SonicOSX 7
Action Profiles

Administration Guide

SONICWALL®

Contents

Security Action Profile 3
Adding Security Action Profiles 4
Bandwidth/QoS 4
Anti-Virus 7
Intrusion Prevention 9
Anti-Spyware 10
Botnet Filter 11
Content Filter 11
Block Page and Logging 18
Miscellaneous 19
Editing Security Action Profiles 20
Cloning Security Action Profiles 21
Deleting Security Action Profiles 22
DoS Action Profile 23
Adding DoS Action Profiles 23
Flood Protection 24
DDoS Protection 28
Attack Protection 29
Connection Limiting 30
Editing DoS Action Profiles 32
Cloning DoS Action Profiles 32
Deleting DoS Action Profiles 33
SonicWall Support 34
About This Document 35

1

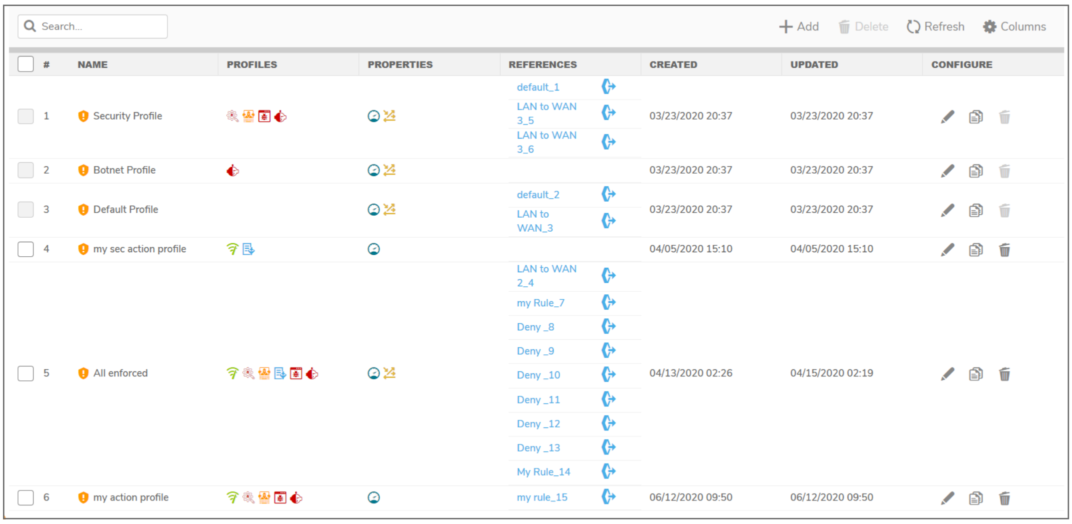
Security Action Profile

Security Rules define how the Security Rule Action policies react to matching events. You can create a custom Security Rule Action object or select the predefined, default action.

To view the Security Action Profiles:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.

   The Security Rule table appears.



#	NAME	PROFILES	PROPERTIES	REFERENCES	CREATED	UPDATED	CONFIGURE
1	Security Profile			default_1 LAN to WAN 3_5 LAN to WAN 3_6	03/23/2020 20:37	03/23/2020 20:37	
2	Botnet Profile				03/23/2020 20:37	03/23/2020 20:37	
3	Default Profile			default_2 LAN to WAN_3	03/23/2020 20:37	03/23/2020 20:37	
4	my sec action profile				04/05/2020 15:10	04/05/2020 15:10	
5	All enforced			LAN to WAN 2_4 my Rule_7 Deny _8 Deny _9 Deny _10 Deny _11 Deny _12 Deny _13 My Rule_14	04/13/2020 02:26	04/15/2020 02:19	
6	my action profile			my rule_15	06/12/2020 09:50	06/12/2020 09:50	

2. From this page, you can **+Add**, **Edit**, **Clone**, or **Delete** Security Rule Action policies. You can also configure **Column** elements.
3. Hover over icons within the columns for additional information about the profile configuration, including enabled and disabled services, policy properties, referenced or associated policies, and so on.

Topics:

- Adding Security Action Profiles
- Editing Security Action Profiles
- Cloning Security Action Profiles
- Deleting Security Action Profiles

Adding Security Action Profiles

Security Action Profiles can include any combination of profile services, with access to each service's configuration within a single page. Within the Security Action Profile pages, you can configure profile options for:

- Bandwidth/QoS
- Anti-Virus
- Intrusion Prevention
- Anti-Spyware
- Botnet Filter
- Content Filter
- Block Page and Logging
- Miscellaneous

Bandwidth/QoS

Application layer bandwidth management (BWM) allows you to create a policy that regulates bandwidth consumption by specific file types within a protocol, while allowing other file types to use unlimited bandwidth. This enables you to distinguish between desirable and undesirable traffic within the same protocol. Application layer bandwidth management is supported for all Application matches, as well as custom Security Action Profiles using HTTP client, HTTP Server, Custom, and FTP file transfer types.

As a best practice, configuring the Bandwidth Management profile settings on the **OBJECT | Profile Objects > Bandwidth** page should always be done before configuring any BWM policies.

Application layer bandwidth management configuration is handled in the same way as Access Rule bandwidth management configuration. However, with Security Action Profiles you can specify all content type, which you cannot do with access rules.

For a bandwidth management use case, as an administrator you might want to limit .mp3 and executable file downloads during work hours to no more than 1 Mbps. At the same time, you want to allow downloads of productive file types such as .doc or .pdf up to the maximum available bandwidth, or even give the highest possible priority to downloads of the productive content. As another example, you might want to limit bandwidth for a certain type of peer-to-peer (P2P) traffic, but allow other types of P2P to use unlimited bandwidth. Application layer bandwidth management allows you to create policies to do this.

