Controlling Secure Internet Access using ISA Server 2004

Microsoft Internet Security and Acceleration (ISA) Server 2004

Introduction

Microsoft® Internet Security and Acceleration (ISA) Server 2004 provides granular control over how clients on your networks access the Internet. With the multi-networking functionality of ISA Server, you can apply this control to clients on any network whose gateway to the Internet is the ISA Server computer.

Multi-Networking

Using ISA Server, you can connect many networks to an ISA Server computer, and control access among the networks. You can therefore control the Internet access of any network for which the ISA Server computer serves as the gateway to the Internet.

Access Rules

Access rules determine how clients on a source network access resources on a destination network.

You can configure access rules to apply to all Internet Protocol (IP) traffic, to a specific set of protocol definitions, or to all IP traffic except selected protocols.

ISA Server includes a list of preconfigured, well-known protocol definitions, including the Internet protocols that are most widely used. You can also add or modify additional protocols.

When a client requests an object using a specific protocol, ISA Server checks the access rules. A request is processed only if an access rule specifically allows the client to communicate using the specific protocol and also allows access to the requested object.

Controlling Internet access depends primarily on the design and order of access rules. The only other factor is configuring the Web Proxy properties to require authentication for Internet requests, as described in Appendix C: Configuring HTTP Policy in this document.

Tip

Controlling Internet access has only two factors:

- Ordered access rules
- Web Proxy properties

The following table summarizes all of the options available in access rule design. The table is organized according to the location of the property on the access rule properties

page. To see an access rule property page, double-click any access rule (such as the Default rule) in the Firewall Policy details pane.

Note

Rule elements referred to in this table are described in Rule Elements in this document.

Tab	Property	Comments	Related rule elements
General	Name	Rule name.	None
General	Description	Rule description.	None
General	Enable	If selected, rule is enabled.	None
Action	Allow/Deny	Does the rule allow or deny access to the Internet for requests matching the rule elements in the rule?	None
Action	Redirect HTTP requests to this page	Optional — when a request for Internet access is denied by a rule, you can provide an explanatory Web page.	None
Action	Log requests matching this rule	Select if you want ISA Server to log requests that match the rule.	None

Protocols	All outbound IP traffic Selected protocols (choose from list) All outbound protocols except selected (choose from list)	The access rule can apply to all protocols, to specific protocols, or to all protocols except for the specified ones. This page also provides access to the HTTP configuration properties, through the **Filtering** button. For more information, see Appendix C: Configuring HTTP Policy in this document.	Protocols
From	Applies to traffic from these sources	The network objects from which the requests will come.	Network objects
From	Exceptions	The rule will not apply to traffic sent from these network objects.	Network objects
To	Applies to traffic sent to these destinations	The network objects requested by the client. In the case of Internet access, this should be the External network.	Network objects

To	Exceptions	The rule will not apply to traffic sent to these network objects.	Network objects
Users	Applies to requests from the following user sets	Specifies the users to whom the rule applies. If you specify users, rather than using the default setting of All Users, users that match the rule will be required to authenticate.	Users
Users	Exceptions	Specifies the users to whom the rule does not apply. If you specify users, in Exceptions, users that match the rule will be required to authenticate.	Users
Schedule	Schedule	Selects the times at which the rule is applied.	Schedules
Content Types	Applies to: All content types Selected content types	For selected content types, the rule applies only to HTTP requests with the specified content type in the response.	Content types

Rule Elements

An ISA Server rule element is an object that you use to refine ISA Server rules. For example, a subnet rule element represents a subnet within a network. You can create a

rule that applies only to a subnet, or a rule that applies to a whole network exclusive of the subnet.

Another example of a rule element is a user set, representing a group of users. By creating a user set and using it in an ISA Server rule, you can create a rule that applies only to that set of users.

You can see the rule elements that are available to you by expanding the ISA Server computer node, clicking **Firewall Policy**, and selecting the **Toolbox** tab in the task pane. There are five types of rule elements:

- **Protocols.** This rule element contains protocols that you can use to limit the applicability of access rules. For example, you can allow or deny access on one or more protocols, rather than on all protocols.
- **Users.** In this rule element, you can create a user set to which a rule will be explicitly applied, or which can be excluded from a rule.
- **Content types.** This rule element provides common content types to which you may want to apply a rule. You can also define new content types.
- **Schedules.** This rule element allows you to designate hours of the week during which the rule applies.
- **Network objects.** This rule element allows you to create sets of computers or URLs to which a rule will apply, or which will be excluded from a rule. For more information, see **Network objects.**

The rule elements you will use in the Internet access solutions described in this document are:

- Network objects, including URL sets, computer sets, and subnets
- Users and user sets
- Content types
- Schedules

Network Objects

The network object rule elements provide a variety of ways to represent computers and URLs.

