Application Firewall in SonicOS Enhanced 4.0

Document Scope

This document describes how to configure and manage the application firewall feature in SonicWALL SonicOS Enhanced 4.0.

This document contains the following sections:

- Application Firewall Overview
- Using Application Firewall
- Use Cases
- Glossary

Application Firewall Overview

This section provides an introduction to the SonicWALL SonicOS Enhanced 4.0 application firewall feature. This section contains the following subsections:

- "What is Application Firewall?" on page 1
- "Benefits" on page 2
- "How Does Application Firewall Work?" on page 3
- "Platforms" on page 14
- "Supported Standards" on page 15

What is Application Firewall?

Application firewall is a set of application-specific policies that gives you granular control over network traffic on the level of users, email users, schedules, and IP-subnets. The primary functionality of this application-layer access control feature is to regulate Web browsing, file transfer, email, and email attachments.

Application firewall's digital rights management component provides the ability to scan files and documents for content and keywords. Using application firewall, you can restrict transfer of certain file names, file types, email attachments, attachment types, email with certain subjects, and email or attachments with certain keywords or byte patterns. You can deny internal or external network access based on various criteria.

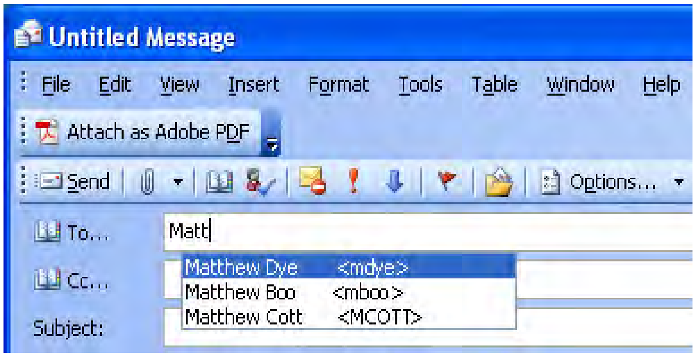
Based on SonicWALL's Deep Packet Inspection technology, application firewall also features intelligent prevention functionality which allows you to create custom, policy-based actions. Examples of custom actions include the following:

- Disabling an attachment
- Sending a custom block page
- Sending a custom email reply
- Redirecting an HTTP request
- Sending a custom FTP reply over an FTP control channel
- Bandwidth throttling for file types when using the HTTP or FTP protocols

While application firewall primarily provides application level access control, application layer bandwidth management and digital rights management functionality, it also includes the ability to create pure custom IPS signatures. You can create a custom policy that matches any protocol you wish, by matching a unique piece of the protocol header. See "Custom Signature" on page 39.

Application firewall provides excellent functionality for preventing the accidental transfer of proprietary documents. For example, when using the automatic address completion feature of Outlook Exchange, it is a common occurrence for a popular name to complete to the wrong address. See Figure 1 for an example.

Figure 1 Outlook Exchange Automatic Address Completion



To... Matt

Matthew Dye <mdye>
Matthew Boo <mboo>
Matthew Cott <MCOTT>

Benefits

Application firewall functionality can be compared to three main categories of products:

- Standalone proxy appliances
- Application proxies integrated into firewall VPN appliances
- Standalone IPS appliances with custom signature support

Standalone proxy appliances are typically designed to provide granular access control for a specific protocol. SonicWALL application firewall provides granular, application level access control across multiple protocols, including HTTP, FTP, SMTP, and POP3.Because application firewall runs on your SonicWALL firewall, you can use it to control both inbound and outbound traffic, unlike a dedicated proxy appliance that is typically deployed in only one direction. Application firewall provides better performance and scalability than a dedicated proxy appliance because it is based on SonicWALL's proprietary Deep Packet Inspection technology.

Today's integrated application proxies do not provide granular, application level access control, application layer bandwidth management, and digital rights management functionality. As with dedicated proxy appliances, SonicWALL application firewall provides much higher performance and far greater scalability than integrated application proxy solutions.

While some standalone IPS appliances provide protocol decoding support, none of these products supports granular, application level access control, application layer bandwidth management, and digital rights management functionality.

In comparing application firewall to SonicWALL Email Security, there are benefits to using either. Email Security only works with SMTP, but it has a very rich policy space. Application firewall works with SMTP, POP3, HTTP, FTP and other protocols, is integrated into SonicOS on the firewall, and has higher performance than Email Security. However, application firewall does not offer all the policy options for SMTP that are provided by Email Security.

How Does Application Firewall Work?

Application firewall scans application layer network traffic as it passes through the gateway and looks for content that matches configured keywords. When it finds a match, it performs the configured action. It can match text or binary content. When you configure application firewall, you create policies that define the type of applications to scan, the direction, the content or keywords to match, optionally the user or domain to match, and the action to perform.

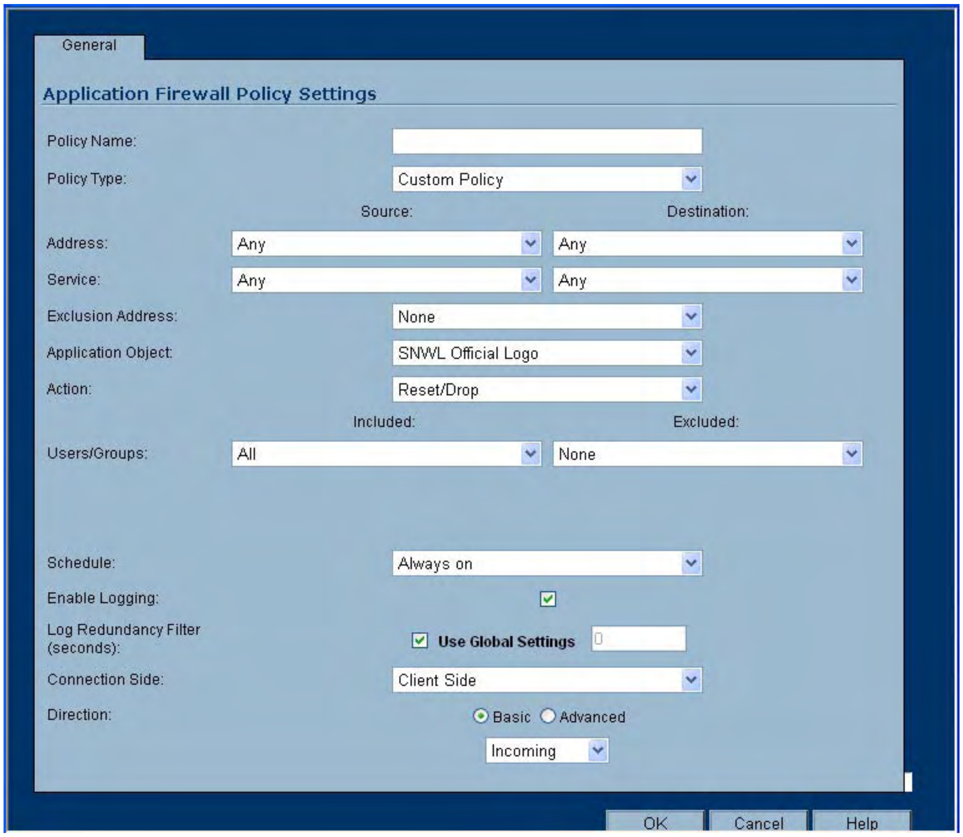
The following sections describe the four main components of application firewall:

- "Policies" on page 3
- "Application Objects" on page 6
- "Actions" on page 11
- "Email User Objects" on page 13

Policies

You can use application firewall to create custom policies to control specific aspects of traffic on your network. A policy is a set of application objects, properties, and specific prevention actions.When you create a policy, you first create an application object, then select and optionally customize an action, then reference these when you create the policy. The Policy Settings screen is shown below:

Figure 2 Policy Settings screen



Application Firewall Policy Settings

Policy Name:		
Policy Type:	Custom Policy	
	Source:	Destination:
Address:	Any	Any
Service:	Any	Any
Exclusion Address:	None	
Application Object:	SNWL Official Logo	
Action:	Reset/Drop	
	Included:	Excluded:
Users/Groups:	All	None
Schedule:	Always on	
Enable Logging:	☑	
Log Redundancy Filter (seconds):	☑ Use Global Settings	0
Connection Side:	Client Side	
Direction:	● Basic ○ Advanced Incoming	

Some examples of policies include:

- Disable .exe and .vbs email attachments
- Do not allow the Mozilla browser on outgoing HTTP connections
- Do not allow outgoing email or MS Word attachments with the keywords “SonicWALL Confidential”, except from the CEO and CFO
- Do not allow outgoing email that includes a graphic or watermark found in all confidential documents

When you create a policy, you select a policy type. Each policy type specifies the values or value types that are valid for the source, destination, application object type, and action fields in the policy. You can further define the policy to include or exclude specific users or groups, select a schedule, turn on logging, and specify the connection side as well as basic or advanced direction types. A basic direction type simply indicates inbound or outbound. An advanced direction type allows zone to zone direction configuration, such as from the LAN to the WAN.

Table 1 describes the characteristics of the available policy types.

Table 1 Policy Types

Policy Type	Description	Valid Source Service / Default	Valid Destination Service / Default	Valid Application Object Type	Valid Action Type	Connection Side
SMTP Client	Policy which is applicable to SMTP traffic that originates on the client	Any / Any (grayed out)	SMTP / SMTP (grayed out)	Filename, file extension, Email To (MIME), Email From (MIME), CC, Subject, Email body, Custom MIME header, File Content Object, E-Mail Size, Custom Object	Reset/Drop, Disable attachment, Block SMTP E-Mail with Error Reply, Block SMTP E-Mail Without Reply, Email – Add Text, no action	Client side
HTTP Client Request	Policy which is applicable to Web browser traffic or any HTTP request that originates on the client	Any / Any (grayed out)	Any / HTTP (configurable)	User-Agent, Host, URI content, Cookie, Web Browser, Referrer, filename, file extension HTTP request custom header, custom object	Reset/Drop, Block page, HTTP redirect, Manage Bandwidth, no action	Client side
HTTP Server Response	Response originated by an HTTP Server	Any / HTTP (configurable)	Any / Any (grayed out)	Set-Cookie header, Active-X ClassID, HTTP Response custom header, custom object	Reset/Drop, Manage Bandwidth, no action	Server Side
FTP Client Request	Any FTP command transferred over the FTP control channel	Any / Any (grayed out)	FTP Control / FTP Control (grayed out)	FTP Command, FTP Command + Value, Custom Object	FTP error notification, Reset/Drop, no action	Client side
FTP Client File Upload Request	An attempt to upload a file over FTP (STOR command)	Any / Any (grayed out)	FTP Control / FTP Control (grayed out)	Filename, file extension	FTP error notification, Manage Bandwidth, Reset/Drop, no action	Client side

Policy Type	Description	Valid Source Service / Default	Valid Destination Service / Default	Valid Application Object Type	Valid Action Type	Connection Side
FTP Client File Download Request	An attempt to download a file over FTP (RETR command)	Any / Any (grayed out)	FTP Control / FTP Control (grayed out)	Filename, file extension	FTP error notification, Manage Bandwidth, Reset/Drop, no action	Client side
FTP Data Transfer Policy	Data transferred over the FTP Data channel	Any / Any (grayed out)	Any / Any (grayed out)	File Content Object	Reset/Drop, no action	Both
POP3 Client Request	POP3 Client request	Any / Any (grayed out)	POP3 / POP3 (grayed out)	Custom Object	Reset/Drop, no action	Client side
POP3 Server Response	Email downloaded from POP3 server	POP3 / POP3 (grayed out)	Any / Any (grayed out)	Filename, file extension, Email To (MIME), Email From (MIME), CC, Subject, Email body, Custom MIME header, Custom Object	Reset/Drop, Disable attachment, no action	Server Side
Custom	IPS-style custom signature	Any / Any	Any / Any	Custom Object	Reset/Drop, Manage Bandwidth, no action	Client side, Server Side, Both

Application Objects

Application objects represent the set of conditions which must be matched in order for actions to take place. This includes the object type, the match type (exact, partial, prefix, or suffix), the input representation (text or hexadecimal), and the actual content to match.

Hexadecimal input representation is used to match binary content such as executable files, while text input representation is used to match things like file or email content. You can also use hexadecimal input representation for binary content found in a graphic image. You could also use text input representation to match the same graphic if it contains a certain string in one of its properties fields.

The File Content application object type provides a way to match a pattern within a compressed file. This type of application object can only be used with FTP Data Transfer or SMTP Client Policies.

Table 2 describes the supported application object types.

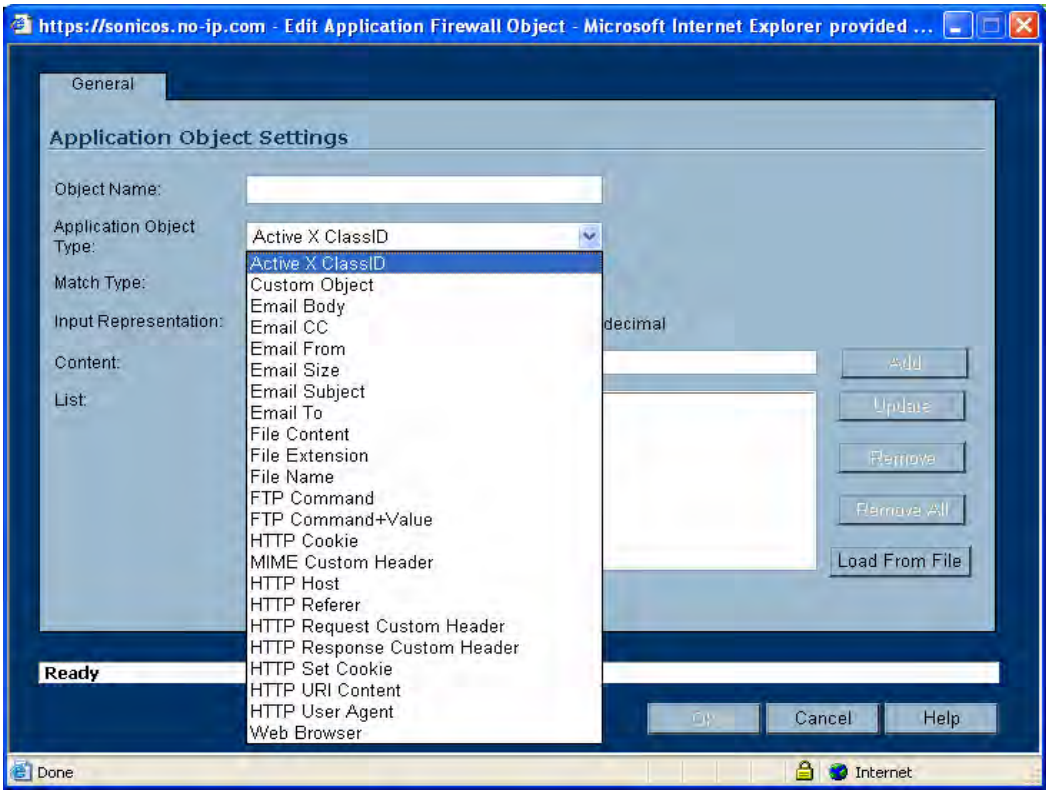
Table 2 Application Object Types

Object Type	Description	Match Types	Negative Matching	Extra Properties
ActiveX ClassID	Class ID of an Active-X component. For example, ClassID of Gator Active-X component is "c1fb8842-5281-45ce-a271-8fd5f117ba5f"	Exact	No	None
Custom Object	Allows specification of an IPS-style custom set of conditions.	Exact	No	There are 4 additional, optional parameters that can be set: offset (describes from what byte in packet payload we should start matching the pattern – starts with 1), depth (describes at what byte in the packet payload we should stop matching the pattern – starts with 1), minimum payload size and maximum payload size.
Email Body	Any content in the body of an email.	Partial	No	None
Email CC (MIME Header)	Any content in the CC MIME Header.	Exact, Partial, Prefix, Suffix	Yes	None
Email From (MIME Header)	Any content in the From MIME Header.	Exact, Partial, Prefix, Suffix	Yes	None
Email Size	Allows specification of the maximum email size that can be sent.	N/A	No	None
Email Subject (MIME Header)	Any content in the Subject MIME Header.	Exact, Partial, Prefix, Suffix	Yes	None
Email To (MIME Header)	Any content in the To MIME Header.	Exact, Partial, Prefix, Suffix	Yes	None
MIME Custom Header	Allows for creation of MIME custom headers.	Exact, Partial, Prefix, Suffix	Yes	A Custom header name needs to be specified.
File Content	Allows specification of a pattern to match in the content of a file. The pattern will be matched even if the file is compressed.	Partial	No	'Disable attachment' action should never be applied to this object.