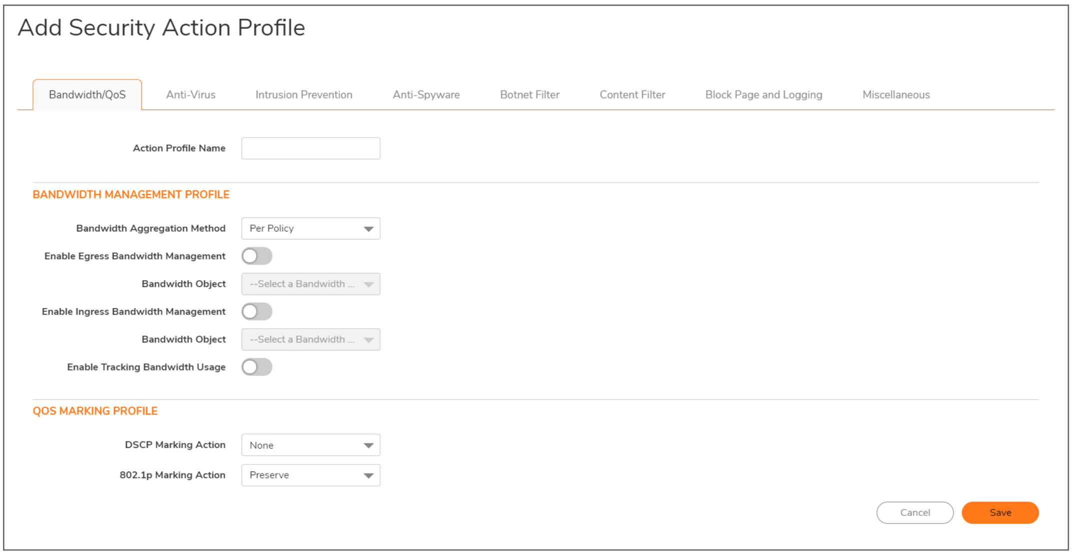
A number of BWM action options are also available in the predefined, default action list. The BWM action options change depending on the Bandwidth Management Type setting on the **OBJECT | Profile Objects > Bandwidth** page.

Guaranteed bandwidth for all levels of BWM combined must not exceed 100%.

To configure a Bandwidth/QoS Security Action Profile:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Click **+Add** or click the **Edit** icon from the **Configure** column.

3. The opening screen is the **Bandwidth/QoS** tab.



Add Security Action Profile

Action Profile Name

BANDWIDTH MANAGEMENT PROFILE

Bandwidth Aggregation Method: Per Policy

Enable Egress Bandwidth Management: ○

Bandwidth Object: --Select a Bandwidth ...

Enable Ingress Bandwidth Management: ○

Bandwidth Object: --Select a Bandwidth ...

Enable Tracking Bandwidth Usage: ○

QOS MARKING PROFILE

DSCP Marking Action: None

802.1p Marking Action: Preserve

4. Enter a friendly **Action Profile Name**.

Bandwidth Management Profile

The Bandwidth Management feature can be implemented in two separate ways:

- **Per Policy Method** – The bandwidth limit specified in a policy is applied individually to each policy.

Example: two policies each have an independent limit of 500kb/s, the total possible bandwidth between those two rules is 1000kb/s.

- **Per Action Aggregate Method** – The bandwidth limit action is applied (shared) across all policies to which it is applied.

Example: two policies share a BWM limit of 500kb/s, limiting the total bandwidth between the two policies to 500kb/s.

1. Select either or both **Enable Egress Bandwidth Management** and **Enable Ingress Bandwidth Management**. These options are not selected by default.
2. Select a **Bandwidth Object** for Ingress or Egress from the drop-down menus.
3. Click **Enable Tracking Bandwidth Usage**.
4. Click **Save**.

You can now associate this **Actions** policy with the **Bandwidth** profile at **OBJECT | Profile Object Objects > Bandwidth**.

QoS Marking Profile

Both 802.1p and DSCP marking as managed by SonicOSX Security Rules, provide four actions: **None**, **Preserve**, **Explicit**, and **Map**. The default action for DSCP is **None** and the default action for 802.1p is **Preserve**.

QoS marking: Behavior describes the behavior of each action on both methods of marking:

QOS MARKING: BEHAVIOR

Action	802.1p (Layer 2 CoS)	DSCP (Layer 3)	Notes
None	When packets matching this class of traffic (as defined by the Security Rule) are sent out the egress interface, no 802.1p tag is added.	The DSCP tag is explicitly set (or reset) to 0.	If the target interface for this class of traffic is a VLAN subinterface, the 802.1p portion of the 802.1q tag is explicitly set to 0. If this class of traffic is destined for a VLAN and is using 802.1p for prioritization, a specific Security Rule using the **Preserve**, **Explicit**, or **Map** action should be defined for this class of traffic.
Preserve	Existing 802.1p tag is preserved.	Existing DSCP tag value is preserved.	
Explicit	An explicit 802.1p tag value can be assigned (0-7) from a drop-down menu that is presented.	An explicit DSCP tag value can be assigned (0-63) from a drop-down menu that is presented.	If either the 802.1p or the DSCP action is set to **Explicit** while the other is set to **Map**, the explicit assignment occurs first, and then the other is mapped according to that assignment.
Map	The mapping setting defined in the **OBJECT | Action Profiles > Security Action Profile** page is used to map from a DSCP tag to an 802.1p tag.	The mapping setting defined in the **OBJECT | Action Profiles > Security Action Profile** page is used to map from an 802.1 tag to a DSCP tag. An additional checkbox is presented to **Allow 802.1p Marking to override DSCP values**. Selecting this checkbox asserts the mapped 802.1p value over any DSCP value that might have been set by the client. This is useful to override clients setting their own DSCP CoS values.	If **Map** is set as the action on both DSCP and 802.1p, mapping only occurs in one direction: if the packet is from a VLAN and arrives with an 802.1p tag, then DSCP is mapped from the 802.1p tag; if the packet is destined to a VLAN, then 802.1p is mapped from the DSCP tag.

