SonicWall® Management Services Security Services

Administration

SONICWALL®

Contents

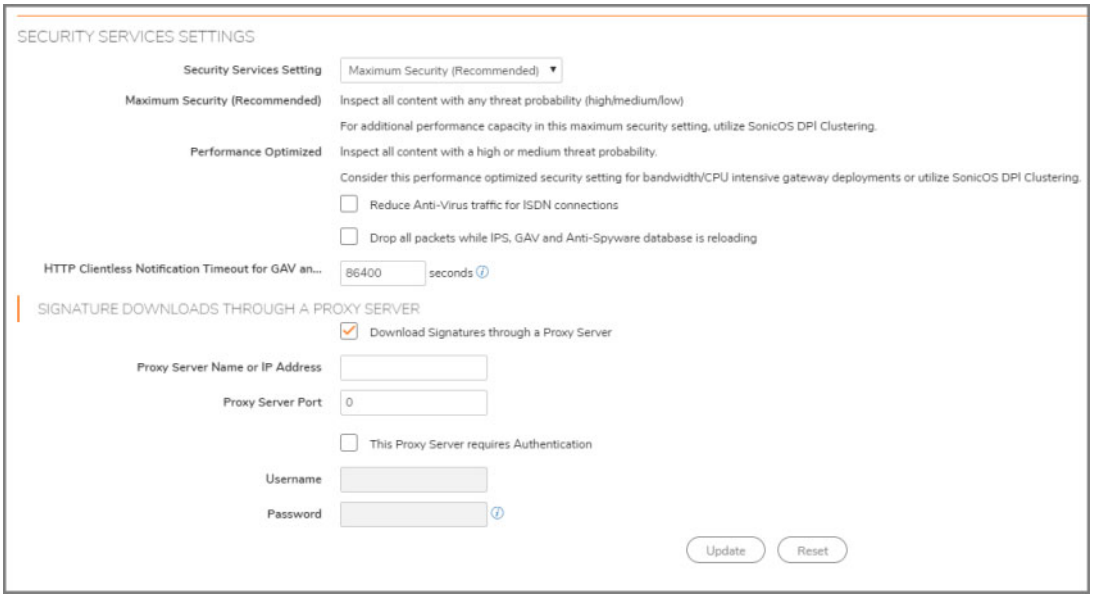
1

Configuring Security Services Settings

This page provides the ability for 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 without compromising privacy.

As shown below, 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 Service Settings

These top-level settings allow operation for maximum security as opposed to operation with less than the highest security level, but with higher network performance levels.

These settings can be made for the global icon, a group, or a SonicWall appliance.

- **Security Services Setting** — There are only two choices:
  - **Maximum Security (Recommended)** — This setting results in the inspection of all traffic, regardless of threat level.
  - **Performance Optimized** — This setting restricts inspection to traffic having high or medium threat level.

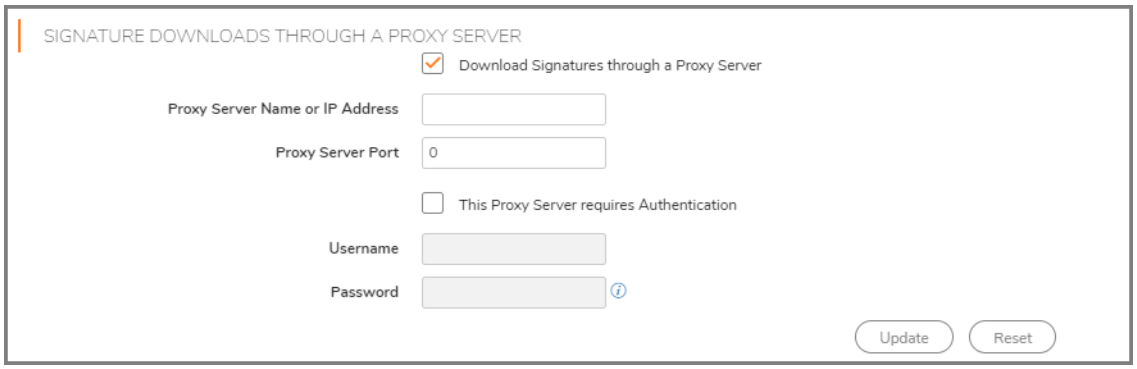
NOTE: SonicOS DPI clustering enables additional performance in the maximum security setting.

There are three other security settings at this level:

- **Reduce Anti-Virus traffic for ISDN connections** — Select this feature to enable the SonicWALL Anti-Virus to check only once a day (every 24 hours) for updates and reduce 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 will wait for a confirmation notification from a client system.

Signature Downloads Through a Proxy Server

Setting up a proxy server is essential to maintain privacy for downloads of threat signatures and appliance registration.



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

1. Select the global icon, a group, or a SonicWall appliance.
2. Expand the **Security Services** tree and click **Settings**.
3. Select **Download Signatures through a Proxy Server**.
4. In the **Proxy Server Name or IP Address** field, enter the hostname or IP address of the proxy server.
5. 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 will remain unchanged.

2

Configuring Client Content Filtering Settings

Configuring the Content Filter Service

The default SonicWall Content Filtering Service (CFS) policy is available with or without a CFS subscription. With a valid CFS subscription, you can create custom CFS policies and apply them to network zones or to groups of users. For example, a school could create one policy for teachers and another for students.

The settings for SonicWall CFS are configured on the **Firewall** > **Content Filter Policies** page in SonicWall Management Service.

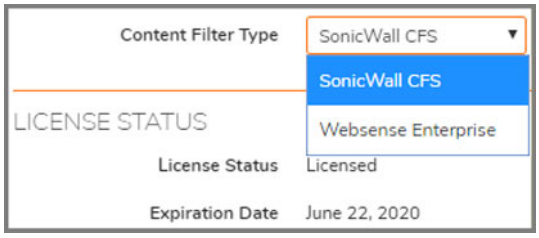
Management Service offers client content filtering protection on a subscription-basis through a partnership with McAfee.

This section describes how to configure Client Content Filtering settings for SonicWall appliances.

Content Filtering Status

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

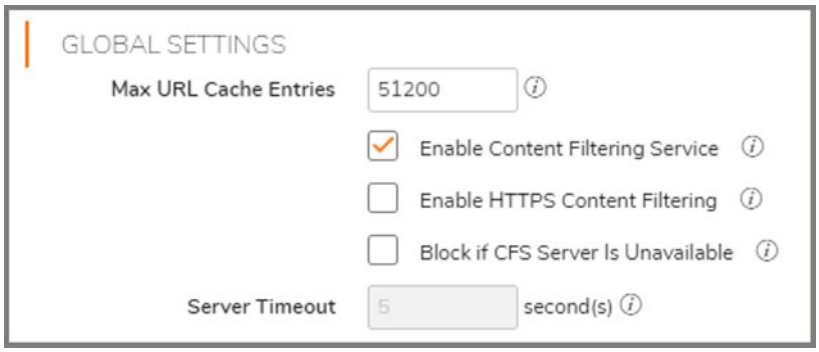
The first sections of the Content Filter page indicate the filtering type, and when the license expires.



- SonicWall CFS — is the standard content filtering service
- 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 which predate 5.9.0.3 support enforcement of web access policies via Websense on HTTP connections only; all HTTPS connection are passed without checking the policy.

Global Settings

This section supports definition of overall CFS policies.



Five settings here include:

- **Max URL Cache Entries** — This defines the number of URL entries that can be cached. The minimum is 25600 and the maximum is 51200.
- **Enable Content Filtering Service** — This setting defaults to Enabled.
- **Enable HTTPS Content Filtering** — Filtering of HTTPS 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 will be silently blocked. Defaults to disabled.
- **Block if CFS Server is Unavailable** — when this box is checked an the CFS server is detected as unavailable, then all web access will be blocked.
- **Server Timeout** — If the firewall does not get a response from the CFS server with this timeout value, then the sever is marked as unavailable. The minimum is 2 seconds, the maximum is 10 seconds, and the default is 5 seconds. This setting is greyed out when **Block if CFS Server is Unavailable** is unmarked.

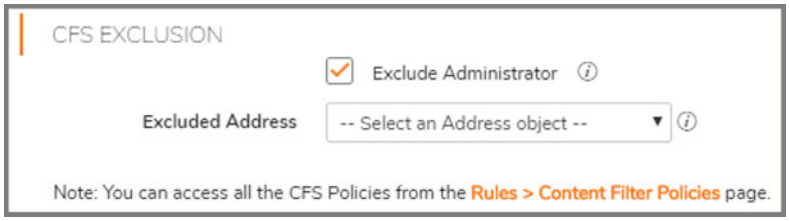
Local CFS Server Settings

If you choose to use a local CFS server rather than one available to the public, use these settings.

- **Enable Local CPS Server** — chooses local CFS server. Defaults to disabled.
- **Primary** and **Secondary Local CFS Servers** — these fields hold IP addresses for local CFS servers.

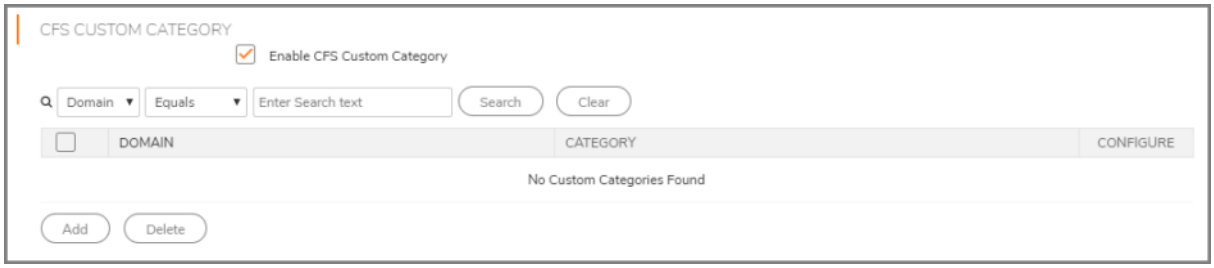
CFS Exclusion

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



- **Excluded Administrator** — all the packets from the administrator will pass through the CFS module if this box is checked. This defaults to enabled.
- **Excluded Address** — the packets of all configured addresses will pass through the CFS module.

This section allows configuration of a custom CFS category entry. CFS allows the administrator not only to create custom policies, but also allows for custom domain name entries to the existing CFS rating categories. This allows for insertion of custom CFS-managed content into the existing and very flexible category structure.



NOTE: For a list of current policies, click the links on this page shown above, or navigate to **Firewall > Content Filter Policies**.

Client CF Enforcement Policies

To configure the Client Content Filtering Enforcement policies:

1. Go to **Security | Security Services > Client CF Enforcement**.
2. Select a grace period for the enforcement to address. 0-5 days.
3. Click **Update**.

Client CF Enforcement Lists

To configure the Client Content Filtering Enforcement Tasks:

1. Go to **Security | Security Services > Client CF Enforcement**.
2. Click the configure icon ( )and select the address object groups from the Client CF Enforcement List.
3. Click **OK**.
4. Click **Update**.

3

Configuring SonicWall Network Anti-Virus

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

This new approach ensures the most current version of the virus definition file is installed and active on each PC on the network, preventing a rogue user from disabling the virus protection and potentially exposing the entire organization to an outbreak. Most importantly, SonicWall Network Anti-Virus offloads the costly and time-consuming burden of maintaining and updating anti-virus software across the entire network.

SonicWall Network Anti-Virus also includes Network Anti-Virus Email Filter to selectively manage inbound Email attachments as they pass through the SonicWall to control the flow of executable files, scripts, and applications into your network.