Object Type	Description	Match Types	Negative Matching	Extra Properties
Filename	In cases of email, this is an attachment name. In cases of HTTP, this is a filename of an uploaded attachment to the Web mail account. In cases of FTP, this is a filename of an uploaded or downloaded file.	Exact, Partial, Prefix, Suffix	Yes	None
Filename Extension	In cases of email, this is an attachment filename extension. In cases of HTTP, this is a filename extension of an uploaded attachment to the Web mail account. In cases of FTP, this is a filename extension of an uploaded or downloaded file.	Exact	Yes	None
FTP Command	Allows selection of specific FTP commands.	N/A	No	None
FTP Command + Value	Allows selection of specific FTP commands and their values.	Exact, Partial, Prefix, Suffix	Yes	None
HTTP Cookie Header	Allows specification of a Cookie sent by a browser.	Exact, Partial, Prefix, Suffix	Yes	None
HTTP Host Header	Content found inside of the HTTP Host header. Represents hostname of the destination server in the HTTP request, such as www.google.com.	Exact, Partial, Prefix, Suffix	Yes	None
HTTP Referrer Header	Allows specification of content of a Referrer header sent by a browser – this can be useful to control or keep stats of which Web sites redirected a user to customer's Web site.	Exact, Partial, Prefix, Suffix	Yes	None

Object Type	Description	Match Types	Negative Matching	Extra Properties
HTTP Request Custom Header	Allows creation of custom HTTP Request headers.	Exact, Partial, Prefix, Suffix	Yes	A Custom header name needs to be specified.
HTTP Response Custom Header	Allows creation of custom HTTP Response headers.	Exact, Partial, Prefix, Suffix	Yes	A Custom header name needs to be specified.
HTTP Set Cookie Header	Set-Cookie headers. Provides a way to disallow certain cookies to be set in a browser.	Exact, Partial, Prefix, Suffix	Yes	None
HTTP URI Content	Any content found inside of the URI in the HTTP request	Exact, Partial, Prefix, Suffix	No	None
HTTP User-Agent Header	Any content inside of a User-Agent header. For example: User-Agent: Skype.	Exact, Partial, Prefix, Suffix	Yes	None
Web Browser	Allows selection of specific Web browsers (MSIE, Netscape, Firefox).	N/A	Yes	None

You can see the available types of application objects in a drop-down list in the Application Objects Setting screen:



Application Object Type: Active X ClassID

In the Application Object screen, you can add multiple entries to create a list of content elements to match. All content that you provide in an application object is case-insensitive for matching purposes. A hexadecimal representation is used to match binary content. You can use a hex editor or a network protocol analyzer like Wireshark (formerly Ethereal) to obtain hex format for binary files. For more information about these tools, see the following sections:

- "Wireshark" on page 41
- "Hex Editor" on page 44

You can use the Load From File button to import content from predefined text files that contain multiple entries for an application object to match. Each entry in the file must be on its own line.

Multiple entries, either from a text file or entered manually, are displayed in the List area. List entries are matched using the logical OR, so if any item in the list is matched, the action for the policy is executed.

An application object can include a total of no more than 8000 characters. If each element within an application object contains approximately 30 characters, then you can enter about 260 elements. The maximum element size is 500 bytes.

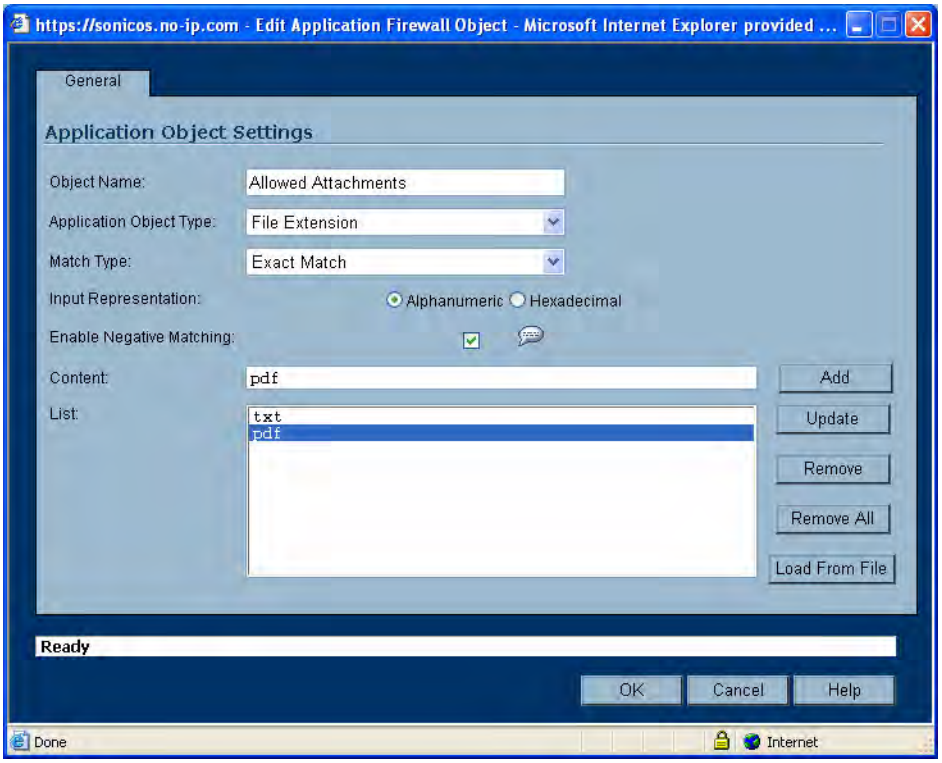
Negative Matching

Negative matching provides an alternate way to specify which content to block. You can enable negative matching in an application object when you want to block everything except a particular type of content. When you use the object in a policy, the policy will execute actions based on absence of the content specified in the application object.

Although all application firewall policies are DENY policies, you can simulate an ALLOW policy by using negative matching. For instance, you can allow email *.txt* attachments and block attachments of all other file types. Or you can allow a few types, and block all others.

Not all application object types can utilize negative matching. For those that can, you will see the Enable Negative Matching checkbox on the Application Object Settings screen.

Figure 3 Enable Negative Matching Checkbox



https://sonicos.no-ip.com - Edit Application Firewall Object - Microsoft Internet Explorer provided ...

Application Object Settings

Object Name: Allowed Attachments

Application Object Type: File Extension

Match Type: Exact Match

Input Representation: ● Alphanumeric ○ Hexadecimal

Enable Negative Matching: ☑

Content: pdf

List:
txt
pdf

Ready

Actions

Actions define how the application firewall policy reacts to matching events. You can choose a customizable action or select one of three predefined actions.

The three predefined actions are:

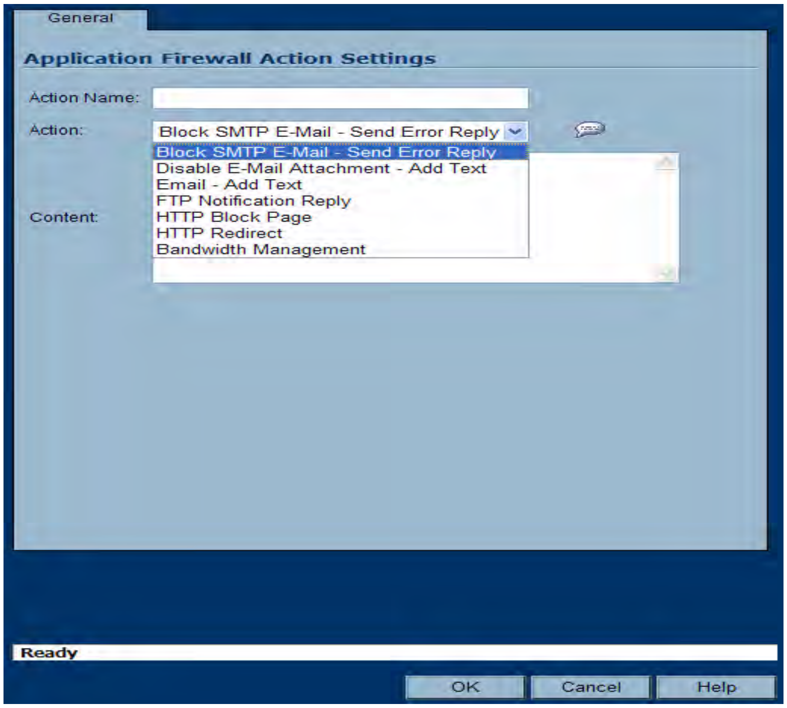
- No Action
- Reset / Drop
- Block SMTP Email Without Reply

The seven customizable actions are:

- Block SMTP Email - Send Error Reply
- Disable Email Attachment - Add Text
- Email - Add Text
- FTP Notification Reply
- HTTP Block Page
- HTTP Redirect
- Bandwidth Management

Note that only the seven customizable actions are available for editing in the Application Firewall Action Settings dialog box. See Figure 4. The three predefined actions cannot be edited or deleted. When you create a policy, the Policy Settings dialog box provides a way for you to select from the predefined actions along with any customized actions that you have defined.

Figure 4 Action Settings



Application Firewall Action Settings

Action Name:

Action: Block SMTP E-Mail - Send Error Reply

Content:

Table 3 describes the available action types.

Table 3 Action Types

Action Type	Description	Predefined or Custom
No Action	Policies can be specified without any action. This allows "log only" policy types.	Predefined
Reset / Drop	For TCP, the connection will be reset. For UDP, the packet will be dropped.	Predefined
Block SMTP Email Without Reply	Blocks SMTP email, but to the sender it looks like email was successfully sent.	Predefined
Block SMTP Email - Send Error Reply	Blocks SMTP email and notifies the sender with a customized error message.	Custom
Disable Email Attachment - Add Text	Disables attachment inside of an email and adds customized text.	Custom
Email - Add Text	Appends custom text at the end of the email.	Custom
FTP Notification Reply	Sends text back to the client over the FTP control channel without terminating the connection.	Custom
HTTP Block Page	Allows a custom HTTP block page configuration with a choice of colors.	Custom
HTTP Redirect	Provides HTTP Redirect functionality. For example, if someone would like to redirect people to the Google Web site, the customizable part will look like: http://www.google.com	Custom
Bandwidth Management	Allows definition of bandwidth management constraints with same semantics as Access Rule BWM policy definition.	Custom

Application Layer Bandwidth Management

Application layer bandwidth management allows you to create policies that regulate bandwidth consumption by specific file types within a protocol, while allowing other file types to use unlimited bandwidth. This enables you to distinguish between desirable and undesirable traffic within the same protocol. Application layer bandwidth management is supported for HTTP Client, HTTP Server, Custom, and FTP file transfer policies. For details about policy types, see Table 1 on page 5.

For example, as an administrator you might want to limit .mp3 and executable file downloads during work hours to no more than 1 Mbps. At the same time, you want to allow downloads of productive file types such as .doc or .pdf up to the maximum available bandwidth, or even give the highest possible priority to downloads of the productive content. Application layer bandwidth management allows you to create policies to do this.

Application layer bandwidth management functionality is supported with a Bandwidth Management type action, available when adding a new action from the Application Firewall > Actions screen.

Application layer bandwidth management configuration is handled in the same way as the current bandwidth management configuration associated with Firewall > Access Rules.

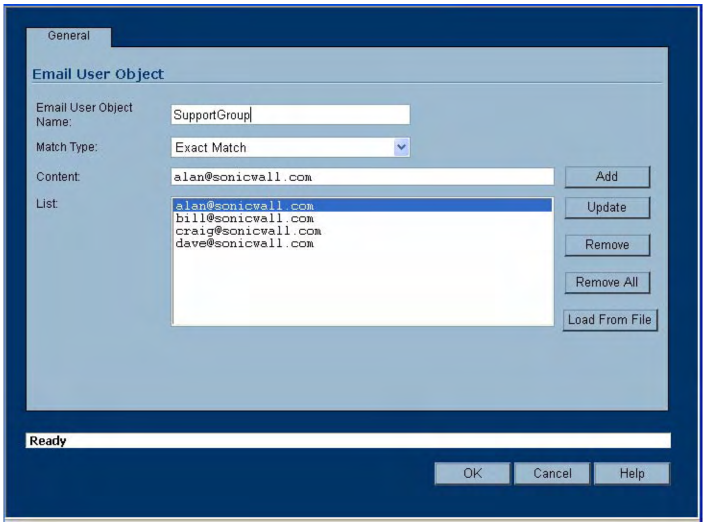
Note Bandwidth management policies defined with Firewall > Access Rules always have priority over application layer bandwidth management policies. Thus, if an access rule bandwidth management policy is applied to a certain connection, then an application layer bandwidth management policy will never be applied to that connection.

Email User Objects

Application firewall allows the creation of custom email user lists as email user objects. You can only use email user objects in an SMTP client policy configuration. Email user objects can represent either individual users or the entire domain. You can also create an email user object that represents a group by adding a list of individual users to the object. This provides a way to easily include or exclude a group of users when creating an SMTP client policy.

For example, you can create an email user object to represent the support group:

Figure 5 Email User Object



Email User Object

Email User Object Name: SupportGroup

Match Type: Exact Match

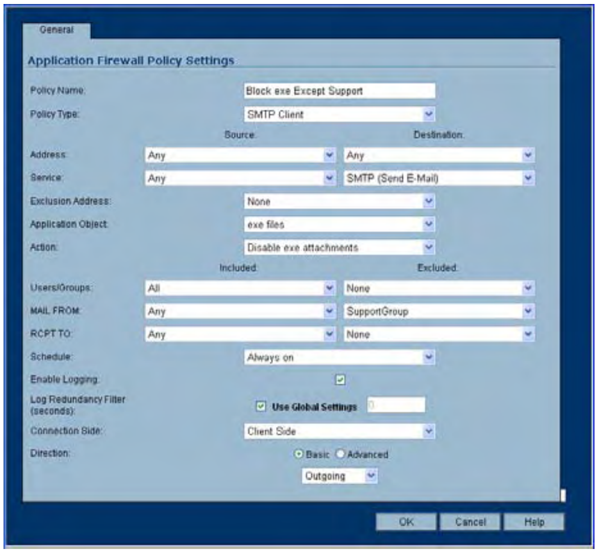
Content: alan@sonicwall.com

List:
alan@sonicwall.com
bill@sonicwall.com
craig@sonicwall.com
dave@sonicwall.com

Ready

After you define the group in an email user object, you can create an SMTP client policy that includes or excludes the group. In Figure 6, the settings exclude the support group from a policy that prevents executable files from being attached to outgoing email. You can use the email user object in either the MAIL FROM or RCPT TO fields of the SMTP client policy. The MAIL FROM field refers to the sender of the email. The RCPT TO field refers to the intended recipient.

Figure 6 SMTP Client Policy



Application Firewall Policy Settings

Policy Name: Block exe Except Support
Policy Type: SMTP Client

	Source:	Destination:
Address:	Any	Any
Service:	Any	SMTP (Send E-Mail)

Exclusion Address: None
Application Object: exe files
Action: Disable exe attachments

	Included:	Excluded:
Users/Groups:	All	None
MAIL FROM:	Any	SupportGroup
RCPT TO:	Any	None

Schedule: Always on
Enable Logging: ☑
Log Redundancy Filter (seconds): ☑ **Use Global Settings** 0
Connection Side: Client Side
Direction: ● Basic ○ Advanced
Outgoing

Although application firewall cannot extract group members directly from Outlook Exchange or similar applications, you can use the member lists in Outlook to create a text file that lists the group members. Then when you create an email user object for this group, you can use the Load From File button to import the list from your text file. Be sure that each email address is on a line by itself in the text file.

Platforms

Application firewall is currently available on the PRO 4060, PRO 4100 and PRO 5060 SonicWALL security appliances running SonicOS Enhanced 4.0. The configuration maximums vary depending on the hardware model, as shown in Table 4.

Table 4 Maximum Configuration per Model

Model	Max Policies	Max Application Objects	Max Actions	Max Email User Objects	Max Email Concurrent Connections
PRO 4060	50	50	50	50	20000
PRO 4100	100	100	100	100	64000
PRO 5060	300	300	300	300	128000

Supported Standards

The SonicOS Enhanced application firewall feature supports the following protocols:

- HTTP
- FTP
- SMTP
- POP3
- Other protocols - generic TCP streams and UDP packet inspection

  You can match any protocol by creating a custom application object.

Using Application Firewall

You can configure application firewall in the user interface of the supported SonicWALL PRO Series security appliances running SonicOS Enhanced 4.0. This section contains the following subsections:

- "Configuration Overview" on page 16
- "Configuration Procedure Using the Wizard" on page 16
- "Manual Configuration Procedure" on page 20
- "Verifying Application Firewall Configuration" on page 27

Configuration Overview

You can configure policies in application firewall using the wizard or manually. The wizard provides a safe method of configuration and helps prevent errors that could result in unnecessary blocking of network traffic. Manual configuration offers more flexibility for situations that require custom policies.

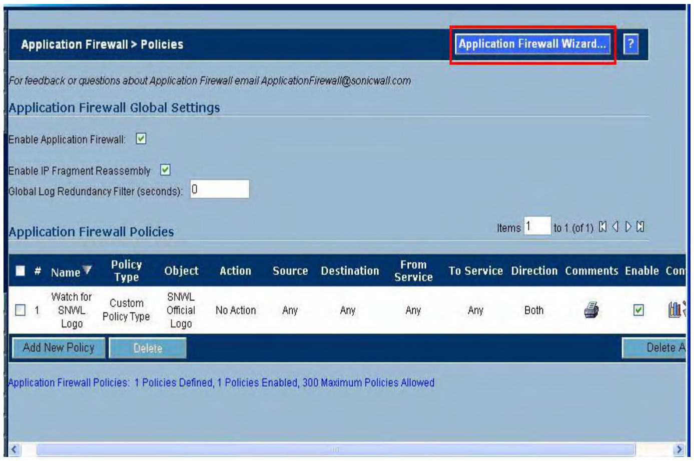
Configuration Procedure Using the Wizard

The application firewall wizard provides safe configuration for many common use cases, but not for everything. If at any time during the wizard you are unable to find the options that you need, you can click Cancel and proceed using manual configuration. See the "Manual Configuration Procedure" section on page 20. To use the wizard to configure application firewall, perform the following steps:

Step 1 Login to the SonicWALL security appliance.

Step 2 In the navigation pane on the left side, click **Application Firewall**. The Application Firewall > Policies screen displays.

Step 3 In the upper right corner, click **Application Firewall Wizard**.



Application Firewall > Policies

For feedback or questions about Application Firewall email ApplicationFirewall@sonicwall.com

Application Firewall Global Settings

Enable Application Firewall: ☑

Enable IP Fragment Reassembly ☑

Global Log Redundancy Filter (seconds): 0

Application Firewall Policies

Items 1 to 1 (of 1)

■	#	Name	Policy Type	Object	Action	Source	Destination	From Service	To Service	Direction	Comments	Enable	Con
□	1	Watch for SNWL Logo	Custom Policy Type	SNWL Official Logo	No Action	Any	Any	Any	Any	Both		☑	

Application Firewall Policies: 1 Policies Defined, 1 Policies Enabled, 300 Maximum Policies Allowed

Step 4 In the Application Firewall Wizard dialog box, click **Next**.

