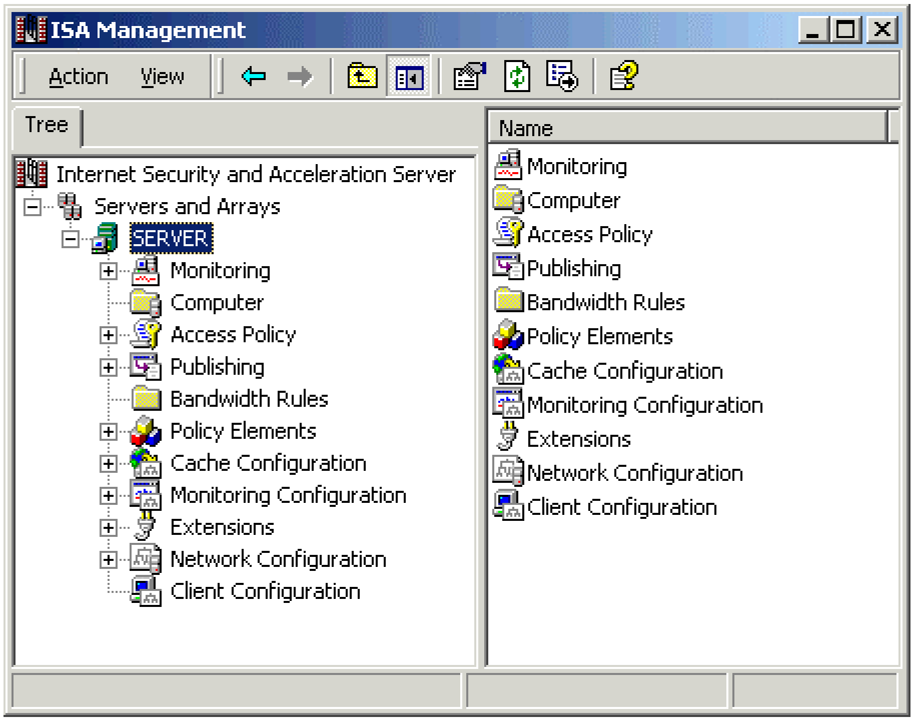
# Permitting Users to View only Specific Authorized Web Sites

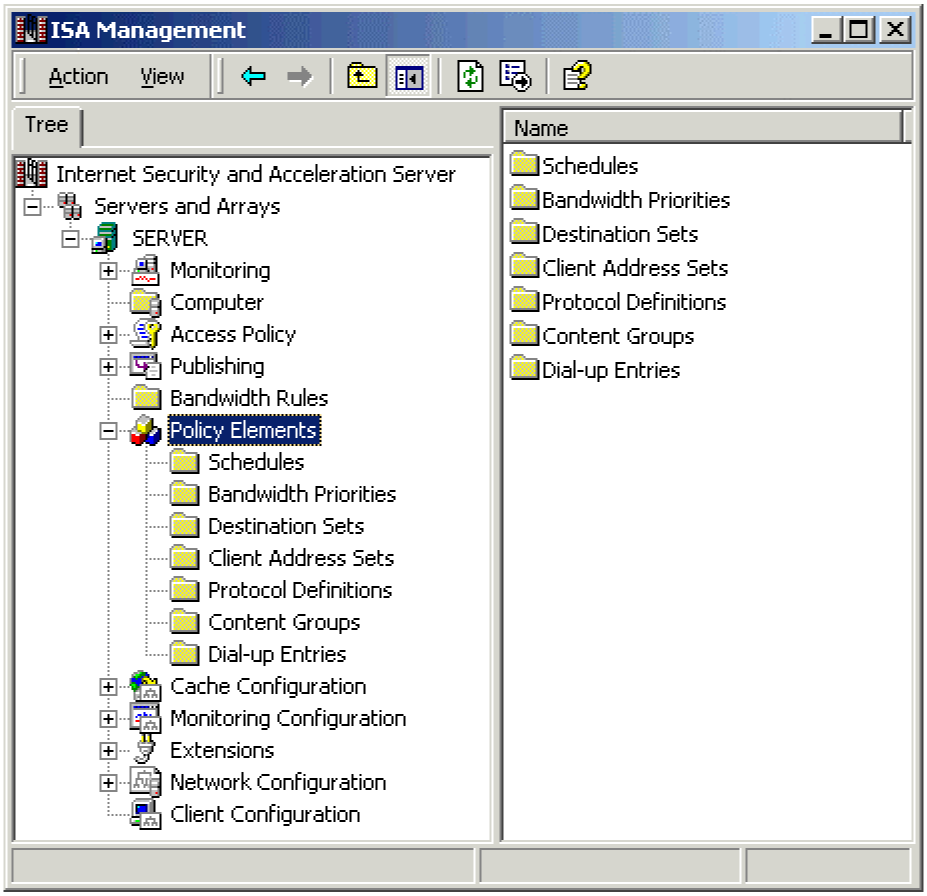
This article describes how an administrator can prevent users from accessing unauthorized Web sites by using the tools (Destination Sets, Site and Content Rules) and that are built into Internet Security and Acceleration (ISA) Server.

