

SonicWall[®] Global Management System MANAGE Security Services

Administration

SONICWALL[®]

Contents

Settings	3
Security Services Settings	3
Client Content Filtering Settings	5
Content Filter	5
Websense Enterprise	8
N2H2	9
DPI-SSL Enforcement	10
Client Anti-Virus Enforcement	12
Anti-virus Settings	12
Force Update Settings	13
Exempt Computers	14
Client Anti-virus Enforcement	15
Client CF Enforcement	17
Client CF Enforcement Policies	18
Gateway Anti-Virus	20
Gateway Anti-virus Status	20
Gateway Anti-virus Settings	20
Protocols	21
Gateway Anti-virus Signatures	24
Anti-Spyware Service	25
Anti-spyware Status	25
Anti-spyware Global Settings	25
Signature Groups	26
Protocols	27
Anti-spyware Signatures	28
Intrusion Prevention Service	30
Overview of IPS	30
SonicWall Deep Packet Inspection	30
Enabling Intrusion Prevention Services	32
IPS Settings	32
IPS Policies	34
Geo-IP Filter	35
Custom List	36
Botnet Filter	40
Settings	40
Custom List	41

Web Block Page	42
Dynamic Botnet List Server	43
Dynamic Botnet List	44
SonicWall Support	45
About This Document	46

Settings

This feature allows SonicWall firewall appliances that operate in networks to access the Internet through a proxy server to download signatures. This feature also allows for registration of SonicWall firewall appliances through a proxy server to avoid compromising privacy.

The **Settings** page consists of two sections:

- **Security Service Settings** defines top-level settings for security.
 - **Signature Downloads Through a Proxy Server** allows access to the Internet to download signatures and register SonicWall appliances without compromising privacy.

SECURITY SERVICES SETTINGS

Security Services Setting Maximum Security (Recommended) ▼

Maximum Security (Recommended) Inspect all content with any threat probability (high/medium/low)
For additional performance capacity in this maximum security setting, utilize SonicOS DPI Clustering.

Performance Optimized Inspect all content with a high or medium threat probability.
Consider this performance optimized security setting for bandwidth/CPU intensive gateway deployments or utilize SonicOS DPI Clustering.

Reduce Anti-Virus traffic for ISDN connections

Drop all packets while IPS, GAV and Anti-Spyware database is reloading

HTTP Clientless Notification Timeout for GAV and AntiSpyware seconds ?

SIGNATURE DOWNLOADS THROUGH A PROXY SERVER

Download Signatures through a Proxy Server

Proxy Server Name or IP Address

Proxy Server Port

This Proxy Server requires Authentication

Username

Password ?

Update Reset

Security Services Settings

These top-level **Security Services Settings** allow a choice of operating for maximum security, or accepting less than the highest security level but with higher network performance levels.

These settings can be selected for the global network, a group, or a single SonicWall appliance.

- **Security Services Setting** — There are two choices of security levels:
 - **Maximum Security (Recommended)** — This setting results in the inspection of all traffic, regardless of the threat level.
 - **Performance Optimized** — This setting restricts inspection to traffic having a high or medium threat level. It speeds up throughput at the expense of the highest level of security

NOTE: SonicOS DPI clustering allows additional performance in the maximum security setting.

There are three other security settings at this level:

- **Reduce Anti-Virus traffic for ISDN connections** — With this setting enabled, SonicWall Anti-Virus checks for updates only once a day (every 24 hours), thereby reducing the frequency of outbound traffic for users who do not have an “always on” Internet connection.
- **Drop all packets while IPS, GAV and Anti-Spyware database is reloading** — Select this option to instruct the SonicWall security appliance to drop all packets whenever the IPS, GAV, and Anti-Spyware database is updating.
- **HTTP Clientless Notification Timeout for GAV and Anti-Spyware** — HTTP Clientless Notification notifies users when an incoming threat from an HTTP server is detected. Set the timeout duration, in seconds, after which the SonicWall security appliance notifies users when GAV or Anti-Spyware detects an incoming threat from an HTTP server. The default timeout is one day (86400 seconds), the minimum time is 10 seconds, and the maximum time is 2147483647 seconds. This defines the length of time the appliance waits for a confirmation notification from a client system.


Signature Downloads Through a Proxy Server

In the following section, you can configure **Signature Downloads Through a Proxy Server**. Setting up a proxy server is essential as a method for maintaining privacy for downloading threat signatures and appliance registration.

To enable signature download or appliance registration through a proxy server:

- 1 Select **Download Signatures through a Proxy Server**.
- 2 If this field is selected, the next two fields become available. In the **Proxy Server Name or IP Address** field, enter the hostname or IP address of the proxy server.
- 3 In the **Proxy Server Port** field, enter the port number used to connect to the proxy server.

Select **This Proxy Server requires Authentication** if the proxy server requires a **username** and **password**.

 **NOTE:** If you leave the password field empty, the current password value for this appliance remains unchanged.

- 4 Click **Update** or **Reset** to apply or discard the changes.

Client Content Filtering Settings

This section allows the administrator to configure client Content Filtering Service (CFS) settings in Global Management System (GMS). The default SonicWall Content Filtering Service policy is available without a CFS subscription. With a valid advanced CFS subscription, you can create custom CFS policies and apply them to network zones or to groups of users within your organization.

The main settings for the SonicWall CFS policy are configured on the **Firewall > Content Filter Policies** page. After you have configured a CFS policy, you can configure client CF settings, as shown in this section.

GMS offers client content filtering protection on a subscription-basis through a partnership with McAfee.

Topics:

- [Content Filter](#)
- [Websense Enterprise](#)
- [N2H2](#)

Content Filter

This section describes how to configure client Content Filtering Service settings for SonicWall appliances from the Content Filter screen. This screen applies only to units running SonicOS 6.2.6 Enhanced and newer. It has the following sections.

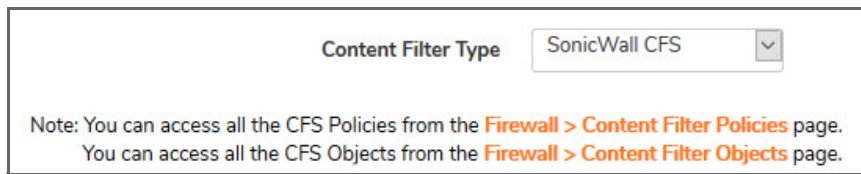
Topics:

- [Content Filter Status](#)
- [Global Settings](#)
- [Local CFS Server Settings](#)
- [CFS Exclusion](#)
- [CFS Custom Category Search](#)
- [CFS Custom Category](#)

Content Filter Status

Navigate to **Security Services > Content Filter**.

The first section of the **Content Filter** page indicates the filtering type and gives the link to the pages for finding SonicWall CFS objects and policies. Click on the **Content Filtering Type** drop-down menu for choices. Clicking each of the three choices brings up a different page:



- **SonicWall CFS** - SonicWall CFS is the standard content filtering service.
- **Websense Enterprise** - Websense Enterprise is an enhancement of the SonicWall Content Filtering Service. It allows organizations that have deployed a joint SonicWall and Websense Enterprise solution to enforce web access policies on HTTPS connections. Versions of SonicOS that predate 5.9.0.3 support enforcement of web access policies through Websense on HTTP connections only. In this mode, all HTTPS connections are passed without checking the policy. This option is explained in a later section.
- **N2H2** - This option is explained in a later section of this chapter.



Global Settings

Clicking SonicWall CFS brings up the information for defining **Global Settings** for CFS policies. Many of the fields on this page have an *i* (information) icon on the right, which gives more information about that field. In the **Global Settings** section, there are five fields where choices can be made:

GLOBAL SETTINGS

Max URL Cache Entries ⓘ

Note: Please enter a value within the supported range for the selected model(s). If unsure, click here for valid ranges.

Enable Content Filtering Service ⓘ

Enable HTTPS Content Filtering ⓘ

Block if CFS Server Is Unavailable ⓘ

Server Timeout second(s) ⓘ

- **Max URL Cache Entries** - The user can select the maximum number of URL entries that can be cached. The minimum is 25,600 and the maximum is 51,200. In the note beneath this field, there is a link on the word "here" that gives the supported range for the selected model.
- **Enable Content Filtering Service** - This setting defaults to **Enabled**.
- **Enable HTTPS Content Filtering** - This filtering is based on IP, and does not inspect the URL. While HTTP content filtering can perform redirects to enforce authentication or provide a block page, HTTPS filtered pages are silently blocked. This field defaults to disabled.
- **Block if CFS Server is Unavailable** - When this box is checked, if the CFS server is detected as unavailable, then all web access is blocked.

- **Server Timeout** — If the firewall does not get a response from the CFS server within this timeout value, the sever is marked as unavailable. The minimum is two seconds, the maximum is 10 seconds, and the default is five seconds. This setting is not available when **Block if CFS Server is Unavailable** is not checked.

Local CFS Server Settings

If you choose to use **LOCAL CFS SERVER SETTINGS** rather than one available to the public, use these settings.

The screenshot shows a configuration panel titled "LOCAL CFS SERVER SETTINGS". It contains the following elements:

- A checkbox labeled "Enable Local CFS Server" with an information icon to its right.
- A text input field labeled "Primary Local CFS Server".
- A text input field labeled "Secondary Local CFS Server".

- **Enable Local CPS Server** - Check this box for the local CFS server. This setting defaults to disabled.
- **Primary and Secondary Local CFS Servers** - These fields hold IP addresses for local CFS servers to be selected from. They become available when **Enable Local CFS Server is checked**.

CFS Exclusion

In this section, **CFS EXCLUSIONS** can be configured to allow packets from the administrator and a number of address objects to pass through unfiltered.

The screenshot shows a configuration panel titled "CFS EXCLUSION". It contains the following elements:

- A checkbox labeled "Exclude Administrator" with an information icon to its right.
- A dropdown menu labeled "Excluded Address" with the text "-- Select an Address object --" and an information icon to its right.