Management Service 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.

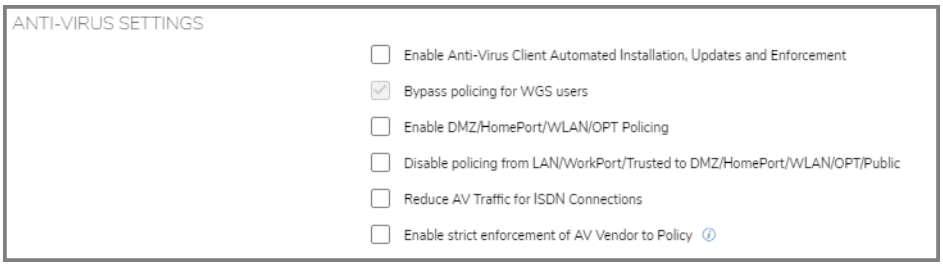
NOTE: SonicWall appliances are entitled to a one-month anti-virus trial subscription.

Anti-Virus Settings

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

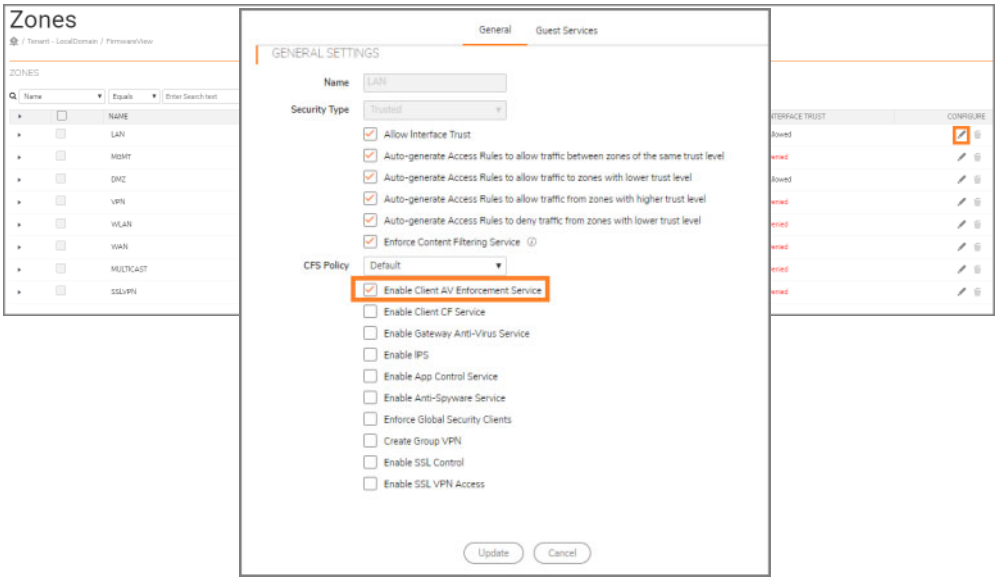
1 Select the global icon, a group, or a SonicWall appliance.

2 Expand the **Security Services** tree and click **Client AV Enforcement**. On the Client AV Enforcement page:

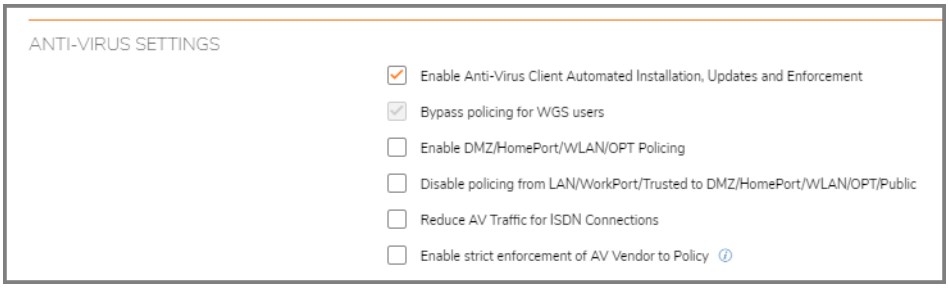


NOTE: The check boxes displayed in the **Anti-Virus Settings** section will vary depending on whether a specific appliance, group or the global icon is selected. .

3 To enable the Client Anti-Virus Service, navigate to the **Network > Zones** page. Click on the pencil edit icon to see the settings for each zone. In the edit box, be sure the **Enable Client AV Enforcement Service** is enabled. After the service is enabled, proceed to the next steps to configure the settings.



4 Select **Enable Anti-Virus Client Automated Installation, Updates and Enforcement**.



5 Clicking **Disable policing from LAN/WorkPort/Trusted** to **DMZ/HomePort/WLAN/OPT/Public** 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. Unchecked, **Disable policing from Trusted to Public...** enforces anti-virus policies on computers located on Trusted zones.

6 To bypass policing to Wireless Guest Services users, click **Bypass policing for WGS users**. This check box is only applicable to SonicOS Standard and is greyed out unless **Enable DMZ/HomePort/WLAN/OPT Policing** is selected.

7 To enforce Anti-Virus protection on the DMZ port or HomePort (if available), select **Enable DMZ/HomePort/WLAN/OPT Policing**.

8 To disable policing from the LAN to the DMZ, select **Disable policing from LAN/WorkPort/Trusted to DMZ/HomePort/WLAN/OPT**.

9 To configure the SonicWall appliance(s) to only check for updates once a day, select **Reduce AV Traffic for ISDN connections**. This is useful for low bandwidth connections or connections that are not “always on.”

10 **Enable Strict Enforcement of AV Vendor to policy** — this field indicates ’Switch McAfee AV to Kaspersky AV’ for clients on Kaspersky enforcement list in Firmware Version 6.1/

Force Update Settings

Management automatically downloads the latest virus definition files. 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** list box.

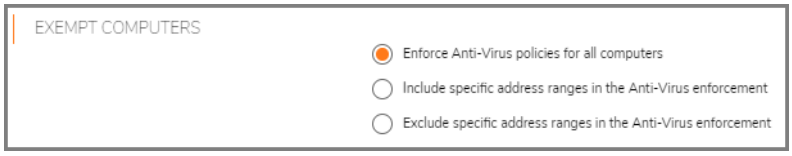
Significant virus events can occur without warning (such as Melissa, ILOVEYOU, and others). When these occur, Management can be configured to block network traffic until the latest virus definition files are downloaded. To configure this feature, determine which types of events will require updating. Then, select **Low Risk**, **Medium Risk**, or **High Risk**.

Force update on alert - SonicWall, Inc. broadcasts virus alerts 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 number of days allowed before forcing update selection. In addition, 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 the virus becomes more and more widespread.
- **High Risk** - To be assigned a high risk rating, it is necessary that a virus is reported frequently in the field. Additionally, the payload must have the ability to cause at least some serious damage. If it causes very serious or unforeseeable damage, high risk might be assigned even with a lower level of prevalence.

Exempt Computers

The Exempt Computers section allows the Management Service administrator to specify address ranges which should be explicitly included or excluded in Anti-Virus enforcement.



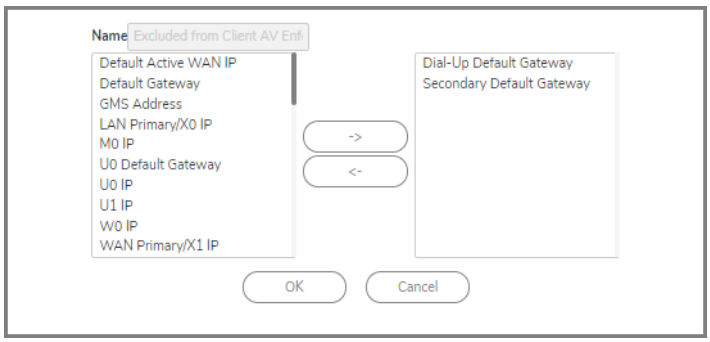
1. Select **Enforce Anti-Virus policies for all computers** to enforce Anti-Virus policies across your entire network. Selecting this option forces computers to install VirusScan ASaP in order to access the Internet or the DMZ. This is the default configuration
2. Select **Include specific address ranges in the Anti-Virus enforcement** to force a specified range of addresses to adhere to Anti-Virus enforcement. Choosing this option allows the administrator to define ranges of IP addresses to receive 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.
3. Select **Exclude specific address ranges in the Anti-Virus enforcement** to exempt a specified range of addresses from Anti-Virus enforcement. See below. Selecting this option allows the administrator 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 entered.

   Address ranges are defined inclusively, with starting and ending addresses.

Client Anti-Virus Enforcement

The Client Anti Virus Enforcement list provides the options to exclude address objects from the Client AV Enforcement list.

You can edit these address objects and groups by clicking the **Edit** (pencil) icon, or add address objects by clicking the **Add** icon for the desired list. In the following example Dial-Up Default Gateway, and Secondary Default Gateway are Address Object that are excluded from anti-virus enforcement.



Select the default enforcement type for computers whose addresses did not fall in any of the client anti-virus enforcement from the drop-down list.

In the above case, this means that computers not on any of the enforcement lists can be set to protected with McAfee or Kaspersky anti-virus scanning or with none at all.

4

Configuring Client CF Enforcement

SonicWall Client 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 these web sites based on their ratings and the policy settings for a user or group.

Businesses can typically control web surfing behavior and content when the browsing is initiated within the perimeter of the security appliance by setting filter policies on the appliance. But when the same device exits the perimeter, the control is lost. Client CF Enforcement kicks into action to address 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 all endpoints have the latest software updates for the ultimate network protection. The client 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 Management Service whose role is to facilitate and verify licensing of CFS and to enable or disable enforcement and configure exclusions and other settings.
- Automatic triggering to install the Client CF Enforcement on any client attempting to access the Internet without the client software installed. Clients will be blocked from accessing Websites until Client CF Enforcement is installed.
- Administration of client policies and client groups using the cloud-based EPRS server accessed from MySonicWall or from Management Service running on the appliance.

Topics:

Enabling and Configuring Client CF Enforcement

This section describes how to enable and configure settings for Client CF Enforcement in Management Service.

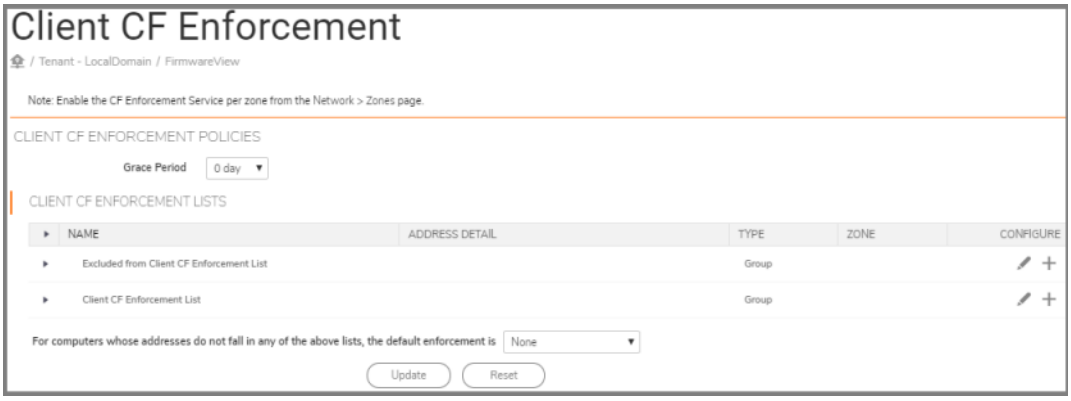
Client CF Enforcement must be enabled on the SonicWall appliance before users will be presented with a Website block page, which prompts the user to install the Client CF Enforcement.

