



Set Up Your Cisco Router

Home > Work With My Routers > Cisco Routers > Set Up Your Cisco Router

Step 8: Set Up Internet Security on a Cisco Router

- Step 1: [SMB Support Assistant Site Survey](#)
- Step 2: [Set Up Your 800 or SB 100 Router Hardware](#)
[Set Up Your 1700 Series Router Hardware](#)
[Set Up Your 1800 Series Router Hardware](#)
[Set Up Your 2600 Series Router Hardware](#)
[Set Up Your 2800 Series Router Hardware](#)
[Set Up Your 3800 Series Router Hardware](#)
- Step 3: [Download and Install Security Device Manager](#)
- Step 4: [Configure Your Router with Security Device Manager](#)
- Step 5: [Configure Wireless Security on an Integrated Services Router](#)
- Step 6: [Add or Remove a Wireless User on an Integrated Service Router](#)
- Step 7: [Set Up an ADSL Internet Connection](#)
[Set Up an Ethernet Internet Connection](#)
[Set Up an ISDN Internet Connection](#)
[Set Up a T1, E1, or Serial Internet Connection](#)
- Step 8: Set Up Internet Security on a Cisco Router**
 - [Introduction](#)
 - [Requirements](#)**
 - [Configure Firewall Inspection Rules](#)**
 - [Add Access Control List Rules](#)**
 - [Apply an ACL Rule to the Outgoing WAN Interface](#)
 - [Apply an ACL Rule to the Incoming LAN Interface](#)
 - [Configure Network Address Translation](#)**
 - [Set Up NAT with Dynamic WAN IP Address](#)
 - [Set Up NAT with Static WAN IP Address](#)
 - [Next Step](#)**
 - [Troubleshoot the Procedure](#)**
 - [Related Information](#)**

Service Requests

- [Open a service request](#)
- [Update a service request](#)

Feedback

Please rate this site:

++ + +/- - --

Suggestions for improvement:

Download PDF

- [Step 8: Set Up Internet Security on a Cisco Router](#)
- [Set Up Your Cisco Router](#)

If Cisco may contact you for more details or for future feedback opportunities, please enter your contact information:

Full Name:
Email:

Introduction

This document explains how to set up Internet Security on your router. The instructions demonstrate how to set up these security measures:

- Dynamic firewall inspection rules for multimedia applications
- Access Control List (ACL) rules
- Network Address Translation (NAT)

[Back to Top](#)

Requirements

- You must have completed the initial configuration in [Configure Your Router with Security Device Manager](#).
- Completed worksheets from the [Site Survey](#):
 - LAN Addressing Worksheet
 - Internet Worksheet
 - Internet Services Worksheet

[Back to Top](#)

Configure Firewall Inspection Rules

To configure firewall inspection rules, follow these steps:

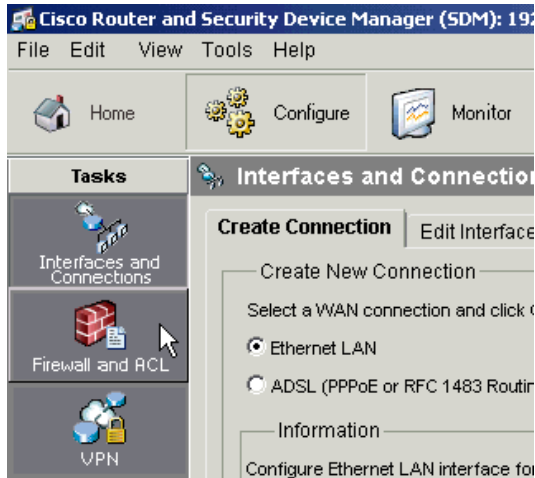
1. Open a web browser and type **http://router-IP-address** in the Address field. Use the IP address that you entered in the LAN Addressing Worksheet (field L6A). Press **Enter** to launch SDM.

Note: For further information about how to launch SDM, refer to Configure Your Router with Security Device Manager.

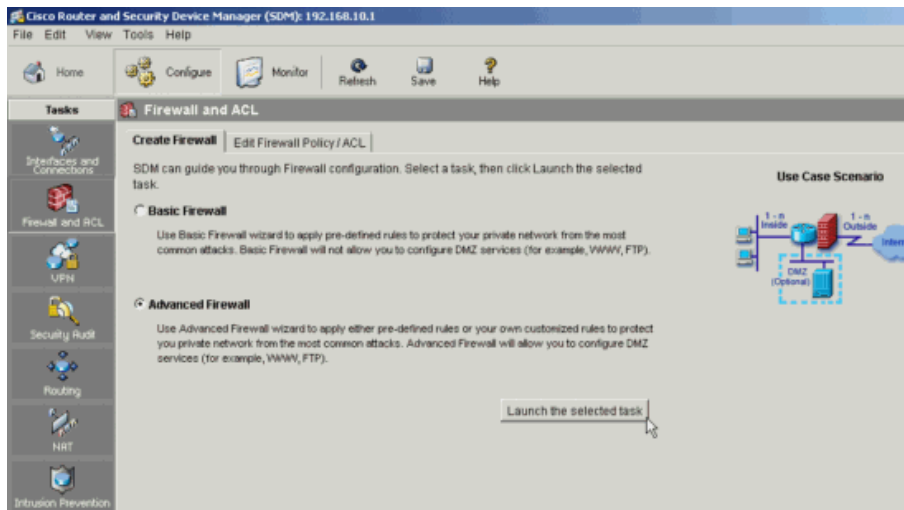
2. Click **Configure**.