- **Exclude Administrator** - All the packets from the administrator pass through the CFS module if this box is checked. It defaults to enabled.
- **Excluded Address** - Select addresses from the drop-down menu, as desired. The packets of all selected addresses pass through the CFS module.

CFS Custom Category Search

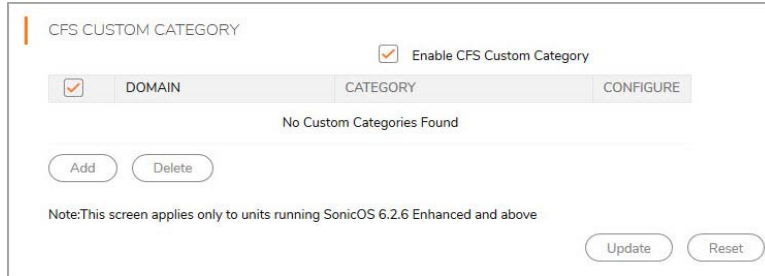
In this section the user can see a list of custom categories available on the system. Click **Search** to begin your search. All current CFS policies are listed at **Firewall > Content Filter Policies**.

The screenshot shows a configuration panel titled "CFS CUSTOM CATEGORY SEARCH". It contains the following elements:

- A search icon (magnifying glass) followed by a dropdown menu set to "Domain".
- A second dropdown menu set to "Equals".
- A text input field with the placeholder text "Enter Search text".
- A "Search" button.
- A "Clear" button.

CFS Custom Category

This section allows the configuration of new custom CFS category entries. The administrator can create custom policies and categories, and insert the domain name entries into the existing, flexible CFS rating category structure. Categories are added and deleted on the page that follows:



Click **Add** to bring up a dialog box where you can choose from a list of categories to add to the CFS categories in your system. Choose the Domain name and the categories, then click **OK** to add them. Click **Update** on the **Content Filter** page to save your changes. If changes have been made, clicking **Update** opens a dialog box to select a schedule for the application and persistence of your changes. The dialog box from which to choose the categories to add follows:



Websense Enterprise

This option on the Content Filter Type field brings up a Content Filter screen for configuring Websense Enterprise settings. Note that this section applies only to units running Sonic OS 6.2.6 Enhanced and newer. Be

sure to click **Update** to apply your changes. More information is available next to certain selections by clicking the *i* (information) icon. This page has the following sections:

Topics:

- [General Settings](#)
- [Block Web Features](#)
- [CFS Exclusion](#)
- [Blocking Page](#)

General Settings

General Settings is the top section, where basic information about the Websense Server can be set. Click the *i* icon to bring up the screen tips that guide the user in making the choices for these fields. When **Enable Websense Probe Monitoring** is clicked, options appear for controlling the probing operation.

Block Web Features

This section sets the blocking system for features and domains, as selected by the user.

CFS Exclusion

This section allows the user to exclude the administrator and any chosen addresses from **Client CFS Enforcement**. Clicking the drop-down menu brings up a list of addresses whose packets the administrator might want to allow to pass through the CFS module.

Blocking Page

This feature shows the message displayed by the Websense Enterprise when a message is blocked.

Click **Update** to apply your changes.

N2H2

This option applies only to units running SonicOS 6.2.6 Enhanced and newer. It directs the user to the **Content Filter > Settings** screen to configure N2H2 settings.

DPI-SSL Enforcement

From this screen, you can add to and edit the **DPI-SSL Client Anti-virus Enforcement** lists.

Note: Enforce the DPI-SSL Enforcement Service per zone from the Network > Zones page.

CLIENT ANTI VIRUS ENFORCEMENT

NAME	ADDRESS DETAIL	TYPE	ZONE	CONFIGURE
DPI-SSL Enforcement List		Group		+
Excluded from DPI-SSL Enforcement List		Group		+

Note: This screen applies only to units running SonicOS 6.5.2 Enhanced and above

To enforce DPI-SSL by zone, go to **Network > Zone**.

This screen applies only to units running SonicOS 6.5.2 Enhanced and newer.

- **DPI-SSL Enforcement List** - By expanding this row, you can bring up the names of the groups that are set for enforcement according to this list. The groups can either be on the list, or specifically excluded from the list.
 - Click the **Config/Edit** pencil to bring up the following dialog box.
 - Move groups as desired from Not In Group to In Group or the opposite.
 - Click **OK** to apply, or **Cancel** to discard the changes.

Name: DPI-SSL Enforcement List

Not In Group

Enter Search string...

- Default Active WAN IP
- Default Gateway
- Dial-Up Default Gateway
- DynDNS.org entries
- LAN Primary/X0 IP
- M0 IP
- Sanctioned DNS Servers
- Secondary Default Gateway
- U0 Default Gateway
- U0 IP

In Group

Enter Search string...

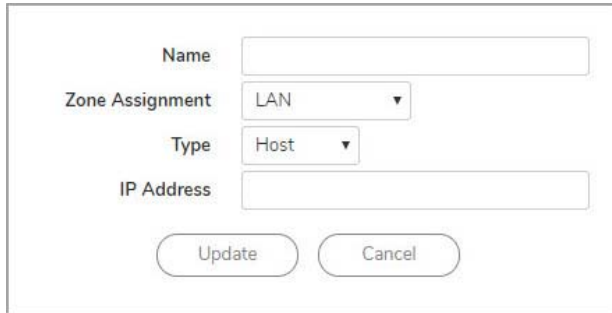
- GMS Address

-->

<--

OK Cancel

- Click the + plus sign to bring up the dialog box to add groups to this list.
 - Put in the required information to add this group to the enforcement list, the **Name**, **Zone Assignment**, **Type**, and **IP Address**.
 - Click **Update** or **Cancel** to apply or discard your changes.



The dialog box is titled 'Add Group' and contains the following fields and controls:

- Name:** A text input field.
- Zone Assignment:** A dropdown menu with 'LAN' selected.
- Type:** A dropdown menu with 'Host' selected.
- IP Address:** A text input field.
- Update:** A button to apply the changes.
- Cancel:** A button to discard the changes.

- **Excluded from DPI-SSL Enforcement List** - By expanding this row, you can bring up the names of the groups that are set for enforcement according to this list. Add to or configure this list as explained previously. The dialog boxes for both lists are similar.

Client Anti-Virus Enforcement

SonicWall Network Anti-Virus (AV) is a distributed, gateway-enforced solution that ensures always-on, always-updated anti-virus software for every client on the network. The firewall constantly monitors virus definition files, and automatically triggers the download and installation of new virus definition files to each user's computer as they become available. In addition, the appliance restricts each user's access to the Internet until the user is protected, thereby acting as an automatic enforcer of the company's virus protection.

This new approach ensures that the most current version of the virus definition file is installed and active on each device on the network, preventing a rogue user from disabling the virus protection and potentially exposing the entire network to a security breach. In addition, SonicWall Network Anti-Virus spreads the costly and time-consuming burden of maintaining and updating anti-virus software across the network.

SonicWall Network Anti-Virus also includes Network Anti-Virus Email Filter. This feature selectively manages inbound Email attachments as they pass through the SonicWall appliance, and also controls the flow of executable files, scripts, and applications into your network.

Global Management System offers anti-virus protection on a subscription-basis through a partnership with McAfee.

This section describes how to configure Anti-Virus settings for SonicWall appliances.

 **NOTE:** Purchasers of a SonicWall appliance benefit from a one-month anti-virus trial subscription.

Topics:

- [Anti-virus Settings](#)
- [Force Update Settings](#)
- [Exempt Computers](#)
- [Client Anti-virus Enforcement](#)

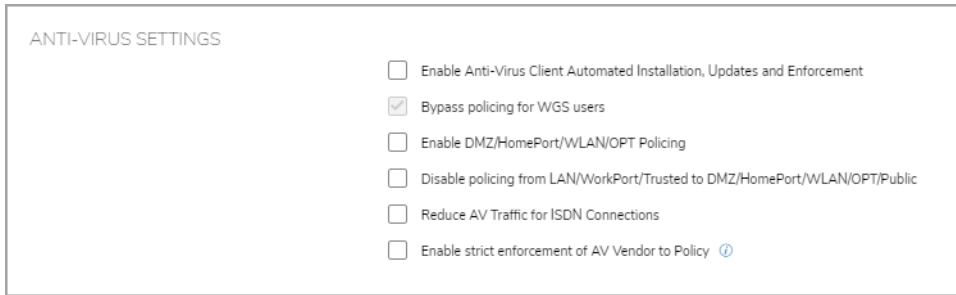
Anti-virus Settings

To enable the Client Anti-Virus Service, navigate to **Network > Zones**. After Client AV is enabled, you can configure Anti-Virus settings, described as follows.

To configure Anti-Virus settings for one or more SonicWall appliances, follow these steps:

- 1 Select the global icon, a group, or a single SonicWall appliance.

- 2 Go to **Security Services > Client AV Enforcement**, to select the desired level of enforcement. The checkboxes displayed in the **Anti-Virus Settings** section vary depending on whether a specific appliance, group or the global icon is selected.



ANTI-VIRUS SETTINGS

- Enable Anti-Virus Client Automated Installation, Updates and Enforcement
- Bypass policing for WGS users
- Enable DMZ/HomePort/WLAN/OPT Policing
- Disable policing from LAN/WorkPort/Trusted to DMZ/HomePort/WLAN/OPT/Public
- Reduce AV Traffic for ISDN Connections
- Enable strict enforcement of AV Vendor to Policy [?](#)

- **Enable Anti-Virus Client Automated Installation, Updates and Enforcement** - This setting enables automated installation, updating and enforcement of anti-virus on clients' computers.
 - **Bypass policing for WGS users** - To bypass policing to Wireless Guest Services users, click this checkbox. It is only applicable to SonicOS Standard, and is greyed out unless **Enable DMZ/HomePort/WLAN/OPT Policing** is selected.
- **Enable DMZ/HomePort/WLAN/OPT Policing** - To enforce Anti-Virus protection on the DMZ port or HomePort (if available), check this box.
- **Disable policing from LAN/WorkPort/Trusted to DMZ/HomePort/WLAN/OPT/Public** - This setting allows computers on a trusted zone (such as a LAN) to access computers on public zones (such as DMZ), even if anti-virus software is not installed on the LAN computers. If left unchecked, **Disable policing from Trusted to Public** enforces anti-virus policies on computers located in trusted zones.
- **Reduce AV Traffic for ISDN connections** - To configure the SonicWall appliance(s) to only check for updates once a day, select this setting. It is useful for low bandwidth connections or connections that are not "always on."
- **Enable Strict Enforcement of AV Vendor to policy** - For information about this setting, read the *i* (information) screen tip.