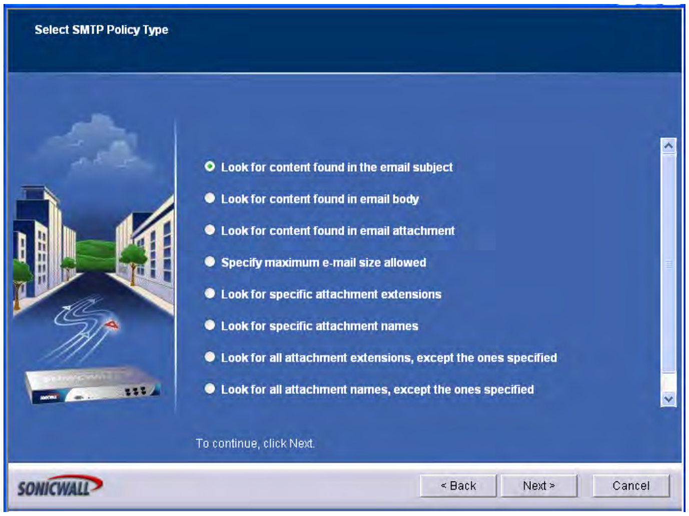
Step 5 In Choose a Policy Type, click a selection for the policy type, and click **Next**.

You can choose among SMTP, incoming POP3, Web Access, or FTP file transfer. The policy that you create will only apply to the type of traffic that you select. The next screen will vary depending on your choice here.

Step 6 In the Select <your choice> Policy Type screen, select the policy type from the choices supplied, and click **Next**.

The screen is one of the four screens shown below, depending on your choice in the previous step:

- Select SMTP Policy Type:

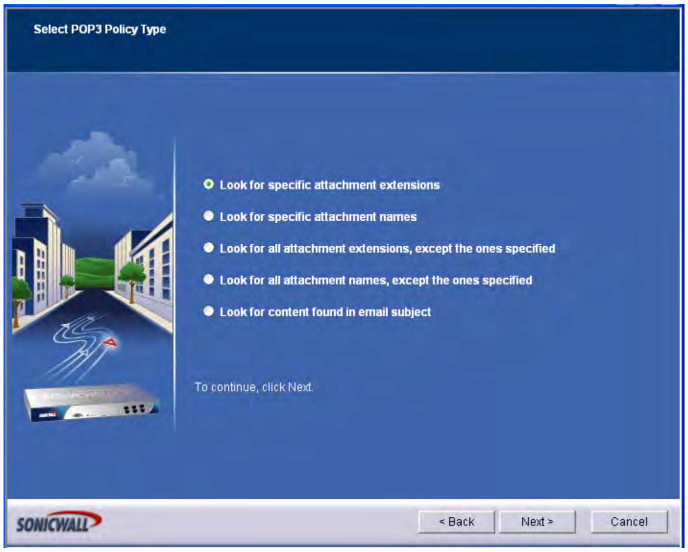


Select SMTP Policy Type

● Look for content found in the email subject
○ Look for content found in email body
○ Look for content found in email attachment
○ Specify maximum e-mail size allowed
○ Look for specific attachment extensions
○ Look for specific attachment names
○ Look for all attachment extensions, except the ones specified
○ Look for all attachment names, except the ones specified

To continue, click Next.

- Select POP3 Policy Type:

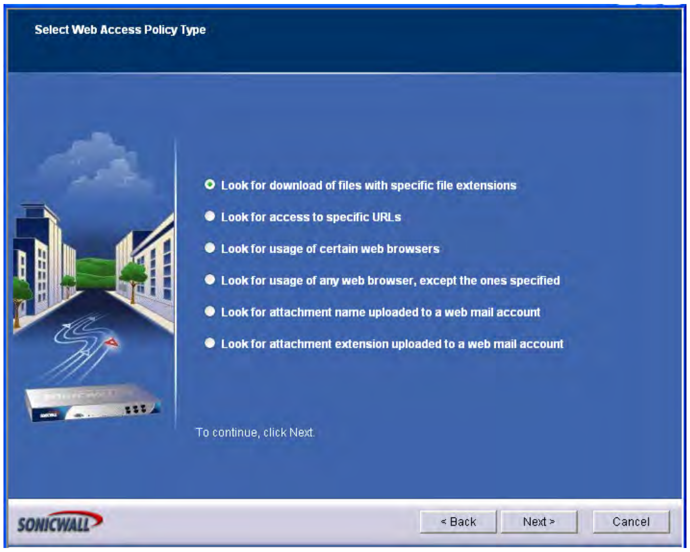


Select POP3 Policy Type

● Look for specific attachment extensions
○ Look for specific attachment names
○ Look for all attachment extensions, except the ones specified
○ Look for all attachment names, except the ones specified
○ Look for content found in email subject

To continue, click Next.

- Select Web Access Policy Type:

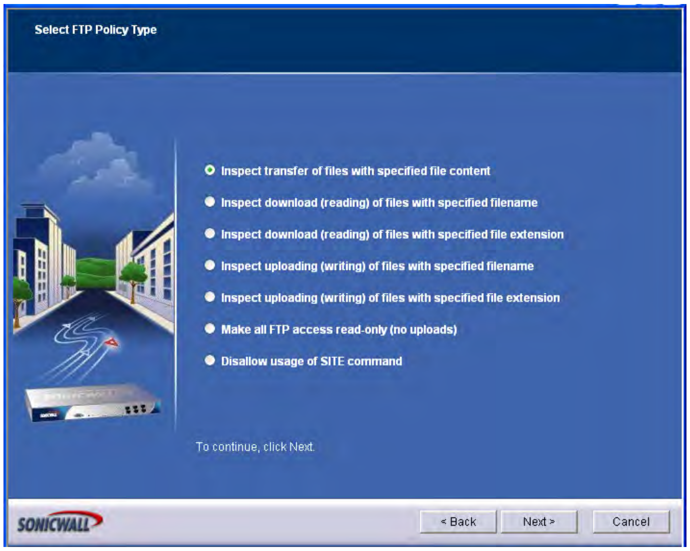


Select Web Access Policy Type

- ◉ Look for download of files with specific file extensions
- ○ Look for access to specific URLs
- ○ Look for usage of certain web browsers
- ○ Look for usage of any web browser, except the ones specified
- ○ Look for attachment name uploaded to a web mail account
- ○ Look for attachment extension uploaded to a web mail account

To continue, click Next.

- Select FTP Policy Type:



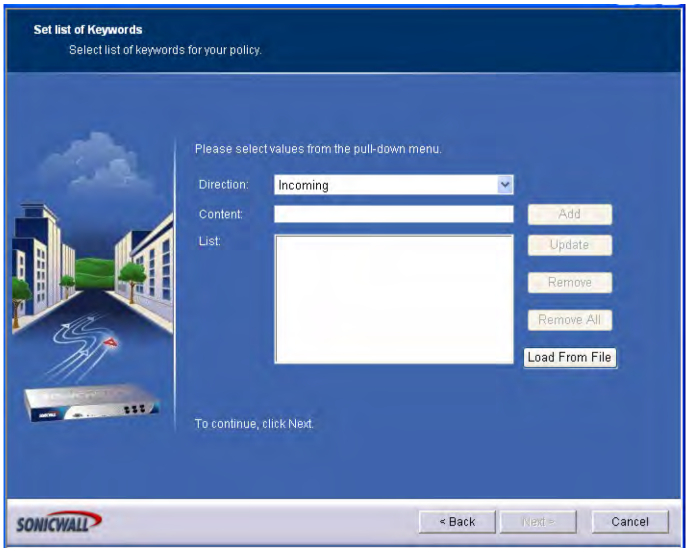
Select FTP Policy Type

- ◉ Inspect transfer of files with specified file content
- ○ Inspect download (reading) of files with specified filename
- ○ Inspect download (reading) of files with specified file extension
- ○ Inspect uploading (writing) of files with specified filename
- ○ Inspect uploading (writing) of files with specified file extension
- ○ Make all FTP access read-only (no uploads)
- ○ Disallow usage of SITE command

To continue, click Next.

Step 7 The screen displayed here will vary depending on your choice for policy type in the previous step. For the following policy types, the wizard displays the Set List of Keywords screen on which you can select the traffic direction to scan, and the content or keywords to match.

- All SMTP policy types *except* **Specify maximum email size**
- All POP3 policy types
- All Web Access policy types
- All FTP policy types *except* **Make all FTP access read-only** and **Disallow usage of SITE command**



Set list of Keywords

Select list of keywords for your policy.

Please select values from the pull-down menu.

Direction: Incoming

Content:

List:

To continue, click Next.

In the Set List of Keywords screen, perform the following steps:

- In the Direction drop-down list, select the traffic direction to scan.
- Do one of the following:

Note If you selected a choice with the words **except the ones specified** in the previous step, content that you enter here will be the only content that does *not* cause the action to occur. See "Negative Matching" on page 10.

  – In the Content text box, type or paste a text or hexadecimal representation of the content to match, and then click **Add**. Repeat until all content is added to the List text box.

  – To import keywords from a predefined text file that contains a list of content values, one per line, click **Load From File**.

- Click **Next**.

If you selected a policy type in the previous step that did *not* result in the Set List of Keywords screen with the standard options, the wizard displays a screen that allows you to select the traffic direction, and certain other choices depending on the policy type.

- In the Direction drop-down list, select the traffic direction to scan.
- SMTP: In the Set Maximum Email Size screen, in the Maximum Email Size text box, enter the maximum number of bytes for an email message.
- Web Access: In the special-case Set List of Keywords screen, the Content text box has a drop-down list with a limited number of choices, and no Load From File button is available. Select a browser from the drop-down list.
- FTP: In the special-case Set List of Keywords screen, you can only select the traffic direction to scan.
- Click **Next**.

Step 8 In the Select Action screen, select the action to take when matching content is found in the specified type of network traffic, and then click **Next**.

You will see one or more of the following choices depending on the policy type, which is shown in parentheses here for reference:

- Blocking Action - block and send custom email reply (SMTP)

- Blocking Action - block without sending email reply (SMTP)
- Blocking Action - disable attachment and add custom text (POP3)
- Blocking Action - custom block page (Web Access)
- Blocking Action - redirect to new location (Web Access)
- Blocking Action - reset connection (Web Access, FTP)
- Blocking Action - add block message (FTP)
- Add Email Banner (append text at the end of email) (SMTP)
- Log Only (SMTP, POP3, Web Access, FTP)

Step 9 In the Set Action Content screen (if it is displayed), in the Content text box, type the text or URL that you want to use, and then click **Next**.

The Set Action Content screen is only displayed when you selected an action in the previous step that requires additional text. For a Web Access policy type, if you selected an action that redirects the user, you can type the new URL into the Content text box.

Step 10 In the Enter Policy Name screen, in the Policy Name text box, type a descriptive name for the policy, and then click **Next**.

Step 11 In the Application Firewall New Policy Configuration Summary screen, review the displayed values for the new policy and do one of the following:

- To create a policy using the displayed configuration values, click **Apply**.
- To change one or more of the values, click **Back**.

Step 12 In the Application Firewall Policy Wizard Complete screen, to exit the wizard, click **Close**.

Manual Configuration Procedure

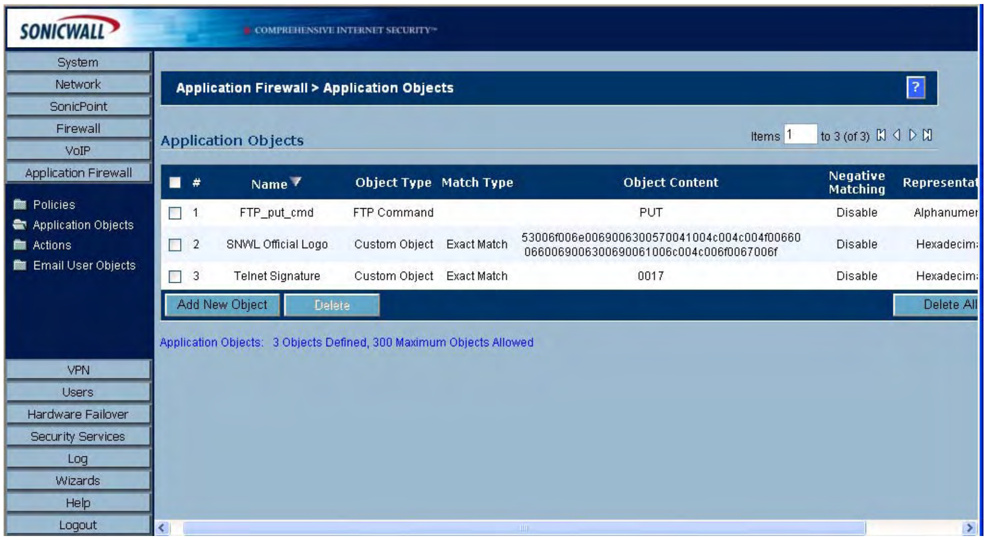
You can configure application firewall without using the wizard. When configuring manually, you must remember to configure all components, including application objects, actions, email user objects if required, and finally, a policy that references them.

Configuring Application Objects

This section describes how to manually create an application object.

For detailed information about application object types, see “Application Objects” on page 6.

Step 1 In the navigation pane on the left side, click **Application Firewall**, and then click **Application Objects**.



Application Firewall > Application Objects

Application Objects

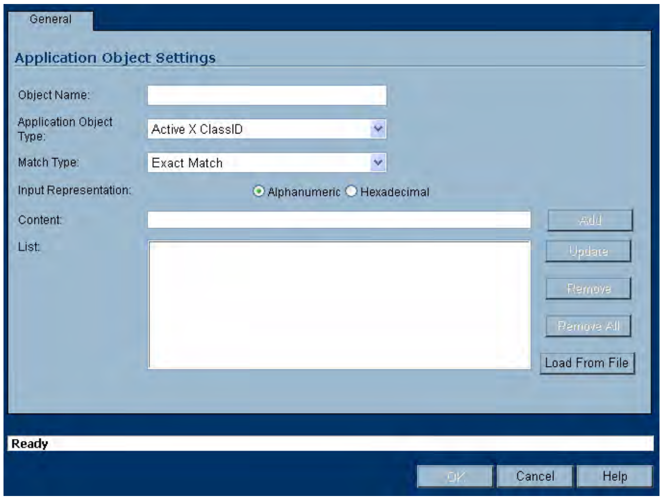
Items 1 to 3 (of 3)

□	#	Name	Object Type	Match Type	Object Content	Negative Matching	Representat
□	1	FTP_put_cmd	FTP Command		PUT	Disable	Alphanumer
□	2	SNWL Official Logo	Custom Object	Exact Match	53006f006e00690063005700410004c004c004f00660 0660069006300690061006c004c006f0067006f	Disable	Hexadecim
□	3	Telnet Signature	Custom Object	Exact Match	0017	Disable	Hexadecim

Application Objects: 3 Objects Defined, 300 Maximum Objects Allowed

Step 2 In the Application Objects screen, click **Add New Object**.

Step 3 In the Application Object Settings dialog box, in the Object Name text box, type a descriptive name for the object.



Application Object Settings

Object Name:

Application Object Type: Active X ClassID

Match Type: Exact Match

Input Representation: ● Alphanumeric ○ Hexadecimal

Content:

List:

Ready

Step 4 Select an Application Object Type from the drop-down list. Your selection here will affect available options in the dialog box. See Table 2 on page 7 for a description of application object types.

Step 5 Select a Match Type from the drop-down list. The available selections depend on the application object type.

Step 6 For the Input Representation, click **Alphanumeric** for a text pattern to match, or click **Hexadecimal** if you want to match binary content.

Step 7 In the Content text box, type the pattern to match, and then click **Add**. The content appears in the List text box. Repeat to add another element to match.

Alternatively, you can click **Load From File** to import a list of elements from a text file. Each element in the file must be on a line by itself.

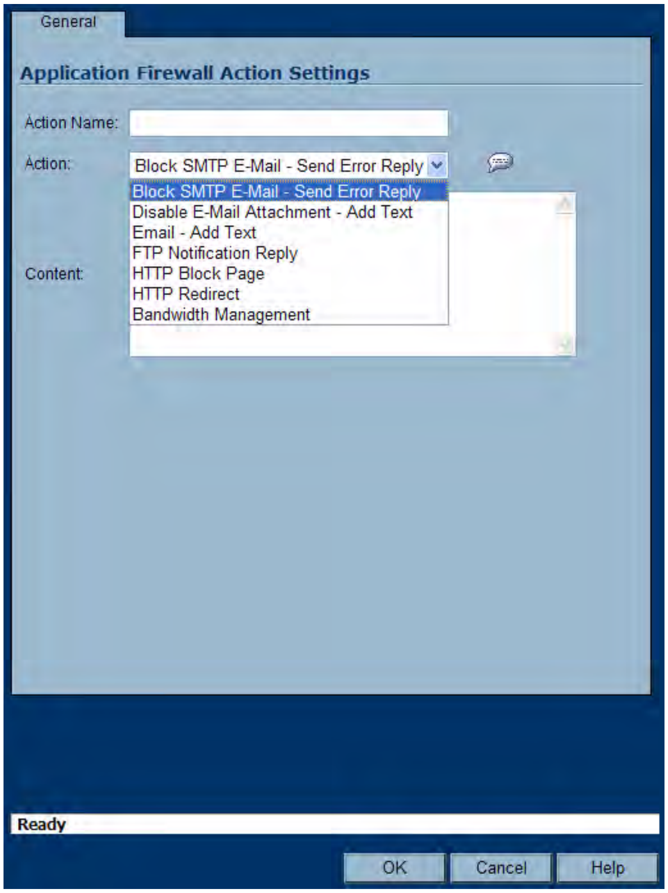
Step 8 Click **OK**.

Configuring Actions

If you do not want one of the three predefined actions, you can select among seven configurable actions. The Actions Settings dialog box provides a way to customize a configurable action with text or a URL. The three predefined actions, plus any configurable actions that you have created, are available for selection in the Policies Settings dialog box.

For more information about actions, see "Actions" on page 11.

