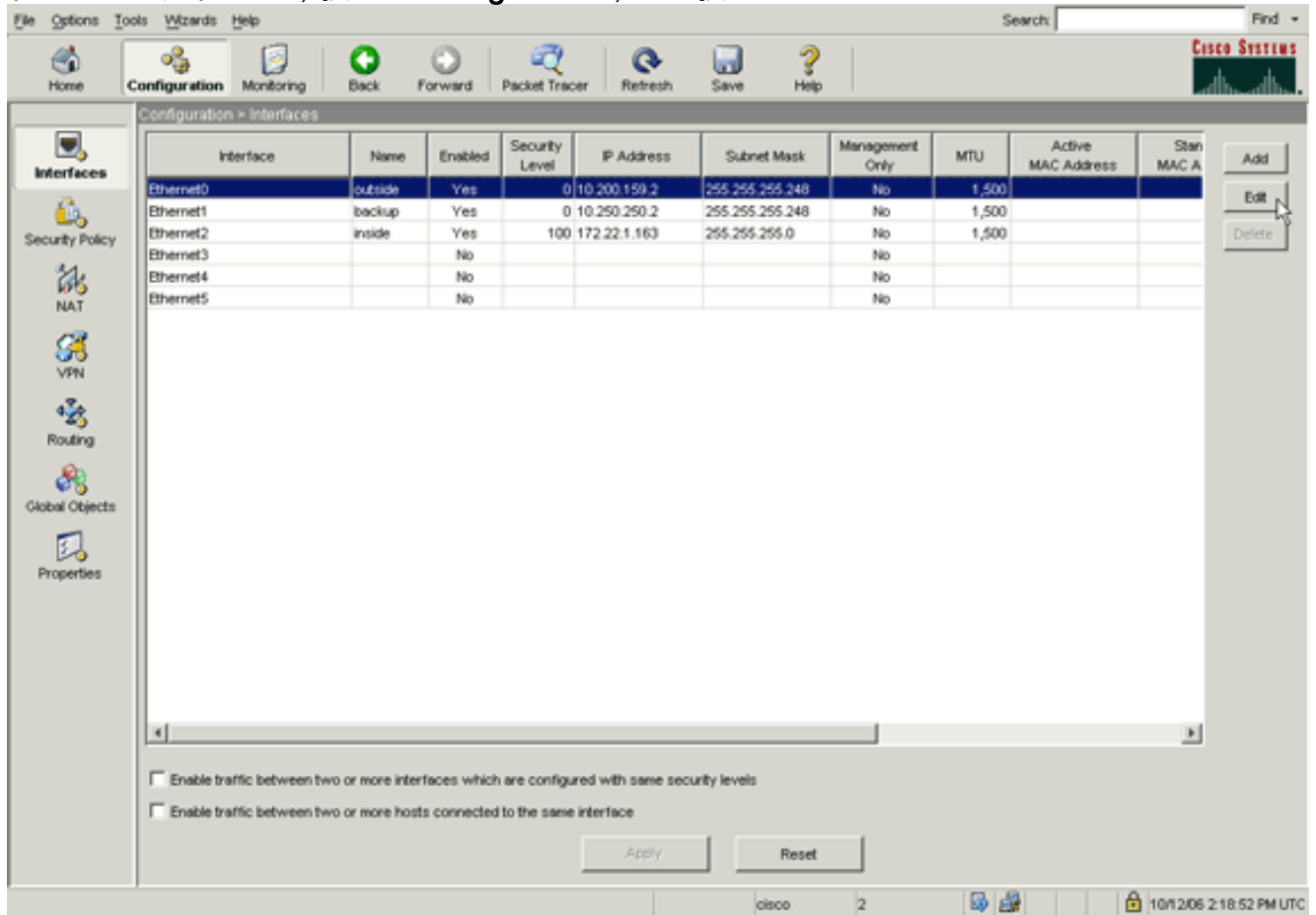
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect 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

```

## ASDM配置

要使用ASDM應用程式配置冗餘或備份ISP支援，請完成以下步驟：

1. 在ASDM應用程式中，按一下Configuration，然後按一下Interfaces。



2. 從Interfaces清單中選擇Ethernet0，然後按一下Edit。出現此對話方塊。

General | Advanced

Hardware Port: Ethernet0 Configure Hardware Properties

Enable Interface  Dedicate this interface to management only

Interface Name:  Security Level:

IP Address

Use Static IP  Obtain Address via DHCP  Use PPPoE

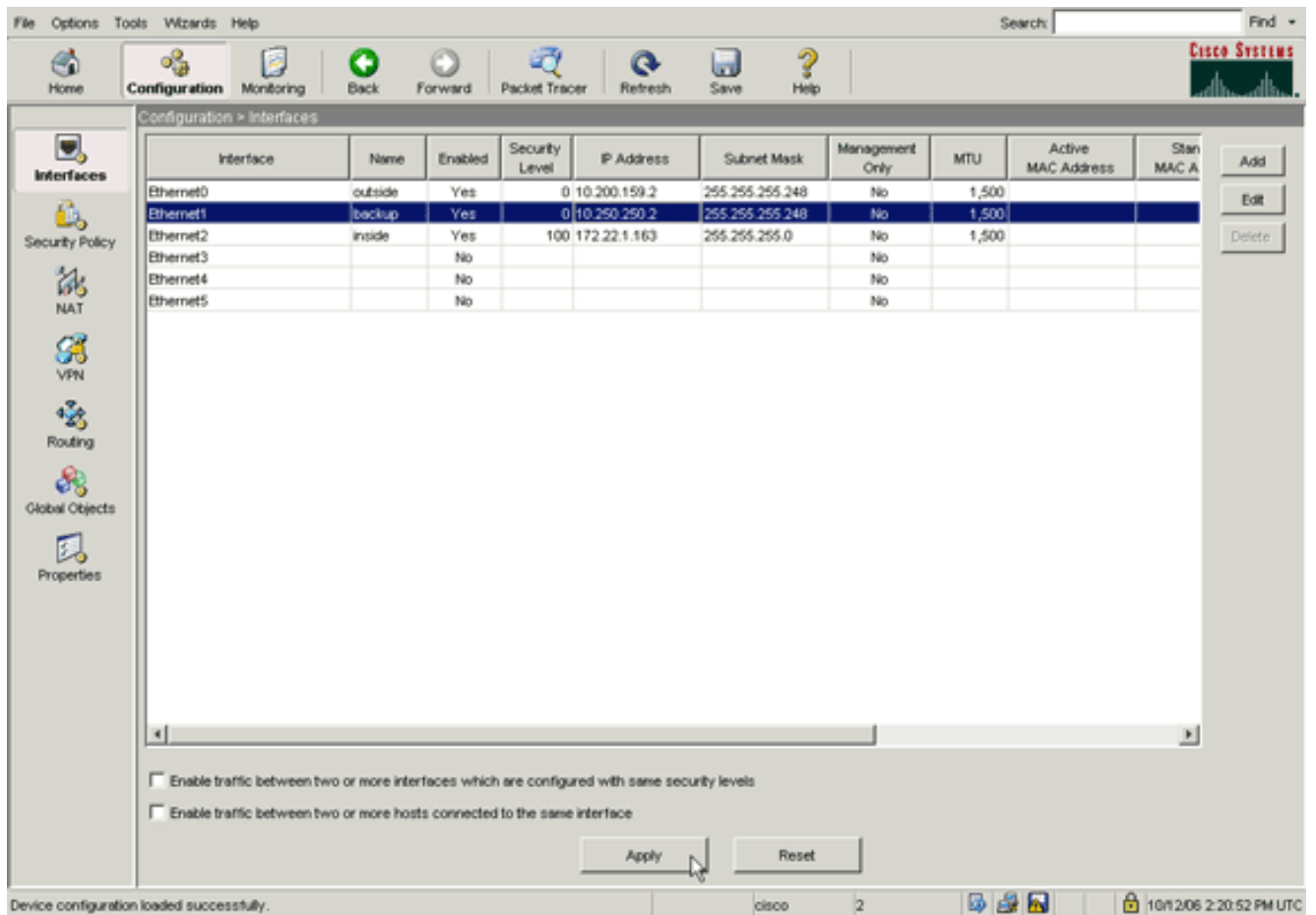
IP Address:

Subnet Mask:

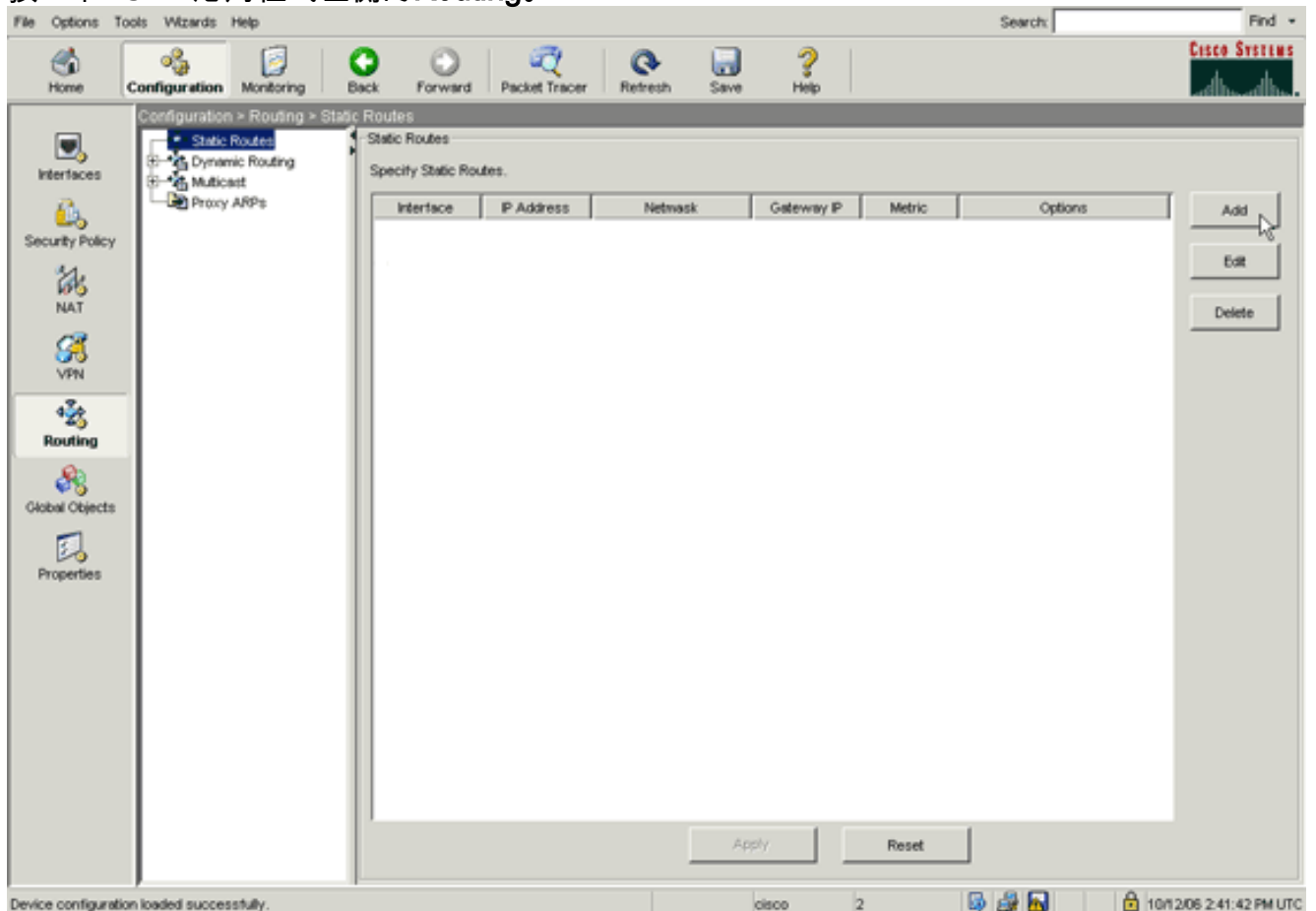