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

Configuring Client CF Enforcement in Security Services

To configure settings for Client CF Enforcement:

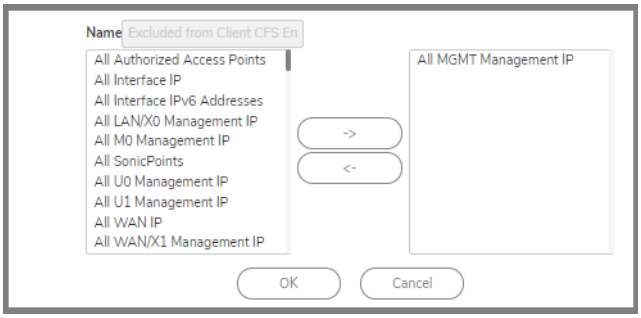
1 Navigate to the **Security | Security Services > Client CF Enforcement** page.



2 Under the **Client CF Enforcement Policies** section, select the number of days from the drop-down list for the **Grace Period** during which CFS enforcement policies remain valid.

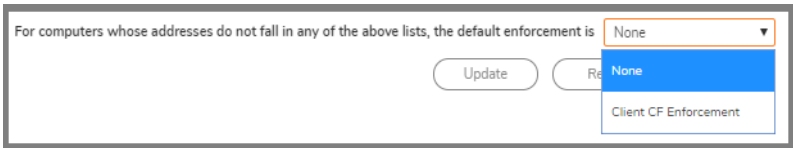
The **Client CF Enforcement Lists** section contains a table including the Client CFS Enforcement List and the Excluded from Client CF Enforcement List.

To configure either of these tables, click the **Configure** icon (the pencil symbol) for the list you wish to configure. The Edit Address Object Group dialog displays. Select from the available list the values to include/not include for the group.

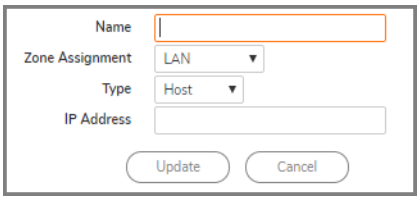


3 For the **Client CF Enforcement List** and **Excluded from Client CF Enforcement List**. If you have made any entries in these lists, you can click the arrow next to the list title to display the entries. To add entries to either list, click the Configure icon in that row.

4 For the field labeled **For computers whose addresses do not fall in any of the above lists, the default enforcement is**, select **Client CF Enforcement** from the drop-down list. This is located below the **Client CF Enforcement Lists** section. Selecting this will prompt all other computers connecting to the Internet through the appliance to install the Enforced Client. You can select **None** from the drop-down list if you only want to enforce the service on computers that you have configured.



5 To add additional addresses to be included or excluded from CF enforcement, click on the **+** icon to the right. Use the dialog box that comes up to set up additional clients for CF enforcement.



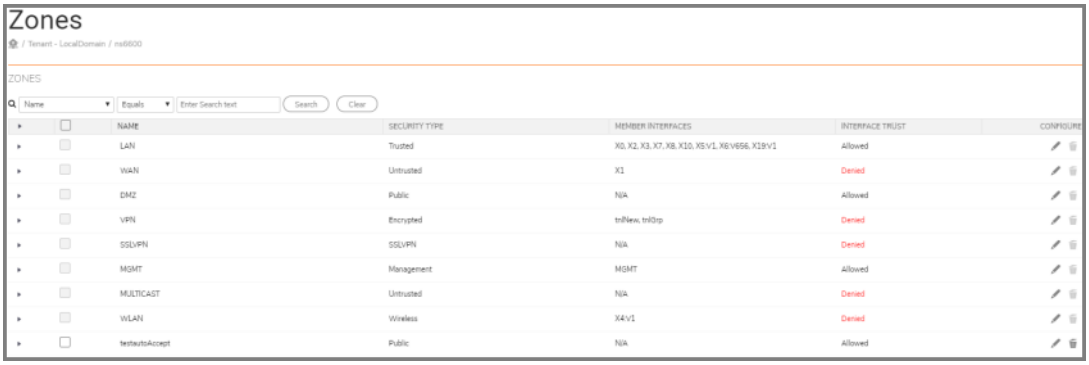
6 Once a new address group is identified, click on **Update**, determine when to have the change take effect and then click on **Accept**.

7 For other changes on Client CFS Enforcement page, click **Update**, determine when to make the changes, and then click **Accept**.

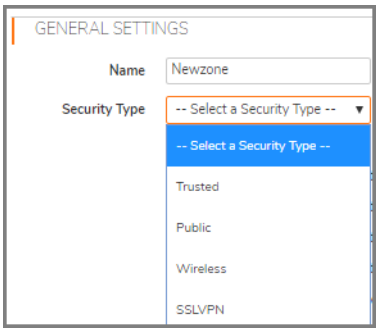
Enabling Client CFS in Network Zones

Client Content Filtering is enforced on a per-zone basis by performing the following steps:

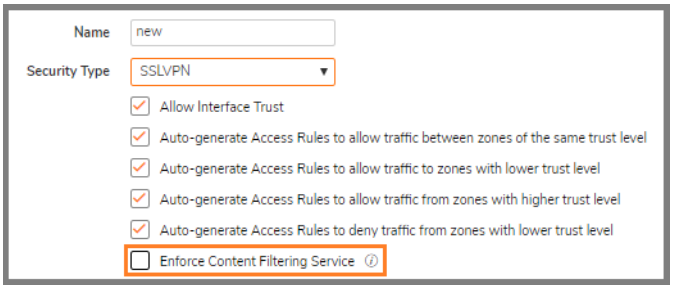
1 At the top of the **Security Services > Client CF Enforcement** page, click the **Network > Zones** link in the **Note**. The **Network > Zones** page displays.



2 To add a new configuration zone, click on **Add**. When the dialog box appears, name the new zone and choose a type of security.

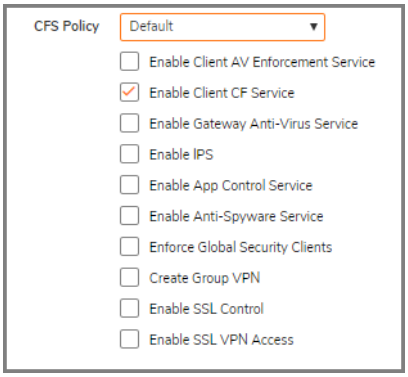


3 Once the name and **Security Type** are defined, choose **Access Rules** and enable **Enforce Content Filtering Service**.

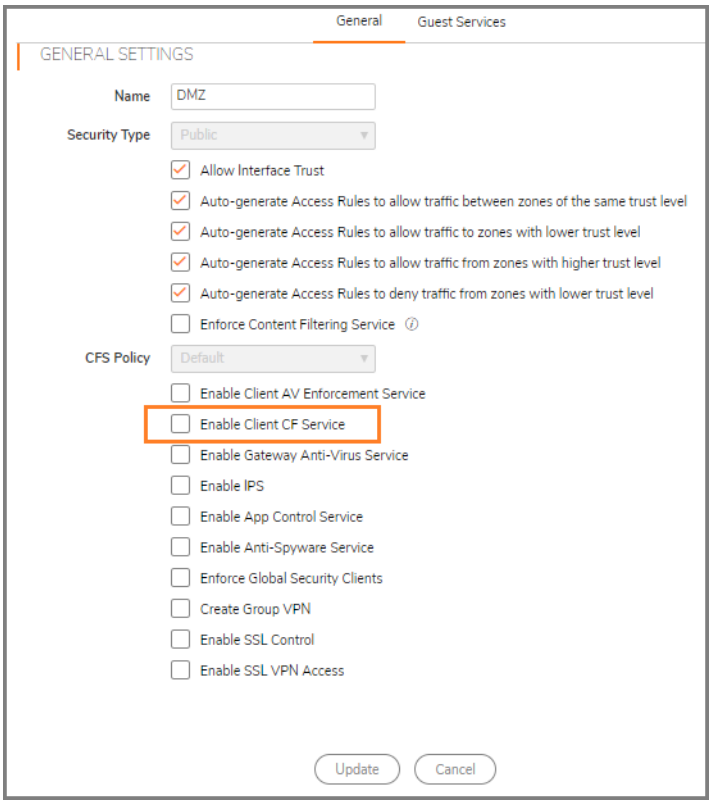


NOTE: The check box is applicable only appliances running SonicOS 6.3 or below. For appliances running on more recent versions, it is only necessary to select Enable Client CF Service.

4 You may choose the Default CFS Policy or enable specific features.

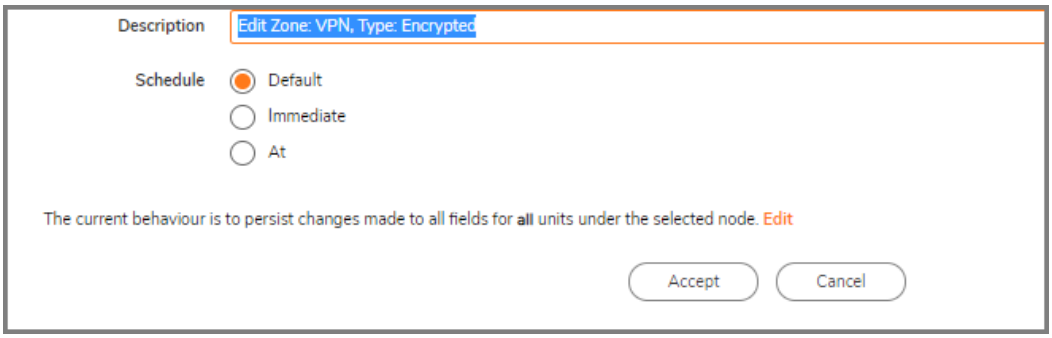


5 To change zone configurations slick the **Configure** button (pencil icon) for the zone on which you want to enforce the Client Content Filtering Service. The dialog box appears.



NOTE: Without adequate permissions, it may not be possible to configure certain zones.

6 When through making changes click on **Update** at the bottom of the **Zone > General Settings** page. The system will respond.