Network

A network rule element represents a network, which is all of the computers connected (directly or through one or more routers) to a single ISA Server computer network adapter. Networks are defined through the **Networks** node of ISA Server Management.

Network set

A network set rule element represents a grouping of one or more networks. You can use this rule element to apply rules to more than one network. An example of this is the All Networks set that is created when you install ISA Server.

Computer

A computer rule element represents a single computer, identified by its IP address.

Computer set

A computer set rule element is a set of one or more computer rule elements.

Address range

An address range rule element is a set of computers represented by a continuous range of IP addresses.

Subnet

A subnet rule element represents a network subnet, specified by a network address and a mask (or the number of significant bits).

URL set

A URL set rule element is a set of URLs, such as http://www.adatum.com or http://www.fabrikam.com/tools/*.

Domain name set

A domain name set rule element is a set of one or more domain names, in the format www.fabrikam.com.

Web listener

A Web listener rule element is an IP address on which the ISA Server computer will listen for Web requests. This rule element is used in Web publishing, not in an access rule controlling Internet access.

Web Proxy Properties

You can configure Web Proxy properties for any network for which the ISA Server computer is providing Internet access. As part of the Web Proxy properties, you can require authentication for Web clients. Setting Web Proxy properties is described in Appendix D: Configuring Web Proxy Properties in this document.

Web Chaining

Access rules determine what access is allowed. Web chaining determines how that access is achieved, specifically when there are other Web Proxy computers between the ISA Server computer and your corporate Internet gateway. For information about how to configure Web chaining, see Appendix E: Configuring Web Chaining in this document.

Scenarios

There are many scenarios in which Internet access control is important:

- Conserving limited bandwidth strictly for corporate use. In this scenario, you may want to limit Internet access to specific websites that have business value.
- Conserving limited bandwidth or reducing employee time spent on the Internet less strictly, by blocking specific sites.
- Blocking of certain content types, either because they are inappropriate to your corporate environment, or because they require too much bandwidth.
- Allowing different levels of Internet access to different groups of users.
- Blocking of specific sites for legal reasons, such as file sharing sites.
- Controlling Internet access in a situation where employees may fail to lock computers, to prevent unauthorized users from accessing the Internet.
- Reducing use of the Internet during work hours by limiting the times during which Internet access is allowed.

Solutions

The solutions to all of the listed scenarios rely on the flexibility of access rules, which are rules of ISA Server 2004 that control resource access, in this case, Internet access. In creating access rules, you will use rule elements. For more information, see access rules and rule elements.

Network Topology

To allow Internet access in an internal network scenario, you need, at a minimum:

- A connection to the Internet. In a laboratory environment, this can be simulated by a Web server connected to the external network adapter of the ISA Server computer. However, this could limit your ability to test the access limitations that you create.
- A computer to serve as the ISA Server computer. The ISA Server computer must have at least two network adapters. One adapter will be connected to the External network (representing the Internet) and one adapter will be connected to the Internal network. If your solution involves additional networks, such as a second internal network, each additional network requires its own network adapter on the ISA Server computer. The configuration of the networks (such as number of computers, users, and subnets) will determine which of the solution options you can apply to your scenario.
- A computer on a network behind the ISA Server computer, for which the ISA Server computer is the default gateway.

Controlling Internet Access — Walk-through

This walk-through guides you through the steps necessary to control Internet access through ISA Server.

Controlling Secure Internet Access Walk-through Procedure 1: Back Up your Current Configuration

We recommend that you back up your configuration before making any changes. If the changes you make result in behavior that you did not expect, you can revert to the previous, backup configuration. Follow this procedure to back up the configuration of your ISA Server computer.

1. Right-click the name of the ISA Server computer, and click **Back Up**.
2. In **Backup Configuration**, provide the location and name of the file to which you want to save the configuration. You may want to include the date of the export in the file name to make it easier to identity, such as **ExportBackup2June2004**.
3. Click **Backup**. If you are exporting confidential information such as user passwords, you will be prompted to provide a password. This password will be needed to restore the configuration from the exported file.
4. When the backup operation has completed, click **OK**.

   Note

   Because the .xml file is being used as a backup, a copy of it should be saved on another computer for disaster recovery purposes.

Controlling Secure Internet Access Walk-through Procedure 2: Make ISA Server the Default Gateway to the Internet

To control Internet access using ISA Server, the ISA Server computer must serve as the default gateway to the Internet for the network you are regulating. If this is not the case, computers on the network may access the Internet through another gateway, thereby bypassing the ISA Server computer.

