ASA/PIX 7.x to Support Dual ISP Links Configuration Example

Document ID: 70559

Introduction

This document provides a sample configuration on how to use dual ISP support on the PIX/Adaptive Security Appliance (ASA) for redundant Internet connections. This feature is known as Static Route Tracking. There are two static routes, one to each ISP. The secondary ISP route has a higher administrative distance. With the use of Static Route Tracking, the PIX/ASA installs the backup ISP route in the routing table as a default route for the Internet if the primary ISP route fails. The security appliance in the main office uses Internet Control Message Protocol (ICMP) echo requests to monitor the reachability of the primary ISP exit route. If that gateway becomes unavailable, the primary default route is removed from the routing table and the floating route to the secondary ISP is used in its place.

This document also describes how to use the Cisco Adaptive Security Device Manager (ASDM) to configure the PIX 500 Series Security Appliance or ASA 5500 Series Security Appliance for Static Route Tracking.

Note: This configuration does not work for load balancing/load sharing. Use this configuration only for backup purposes. 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

When you select a monitoring target, make sure it can respond to ICMP echo requests. The target can be any network object that you choose, but consider the use of:

- the ISP gateway address
- the next hop gateway address (if you are concerned about the availability of the ISP gateway)

- a server on the target network, such as an AAA server, for which the security appliance needs to communicate
- a persistent network object on the destination network (desktop or notebook computer that you can shut down at night is not a good choice)

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

Note: Refer to Allowing HTTPS Access for ASDM to allow the ASDM to configure the device.

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

This configuration can also be used with Cisco ASA 5500 Series Security Appliance version 7.2(1).

Note: The configuration of the fourth interface on ASA 5505 requires the **backup interface** command

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

One of the problems with static routes is that there is no inherent mechanism for determining if the route is up or down. They remain in the routing table even if the next hop gateway becomes unavailable. Static routes are only removed from the routing table if the associated interface on the security appliance goes down.

The static route tracking feature provides a method to track the availability of a static route and install a backup route if the primary route fails. For example, this allows you to define a default route to an ISP gateway and a backup default route to a secondary ISP in case the primary ISP becomes unavailable.

The security appliance does this by associating a static route with a monitoring target that you define. It monitors the target using ICMP echo requests. If an echo reply is not received within a specified time period, 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 removed route.

Configure

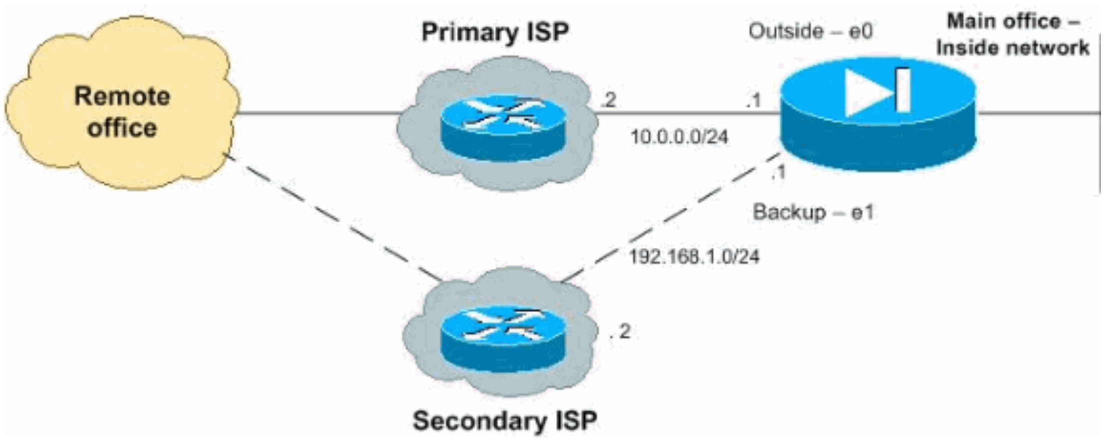
In this section, you are presented with the information to configure the features described in this document.

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

Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which have been used in a lab environment.

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations:

- PIX
- ASDM

PIX

```
pix#show run
: Saved
:
PIX Version 7.2(1)
!
hostname pix
enable password 8Ry2YjIyt7RRXU24 encrypted
names
dns-guard
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.0.0.1 255.255.255.0
!
interface Ethernet1
 nameif backup
 security-level 0
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet2
 nameif inside
 security-level 100
 ip address 172.16.1.1 255.255.255.0
```

```
!

!--- For testing only. Be more specific about what IP
!--- addresses you accept ICMP packets from.

access-list 101 extended permit ip any any
access-list 102 extended permit icmp any any
pager lines 24

mtu outside 1500
mtu outside1 1500
mtu inside 1500
mtu inside2 1500

icmp permit any outside
icmp permit any inside
icmp permit any inside2
asdm image flash:/asdm-511.bin
no asdm history enable
arp timeout 14400

nat (inside) 1 access-list 101
global (outside) 1 10.0.0.1
global (backup) 1 192.168.1.1

access-group 102 in interface outside
access-group 102 in interface backup


!--- 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.


route outside 0.0.0.0 0.0.0.0 10.0.0.2 1 track 1


!--- 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, the backup route
!--- is installed in the routing
!--- table instead of the tracked route.

route backup 0.0.0.0 0.0.0.0 192.168.1.2 254

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

http server enable
http 172.16.1.0 255.255.255.0 inside

no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart


!--- Configures an SLA operation with an ID of 123 and creates a tracking entry with
!--- the ID of 1 to track the reachability of the SLA. You can create a maximum
!--- of 2000 SLA operations.
!--- You can only debug 32 SLA operations at any time.
```