To permit users to view only specific authorized Web sites, follow these steps.

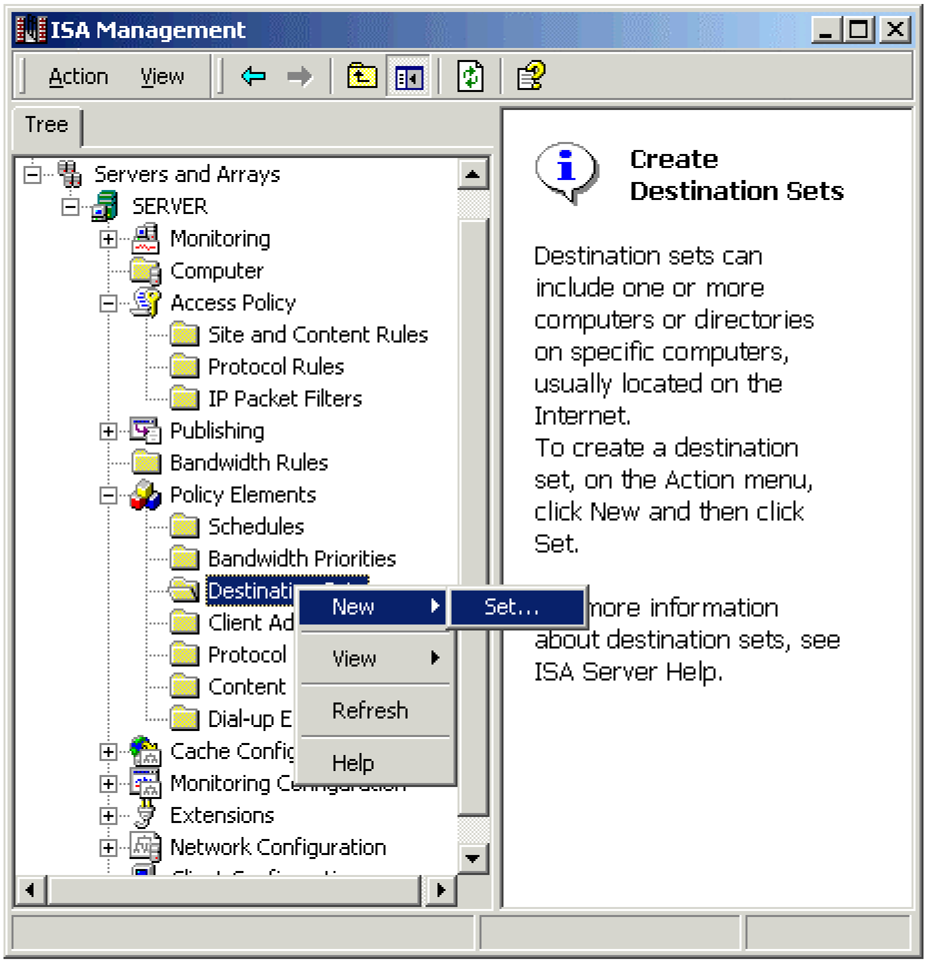
1. Click **Start➔ Programs➔ Microsoft ISA Server➔ ISA Management**. The ISA Management window is displayed.
2. Click the **plus sign** (+) to expand **Servers and Arrays**, and then click the **plus sign** (+) to expand Desired ISA Server tree.