Anti-Virus

SonicWall Gateway Anti-Virus (GAV) service delivers real-time virus protection directly on the SonicWall network security appliance by using SonicWall's IPS-Deep Packet Inspection v2.0 engine to inspect all traffic that traverses the SonicWall gateway. Building on SonicWall's reassembly-free architecture, SonicWall GAV inspects multiple application protocols, as well as generic TCP streams, and compressed traffic. Because SonicWall GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding, ZIP, LHZ, and GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis.

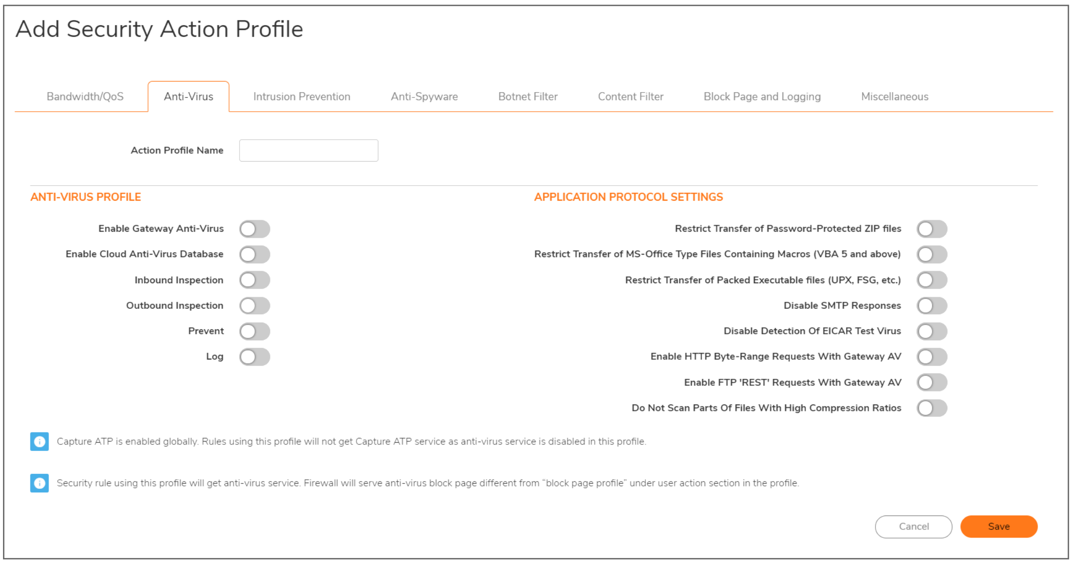
SonicWall GAV delivers threat protection by matching downloaded or emailed files against an extensive and dynamically updated database of threat virus signatures. Virus attacks are caught and suppressed before they travel to desktops. New signatures are created and added to the database by a combination of SonicWall's SonicAlert Team, third-party virus analysts, open source developers, and other sources.

SonicWall GAV can be configured to protect against internal threats as well as those originating outside the network. It operates over a multitude of protocols including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications, and dozens of other stream-based protocols, to provide you with comprehensive network threat prevention and control. Because files containing malicious code and viruses can also be compressed and therefore inaccessible to conventional anti-virus solutions, SonicWall GAV integrates advanced decompression technology that automatically decompresses and scans files on a per-packet basis.

SonicWall GAV parses supported email protocols for the header fields To, CC, and BCC. The information in these fields are displayed and logged in Capture ATP for both sender and receiver.

To configure a Anti-Virus Security Action Profile:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Click **+Add** or click the **Edit** icon from the **Configure** column.
3. Click the **Anti-Virus** tab.



Action Profile Name

ANTI-VIRUS PROFILE

Enable Gateway Anti-Virus ○
Enable Cloud Anti-Virus Database ○
Inbound Inspection ○
Outbound Inspection ○
Prevent ○
Log ○

APPLICATION PROTOCOL 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.) ○
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 ○

Capture ATP is enabled globally. Rules using this profile will not get Capture ATP service as anti-virus service is disabled in this profile.

Security rule using this profile will get anti-virus service. Firewall will serve anti-virus block page different from "block page profile" under user action section in the profile.

4. Enter a friendly **Action Profile Name**.

5. Select **Enable Gateway Anti-Virus** to enable SonicWall Gateway Anti-Virus.

   ⓘ **NOTE:** You must specify the zones you want SonicWall Gateway Anti-Virus protection on the **NETWORK | System > Interfaces** page.

6. If your Anti-Virus software exists in the Cloud, select **Enable Cloud Gateway Anti-Virus Database** to enable SonicWall Anti-Virus protection.
7. Enable **Inbound Inspection**. By default, SonicWall Gateway Anti-Virus inspects all inbound HTTP, FTP, IMAP, SMTP and POP3 traffic. Within the context of SonicWall Gateway Anti-Virus, the enabling the **Inbound Inspection** protocol traffic handling refers to:
   - Non-SMTP traffic initiating from a Trusted, Wireless, or Encrypted zone destined to any zone.
   - Non-SMTP traffic from a Public zone destined to an Untrusted zone.
   - SMTP traffic initiating from a non-Trusted zone destined to a Trusted, Wireless, Encrypted, or Public zone.
   - SMTP traffic initiating from a Trusted, Wireless, or Encrypted zone destined to a Trusted, Wireless, or Encrypted zone.
8. Enable **Outbound Inspection** for HTTP, FTP, SMTP, and TCP traffic
9. You can restrict the transfer of files with specific attributes by enabling **Prevent**. **Prevent** restricts data file transfers for each protocol, except the TCP Stream.
10. Enable **Log** to keep a record of your SonicWall Gateway Anti-Virus traffic.