[firewall_sdm_conf.gif](#)

3. Click the **Firewall and ACL** tab.

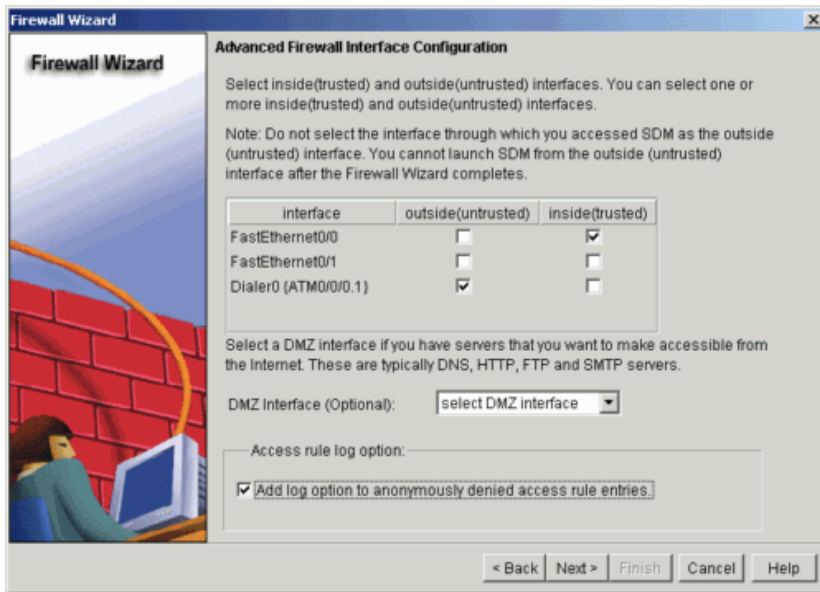


4. Choose **Advanced Firewall** and click **Launch the Selected Task**.



5. Click **Next** at the **Advanced Firewall Configuration Wizard** screen.

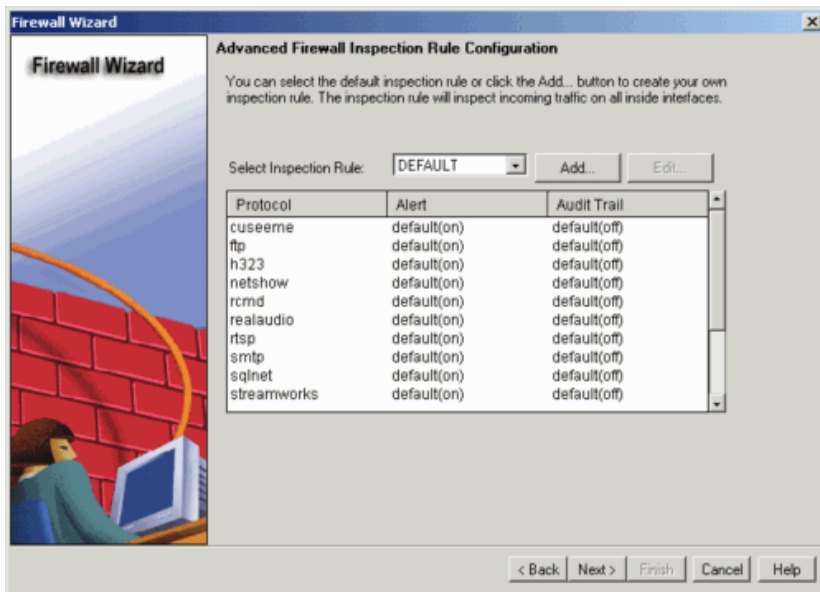
6. Select your inside (trusted) and outside (untrusted) interfaces. The outside (untrusted) interface is your Internet connection, and the inside (trusted) interface is your LAN interface. Do not select a DMZ interface.



Note: The Firewall Wizard automatically creates access control list (ACL) rules to block incoming traffic from IP non-public IP addresses such as 192.168.0.0, 172.0.0.0, and 10.0.0.0. If your Internet Service Provider (ISP) uses non-public IP address inside its network, you need to modify the router ACL rules to allow incoming traffic from private IP address ranges.

Note: To determine if your ISP uses non-public IP addresses, review the addresses in the ISP Address Assignments section of the Internet Worksheet or contact your ISP.

- Click **OK** to confirm the SDM firewall warning message.
- Click **Next** to use the default Firewall Inspection Rules.



- Review the summary of the Firewall inspection rules and click **Finish** to complete the Wizard. Click **OK** to confirm the Commands Delivery Status. Click **OK** again to exit the Wizard.

[Back to Top](#)

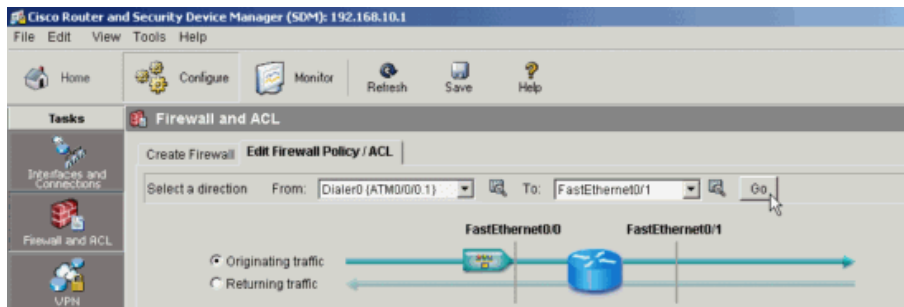
Add Access Control List Rules

To add Access Control List (ACL) rules to the router for additional security, follow these steps:

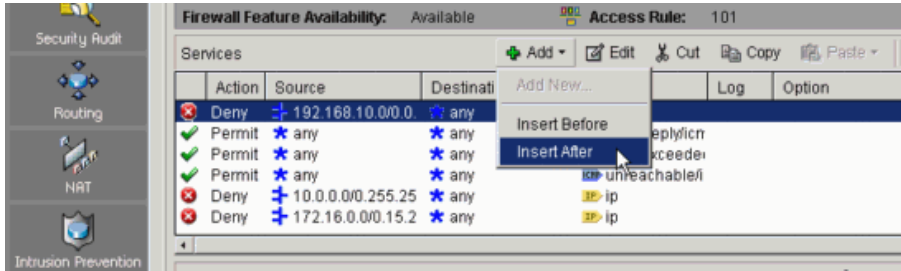
Apply an ACL Rule to the Outgoing WAN Interface