3. On the tree, click the **plus sign** (+) to expand **Policy Elements**.



4. Right-click the **Destination Sets** ➔Click **New** and then click **Set**.

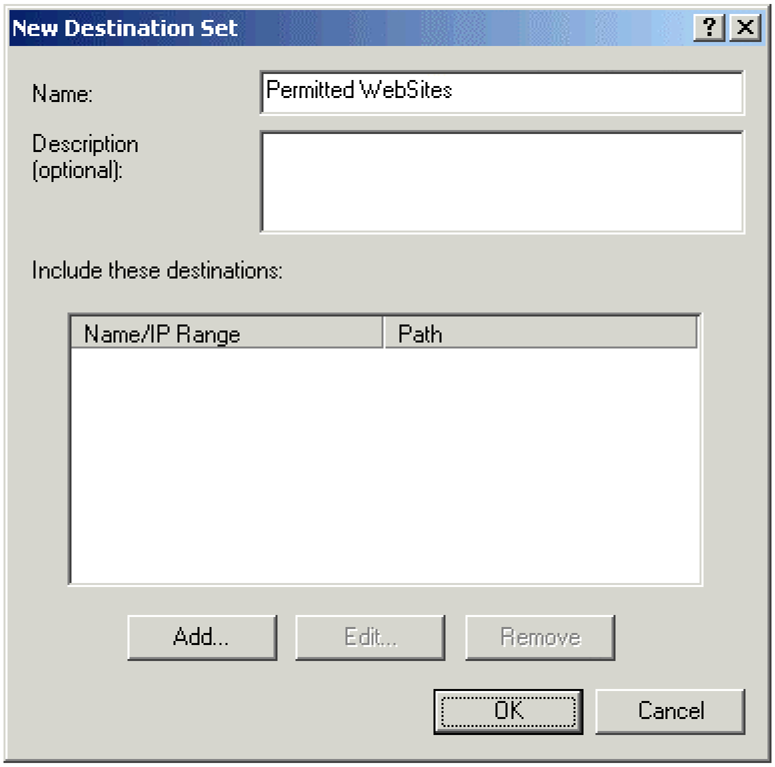


Create Destination Sets

Destination sets can include one or more computers or directories on specific computers, usually located on the Internet.
To create a destination set, on the Action menu, click New and then click Set.

more information about destination sets, see ISA Server Help.

5. In the **New Destination Set** dialog box. Enter a friendly name for your list of permitted Web sites, like "Permitted WebSites".



New Destination Set

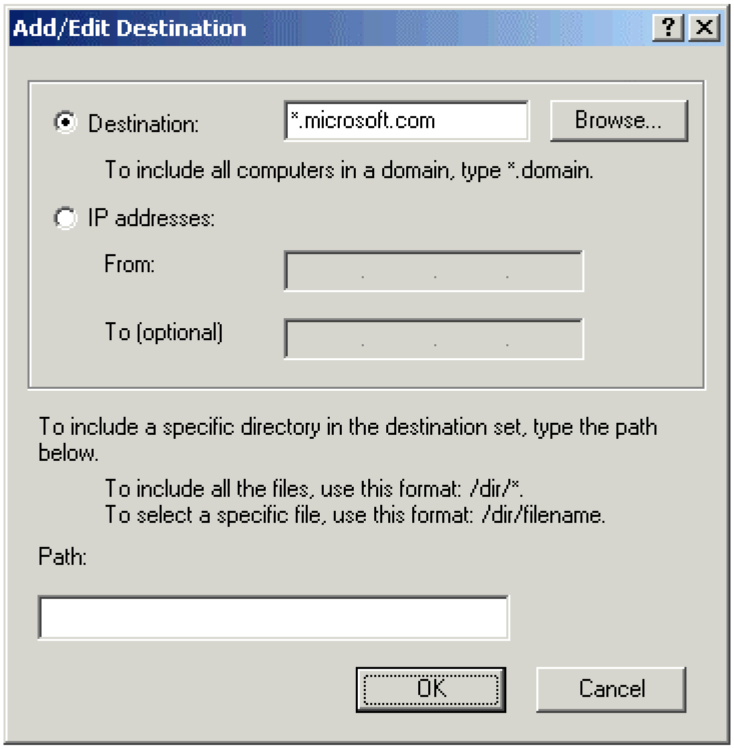
Name: Permitted WebSites

Description (optional):

Include these destinations:

**NOTE**: you can also add a helpful comment, such as, the date that the list had been entered.

6. Click **Add**, and a dialog box is displayed.
7. Select **Destination** option and type *.microsoft.com as the only permitted website.



Add/Edit Destination

● Destination: *.microsoft.com

To include all computers in a domain, type *.domain.