Application Protocol Settings

1. **Restrict Transfer of password-protected Zip files -** Disables the transfer of password protected ZIP files over any enabled protocol. This option only functions on protocols (for example, HTTP, FTP, SMTP) that are enabled for inspection.
2. **Restrict Transfer of MS-Office type files containing macros (VBA 5 and above) -** Disables the transfers of any MS Office 97 and above files that contain VBA macros.
3. **Restrict Transfer of packed executable files (UPX, FSG, etc.) -** Disables the transfer of packed executable files.

   Packers are utilities that 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.

   SonicWall Gateway Anti-Virus currently recognizes the most common packed formats: UPX, FSG, PKLite32, Petite, and ASPack. Additional formats are dynamically added along with SonicWall Gateway Anti-Virus signature updates.
4. To suppress the sending of e-mail messages (SMTP) to clients from SonicWall Gateway Anti-Virus when a virus is detected in an e-mail or attachment, select **Disable SMTP Responses**. This option is not selected by default.
5. The EICAR Standard Anti-Virus Test file is a special virus simulator file that checks and confirms the correct operation of the SonicWall Gateway Anti-Virus service. To suppresses the detection of the EICAR, select **Disable detection of EICAR Test Virus**. This option is selected by default.
6. To allow the sending of byte serving, the process of sending only a portion of an HTTP message or file, select **Enable HTTP Byte-Range requests with Gateway AV**. This option is selected by default.

The SonicWall Gateway Anti-Virus security service, by default, suppresses the use of HTTP Byte-Range requests to prevent the sectional retrieval and reassembly of potentially malicious content. This is done by terminating the connection and thus preventing the user from receiving the malicious payload. By enabling this setting you override this default behavior.

1. To allow the use of the FTP REST request to retrieve and reassemble sectional messages and files, select **Enable FTP 'REST' requests with Gateway AV**. This option is selected by default.

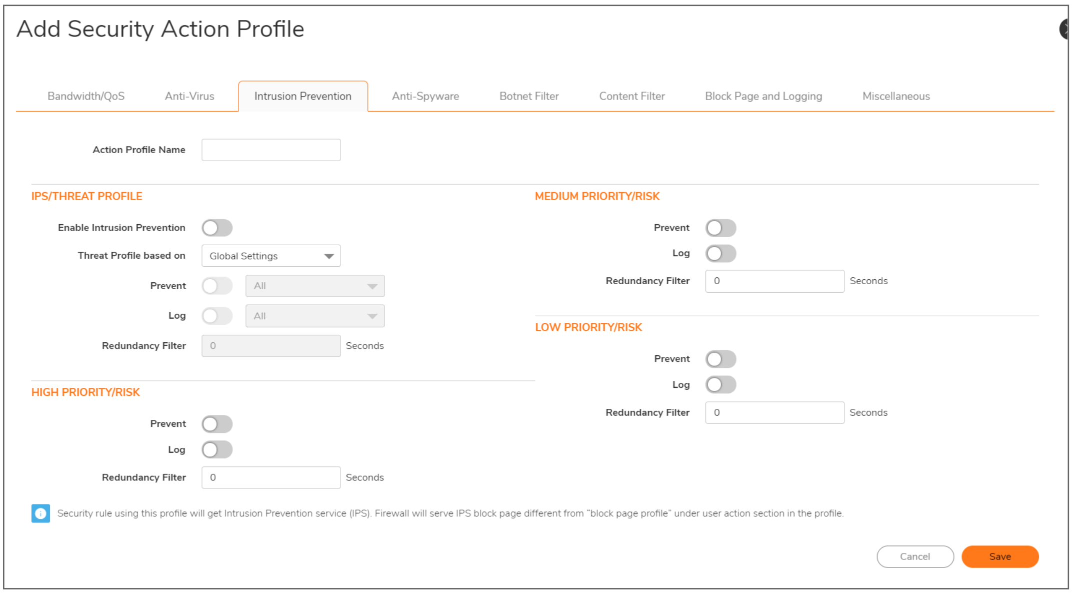
   The Gateway Anti-Virus service, by default, suppresses the use of the FTP 'REST' (restart) request to prevent the sectional retrieval and reassembly of potentially malicious content. This is done by terminating the connection and thus preventing the user from receiving the malicious payload. By enabling this setting you override this default behavior.
2. To suppresses the scanning of files, or parts of files, that have high compression rates, select **Do not scan parts of files with high compression rates**. This option is selected by default.
3. To block files containing multiple levels of zip and/or gzip compression, select **Block files with multiple levels of zip/gzip compression**. This option is not selected by default.

Intrusion Prevention

In this section you can create Intrusion Prevention Action objects to be used along with the Intrusion Preventions created at **OBJECT | Profile Objects > Intrusion Prevention**.

To configure the Intrusion Prevention tab:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Click **+Add** or click the **Edit** icon from the **Configure** column for the Action you would like to modify.
3. Click the **Intrusion Prevention** page.


Add Security Action Profile

Action Profile Name

IPS/THREAT PROFILE

Enable Intrusion Prevention ○

Threat Profile based on: Global Settings

Prevent ○ All

Log ○ All

Redundancy Filter: 0 Seconds

HIGH PRIORITY/RISK

Prevent ○

Log ○

Redundancy Filter: 0 Seconds

MEDIUM PRIORITY/RISK

Prevent ○

Log ○

Redundancy Filter: 0 Seconds

LOW PRIORITY/RISK

Prevent ○

Log ○

Redundancy Filter: 0 Seconds

Security rule using this profile will get Intrusion Prevention service (IPS). Firewall will serve IPS block page different from “block page profile” under user action section in the profile.

4. Enter a friendly **Action Profile Name**.
5. Select **Enable Intrusion Prevention** to enable the SonicWall Threat Prevention Service (IPS).

6. Select whether to build this Action object using **Global Settings** or your own **Profile Settings**.

   ⓘ **NOTE:** Selecting **Profile Settings** grays out the Low, Medium, and High Priority/Risk options because your Threat Protection Profile addresses those capabilities.