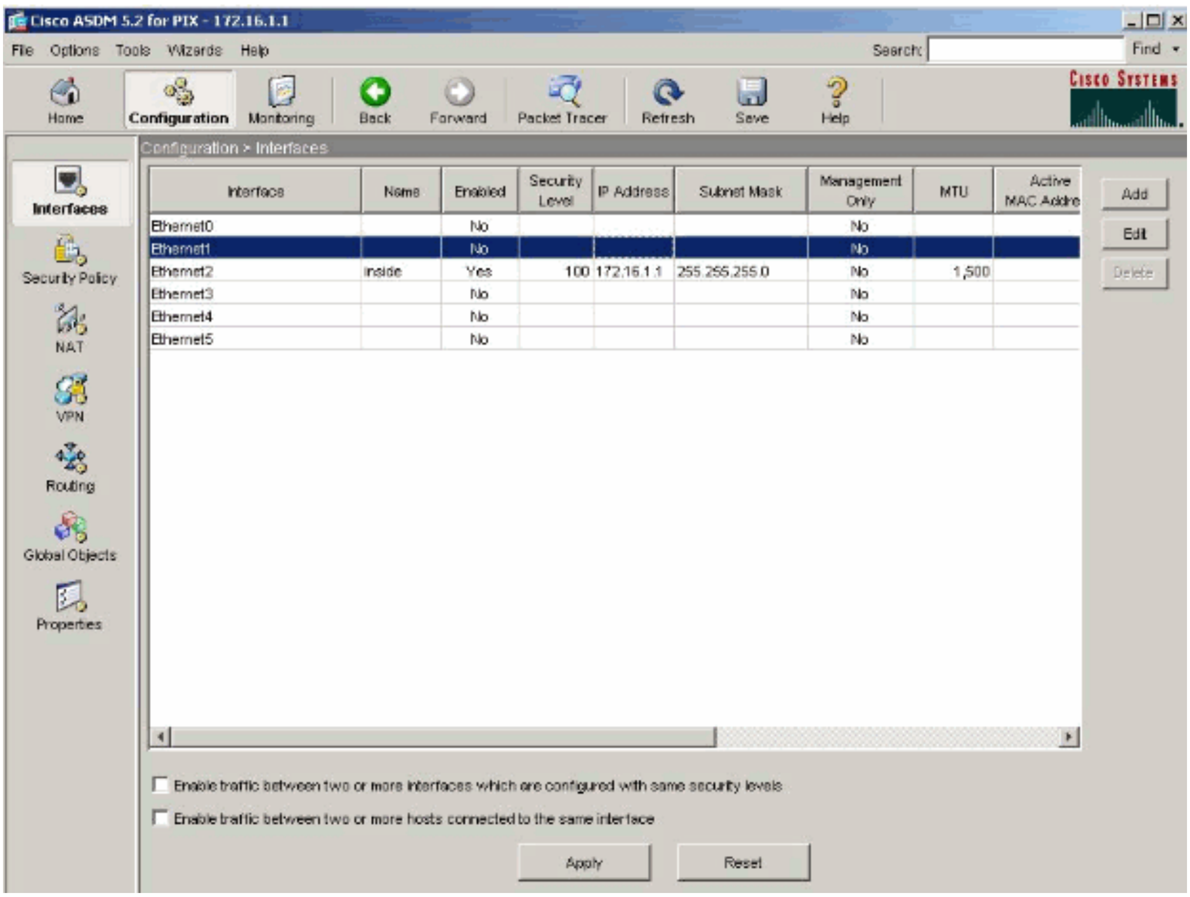
```
sla monitor 123


!--- In SLA monitor configuration mode, specify the monitoring protocol.
!--- In this case it is an ICMP protocol and
!--- the target IP address to poll using ICMP protocol is specified.



 type echo protocol ipIcmpEcho 10.0.0.2 interface outside
 num-packets 3


!--- Specify the rate at which the SLA operation repeats (in seconds)
!--- in SLA monitor configuration mode.


 frequency 10


!--- After you configure an SLA operation, you must schedule the operation
!--- with the sla monitor schedule command.
!--- This sets the time when the SLA operation starts.


sla monitor schedule 123 life forever start-time now


!--- Create a tracking entry to poll the SLA. Enter this command in order to
!--- associate a tracked static route with the SLA monitoring process.


track 1 rtr 123 reachability

telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  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:5681a36389cbdcea8759928009e50777
: end
```