To apply an Access Control List (ACL) rule to the outgoing WAN interface, follow these steps:

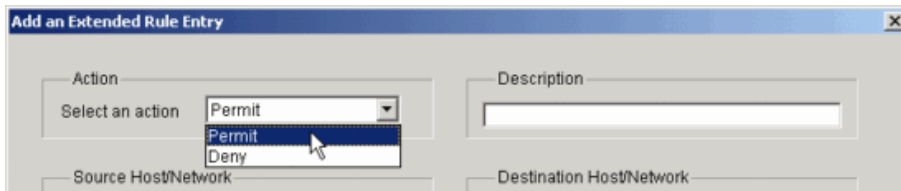
- Click **Edit Firewall Policy/ACL**.
- In the **From** interface, select your LAN interface and click **Go**. In the **To** interface select your WAN interface.



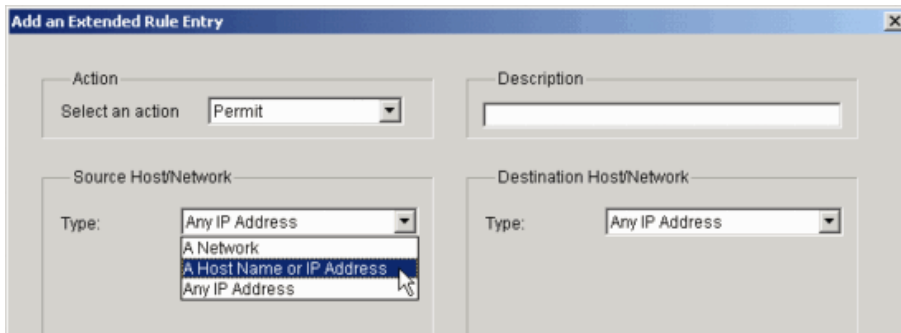
3. Click **Originating Traffic**.
4. Create an ACL rule to block outbound traffic that does not originate from the router WAN IP address.
 - a. Click **Edit Firewall Policy/ACL**.
 - b. Next to **Services**, click **Add > Insert After**.



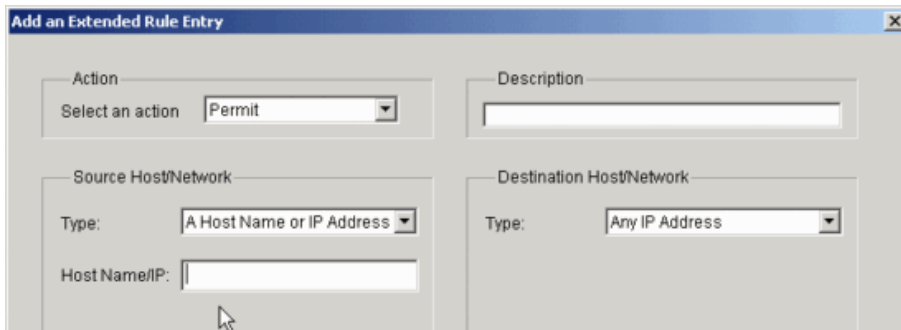
- c. Next to **Select an action**, choose **Permit**.



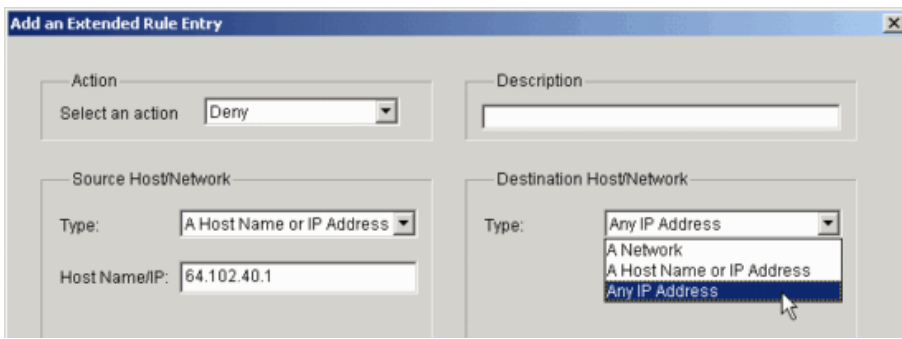
- d. Under **Source Host/Network**, choose **A Host Name or IP Address**.



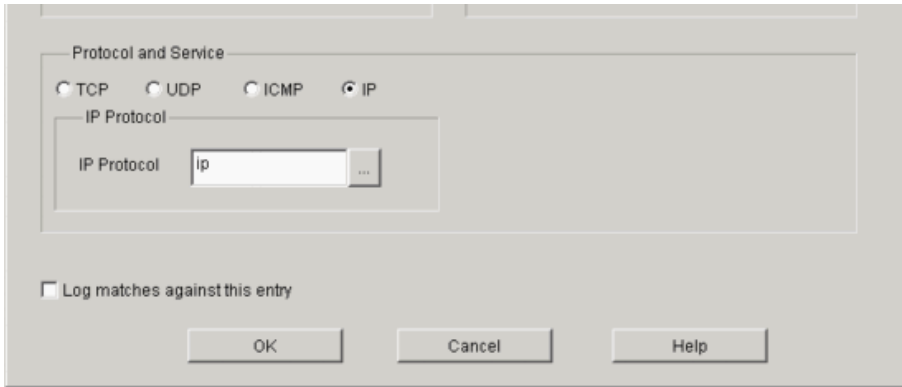
- e. Next to **Hostname/IP**, enter the Router IP address you entered in the Internet Worksheet (B46).