Force Update Settings

Management automatically downloads the latest virus definition files on a set schedule. To configure the maximum number of days that can pass before Management downloads the latest files, select the number of days from the **Maximum Days Allowed Before Forcing Update** field.



FORCE UPDATE SETTINGS

Maximum Days Allowed Before Forcing Update [Change](#)

Force Update on Alert Low Risk
 Medium Risk
 High Risk

Significant virus events can occur without warning. The appliance can be configured to block network traffic until the latest virus definition files are downloaded. To configure this feature, determine which types of events require updating. **Force update on alert** on this screen gives administrators a choice of which level of risk causes SonicWall, Inc. to broadcast a virus alert to all SonicWall appliances with an Anti-Virus subscription. Three levels of alerts are available, and you can select more than one. When an alert is received with this option selected, users are upgraded to the latest version of VirusScan ASaP before they can access the Internet. This option

overrides the **Maximum Days Allowed Before Forcing Update** selection. Every virus alert is logged, and an alert message is sent to the administrator.

- **Low Risk** - A virus that is not reported in the field and is considered unlikely to be found in the field in the future has a low risk. Even if such a virus includes a very serious or unforeseeable damage payload, its risk is still low.
- **Medium Risk** - If a virus is found in the field, and if it uses a less common infection mechanism, it is considered to be medium risk. If its prevalence stays low and its payload is not serious, it can be downgraded to a low risk. Similarly, it can be upgraded to high risk if it becomes more widespread.
- **High Risk** - To be assigned a high risk rating, a virus must be reported frequently in the field. The payload must have the ability to cause at least some serious damage. If it causes very serious or unpredictable damage, a high risk rating might be assigned even with a lower level of prevalence.

Exempt Computers

The **Exempt Computers** section allows the administrator to specify address ranges that should be explicitly included or excluded from anti-virus enforcement.

EXEMPT COMPUTERS

Enforce Anti-Virus policies for all computers

Include specific address ranges in the Anti-Virus enforcement

Exclude specific address ranges in the Anti-Virus enforcement

	ADDR RANGE BEGIN	ADDR RANGE END
Address Range Begin	<input type="text"/>	<input type="text"/>
Address Range End	<input type="text"/>	<input type="text"/>

Add Range

- **Enforce Anti-Virus policies for all computers** - This setting enforces anti-virus policies across your entire network. Selecting this option forces computers to install VirusScan ASaP before they can access the Internet or the DMZ. This is the default configuration.
- **Include specific address ranges in the Anti-Virus enforcement** - This setting forces a specified range of addresses to adhere to anti-virus enforcement. If you select this option, specify a range of IP addresses to be enforced. Any computer requiring enforcement needs a static IP address within the specified range of IP addresses. Up to 64 IP address ranges can be entered for enforcement.
- **Exclude specific address ranges in the Anti-Virus enforcement** - Use this setting to exempt a specified range of addresses from anti-virus enforcement. Selecting this option allows you to define ranges of IP addresses that are exempt from Anti-Virus enforcement. If you select this option, specify the range of IP addresses that are exempt. Any computer requiring unrestricted Internet access needs a static IP address within the specified range of IP addresses. Up to 64 IP address ranges can be configured.

Address ranges are defined inclusive of starting and ending addresses.

Client Anti-virus Enforcement

The **Client Anti-Virus Enforcement** list provides the option to exclude address objects from the client AV enforcement list.

CLIENT ANTI VIRUS ENFORCEMENT

▶	NAME	ADDRESS DETAIL	TYPE	ZONE	CONFIGURE
▶	Kaspersky Client AV Enforcement List		Group		+
▶	McAfee Client AV Enforcement List		Group		+
▶	Excluded from McAfee Client AV Enforcement List		Group		+
▶	Excluded from Kaspersky Client AV Enforcement List		Group		+
▶	Capture Client Enforcement List		Group		+
▶	Excluded from Capture Client Enforcement List		Group		+

For computers whose addresses do not fall in any of the above lists, the default enforcement is

- Client enforcement lists can be expanded to show all the entries in the list.
- Edit these address objects and groups by clicking the **Conf/Edit** pencil in the list row and selecting the address object groups from the Client CF Enforcement List dialog box to move to the **Not in Group side** or to the **In Group** side.

Name: Excluded from Client AV Ent

Default Active WAN IP		Dial-Up Default Gateway
Default Gateway		Secondary Default Gateway
GMS Address		
LAN Primary/X0 IP		
M0 IP		
U0 Default Gateway		
U0 IP		
U1 IP		
W0 IP		
WAN Primary/X1 IP		

- Click **OK**.
- Click **Update** to apply your choices, or **Cancel** to discard them.

- Clicking **Add** brings up the screen where you can fill in information about a group you want to add to the enforcement list or exclusion list:

The screenshot shows a dialog box with the following fields and buttons:

- Name:** A text input field.
- Zone Assignment:** A dropdown menu currently set to 'LAN'.
- Type:** A dropdown menu currently set to 'Host'.
- IP Address:** A text input field.
- Buttons:** 'Update' and 'Cancel' buttons at the bottom.

- **For Computers whose addresses do not fall in any of the above lists, the default enforcement is:** Select the default enforcement type from the drop-down menu for computers whose addresses are not covered by any of the client anti-virus enforcement criteria. Computers not on any of the enforcement lists can be set to be protected with McAfee, Kaspersky anti-virus scanning, or no protection.

The screenshot shows a configuration screen with the following elements:

- Enforcement Lists:**
 - Excluded from Client AV Enforcement List
 - McAfee Client AV Enforcement List
 - Kaspersky Client AV Enforcement List
 - For computers whose addresses do not fall in any...
- Dropdown Menu:** Open for the 'For computers...' category, showing options: None, McAfee Anti-Virus, Kaspersky Anti-Virus, and None.
- Buttons:** 'Update' and 'Reset' buttons at the bottom.

When you have completed the configuration of all the fields on this page, you have two choices:

Reset - Click this option to discard your changes.

Update - This selection brings up a dialog box where you can make choices concerning the timetable for the changes and the persistence of the changes on various units in your system.

- **Description** - In this field, type a description of the changes made.
- **Schedule** - There are three options for the timetable for your changes.
 - **Default** - Selecting this option makes your changes the default.
 - **Immediate** - Selecting this option applies your changes immediately.
 - **At** - This option brings up a dialog box with fields where you can select the time and date for the changes to take place. The selections in this box can be accepted or canceled.
 - **The current behavior is to persist changes made to all fields for all units under the selected node. Edit** - Clicking **Edit** brings up more options concerning the persistence of the changes.
 - **Persist changes at the selected node** - This option has a checkbox that relates to whether the fields and units in the lists beneath it should become persistent.
 - **Fields selected for the Change creation** - Expand this row to make a selection in the checkbox to determine the persistence of the areas where changes were made.
 - **Units for which the Change applies** - Expand this row to make a selection in the checkbox to determine the persistence of the changes on each appliance.

Accept - This option clicked on any of the dialog boxes completes the configuration of all changes made on this page.

Client CF Enforcement

SonicWall **Client Content Filtering (CF) Enforcement** provides protection and productivity policy enforcement for businesses, schools, libraries and government agencies. SonicWall has created a revolutionary content filtering architecture, utilizing a scalable, dynamic database to block objectionable and unproductive web content.

Client CF Enforcement provides the ideal combination of control and flexibility, to ensure the highest levels of protection and productivity. Client CF enforcement prevents individual users from accessing inappropriate content, while reducing organizational liability and increasing productivity. Web sites are rated according to the type of content they contain. The Content Filtering Service (CFS) blocks or allows access to web sites based on their ratings and the policy settings for a user or group.

By setting filter policies on an appliance, a business can control web surfing behavior and content accessed when the browsing is initiated within the perimeter of the security appliance. When the same device exits the perimeter, traditional filter control is lost. Client CF Enforcement addresses this gap, by blocking objectionable and unproductive Web content outside the security appliance perimeter.

SonicWall security appliances, working in conjunction with Client CF Enforcement, automatically and consistently ensure that all endpoints have the latest software updates for the highest level of network protection. This feature is designed to work with both Windows and Mac PCs.

Client CF Enforcement consists of the following three main components:

- A Network Security Appliance running GMS, whose role is to facilitate and verify licensing of CFS and to enable or disable enforcement and configure exclusions and other settings.
- Automatic triggering of Client CF Enforcement for any client attempting to access the Internet without the client software installed. Clients are automatically blocked from accessing Websites until appropriate levels of Client CF Enforcement are installed.

The administration of client policies and client groups uses the cloud-based EPRS server, accessed from MySonicWall or from GMS running on the appliance. This section describes how to enable and configure settings for Client CF Enforcement in GMS.

Client CF Enforcement must be enabled on the SonicWall appliance before users are presented with a Website block page that prompts the user to install the Client CF Enforcement.

i | **NOTE:** If the Content Filtering Client (CFS) is not activated on MySonicWall, you must activate it to enforce client content filtering policies on client systems.

i | **NOTE:** The note at the top of the page has a link to go to the **Zones** page to enable enforcement by zone.

Client CF Enforcement Policies

After CF Enforcement Service has been enabled by zone from the **Network > Zones** page, you can configure CF policies.

Select a grace period for the enforcement to apply, between 0 and 5 days.

Note: Enable the CF Enforcement Service per zone from the Network > Zones page.