ASDM Configuration

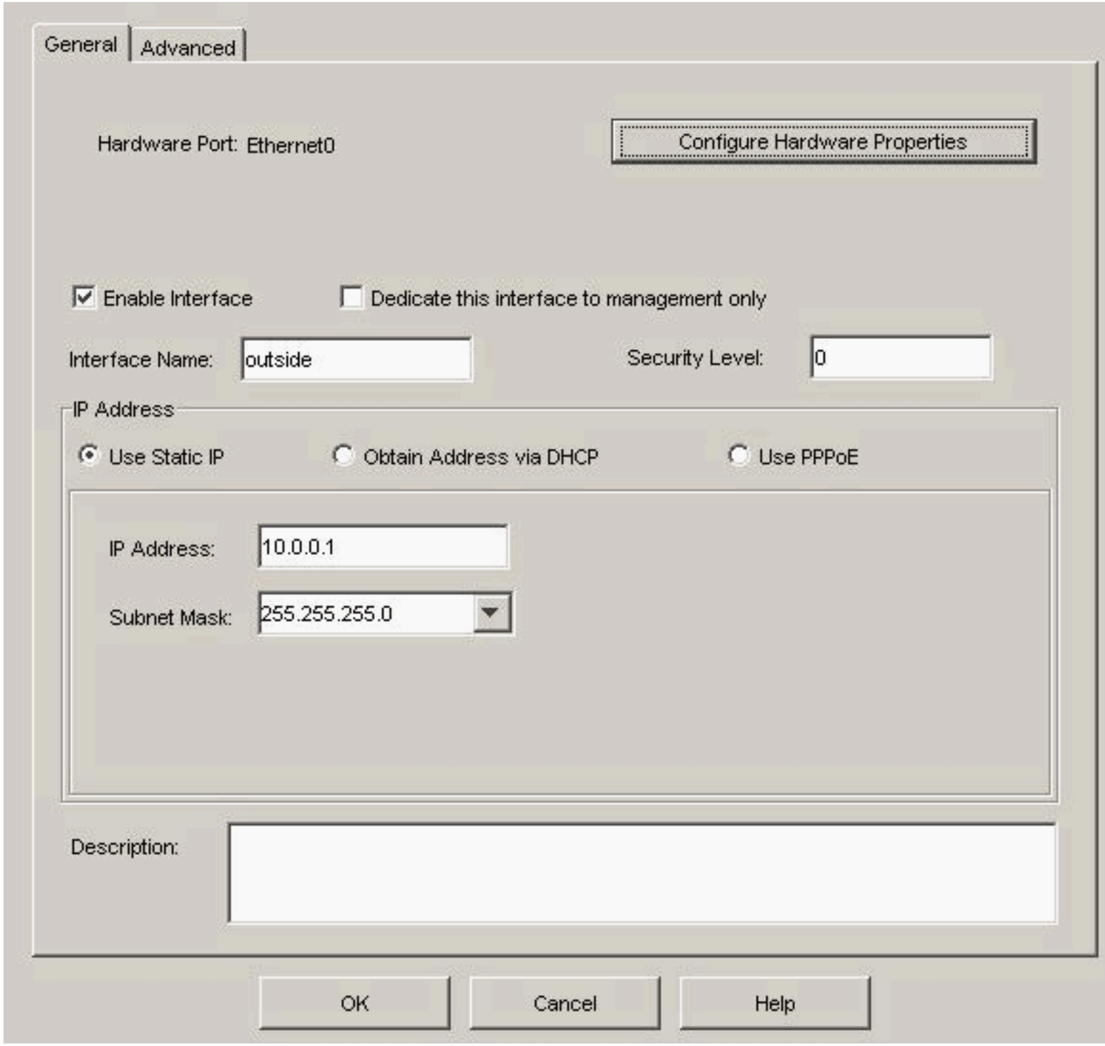
Complete these steps in order to configure dual ISP support using ASDM.