Controlling Secure Internet Access Walk-through Procedure 3: Configure ISA Server Solutions

Each solution uses one or more of the following procedures on the ISA Server computer:

- Creation of rule elements. This is described in Appendix A: Creating Rule Elements in this document.
- Design and creation of access rules. The properties of each rule are described in this procedure. A walk-through for the New Access Rule Wizard is provided in Appendix B: Using the New Access Rule Wizard in this document.
- Configuration of Web Proxy properties. This is important specifically for requiring authentication for Internet requests. The property settings are described in the

procedural section, and specific details about accessing the properties are provided in Appendix D: Configuring Web Proxy Properties in this document.

The following solutions are described:

- Access controlled by schedule and by user set
- Access controlled by network entity
- Access controlled by authentication
- Access controlled by content type
- Access controlled by schedule

Access controlled by schedule and by user set

In this scenario, you have two sets of users in the company. One set, the managers, is allowed unrestricted access to the Internet at all times. The other set, the staff, is allowed access to work-related sites during work hours, and is allowed unrestricted access before work, after work, and during lunch, but not on weekends. The scenario assumes that all of these users will access the Internet from the Internal network.

This solution requires the creation of two access rules. The first is a deny rule, denying staff access to all Internet sites except for the approved sites during work hours. The second is an allow rule, allowing everyone access to all sites. By ordering the deny rule first, only managers will have complete access during work hours, whereas staff will be restricted to the work-related sites during work hours.

Follow these steps to create a solution for this scenario. The procedures for creating the user set, URL set, and schedule rule elements are described in Appendix A: Creating Rule Elements in this document.

Step 1: Create the user sets

Create the user set, Staff, including all of the users who are considered staff and who should have restricted Internet access.

Step 2: Create a URL set

Create a URL set containing the work-related sites that Staff are allowed to access during work hours.

Step 3: Create a schedule

Create a schedule that represents the work hours for the Staff users. There is a Work Hours schedule that is provided with ISA Server, which may meet your needs.

Step 4: Create an allow access rule for all users at all times

Create an access rule allowing unrestricted access to the Internet for all users on the Internal network. Follow the procedure in Appendix B: Using the New Access Rule Wizard in this document, using the properties shown in the following table.

Tab	Property	Setting
General	Name	Allow all to Internet

Tab	Property	Setting
General	Description	Allows unrestricted Internet access to all users
General	Enable	Selected
Action	Allow/Deny	Allow
Action	Redirect HTTP requests to this page	Unselected
Action	Log requests matching this rule	Select if you want ISA Server to log requests that match the rule
Protocols	Applies to	Selected protocols: HTTP HTTPS FTP
From	Applies to traffic from these sources	Internal network
From	Exceptions	None
To	Applies to traffic sent to these destinations	External network (the Internet)
To	Exceptions	None
Users	Applies to requests from the following user sets	All users
Users	Exceptions	None
Schedule	Schedule	Always
Content Types	Applies to: All content types Selected content types	All content types

Step 5: Create a deny access rule for Staff on the Internal network

Create an access rule for Staff, denying the Staff user set access to the Internet except for the URL set of allowed sites, during the times indicated in the Work Hours schedule. Follow the procedure in Appendix B: Using the New Access Rule Wizard in this document, using the properties shown in the following table.

Tab	Property	Setting
General	Name	Internal Network Internet Access Deny Rule

Tab	Property	Setting
General	Description	Denies access to the Internet from the Internal network, except for specific sites
General	Enable	Selected
Action	Allow/Deny	Deny
Action	Redirect HTTP requests to this page	Optional — you may select this option, and provide a Web page location
Action	Log requests matching this rule	Select if you want ISA Server to log requests that match the rule
Protocols	This rule applies to	Selected protocols: HTTP HTTPS FTP
From	Applies to traffic from these sources	Internal network
From	Exceptions	None
To	Applies to traffic sent to these destinations	External network (the Internet)
To	Exceptions	The URL set of acceptable work-hour sites
Users	Applies to requests from the following user sets	Staff user set
Users	Exceptions	None
Schedule	Schedule	Work hours
Content Types	Applies to: All content types Selected content types	All content types

Step 6: Consider rule order

Always consider rule order when creating access rules. In this solution, the rule denying access to the Staff user set during work hours must appear before the rule allowing access to all users at all times. If it appears later in the order, when a request arrives from a Staff user, ISA Server will read the allow rule first and allow access to the entire Internet during work hours.

Access controlled by network entity

In this scenario, you allow all of your users on the Internal network to access the Internet. However, you want them to access only business-related sites from their office computers. There will be several computers available in the employee break room, where users can access all other sites.

