ASA/PIX 7.x: Redundant or Backup ISP Links Configuration Example

Document ID: 70559

Introduction

A problem with static routes is that no inherent mechanism exists to determine if the route is up or down. The route remains in the routing table even if the next hop gateway becomes unavailable. Static routes are removed from the routing table only if the associated interface on the security appliance goes down. In order to solve this problem, a static route tracking feature is used to track the availability of a static route and, if that route fails, remove it from the routing table and replace it with a backup route.

This document provides an example of how to use the static route tracking feature on the PIX 500 Series Security Appliance or the ASA 5500 Series Adaptive Security Appliance in order to enable the device to use redundant or backup Internet connections. In this example, static route tracking allows the security appliance to use an inexpensive connection to a secondary Internet service provider (ISP) in the event that the primary leased line becomes unavailable.

In order to achieve this redundancy, the security appliance associates a static route with a monitoring target that you define. The service level agreement (SLA) operation monitors the target with periodic Internet Control Message Protocol (ICMP) echo requests. If an echo reply is not received, the object is considered down, and the associated route is removed from the routing table. A previously configured backup route is used in place of the route that is removed. While the backup route is in use, the SLA monitor operation continues to try to reach the monitoring target. Once the target is available again, the first route is replaced in the routing table, and the backup route is removed.

Note: The configuration described in this document can not be used for load balancing or load sharing as it is not supported on ASA/PIX . Use this configuration for redundancy or backup purposes only. Outgoing traffic uses the primary ISP and then the secondary ISP, if the primary fails. Failure of the primary ISP causes a temporary disruption of traffic.

Prerequisites

Requirements

Choose a monitoring target that can respond to ICMP echo requests. The target can be any network object that you choose, but a target that is closely tied to your ISP connection is recommended. Some possible monitoring targets include:

- The ISP gateway address

- Another ISP-managed address

- A server on another network, such as a AAA server, with which the security appliance needs to communicate

- A persistent network object on another network (a desktop or notebook computer that you can shut down at night is not a good choice)

This document assumes that the security appliance is fully operational and configured to allow the Cisco ASDM to make configuration changes.

Note: For information about how to allow the ASDM to configure the device, refer to [Allowing HTTPS Access for ASDM](#).

Components Used

The information in this document is based on these software and hardware versions:

- Cisco PIX Security Appliance 515E with software version 7.2(1) or later

- Cisco Adaptive Security Device Manager 5.2(1) or later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

You can also use this configuration with the Cisco ASA 5500 Series Security Appliance version 7.2(1).

Note: The **backup interface** command is required to configure the fourth interface on the ASA 5505. Refer to [backup interface](#) for more information.

Conventions

For more information about document conventions, refer to the [Cisco Technical Tips Conventions](#).

Background Information

In this example, the security appliance maintains two connections to the Internet. The first connection is a high speed leased line that is accessed through a router provided by the primary ISP. The second connection is a lower speed digital subscriber line (DSL) line that is accessed through a DSL modem provided by the secondary ISP.

Note: Load balancing does not occur in this example.

The DSL connection is idle as long as the leased line is active and the primary ISP gateway is reachable. However, if the connection to the primary ISP goes down, the security appliance changes the routing table to direct traffic to the DSL connection. Static route tracking is used to achieve this redundancy.

The security appliance is configured with a static route that directs all Internet traffic to the primary ISP. Every 10 seconds the SLA monitor process checks to confirm that the primary ISP gateway is reachable. If the SLA monitor process determines that the primary ISP gateway is not reachable, the static route that directs traffic to that interface is removed from the routing table. In order to replace that static route, an alternate static route that directs traffic to the secondary ISP is installed. This alternate static route directs traffic to the secondary ISP through the DSL modem until the link to the primary ISP is reachable.