1. Choose **Configuration** > **Interfaces** from the Home window of the ASDM in order to configure the interfaces.

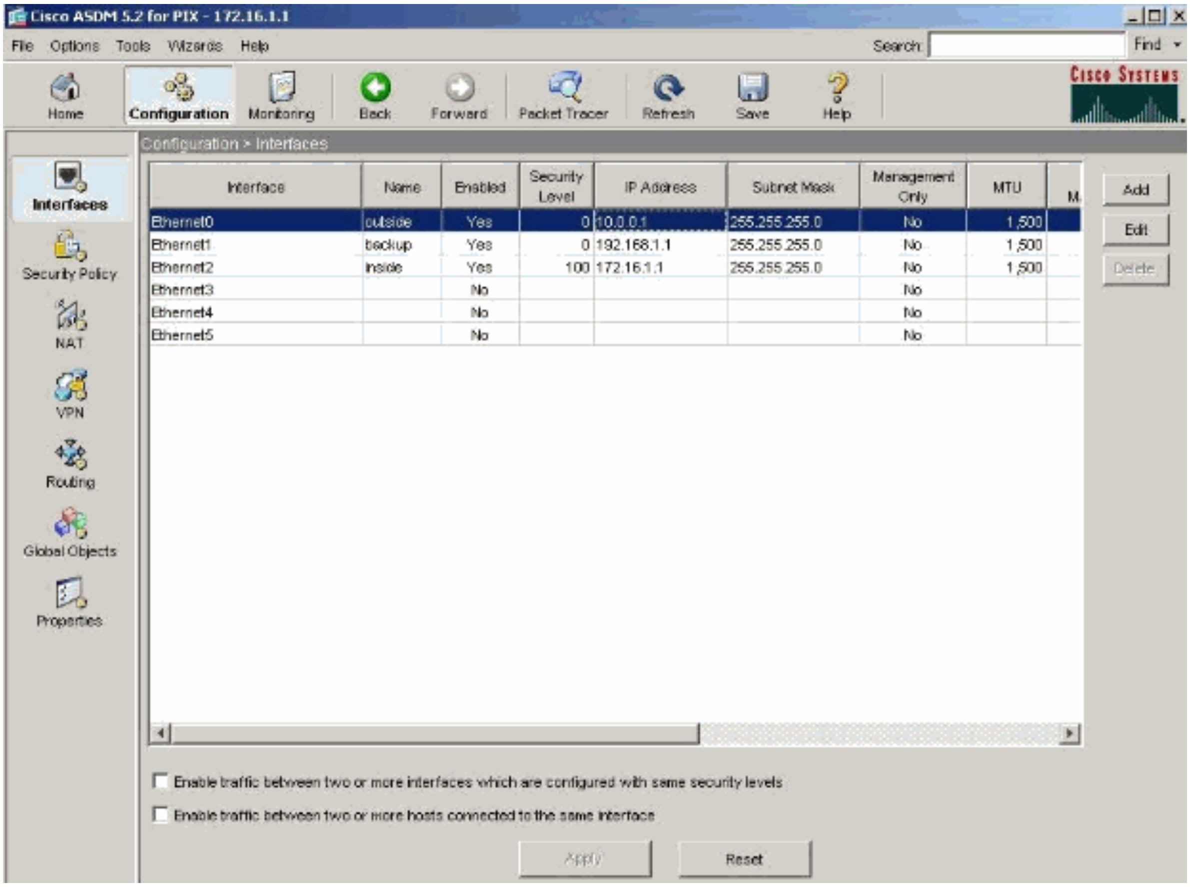


2. Click **Edit** and and check **Enable Interface** in order to configure the interface (Ethernet0).

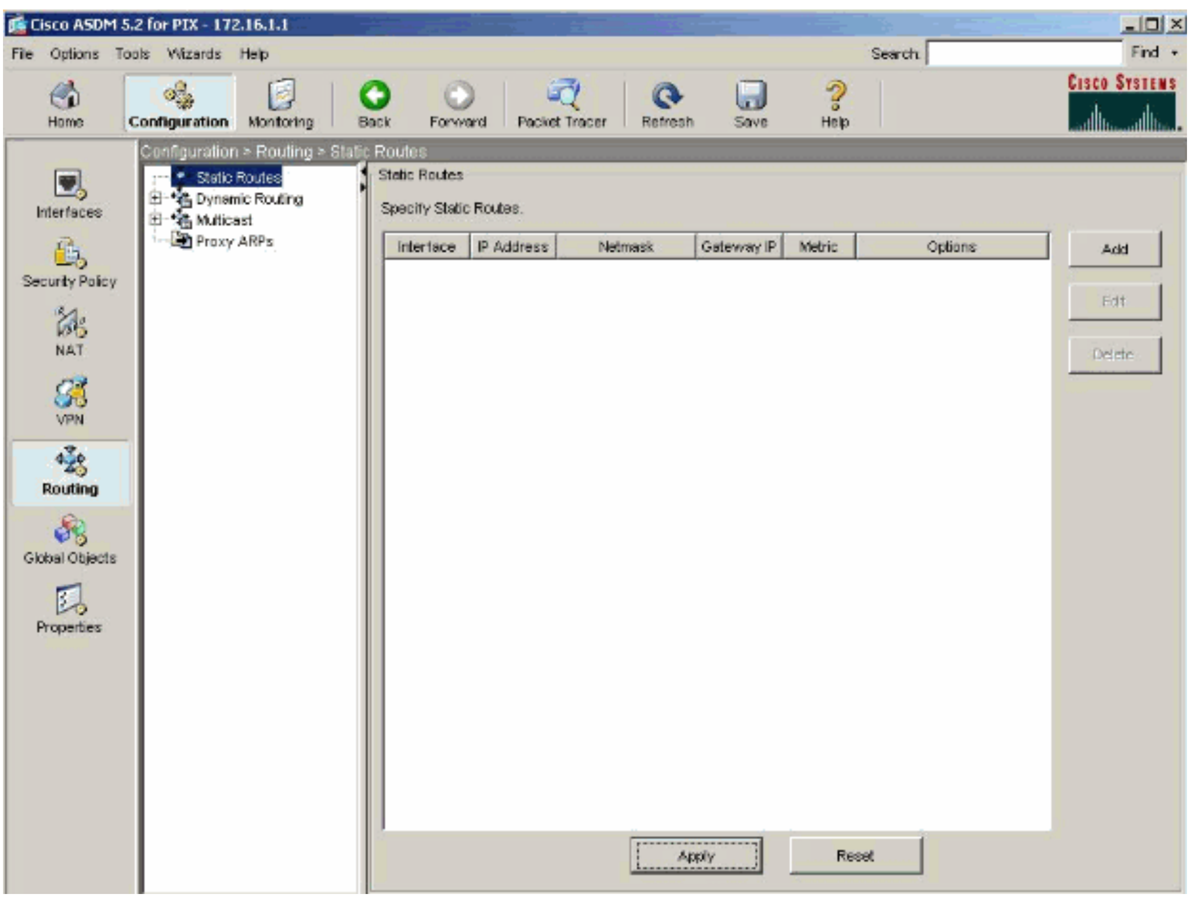
   Provide the Interface Name, Security level, IP Address with Subnet Mask and click **OK** in order to continue to the main page.