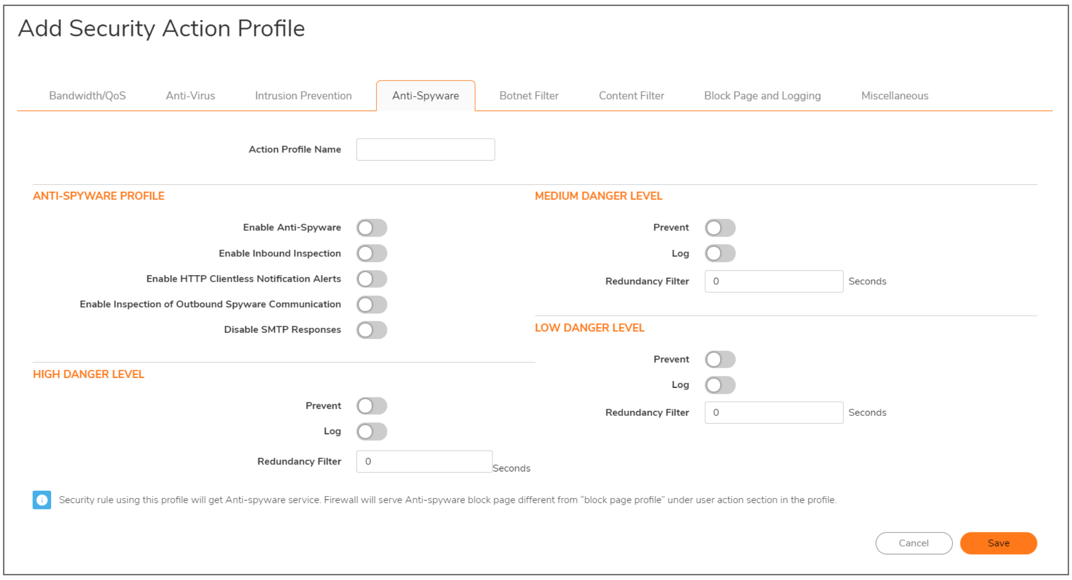
7. Select the remaining options based on your needs to **Prevent**, **Log**, and for how long to use the **Redundancy Filters**.
8. Click **Save**.

Anti-Spyware

In this section you can create Anti-Spyware Security Action Profile objects.

To configure an Anti-Spyware Security Action Profile:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Click **+Add** or click the **Edit** icon from the **Configure** column for the Action you would like to modify.
3. Click the **Anti-Spyware** tab.



Add Security Action Profile

Action Profile Name

ANTI-SPYWARE PROFILE

Enable Anti-Spyware ○
Enable Inbound Inspection ○
Enable HTTP Clientless Notification Alerts ○
Enable Inspection of Outbound Spyware Communication ○
Disable SMTP Responses ○

HIGH DANGER LEVEL

Prevent ○
Log ○
Redundancy Filter 0 Seconds

MEDIUM DANGER LEVEL

Prevent ○
Log ○
Redundancy Filter 0 Seconds

LOW DANGER LEVEL

Prevent ○
Log ○
Redundancy Filter 0 Seconds

Security rule using this profile will get Anti-spyware service. Firewall will serve Anti-spyware block page different from “block page profile” under user action section in the profile.

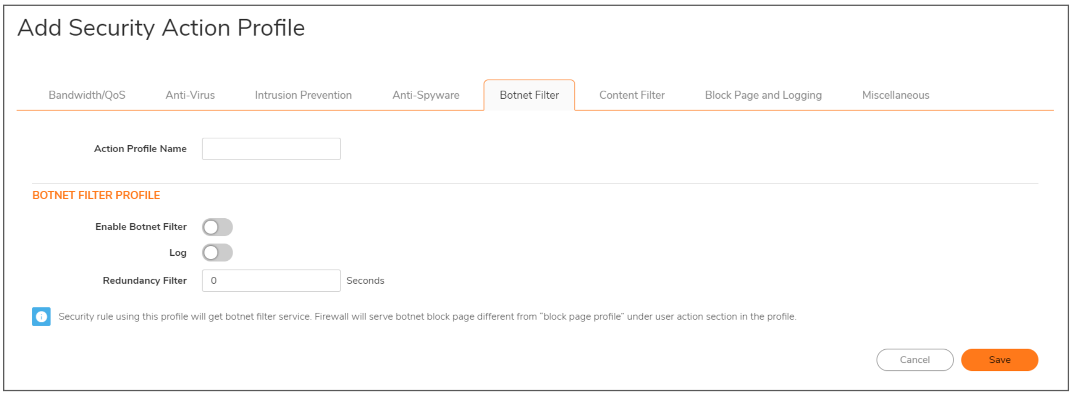
4. Enter a friendly **Action Profile Name**.
5. Select **Enable Anti-Spyware** to activate SonicWall's Anti-Spyware protection.
6. Select **Enable Inbound Inspection** to make inbound traffic available for inspection.
7. Enable **HTTP Clientless Notification Alerts**to show an error message when blocking a request.
8. Enable **Inspection of Outbound Spyware Communication** to make outbound traffic available for inspection.
9. Click **Disable SMTP Responses** to suppress the sending of email messages (SMTP) to clients from SonicWall Anti-Spyware when a virus is detected in an email or attachment.
10. Select the remaining options based on your needs to **Prevent**, **Log**, and for how long to use the **Redundancy Filters**.

Botnet Filter

In this section you can create a Botnet Filtering Security Action Profile.

To configure the Botnet Filter Security Action Profile:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Click **+Add** or click the **Edit** icon from the **Configure** column for the Action you would like to modify.
3. Click the **Botnet Filter** tab.



Add Security Action Profile

Action Profile Name

BOTNET FILTER PROFILE

Enable Botnet Filter ○

Log ○

Redundancy Filter 0 Seconds

Security rule using this profile will get botnet filter service. Firewall will serve botnet block page different from "block page profile" under user action section in the profile.