This configuration provides a relatively inexpensive way to ensure that outbound Internet access remains available to users behind the security appliance. As described in this document, this setup may not be suitable for inbound access to resources behind the security appliance. Advanced networking skills are required to achieve seamless inbound connections. These skills are not covered in this document.
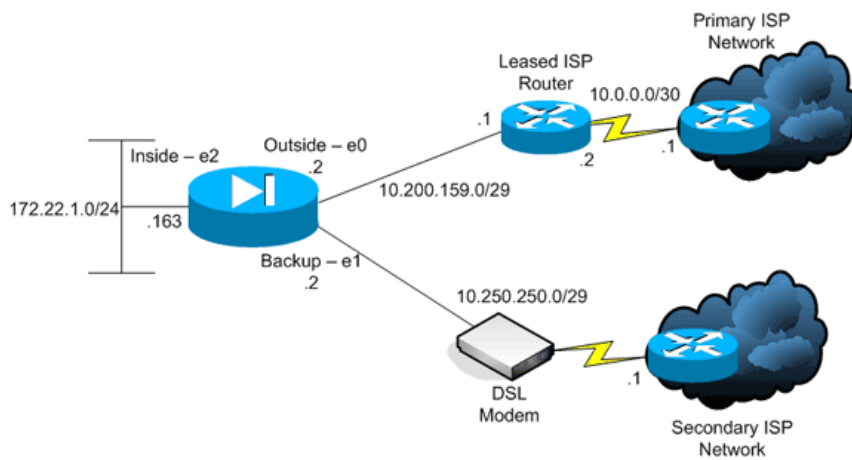
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: The IP addresses used in this configuration are not legally routable on the Internet. They are [RFC 1918](#) addresses which are used in a lab environment.

Network Diagram

This document uses this network setup:

Configurations

This document uses these configurations:

- Command-Line Interface (CLI)

- Adaptive Security Device Manager (ASDM)