○ IP addresses:

From:

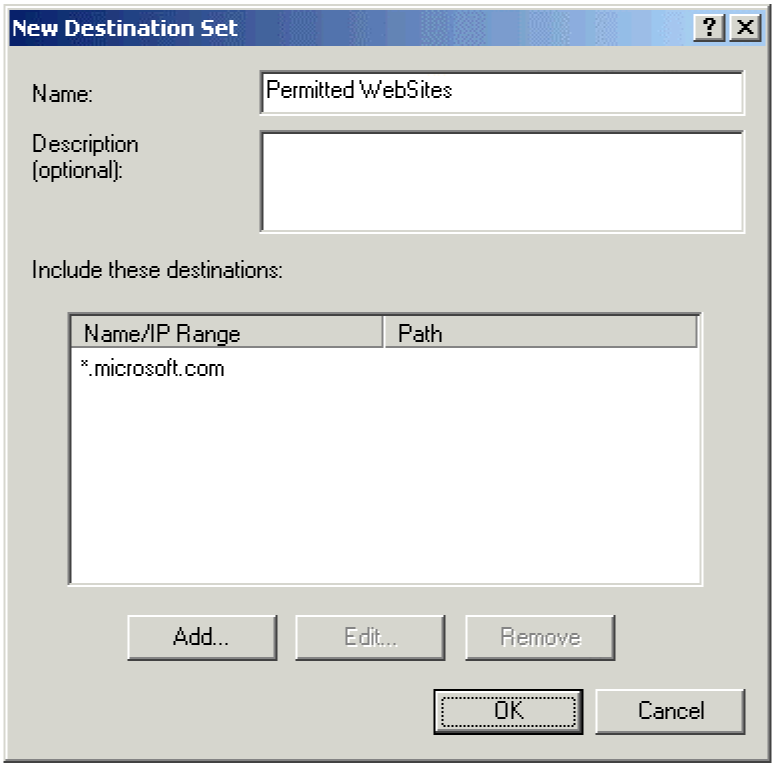
To (optional)

To include a specific directory in the destination set, type the path below.

To include all the files, use this format: /dir/*.
To select a specific file, use this format: /dir/filename.

Path:

8. Click **OK** to close this window and also click **OK** to close the New Destination Set Window.



New Destination Set

Name: Permitted WebSites

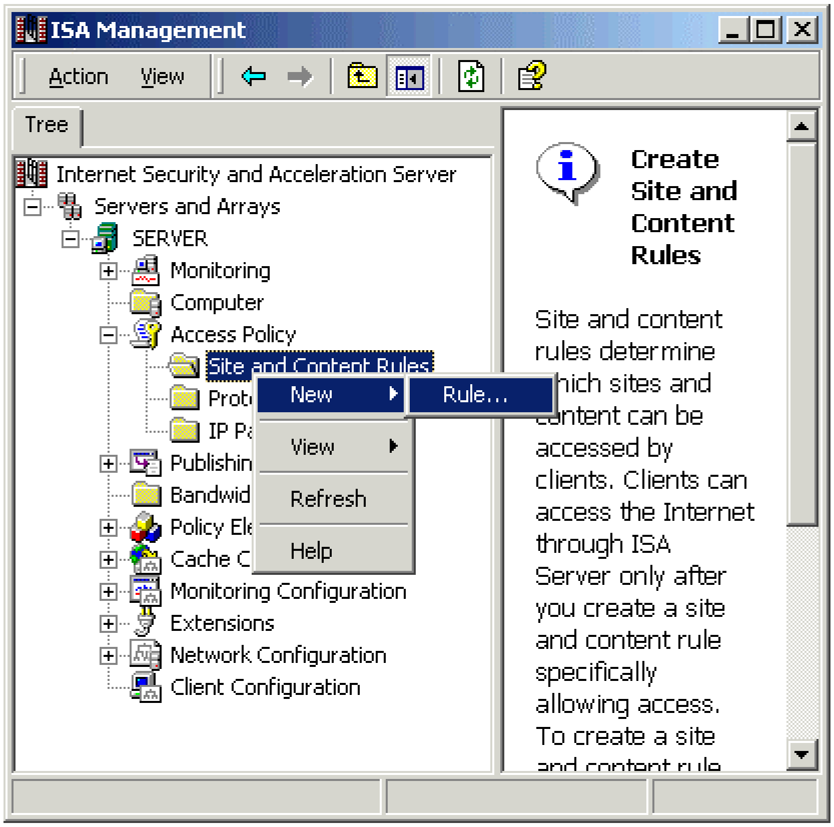
Description (optional):

Include these destinations:

| Name/IP Range | Path |
|---|---|
| *.microsoft.com | |

A Destination Set has been created for the Site and content rule.