4. Enter a friendly **Action Profile Name**.
5. Select **Enable Botnet Filter** to activate SonicWall's Botnet Filtering service.
6. Select the remaining options based on your needs to **Log** and for how long to use the **Redundancy Filters**.
7. Click **Save**.

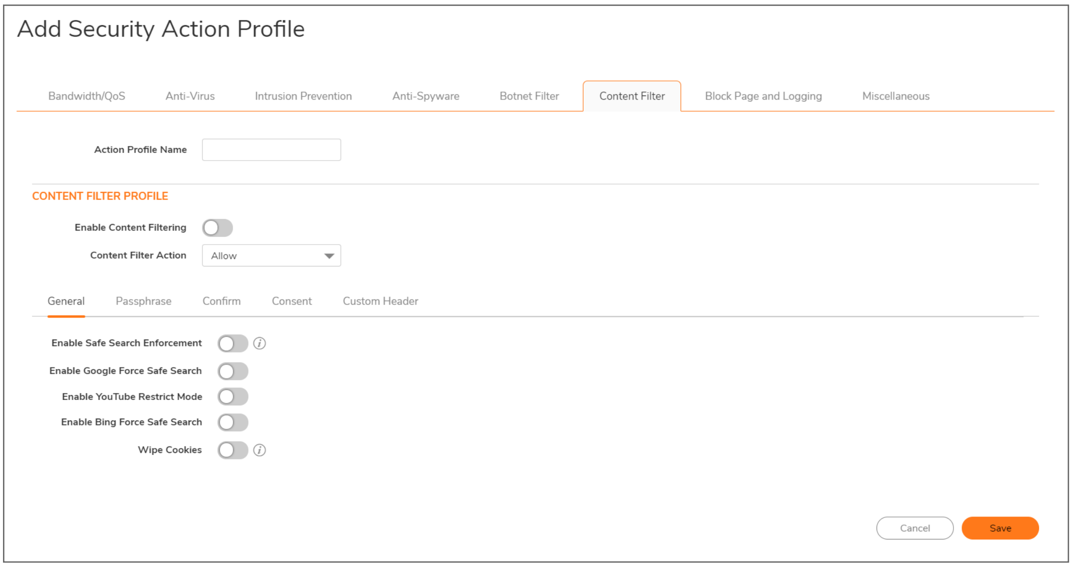
Content Filter

In this section you can create Content Filtering Service (CFS) Security Action Profile.

To configure the Content Filter Security Action Profile:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Click **+Add** or click the **Edit** icon from the **Configure** column for the Action you would like to modify.

3. Click the **Content Filter** tab.



Add Security Action Profile

Action Profile Name

CONTENT FILTER PROFILE

Enable Content Filtering ○

Content Filter Action Allow

Enable Safe Search Enforcement ○

Enable Google Force Safe Search ○

Enable YouTube Restrict Mode ○

Enable Bing Force Safe Search ○

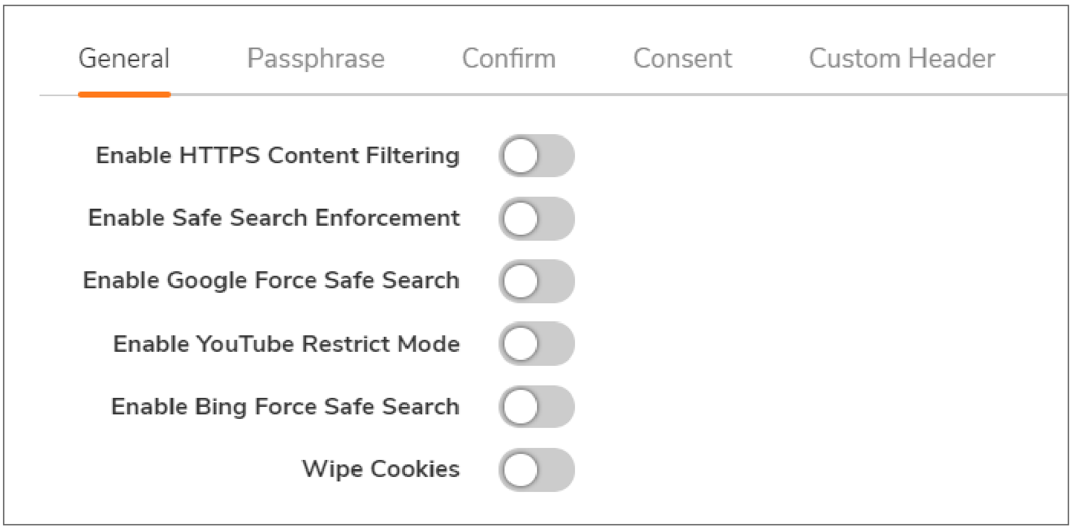
Wipe Cookies ○

4. Enter a friendly **Action Profile Name**.
5. Select **Enable Content Filtering** to activate SonicWall's Botnet Filtering service.
6. Select a **Content Filter Action**; **Allow**, **Confirm**, or **Passphrase**, and the Content filter action is applied to your security rule using the profile that has the Action set to CFS. Blocked pages served are different from the **General** action profile section of this profile.

General

To open the dialog:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile | Content Filter** tab. Scroll to the **General** tab section.



Enable HTTPS Content Filtering ○

Enable Safe Search Enforcement ○

Enable Google Force Safe Search ○

Enable YouTube Restrict Mode ○

Enable Bing Force Safe Search ○

Wipe Cookies ○

By default, none of the options are selected.

2. To enable content filtering for HTTPS sites, select the **Enable Content Filtering** option.

   HTTPS content filtering is IP based and does not inspect the URL, but uses other methods to obtain the URL rating. When this option is enabled, CFS performs URL rating lookup in this order:

   - Searches the client hello for the Server Name, which CFS uses to obtain the URL rating.
   - If the Server Name is not available, searches the SSL certificate for the Common Name, which CFS uses to obtain the URL rating.
   - If neither Server Name nor Common Name is available, CFS uses the IP address to obtain the URL rating.