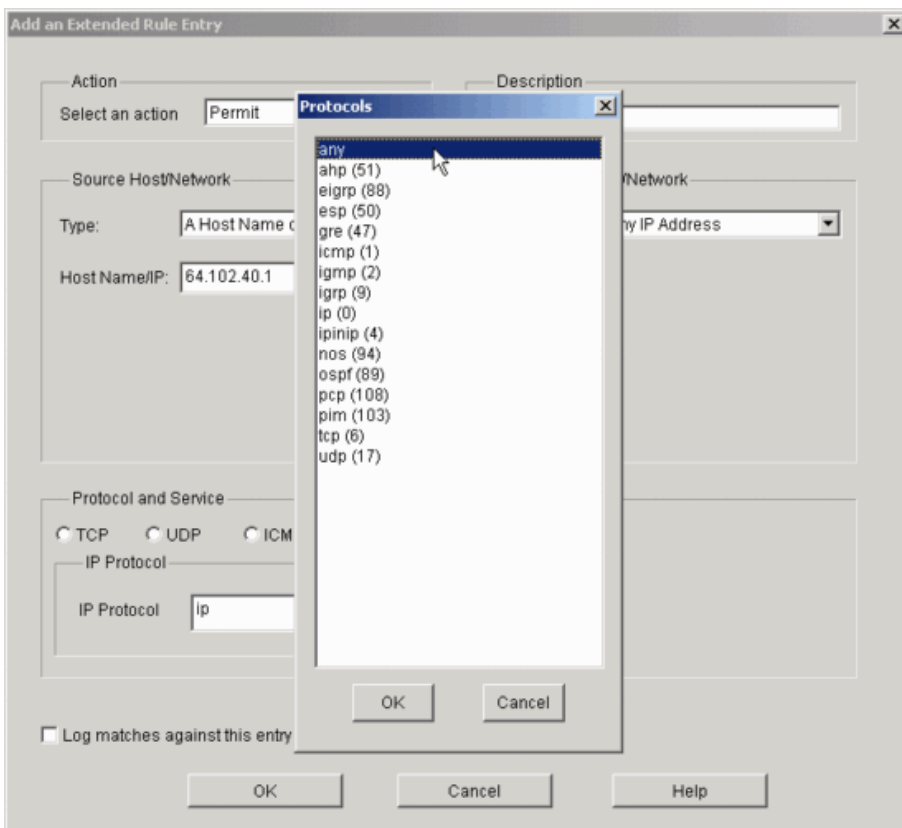
- f. Under **Destination Host/Network**, choose **Any IP Address**.



g. Under **Protocol and Service**, choose **IP**.



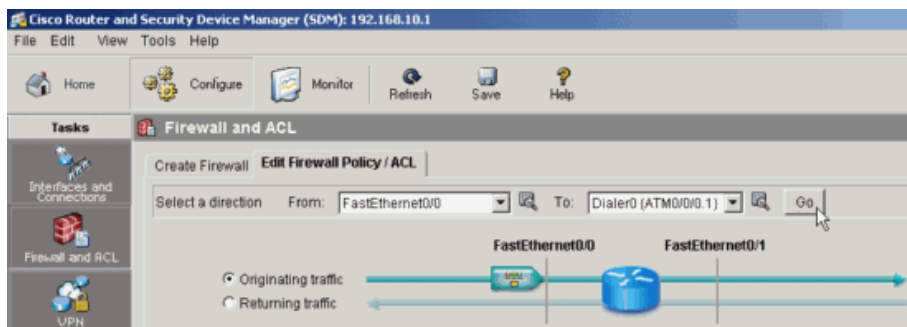
h. Under **IP Protocol**, click the details button (...) and select **any**. Click **OK** to select the service, then click **OK** to confirm the rule.



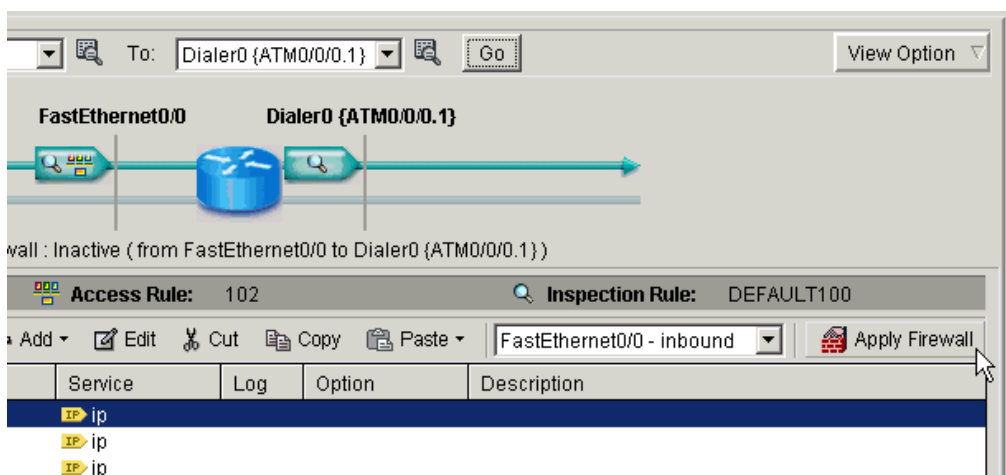
Apply an ACL Rule to the Incoming LAN Interface

To apply an Access Control List (ACL) rule to the incoming WAN interface, follow these steps:

1. In the **From** interface, select your LAN interface and click **Go**. In the **To** interface select your WAN interface.