There are at least three possible approaches to this solution:

- Create an allow rule, allowing access to the entire Internet from the break room computers. Create a deny rule, denying access from the Internal network to the Internet except for the URL set of allowed sites. Order the allow rule before the deny rule.
- Create two specific allow rules, one for the break room set of computers, allowing access to the entire Internet, and one for the Internal network, allowing access only to business-related sites.
- Create an allow rule for all of the computers on the Internal network. Create a deny rule for a set of computers including all of the computers on the Internal network except for those in the break room, denying access to the Internet except for business-related sites. Place the deny rule before the allow rule.

  Companion scenario

  You may have the opposite situation: an Internal network from which access to the entire Internet is allowed, and computers in a lobby that should not have any access to the Internet. In this case, you would create a computer set including the lobby computers, and an allow rule allowing access from the Internal network to the External network, but listing the Lobby Computers computer set as an exception in the **From** tab.

The solution presented is the first one, because it is easier to create a small computer set including the break room computers, than to create a set of all of the other computers on the Internal network.

Follow these steps to create the solution. The procedures for creating the network entity and URL set rule elements are described in Appendix A: Creating Rule Elements in this document.

Step 1: Create the network entity

The network entity you create will be a set of IP addresses that is a subset of a network defined in ISA Server. In this example, you want to create a computer set that contains the break room computers, which is a set of computers in the Internal network.

Step 2: Create a URL Set

Create a URL set containing the work-related sites that can be accessed from all computers.

Step 3: Create a deny access rule for the Internal network

Create an access rule for Staff, denying access from the Internal network to the Internet except for the URL set of allowed sites. Follow the procedure in Appendix B: Using the New Access Rule Wizard in this document, using the properties shown in the following table.

Tab	Property	Setting
General	Name	Internal Network Internet Access Deny Rule
General	Description	Denies access to the Internet from the Internal network, except for specific sites
General	Enable	Selected
Action	Allow/Deny	Deny
Action	Redirect HTTP requests to this page	Optional — you may select this option, and provide a Web page location
Action	Log requests matching this rule	Select if you want ISA Server to log requests that match the rule
Protocols	Applies to	Selected protocols: HTTP HTTPS FTP
From	Applies to traffic from these sources	Internal network
From	Exceptions	None
To	Applies to traffic sent to these destinations	External network (the Internet)
To	Exceptions	The URL set of acceptable work-related sites
Users	Applies to requests from the following user sets	All users
Users	Exceptions	None
Schedule	Schedule	Always
Content Types	Applies to: All content types Selected content types	All content types

Step 4: Create an allow access rule for the Break Room computer set

Create an access rule allowing access to the Internet for all users from the Break Room computer set, at all times of the day. Follow the procedure in Appendix B: Using the New Access Rule Wizard in this document, using the properties shown in the following table.

Tab	Property	Setting
General	Name	Internet Access Allow Rule for the Break Room
General	Description	Allows unrestricted Internet access to all users on the break room computers
General	Enable	Selected
Action	Allow/Deny	Allow
Action	Redirect HTTP requests to this page	Unselected
Action	Log requests matching this rule	Select if you want ISA Server to log requests that match the rule
Protocols	Applies to	Selected protocols: HTTP HTTPS FTP
From	Applies to traffic from these sources	Break Room computer set
From	Exceptions	None
To	Applies to traffic sent to these destinations	External network (the Internet)
To	Exceptions	None
Users	Applies to requests from the following user sets	All users
Users	Exceptions	None
Schedule	Schedule	Always
Content Types	Applies to: All content types Selected content types	All content types

Note

The critical item in this list of properties is the setting of the From property to the Break Room computer set.

Step 5: Consider rule order

Always consider rule order when creating access rules. If the deny rule precedes the allow rule, ISA Server will process the deny rule and deny the request, even if it comes from a break room computer.

If the allow rule precedes the deny rule, it will be processed first, allowing requests from break room computers. Requests from other computers will not be processed by the allow rule, and will be denied by the deny rule, unless they are for a permitted, business-related site.

Access controlled by authentication

In this scenario, physical access to your corporate computers is not always secure. For example, maintenance workers have access to all of the offices, and employees may forget to lock computers at night. For this reason, you want users to be authenticated when they connect to the Internet.

Step 1: Create an access rule

Create an access rule allowing all users access to the Internet, such as that described in Create an allow access rule for all users at all times in this document. Or, if you want to apply additional restrictions, create a rule or rules as described in other solutions in this document.

Step 2: Require authentication

You can require authentication from Web Proxy clients on any network that sends Web requests through ISA Server to the Internet. Configure this in the Web Proxy properties, as described in Appendix D: Configuring Web Proxy Properties in this document.