While HTTP content filtering can perform redirects to enforce authentication or provide a block page, HTTPS filtered pages are silently blocked.

3. To enforce Safe Search when searching on any of the following websites, select the **Enable Safe Search Enforcement** option:

   - www.yahoo.com
   - www.ask.com
   - www.dogpile.com
   - www.lycos.com

This enforcement cannot be configured at the policy level as the function employs DNS redirection to HTTPS sites. For HTTPS sites, client DPI-SSL with content filter must be enabled.

4. To override the Safe Search option for Google inside each CFS Policy and its corresponding CFS Action, select the **Enable Google Force Safe Search** option.

   Typically, Safe Search happens automatically and is powered by Google, but when this option is enabled, SonicOSX rewrites the Google domain in the DNS response to the Google Safe Search virtual IP address.

   This feature takes effect only after the DNS cache of the client host is refreshed.

5. To access YouTube in Restrict (Safe Search) mode, select the **Enable YouTube Restrict Mode** option.

   YouTube provides a new feature to screen videos that may contain inappropriate content flagged by users and other signals. When this feature is enabled, SonicOSX rewrites the DNS response for the YouTube domain to its Safe Search virtual IP address.

   This feature takes effect only after the DNS cache of the client host is refreshed.

6. To override the Safe Search option for Bing inside each CFS Policy and its corresponding CFS Action, select the **Enable Bing Force Safe Search** option.

   When this feature is enabled, SonicOSX rewrites the DNS response for the Bing domain to its Safe Search virtual IP address.

   This feature takes effect only after the DNS cache of the client host is refreshed.

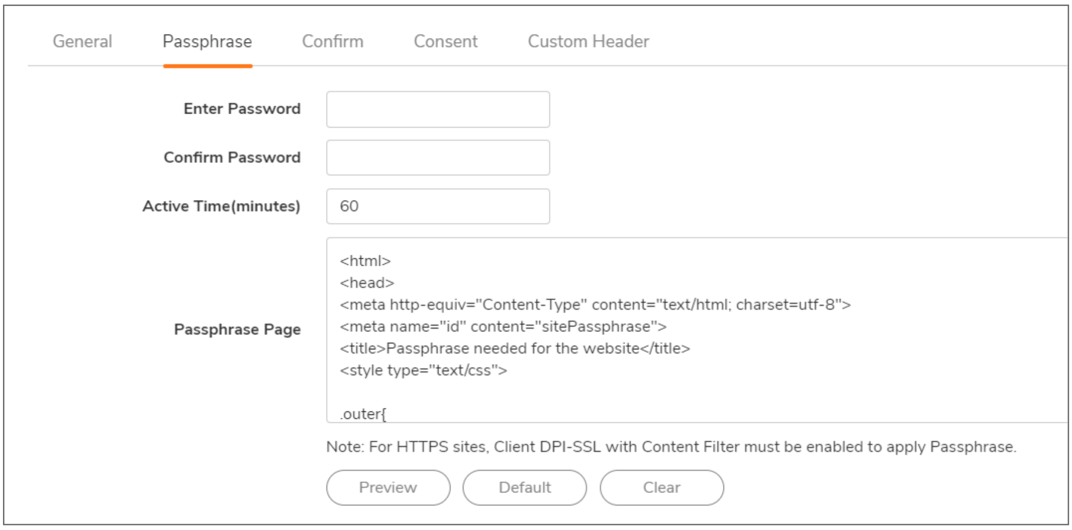
7. Click **Wipe Cookies** to remove cookie trace pages of visited websites.
8. Click **Save**.

Passphrase

This screen appears in the **Add Security Rule Action** dialog.

To create a password-protected web page:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**. Click **+Add/Edit** and click the **Content Filter** tab.
2. Scroll to the **Passphrase** tab.



Enter Password

Confirm Password

Active Time(minutes) 60

Passphrase Page

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<meta name="id" content="sitePassphrase">
<title>Passphrase needed for the website</title>
<style type="text/css">