Figure 7 Action Settings



Application Firewall Action Settings

Action Name:

Action: Block SMTP E-Mail - Send Error Reply

Content:

Ready

Step 1 In the navigation pane on the left side, click **Application Firewall**, and then click **Actions**.

Step 2 In the Actions screen, click **Add New Action**.

Step 3 In the Application Firewall Action Settings dialog box, type a descriptive name for the action.

Step 4 In the Actions drop-down list, select the action that you want.

Step 5 In the Content text box, type the text or URL to be used in the action and then click **Add**.

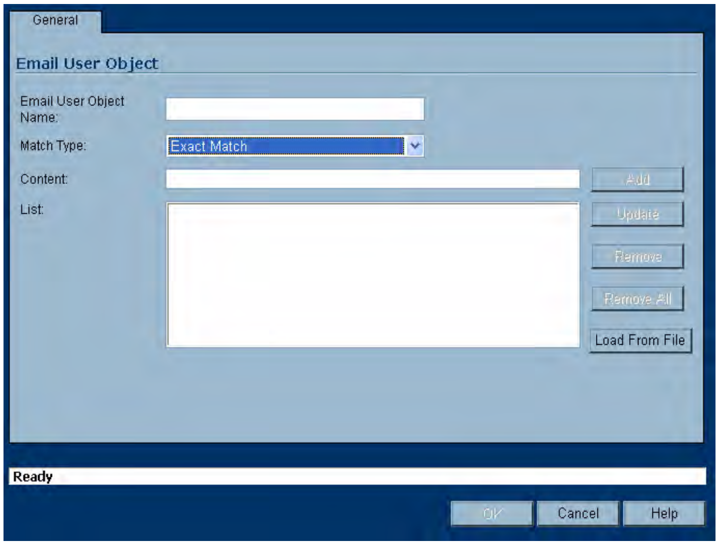
Step 6 Click **OK**.

Configuring Email User Objects

You can create email user objects for use with SMTP Client policies. An email user object can be a list of users or an entire domain.

For more information about email user objects, see "Email User Objects" on page 13.

Figure 8 Email User Object dialog box



Step 1 In the navigation pane on the left side, click Application Firewall, and then click **Email User Objects**.

Step 2 In the Email User Objects screen, click **Add New Email User Object**.

Step 3 In the Email User Object dialog box, type a descriptive name for the email user object.

Step 4 For Match Type, select **Exact Match** or **Partial Match**. Use Partial Match when you want to match on the domain only. To match on individual users, select Exact Match.

Step 5 In the Content text box, type the content to match and then click **Add**.

To match on a domain, type @ followed by the domain name, for example: **@sonicwall.com**. To match on an individual user, type the full email address, for example: **jsmith@sonicwall.com**. Repeat this step until you have added as many elements as you want.

Alternatively, you can click **Load From File** to import a list of elements from a text file. Each element in the file must be on a line by itself.

By defining an email user object with a list of users, you can use application firewall to simulate groups.

Step 6 Click **OK**.

Configuring Application Layer Bandwidth Management

To use application layer bandwidth management, you must first enable bandwidth management on the interface that will handle the traffic.

To enable bandwidth management on an interface, perform the following steps:

Step 1 In the navigation pane on the left side, click **Network**, and then click **Interfaces**.

Step 2 In the Interface Settings table, click the icon under **Configure** for the desired interface.

Step 3 In the Edit Interface dialog box, click the **Advanced** tab.

Step 4 Do one or both of the following:

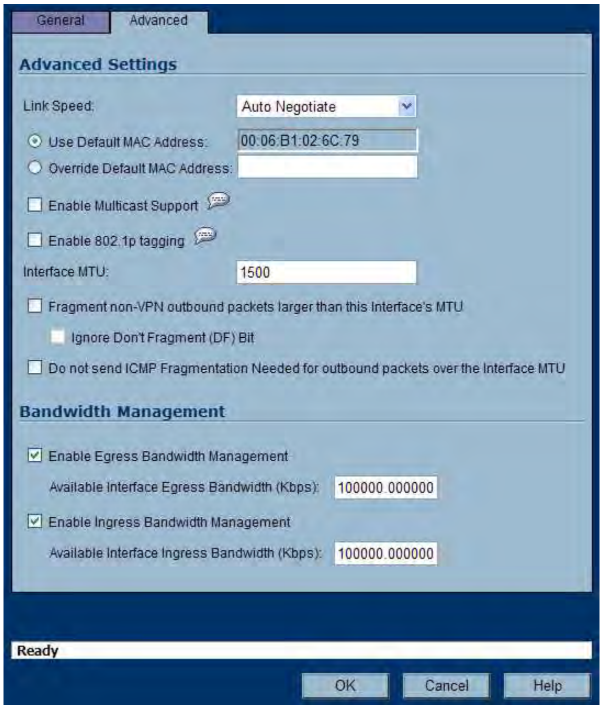
- Under Bandwidth Management, to manage outbound bandwidth, select the **Enable Egress Bandwidth Management** checkbox, and optionally set the **Available Interface Egress Bandwidth (Kbps)** field to the maximum for the interface.

- Under Bandwidth Management, to manage inbound bandwidth, select the **Enable Ingress Bandwidth Management** checkbox and optionally set the **Available Interface Ingress Bandwidth (Kbps)** field to the maximum for the interface.

Table 5 Maximum Interface Bandwidth Settings

SonicWALL Appliance Model	Interface Rating	Max Bandwidth in Kbits/sec
SonicWALL PRO 4060	100 Megabits per second	100000
SonicWALL PRO 4100	1 Gigabit per second	1000000
SonicWALL PRO 5060	1 Gigabit per second	1000000

Figure 9 Edit Interface - Advanced



Advanced Settings

Link Speed: Auto Negotiate

● Use Default MAC Address: 00:06:B1:02:6C:79

○ Override Default MAC Address:

□ Enable Multicast Support

□ Enable 802.1p tagging

Interface MTU: 1500

□ Fragment non-VPN outbound packets larger than this Interface's MTU

□ Ignore Don't Fragment (DF) Bit

□ Do not send ICMP Fragmentation Needed for outbound packets over the Interface MTU

Bandwidth Management

☑ Enable Egress Bandwidth Management

Available Interface Egress Bandwidth (Kbps): 100000.000000

☑ Enable Ingress Bandwidth Management

Available Interface Ingress Bandwidth (Kbps): 100000.000000

Ready

Step 5 Click **OK**.

After bandwidth management is enabled on the interface, you can configure Bandwidth Management as an action setting for an object in Application Firewall.

To configure Bandwidth Management as an action setting:

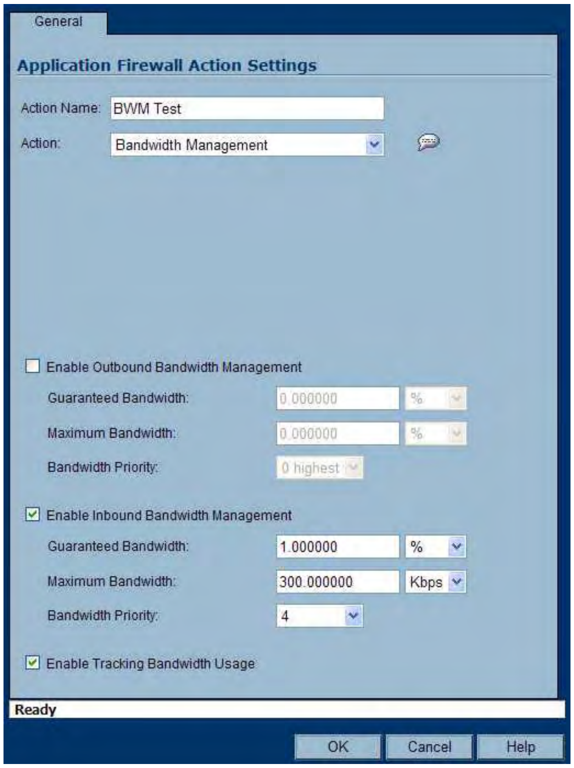
Step 1 In the navigation pane on the left side, click **Application Firewall**, and then click **Actions**.

Step 2 In the Actions screen, click **Add New Action**.

Step 3 In the Application Firewall Action Settings dialog box, type a descriptive name for the action.

Step 4 In the Actions drop-down list, select **Bandwidth Management**.

Figure 10 Creating a Bandwidth Management action



Application Firewall Action Settings

Action Name: BWM Test

Action: Bandwidth Management

□ Enable Outbound Bandwidth Management

Guaranteed Bandwidth: 0.000000 %

Maximum Bandwidth: 0.000000 %

Bandwidth Priority: 0 highest

☑ Enable Inbound Bandwidth Management

Guaranteed Bandwidth: 1.000000 %

Maximum Bandwidth: 300.000000 Kbps

Bandwidth Priority: 4

☑ Enable Tracking Bandwidth Usage

Ready

Step 5 Do one or both of the following:

- To manage outbound bandwidth, select the **Enable Outbound Bandwidth Management** checkbox.
- To manage inbound bandwidth, select the **Enable Inbound Bandwidth Management** checkbox.

Step 6 For **Guaranteed Bandwidth**, optionally enter a value either as a percentage or as kilobits per second. In the drop-down list, select either **%** or **Kbps**.

If you plan to use this custom action for rate limiting rather than guaranteeing bandwidth, you do not need to change the Guaranteed Bandwidth field.

Step 7 For **Maximum Bandwidth**, optionally enter a value either as a percentage or as kilobits per second. In the drop-down list, select either **%** or **Kbps**.

If you plan to use this custom action for guaranteeing bandwidth rather than rate limiting, you do not need to change the Maximum Bandwidth field.

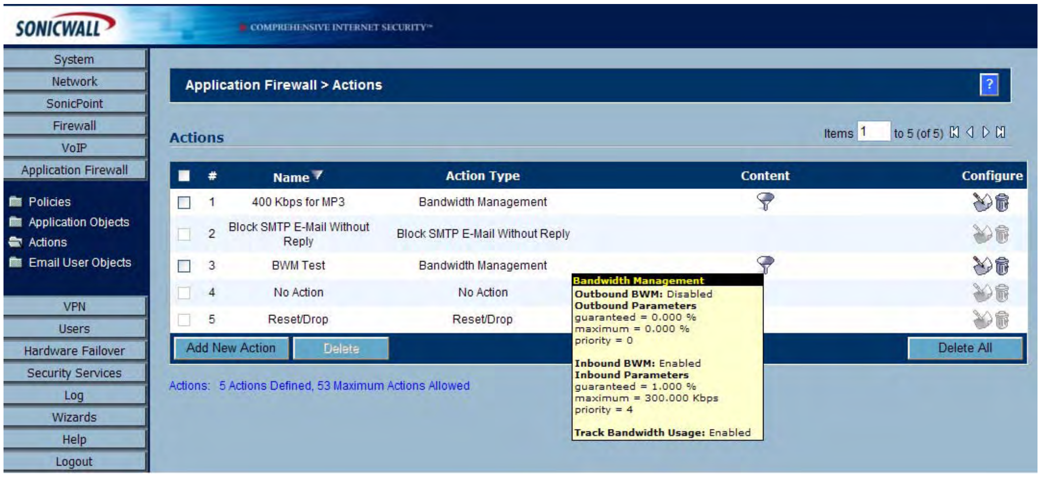
Step 8 For **Bandwidth Priority**, select a priority level from the drop-down list, where 0 is the highest and 7 is the lowest.

Step 9 Optionally select **Enable Tracking Bandwidth Usage** to track the usage.

Step 10 Click **OK**.

You can see the resulting action in the Actions screen, as shown in Figure 11.

Figure 11 Bandwidth Management Action



Application Firewall > Actions

Actions

Items 1 to 5 (of 5)

■	#	Name	Action Type	Content	Configure
□	1	400 Kbps for MP3	Bandwidth Management		
□	2	Block SMTP E-Mail Without Reply	Block SMTP E-Mail Without Reply		
□	3	BWM Test	Bandwidth Management		
□	4	No Action	No Action		
□	5	Reset/Drop	Reset/Drop		

Add New Action | Delete | Delete All

Actions: 5 Actions Defined, 53 Maximum Actions Allowed

Bandwidth Management
Outbound BWM: Disabled
Outbound Parameters
guaranteed = 0.000 %
maximum = 0.000 %
priority = 0

Inbound BWM: Enabled
Inbound Parameters
guaranteed = 1.000 %
maximum = 300.000 Kbps
priority = 4

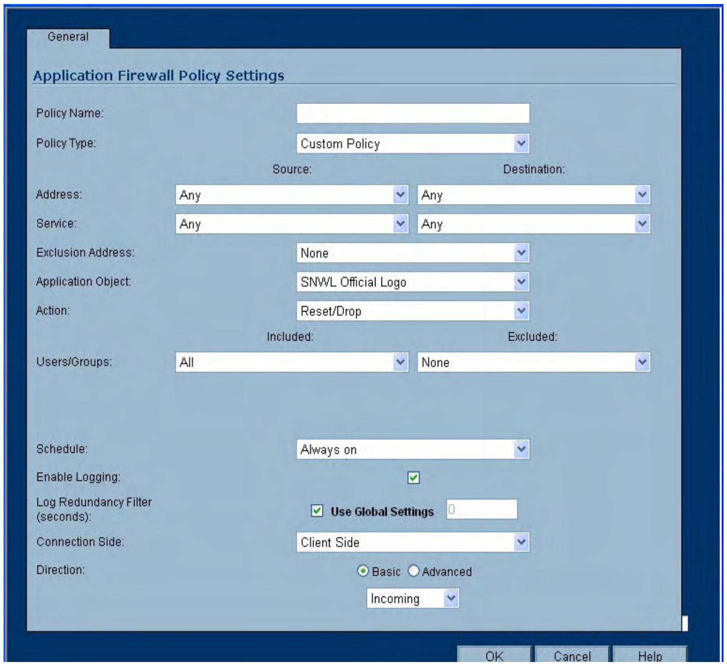
Track Bandwidth Usage: Enabled

Configuring a Policy

When you have created an application object, and optionally, an action or an email user object, you are ready to create a policy that uses them.

For information about policies and policy types, see "Policies" on page 3.

Figure 12 Policy Settings



Application Firewall Policy Settings

Policy Name:		
Policy Type:	Custom Policy	
	Source:	Destination:
Address:	Any	Any
Service:	Any	Any
Exclusion Address:	None	
Application Object:	SNWL Official Logo	
Action:	Reset/Drop	
	Included:	Excluded:
Users/Groups:	All	None
Schedule:	Always on	
Enable Logging:	☑	
Log Redundancy Filter (seconds):	☑ Use Global Settings 0	
Connection Side:	Client Side	
Direction:	● Basic ○ Advanced Incoming	

Step 1 In the navigation pane on the left side, click **Application Firewall**, and then click **Policies**.

Step 2 In the Application Firewall Global Settings screen, click **Add New Policy**.

Step 3 In the Application Firewall Policies Settings dialog box, type a descriptive name for the policy.

Step 4 Select a Policy Type from the drop-down list. Your selection here will affect available options in the dialog box. For information about available policy types, see "Policies" on page 3.

Step 5 Select a source and destination address from the Address drop-down lists, and select the source or destination service. Some policy types do not provide a choice of service.

Step 6 For Exclusion Address, optionally select an address from the drop-down list. This address will not be affected by the policy.

Step 7 For Application Object, select an application object from the drop-down list. The list contains the defined application objects that are applicable to the policy type.

Step 8 For Action, select an action from the drop-down list. The list contains actions that are applicable to the policy type, and can include the three predefined actions, plus any customized actions.

Step 9 For Users/Groups, select from the drop-down lists for both Included and Excluded. The selected users or group under Excluded will not be affected by the policy.

Step 10 If the policy type is SMTP, select from the drop-down lists for Mail From and Rcpt To, for both Included and Excluded. The selected users or group under Excluded will not be affected by the policy.

Step 11 For Schedule, select from the drop-down list. A variety of schedules for the policy to be in effect is available in the list.

Step 12 If you want the policy to create a log entry when a match is found, check **Enable Logging**.

Step 13 For Log Redundancy Filter, you can either check **Global Settings** to use the default, or you can enter a number to indicate how many policy matches are required for each log entry.

Step 14 For Connection Side, select from the drop-down list. The available choices depend on the policy type.

Step 15 For Direction, click either **Basic** or **Advanced**. Basic allows you to select incoming, outgoing, or both. Advanced allows you to select between zones, such as LAN to WAN.

Step 16 Click **OK**.

Verifying Application Firewall Configuration

To verify your policy configuration, you can send some traffic that should match your policy. You can use a network protocol analyzer such as Wireshark to view the packets. Be sure to test for both included and excluded users and groups. You should also run tests according to the schedule that you configured, to determine that the policy is in effect when you want it to be. Check for log entries by using the Logging screen in the SonicOS Enhanced user interface.

Use Cases

Application firewall provides the functionality to handle several types of access control very efficiently. The following use cases are presented in this section:

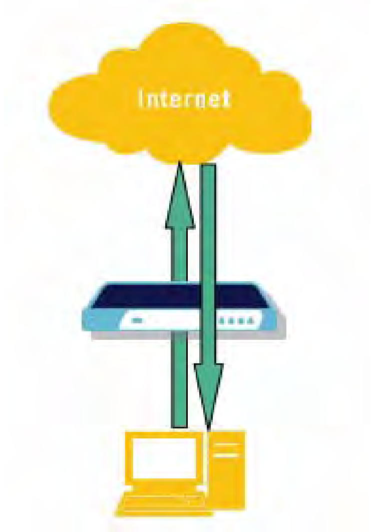
- "Compliance Enforcement" on page 28
- "Hosted Email Environments" on page 29
- "Server Protection" on page 29
- "Web Browser Control" on page 30
- "Email Control" on page 31
- "ActiveX Control" on page 31
- "FTP Control" on page 34
- "Bandwidth Management" on page 37
- "Custom Signature" on page 39

Compliance Enforcement

Many businesses and organizations need to ensure compliance with their policies regarding outbound file transfer. Application firewall provides this functionality in HTTP, FTP, POP3, and SMTP contexts. This can help companies meet regulatory requirements such as HIPPA, SOX, and PCI.