Access controlled by content type

In this scenario, you have to preserve limited bandwidth for business use, and therefore want to prevent access to video and audio files, which use a large amount of bandwidth. There are two possible solutions for this scenario.

- Create an allow rule, allowing all users access to the Internet without exceptions, and then create a deny rule, denying all users access to the specific content types. Make sure that the deny rule precedes the allow rule in the rule order.
- Create an allow rule, allowing all users access to the Internet, but only for specific content types.

The second approach is described, because it requires only one access rule. Follow the procedure in Appendix B: Using the New Access Rule Wizard in this document, using the properties shown in the following table.

Important

You cannot set content types when creating a rule. You have to set those properties on the rule's property dialog box. After you create the rule using the New Access Rule Wizard, find the rule in the Firewall Policy details pane, and

double-click it to open its properties. Select the Content Types tab and make the necessary changes.

Tab	Property	Setting
General	Name	Internal Network Internet Access Allow Rule Except Audio and Video
General	Description	Allows access to the Internet from the Internal network for all content except for audio and video
General	Enable	Selected
Action	Allow/Deny	Allow
Action	Redirect HTTP requests to this page	Optional — you may select this option, and provide a Web page location
Action	Log requests matching this rule	Select if you want ISA Server to log requests that match the rule
Protocols	Applies to	Selected protocols: HTTP HTTPS FTP
From	Applies to traffic from these sources	Internal network
From	Exceptions	None
To	Applies to traffic sent to these destinations	External network (the Internet)
To	Exceptions	None
Users	All users	None
Users	Exceptions	None
Schedule	Schedule	Always
Content Types	Applies to: All content types Selected content types	Selected content types Select all of the content types except for audio and video

Access controlled by schedule

In this scenario, you want to make sure that late night, non-core personnel, such as security and maintenance staff, do not access the Internet through computers that were mistakenly left unlocked overnight. Follow these steps to create a solution for this scenario.

Step 1: Create a schedule

Create a schedule that represents the hours during which only authorized personnel are on site. For example, this may be 07:00 to 21:00, weekdays only.

Step 2: Create an access rule

Create an access rule allowing all users access to the Internet, but only during the times selected in the newly created schedule.

Controlling Secure Internet Access Walk-through Procedure 4: View Internet Access Information in the ISA Server Log

If you selected **Log requests matching this rule** on the **Action** page of the access rule properties, ISA Server will log the requests that match a specific rule.

To view the information in the log, perform the following steps:

1. In the Microsoft ISA Server Management console tree, select **Monitoring**.
2. In the Monitoring details pane, select the **Logging** tab.
3. Create a filter so that you receive only the log information regarding Internet access attempts. In the task pane, on the **Tasks** tab, click **Edit Filter Properties** to open the **Edit Filter** dialog box. The filter has three default conditions, specifying that the log time is **live**, that log information from both the firewall and the Web Proxy should be provided, and that connection status should not be provided. You can edit these conditions, and add additional conditions to limit the information retrieved during the query.
4. For example, select **Log Time**. From the **Condition** drop-down menu, select **Last 24 Hours**, and then click **Update**.

   Note

   Changes to the log filter expressions, and new expressions that you create, are not saved until you click **Start Query** in the **Edit Filter** dialog box.
5. Select **Log Record Type**. From the **Value** drop-down menu, select **Web Proxy Filter**, and then click **Update**.
6. Click **Start Query**. The **Start Query** command is also available in the task pane on the **Tasks** tab. The changes you made may have sufficiently limited the information in the log. However, you may want to limit the information further by adding an additional filter expression, as described in the next steps.
7. In the task pane, on the **Tasks** tab, click **Edit Filter Properties** to open the **Edit Filter** dialog box. To add another expression, select an item from the **Filter by**

drop-down menu, and then provide a **Condition** and **Value**. Some examples are shown in the following table.

Filter by	Condition	Value	Effect
Client IP	Equals	The IP address of a client computer	Provides a log of Internet access attempts by a specific client computer.
Client username	Equals	The name of a user	Provides a log of Internet access attempts by a specific user.
Destination host name	Equals	The name of a destination host	Provides a log of attempts to access a specific host.
Destination host IP	Equals	The IP address of a destination host	Provides a log of attempts to access a specific host.
Protocol	Equals	A protocol	Provides a log of attempts to access the Internet on a specific protocol, such as HTTPS.
URL	Equals	A URL	Provides a log of attempts to access a specific URL.
URL	Contains	A URL	Provides a log of attempts to access URLs containing a specific string, such as *gambling.*

8. After you have created an expression, click **Add to list** to add it to the query list, and then click **Start Query** to start the query. You must click **Start Query** to save your changes.