3. Similarly, configure the other interfaces like Ethernet1 and click **Apply** in the main menu in order to update the PIX Security Appliance configuration.

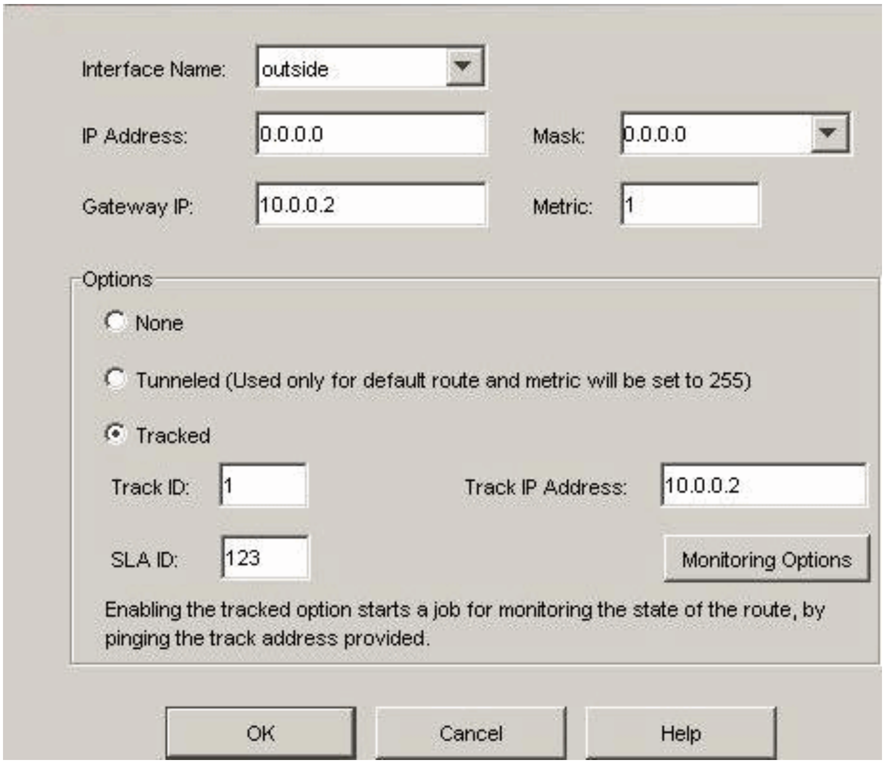


4. Click **Routing** from the Configuration menu and click **Add** in order to add the new static routes.

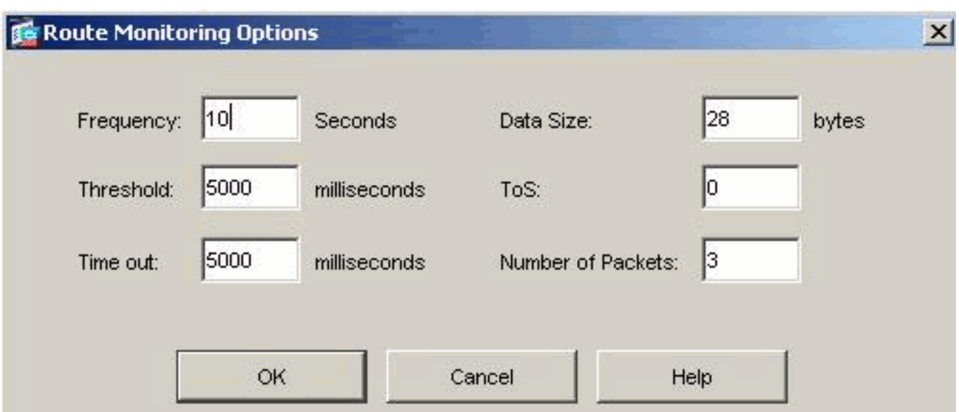


Choose the interface name and configure the default route to reach the gateway. (In this case, 10.0.0.2 is the primary ISP gateway to reach the main office and also to monitor the remote gateway using ICMP protocol.)