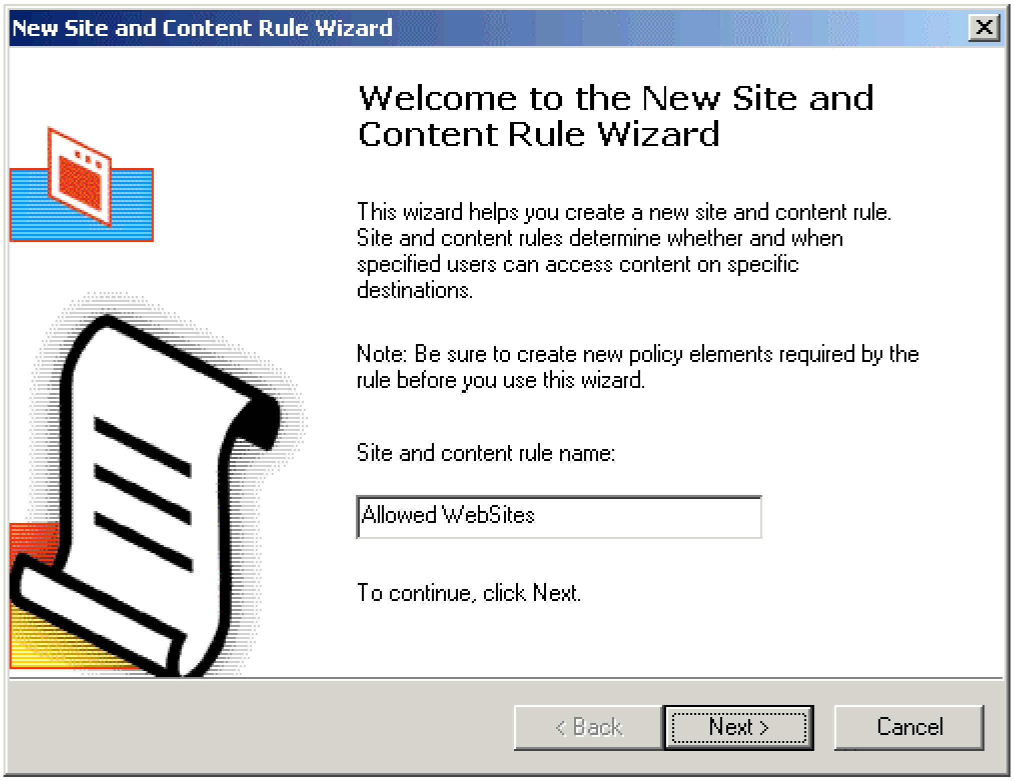
9. After expanding the **Access Policy** node, right-click **Site and Content Rules**, click **New**, click **Rule** to create a New **Site and Content Rule**.



**Create Site and Content Rules**

Site and content rules determine which sites and content can be accessed by clients. Clients can access the Internet through ISA Server only after you create a site and content rule specifically allowing access. To create a site and content rule

10. Enter a friendly name, such as, Allowed WebSites, in the **Site and Content Rule Name** dialog box, and then click **Next**.



Welcome to the New Site and Content Rule Wizard

This wizard helps you create a new site and content rule. Site and content rules determine whether and when specified users can access content on specific destinations.

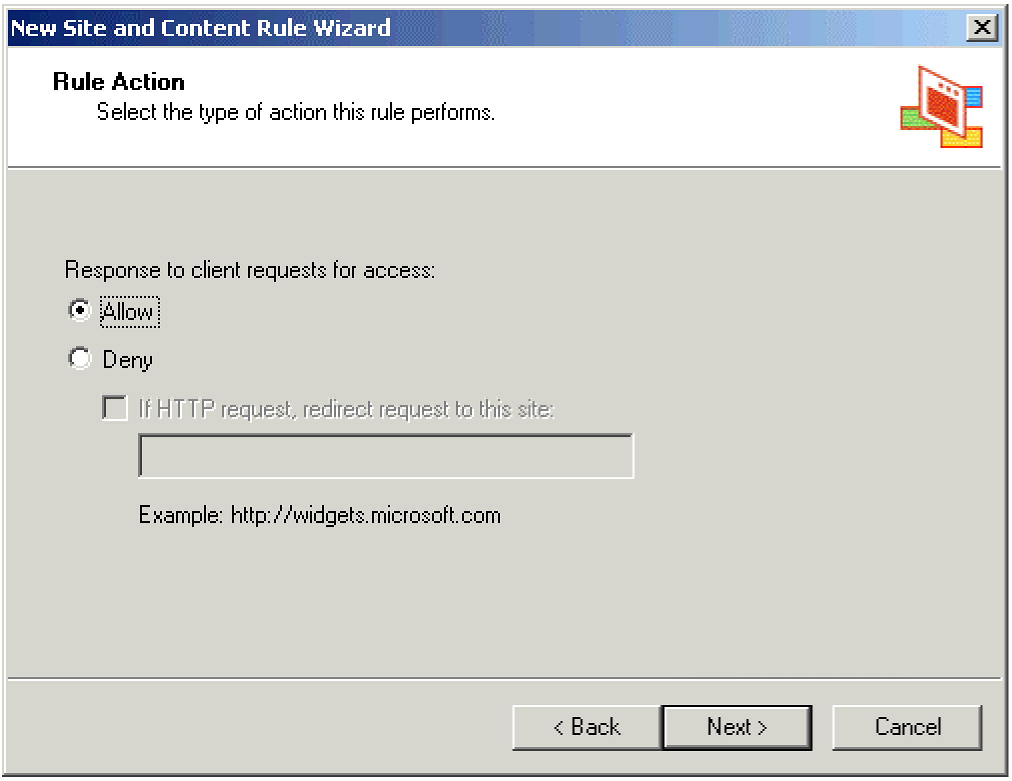
Note: Be sure to create new policy elements required by the rule before you use this wizard.