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

CLI Configuration

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
```
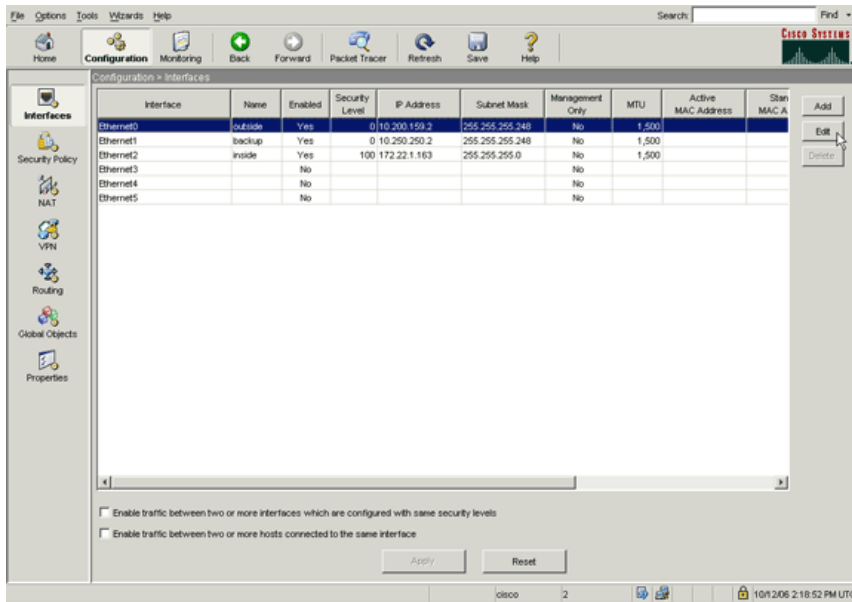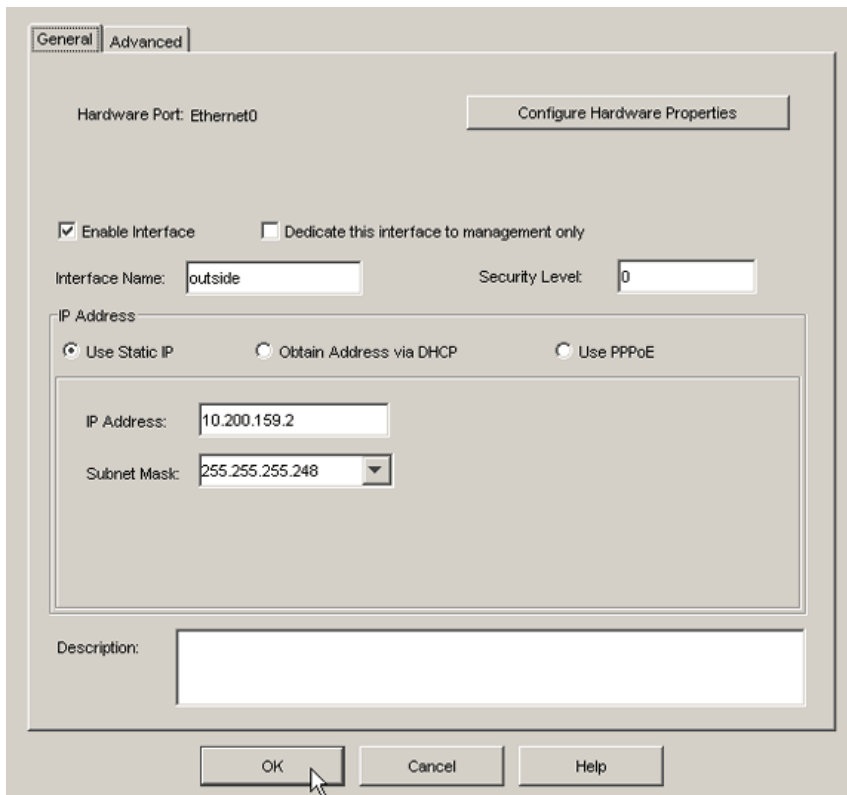
ASDM Configuration

In order to configure redundant or backup ISP support with the ASDM application, complete these steps:

1. In the ASDM application, click **Configuration**, and then click **Interfaces**.

2. From the Interfaces list, select **Ethernet0**, and then click **Edit**.
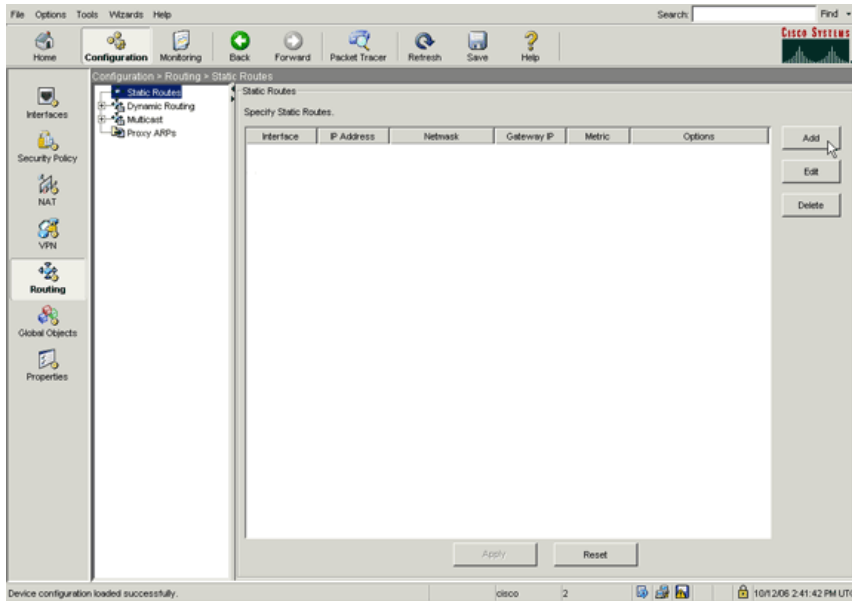
    This dialog box appears.

3. Check the **Enable Interface** check box, and enter values in the Interface Name, Security Level, IP Address, and Subnet Mask fields.

4. Click **OK** in order to close the dialog box.

5. Configure other interfaces as needed, and click **Apply** in order to update the security appliance configuration.
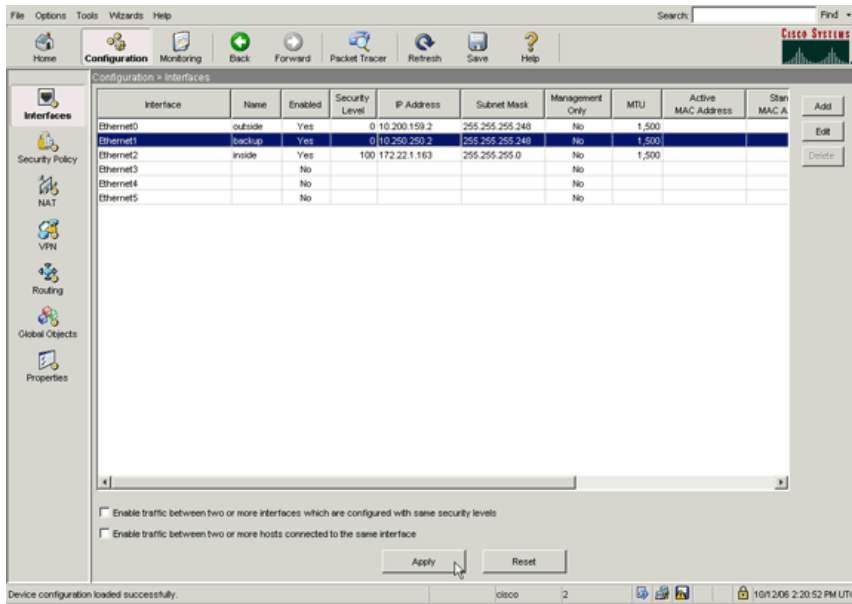
6. Click **Routing** located on the left side of the ASDM application.

7. Click **Add** in order to add the new static routes.

   This dialog box appears.

8. From the Interface Name drop-down list, choose the interface on which the route resides, and configure the default route to reach the gateway. In this example, 10.0.0.1 is the primary ISP gateway, as well as the object to monitor with ICMP echos.