5. Click the **Tracked** radio button under Options in order to configure the Track ID, SLA ID and Track IP Address.

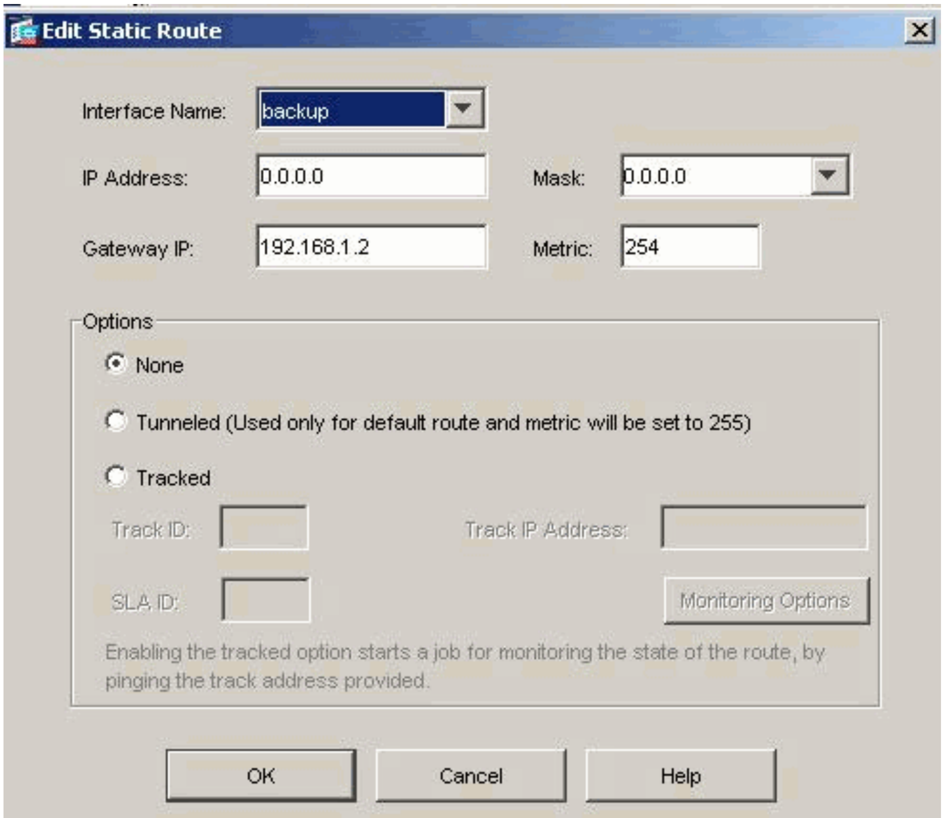


6. Click **Monitoring Options** in order to set the Frequency and other monitoring options and click **OK** to continue.

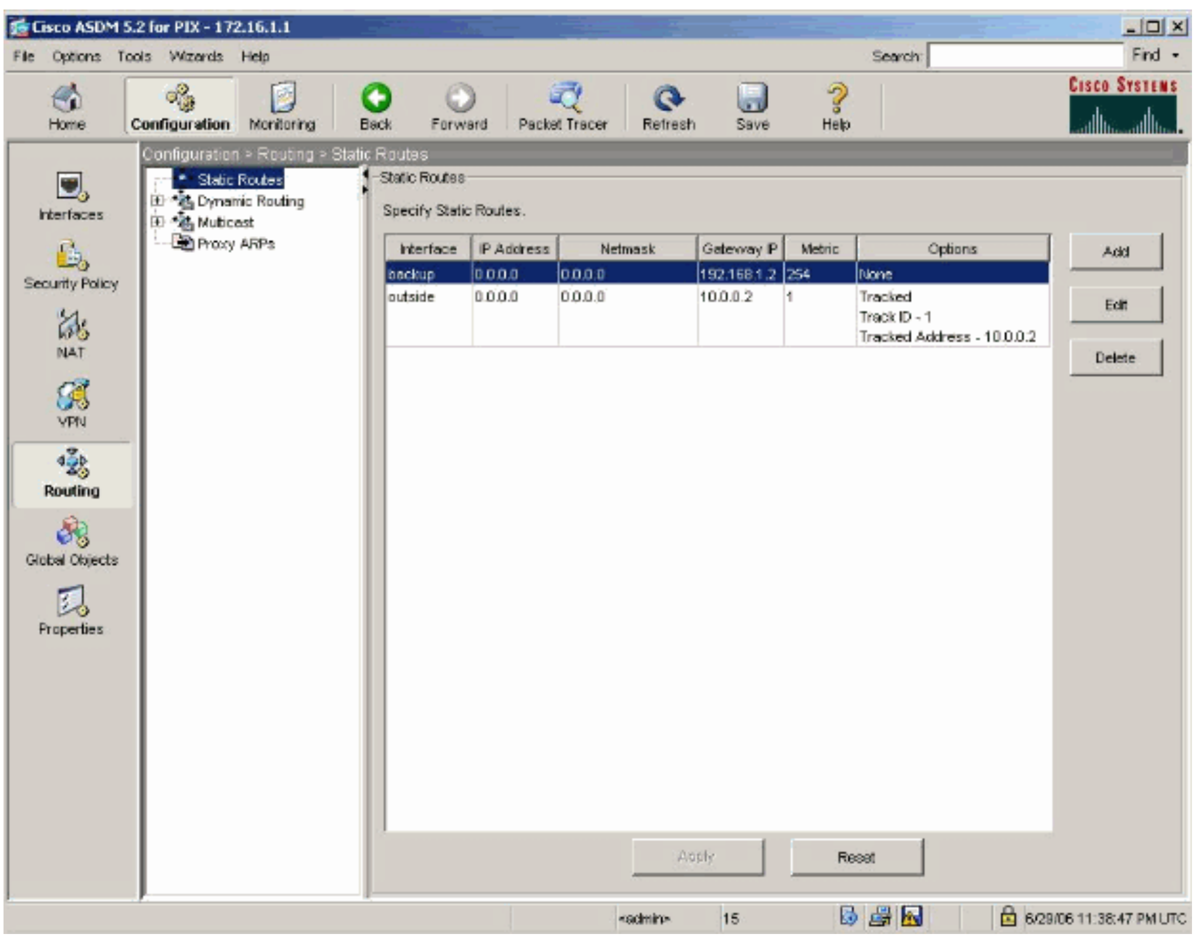


7. Add another static route for the secondary ISP as a backup route to reach the Internet.

Note: Configure the static route with a higher Metric, such as 254, in order to make it a secondary route. If the primary route (Primary ISP) fails, the secondary route (Secondary ISP) is installed in the routing table of the PIX. Click **OK** to return to the main window.