CLIENT CF ENFORCEMENT POLICIES

Grace Period

CLIENT CF ENFORCEMENT LISTS

NAME	ADDRESS DETAIL	TYPE	ZONE	CONFIGURE
Excluded from Client CF Enforcement List		Group		+
Client CF Enforcement List		Group		+

For computers whose addresses do not fall in any of the above lists, the default enforcement is

Client CF Enforcement Lists

- Client CF Enforcement Lists can be expanded to show all entries in the list.
- Edit these address objects and groups by clicking the **Conf/Edit** pencil in the list row and select the address object groups from the Client CF Enforcement List dialog box to move to the **Not in Group side** or to the **In Group side**.

Name

Not In Group

- All Authorized Access Points
- All Interface IP
- All Interface IPv6 Addresses
- All LAN/X0 Management IP
- All M0 Management IP
- All MGMT Management IP
- All SonicPoints
- All U0 Management IP
- All U1 Management IP
- All WAN IP

In Group

- Click **OK**.
- Click **Update** to apply your choices, or **Cancel** to discard them.

- Clicking **Add** brings up the screen where you can fill in information about a group you want to add to the enforcement list or exclusion list:

The screenshot shows a configuration form with the following elements:

- Name:** A text input field.
- Zone Assignment:** A dropdown menu currently set to 'LAN'.
- Type:** A dropdown menu currently set to 'Host'.
- IP Address:** A text input field.
- Buttons:** 'Update' and 'Cancel' buttons at the bottom.

- For computers whose addresses do not fall in any of the previously mentioned lists, select:
 - **Client CF Enforcement** - Select this option to prompt all other computers connected to the Internet through this appliance to install the enforced client protection.
 - **None** - Select this option from the drop-down menu if you only want to enforce the service on computers that you have configured.

The screenshot shows the configuration page with the following elements:

- Text:** "For computers whose addresses do not fall in any of the above lists, the default enforcement is"
- Dropdown:** A dropdown menu currently set to 'None', which is open to show 'None' and 'Client CF Enforcement' options.
- Buttons:** 'Update' and 'Reset' buttons.

When you have completed the configuration of all the fields on this page, you have two choices:

Reset - Click this option to discard your changes.

Update - This selection brings up a dialog box where you can make choices concerning the timetable for the changes and the persistence of the changes on various units in your system.

- **Description** - In this field, type a description of the changes made.
- **Schedule** - There are three options for the timetable for your changes.
 - **Default** - Selecting this option makes your changes the default.
 - **Immediate** - Selecting this option applies your changes immediately.
 - **At** - This option brings up a dialog box with fields where you can select the time and date for the changes to take place. The selections in this box can be accepted or canceled.
 - **The current behavior is to persist changes made to all fields for all units under the selected node. Edit** - Clicking **Edit** brings up more options concerning the persistence of the changes.
 - **Persist changes at the selected node** - This option has a checkbox that relates to whether the fields and units in the lists below it should become persistent.
 - **Fields selected for the Change creation** - Expand this row to make a selection in the checkbox to determine the persistence of the areas where changes were made.
 - **Units for which the Change applies** - Expand this row to make a selection in the checkbox to determine the persistence of the changes on each appliance.

Accept - This option clicked on any of the dialog boxes completes the configuration of all changes made on this page.

Gateway Anti-Virus

To configure SonicWall Gateway Anti-Virus (AV):

- Select the Global option, a group, or a single appliance.
- Click on **Security Services > Gateway Anti-Virus**. The Gateway Anti-Virus screen appears:

The screenshot shows the SonicWall Gateway Anti-Virus configuration interface. At the top, it displays the status and a warning: "Warning: No Zones have GAV enabled". The main section is "GATEWAY ANTI-VIRUS SETTINGS", which includes checkboxes for "Enable Gateway Anti-Virus", "Enable Cloud Anti-Virus Database", and "On Interface" (with sub-options for WAN, LAN/Wireless, and DMZ/HomePort/WLAN/GPT). Below this is a table for "PROTOCOLS" with columns for HTTP, FTP, NNTP, SMTP, POP3, CIFS/SMBIOS, and TCP STREAM. The "Enable Inbound Inspection" row has checkboxes for all protocols, while "Enable Outbound Inspection" only has checkboxes for HTTP and FTP. There are also "Protocol Settings" links for each protocol. At the bottom of the settings section are buttons for "Configure Settings", "Update Signatures Database", "Reset Settings", and "Cloud AV DB Exclusion Settings". The "GATEWAY ANTI-VIRUS SIGNATURES" section shows a table with columns for ID, NAME, and ENABLE. Two entries are visible: ID 1 with NAME "A" and ID 2 with NAME "A..32", both with the ENABLE checkbox checked. There are also "Update" and "Reset" buttons at the bottom right of the signatures section.

Topics:

- [Gateway Anti-virus Status](#)
- [Gateway Anti-virus Settings](#)
- [Protocols](#)
- [Gateway Anti-virus Signatures](#)

Gateway Anti-virus Status

- **Gateway Anti-Virus Status** section gives the current status of the system. You can manually update your SonicWall database at any time by clicking **Update** at the bottom of this screen. By default, the SonicWall security appliance running SonicWall GAV automatically checks for new signatures once every hour.
- If you wish to enable Gateway AV by zone, click on **Zones** in this section for a link to the **Zones** page.

Gateway Anti-virus Settings

- **Enable Gateway Anti-Virus** - This option enables Gateway AV on your system. When this option is selected, the next four fields are available.

- **Enable Cloud Anti-Virus Database** - Select this option to enable the Cloud AV database. This option is only available when **Enable Gateway Anti-Virus** is checked.
- **WAN, LAN/WorkPort, and DMZ/HomePort/WLAN/OPT** - If you have SonicWall GMS-managed SonicWall firewall appliances running SonicOS Standard, select the interface on which you want to enable **Gateway Anti-Virus**. These three settings apply only to SonicOS Standard, and are only available when **Enable Gateway Anti-Virus** is checked.

GATEWAY ANTI-VIRUS SETTINGS

Enable Gateway Anti-Virus

Enable Cloud Anti-Virus Database

On Interface

WAN

LAN/WorkPort

DMZ/HomePort/WLAN/OPT

(The LAN/WAN/DMZ checkboxes above apply only to units not running SonicOS enhanced firmware.)

Enable Gateway Anti-Virus

Enable Cloud Anti-Virus Database

On Interface

WAN

LAN/WorkPort

DMZ/HomePort/WLAN/OPT

(The LAN/WAN/DMZ checkboxes above apply only to units not running SonicOS enhanced firmware.)

Protocols

Application-level awareness of the type of protocol that is transporting the violation allows SonicWall **Gateway Anti-Virus** to execute specific actions within the context of the application to handle rejection of the payload.

NOTE: If your SonicWall firewall appliance is running SonicOS Enhanced, you must enable Gateway Anti-Virus on the appropriate zone on the **Network > Zones** page before continuing.

PROTOCOLS	HTTP	FTP	IMAP	SMTP	POP3	CIFS/NETBIOS	TCP STREAM
Enable Inbound Inspection	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Enable Outbound Inspected	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>			<input type="checkbox"/>
Protocol Settings							

Configure Settings
Update Signature Database
Reset Settings
Cloud AV DB Exclusion Settings

Restrict Transfer of password-protected ZIP files

Restrict Transfer of MS-Office type files containing macros (VBA 5 and above)

Restrict Transfer of packed executable files (UPX, FSG, etc)

Update Reset

- **Enable Inbound Inspection** - In the Protocol section of the screen, select which types of traffic to inspect for in the checkboxes below the names of the protocols.
- **Enable Outbound Inspection** To scan outgoing mail, check the appropriate box.
- **Protocol Settings** - For more granular control over protocol traffic inspection, click **Edit/Config** for the protocol you have chosen. The protocol settings window appears to allow you to restrict transfer of the following possibly dangerous file types:

Gateway AV File Transfer Restrictions

File Type	Security Issues
Password protected ZIP files	This option only functions on protocols (for example, HTTP, FTP, SMTP) that are enabled for inspection.

Gateway AV File Transfer Restrictions (Continued)

File Type	Security Issues
MS-Office type files containing macros	Restricts transfer of any MS Office 5 and newer files that contain VBA macros.
Packed executable files (UPX, FSG, and so on.)	Disables the transfer of packed executable files. Packers are utilities which compress and sometimes encrypt executables. Although there are legitimate applications for these, they are also sometimes used with the intent of obfuscation, so as to make the executables less detectable by anti-virus applications. The packer adds a header that expands the file in memory, and then executes that file.

The previous restrictions could be selected across all protocols for inbound and outbound traffic with the three checkboxes.

The four configuration icons associated with the **Protocol Settings Edit/Config** pencils are explained as follows:

- **Configure Settings** - Select this option to configure SonicWall Gateway Anti-Virus settings and notification preferences. The following dialog box appears:
 - **GateWay AV Settings** - Select one or several of the following options:
 - **Disable SMTP Responses** -
 - **Disable detection of EICAR test virus** -
 - **Enable HTTP Byte-Range requests with Gateway AV** -
 - **Enable FTP 'REST' requests with Gateway AV** -
 - **Do not scan parts of files with high compression ratios** -
 - **Enable detection-only mode** -
 - **Block files with multiple levels of zip/gzip compression** -
 - **HTTP Clientless Notification**
 - **Enable HTTP Clientless Notification Alerts** -
 - **This request is blocked by Firewall Gateway Anti-Virus Service** -
 - **Gateway AV Exclusion List**
 - **Enable Gateway AV Exclusion List** - Check this box to make the details of the list available for configuration.
 - **Use Address Object** - This option is automatically checked when the previous option is selected.
 - **Select an address object** - This is a drop-down menu for choosing an address object.
 - **Use Address Range** - This icon is available when the exclusion option is selected. It is an alternative to selecting a specific address object. Type in the IP addresses for the limits of the range, and click **Add**.

- Click **OK** to apply your selections, or **Cancel** to discard them.

- **Update Signature Database** - Click this button to bring up a dialog box with the settings to schedule the update.
- **Reset Settings** - Select this option to reset all GAV settings to factory default values. A dialog box comes up asking for confirmation.
- **Cloud AV DB Exclusion Settings** - This button makes the cloud AV DB exclusion settings available for configuration.
 - **Cloud AV Exclusions List** - Fill in the **Cloud AV Signature ID** and a read-only list appears.
 - The options are **Add, Update, Remove, Sig Info, OK, or Cancel**.