Description:

OK Cancel Help

3. 選中**Enable Interface**覈取方塊，並在Interface Name、Security Level、IP Address和Subnet Mask欄位中輸入值。
4. 按一下「**OK**」以關閉對話方塊。
5. 根據需要配置其他介面，然後按一下**Apply**以更新安全裝置配置。



6. 按一下ASDM應用程式左側的Routing。



7. 按一下Add以新增新的靜態路由。出現此對話方塊。



Interface Name:

IP Address:  Mask:

Gateway IP:  Metric:

Options

None

Tunneled (Used only for default route and metric will be set to 255)

Tracked

Track ID:  Track IP Address:

SLA ID:

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

8. 從Interface Name下拉選單中，選擇路由所在的介面，並配置到達網關的預設路由。在本例中，10.0.0.1是主ISP網關，以及使用ICMP回應監控的對象。
9. 在「選項」區域中，按一下**Tracked**單選按鈕，然後在「跟蹤ID」、「SLA ID」和「跟蹤IP地址」欄位中輸入值。
10. 按一下**Monitoring Options**。出現此對話方塊。

Frequency:  Seconds Data Size:  bytes

Threshold:  milliseconds ToS:

Time out:  milliseconds Number of Packets:

11. 輸入頻率值和其他監視選項，然後按一下**確定**。
12. 為輔助ISP新增另一條靜態路由，以便提供到達Internet的路由。為了使其成為輔助路由，請用更高的度量配置此路由，如254。如果主路由（主ISP）失敗，該路由將從路由表中刪除。此輔助路由（輔助ISP）安裝在PIX路由表中。
13. 按一下「**OK**」以關閉對話方塊。

Interface Name:

IP Address:  Mask:

Gateway IP:  Metric:

**Options**

None

Tunneled (Used only for default route and metric will be set to 255)

Tracked

Track ID:  Track IP Address:

SLA ID:

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

配置將顯示在介面清單中。

File Options Tools Wizards Help Search Find

Home Configuration Monitoring Back Forward Packet Tracer Refresh Save Help

Configuration > Routing > Static Routes

Static Routes

Specify Static Routes.

Interface	IP Address	Network	Gateway IP	Metric	Options
backup	0.0.0.0	0.0.0.0	10.250.250.1	254	None
outside	0.0.0.0	0.0.0.0	10.200.159.1	1	Tracked Track ID - 1 Tracked Address - 10.0.0.1

Device configuration loaded successfully. cisco 2 10/1/206 2:47:32 PM UTC

14. 選擇路由配置，然後按一下Apply以更新安全裝置配置。

## 驗證

使用本節內容，確認您的組態是否正常運作。

## 確認配置已完成

使用這些show命令驗證您的配置是否完成。

[輸出直譯器工具](#)(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析

。

- **show running-config sla monitor** — 顯示配置中的SLA命令。