2. Click **Returning Traffic**.
3. Create an ACL rule to block traffic from LAN that does not have a valid LAN IP address.
 - a. Next to **Services**, click **Add > Insert After**.
 - b. Next to **Select an action**, choose **Permit**.
 - c. Under **Source Host/Network**, choose **A Network**.
 - d. Next to **IP Address**, enter the subnet that you entered in the LAN Addressing Worksheet (L1A), and next to **Wildcard Mask** choose **0.0.0.255**.
 - e. Under **Destination Host/Network**, choose **Any IP Address**.
 - f. Under **Protocol and Service**, choose **IP**.
 - g. Under **IP Protocol**, click the details button (...) and select **any**. Click **OK** to select the service, then click **OK** to confirm the rule.
4. Create an ACL rule to allow broadcast traffic from LAN in order to allow DHCP.
 - a. Next to **Services**, click **Add > Insert After**.
 - b. Next to **Select an action**, choose **Permit**.
 - c. Under **Source Host/Network**, choose **A Network**.
 - d. Next to **IP Address**, enter the subnet that you entered in the LAN Addressing Worksheet (L1A). Next to Wildcard Mask select **0.0.0.255**.
 - e. Under **Destination Host/Network**, choose **Any IP Address** and enter **255.255.255.255**.
 - f. Under **Protocol and Service**, choose **IP**.
 - g. Under **IP Protocol**, click the details button (...) and select **any**. Click **OK** to select the service, then click **OK** to confirm the rule.
5. Click **Apply Firewall**.



[Back to Top](#)

Configure Network Address Translation

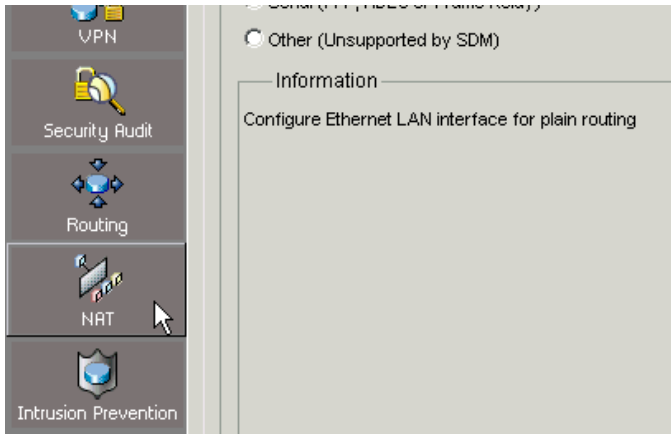
Network Address Translation (NAT) uses an internal address scheme to provide additional security for your network. In order to

set up NAT, you need to know whether your WAN connection uses a static or dynamic IP address. Refer to the Internet Worksheet (B45, B46) for more information.

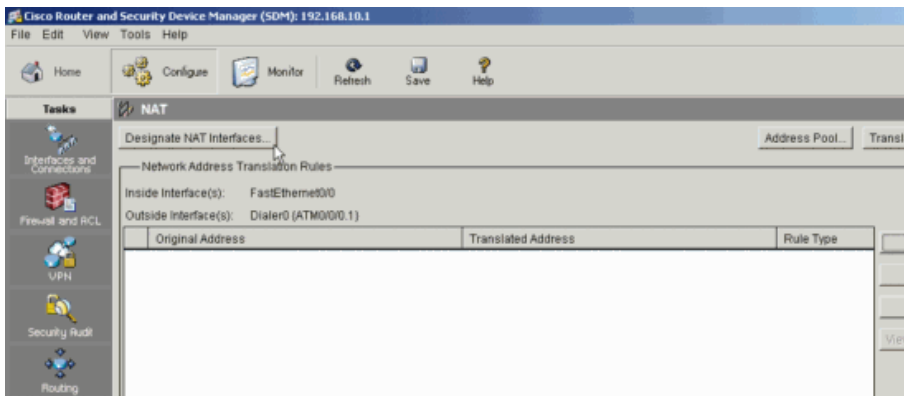
Set Up NAT with Dynamic WAN IP Address

To set up NAT with a dynamic WAN IP address, follow these steps:

1. Click the **NAT** tab.

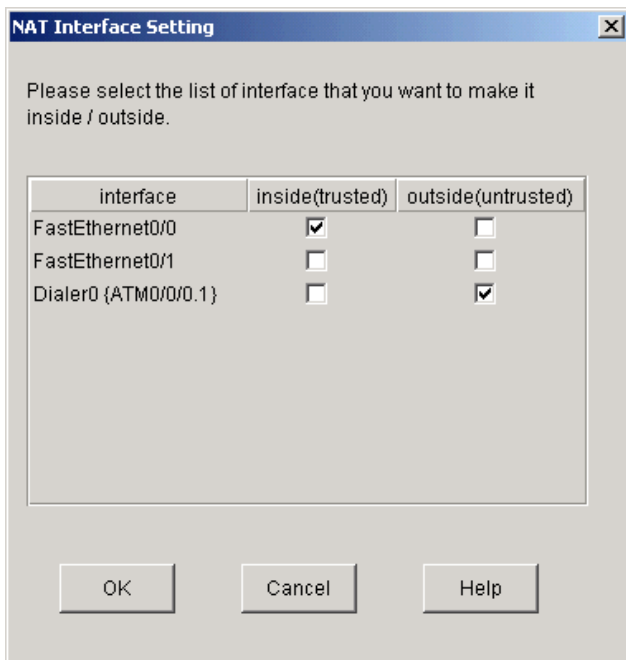


2. Click **Designate NAT Interfaces**.

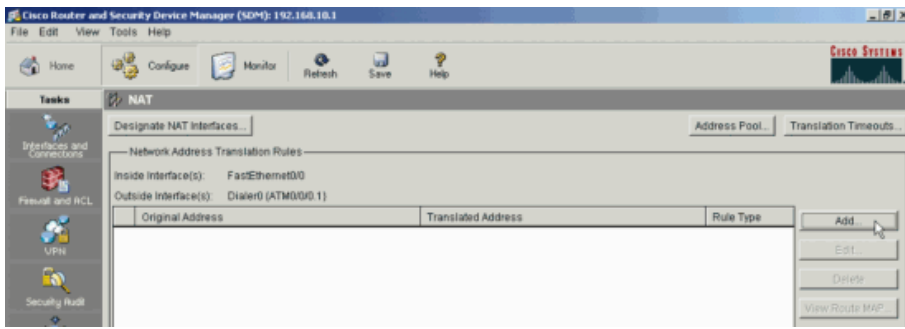


3. Check the Inside (Trusted) and Outside(Untrusted) interfaces and click **OK**.

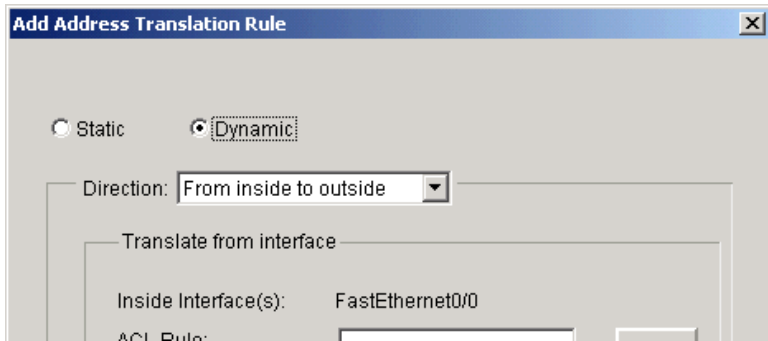
Note: Designate your WAN interface as the outside/untrusted interface.



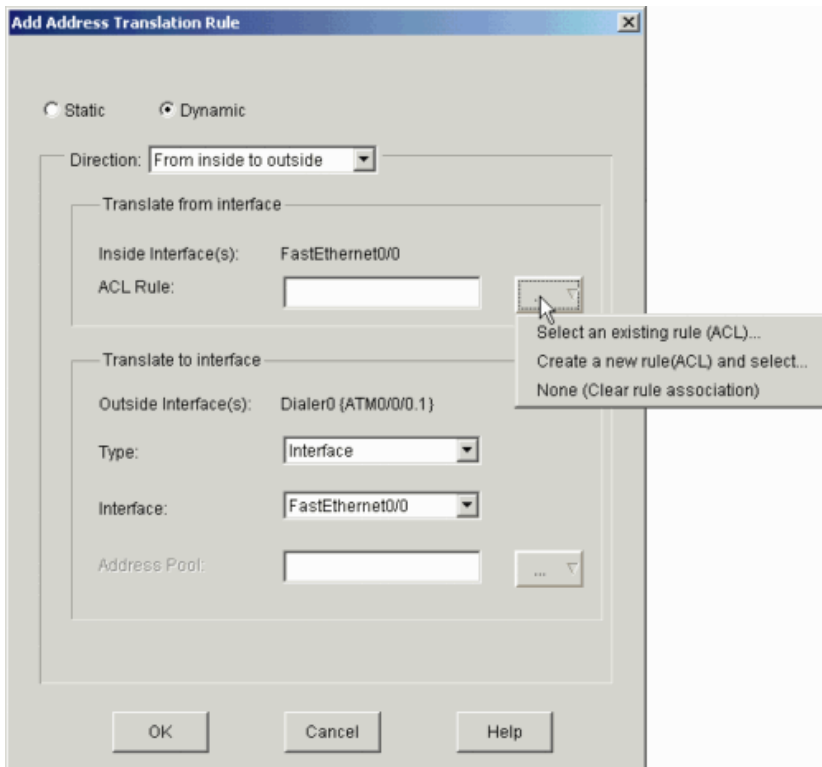
4. Click **Add** to add a new translation rule.



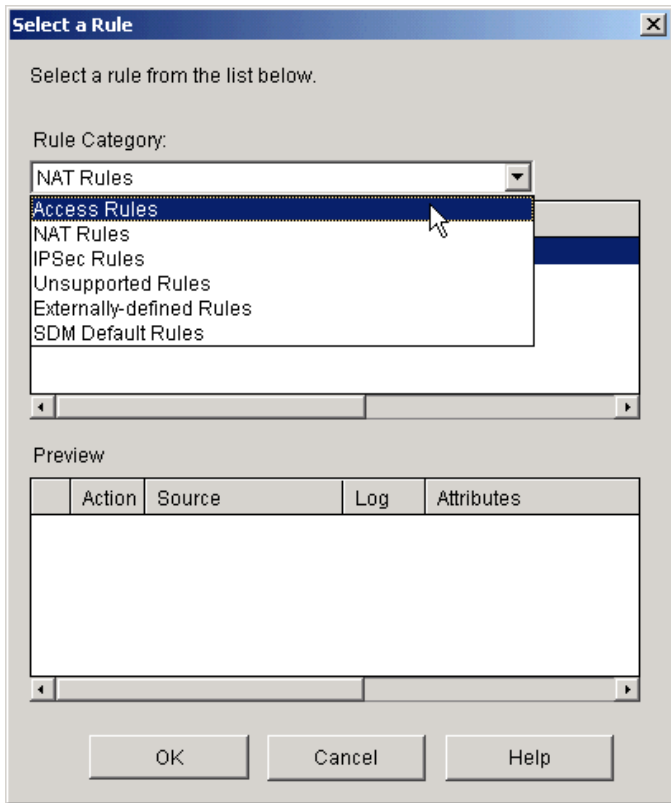
5. At the **Add Address Translation Rule** screen, choose **Dynamic**. Next to **Direction**, choose **From inside to outside**.