When you have completed the configuration of all the fields in this section, you have two choices:

Reset - Click this option to discard your changes.


Update - This selection brings up a dialog box where you can make choices concerning the timetable for the changes and the persistence of the changes on various units in your system. The **Update** button at the bottom of the page gives the same choices.

- **Description** - In this field, type a description of the changes you made.
- **Schedule** - There are three options for the timetable for your changes.
 - **Default** - Selecting this option makes your changes the default.
 - **Immediate** - Selecting this option applies your changes immediately.

- **At** - This option brings up a dialog box with fields where you can select the time and date for the changes to take place. The selections in this box can be accepted or canceled.
- **The current behavior is to persist changes made to all fields for all units under the selected node. Edit** - Clicking **Edit** brings up more options concerning the persistence of the changes.
 - **Persist changes at the selected node** - This option has a checkbox that relates to whether the fields and units in the lists below it should become persistent.
 - **Fields selected for the Change creation** - Expand this row to make a selection in the checkbox to determine the persistence of the areas where changes were made.
 - **Units for which the Change applies** - Expand this row to make a selection in the checkbox to determine the persistence of the changes on each appliance.

Gateway Anti-virus Signatures

The Gateway Anti-Virus Signatures section allows you to view the contents of the SonicWall GAV signature database. All the entries displayed in the Gateway Anti-Virus Signatures table are from the SonicWall GAV signature database downloaded to your SonicWall security appliance on a regular basis.

 **NOTE:** Signature entries in the database change over time in response to new threats.


You can display the signatures in a variety of ways using the menu at the top of the table, described from left to right:

- **View Style: First letter** - This field provides a drop-down menu with the following filters:
 - **All Signatures** - This option displays all the signatures in the table, 50 to a page.
 - **0 - 9** - The choices are to display signature names beginning with the number you select from the menu.
 - **A-Z** - You can display signature names beginning with the letter you select from menu.
- **Items** - Choose the range of items to display from those selected according to your filter.
- **Navigation buttons** - These buttons help you navigate through large sets of signatures. The SonicWall GAV signatures are displayed fifty to a page in the table. If you are displaying the first page of a signature table, the entry might be **Items 1 to 50 (of 58)**.
- **Lookup Signatures Containing String:** Select a string to define the signature(s) to display.
- **Signature Rows** - Each row has the **Number** of the signature, its **Name**, and a checkbox to **Enable GAV** against that virus.

When you have made your selection, click **Reset** or **Update**. **Update** brings up a dialog box where you can make choices concerning the timetable for the changes and the persistence of the changes on various units in your system.

Anti-Spyware Service

SonicWall Anti-Spyware is included in the SonicWall Gateway Anti-Virus (GAV), Anti-Spyware and Intrusion Prevention Service (IPS) unified threat management solution. Together, SonicWall GAV, Anti-Spyware and IPS deliver a comprehensive, real-time, gateway security solution for your entire network.

 **WARNING:** After activating your SonicWall Anti-Spyware license, you must enable and configure SonicWall Anti-Spyware on the SonicWall management interface. Only when this is done can the anti-spyware policies be applied to your network traffic.

For instructions on setting up SonicWall Anti-Spyware Service, refer to the *SonicWall Anti-Spyware Service Administration Guide* available on the SonicWall website at:

<https://www.SonicWall.com/support/technical-documentation>

To enable and configure Anti-Spyware for your SonicWall security appliance, go to **Security > Security Services**. The **Anti-Spyware** management interface screen is divided into the following sections:

Topics:

- [Anti-spyware Status](#)
- [Anti-spyware Global Settings](#)
- [Signature Groups](#)
- [Protocols](#)
- [Anti-spyware Signatures](#)

Anti-spyware Status

- This section of the screen displays status information on the signature database, your SonicWall Anti-Spyware license, and other details. It gives the date and time of the latest available database. If you want to enable Anti-Spyware Service for a zone, click on the word **Zone** for a link to the **Zone** screen.

Anti-spyware Global Settings

- **Enable Anti-Spyware** - Click this checkbox to make key settings available for enabling Anti-Spyware on your SonicWall security appliance.

- **WAN, LAN/WorkPort, and DMZ/HomePort/WLAN/OPT** - After you enable Anti-Spyware, these three interface checkboxes become available. Check the ones where you want to activate the spyware. SonicWall Anti-Spyware must first be globally enabled on your SonicWall security appliance.

ANTI-SPYWARE GLOBAL SETTINGS

Enable Anti-Spyware

On Interface WAN

LAN/WorkPort

DMZ/HomePort/WLAN/OPT

Signature Groups

- You can select different protection for each of three different danger levels, **High Danger Level Spyware**, **Medium Danger Level Spyware**, and **Low Danger Level Spyware**.

SIGNATURE GROUPS	PREVENT ALL	DETECT ALL	LOG REDUNDANCY FILTER (SECONDS)
High Danger Level Spyware	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
Medium Danger Level Spyware	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
Low Danger Level Spyware	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>

- **Prevent All** - Select this option to detect, log, and prevent all attacks of this level.

CAUTION: SonicWall recommends enabling **Prevent All** for **High Danger Level Spyware** and **Medium Danger Level Spyware** signature groups to provide anti-spyware protection against the most damaging and disruptive spyware applications. You can also enable **Detect All** for spyware logging and alerting.

- **Detect All** - Select this option to detect and log only.
- **Log Redundancy Filter (Seconds)** - To prevent the log from becoming overloaded with entries for the same attack, enter a value in the field. For example, if you entered a value of 30 seconds and there were 100 SubSeven attacks during that period of time, only one attack would be logged during that 30 second period.

- **Configure Settings** - This is one of the buttons below the attack level chart. It brings up the following dialog box.

- **Anti-spyware Settings**
 - **Disable SMTP Responses** - Click this checkbox to suppress the sending of email messages (SMTP) to clients from SonicWall Anti-Spyware when a virus is detected in an email or attachment.
- **HTTP Clientless Notification**
 - **Enable HTTP Clientless Notification Alerts** - Checking this box allows the message in the box below to be shown when blocking a request.
- **Anti-spyware Exclusion List**
 - **Enable Anti-Spyware Exclusion List** - Click this checkbox to allow the spyware to be limited by an exclusion list. The security appliance bypasses Anti-Spyware enforcement for a specified address object or IP range. Selecting this box makes the next fields available to identify the addresses of the excluded objects.
 - Select an address object or an address range to add to the exclusion list.
- **Update Signature Database** - Click to refresh the list on the lower part of this page. A dialog box appears requesting more information about the schedule for your changes.
- **Reset Settings** - Click to reset the settings to the factory defaults. A dialog box appears requesting more information about the schedule for your changes.

Protocols

- You can choose on which protocols you want to **Enable Inbound Inspection** by the Anti-Spyware software.
 - Click the checkbox for each selected protocol.
 - **Enable Inspection of Outbound Spyware Communication** - Clicking this choice makes the outbound traffic available for inspection.

Anti-spyware Signatures

SonicWall Anti-Spyware allows you to configure anti-spyware policies at the category and signature level, to provide flexible granularity for tailoring SonicWall Anti-Spyware protection based on your network environment requirements. If you are using GMS to configure a device that runs SonicOS Enhanced, you can apply these custom SonicWall Anti-Spyware policies to Address Objects, Address Groups, and User Groups, as well as create enforcement schedules.

ANTI-SPYWARE SIGNATURE SETTINGS

Product: 7FaSSt

Signature Name: 7FaSSt ActiveX component download

Signature ID: 2518

Danger Level: 2

Prevention: Use Product Setting

Detection: Use Product Setting

Included Users/Groups: Use Product Settings

Excluded Users/Groups: Use Product Settings

Included IP Address Range: Use Product Settings

Excluded IP Address Range: Use Product Settings

Schedule: Use Product Settings

Log Redundancy Filter: Use Product Settings 30 seconds

OK Cancel

The previous screen appears when you click **Edit/Config** on the **Signature** row. Configure the fields in the Anti-Spyware Signature Settings dialog box as described in the following table:

Anti-Spyware Product Settings

Field	Description
Product Name	The name in the row you chose to configure
Prevention	Allows you to enable and disable anti-spyware prevention for the device
Detection	Allows you to enable and disable anti-spyware detection for the device
Included Users/Groups	Applies the anti-spyware settings to members of the following group types: All, Administrators, Everyone, Guest Services, Trusted Users, Content Filtering Bypass, and Limited Administrators
Excluded Users/Groups	Does not apply the anti-spyware settings to members of the following group types: All, Administrators, Everyone, Guest Services, Trusted Users, Content Filtering Bypass, and Limited Administrators
Included IP Address Range	Allows you to apply the anti-spyware settings to all users that fall within a specified IP address range of a specified category
Excluded IP Address Range	Allows you to exclude all users that fall within a specified IP address range of a specified category
Schedule	Allows you to set a schedule

Anti-Spyware Product Settings (Continued)

Field	Description
Log Redundancy Filter	Check this box to set the filter
Use Product Settings in seconds	If the filter box is checked, this setting is not available

Intrusion Prevention Service

The Intrusion Prevention Service (IPS) is a subscription-based service that is frequently updated to protect your networks from new attacks and undesired uses that expose your network to potential risks. The following topics are covered in this section:

Topics:

- [Overview of IPS](#)
- [SonicWall Deep Packet Inspection](#)
- [Enabling Intrusion Prevention Services](#)
- [IPS Settings](#)
- [IPS Policies](#)

Overview of IPS

SonicWall Intrusion Prevention Service (SonicWall IPS) delivers a configurable, high performance Deep Packet Inspection (DPI) engine for extended protection of key network services such as Web, Email, file transfer, Windows services and DNS. SonicWall IPS is designed to protect against application vulnerabilities, as well as worms, Trojans, and peer-to-peer, spyware and back door exploits. The extensible signature language used in SonicWall's Deep Packet Inspection engine also provides proactive defense against newly-discovered application and protocol vulnerabilities. SonicWall IPS offloads the costly and time-consuming burden of maintaining and updating signatures for new attacks through SonicWall's industry-leading Distributed Enforcement Architecture (DEA). Signature granularity allows SonicWall IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

SonicWall Deep Packet Inspection

Deep Packet Inspection (DPI) looks at the data portion of the packet. The Deep Packet Inspection technology includes intrusion detection and intrusion prevention. Intrusion detection finds anomalies in the traffic and alerts the administrator. Intrusion prevention finds anomalies in the traffic and reacts, preventing the traffic from passing through.