Controlling Secure Internet Access Walk-through Procedure 5: Create an Internet Access Report

You can create reports that summarize Internet access through the ISA Server computer. You can create either a report that runs once, or a recurring report that runs at a frequency that you specify.

Follow this general procedure to create a report that runs once.

9. In the Microsoft ISA Server Management console tree, select **Monitoring.**
10. In the Monitoring details pane, select the **Reports** tab.
11. On the **Tasks** tab, select **Generate a new report** to start the New Report Wizard.
12. On the **Welcome** page, provide a name for the report, such as **Internet Access Report for *Date***.
13. On the **Report Content** page, select **Web Usage** (verify that the other types are not selected), and click **Next**. For information about other report types, see ISA Server Help.
14. On the **Report Period** page, use the **Start Date** and **End Date** fields to set the period of time that will be covered by the report.
15. On the **Report Publishing** page, you can select **Publish reports to a directory** and provide a directory in which to store the reports in HTML format. If you publish a report to a shared directory, other users with access to the directory can view the report. If you do not publish the report, it will be viewable only on the ISA Server computer. Click **Next**.
16. On the **Send E-mail Notification** page, you can select options for sending e-mail messages when the report is completed, and then click **Next**.
17. Review the information on the summary page, and then click **Finish**. The report will be displayed in the Monitoring details pane on the **Reports** tab.

Follow this general procedure to create a recurring report.

1. In the Microsoft ISA Server Management console tree, select **Monitoring.**
2. In the Monitoring details pane, select the **Reports** tab.
3. On the **Tasks** tab, select **Create and Configure Report Jobs** to open the **Report Jobs Properties** dialog box.
4. Click **Add** to start the New Report Job Wizard.
5. On the **Welcome** page, provide a name for the report, such as **Weekly Internet Access Report**.
6. On the **Report Content** page, select **Web Usage** (verify that the other types are not selected), and click **Next**. For information about other report types, see ISA Server Help.

7. On the **Report Job Schedule** page, select a frequency for the report. A daily report will cover one day's activity, a weekly report one week's activity, and a monthly report one month's activity. Note that if you choose to generate monthly reports toward the end of the month, they may not be generated during certain months. For example, a report generated on the twenty-ninth will not be generated in February, except during leap years. To cover an entire calendar month, have the report generated on the first of the month. Because the report is generated at 01:00, the entire previous month will be included in the report.
8. On the **Report Publishing** page, you can select **Publish reports to a directory** and provide a directory in which to store the reports in HTML format. If you publish a report to a shared directory, other users with access to the directory can view the report. If you do not publish the report, it can be viewed only on the ISA Server computer. Click **Next**.
9. On the **Send E-mail Notification** page, you can select options for sending e-mail messages when the report is completed, and then click **Next**.
10. Review the information on the summary page, and then click **Finish**. After the report has been generated, it will be displayed in the Monitoring details pane on the **Reports** tab.

Appendix A: Creating Rule Elements

Follow this general procedure to create a rule element.

1. Expand Microsoft ISA Server Management.
2. Expand the **ISA Server computer** node.
3. Select **Firewall Policy**, and in the task pane, select the **Toolbox** tab.
4. Select the rule element type by clicking the header for that element.
5. At the top of the list of elements, click **New**. If there are several choices of rule elements, as in the case of network objects, a drop-down list will appear, and you can select the element that you want to create.
6. Provide the information required by the wizard or a dialog box. When you have completed the wizard or clicked **OK** in the dialog box, your new rule element will be created.
7. Click **Apply** in the details pane to apply changes. If you prefer, you can click **Apply** after you have created your access rules, that is, after you have made all of your changes, rather than after each change. It will take a few moments for the changes to be applied.

Appendix B: Using the New Access Rule Wizard

This procedure describes the New Access Rule Wizard in general terms.