When you configure the policy or policies for this purpose, you can select Direction > Basic > Outgoing to specifically apply your file transfer restrictions to outbound traffic. Or, you can select Direction > Advanced and then specify the exact zones between which to prevent file transfer. For example, you can specify LAN to WAN, LAN to DMZ, or any other zones that you have defined.

Figure 13 Compliance Enforcement



Hosted Email Environments

A hosted email environment is one in which email is available on a user's Internet Service Provider (ISP). Typically, POP3 is the protocol used for email transfer in this environment. Many small-business owners use this model, and would like to control email content as well as email attachments. Running application firewall on the gateway provides a solution for controlling POP3-based as well as SMTP-based email.

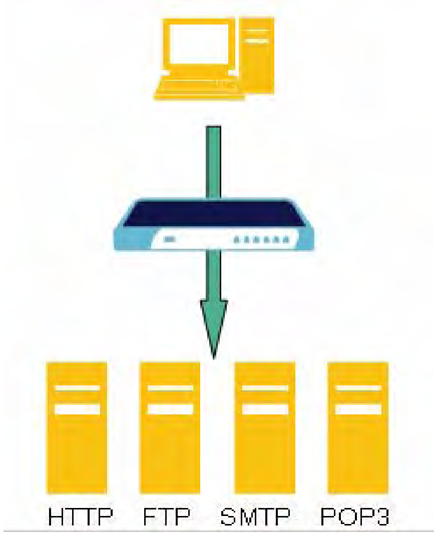
Application firewall can also scan HTTP, which is useful for email hosted by sites such as Yahoo or Hotmail. You can also use application firewall to control FTP when accessing database servers.

If you want a dedicated SMTP solution, you can use SonicWALL Email Security. Email Security is used by many larger businesses for controlling SMTP-based email, but it does not support POP3. For controlling multiple email protocols, application firewall provides an excellent solution.

Server Protection

Servers are typically accessed by many untrusted clients. For best protection of these valuable resources, you should have multiple lines of defense. With application firewall on your gateway, you can configure policies to protect your servers. For example, you can create a policy that blocks all FTP **put** commands to prevent anyone from writing a file to a server (see "Blocking FTP Commands" on page 35). Even though the server itself may be configured as read-only, this adds a layer of security that is controlled by the firewall administrator. Your server will still be protected even if its configuration is changed by an error, a side-effect of a patch, or by someone with malicious intent. With application firewall, you can effectively control content upload for servers using HTTP, SMTP, POP3, and FTP.

Figure 14 Server Protection from Content Upload



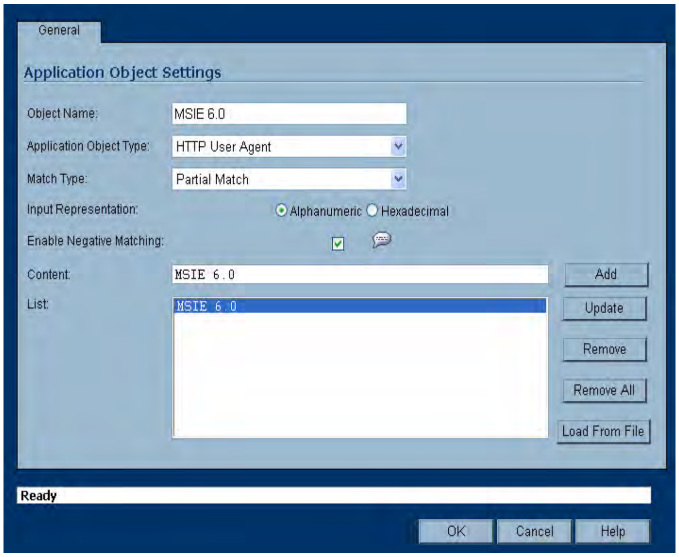
An example of policies that affect servers might be a small ISP providing three levels of service to its customers, whose servers are sitting in its rack. At the gold level, a customer can host a Web server, Email server, and FTP server. At the silver level, a customer can host only a Web server and Email server. At the bronze level, the hosting package only allows a Web server. The ISP could use application firewall to enforce these restrictions, by creating a policy for each customer.

Web Browser Control

You can also use application firewall to protect your Web servers from undesirable browsers. Application firewall supplies application object types for Netscape, MSIE, and Firefox. You can define an application object using one of these types, and reference it in a policy to block that browser.

You can also access browser version information by using an HTTP User Agent application object type. For example, older versions of various browsers can be susceptible to security problems. Using application firewall, you can create a policy that denies access by any problematic browser, such as Internet Explorer 5.0. You can also use negative matching to exclude all browsers except the one(s) you want. For example, you might want to allow Internet Explorer version 6 only, due to flaws in version 5, and because you haven't tested version 7. To do this, you would use a network protocol analyzer such as Wireshark to determine the Web browser identifier for IEv6, which is "MSIE 6.0". Then you could create an application object of type HTTP User Agent, with content "MSIE 6.0" and enable negative matching. See Figure 15.

Figure 15 MSIE 6.0 Application Object



Application Object Settings

Object Name: MSIE 6.0

Application Object Type: HTTP User Agent

Match Type: Partial Match

Input Representation: ● Alphanumeric ○ Hexadecimal

Enable Negative Matching: ☑

Content: MSIE 6.0

List: MSIE 6.0

Ready

You can use this application object in a policy to block browsers that are not MSIE 6.0. For information about using Wireshark to find a Web browser identifier, see "Wireshark" on page 41. For information about negative matching, see "Negative Matching" on page 10.

Another example of a use case for controlling Web browser access is a small e-commerce site that is selling discounted goods that are salvaged from an overseas source. If the terms of their agreement with the supplier is that they cannot sell to citizens of the source nation, they could configure application firewall to block access by the in-country versions of the major Web browsers.

Application firewall supports a pre-defined selection of well-known browsers, and you can add others as custom application objects. Browser blocking is based on the HTTP User Agent reported by the browser. Your custom application object must contain content specific enough to identify the browser without creating false positives. You can use Wireshark or another network protocol analyzer to obtain a unique signature for the desired browser.

Email Control

Application firewall can be very effective for certain types of email control, especially when a blanket policy is desired. For example, you can prevent sending attachments of a given type, such as *.exe,* on a per-user basis, or for an entire domain. Note that you can also do this on your email server if you have one. If not, then application firewall provides the functionality.

You can create an application object that scans for file content matching strings such as “confidential”, “internal use only” and “proprietary” to implement basic controls over the transfer of proprietary data.

You can also create a policy that prevents email to or from a specific domain or a specific user. You can use application firewall to limit email file size, but not to limit the number of attachments. Application firewall can block files based on MIME type. It cannot block encrypted SSL or TLS traffic.

Application firewall can scan email attachments that are text-based or are compressed, but not encrypted. Table 6 lists file formats that application firewall can scan for keywords. Other formats should be tested before you use them in a policy.

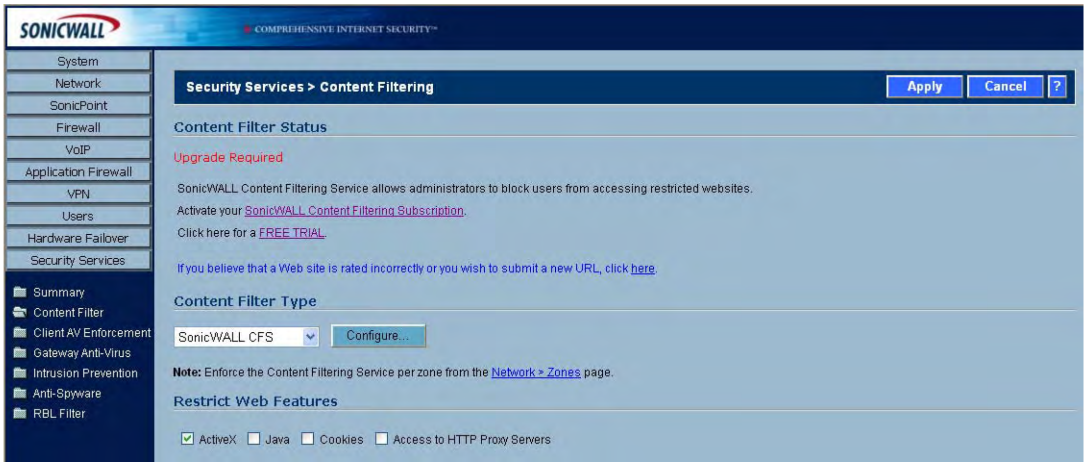
Table 6 Supported File Formats

File Type	Common Extension
C source code	c
C+ source code	cpp
Comma-separated values	csv
HQX archives	hqx
HTML	htm
Lotus 1-2-3	wks
Microsoft Access	mdb
Microsoft Excel	xls
Microsoft PowerPoint	ppt
Microsoft Visio	vsd
Microsoft Visual Basic	vbp
Microsoft Word	doc
Microsoft Works	wps
Portable Document Format	pdf
Rich Text Format	rft
SIT archives	sit
Text files	txt
WordPerfect	wpd
XML	xml
ZIP archives	zip

ActiveX Control

One of the most useful capabilities of application firewall is the ability to distinguish between different types of ActiveX or Flash network traffic. This allows you to block games while permitting Windows updates. Prior to application firewall, you could configure SonicOS to block ActiveX with Security Services > Content Filter, but this blocked all ActiveX controls, including your software updates. See Figure 16.

Figure 16 Security Services > Content Filter



Content Filter Status

Upgrade Required

SonicWALL Content Filtering Service allows administrators to block users from accessing restricted websites.
Activate your SonicWALL Content Filtering Subscription.
Click here for a FREE TRIAL.

If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click here.

Content Filter Type

SonicWALL CFS

Note: Enforce the Content Filtering Service per zone from the Network > Zones page.

Restrict Web Features

☑ ActiveX ☐ Java ☐ Cookies ☐ Access to HTTP Proxy Servers

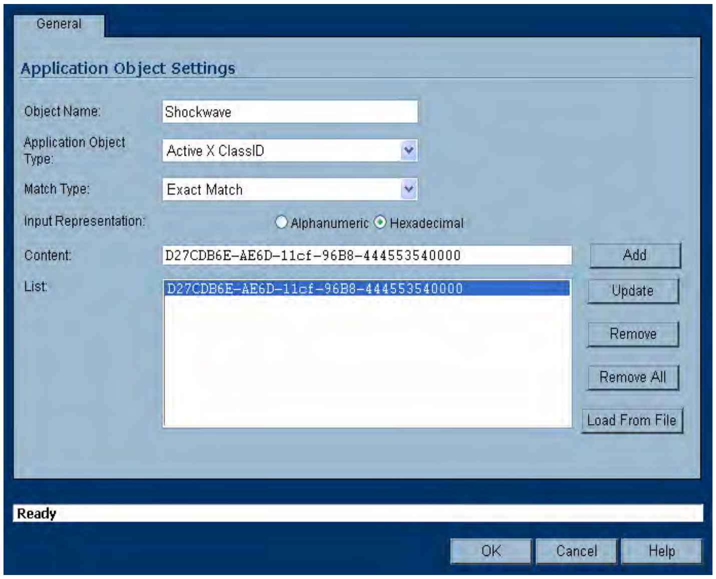
Application firewall achieves this distinction by scanning for the value of *classid* in the HTML source. Each type of ActiveX has its own class ID, and the class ID can change for different versions of the same application. Some ActiveX types and their classid's are shown in Table 7.

Table 7 ActiveX Class IDs

ActiveX Type	Classid
Apple Quicktime	02BF25D5-8C17-4B23-BC80-D3488ABDDC6B
Macromedia Flash v6, v7	D27CDB6E-AE6D-11cf-96B8-444553540000
Macromedia Shockwave	D27CDB6E-AE6D-11cf-96B8-444553540000
Microsoft Windows Media Player v6.4	22d6f312-b0f6-11d0-94ab-0080c74c7e95
Microsoft Windows Media Player v7-10	6BF52A52-394A-11d3-B153-00C04F79FAA6
Real Networks Real Player	CFCDAA03-8BE4-11cf-B84B-0020AFBBCCFA
Sun Java Web Start	5852F5ED-8BF4-11D4-A245-0080C6F74284

Figure 17 shows an ActiveX type application object that is using the Macromedia Shockwave class ID. You can create a policy that uses this application object to block online games or other Shockwave-based content.

Figure 17 *ActiveX Application Object*



Application Object Settings

Object Name: Shockwave

Application Object Type: Active X ClassID

Match Type: Exact Match

Input Representation: ○ Alphanumeric ● Hexadecimal

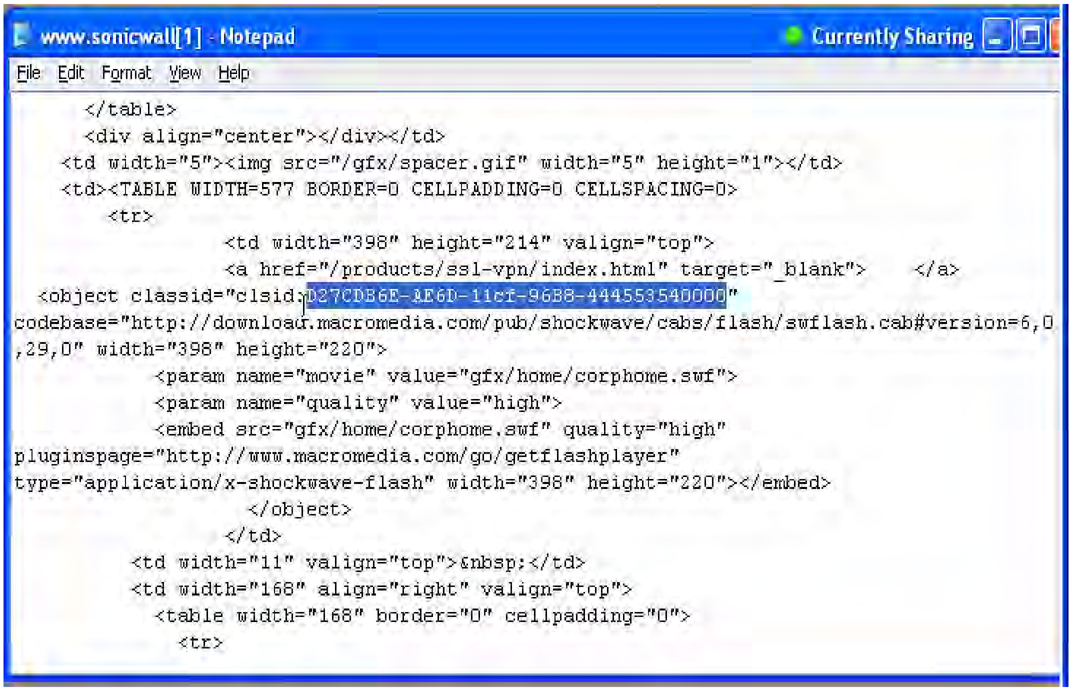
Content: D27CDB6E-AE6D-11cf-96B8-444553540000

List: D27CDB6E-AE6D-11cf-96B8-444553540000

Ready

You can look up the class ID for these Active X controls on the Internet, or you can view the source in your browser to find it. For example, Figure 18 shows a source file with the class ID for Macromedia Shockwave or Flash.

Figure 18 *Shockwave/Flash Class ID*



```
      </table>
      <div align="center"></div></td>
    <td width="5"><img src="/gfx/spacer.gif" width="5" height="1"></td>
    <td><TABLE WIDTH=577 BORDER=0 CELLPADDING=0 CELLSPACING=0>
        <tr>
                  <td width="398" height="214" valign="top">
                  <a href="/products/ssl-vpn/index.html" target="_blank">    </a>
  <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0
,29,0" width="398" height="220">
            <param name="movie" value="gfx/home/corphome.swf">
            <param name="quality" value="high">
            <embed src="gfx/home/corphome.swf" quality="high"
pluginspage="http://www.macromedia.com/go/getflashplayer"
type="application/x-shockwave-flash" width="398" height="220"></embed>
                    </object>
                  </td>
          <td width="11" valign="top">&nbsp;</td>
          <td width="168" align="right" valign="top">
            <table width="168" border="0" cellpadding="0">
              <tr>
```

FTP Control

Application firewall provides control over the FTP control channel, data channel, uploads, and downloads with four available application object types. Using these, you can regulate FTP usage very effectively. The following two use cases are described in this section:

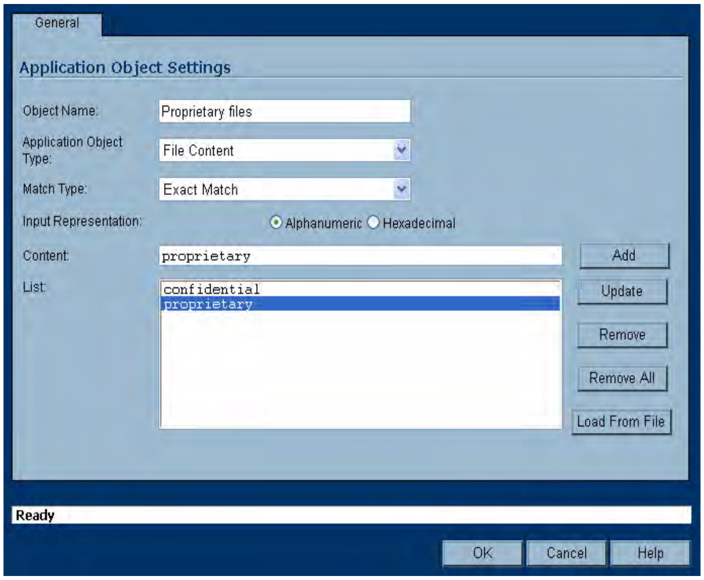
- "Blocking Outbound Proprietary Files Over FTP" on page 34
- "Blocking FTP Commands" on page 35

Blocking Outbound Proprietary Files Over FTP

For example, to block outbound file transfers of proprietary files over FTP, you can create a policy based on keywords or patterns inside the files.