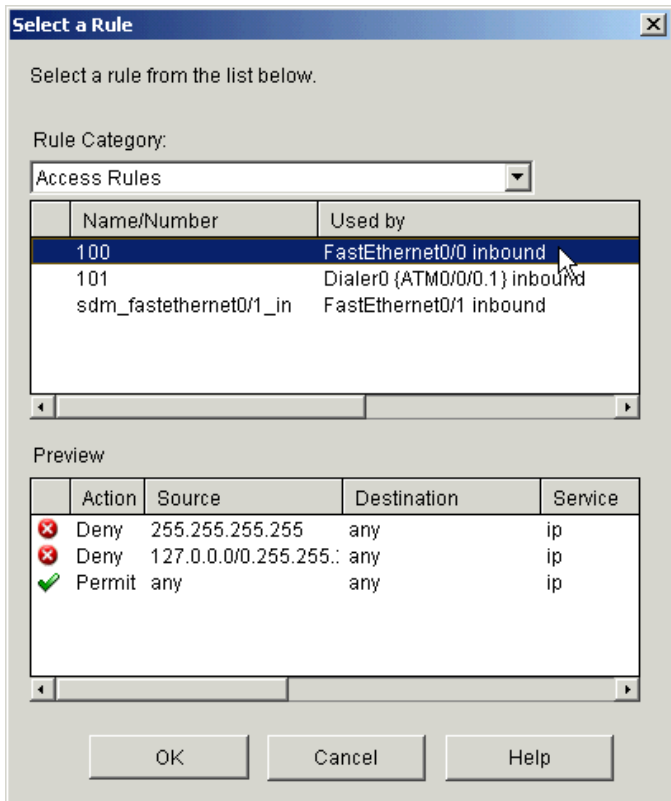
6. Click the **ACL Rule** details button and click **Select an existing rule (ACL)...**



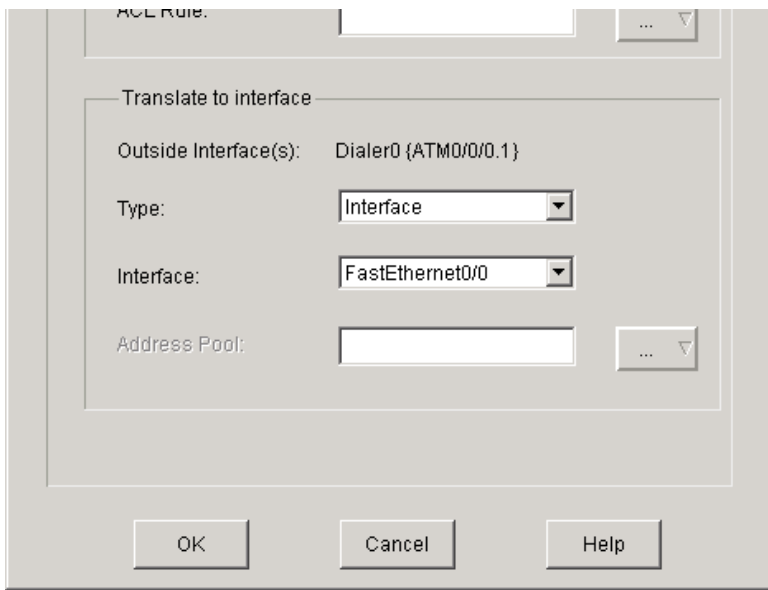
7. In the **Rules Category** box, choose **Access Rules**.



8. Select the Access Rule that is used by your FastEthernet or Ethernet interface and click **OK**.



9. Go to the Translate to interface area and next to **Type** choose **Interface**. Next to **Interface** choose your WAN interface. Click **OK** to confirm.

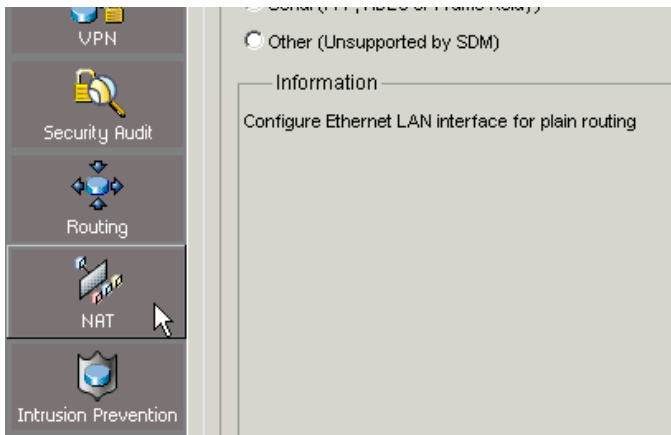


10. Click **File > Write to Startup Config** to save your configuration.

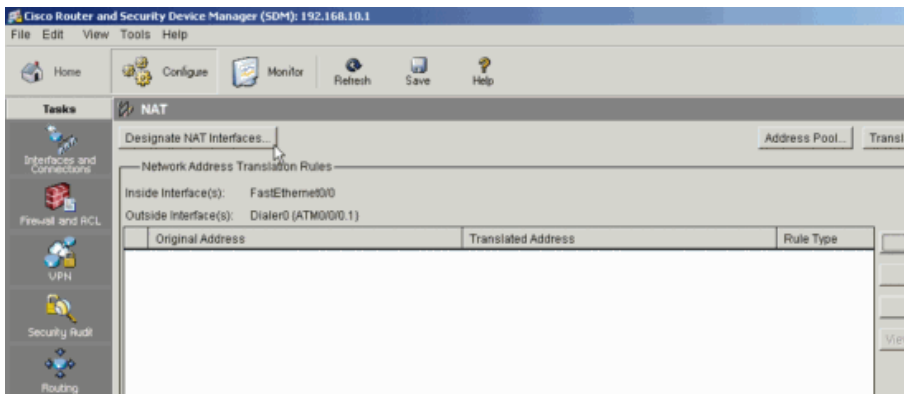
Set Up NAT with Static WAN IP Address

To set up NAT with a static WAN IP address, follow these steps:

1. Click the **NAT** tab.

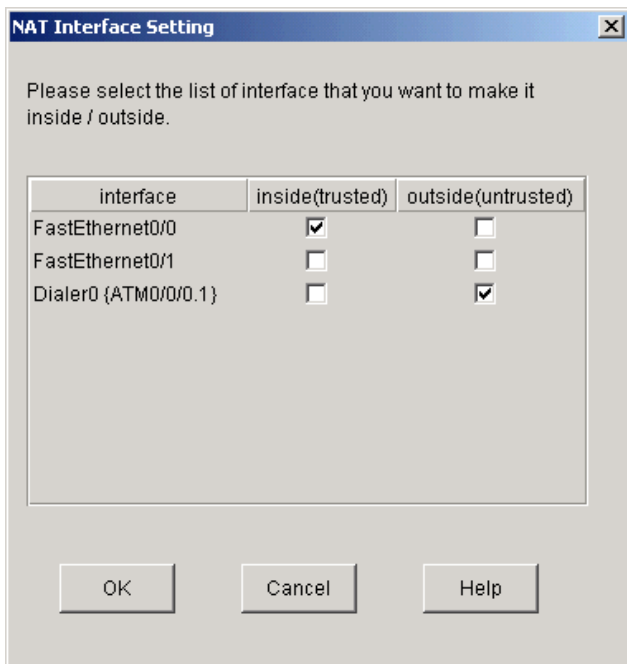


2. Click **Designate NAT Interfaces**.

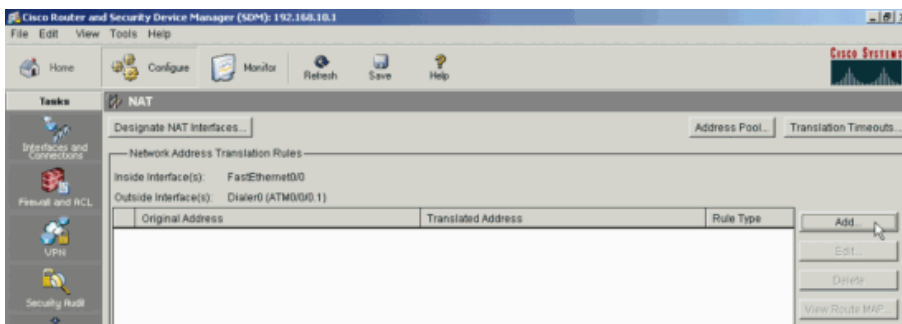


3. Check the Inside (Trusted) and Outside(Untrusted) interfaces and click **OK**.

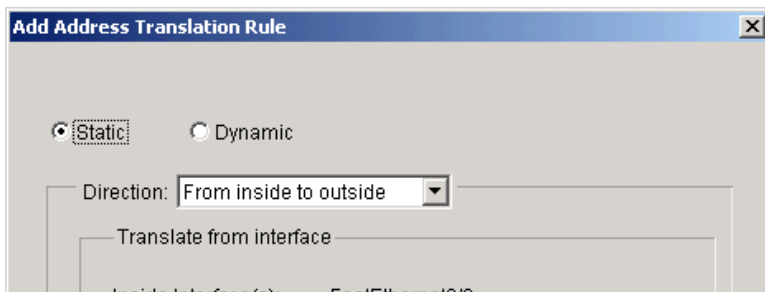
Designate WAN interface you just set up as the outside/untrusted interface.



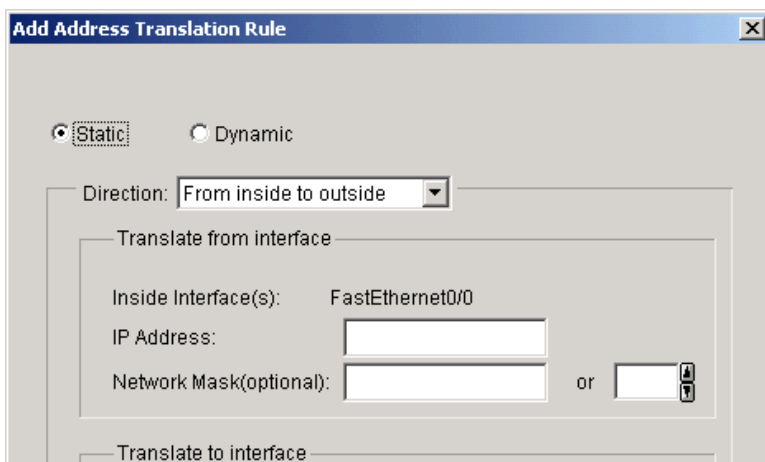
- Click **Add** to add a new translation rule.



- At the **Add Address Translation Rule** screen, choose **Static**. Next to **Direction**, choose **From inside to outside**.



- Under **Inside Interface(s)**, enter the Router IP Address that you entered in the LAN Addressing worksheet (L6A). Leave the **Network Mask** blank.



7. Under **Outside Interface(s)**, enter the Router IP Address you entered in the Internet Worksheet (B46).

Network Configuration

Translate to interface

Outside Interface(s): Dialer0 {ATM0/0/0.1}

IP Address:

Redirect Port

TCP UDP

Original Port:

Translated Port:

OK Cancel Help

8. Click **OK** to confirm.

9. Click **File > Write to Startup Config** to save your configuration.

[Back to Top](#)

Next Step

You have now configured a firewall on your router.

To make further changes to your router, refer to the [Router Support Page](#).

To configure other devices in your network, refer to the [Configuration Overview Page](#).

[Back to Top](#)

Troubleshoot the Procedure

This section provides information about common problems that you may encounter. If this information does not solve your problem, contact the [SMB Technical Assistance Center \(SMB TAC\)](#) for assistance.

Problem	Cause(s) and Suggested Solution(s)
I added a new firewall rule and I cannot access the router.	Contact the SMB Technical Assistance Center (SMB TAC) for assistance.

[Back to Top](#)

Related Information

- [Configure Your Router with Security Device Manager](#)
- [Site Survey](#)
- [Create a HyperTerminal Connection](#)
- [Cable Descriptions](#)