Site and content rule name:

Allowed WebSites

To continue, click Next.

11. Click **Allow,** which is listed under the line **"Response to client requests for access",** and then click **Next.**



New Site and Content Rule Wizard

**Rule Action**

Select the type of action this rule performs.

Response to client requests for access:

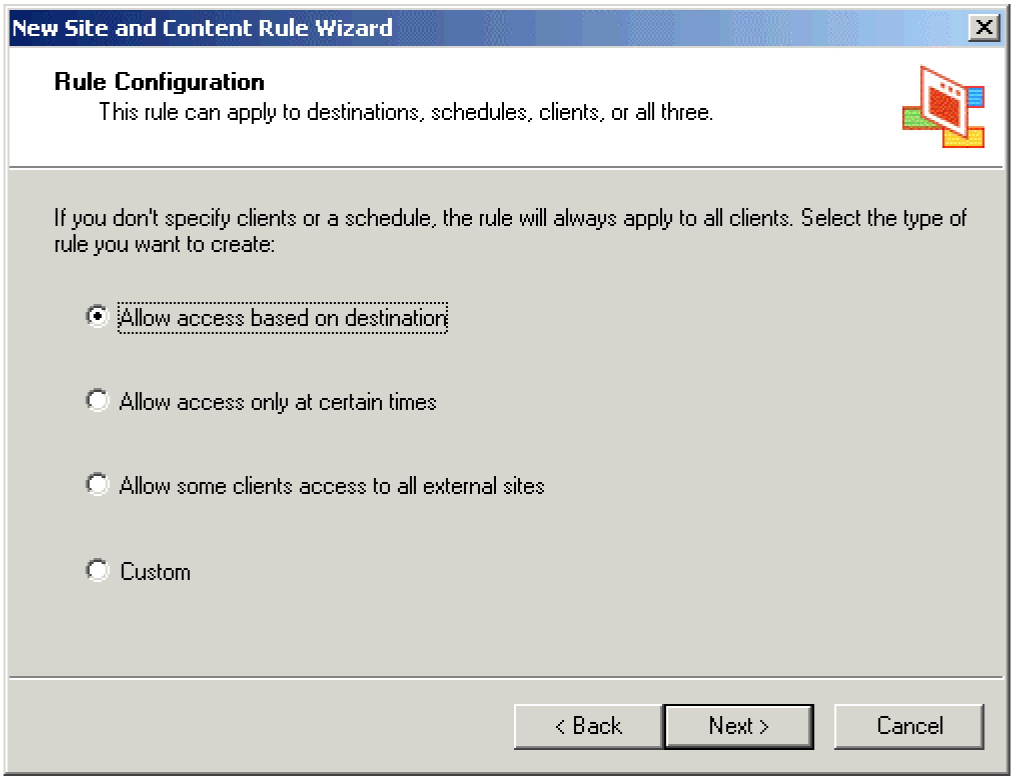
● Allow

○ Deny

□ If HTTP request, redirect request to this site:

Example: http://widgets.microsoft.com

12. Click **Allow Access Based on Destination**, and then click **Next**.



New Site and Content Rule Wizard

**Rule Configuration**

This rule can apply to destinations, schedules, clients, or all three.