Deep Packet Inspection is a technology that allows a SonicWall security appliance to classify passing traffic based on rules. These rules include information about layer 3 and layer 4 content of the packet, as well as the information that describes the contents of the packet's payload, including the application data (for example, an FTP session, an HTTP Web browser session, or even a middleware database connection). This technology allows the administrator to detect and log intrusions that pass through the SonicWall security appliance, as well as prevent them (such as dropping the packet or resetting the TCP connection). SonicWall's DPI technology also correctly handles TCP fragmented byte stream inspection as if no TCP fragmentation had occurred.

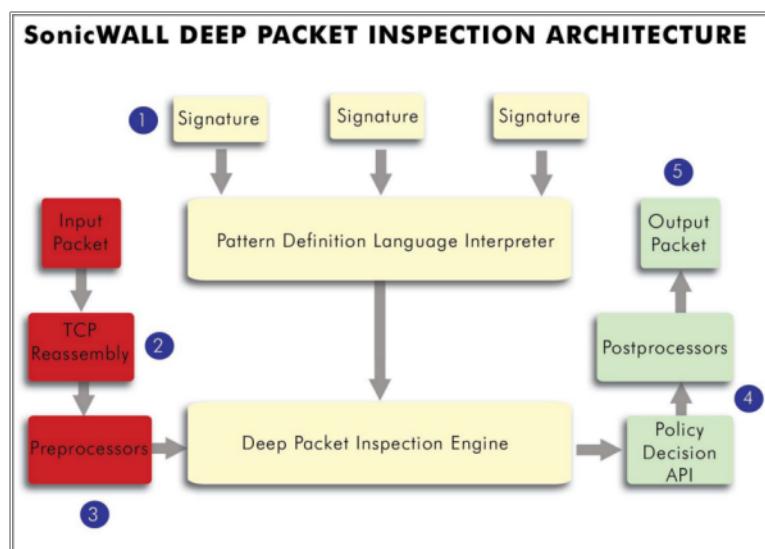
How the SonicWall Deep Packet Inspection Architecture Works

Deep Packet Inspection (DPI) technology enables the SonicWall firewall appliance to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities. This is the technology behind SonicWall Intrusion Prevention Service. SonicWall's Deep Packet Inspection technology enables dynamic signature updates pushed from the SonicWall Distributed Enforcement Architecture.

The following steps describe how the SonicWall Deep Packet Inspection Architecture works:

- 1 Pattern Definition Language Interpreter uses signatures that can be written to detect and prevent against known and unknown protocols, applications and exploits.
- 2 TCP packets arriving out-of-order are reassembled by the Deep Packet Inspection framework.
- 3 Deep Packet Inspection engine preprocessing involves normalization of the packet's payload. For example, a HTTP request might be URL encoded and so the request is URL decoded in order to execute correct pattern matching on the payload.
- 4 Deep Packet Inspection engine post-processors execute actions that might either simply pass the packet without modification, or could drop a packet, or could even reset a TCP connection.
- 5 SonicWall's Deep Packet Inspection framework supports complete signature matching across the TCP fragments without completing any reassembly (unless the packets are out of order). This results in a more efficient use of the processor and memory for greater performance.

SonicWall Deep Packet Inspection Architecture



If TCP packets arrive out of order, the SonicWall IPS engine reassembles them before inspection. However, SonicWall's IPS framework supports complete signature matching across the TCP fragments without having to do a complete reassembly. SonicWall's unique reassembly-free matching solution dramatically reduces CPU and memory resource requirements.

Enabling Intrusion Prevention Services

To configure IPS settings for one or more SonicWall appliances:

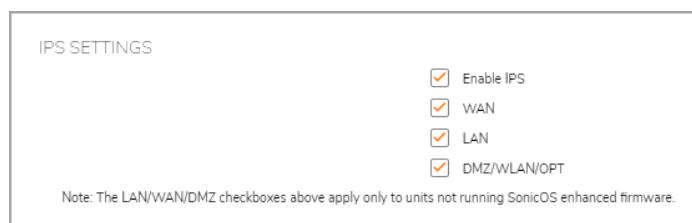
- 1 Select the global icon, a group, or a SonicWall appliance.
- 2 Go to **Security Services > Intrusion Prevention** and make changes as required on the three sections on the Intrusion Prevention screen:

IPS Status

- The top part of the screen give the status of IPS on the system. It gives the date and time of the **Latest available Signature Database**, and the zones that are IPS enabled. If you want to enable IPS in a certain zone, click on the word Zone in this section to get a link to the **Zone** page.

IPS Settings

- **Enable IPS** - Click this setting to enable the IPS service. After service is enabled, the next three checkboxes become available.
- Select the checkboxes of the interface ports to monitor, **WAN, LAN, or DMZ/WLAN/OPT**. These three checkboxes become available when **Enable IPS** is checked.



IPS SETTINGS

- Enable IPS
- WAN
- LAN
- DMZ/WLAN/OPT

Note: The LAN/WAN/DMZ checkboxes above apply only to units not running SonicOS enhanced firmware.

- The next section allows you to configure the level of attack to monitor and in what way. You can set different levels of protection for **High Priority Attacks, Medium Priority Attacks, and Low Priority Attacks**.

SIGNATURE GROUPS	PREVENT ALL	DETECT ALL	LOG REDUNDANCY FILTER (SECONDS)
High Priority Attacks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
Medium Priority Attacks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
Low Priority Attacks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="60"/>

- **Prevent All** - Select this option to detect, log, and prevent all attacks of this level.
- **Detect All** - Select this option to detect and log only.
- **Log Redundancy Filter (Seconds)** - To prevent the log from becoming overloaded with entries for the same attack, enter a value in the field. For example, if you entered a value of 30 seconds and there were 100 SubSeven attacks during that period of time, only one attack would be logged during that 30 second period.
- **Configure IPS Settings** - This is one of four buttons below the attack level chart. It brings up the following dialog box.
 - **IPS Exclusion List**

- **Enable IPS Exclusion List** - Select this field to configure the SonicWall security appliance to skip IPS enforcement for a specified IP address object or range of address objects. The fields that follow are only available when this field is selected.
 - **Use Address Object** — Select an address object from the drop-down menu.
 - **Use Address Range** — Fill in the address range limits to exclude. If the address range is selected, you can **Add** or **Delete All** of the choices.
 - Click **OK** or **Cancel** when you are done with this page.
- 3 **Update IPS Signature Database** - Select to force the firmware to download all signatures.
 - 4 **Reset IPS Settings & Policies** - Click to reset your IPS settings to the defaults.
 - 5 **Import CSV File** - This button imports the CSV file.
 - 6 **Reset** clears all the settings on the screen. **Update** - brings up a dialog box requesting more information about the schedule and persistence of the individual changes you have made.

IPS Policies

This section allows the administrator to configure settings for individual attacks.

- 1 Locate the type of attack that you would like to view. To sort by category, select a category from the **Categories** list box. To sort by priority, select a priority level from the **Priority** list box.
- 2 After locating a type of attack to configure, click **Config/Edit** on its row. A dialog box appears where you can give specific information about the **IPS Signature Settings** for the selected attack. The top part of the dialog box is populated with the information from the selected Signature row. Configure the fields in the dialog box for each type of attack you need to edit.

IPS SIGNATURE SETTINGS

Signature Category: EXPLOIT-KIT

Signature Name: Suspicious Rtg Exploit Delivery 1

Signature ID: 11515

Priority: High

Direction: Outgoing, to Server

Prevention: Use Global Settings

Detection: Use Global Settings

Included Users/Groups: Use Category Settings

Excluded Users/Groups: Use Category Settings

Included IP Address Range: Use Category Settings

Excluded IP Address Range: Use Category Settings

Schedule: Use Category Settings

Log Redundancy Filter (seconds): Use Category Settings

Update Reset

- **Prevention** - Select whether attack prevention for this type of attack is enabled, disabled, or uses the default global settings for the attack category from the list.
- **Detection** - Select whether attack detection for this type of attack is enabled, disabled, or uses the default global settings for the attack category from the list.
- **Included Users/Groups** - Select which users or groups to include for this attack type from the list.
- **Excluded Users/Groups** - Select which users or groups to exclude for this attack type from the list.
- **Included IP Address Range** - Select an IP address range to include for this attack type from the list.
- **Excluded IP Address Range** - Select an IP address range to exclude for this attack type in the list box.
- **Schedule** - Select a time range to enforce attack protection on this attack type the list.
- **Log Redundancy Filter (seconds)** - Enter a timespan (in seconds) to set the filter, or select Use Category Settings.
- **Update** - This selection returns you to the Intrusion Prevention page. Your changes have been applied.
- **Reset** - This selection discards your changes.

Geo-IP Filter

The Geo-IP Filter feature allows you to block connections to and from individual geographic locations. GMS uses the IP address to determine the location of the attempted connection. The Geo-IP Filter feature also allows you to create custom country lists to control traffic to and from certain IP addresses.

The Geo-IP Filtering feature is available on TZ300 series and higher appliances.

Topics:

- [Settings](#)
- [Custom List](#)
- [Web Block Page](#)

Settings

The settings screen gives a group of settings that can be configured for Geo-IP Filtering. Several of the settings have (information) icons next to them that give screen tips about that setting.