First, you would create an application object that matches on keywords in files. See Figure 19.

Figure 19 Keywords in File Content



Application Object Settings

Object Name: Proprietary files

Application Object Type: File Content

Match Type: Exact Match

Input Representation: ● Alphanumeric ○ Hexadecimal

Content: proprietary

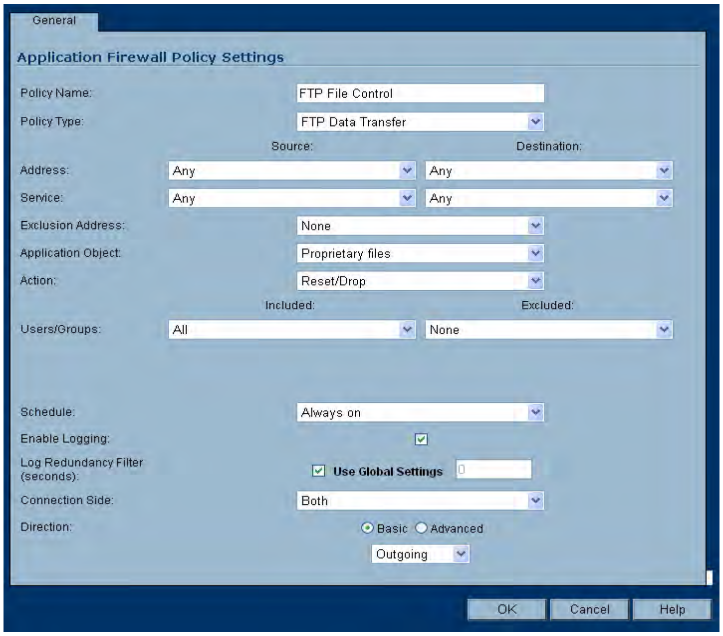
List:
confidential
proprietary

Ready

Optionally, you can create a customized FTP notification action that sends a message to the client.

Next, you would create a policy that references this application object and action. If you prefer to simply block the file transfer and reset the connection, you can select the Reset/Drop action when you create the policy. See Figure 20.

Figure 20 FTP File Control Policy



Application Firewall Policy Settings

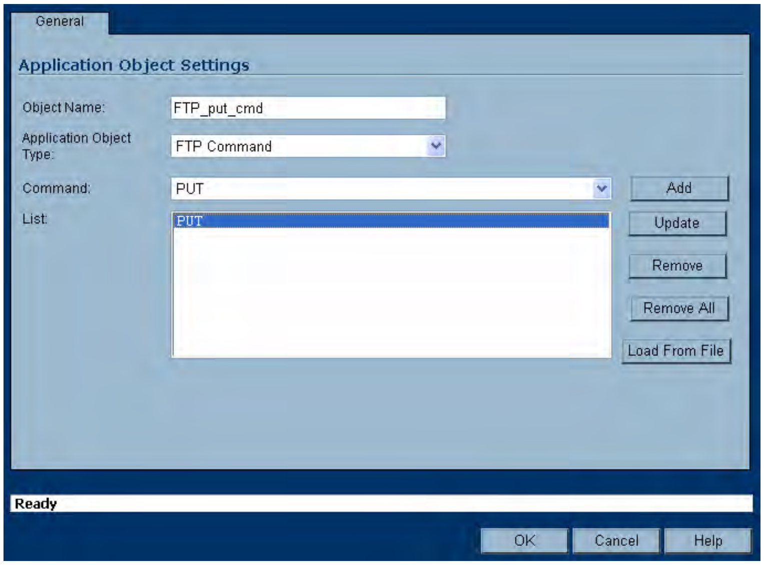
Policy Name: FTP File Control
Policy Type: FTP Data Transfer
Source: / Destination:
Address: Any / Any
Service: Any / Any
Exclusion Address: None
Application Object: Proprietary files
Action: Reset/Drop
Included: / Excluded:
Users/Groups: All / None
Schedule: Always on
Enable Logging: ☑
Log Redundancy Filter (seconds): ☑ Use Global Settings 0
Connection Side: Both
Direction: ● Basic ○ Advanced
Outgoing

Blocking FTP Commands

You can use application firewall to ensure that your FTP server is read-only by blocking **put** and **mput** FTP commands.

The first step is to create an application object that matches on the **put** command. Because the **mput** command is a variation of the **put** command, an application object that matches on the **put** command will also match on the **mput** command. See Figure 21.

Figure 21 FTP put Command

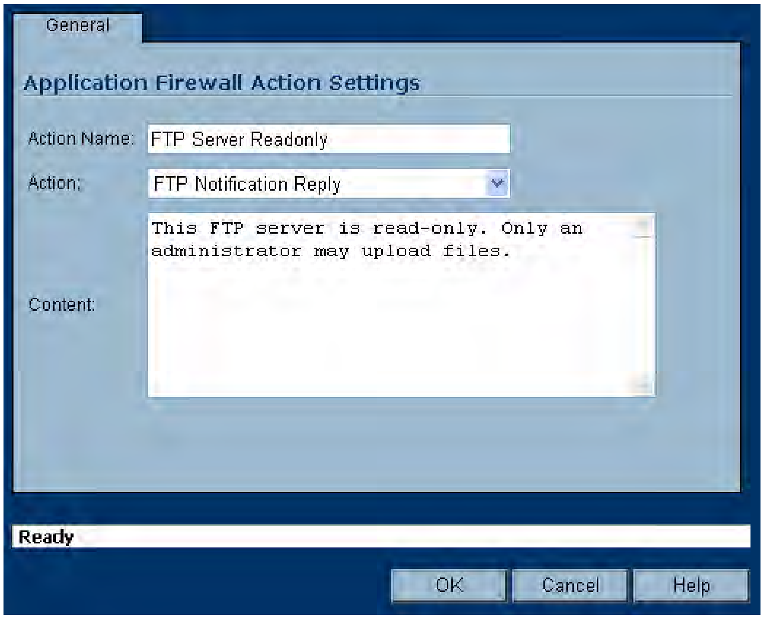


Application Object Settings

Object Name: FTP_put_cmd
Application Object Type: FTP Command
Command: PUT
List: PUT
Ready

Optionally, you can create a customized FTP notification action that sends a message to the client. A customized action is shown in Figure 22.

Figure 22 Customized FTP Notification



Application Firewall Action Settings

Action Name: FTP Server Readonly

Action: FTP Notification Reply

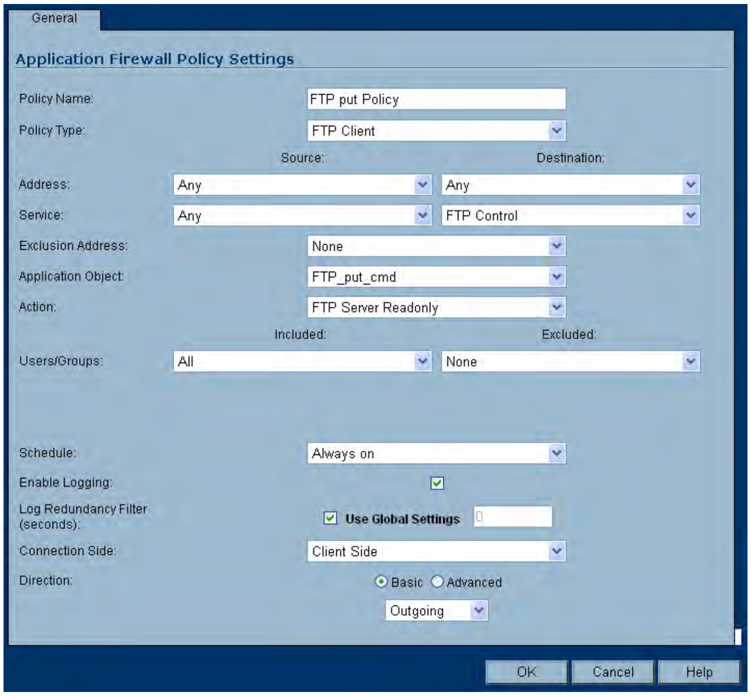
Content:

```
This FTP server is read-only. Only an
administrator may upload files.
```

Ready

Next, you would create a policy that references this application object and action. If you prefer to simply block the **put** command and reset the connection, you can select the Reset/Drop action when you create the policy. See Figure 23.

Figure 23 FTP Put Policy



Application Firewall Policy Settings

Policy Name:	FTP put Policy	
Policy Type:	FTP Client	
	Source:	Destination:
Address:	Any	Any
Service:	Any	FTP Control
Exclusion Address:	None	
Application Object:	FTP_put_cmd	
Action:	FTP Server Readonly	
	Included:	Excluded:
Users/Groups:	All	None
Schedule:	Always on	
Enable Logging:	☑	
Log Redundancy Filter (seconds):	☑ Use Global Settings 0	
Connection Side:	Client Side	
Direction:	● Basic ○ Advanced Outgoing	

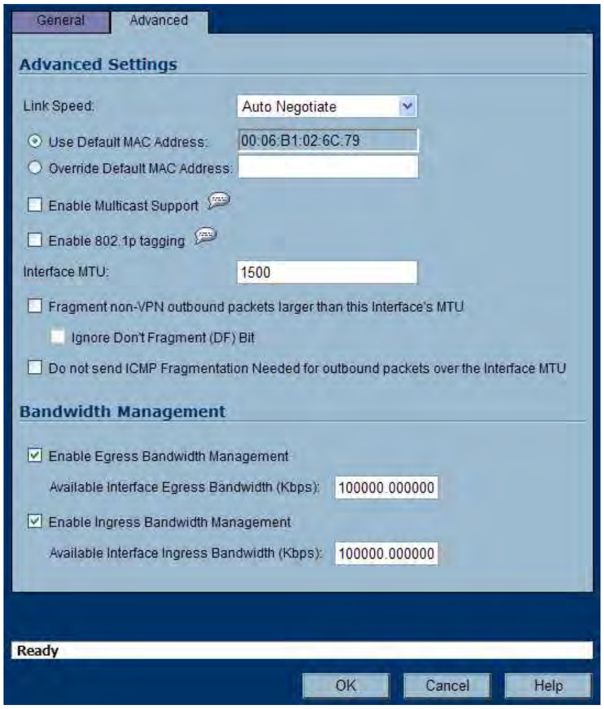
Bandwidth Management

You can use application layer bandwidth management to control the amount of network bandwidth that can be used to transfer certain file types. This allows you to discourage non-productive traffic and encourage productive traffic on your network.

For example, you can limit the bandwidth used to download MP3 files over FTP to no more than 400 kilobits per second (kbps).

The first step is to enable bandwidth management on the interface that will handle the traffic. You can access this setting on the Network > Interfaces screen of the SonicOS management interface. For complete instructions, see "Configuring Application Layer Bandwidth Management" on page 23.

Figure 24 Enabling Bandwidth Management on an Interface



Advanced Settings

Link Speed: Auto Negotiate

● Use Default MAC Address: 00:06:B1:02:6C:79

○ Override Default MAC Address:

☐ Enable Multicast Support

☐ Enable 802.1p tagging

Interface MTU: 1500

☐ Fragment non-VPN outbound packets larger than this Interface's MTU

☐ Ignore Don't Fragment (DF) Bit

☐ Do not send ICMP Fragmentation Needed for outbound packets over the Interface MTU

Bandwidth Management

☑ Enable Egress Bandwidth Management

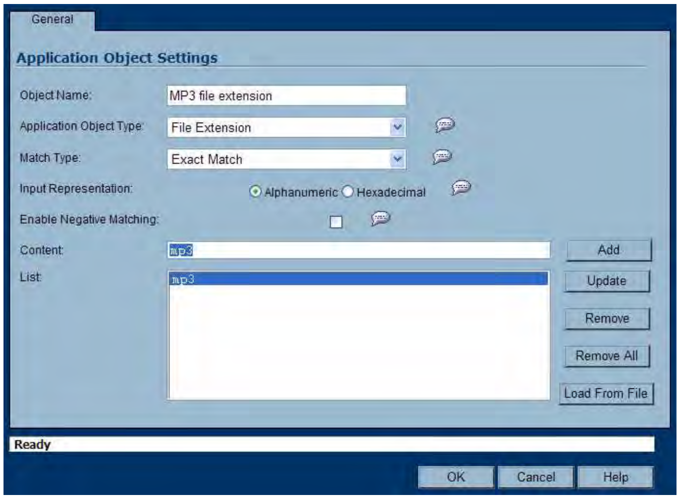
Available Interface Egress Bandwidth (Kbps): 100000.000000

☑ Enable Ingress Bandwidth Management

Available Interface Ingress Bandwidth (Kbps): 100000.000000

Next, define an application object for the MP3 file extension.

Figure 25 MP3 File Extension Application Object



Application Object Settings

Object Name: MP3 file extension

Application Object Type: File Extension

Match Type: Exact Match

Input Representation: ● Alphanumeric ○ Hexadecimal

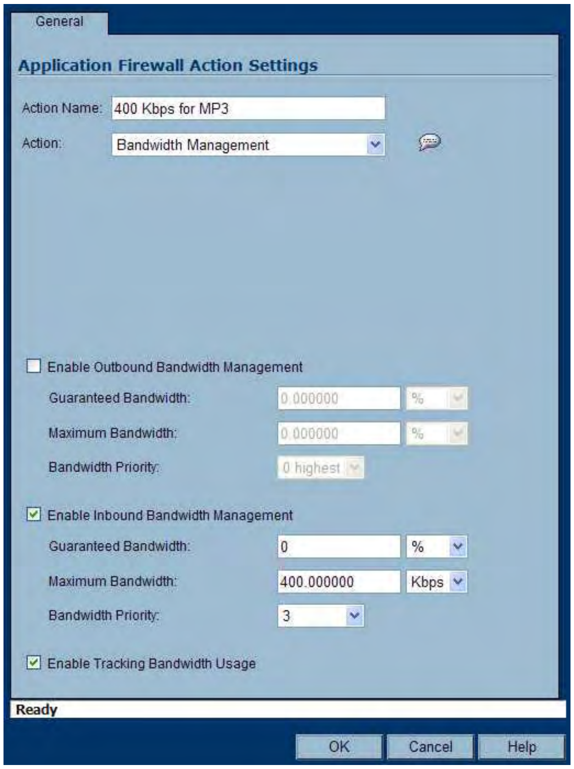
Enable Negative Matching: ☐

Content: mp3

List: mp3

Next, you can create an application layer bandwidth management action that limits inbound transfers to 400 kbps.

Figure 26 Application Layer Bandwidth Management Action



Application Firewall Action Settings

Action Name: 400 Kbps for MP3

Action: Bandwidth Management

□ Enable Outbound Bandwidth Management

Guaranteed Bandwidth: 0.000000 %

Maximum Bandwidth: 0.000000 %

Bandwidth Priority: 0 highest

☑ Enable Inbound Bandwidth Management

Guaranteed Bandwidth: 0 %

Maximum Bandwidth: 400.000000 Kbps

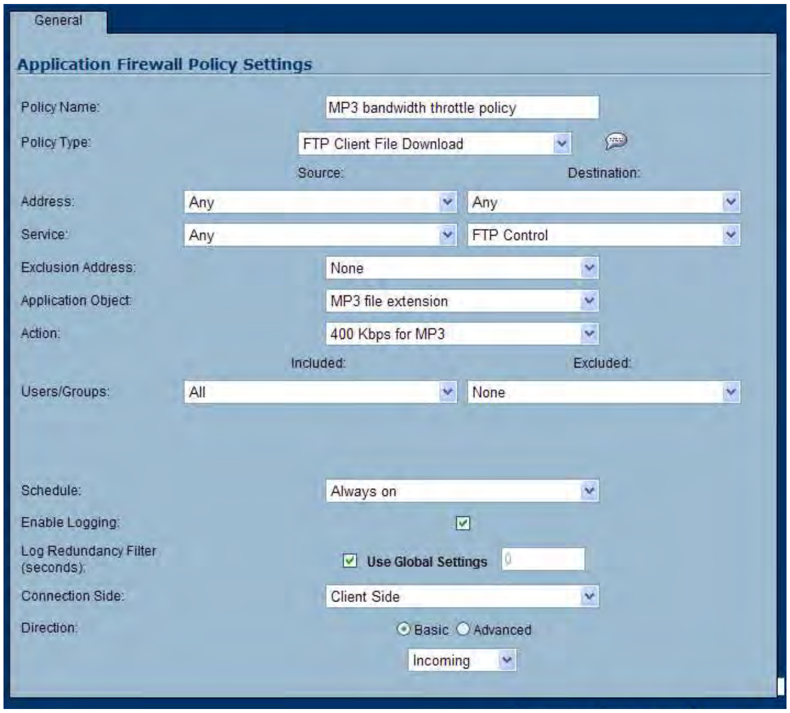
Bandwidth Priority: 3

☑ Enable Tracking Bandwidth Usage

Ready

Now you are ready to create a policy that applies the bandwidth management action to the MP3 file extension object.