8. Check the **Routing** configuration in the main menu and click **Apply** in order to update the PIX Security Appliance configuration. .



Verify

Use this section to confirm that your configuration was successful.

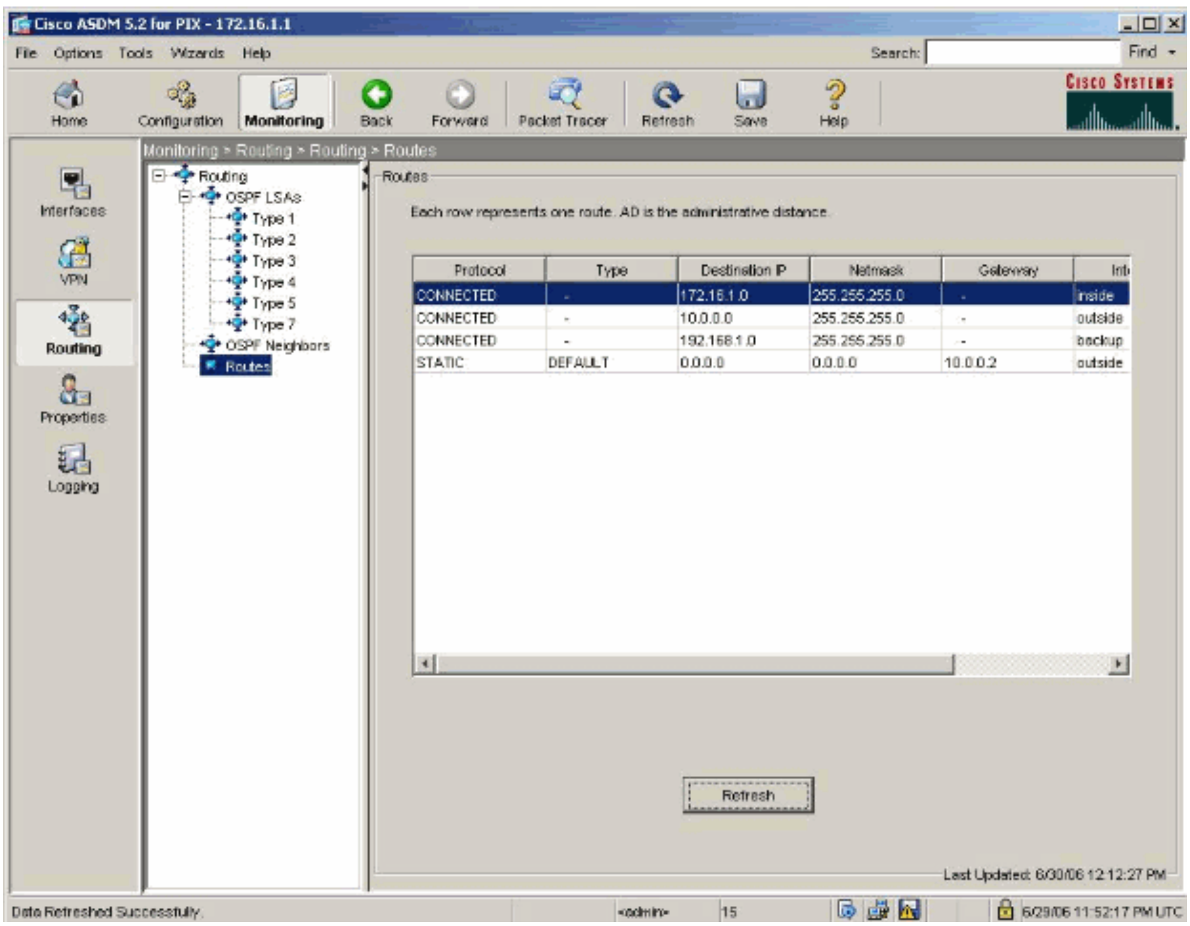
The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show sla monitor** Displays the current configuration settings of the operation.
- **show sla monitor operation−state** Displays the operational statistics of the SLA operation.
- **show running−config sla monitor** Displays the SLA commands in the configuration.