SETTINGS

- Block connections to/from following countries ⓘ
- All Connections
- Firewall Rule-based
- Block all connections to public IPs if GeoIP DB is not downloaded ⓘ
- Enable Logging ⓘ
- Enable Custom List ⓘ
- Override Firewall Countries By Custom List ⓘ

<input type="checkbox"/>	BLOCKED	COUNTRY
<input type="checkbox"/>		Afghanistan
<input type="checkbox"/>		Aland Islands
<input type="checkbox"/>		Albania
<input type="checkbox"/>		Algeria
<input type="checkbox"/>		American Samoa
<input type="checkbox"/>		Andorra
<input type="checkbox"/>		Angola

Block All UNKNOWN countries ⓘ

Geo-IP Exclusion Object: Default Geo-IP and Botnet Exclusion Group ⓘ

- **Block connections to/from following countries** - This option is selected by default. If this option is enabled, all connections to/from the selected list of countries are blocked. You can specify an exclusion list to exclude blocking for selected IPs. When this option is selected, the next two options become available.
- **All Connections**— This selects one of the two modes of Geo-Filter. All connections to and from the firewall are filtered. This option is selected by default.

- **Firewall Rule-Based Connections** — With this selection only connections that match an access rule configured on the firewall are filtered for blocking.
- **Block all connections to public IPs if Geo-IP DB is not downloaded.** This option is not selected by default. If the Geo-IP database is not downloaded, this selection drops all attempted connections from public IP addresses.
- **Enable Logging.** This option is not selected by default. It enables logging of filter events.
- **Enable Custom List.** This option is not selected by default. Custom lists are sometimes used to correct a false country assignment for an IP address. If the checkbox is selected, the **Override Firewall Countries by Custom List** is made available.
 - **Override Firewall Countries by Custom List** - This selection is only available if **Enable Custom List** is clicked. It allows your custom list to override the firewall list where there are differences. Unless you select this **Override**, the firewall list takes precedence, even when you have enabled a custom list.
- **Blocked Country table** - Click the checkbox for the countries to be blocked. By default, no countries are blocked. By clicking on the checkbox at the top of the table, you can select all countries, then exclude countries from blocking by clicking on them separately.
- **Block All UNKNOWN countries** - Select this option to block any countries that are not listed. All connections to unknown public IPs are blocked. This option is not selected by default.
- **Geo-IP Exclusion Object** - This setting allows you to configure an exclusion list of all connections to approved IP addresses:
 - Select an address group from the drop-down menu. The default is **Default Geo-IP and Botnet Exclusion Group**.

The **Geo-IP Exclusion Object** is a network address object group that specifies a group or a range of IP addresses to be excluded from the Geo-IP filter blocking. All IP addresses in the address object or group are allowed, even if they are from a blocked country.

For example, if all IP addresses coming from Country A are set to be blocked and an IP address from Country A is detected, but it is in the **Geo-IP Exclusion Object** list, then traffic to and from this IP address is allowed to pass.

For this feature to work correctly, the country database must be downloaded to the firewall. The Status indicator at the top right of the page turns yellow if this download fails. Green status indicates that the database has been successfully downloaded.

For the country database to be downloaded, the firewall must be able to resolve the address, `geodnsd.global.SonicWall.com`.

When a user attempts to access a web page that is from a blocked country, a block page message is displayed on the user's web browser.

i **NOTE:** If a connection to a blocked country is short-lived and the firewall does not have a cache for the IP address, then the connection might not be blocked immediately. As a result, connections to blocked countries might occasionally appear in the App Flow Monitor. However, additional connections to the same IP address are blocked immediately.

- Click **Update** to apply your changes, **Reset** to cancel them. With **Update**, you see a dialog box that requests more information about the schedule and the persistence of your changes. Click **Accept** to confirm your changes.

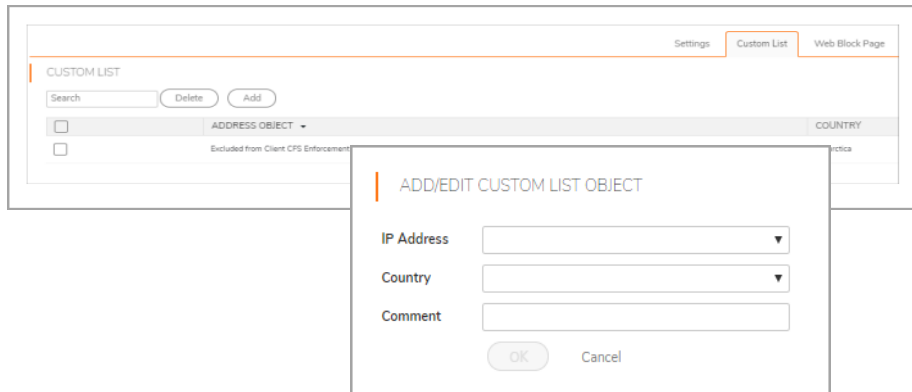
Custom List

This section allows you to create a custom list of IP addresses to either block or allow. This can be useful, for example, if an IP address is mistakenly associated with a blocked country, and you want it to be allowed. Having

a custom country list can solve this problem by overriding the firewall country associated with the particular IP address.

NOTE: For the firewall to use the Custom List first, you must enable it and select **Override Firewall List**.

- 1 To add a custom list address object, click **Add** to bring up the **Add/Edit Custom List Object** dialog box.



- 2 Select an **IP Address** for the IP Address field.
- 3 Select a country from the **Country** drop-down menu.
- 4 If desired, you can add a comment in the **Comment** field.
- 5 Click **OK**.

Editing a Custom List Entry

- 1 To edit an object, click **Edit/Config** in the **Configure** column for the entry to be edited. The **Add/Edit Custom List Object** dialog appears with the IP address and any comment about the entry already populated.
- 2 Select the country from the **Country** drop-down menu.
- 3 Click **OK**. The **Custom List** table is updated.

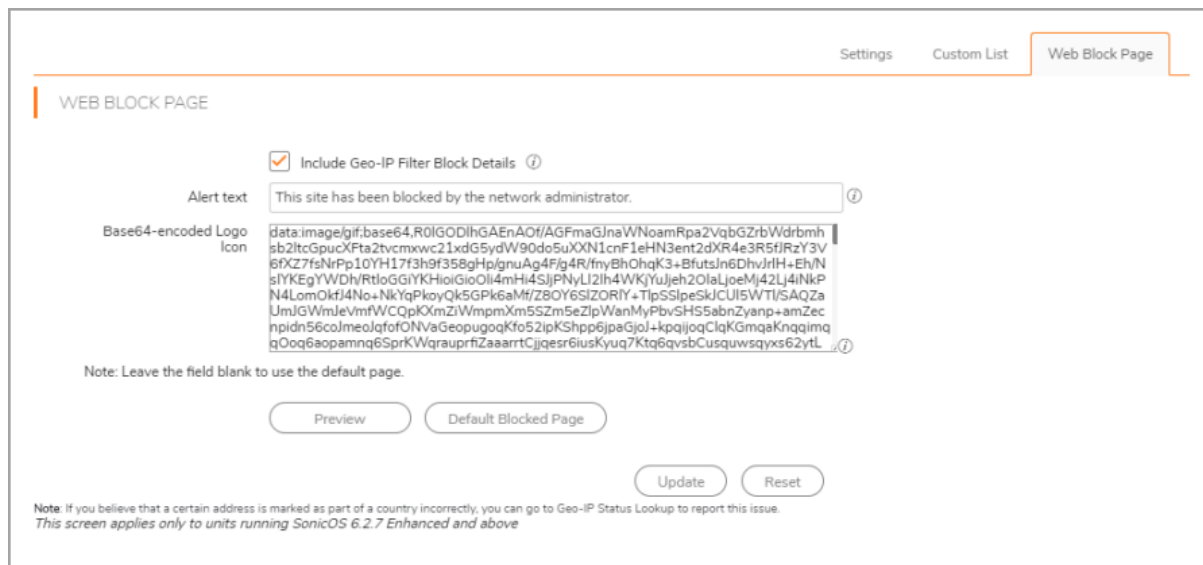
Deleting Custom List Entries

- 1 You can delete an entry by clicking **Delete** in the **Configure** column for the entry, or by clicking the checkbox for the entry and clicking **Delete** in the top row. A confirmation message appears.
- 2 Click **OK**.
- 3 To delete multiple entries, select the checkboxes of the entries to be deleted, or all entries at the top. **Delete** becomes available.
- 4 Click **Delete** to bring up a confirmation message.
- 5 Click **OK**.

Web Block Page

The Geo-IP Filter has a message that can be displayed when a user attempts to access a blocked page. You can have the message display detailed information, such as the reason why this IP address is blocked, as well as the

IP address and the country from which it was detected. You can also create a custom message and include a custom logo.



- **Include Geo-IP Filter Block Details** - Select this option to show blocking details, such as reason for the blocking, the IP address, and the country. When disabled, no information is displayed. By default, this option is selected.
- **Alert Text**
 - To use the default message displayed in the **Alert text** field, **This site has been blocked by the network administrator**, click **Default Blocked Page**.
 - Fill in a custom message, if desired, to be displayed as the **Alert text**. The message can be up to 100 characters long, and can include only the following: Alphanumeric, Whitespace, Period (.), and Underscore (_).
- **Base64-encoded Logo Icon** - In this field, you can specify a Base 64-encoded GIF icon to be displayed instead of the default SonicWall logo.
 - **NOTE:** Make sure this icon is valid and make the size as small as possible. The recommended size is 400x65.
- **Preview** - Click to display the **Web Site Page** preview window. This gives you a chance to verify your configuration and make changes if needed.
 - To set the web block page settings back to default, click **Default Blocked Page**.
 - **NOTE:** The base64-encoded Logo Icon text-field must be left blank.
 - Click **Accept** or **Cancel**.
 - Click **Update** or **Reset** when finished. For Update, a dialog box appears the requests information about the schedule for your updates, and editing the fields selected for the Change creation.

Botnet Filter

The Botnet Filter feature allows you to block connections to or from Botnet command and control servers, and make custom Botnet lists. It also allows you to create a custom message to send when you block a web site. Many of the selections on this page have an (information) icon that you can hover over for a screen tip. The Botnet filter page has the following sections:

NOTE: The Botnet Filtering feature is available on TZ300 series and higher appliances.