```
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** — 顯示操作的當前配置設定。

```
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** — 顯示SLA操作的操作統計資訊。在主ISP發生故障之前，這是運行狀態：

```
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
在主ISP發生故障 (且ICMP回應超時) 後，這是運行狀態：
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

```

## 確認備份路由已安裝 (CLI方法)

使用show route命令確定備份路由的安裝時間。

- 在主ISP發生故障之前，路由表為：

```

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

```

- 在主ISP發生故障、靜態路由被刪除並安裝了備份路由後，路由表為：

```

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

```

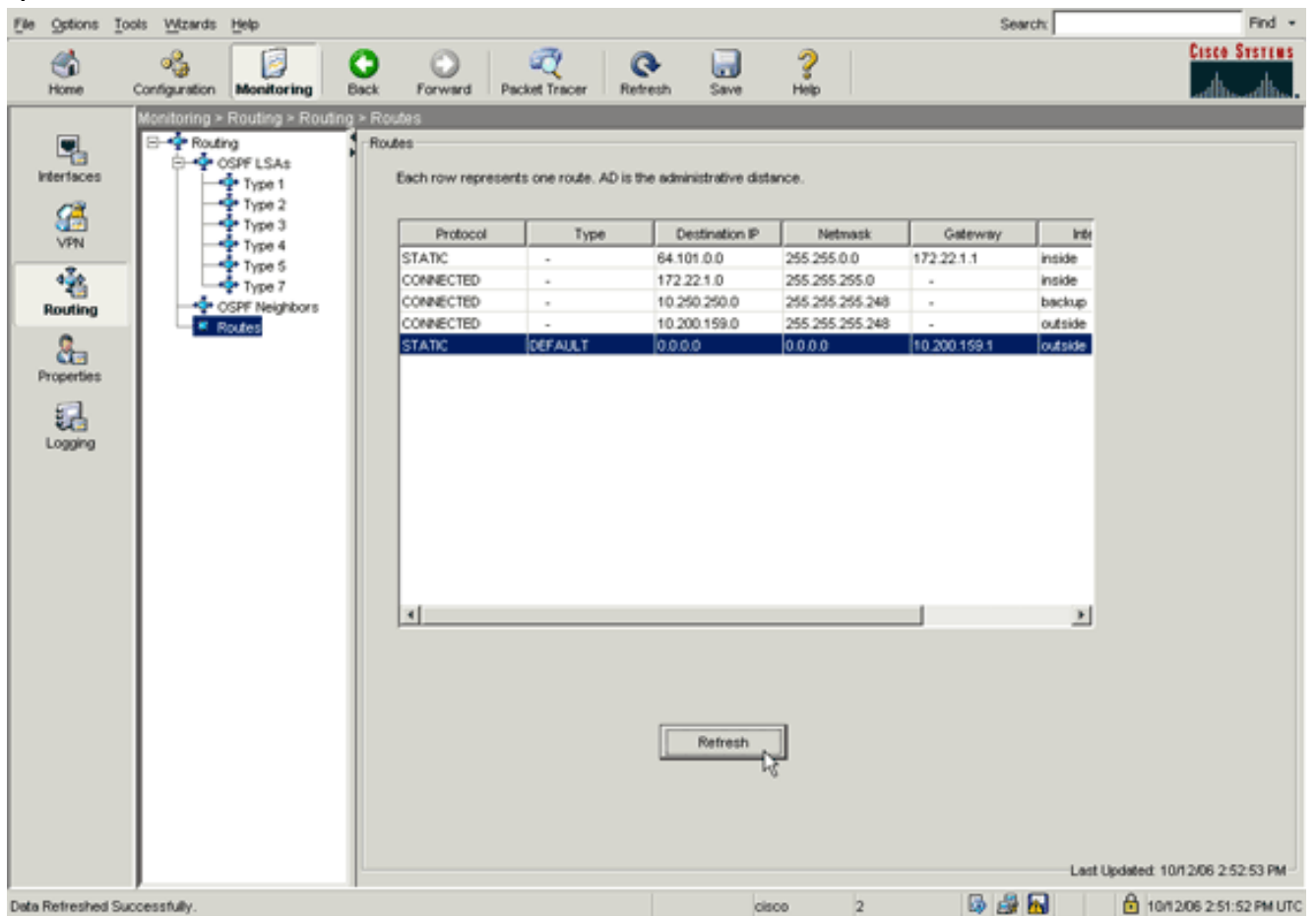
Gateway of last resort is 10.250.250.1 to network 0.0.0.0