9. In the Options area, click the **Tracked** radio button, and enter values in the Track ID, SLA ID, and Track IP Address fields.

10. Click **Monitoring Options**.

   This dialog box appears.

11. Enter values for frequency and other monitoring options, and click **OK**.

12. Add another static route for the secondary ISP in order to provide a route to reach the Internet.

   In order to make it a secondary route, configure this route with a higher metric, such as 254. If the primary route (primary ISP) fails, that route is removed from the routing table. This secondary route (secondary ISP) is installed in the PIX routing table instead.

13. Click **OK** in order to close the dialog box.

The configurations appear in the Interface list.
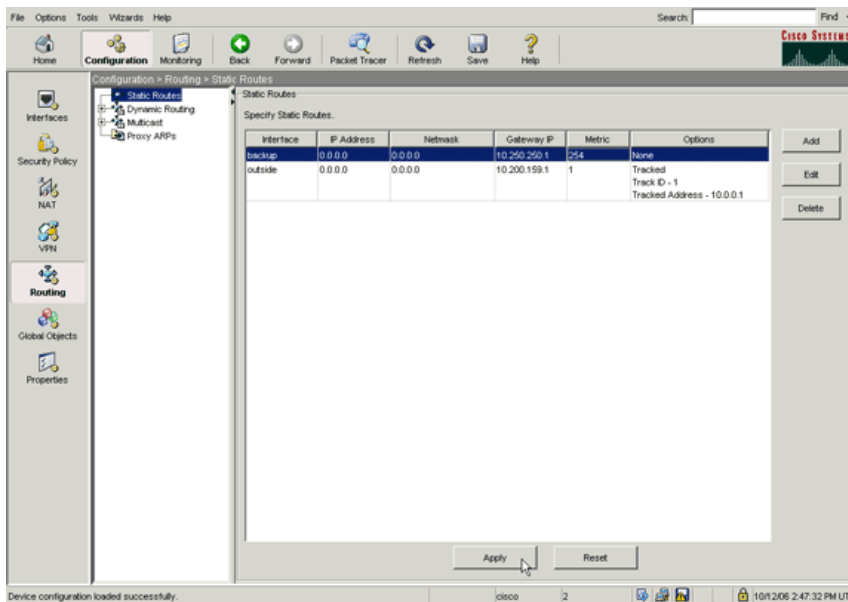
14. Select the routing configuration, and click **Apply** in order to update the security appliance configuration.

Verify

Use this section to confirm that your configuration works properly.

Confirm the Configuration is Complete

Use these **show** commands to verify that your configuration is complete.

The <u>Output Interpreter Tool</u> (<u>registered</u> customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show running-config sla monitor**—Displays the SLA commands in the configuration.