If you don't specify clients or a schedule, the rule will always apply to all clients. Select the type of rule you want to create:

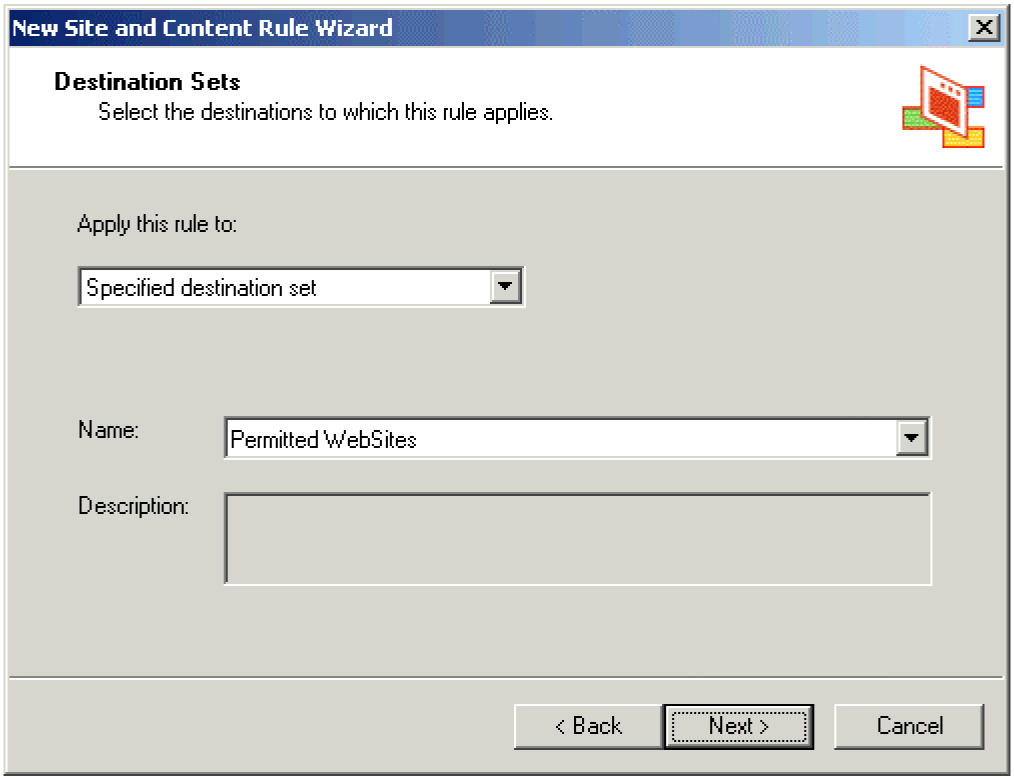
● Allow access based on destination

○ Allow access only at certain times

○ Allow some clients access to all external sites

○ Custom

13. In the **Apply this Rule To** list, click **Specified Destination Set**. Examine the **Name** list. You can observe the friendly name of the list that you entered when you made up the list of permitted Web sites (in this example, you named it "Permitted WebSites"). Click your list of permitted Web sites, and then click **Next**.



New Site and Content Rule Wizard

**Destination Sets**

Select the destinations to which this rule applies.

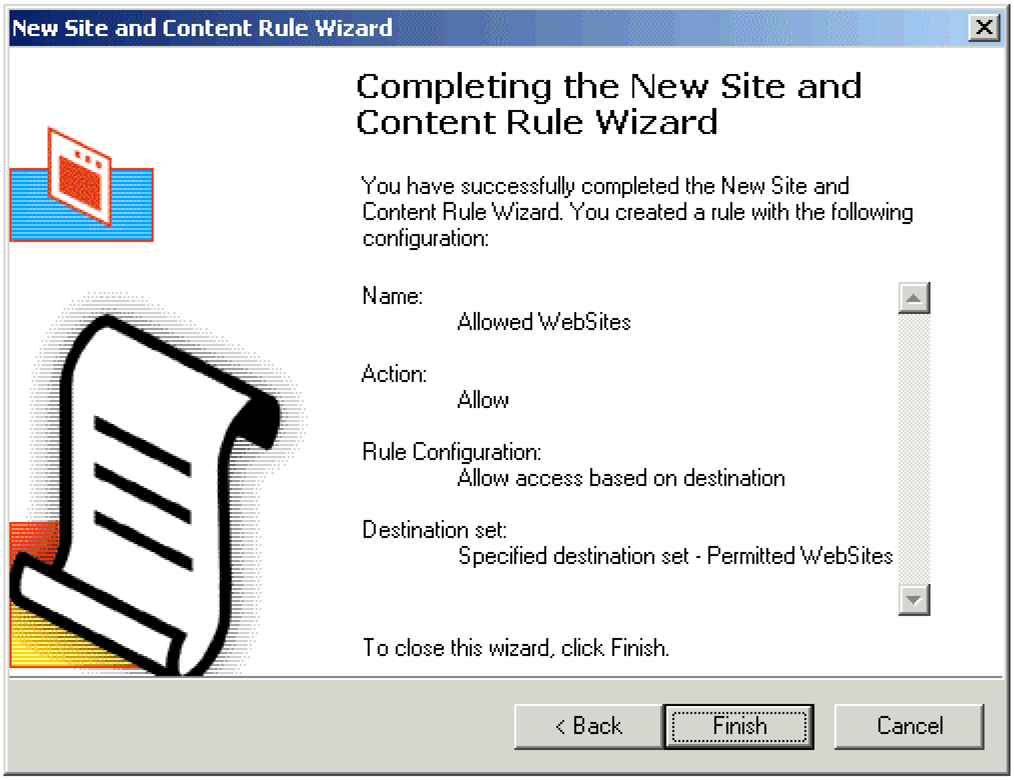
Apply this rule to:

Specified destination set

Name: Permitted WebSites

Description:

14. A summary screen is displayed, which displays your selections. If the selections are correct, click **Finish**. The Wizard disappears, and you are returned to the ISA Management window.



Completing the New Site and Content Rule Wizard

You have successfully completed the New Site and Content Rule Wizard. You created a rule with the following configuration:

Name:
Allowed WebSites

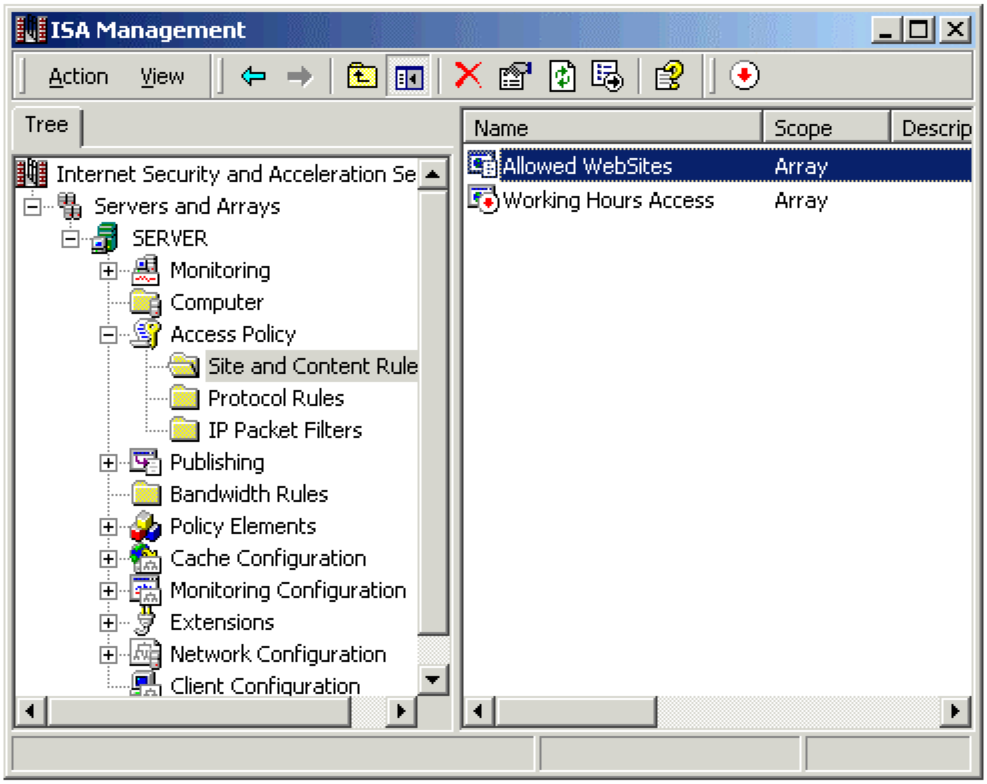
Action:
Allow

Rule Configuration:
Allow access based on destination

Destination set:
Specified destination set - Permitted WebSites

To close this wizard, click Finish.

**Note:** Your new rule is displayed in the right pane of the window. If there are any other rules that are displayed in the right pane of the ISA Management window, you can disable the rule by pointing to the rule, right-clicking the rule, and then clicking **Disable**. A disabled rule displays a red arrow beside the name of the rule.



| Name | Scope | Descrip |
|---|---|---|
| Allowed WebSites | Array | |
| Working Hours Access | Array | |

Now the only permitted sites are of Microsoft.com (Ftp.microsoft.com, www.microsoft.com etc). To test this rule, use any client browser with Proxy settings pointing to this ISA server and try to access other websites. Each time you will try to access sites other than Microsoft.com, you will get an error message from ISA server.

**Note:** If you like this article, then please cast your vote in the forum and give any comments if you have.