```
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
```

## 確認已安裝備份路由 (ASDM方法)

要與ASDM確認備份路由已安裝，請完成以下步驟：

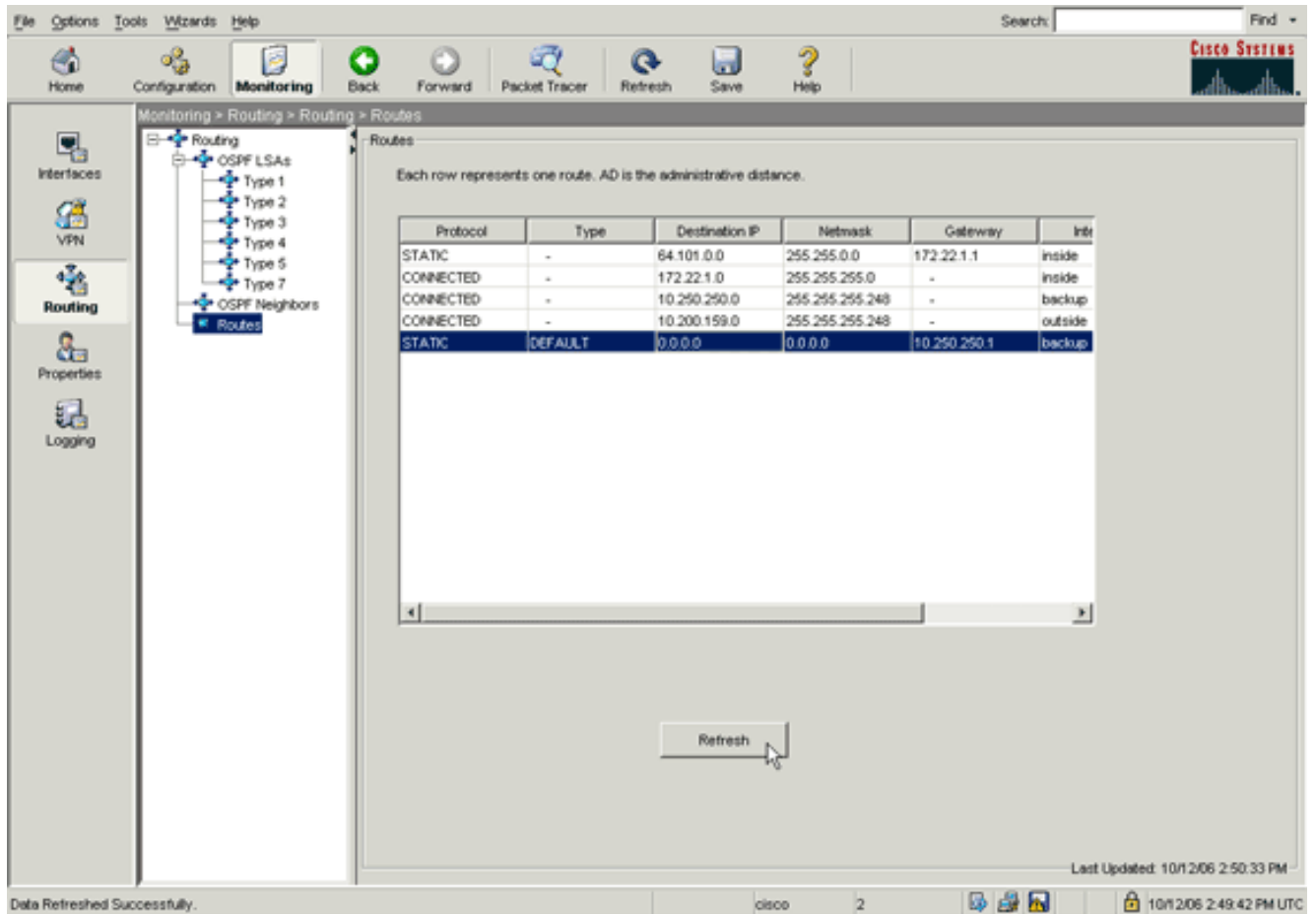
1. 按一下**Monitoring**，然後按一下**Routing**。
2. 從路由樹中選擇**Routes**。在主ISP發生故障之前，路由表為：



The screenshot shows the Cisco ASDM interface. The left sidebar has 'Monitoring' selected, and the main window displays 'Routing > Routes'. A tree view on the left shows 'Routing' expanded to 'Routes'. The main area contains a table of routes. Below the table is a 'Refresh' button. The status bar at the bottom indicates 'Data Refreshed Successfully' and 'Last Updated: 10/12/06 2:52:53 PM'.

Protocol	Type	Destination IP	Netmask	Gateway	Intf
STATIC	-	64.101.0.0	255.255.0.0	172.22.1.1	inside
CONNECTED	-	172.22.1.0	255.255.255.0	-	inside
CONNECTED	-	10.250.250.0	255.255.255.248	-	backup
CONNECTED	-	10.200.159.0	255.255.255.248	-	outside
STATIC	DEFAULT	0.0.0.0	0.0.0.0	10.200.159.1	outside

預設路由通過外部介面指向10.0.0.2。在主ISP發生故障後，會刪除該路由，並安裝備用路由。預設路由現在通過備份介面指向10.250.250.1。



## 疑難排解

### Debug指令

- **debug sla monitor trace** — 顯示回顯操作的進度。跟蹤的對象 ( 主ISP網關 ) 已啟動 , ICMP響應成功。