7 Choose a time and click **Accept**.

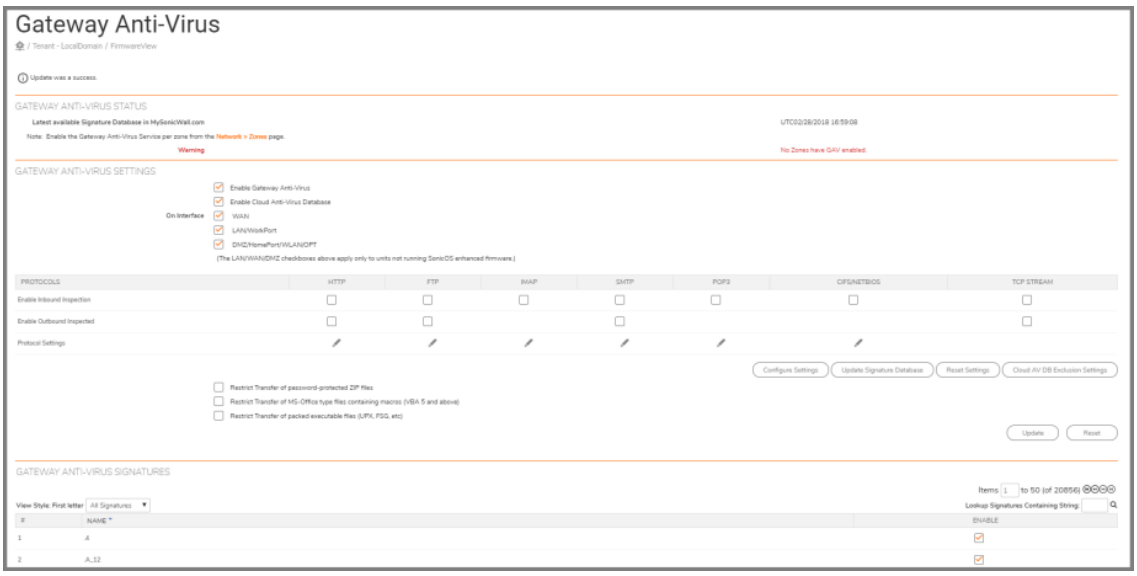
5

Configuring the SonicWall Gateway Anti-Virus

To configure SonicWall Gateway Anti-Virus to begin protecting your network:

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

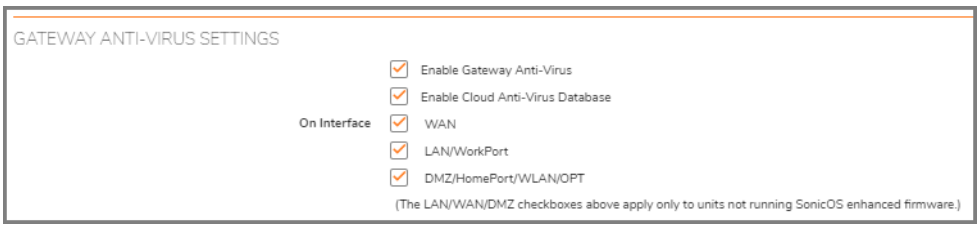
2 Expand the **Security Services** tree and click **Gateway Anti-Virus**. The Gateway AntiVirus screen displays.



3 You can manually update your SonicWall GAV database at any time by clicking **Update** at the bottom of this screen. However, by default, the SonicWall security appliance running SonicWall GAV automatically checks for new signatures once an hour.

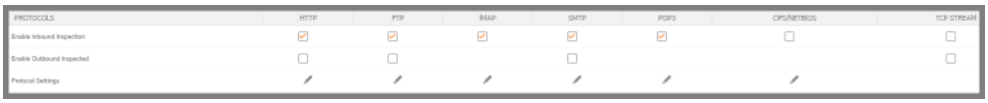
4 Check **Enable Gateway Anti-Virus**.

5 If you have SonicWall Management Service-managed SonicWall firewall appliances running SonicOS Standard, select the interface you want to enable **Gateway Anti-Virus** on. You can select from **WAN**, **LAN/WorkPort**, **DMZ/HomePort/WLAN/OPT**.



6 Check the boxes corresponding to the **Protocols** you wish to enforce Inbound and Outbound inspection on.

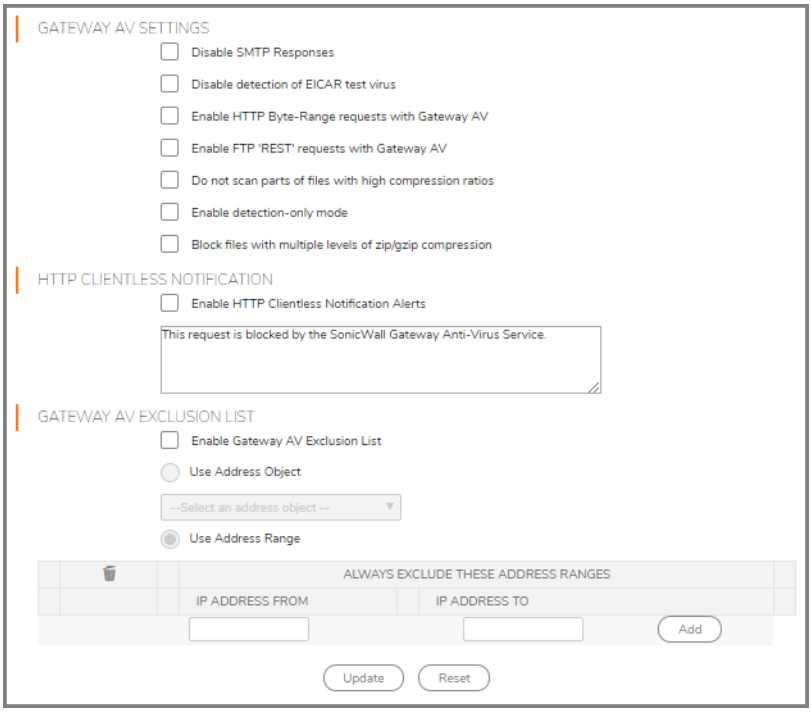
NOTE: If your SonicWall firewall appliance is running SonicOS Enhanced, you must enable Gateway Anti-Virus on the appropriate zone in the **Network > Zones** page before continuing.



Configuring GAV Settings

To configure SonicWall Gateway Anti-Virus settings and notification preferences, select* Configure*:

1 Select **Enable Client Notification Alerts** to send relevant blocked file notifications to users of the SonicWall Desktop Anti-Virus client.



2 Select **Disable SMTP Responses** to suppress the sending of email notifications when viruses are blocked at the gateway.

3 Select **Disable detection of EICAR test virus** to ignore this test file. The EICAR file is a small file (but not actually a real virus) often used to test how virus protection mechanisms respond to a threat.

4 It is not recommended to check the options for **Enable HTTP Byte-Range requests with Gateway AV** or **Enable FTP 'REST' requests with Gateway AV** unless directed to do so by a SonicWall representative.

5 Select **Do not scan parts of files with high compression ratios** to stop the gateway AV from scanning parts of files with high compression ratios.

6 To have the Gateway AV service in detection-only mode, which only detects and logs virus traffic without stopping such traffic, select **Enable detection-only mode**. This setting is not selected by default.

7 Select **Block files with multiple levels of zip/gzip compression** to enable the gateway AV to block files with multiple levels of zip/gzip compression.

8 Select **Enable HTTP Clientless Notification Alerts** to enable alerts about blocked content for clients who do not have SonicWall Client Anti-Virus installed. These alerts are delivered by way of a standard HTML browser window. You might also enter a message below if using this notification type.

9 If **Enable Gateway AV Exclusion List i**s selected, the SonicWall security appliance bypasses AV enforcement for a specified IP range or address object.
Select one of the following:

- **Use Address Object** — Select an address object from the drop-down list.
- **Use Address Range** — Enter an IP address range to exclude.

Configuring GAV Protocols

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

1 Select which types of traffic to **Enable Inbound Inspection** for.

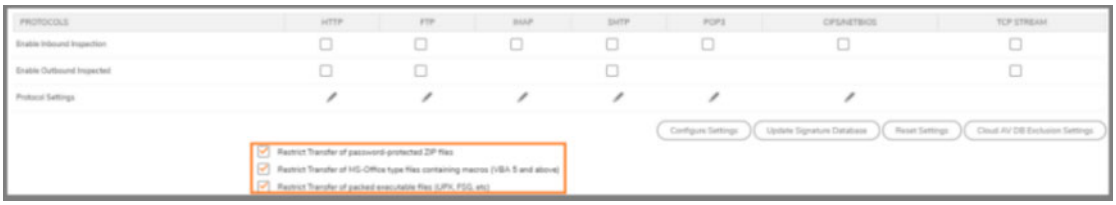
2 To scan outgoing SMTP mail, select to **Enable Outbound Inspection** on SMTP.

3 For more granular control over protocol traffic inspection, click the settings icon  for each of the protocols you choose. The settings window displays and allows you to restrict transfer of the following possibly dangerous file types:

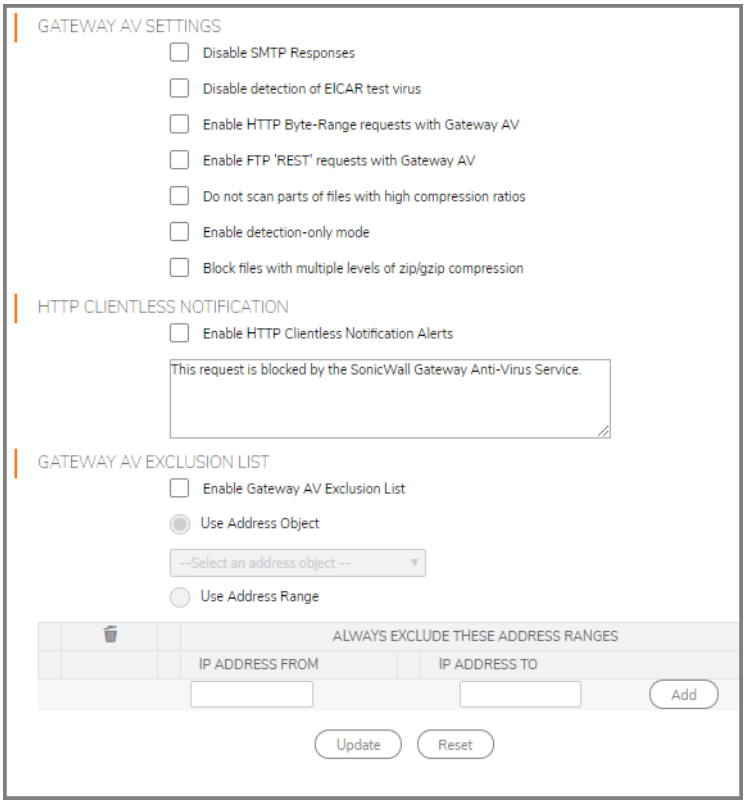
Gateway AV File Restrictions

File Type	Security Issues
Password protected ZIP files	This option only functions on protocols (e.g. HTTP, FTP, SMTP) that are enabled for inspection.
MS-Office type files containing macros	Transfers of any MS Office 97 and above 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 above restrictions may be selected across all protocols for inbound and outbound traffic for the all of the protocols.

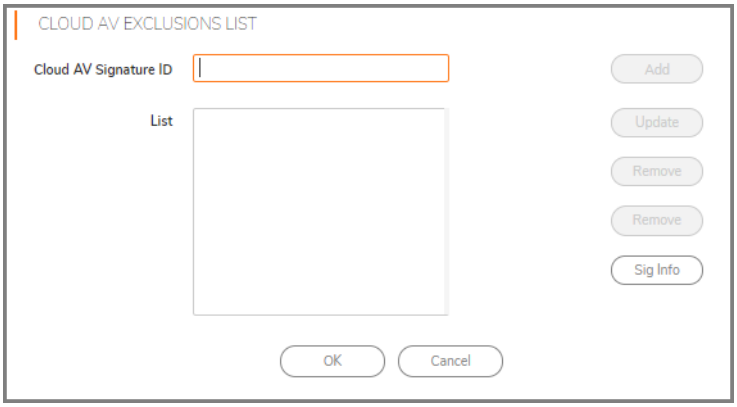


4 Click the **Configure Settings** link. The Gateway AV settings window displays. This window allows you to configure client notification alerts and create a SonicWall GAV exclusion list.



5 To download the latest signature database from mysonicwall.com, click the **Update Signature Database** link.

6 Cloud AV DB Exclusion settings.



7 Click **Update** when you are ready to save your changes.

8 **Reset Settings** causes all firewall AV setting to revert to their settings before the current session.

Viewing SonicWall GAV 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.

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

Displaying Signatures

You can display the signatures in a variety of views using the View Style menu.

Use Search String - Allows you to display signatures containing a specified string entered in the Lookup Signatures Containing String field.