1. In the Microsoft ISA Server Management console tree, select **Firewall Policy**.

2. In the task pane, on the **Tasks** tab, select **Create New Access Rule** to start the New Access Rule Wizard.
3. On the **Welcome** page of the wizard, enter the name for the access rule. Use a descriptive name, such as **Internet access for staff during work hours**, and then click **Next**.
4. On the **Rule Action** page, select **Allow** if you are allowing access, or **Deny** if you are denying access, and then click **Next**.
5. On the **Protocols** page, the default setting of **This rule applies to** is **All outbound protocols**. You may want to select **Selected protocols** and use the **Add** button to add the specific Web protocols from the **Add Protocols** dialog box, such as HTTP, HTTPS, and FTP. When you have made these selections, click **Next**.
6. On the **Access Rule Sources** page, click **Add** to open the **Add Network Entities** dialog box, click the category for which you are creating access, select the specific object, click **Add** (repeat to add additional network objects), and then click **Close**. On the **Access Rule Sources** page, click **Next**.
7. On the **Access Rule Destinations** page, click **Add** to open the **Add Network Entities** dialog box, click **Networks**, select the External network (representing the Internet), click **Add**, and then click **Close**. On the **Access Rule Destinations** page, click **Next**.
8. On the **User Sets** page, if your rule applies to all users, you can leave the user set **All users** in place and proceed to the next page of the wizard. If the rule applies to specific users, select **All users** and click **Remove.** Then, use the **Add** button to open the **Add Users** dialog box, from which you can add the user set to which the rule applies. The **Add Users** dialog box also provides access to the New User Sets Wizard through the **New** menu item. When you have completed the user set selection, click **Next**.
9. Review the information on the wizard summary page, and then click **Finish**.
10. In the Firewall Policy details pane, click **Apply** to apply the new access rule. It may take a few moments for the rule to be applied. Order your access rules to match your Internet access policy. If you change the order, you will need to click **Apply** to apply the changes.

Appendix C: Configuring HTTP Policy

There are several properties that you cannot set in the New Access Rule Wizard. After you create an access rule, you can view and edit all of its properties by double-clicking the rule in the Firewall Policy details pane. One of these properties is HTTP Policy, in which you can configure HTTP settings for requests that match a specific allow access rule.

ISA Server is an application layer firewall, and applies an application filter to HTTP traffic. Because ISA Server can examine HTTP requests, applications that are tunneled through HTTP can be blocked, depending on how you configure the HTTP application filter. The HTTP application filter provides granular control over the HTTP requests allowed by your firewall policy. You can use the HTTP policy to block applications, such

as messaging applications or peer-to-peer file sharing applications, that tunnel over HTTP.

HTTP policy encompasses the following settings:

- Request header maximum length
- Request payload length
- URL Protection
- Executable Blocking
- Denied Methods
- Specified actions for specific file extensions
- Deny specific headers
- Modify Server and Via headers
- Deny specific signatures

To configure HTTP policy, follow this procedure.

1. In the properties of the allow access rule, select the **Protocols** tab.
2. Click **Filtering** and select **Configure HTTP** to open the Configure HTTP policy for the rule dialog box.
3. Select the appropriate tab and configure the policy settings.

Appendix D: Configuring Web Proxy Properties

You can configure the Web Proxy properties to require authentication for Internet requests by following this procedure. Note that when an access rule applies to specific user sets, or excludes specific user sets, authentication will be required of users who match the rule, even if it is not required in the Web Proxy properties. However, a rule that applies to All Users will not require authentication unless you follow this procedure.

1. In the Microsoft ISA Server Management console tree, expand the **Configuration** node and select **Networks**.
2. Double-click the network whose Web access properties you want to configure, to open its properties dialog box. Typically, this would be the Internal network. Select the **Web Proxy** tab.
3. Select **Enable Web Proxy clients** (this is the default setting for the Internal network).
4. Click **Authentication** to open the **Authentication** dialog box. You can select an authentication type.
5. Select **Require all users to authenticate**.
    - To select a default domain for authentication, click **Select Domain**. This option is available only when Basic, Digest, or RADIUS authentication is used.

- To select RADIUS servers for authentication, click **RADIUS Servers**.

6. Click **OK** to close the **Authentication** dialog box, and then click **OK** to close the network properties dialog box.

   Note

   Web Proxy clients are any CERN-compatible Web application. Requests from Web Proxy clients are directed to the Microsoft Firewall service on the ISA Server computer to determine if access is allowed. The Firewall service may also cache the requested object or serve the object from the ISA Server cache.

   Regardless of client type, when ISA Server receives an HTTP request, the client is treated as if it were a Web Proxy client. Even when a Firewall client or a SecureNAT client makes an HTTP request, the client is considered a Web Proxy client.

Appendix E: Configuring Web Chaining

Access rules determine what type of access is allowed. Web chaining determines how that access is achieved, specifically when there are other Web Proxy computers between the ISA Server computer and your corporate Internet gateway.

Configure Web chaining

Follow this general procedure to configure Web chaining.