Figure 27 MP3 Bandwidth Management Policy



Application Firewall Policy Settings

Policy Name: MP3 bandwidth throttle policy

Policy Type: FTP Client File Download

	Source:	Destination:
Address:	Any	Any
Service:	Any	FTP Control

Exclusion Address: None

Application Object: MP3 file extension

Action: 400 Kbps for MP3

	Included:	Excluded:
Users/Groups:	All	None

Schedule: Always on

Enable Logging: ☑

Log Redundancy Filter (seconds): ☑ Use Global Settings 0

Connection Side: Client Side

Direction: ● Basic ○ Advanced

Incoming

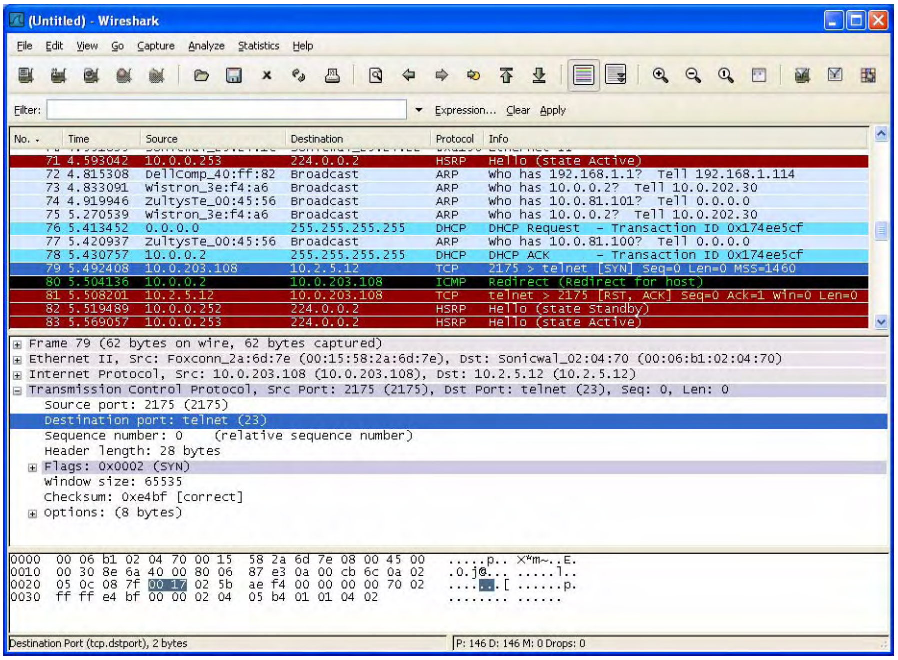
Custom Signature

You can create a custom application object that matches any part of a packet if you want to control traffic that does not have a predefined object type in application firewall. This allows you to create a custom signature for any network protocol.

For instance, you can create a custom signature to match a **telnet** packet. You might use this if you want to prevent the use of **telnet** on a server or in part of your network.

To determine a unique identifier for a **telnet** packet, you can use the Wireshark network protocol analyzer to view the packet header. For more information about using Wireshark, see "Wireshark" on page 41. In Wireshark, capture some packets that include the traffic you are interested in. In this case, you want to capture a **telnet** SYN packet. You can use **putty** to generate the **telnet** packet. Figure 28 shows a **telnet** SYN packet displayed by Wireshark.

Figure 28 Telnet Packet in Wireshark



```
No. -  Time      Source               Destination      Protocol  Info
  71 4.593042  10.0.0.253           224.0.0.2         HSRP      Hello (state Active)
  72 4.815308  DellComp_40:ff:82    Broadcast         ARP       Who has 192.168.1.1?  Tell 192.168.1.114
  73 4.833091  Wistron_3e:f4:a6     Broadcast         ARP       Who has 10.0.0.2?  Tell 10.0.202.30
  74 4.919946  ZultysTe_00:45:56    Broadcast         ARP       Who has 10.0.81.101?  Tell 0.0.0.0
  75 5.270539  Wistron_3e:f4:a6     Broadcast         ARP       Who has 10.0.0.2?  Tell 10.0.202.30
  76 5.413452  0.0.0.0              255.255.255.255   DHCP      DHCP Request  - Transaction ID 0x174ee5cf
  77 5.420937  ZultysTe_00:45:56    Broadcast         ARP       Who has 10.0.81.100?  Tell 0.0.0.0
  78 5.430757  10.0.0.2             255.255.255.255   DHCP      DHCP ACK      - Transaction ID 0x174ee5cf
  79 5.492408  10.0.203.108         10.2.5.12         TCP       2175 > telnet [SYN] Seq=0 Len=0 MSS=1460
  80 5.504136  10.0.0.2             10.0.203.108      ICMP      Redirect (Redirect for host)
  81 5.508201  10.2.5.12            10.0.203.108      TCP       telnet > 2175 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
  82 5.519489  10.0.0.252           224.0.0.2         HSRP      Hello (state Standby)
  83 5.569057  10.0.0.253           224.0.0.2         HSRP      Hello (state Active)
```

```
⊞ Frame 79 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: Foxconn_2a:6d:7e (00:15:58:2a:6d:7e), Dst: Sonicwal_02:04:70 (00:06:b1:02:04:70)
⊞ Internet Protocol, Src: 10.0.203.108 (10.0.203.108), Dst: 10.2.5.12 (10.2.5.12)
⊟ Transmission Control Protocol, Src Port: 2175 (2175), Dst Port: telnet (23), Seq: 0, Len: 0
    Source port: 2175 (2175)
    Destination port: telnet (23)
    Sequence number: 0    (relative sequence number)
    Header length: 28 bytes
  ⊞ Flags: 0x0002 (SYN)
    Window size: 65535
    Checksum: 0xe4bf [correct]
  ⊞ Options: (8 bytes)
```

```
0000  00 06 b1 02 04 70 00 15  58 2a 6d 7e 08 00 45 00   .....p.. X*m~..E.
0010  00 30 8e 6a 40 00 80 06  87 e3 0a 00 cb 6c 0a 02   .0.j@... .....l..
0020  05 0c 08 7f 00 17 02 5b  ae f4 00 00 00 00 70 02   .......[ ......p.
0030  ff ff e4 bf 00 00 02 04  05 b4 01 01 04 02         ........ ......
```

Destination Port (tcp.dstport), 2 bytes | P: 146 D: 146 M: 0 Drops: 0

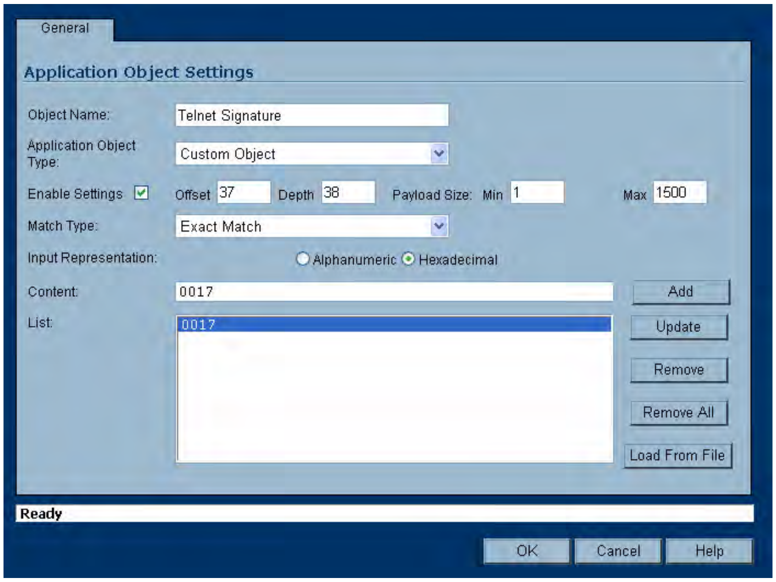
In the top pane of Wireshark, scroll down to find the **telnet** SYN packet, and click on that line. The packet is displayed in the two lower panes. For a SYN packet, the center pane provides a human-readable interpretation of the packet header, and the actual header bytes are displayed in hexadecimal in the lower pane.

In the center pane, expand the Transmission Control Protocol section, and locate the entry that identifies this packet as a **telnet** packet. In this case, the identifier is the port used by **telnet** packets, **Destination port: telnet (23)**. Click on this to highlight the corresponding bytes in the lower pane.

You can determine the offset and the depth of the highlighted bytes in the lower pane. Offset and depth are terms used by application firewall. Offset indicates which byte in the packet to start matching against, and depth indicates the last byte to match. When you calculate offset and depth, note that the first byte in the packet is counted as number one (not zero). In this case, the offset is 37 (in decimal) and the depth is 38.

Now you can create a custom application object that uses this information. See Figure 29.

Figure 29 Telnet Signature Application Object Settings



Application Object Settings

Object Name: Telnet Signature

Application Object Type: Custom Object

Enable Settings ☑ Offset 37 Depth 38 Payload Size: Min 1 Max 1500

Match Type: Exact Match

Input Representation: ○ Alphanumeric ● Hexadecimal

Content: 0017

List: 0017

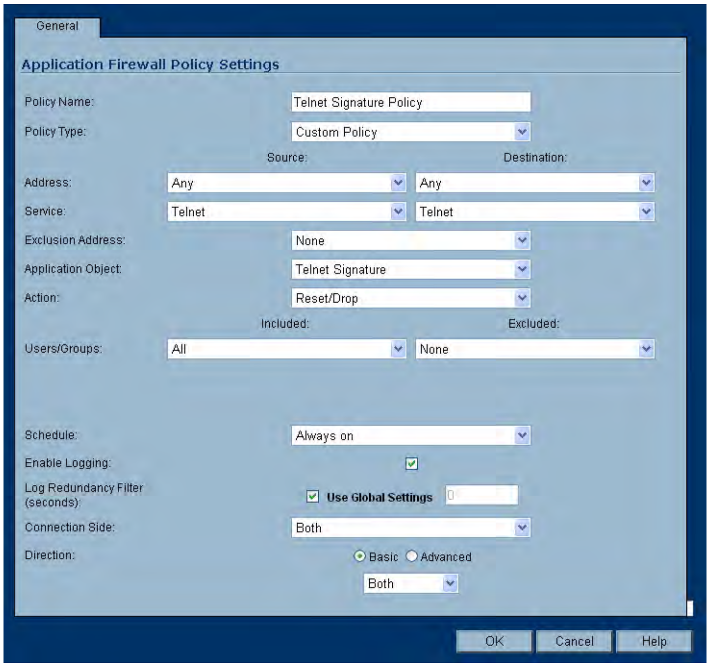
Ready

In the Application Object Settings dialog box, type a descriptive name for the object and then select Custom Object from the Type drop-down list. Check the Enable Settings check box. In the Offset text box, type **37** (the starting byte of the identifier). In the Depth text box, type **38** (the last byte of the identifier). You can leave the Payload Size set to the default. The Payload Size is used to indicate the amount of data in the packet, but in this case we are only concerned with the packet header.

For Input Representation, click Hexadecimal. In the Content text box, type the bytes as shown by Wireshark: **0017**. Do not use spaces in hexadecimal content.

The next step is to use this application object in a policy. In the Application Firewall Policy Settings dialog box (Figure 30), type a descriptive policy name and select Custom Policy for the policy type. You can select Telnet from the Services drop-down list. In the Application Object drop-down list, select the application object that you just defined. For a Custom Policy, the available actions are Reset/Drop or No Action. You can also modify other settings. For more information about creating a policy, see "Configuring a Policy" on page 26.

Figure 30 Telnet Signature Policy



Application Firewall Policy Settings

	Source:	Destination:
Policy Name:	Telnet Signature Policy	
Policy Type:	Custom Policy	
Address:	Any	Any
Service:	Telnet	Telnet
Exclusion Address:	None	
Application Object:	Telnet Signature	
Action:	Reset/Drop	
	Included:	Excluded:
Users/Groups:	All	None
Schedule:	Always on	
Enable Logging:	☑	
Log Redundancy Filter (seconds):	☑ Use Global Settings 0	
Connection Side:	Both	
Direction:	● Basic ○ Advanced Both	

Useful Tools

This section describes two software tools that can help you use application firewall to the fullest extent. The following tools are described:

- "Wireshark" on page 41
- "Hex Editor" on page 44

Wireshark

Wireshark is a network protocol analyzer that you can use to capture packets from applications on your network. You can examine the packets to determine the unique identifier for an application, which you can use to create an application object for use in an application firewall policy.

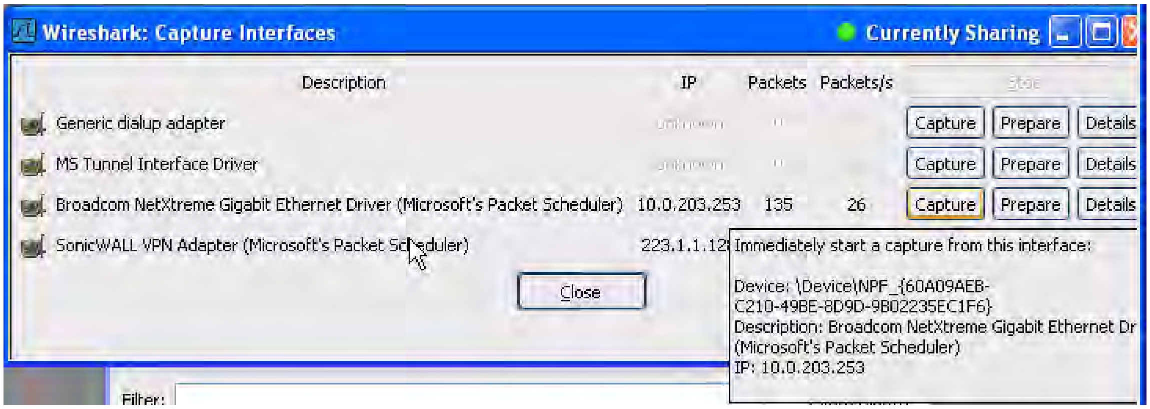
Wireshark is freely available at the following location:

http://www.wireshark.org/

The process of finding the unique identifier or signature of a Web browser is illustrated in the following packet capture sequence.

Step 1 In Wireshark, click **Capture > Interfaces** to view your local network interfaces.

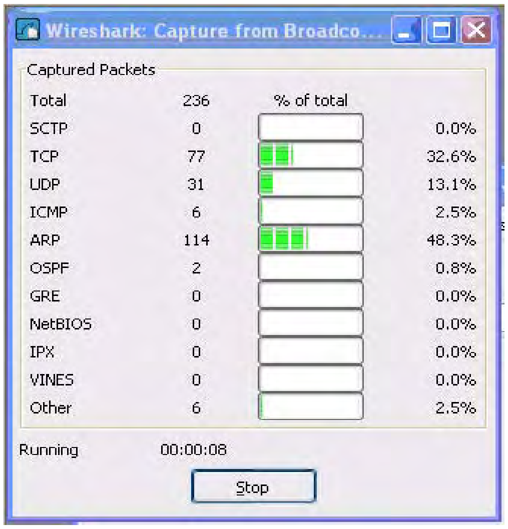
Step 2 In the Capture Interfaces dialog box, click **Capture** to start a capture on your main network interface:



Description	IP	Packets	Packets/s	Stop		
Generic dialup adapter	unknown	0		Capture	Prepare	Details
MS Tunnel Interface Driver	unknown	0		Capture	Prepare	Details
Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Packet Scheduler)	10.0.203.253	135	26	Capture	Prepare	Details
SonicWALL VPN Adapter (Microsoft's Packet Scheduler)	223.1.1.12					

Immediately start a capture from this interface:

Device: \Device\NPF_{60A09AEB-C210-49BE-8D9D-9B02235EC1F6}
Description: Broadcom NetXtreme Gigabit Ethernet Dr
(Microsoft's Packet Scheduler)
IP: 10.0.203.253



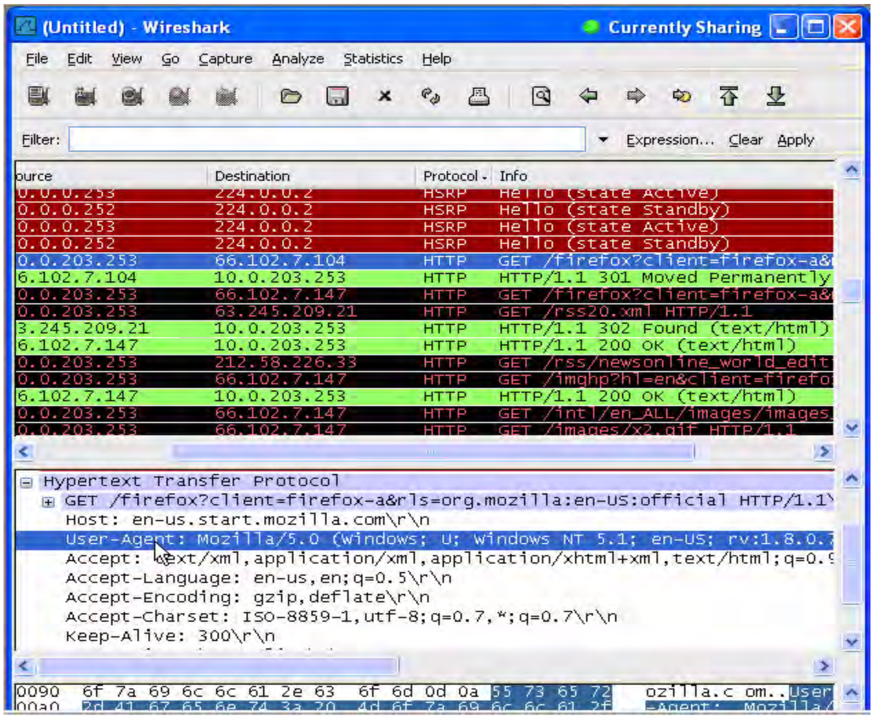
Captured Packets

Total	236	% of total	
SCTP	0		0.0%
TCP	77		32.6%
UDP	31		13.1%
ICMP	6		2.5%
ARP	114		48.3%
OSPF	2		0.8%
GRE	0		0.0%
NetBIOS	0		0.0%
IPX	0		0.0%
VINES	0		0.0%
Other	6		2.5%

Running 00:00:08

Step 3 As soon as the capture begins, start the browser and then stop the capture. In this example, Firefox is started.

Step 4 In the captured output, locate and click the **HTTP GET** command in the top pane, and view the source for it in the center pane. In the source code, locate the line beginning with **User-Agent**.