All Signatures - Displays all the signatures in the table, 50 to a page.

0 - 9 - Displays signature names beginning with the number you select from the menu.

A-Z - Displays signature names beginning with the letter you select from menu.

Navigating the Gateway Anti-Virus Signatures Table

The SonicWall GAV signatures are displayed fifty to a page in the **Gateway Anti-Virus Signatures** table. The **Items** field displays the table number of the first signature. If you are displaying the first page of a signature table, the entry might be **Items** 1 to 50 (of 58). Use the navigation buttons to navigate the table.

Searching the Gateway Anti-Virus Signature Database

You can search the signature database by entering a search string in the Lookup Signatures Containing String field at the top right of the table. At the top left, you can choose to search for the first character in the virus signature name from A to Z and 0 to 9.

6

Configuring the SonicWall Anti-Spyware Service

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

Activating the SonicWall Anti-Spyware license on your SonicWall security appliance does not automatically enable the protection.

To configure SonicWall Anti-Spyware to begin protecting your network:

1 Enable SonicWall Anti-Spyware.

2 Specify Spyware Danger Level Protection.

3 Apply SonicWall Anti-Spyware Protection to Zones.

NOTE: For complete instructions on setting up SonicWall Anti-Spyware Service, refer to the SonicWall Anti-Spyware Service Administration Guide available on the SonicWall Web site https://support.sonicwall.com/sonicwall-enforced-anti-virus-and-anti-spyware/mcafee/technical-documents

After you configure these basic anti-spyware protection settings, you can complete additional configuration options to tailor SonicWall Spyware protection for your network environment.

Selecting **Security Services > Anti-Spyware** displays the configuration settings for SonicWall Anti-Spyware on your SonicWall security appliance.

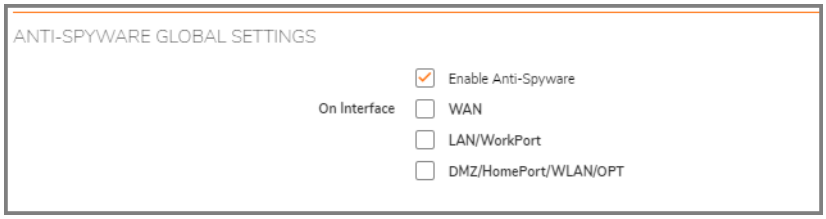
The **Anti-Spyware** page for Management Enhanced is divided into three sections:

- **Anti-Spyware Status** - displays status information on the state of the signature database, your SonicWall Anti-Spyware license, and other information.
- **Anti-Spyware Global Settings** - provides the key settings for enabling SonicWall Anti-Spyware on your SonicWall security appliance, specifying global SonicWall Anti-Spyware protection based on three classes of spyware, and other configuration options.
- **Anti-Spyware Signatures** - shows the status and contents of your signature database.

WARNING: After activating your SonicWall Anti-Spyware license, you must enable and configure SonicWall Anti-Spyware on the SonicWall management interface before anti-spyware policies are applied to your network traffic.

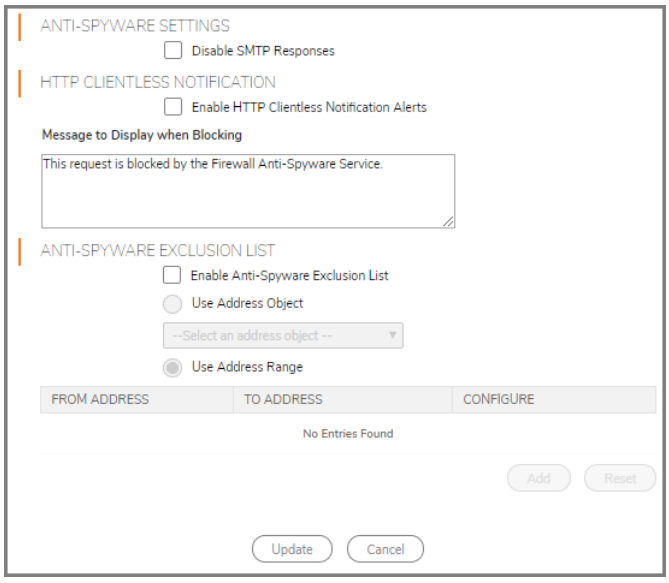
Enabling SonicWall Anti-Spyware

SonicWall Anti-Spyware must be globally enabled on your SonicWall security appliance. Select **Enable Anti-Spyware** (a checkmark is displayed), and then click select the interfaces to activate it on.



Checking **Enable Anti-Spyware** does not automatically start SonicWall Anti-Spyware protection. You must also specify a **Prevent All** action in the **Signature Groups** table to activate anti-spyware on the SonicWall security appliance, and then specify the zones you want to protect on the **Network > Zones** page. You can also select **Detect All** for spyware event logging and alerting.

To configure the Anti-Spyware settings, click on Configure Settings:



1 Click **Enable Client Notification Alerts** if you want clients on your network to receive notifications on their desktop when a HTTP file download is blocked by Anti-Spyware.

> **NOTE:** Desktop client installation is required for this feature to work.

2 Click **Disable SMTP Responses** to suppress the sending of e-mail messages (SMTP) to clients from SonicWall Anti-Spyware when a virus is detected in an e-mail or attachment.

3 If **Enable Anti-Spyware Exclusion List** is selected, the SonicWall security appliance bypasses Anti-Spyware enforcement for a specified IP range or address object.
Select one of the following:

- **Use Address Object** — Select an address object from the drop-down list.
- **Use Address Range** — Enter an IP address range to exclude.

Specifying Spyware Danger Level Protection

SonicWall Anti-Spyware allows you to globally manage your network protection against attacks by simply selecting the class of attacks: **High Danger Level Spyware**, **Medium Danger Level Spyware** and **Low Danger Level Spyware**.

Selecting **Prevent All** and **Detect All** for **High Danger Level Spyware** and **Medium Danger Level Spyware** in the **Signature Groups** table, and then clicking **Apply** protects your network against the most dangerous spyware.

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.

To prevent the log from becoming overloaded with entries for the same attack, enter a value in the **Log Redundancy Filter** field. For example, if you entered a value of 30 seconds and there were 100 attacks during that period of time, only one attack would be logged during that 30 second period.

SonicWall Anti-Spyware also 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 running 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. For more information, refer to the SonicWall Anti-Spyware Administration Guide available on the SonicWall Web site:

https://support.sonicwall.com/sonicwall-enforced-anti-virus-and-anti-spyware/mcafee/technical-documents

Applying SonicWall Anti-Spyware Protection to Zones (Enhanced)

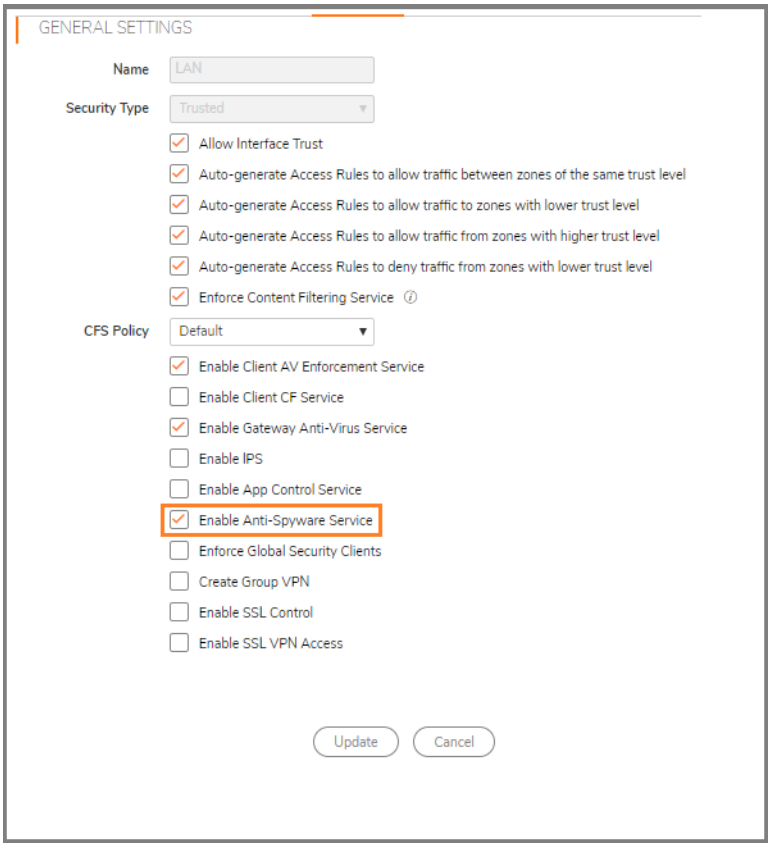
For SonicWall security appliances running SonicOS Enhanced 3.0, you apply SonicWall Anti-Spyware to Zones on the **Network > Zones** page to enforce SonicWall Anti-Spyware not only between each network zone and the WAN, but also between internal zones. For example, enabling SonicWall Anti-Spyware on the LAN zone enforces SonicWall Anti-Spyware on all incoming and outgoing LAN traffic.

In the **Anti-Spyware Status** section of the **Security Services > Anti-Spyware** page, click the **Network > Zones** link to access the **Network > Zones** page or select the **Network > Zones** page. Apply SonicWall Anti-Spyware policies to a zone listed on the **Network > Zones** page.

To enable SonicWall Anti-Spyware on a zone:

1. In the SonicWall security appliance management interface, select **Network > Zones** or from the **Anti-Spyware Status** section, on the **Security Services > Anti-Spyware** page, click the **Network > Zones** link. The **Network > Zones** page is displayed.

2 In the **Configure** column in the **Zone Settings** table, click the **Edit** icon for the zone to which you want to apply SonicWall Anti-Spyware Service. The **Edit Zone** window is displayed.



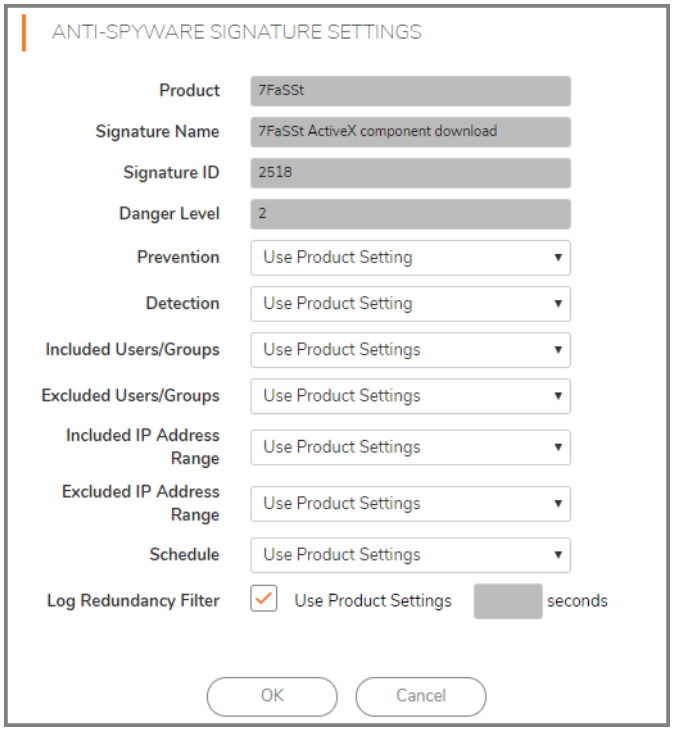
3 Click **Enable Anti-Spyware Service**. A checkmark appears. To disable SonicWall Anti-Spyware Service, uncheck the box.