1. In the Microsoft ISA Server Management console tree, expand the **Configuration** node and select **Networks**.
2. In the Networks details pane, select the **Web Chaining** tab.
3. In the task pane, on the **Tasks** tab, click **Create New Web Chaining Rule** to start the New Web Chaining Rule Wizard.
4. On the **Welcome** page, provide a name for the rule and click **Next**.
5. On the **Web Chaining Rule Destination** page, click **Add** to open the **Add Network Entities** dialog box. Select **Networks**, click **External**, click **Add**, and then click **Close**. This adds the External network (the Internet) as the destination, because you want to route Internet requests. On the **Web Chaining Rule Destination** page, click **Next**.
6. On the **Request Action** page, select how the request will be processed:
   - **Retrieve requests directly from the specified destination.** This option does not use Web chaining.
   - **Redirect requests to a specified upstream server.** If you select this option, the next page of the wizard will request the upstream server information on the **Primary Routing** page. To continue, see Step 8.

   Note

   If you select **Redirect requests to a specified upstream server**, you may also select **Allow delegation of basic authentication credentials**. ISA Server can handle user authentication when **Delegation of Basic authentication**

the request arrives, and then pass the authentication information to the Web server so that the user does not have to supply credentials again.

- **Redirect requests to a Hosted site.** This option redirects requests to a specified website, for which you provide the site name and ports.
- The **Request Action** page also allows you to use a dial-up entry as the route for the request, by selecting **Use automatic dial-up**. Before you can use a dial-up entry, you must specify an automatic dial-up connection, as described in Appendix F: Specifying an Automatic Dial-up Connection in this document.
- After specifying an action, click **Next**.

7. If you selected **Retrieve requests directly from the specified destination**, or **Redirect requests to a Hosted site**, you next see the summary page. Review the information, and then click **Finish**. In the details pane, click **Apply** to apply your changes.
8. If you selected **Redirect requests to a specified upstream server** in Step 6, you next see the **Primary Routing** page, on which you can select the primary route to which requests will be routed.
   - Provide the **Server**, **Port**, and **SSL Port** information. You can also click **Browse**, to browse to the server. The default port numbers provided are those that an upstream ISA Server computer would listen on. Your upstream server may listen on different ports.
   - If specific credentials are needed to access the server, select **Use this account** and click **Set Account** to open the **Set Account** dialog box.
   - In the **Set Account** dialog box, provide credentials that will be accepted by the server, and click **OK**.
   - In **Authentication**, select an authentication method.
   - Click **Next.**
9. If you selected **Redirect requests to a specified upstream server** in Step 6, you next see the **Backup Action** page, on which you can select backup routing options:
   - **Ignore requests.**
   - **Retrieve requests directly from the specified destination.** This option does not use Web chaining.
   - **Route requests to an upstream server.** This will enable you to select a backup route (on the next page of the wizard).
   - The **Backup Action** page also allows you to use a dial-up entry as the backup route for the request, by selecting **Use automatic dial-up**. Before you can use a dial-up entry, you must specify an automatic dial-up connection, as described in Appendix F: Specifying an Automatic Dial-up Connection in this document.
   - Click **Next**.
10. If you selected **Route requests to an upstream server** in Step 9, you next see the **Backup Routing** page, on which you can select the backup route to which requests will be routed:

- Provide the **Server**, **Port**, and **SSL Port** information. You can also click **Browse**, to browse to the server. The default port numbers provided are those that an upstream ISA Server computer would listen on. Your upstream server may listen on different ports.
- If specific credentials are needed to access the server, select **Use this account** and click **Set Account** to open the **Set Account** dialog box.
- In the **Set Account** dialog box, provide credentials that will be accepted by the server, and click **OK**.
- In **Authentication**, select an authentication method.
- Click **Next.**

11. On the summary page, review the information, and then click **Finish**.

Appendix F: Specifying an Automatic Dial-up Connection

You can configure ISA Server to dial automatically to establish a connection with one network. For example, if you have a dial-up connection to the Internet, you can configure ISA Server to dial automatically to the External network. If you have a high-speed Internet connection, the dial-up connection can serve as your backup route to the Internet, as described in Appendix E: Configuring Web Chaining in this document.

1. In the Microsoft ISA Server Management console tree, expand the **Configuration** node and select **General**.
2. In the details pane, select **Specify Dial-up Preferences**.
3. Select **Allow automatic dialing to this network**, and select the network to which you will set up an automatic dial-up connection. In the case of using a dial-up connection for Internet access, specify the External network.
4. If the dial-up connection is the primary way you connect to the Internet, select **Configure this dial-up connection as the default gateway**.
5. Under **Dial-up connection**, in **Use the following dial-up connection**, provide the name of the dial-up connection, or locate it by clicking **Select**.
6. If the dial-up connection is associated with a specific user account, provide the user name and password under **Dial-up account** by clicking **Set Account**.

Do you have comments about this document? Send feedback.