Topics:

- [Settings](#)
- [Custom List](#)
- [Web Block Page](#)
- [Dynamic Botnet List Server](#)
- [Dynamic Botnet List](#)

Settings

Configure Botnet settings on the screen that follows. Some of the fields have additional information in a screen tip.

- **Block connections to/from Botnet Command and Control Servers** - All connection attempts to/from Botnet command and control servers are blocked. This option is not selected by default. When this selection is clicked, the next two buttons are available to choose the set of connections to be included in the blocking.
 - **All Connections** - Clicking this button includes all IPs in the blocking. This is the default.

- **Firewall Rule-based** - If this button is clicked, the appliance follows the access rules configured on the firewall. This is not the default mode for Botnet blocking.
 - **Block all connections to public IPs if BOTNET DB is not downloaded** - When the database is not downloaded, clicking this field blocks all public IPs. This option is not selected by default.
 - **Enable Logging** - Selecting this field enables/disables filter event logging.
 - **Enable Custom botnet List** - See the screen tip for the details of how this selection works. This option is not selected by default. If this option is not selected, then only the firewall's country database is searched. If this option is selected, the custom list is searched first, then if the IP address is not resolved, the firewall's country database is searched.
 - **Enable Dynamic Botnet List** - See the screen tip for the details of how this selection works. If an IP address is resolved from the custom Botnet list, it can be identified as either a Botnet. If **Enable Dynamic Botnet List** is enabled, the IP address is looked up against the dynamic botnet list. If not found, the default list from the backend database is searched. If you want to enable the dynamic list, then set up the server from which it is downloaded, as described in the next section. When **Enable Custom Botnet List** is enabled, the custom list takes precedence over the dynamic botnet list. Therefore, an IP in the dynamic botnet list is allowed by the firewall if it is marked as not a botnet in the custom list.
 - **Botnet Exclusion Object** - This field allows you to choose a set of IP addresses to exclude from Botnet filter blocking. All IPs on the selected exclusion list are excluded from blocking. The default exclusion object is **Default Geo-IP and Botnet Exclusion Group**.
 - Click **Reset** to discard your selections, or **Update** to apply them. Clicking **Update** brings up a dialog that requests more information about the schedule and persistence for your changes.
- NOTE:** If you believe that a certain address is marked as a botnet incorrectly, you can go to Botnet IP Status Lookup to report this issue.

Custom List

There are several reasons why you might want to create a custom botnet list. An IP address can be wrongly marked as Botnet, which can cause incorrect or unwanted filtering. A custom Botnet list you create can solve this problem by overriding the Botnet tag for selected IP addresses. For the firewall to use the custom list, you must enable it, as described in the previous section.

- **Search** - This field can be used to search for the IP addresses you want to put on your custom list or to configure.
- **Delete** - Use this button to delete an IP address from your custom list, and allow it to follow the configured Botnet rules. Select the checkbox next to the IP address you wish to delete, then click **Delete**. You can also click **Delete** in the IP address row. A confirmation message appears.
- **Delete multiple entries** - Select the checkboxes of the entries to be deleted. **Delete** becomes available. Click **Delete**. A confirmation message displays. Click **OK**.

- **Delete all entries** - Click the checkbox in the table header. Click **Delete**, and a confirmation message appears. Click **OK**.
- **Add** - Click **Add** to bring up the **Add/Edit Custom Botnet List Object** dialog box to allow you to add an IP address to your custom list.
 - **IP Address** - Fill in the IP address you want to add. Hover over the *i* (information) icon to find out the restrictions applied to this field.
 - **Enabled** - Click the checkbox to enable the IP address on the list.
 - **Comment** - Add a comment if desired.
 - **OK or Cancel** - Click **OK** to apply your addition, or **Cancel** to cancel it.
- **Config/Edit** - Click the **Config/Edit** icon in the **Configure** column to edit the entry. The **Add/Edit** dialog box appears with the selected entry in the IP address field. Make any changes you wish to make.
 - Click **OK**. The **Custom Botnet List** table is updated.

Web Block Page

The Botnet Filter has a message that can be displayed when a user attempts to access a blocked page. You can have the message display detailed information, such as the reason why this IP address is blocked, as well as the IP address and the country from which it was detected. You can also create a custom message and include a custom logo.

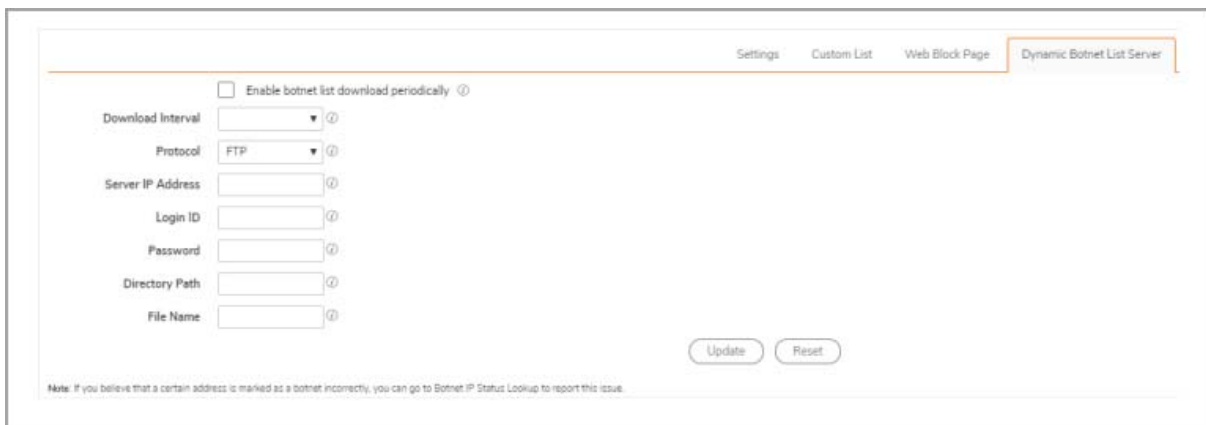
The screenshot shows the configuration page for the Web Block Page. At the top right, there are tabs for 'Settings', 'Custom List', and 'Web Block Page'. The main heading is 'WEB BLOCK PAGE'. There is a checked checkbox for 'Include Geo-IP Filter Block Details'. Below this, the 'Alert text' field contains the message 'This site has been blocked by the network administrator.' The 'Base64-encoded Logo Icon' field contains a long Base64 string. Below the fields, there are buttons for 'Preview', 'Default Blocked Page', 'Update', and 'Reset'. A note at the bottom states: 'Note: If you believe that a certain address is marked as part of a country incorrectly, you can go to Geo-IP Status Lookup to report this issue. This screen applies only to units running SonicOS 6.2.7 Enhanced and above'.

- **Include Botnet Filter Block Details** - Select this option to show blocking details, such as reason for the blocking, the IP address, and the country. When disabled, no information is displayed. By default, this option is selected.
- **Alert Text**
 - To use the default message displayed in the **Alert text** field, **This site has been blocked by the network administrator**, click **Default Blocked Page**.
 - Fill in a custom message to be displayed as the **Alert text**. The message can be up to 100 characters long, and can include only the following: Alphanumeric, Whitespace, Period (.), and Underscore (_).

- **Base64-encoded Logo Icon** - In this field, you can specify a Base 64-encoded GIF icon to be displayed instead of the default SonicWall logo.
 - **NOTE:** Make sure this icon is valid and make the size as small as possible. The recommended size is 400x65.
- **Preview** - Click to display the **Web Block Page** preview window. This gives you a chance to verify your configuration and make changes if needed.
- To set the web block page settings back to default, click **Default Blocked Page**.
 - **NOTE:** The base64-encoded Logo Icon text-field must be left blank.
- Click **Update** when finished. A dialog box appears that requests information about the schedule and the persistence for your updates.

Dynamic Botnet List Server

To connect to a **Dynamic Botnet List Server**, navigate to **Security Services > Botnet Filter | Dynamic Botnet List**. Many of the selections on this page have an *i* (information) icon you can hover over to read more information about this selection.



- **Enable botnet list download periodically** — This selection enables automatic, periodic downloading of the Botnet list from the server are described in the paragraphs that follow.
- **Download Interval** — Specify the download interval (in minutes). The range is 5 to 1440. The firewall downloads the botnet file from the server at the specified interval.
- **Protocol** — FTTP or HTTPS. Specifies the protocol in which the firewall has to communicate with the backend server to get the file.
- **Server IP Address** — Specify the IP address of the sever from which the botlist is to be downloaded.
- **Login ID** — The firewall uses this ID to connect to the Botnet list server.
- **Password** — Enter the password the firewall must use to connect to the Botnet list server.
- **Directory Path** — Specify the directory path. The firewall fetches the botnet file from this location relative to the server's root directory.
- **Filename** — Specify the file name to be downloaded. The firewall looks for this file name on the server.
- Click **Reset** to discard you changes, and **Update** to apply them. If you click **Update**, a dialog box appears requesting more information about the schedule and persistence of your changes.

Dynamic Botnet List

This section gives configuration options for building and editing the dynamic Botnet list.

- **Search** - You can search for an IP Address to add to the list.
- **Download** - This option gives you a prompt asking if you wish to download IPs from the configured list. Selecting **OK** sends you to the **Settings** section to configure the settings for the list.
- **Flush** - This option gives you a prompt asking if you wish to flush the downloaded IPs of Botnet Servers. Selecting **OK** sends you to the **Settings** section to configure the settings for the IPs.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to <https://www.SonicWall.com/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit <https://www.SonicWall.com/support/contact-support>.

About This Document

Legend



WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.



CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.



IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Global Management System Security Services Administration
Updated - December 2019
Software Version - 9.2
232-005142-00 RevA

Copyright © 2019 SonicWall Inc. All rights reserved.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.SonicWall.com/legal>.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.SonicWall.com/en-us/legal/license-agreements>.

Open Source Code

SonicWall is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc." to:

General Public License Source Code Request
SonicWall Inc. Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035