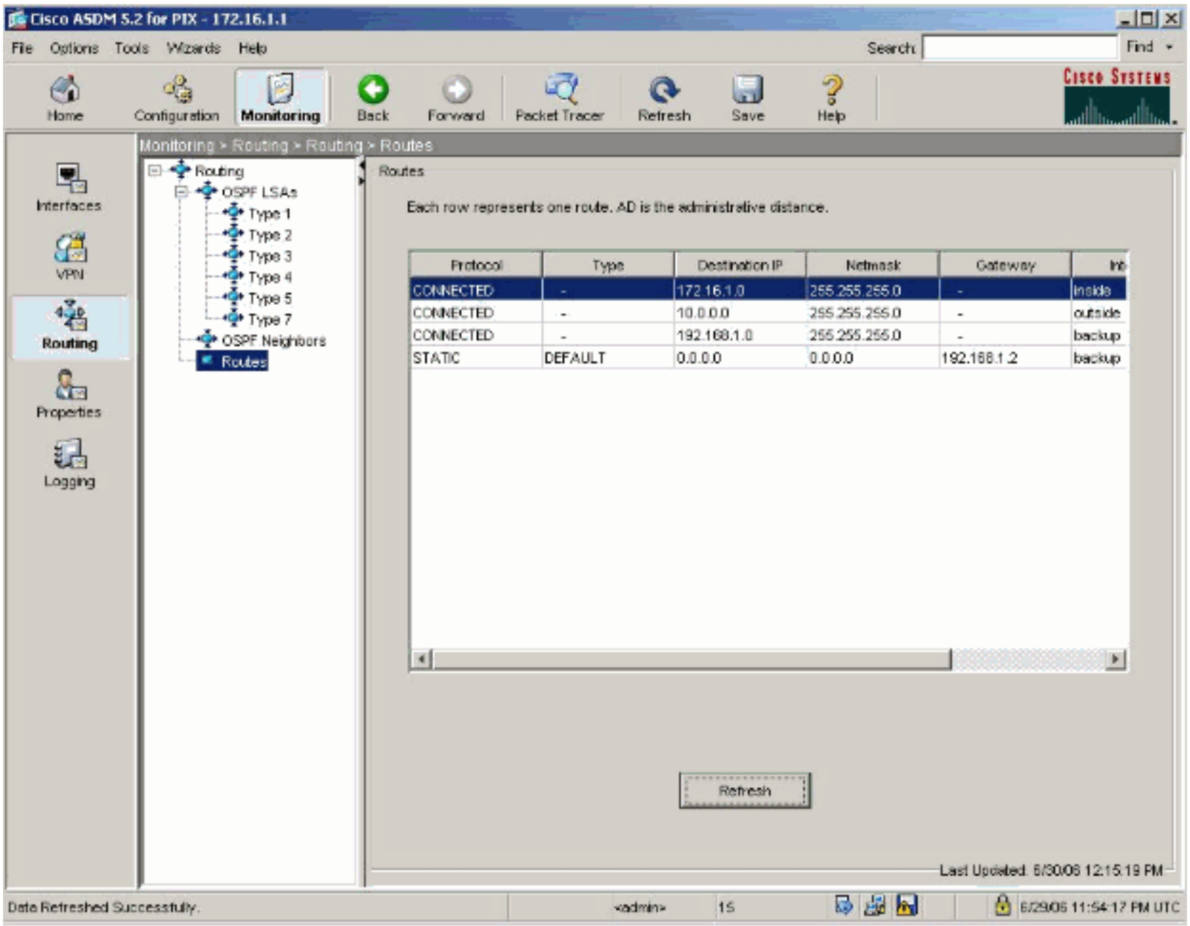
Complete these steps in order to verify the route installed in the routing table using ASDM:

1. Choose **Monitoring** > **Routing** > **Routes** from the Home window of the ASDM.

   The default route installed in the routing table is 10.0.0.2 and is the gateway (Primary ISP) for reaching home office. In CLI mode, use the **show route** command in order to check the routing tables.

2. If the primary gateway (10.0.0.2) is unreachable, the backup route (which is the secondary ISP [192.168.1.2]) is installed in the routing table instead of the tracked route.



Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

NetPro Discussion Forums − Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums − Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

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 03, 2006 Document ID: 70559