```
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** —Displays the current configuration settings of the operation.

```
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**—Displays the operational statistics of the SLA operation.

  - Before the primary ISP fails, this is the operational state:

```
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
```

  - After the primary ISP fails (and the ICMP echos time out), this is the operational state:

```
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
```

Confirm the Backup Route is Installed (CLI Method)

Use the **show route** command to determine when the backup route is installed.

- Before the primary ISP fails, this is the routing table:

```
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
```

- After the primary ISP fails, the static route is removed, and the backup route is installed, this is the routing table:

```
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
```
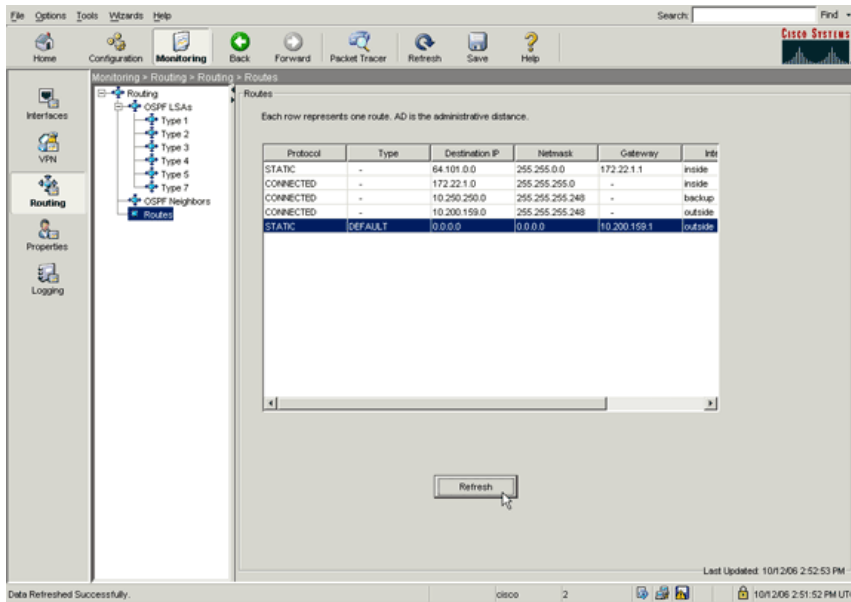
**Confirm the Backup Route is Installed (ASDM Method)**

In order to confirm with the ASDM that the backup route is installed, complete these steps:

1. Click **Monitoring**, and then click **Routing**.

2. From the Routing tree, choose **Routes**.

   ○ Before the primary ISP fails, this is the routing table:

The DEFAULT route points to 10.0.0.2 through the outside interface.

- After the primary ISP fails, the route is removed, and the backup route is installed. The DEFAULT route now points to 10.250.250.1 through the backup interface.
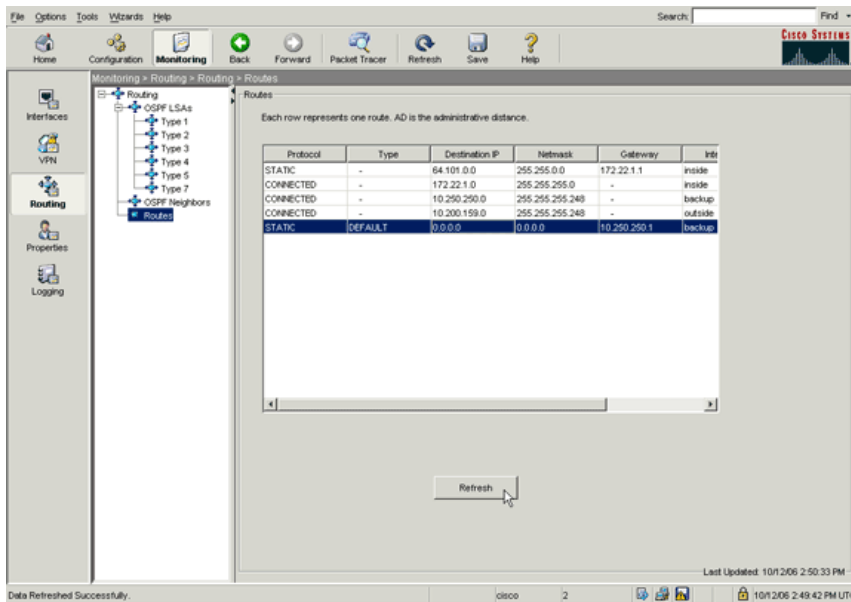
Troubleshoot

Debug Commands

- **debug sla monitor trace**—Displays progress of the echo operation.

  - The tracked object (primary ISP gateway) is up, and ICMP echos succeed.

    ```
    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
    ```

  - The tracked object (primary ISP gateway) is down, and ICMP echos fail.