4 Click **Update**.

You can also enable SonicWall Anti-Spyware for new zones you create on the **Network > Zones** page. Clicking **Add** displays the **Add Zone** window that includes the same settings as the **Edit Zone** window.

Configuring the Anti-Spyware Category

SonicWall Anti-Spyware also 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 Management Service 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. For more information, refer to the *SonicWall Anti-Spyware Administration Guide* available on the SonicWall Web.

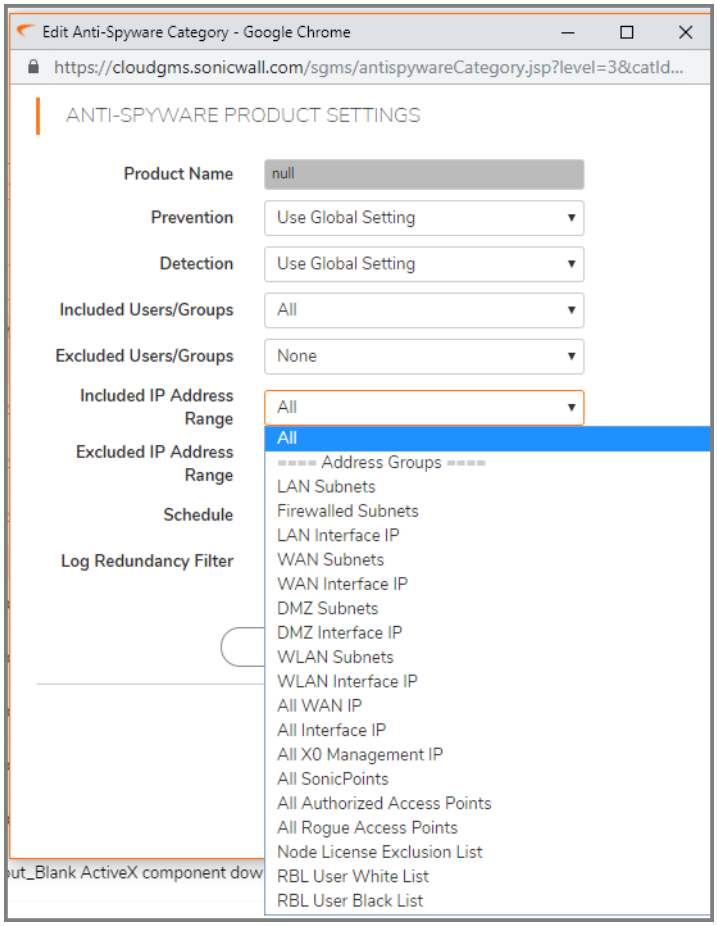


Configure the fields in the Anti-Spyware Product Settings dialog box as described in the following table.

Anti-Spyware Product Settings

Field	Description
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. For more details on the categories, see the table below.

For a bird's eye view of the categories, refer to the following figure:


Edit Anti-Spyware Category - Google Chrome
https://cloudgms.sonicwall.com/sgms/antispywareCategory.jsp?level=3&catId...
ANTI-SPYWARE PRODUCT SETTINGS
Product Name
null
Prevention
Use Global Setting
Detection
Use Global Setting
Included Users/Groups
All
Excluded Users/Groups
None
Included IP Address Range
All
Excluded IP Address Range
Schedule
Log Redundancy Filter
All
Address Groups
LAN Subnets
Firewalled Subnets
LAN Interface IP
WAN Subnets
WAN Interface IP
DMZ Subnets
DMZ Interface IP
WLAN Subnets
WLAN Interface IP
All WAN IP
All Interface IP
All X0 Management IP
All SonicPoints
All Authorized Access Points
All Rogue Access Points
Node License Exclusion List
RBL User White List
RBL User Black List
ut_Blank ActiveX component dow

7

Configuring the SonicWall 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 such as Instant Messaging (IM) or Peer-to-Peer (P2P) applications.

This section contains the following subsections:

Overview of IPS

SonicWall Intrusion Prevention Service (SonicWall IPS) delivers a configurable, high performance Deep Packet Inspection 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 backdoor 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 hacker 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 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 the anomalies in the traffic and reacts to it, 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 Deep Packet Inspection technology also correctly handles TCP fragmented byte stream inspection as if no TCP fragmentation has occurred.

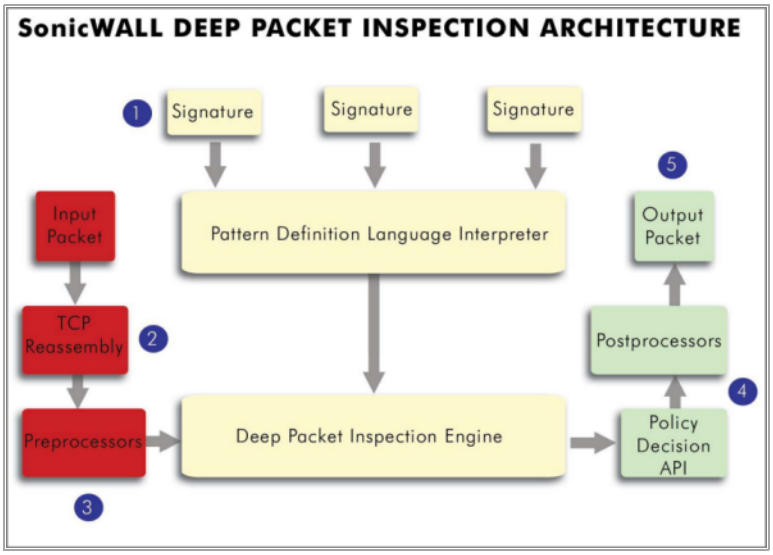
How SonicWall's Deep Packet Inspection Architecture Works

Deep Packet Inspection 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 thus 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:

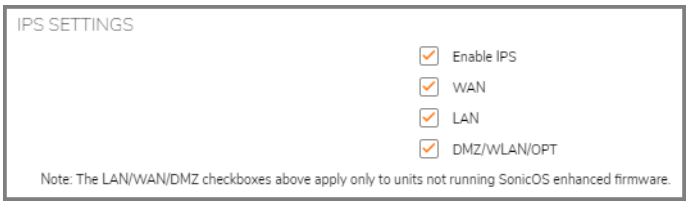
1 Select the global icon, a group, or a SonicWall appliance.

2 Expand the **Security Services** tree and click **Intrusion Prevention**.

The Intrusion Prevention page appears. There are three sections:

- IPSStatus
- IPS Settings
- IPS Policies

3 In IPS Settings, check **Enable IPS** to enable the service.



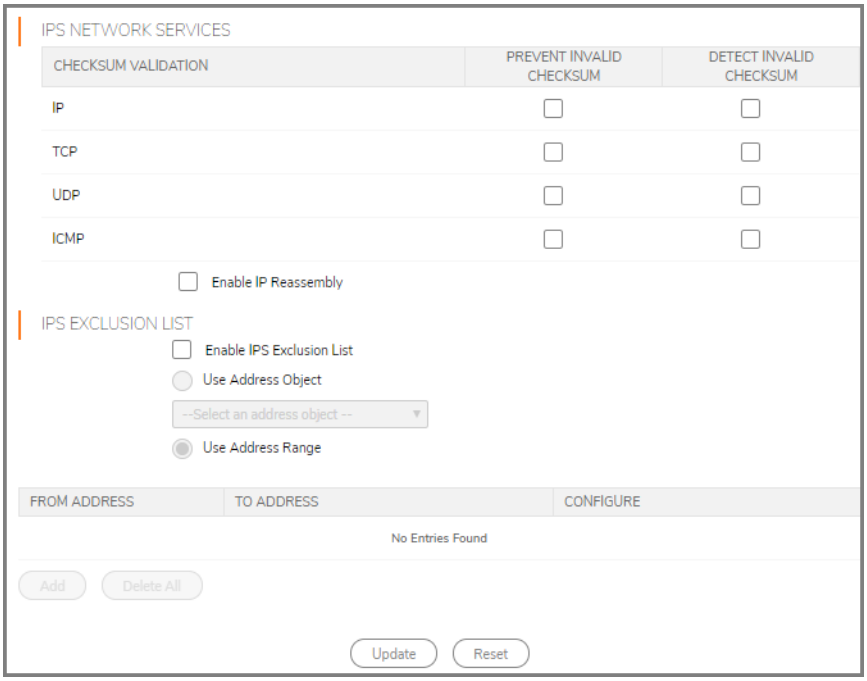
4 Select the check boxes of the interface ports to monitor.

5 Configure the following settings for **High Priority Attacks** in the **IPS Settings** area:

- To to detect, log, and prevent all high priority attacks, select **Prevent All**.
- To detect and log all high priority attacks, select **Detect All**.
- To prevent the log from becoming overloaded with entries for the same attack, enter a value in the **Log Redundancy Filter** 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.

6 Repeat Step 5 for the remaining categories as applicable, including **Medium Priority Attacks, Low Priority Attacks, IM (Instant Messaging) Applications, and P2P (Peer-to-Peer) Applications**.

7 Click **Configuring IPS Settings** to choose one of the following options:



- In the IPS Network section, if **Enable IP Reassembly** is enabled, the SonicWall security appliance reassembles fragmented packets for full application layer inspection.
- If **Prevent Invalid Checksum** is enabled, the SonicWall security appliance automatically drops and resets the connection, to prevent the traffic from reaching its destination.
- If **Detect Invalid Checksum** is enabled, the SonicWall security appliance logs and alerts any traffic, but does not take any action against the traffic. The connection proceeds to its intended destination.
- In the IPS Exclusion List, if **Enable IPS Exclusion List** is selected, the SonicWall security appliance bypasses IPS enforcement for a specified IP range or address object.
  Select one of the following:
  - **Use Address Object** — Select an address object from the drop-down list.
  - **Use Address Range** — Click Add IPS Range, then enter an IP address range to exclude.

8 To force the firmware to download all signatures, click **Update IPS Signature Database**.

9 To reset your IPS settings to the defaults, click **Reset IPS Settings & Policies**.

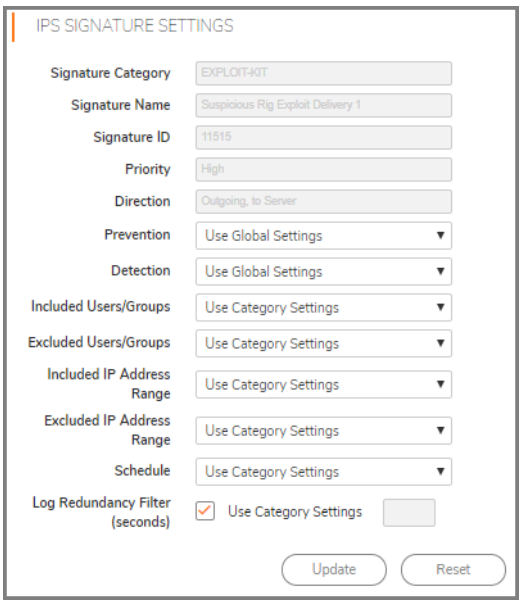
10 When you are finished, click **Update**. The settings are changed for each selected SonicWall appliance. To clear all screen settings and start over, click **Reset**.

Configuring 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 its **Configure** Icon ( ). The Configure IPS dialog box appears.



3 Select whether attack detection for this type of attack is enabled, disabled, or uses the default global settings for the attack category from the **Prevention** list box.

4 Select whether attack prevention for this type of attack is enabled, disabled, or uses the default global settings for the attack category from the **Detection** list box.