```
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
```

跟蹤的對象 ( 主ISP網關 ) 已關閉 , ICMP響應失敗。

```
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** — 顯示SLA監控進程遇到的錯誤。跟蹤的對象 ( 主ISP網關 ) 已啟動 , ICMP成功。

```
%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
```

跟蹤的對象 ( 主ISP網關 ) 關閉，並且刪除跟蹤的路由。

```
%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.
```

## 不必要地刪除跟蹤的路由

如果不必要地刪除了跟蹤的路由，請確保您的監控目標始終可用於接收回應請求。此外，請確保監控目標的狀態 ( 即目標是否可訪問 ) 與主ISP連線的狀態密切相關。

如果您選擇的監控目標比ISP網關更遠，則沿該路由的另一條鏈路可能會發生故障，或者其它裝置可能會干擾。此配置可能導致SLA監控器斷定與主ISP的連線失敗，並導致安全裝置不必要地故障切換到輔助ISP鏈路。

例如，如果您選擇分支機構路由器作為監控目標，到分支機構的ISP連線以及此過程中的任何其他鏈路都可能失敗。監控操作傳送的ICMP響應失敗後，即使主ISP鏈路仍然處於活動狀態，主跟蹤路由也會被刪除。

在本示例中，用作監控目標的主ISP網關由ISP管理，位於ISP鏈路的另一端。此配置可確保如果監控操作傳送的ICMP回應失敗，ISP鏈路幾乎肯定會關閉。

## ASA上的SLA監控

問題：

ASA升級到版本8.0後，SLA監控不起作用。

解決方案：

問題可能是由於OUTSIDE介面中配置的IP Reverse-Path命令。刪除ASA中的命令並嘗試檢查

SLA監控。

## 相關資訊

- [配置靜態路由跟蹤](#)
- [PIX/ASA 7.2命令參考](#)
- [Cisco ASA 5500系列安全裝置](#)
- [Cisco PIX 500系列安全裝置](#)
- [技術支援與文件 - Cisco Systems](#)