```
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**—Displays errors that the SLA monitor process encounters.

  - The tracked object (primary ISP gateway) is up, and ICMP succeeds.

    ```
    %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
    ```

  - The tracked object (primary ISP gateway) is down, and the tracked route is removed.

    ```
    %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.
    ```

Tracked Route is Removed Unnecessarily

If the tracked route is removed unnecessarily, ensure that your monitoring target is always available to receive echo requests. In addition, ensure that the state of your monitoring target (that is, whether or not the target is reachable) is closely tied to the state of the primary ISP connection.

If you choose a monitoring target that is farther away than the ISP gateway, another link along that route may fail or another device may interfere. This configuration may cause the SLA monitor to conclude that the connection to the primary ISP has failed and cause the security appliance to unnecessarily fail over to the secondary ISP link.

For example, if you choose a branch office router as your monitoring target, the ISP connection to your branch office could fail, as well as any other link along the way. Once the ICMP echos that are sent by the monitoring operation fail, the primary tracked route is removed, even though the primary ISP link is still active.

In this example, the primary ISP gateway that is used as the monitoring target is managed by the ISP and is located on the other side of the ISP link. This configuration ensures that if the ICMP echos that are sent by the monitoring operation fail, the ISP link is almost surely down.

SLA Monitoring on ASA

Problem:

SLA monitoring does not work after the ASA is upgrade to version 8.0.

Solution:

The problem is possibly be due to the **IP Reverse-Path** command configured in the **OUTSIDE** interface. Remove the command in ASA and try to check the SLA Monitoring.

Cisco Support Community - Featured Conversations

Cisco Support Community is a forum for you to ask and answer questions, share suggestions, and collaborate with your peers. Below are just some of the most recent and relevant conversations happening right now.

Want to see more? Join us by clicking **here**

ASA/PIX 7.x to Support Dual ISP Links **p.mckay** **7 Replies** 4 years, 1 month ago

Redundant or Backup ISP Links **pravinxyz** **2 Replies** 2 years, 41 minutes ago

Redundant VPN connection through a... **rbaker46725** **1 Reply** 7 months, 3 weeks ago

ASA and redundant/backup ISP connections **p-weir** **0 Replies** 3 years, 9 months ago

ASA5510 with two ISP **osoamazin** **8 Replies** 3 years, 6 months ago

ASA 5505 with two ISP connections **mohammed.amer** **3 Replies** 8 months, 1 week ago

Redundant ISP Links **mark.j.hodge** **2 Replies** 2 years, 9 months ago

Redundant IPSEC Tunnels - ASA 5505 to... **scondon** **2 Replies** 3 years, 1 month ago

Valid redundant dual-homed ISP config... **jlaay-diode** **13 Replies** 2 years, 8 months ago

IPsec site to site VPN with PAT through... **2colin-cant** **3 Replies** 1 month, 2 weeks ago

Start A New Discussion   **Subscribe**

Related Information

- **Configuring Static Route Tracking**
- **PIX/ASA 7.2 Command Reference**
- **Cisco ASA 5500 Series Security Appliances**
- **Cisco PIX 500 Series Security Appliances**
- **Technical Support & Documentation - Cisco Systems**

Updated: Oct 13, 2008   Document ID: 70559