5 Select which users or groups to include for this attack type in the **Included Users/Groups** list box.

6 Select which users or groups to exclude for this attack type in the **Excluded Users/Groups** list box.

7 Select an IP address range to include for this attack type in the **Included IP Address Range** list box.

8 Select an IP address range to exclude for this attack type in the **Excluded IP Address Range** list box.

9 Select a time range to enforce attack protection on this attack type from the **Schedule** list box.

10 Enter a timespan (in seconds) to run the **Log Redundancy Filter (seconds)** field, or select **Use Category Settings**.

11 When you are finished, click **Update**. You are returned to the Intrusion Prevention page.

12 Repeat Step 2 through Step 13 for each attack to edit.

13 To reset all attacks to their default settings, click **Reset ALL IPS Settings and Policies**.

Manual Upload of Keyset and Signature Files

Management Service now enables you to manually upload signature files in instances when the Internet is not active on your system. This is useful for SonicWall security appliances that do not have direct Internet connectivity such as those deployed in high-security environments. In these situations, Management Service retrieves the new signatures and then uploads them to the SonicWall security appliance.

To enable manual upload signature files:

1. Navigate to the Console tab.
2. Click the **Management** menu.
3. Click the Management Service Settings (or Cloud Settings options) option. The **Management Service Settings** dialog box displays.
4. Check **Manage Signature Uploads**. This indicates that the SonicWall appliances managed by Management Service cannot directly reach the Internet.

   NOTE: Note that keyset files are uploaded at the time of registering a unit or when there is a change in the user license.

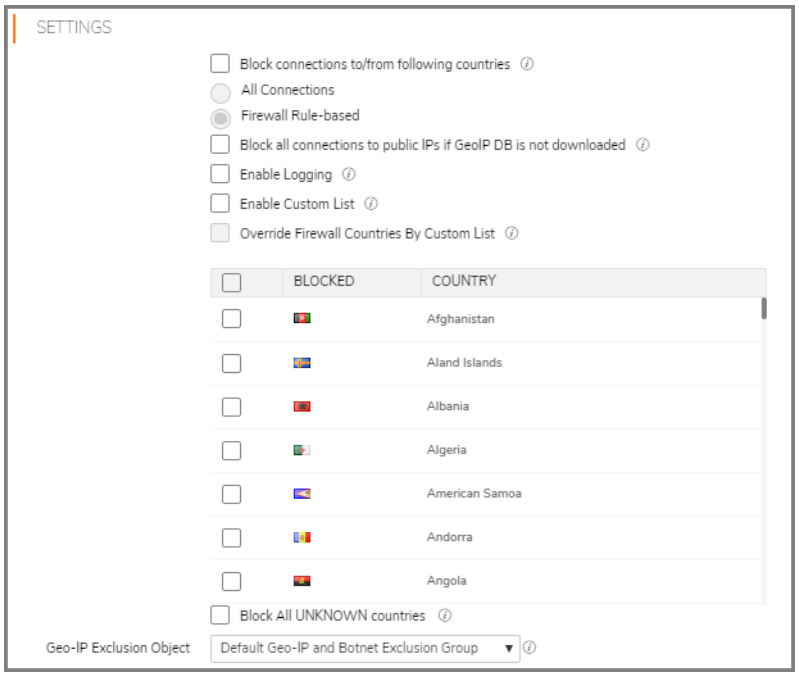
5. In the **Policies** tab, navigate to the **System > Tools** page to upload keyset and signature files.
6. Click **Upload Signatures Now**.

8

Configuring Geo-IP Filters

NOTE: The Geo-IP Filtering feature is available on TZ300 series and above appliances.

The Geo-IP Filter feature allows administrators to block connections to or from a geographic location. The SonicWall appliance uses IP addresses to determine to the location of the connection. The Geo-IP Filter feature also allows you to create custom country lists.



The Geo-IP Filter feature allows you to block connections to or from a geographic location. Management Service uses the IP address to determine to the location of the connection. The Geo-IP Filter feature also allows you to create custom country lists that affect the identification of an IP address.

The Geo-IP Filter feature also allows you to create a custom message when you block a web site.

Topics:

- Configuring Geo-IP Filtering
- Creating a Custom Country List
- Customizing Web Block Page Settings

Configuring Geo-IP Filtering

To configure Geo-IP Filtering:

1 Navigate to **Security Services > Geo-IP Filter** page.

2 To block all connections to and from specific countries, select **Block connections to/from countries listed in the table below**. 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 this behavior for selected IPs, as described in Step 9.

When this option is selected, the next two options become available.

3 Select one of the following two modes for Geo-IP Filtering:

- **All Connections**— All connections to and from the firewall are filtered. This option is selected by default.
- **Firewall Rule-Based Connections** — Only connections that match an access rule configured on the firewall are filtered for blocking. See **Firewall > Access Rules**.

4 To block all connections to public IPs when the Geo-IP database is not downloaded, select **Block all connections to public IPs if Geo-IP DB is not downloaded**. This option is not selected by default.

5 To log Geo-IP Filter-related events, select **Enable logging**. This option is not selected by default.

6 To enable your custom list, select **Enable Custom List**. This option is not selected by default.

If the Enable Custom List checkbox is:

- Not selected, then only the firewall's country database is searched. Go to Step 5.
- Selected, the **Override Firewall Countries By Custom List** checkbox becomes available.

Enabling a custom list by selecting the Enable Custom List checkbox can affect country identification for an IP address. If the **Override Firewall Countries By Custom List** is:

- Not selected also, then country identification is done in this order:
  1) The firewall country database is searched. If the identification is not resolved, then:
  2) The custom country list is searched.
- Also selected, then country identification is done in this order:
  1) The custom country database is searched. If the identification is not resolved, then:
  2) The firewall country list is searched.

In either case, action is taken according to the resolution.

7 Under **Countries**, in the **Blocked Country** table, select the countries to be blocked. By default, no countries are blocked.

TIP: Selecting the checkbox next to **Blocked Country** at the top of the table selects all countries, and then you can select countries to be excluded from blocking by deselecting them.

NOTE: Blocked countries are highlighted.

8 If you want to block any countries that are not listed, select **Block All UNKNOWN countries**. All connections to unknown public IPs are blocked. This option is not selected by default.

9 Optionally, you can configure an exclusion list of all connections to approved IP addresses by doing the following:

- Select an address group from the **Geo-IP Exclusion Object** 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. Click **Geo-IP Status Lookup** to display more information.

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.

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 may not be blocked immediately. As a result, connections to blocked countries may occasionally appear in the App Flow Monitor. However, additional connections to the same IP address are blocked immediately.

10 Click **Update** and then **Accept** to enable your changes.

Creating a Custom Country List

Address Object	Name given to the address object.
Country	Flag icon (if known) and name of country.
Comments	Comment when address object was created.
Configure	Contains an **Edit** icon and a **Delete** icon.

IMPORTANT: 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.

An IP address can be associated with a wrong country, however. This kind of misclassification can cause incorrect/unwanted filtering of an IP address. Having a custom country list can solve this problem by overriding the firewall country associated with a particular IP address.

Topics:

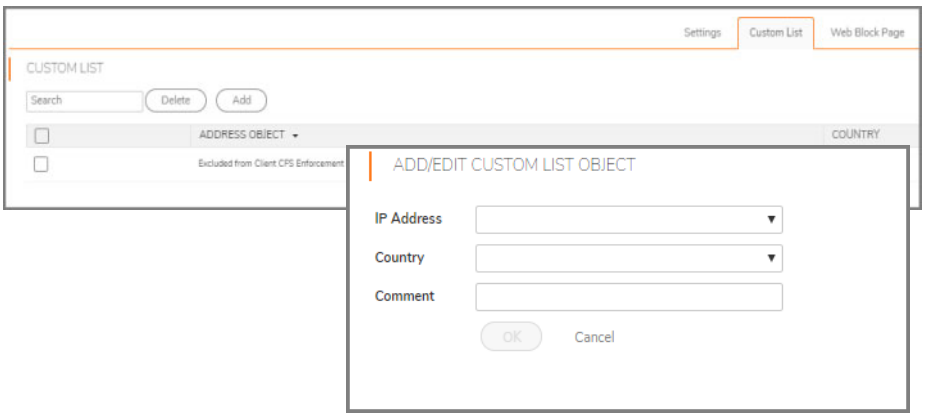
- Creating a Custom List
- Editing a Custom List Entry
- Deleting Custom List Entries

Creating a Custom List

IMPORTANT: For the firewall to use the custom country list, you must enable it as described in Configuring Geo-IP Filtering.

To create a custom country list:

1. Navigate to **Security Services > Geo-IP Filter**.
2. Click the **Custom List** tab.
3. Click **Add**. The **Add/Edit Custom List Object** dialog displays.

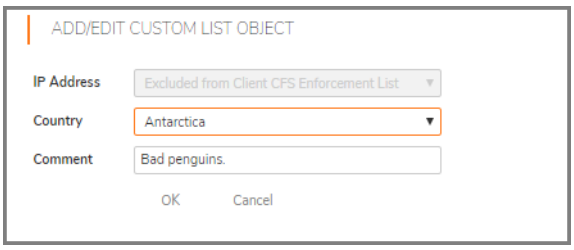


4. Select a country from the **Country** drop-down menu.
5. Optionally, add a comment in the **Comment** field.
6. Click **OK**.

Editing a Custom List Entry

To edit a custom list entry:

1 On the **Custom List** tab, click the **Edit** icon in the **Configure** column for the entry to be edited. The **Add Custom List** dialog displays with the IP address and any comment about the entry.



2 Select the country from the **Country** drop-down menu and make any other changes.

3 Click **OK**. The **Custom List** table is updated.

Deleting Custom List Entries

To delete a custom list entry:

1 Do one of these:

- Click the **Delete** icon in the **Configure** column for the entry.
- Select the checkbox for the entry and then click on the **Delete** icon.

A confirmation message displays.

2 Click **OK**.

To delete multiple entries:

1 Select the checkboxes of the entries to be deleted. **Delete** becomes available.

2 Click **Delete**. A confirmation message displays.

3 Click **OK**.

To delete all entries:

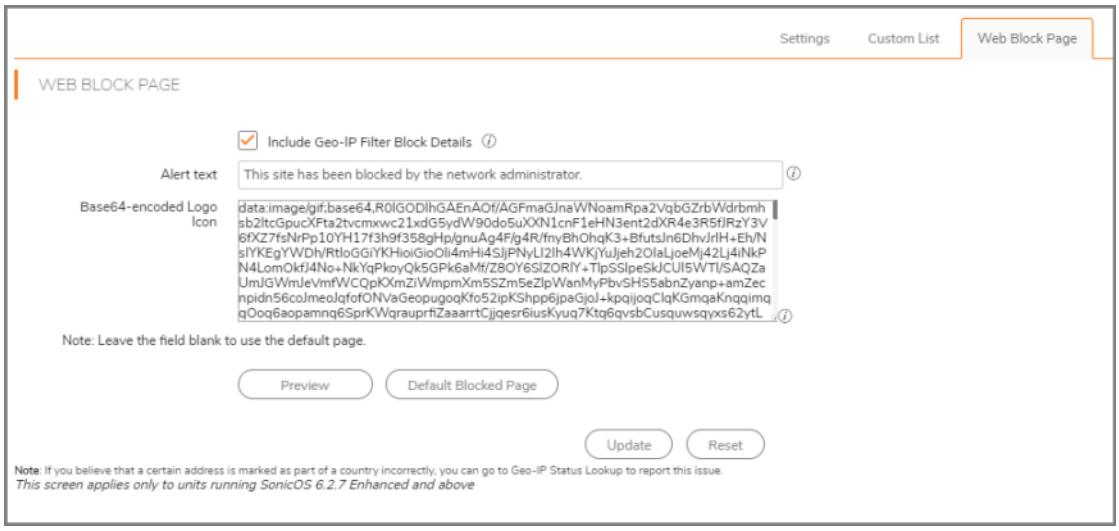
1 Click the checkbox in the table header.