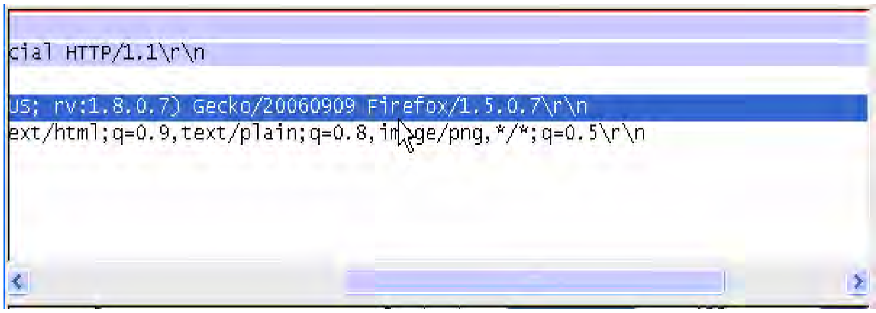

(Untitled) - Wireshark
Currently Sharing
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
ource          Destination     Protocol  Info
0.0.0.253      224.0.0.2       HSRP      Hello (state Active)
0.0.0.252      224.0.0.2       HSRP      Hello (state Standby)
0.0.0.253      224.0.0.2       HSRP      Hello (state Active)
0.0.0.252      224.0.0.2       HSRP      Hello (state Standby)
0.0.203.253    66.102.7.104    HTTP      GET /firefox?client=firefox-a&
6.102.7.104    10.0.203.253    HTTP      HTTP/1.1 301 Moved Permanently
0.0.203.253    66.102.7.147    HTTP      GET /firefox?client=firefox-a&
0.0.203.253    63.245.209.21   HTTP      GET /rss20.xml HTTP/1.1
3.245.209.21   10.0.203.253    HTTP      HTTP/1.1 302 Found (text/html)
6.102.7.147    10.0.203.253    HTTP      HTTP/1.1 200 OK (text/html)
0.0.203.253    212.58.226.33   HTTP      GET /rss/newsonline_world_edit
0.0.203.253    66.102.7.147    HTTP      GET /imghp?hl=en&client=firefo
6.102.7.147    10.0.203.253    HTTP      HTTP/1.1 200 OK (text/html)
0.0.203.253    66.102.7.147    HTTP      GET /intl/en_ALL/images/images
0.0.203.253    66.102.7.147    HTTP      GET /images/x2.gif HTTP/1.1
```

```
⊟ Hypertext Transfer Protocol
  ⊞ GET /firefox?client=firefox-a&rls=org.mozilla:en-US:official HTTP/1.1\
    Host: en-us.start.mozilla.com\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.0.7
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
```

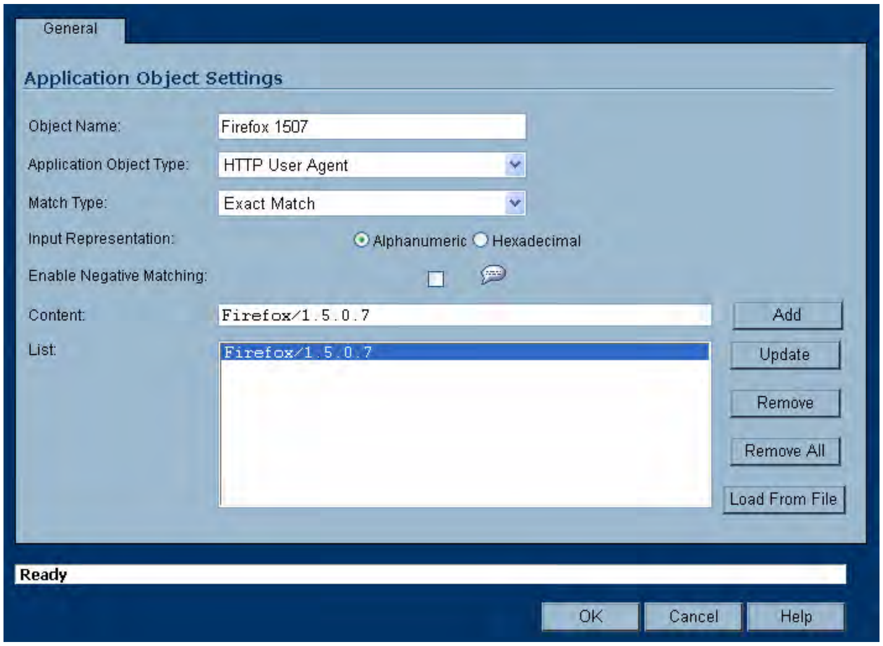
```
0090  6f 7a 69 6c 6c 61 2e 63  6f 6d 0d 0a 55 73 65 72   ozilla.c om..User
00a0  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
```

Step 5 Scroll to the right to find the unique identifier for the browser. In this case it is **Firefox/1.5.0.7**.



```
cial HTTP/1.1\r\n

US; rv:1.8.0.7) Gecko/20060909 Firefox/1.5.0.7\r\n
ext/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5\r\n
```

Step 6 Type the identifier into the Content text box in the Application Objects Settings screen and click **OK** to create an application object that you can use in a policy.



Application Object Settings

Object Name: Firefox 1507

Application Object Type: HTTP User Agent

Match Type: Exact Match

Input Representation: ● Alphanumeric ○ Hexadecimal

Enable Negative Matching: □

Content: Firefox/1.5.0.7

List: Firefox/1.5.0.7

Ready

Hex Editor

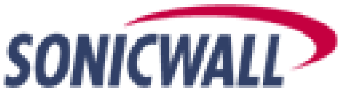
You can use a hexadecimal (hex) editor to view the hex representation of a file or a graphic image. One such hex editor is **XVI32**, developed by Christian Maas and available at no cost at the following URL:

http://www.chmaas.handshake.de/delphi/freeware/xvi32/xvi32.htm

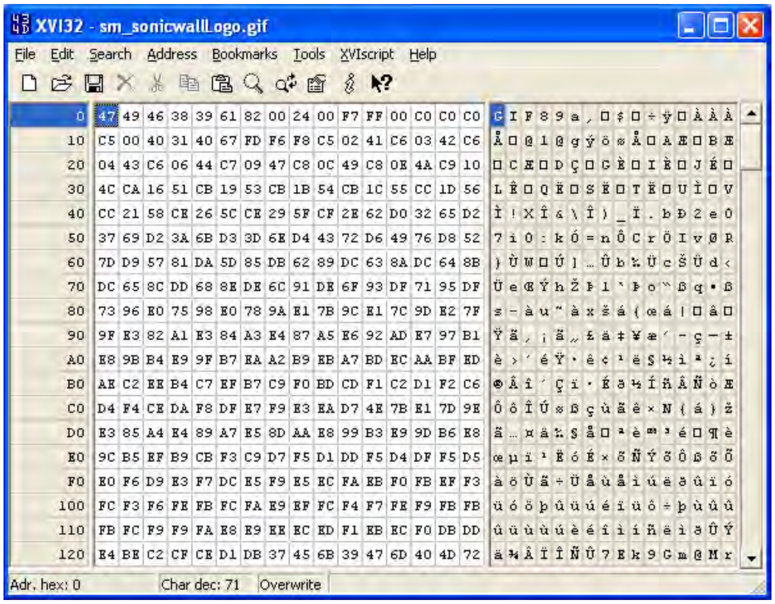
For example, if there is a certain graphic contained within all confidential company documents, you could use the hex editor to obtain a unique identifier for the graphic, and then use the identifying hex string to create an application object. You could reference the application object in a policy that blocks the transfer of files with content matching that graphic.

Using the SonicWALL graphic in Figure 31 as an example, you would take the following steps:

Figure 31 SonicWALL Graphic



Step 1 Start **XVI32** and click **File > Open** to open the graphic image GIF file.


XVI32 - sm_sonicwallLogo.gif
File Edit Search Address Bookmarks Tools XVIscript Help

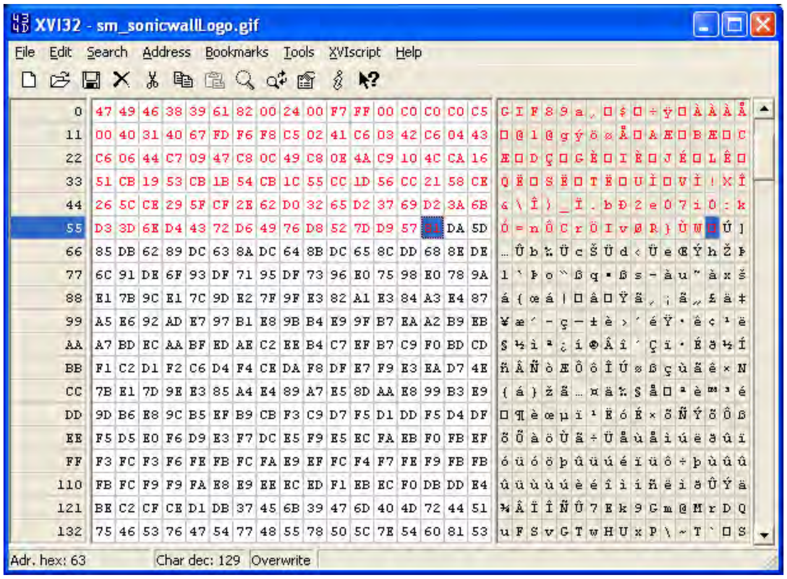
```
  0  47 49 46 38 39 61 82 00 24 00 F7 FF 00 C0 C0 C0
 10  C5 00 40 31 40 67 FD F6 F8 C5 02 41 C6 03 42 C6
 20  04 43 C6 06 44 C7 09 47 C8 0C 49 C8 0E 4A C9 10
 30  4C CA 16 51 CB 19 53 CB 1B 54 CB 1C 55 CC 1D 56
 40  CC 21 58 CE 26 5C CE 29 5F CF 2E 62 D0 32 65 D2
 50  37 69 D2 3A 6B D3 3D 6E D4 43 72 D6 49 76 D8 52
 60  7D D9 57 81 DA 5D 85 DB 62 89 DC 63 8A DC 64 8B
 70  DC 65 8C DD 68 8E DE 6C 91 DE 6F 93 DF 71 95 DF
 80  73 96 E0 75 98 E0 78 9A E1 7B 9C E1 7C 9D E2 7F
 90  9F E3 82 A1 E3 84 A3 E4 87 A5 E6 92 AD E7 97 B1
 A0  E8 9B B4 E9 9F B7 EA A2 B9 EB A7 BD EC AA BF ED
 B0  AE C2 EE B4 C7 EF B7 C9 F0 BD CD F1 C2 D1 F2 C6
 C0  D4 F4 CE DA F8 DF E7 F9 E3 EA D7 4E 7B E1 7D 9E
 D0  E3 85 A4 E4 89 A7 E5 8D AA E8 99 B3 E9 9D B6 E8
 E0  9C B5 EF B9 CB F3 C9 D7 F5 D1 DD F5 D4 DF F5 D5
 F0  E0 F6 D9 E3 F7 DC E5 F9 E5 EC FA EB F0 FB EF F3
100  FC F3 F6 FE FB FC FA E9 EF FC F4 F7 FE F9 FB FB
110  FB FC F9 F9 FA E8 E9 EE EC ED F1 EB EC F0 DB DD
120  E4 BE C2 CF CE D1 DB 37 45 6B 39 47 6D 40 4D 72

Adr. hex: 0        Char dec: 71    Overwrite
```

Step 2 In the left pane, mark the first 50 hex character block by using the following sequence:

- Click on the first character (#0).
- Press **Ctrl+B**.
- Click on the character in position #49.
- Press **Ctrl+B**.

To locate the character in position #49, click on a character in the right pane (the text pane) and then look at the bottom left corner for the decimal address. Try different characters until it shows **Adr. dec: 49**. Note that you must click on the corresponding location in the *left* pane before you press **Ctrl+B** to mark the block.

When the block is marked, it changes to red font. To unmark a block of characters, press **Ctrl+U**.


XVI32 - sm_sonicwallLogo.gif
File Edit Search Address Bookmarks Tools XVIscript Help

```
  0  47 49 46 38 39 61 82 00 24 00 F7 FF 00 C0 C0 C0 C5
 11  00 40 31 40 67 FD F6 F8 C5 02 41 C6 03 42 C6 04 43
 22  C6 06 44 C7 09 47 C8 0C 49 C8 0E 4A C9 10 4C CA 16
 33  51 CB 19 53 CB 1B 54 CB 1C 55 CC 1D 56 CC 21 58 CE
 44  26 5C CE 29 5F CF 2E 62 D0 32 65 D2 37 69 D2 3A 6B
 55  D3 3D 6E D4 43 72 D6 49 76 D8 52 7D D9 57 81 DA 5D
 66  85 DB 62 89 DC 63 8A DC 64 8B DC 65 8C DD 68 8E DE
 77  6C 91 DE 6F 93 DF 71 95 DF 73 96 E0 75 98 E0 78 9A
 88  E1 7B 9C E1 7C 9D E2 7F 9F E3 82 A1 E3 84 A3 E4 87
 99  A5 E6 92 AD E7 97 B1 E8 9B B4 E9 9F B7 EA A2 B9 EB
 AA  A7 BD EC AA BF ED AE C2 EE B4 C7 EF B7 C9 F0 BD CD
 BB  F1 C2 D1 F2 C6 D4 F4 CE DA F8 DF E7 F9 E3 EA D7 4E
 CC  7B E1 7D 9E E3 85 A4 E4 89 A7 E5 8D AA E8 99 B3 E9
 DD  9D B6 E8 9C B5 EF B9 CB F3 C9 D7 F5 D1 DD F5 D4 DF
 EE  F5 D5 E0 F6 D9 E3 F7 DC E5 F9 E5 EC FA EB F0 FB EF
 FF  F3 FC F3 F6 FE FB FC FA E9 EF FC F4 F7 FE F9 FB FB
110  FB FC F9 F9 FA E8 E9 EE EC ED F1 EB EC F0 DB DD E4
121  BE C2 CF CE D1 DB 37 45 6B 39 47 6D 40 4D 72 44 51
132  75 46 53 76 47 54 77 48 55 78 50 5C 7E 54 60 81 53

Adr. hex: 63       Char dec: 129   Overwrite
```

Step 3 After you mark the block, click **Edit > Clipboard > Copy As Hex String**.

Step 4 In Textpad or another text editor, press **Ctrl+V** to paste the selection and then press **Enter** to end the line.

This intermediary step is necessary to allow you to remove spaces from the hex string.

Step 5 In Textpad, click **Search > Replace** to bring up the Replace dialog box. In the Replace dialog box, type a space into the Find text box and leave the Replace text box empty. Click **Replace All**.

The hex string now has 50 hex characters with no spaces between them.

Step 6 Double-click the hex string to select it, then press **Ctrl+C** to copy it to the clipboard.

Step 7 In the SonicOS user interface, navigate to Application Firewall > Application Object and click **Add Application Object**.

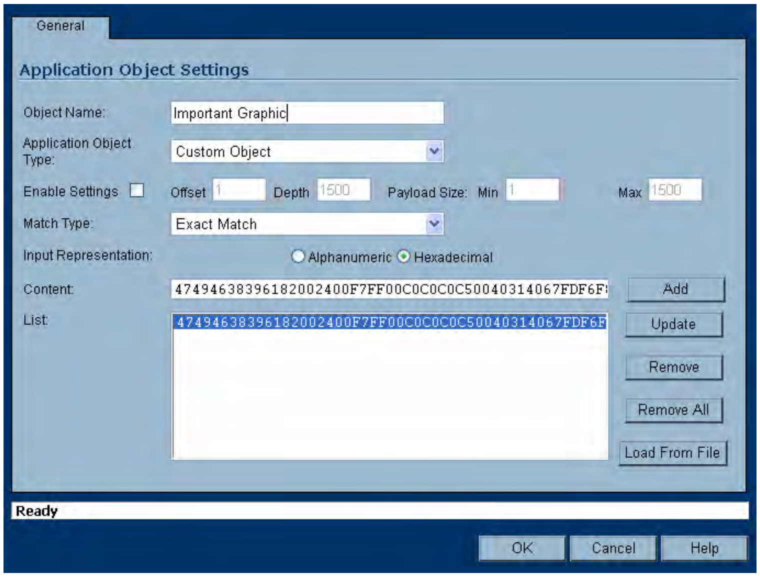
Step 8 In the Application Object Settings dialog box, type a descriptive name into the Object Name text box.

Step 9 In the Application Object Type drop-down list, select **Custom Object**.

Step 10 For Input Representation, click **Hexadecimal**.

Step 11 In the Content text box, press **Ctrl+V** to paste the contents of the clipboard.

Step 12 Click **Add**.



General

Application Object Settings

Object Name: Important Graphic

Application Object Type: Custom Object

Enable Settings □ Offset 1 Depth 1500 Payload Size: Min 1 Max 1500

Match Type: Exact Match

Input Representation: ○ Alphanumeric ● Hexadecimal

Content: 4749463839618200 2400F7FF00C0C0C0C50040314067FDF6F

List: 4749463839618200 2400F7FF00C0C0C0C50040314067FDF6F

Ready

Step 13 Click **OK**.

You now have an Application Object containing a unique identifier for the image. You can create a policy to block or log traffic that contains the image matched by this Application Object. For information about creating a policy, see "Configuring a Policy" on page 26.

Glossary

Application layer: The seventh level of the 7-layer OSI model; examples of application layer protocols are AIM, DNS, FTP, HTTP, IMAP, MSN Messenger, POP3, SMTP, SNMP, TELNET, and Yahoo Messenger

Client: Typically, the client (in a client-server architecture) is an application that runs on a personal computer or workstation, and relies on a server to perform some operations

Digital rights management: Technology used by publishers or copyright owners to control access to and usage of digital data

FTP: File Transfer Protocol, a protocol for exchanging files over the Internet

Gateway: A computer that serves as an entry point for a network; often acts as a firewall or a proxy server

Granular control: The ability to control separate components of a system

Hexadecimal: Refers to the base-16 number system

HTTP: Hyper Text Transfer Protocol, the underlying protocol used by the World Wide Web

HTTP redirection: Also known as URL redirection, a technique on the Web for making a Web page available under many URLs

IPS: Intrusion Prevention System

MIME: Multipurpose Internet Mail Extensions, a specification for formatting non-ASCII messages such as graphics, audio, or video, so that they can be sent over the Internet

POP3: Post Office Protocol, a protocol used to retrieve email from a mail server; can be used with or without SMTP

Proxy: A computer that operates a network service that allows clients to make indirect network connections to other network services

SMTP: Simple Mail Transfer Protocol, a protocol used for sending email messages between servers

UDP: User Datagram Protocol, a connectionless protocol that runs on top of IP networks