2 Click **Delete**. A confirmation message displays.

3 Click **OK**.

Customizing Web Block Page Settings

The Geo-IP Filter has a default message that is 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 also can create a custom message and include a custom logo.



To create a custom web-block message:

1. Navigate to the **Security Services > Geo-IP Filter** page.
2. Click the **Web Block Page** tab.
3. Ensure **Include Geo-IP Filter Block Details** is selected. When enabled, this option shows block details such as reason for the block, IP address, and country. When disabled, no information is displayed. By default, this option is selected. This option is selected by default.
4. Do one of the following:
   - To use the default message displayed in the Alert text field, This site has been blocked by the network administrator, click **Default Blocked Page** and then go to Step 6.
   - Specify a custom message to be displayed in the **Geo-IP Filter Block** page in the **Alert text** field. Your message can be up to 100 characters long.

     NOTE: The Alert Test field can only contain the following characters: Alphanumeric, Whitespace, Period (.), and Underscore (_).
5. Optionally, in the **Base64-encoded Logo Icon** 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.
6. Click **Preview** to display the Web Site Blocked pop-up window. This gives you a chance to verify your configuration and make changes if needed.
7. 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.
8. Click **Update** when finished.

9

Configuring Botnet Filters

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

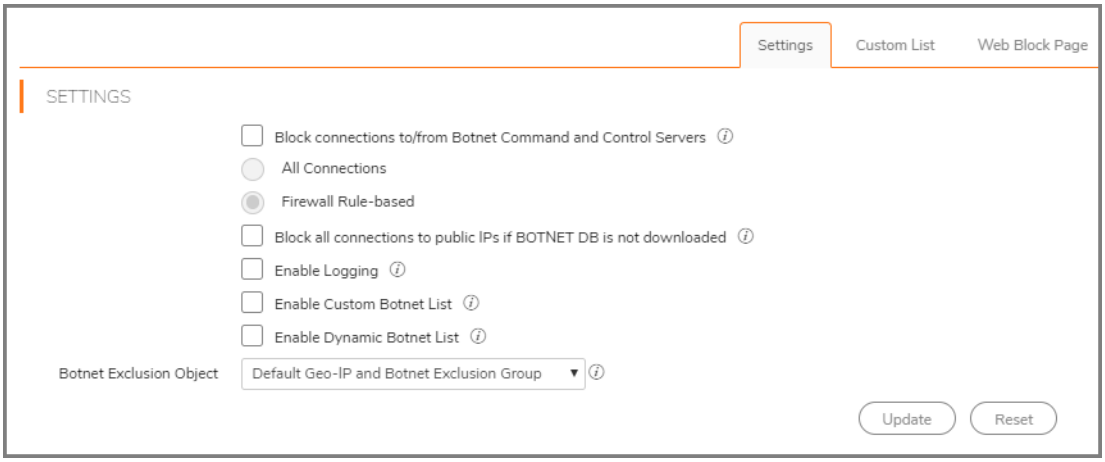
The Botnet Filtering feature allows you to block connections to or from the Botnet command and control servers and to make custom Botnet lists. The Botnet Filtering feature also allows you to create a custom message when you block a web site.

Topics:

Configuring Botnet Filtering

To configure Botnet filtering:

1 Navigate to the **Security Services > Botnet Filter** page.

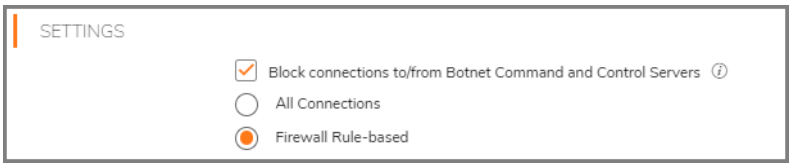


2 To block all servers that are designated as Botnet command and control servers, select **Block connections to/from Botnet Command and Control Servers**. All connection attempts to/from Botnet command and control servers will be blocked. This option is not selected by default.

If this option is selected, the radio buttons and the **Block all connections to public IPs if BOTNET DB is not downloaded** option become available.

To exclude selected IPs from this blocking behavior, use exclusion lists as described in the following steps and/or create a custom Botnet list as described in Connect to Dynamic Botlist Server.

3 If **Block connections to/from Botnet Command and Control Servers** is selected, these options become available:



   a Select one of the following two modes for Botnet Filtering:

      - **All Connections**: All connections to and from the firewall are filtered. This is the default Botnet block mode.
      - **Firewall Rule-based**: Only connections that match an access rule configured on the firewall are filtered.

   b If you want to block all connections to public IPs when the Botnet database is not downloaded, select the **Block all connections to public IPs if BOTNET DB is not downloaded**. This option is not selected by default.

4 Select **Enable logging** to log Botnet Filter-related events.

5 To enable the Custom Botnet List, select **Enable Custom Botnet List**. This option is not selected by default.

   If **Enable Custom Botnet List** is not selected, then only the firewall's country database is searched. Go to Step 4.

   Enabling a custom list by selecting **Enable Custom Botnet List** can affect country identification for an IP address:

   a During Botnet identification, the custom Botnet list is searched first.

   b If the IP address is not resolved, the firewall's Botnet database is searched.

   If an IP address is resolved from the custom Botnet list, it can be identified as either a Botnet IP address or a non-Botnet IP address, and action taken accordingly.

6 Checking **Enable Dynamic Botnet List** will affect the botnet identification, for an IP address, in the following ways.

      - 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 will be searched.

NOTE: If the **Enable Dynamic Botnet List** is enabled, then set up the server from which it is downloaded as described in:

      - When **Enable Custom Botnet List** is enabled, the custom list will take precedence over the dynamic botnet list. So an IP in the dynamic botnet list will be allowed by the firewall if it is marked a not a botnet in the custom list.

7 Optionally, you can configure an exclusion list of all IPs belonging to the configured address object/address group. All IPs belonging to the list are excluded from being blocked. To enable an exclusion list, select an address object or address group from the **Botnet Exclusion Object** drop-down menu.

   The default exclusion object is **Default Geo-IP and Botnet Exclusion Group**.

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.

8 Click **Update** to enable your changes.

Connect to Dynamic Botlist Server

To connect to a Dynamic Botlist Server:

1 Navigate to **Security Services > Botnet Filter**.

2 Click the **Dynamic Botlist Server** tab.

- **Enable botlist download periodically** — Enables automatic downloading of botlist from the server described below.
- **Download Interval** — Specify download interval (in minutes). Range is 5 to 1440. Firewall wil download the botnet file from the server at the specified rate.
- **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 will be downloaded.
- **Login ID** — The firewall will use this ID to connect to the botlist server.
- **Password** — Enter the password the firewall will use to connect to the botlist server.
- **Directory Path** — Specify directory path. The firewall will fetch the botnet file from this location relative to the sever's root directory.
- **Filename** — Specify the file name to be downloaded. The firewall will look for this file name on the server.

When the dialog box is complete, click on the **Update** button.

Creating a Custom Botnet List

Address Object	Name of the address object or address group object.
Comments	Any comments you added about the entry.
Configure	Contains **Edit** and **Delete** icons for the entry.

An IP address can be wrongly marked as Botnet. This kind of misclassification can cause incorrect/unwanted filtering of an IP address. Having a custom Botnet list can solve this problem by overriding the Botnet tag for a particular IP address.

Topics:

Creating a Custom Botnet List

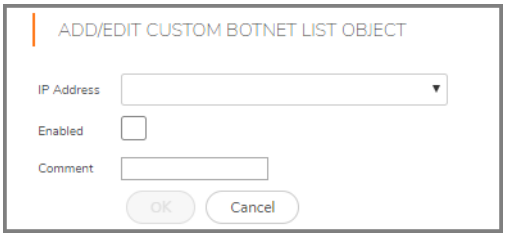
IMPORTANT: For the firewall to use the custom Botnet list, you must enable it as described in Configuring Botnet Filtering.

To create a custom Botnet list:

1 Navigate to **Security Services > Botnet Filter**.

2 Click the **Custom List** tab.

3 Click **Add**. The **Add/Edit Custom Botnet List Object** dialog displays.



4 Select an IP address object from the **IP Address** drop-down menu:

IMPORTANT: An address object cannot overlap any other address objects in the custom country list. Different address objects, however, can have the same country ID.

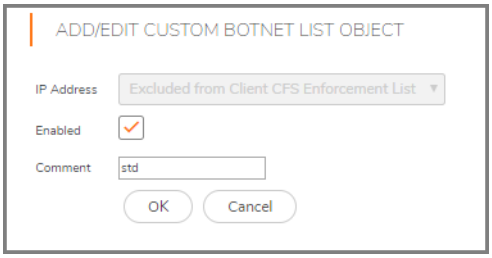
5 Optionally, add a comment in the **Comment** field.

6 Click **OK**.

Editing a Custom Botnet List Entry

To edit a custom Botnet list entry:

1 On the **Custom Botnet Lis**t tab, click the **Edit** icon in the **Configure** column for the entry to be edited. The **Add/Edit Custom Botnet List Object** dialog displays the entry.



2 Make your changes.

3 Click **OK**. The **Custom Botnet List** table is updated.

Deleting Custom Botnet List Entries

To delete a custom Botnet list entry:

1 Do one of these:

- Click the **Delete** icon ( )in the **Configure** column for the entry.
- Select the checkbox for the entry and then click **Delete**.

A confirmation message displays.

2 Click **OK**.

To delete multiple entries:

1 Select the checkboxes of the entries to be deleted. The **Delete** button becomes available.

2 Click the **Delete** button. A confirmation message displays.

3 Click **OK**.

To delete all entries:

1 Click the checkbox in the table header.

2 Click **Delete**. A confirmation message displays.

3 Click **OK**.

Customizing Web Block Page Settings

The Botnet Filter has a default message that is displayed when a page is blocked. You can create a custom message and include a custom logo.

To create a custom message and include a custom logo:

1 Navigate to the **Security Services > Botnet Filter** page.

2 Click the **Web Block Page** tab.

3 Click **Include Botnet Filter Block Details** to allow the user to view the reason for blocking a web page on the Web Site Blocked pop-up window. This option is selected by default.

When enabled, this option shows block details such as reason for the block, IP address, and country. When disabled, this option hides all information.

4 Do one of the following:

- To use the default message displayed in the **Alert text** field, `This site has been blocked by the network administrator.`, click **Default Blocked Page** and then go to Step 5.
- Specify a custom message to be displayed in the Botnet Filter Block page in the **Alert text** field. Your message can be up to 100 characters long.

5 Optionally, in the **Base64-encoded Logo Icon** field, you can specify a Base 64-encoded GIF icon to be displayed as well.

> **NOTE:** Ensure the icon is valid and make the size as small as possible. The recommended size is 400 x 65.

6 To see a preview of your customized message and logo (or the default message and logo), click **Preview**. A warning message displays.

7 Click **OK**. The **Web Site Blocked** message displays.

8 Close the **Web Site Blocked** message.

9 Click **Update**.

10

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.

Management Services Security Services Administration
Updated - November 2018
232-004563-00 Rev A