.outer{
```

Note: For HTTPS sites, Client DPI-SSL with Content Filter must be enabled to apply Passphrase.

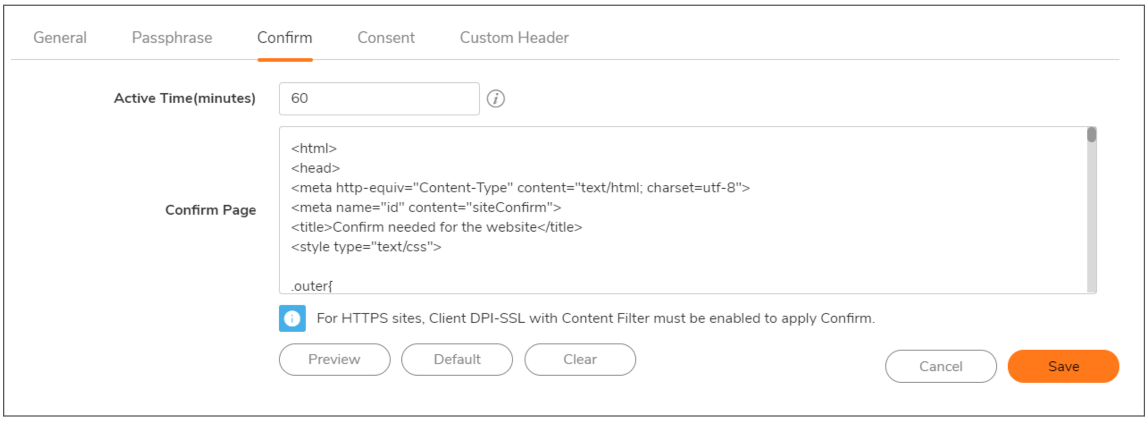
3. In the **Enter Password** field, enter the passphrase/password for the web site. The password can be up to 64 characters. You can enable or disable **Mask Password** to hide or reveal your password entry.
4. Enter your password again in the **Confirm Password** field.
5. Enter the time, in minutes, of the effective duration for a passphrase based on category or domain in the **Active Time (minutes)** field. The minimum time is 1 minute, the maximum is 9999, and the default is **60** minutes.
6. A default **Passphrase Page** is defined already, but you can fully customize the web page that is displayed when users attempt to access a blocked site. Or, you can create your own page.

   To create the page that displays when a site is blocked:

   - To see a preview of the display, click **Preview**.
   - If you have not modified the provided code, clicking **Preview** displays the default web page. The web site URL, Client IP address, policy, reason, and active minutes are shown along with a field for entering the password.
   - To remove all content from the Passphrase Page field, click **Clear**.
   - To revert to the default passphrase page message, click **Default**.
7. Click **Save**.
8. Click the **Confirm** tab.

Confirm

Requiring confirmation (consent) only works for HTTP requests. HTTPS requests cannot be redirected to a **Confirm** page.



Active Time(minutes) 60

Confirm Page

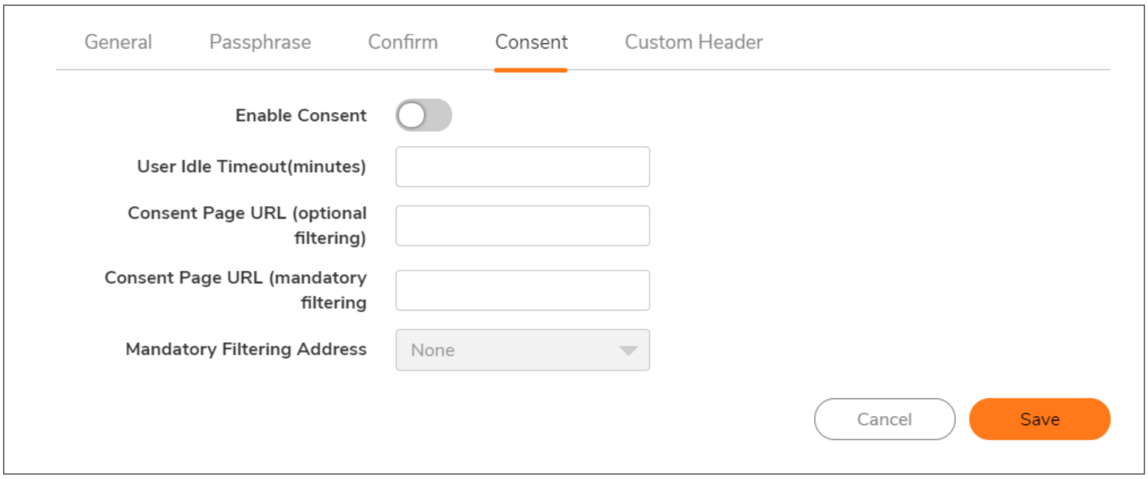
```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<meta name="id" content="siteConfirm">
<title>Confirm needed for the website</title>
<style type="text/css">

.outer{
```

For HTTPS sites, Client DPI-SSL with Content Filter must be enabled to apply Confirm.

To create a restricted web page that requires confirmation before a user can view it:

1. Enter the time, in minutes, of the effective duration for a confirmed user, based on category or domain in the **Active Time (minutes)** field. The minimum time is 1 minute, the maximum is 9999, and the default is **60** minutes.
2. A default page is defined already, but you can fully customize the web page that is displayed to the user when access to a confirm site is attempted. Or, you can create your own page.
3. To see a preview of the display, click **Preview**.
4. If you have not modified the provided code, clicking **Preview** displays the default web page. The web site URL, Client IP address, block policy, and the reason for the block are shown along with a field for entering the confirmation.
5. To remove all content from the **Confirm Page** field, click **Clear**.
6. To revert to the default blocked page message, click **Default**.
7. Click **Save**.
8. Click the **Consent** tab.

Consent



Enable Consent ○

User Idle Timeout(minutes)

Consent Page URL (optional filtering)

Consent Page URL (mandatory filtering

Mandatory Filtering Address: None

Consent only works for HTTP requests. HTTPS requests cannot be redirected to a **Confirm** (consent) page.

1. To enable consent, which displays the Consent (Confirm) page when a user visits a site requiring consent before access, select the **Enable Consent** option. This option is not selected by default.

   When this option is selected, the other options become available.
2. To remind users that their time has expired by displaying the **Consent** page, enter the idle-time duration in the **User Idle Timeout (minutes)** field. The minimum idle time is one minute, the maximum is 9999 minutes, and the default is 15 minutes.
3. In the **Consent Page URL (optional filtering)** field, enter the URL of the website where a user is redirected if they go to a website requiring consent. The **Consent** page must:
   - Reside on a web server and be accessible as a URI by users on the network.
   - Contain links to the following two pages in the SonicWall appliance, which, when selected, tell the firewall the type of access the user wishes to have:
     - Unfiltered access: `<appliance's LAN IP address>/iAccept.html`
     - Filtered access: `<appliance's LAN IP address>/iAcceptFilter.html`
4. In the **Consent Page URL (mandatory filtering)** field, enter the website URL where the user is redirected if they go to a website requiring mandatory filtering. The Consent page must:
   - Reside on a web server and be accessible as a URI by users on the network.
   - Contain a link to the `<appliance's LAN IP address>/iAcceptFilter.html` page in the SonicWall appliance, which tells the firewall that the user accepts filtered access.
5. From the **Mandatory Filtering Address** drop-down menu, choose an Address Object that contains the configured IP addresses requiring mandatory filtering.

   ⓘ | **NOTE: Enable Consent** must be enabled to activate this feature.
6. Click **Save**.
7. Click the **Custom Header** tab.

Custom Header

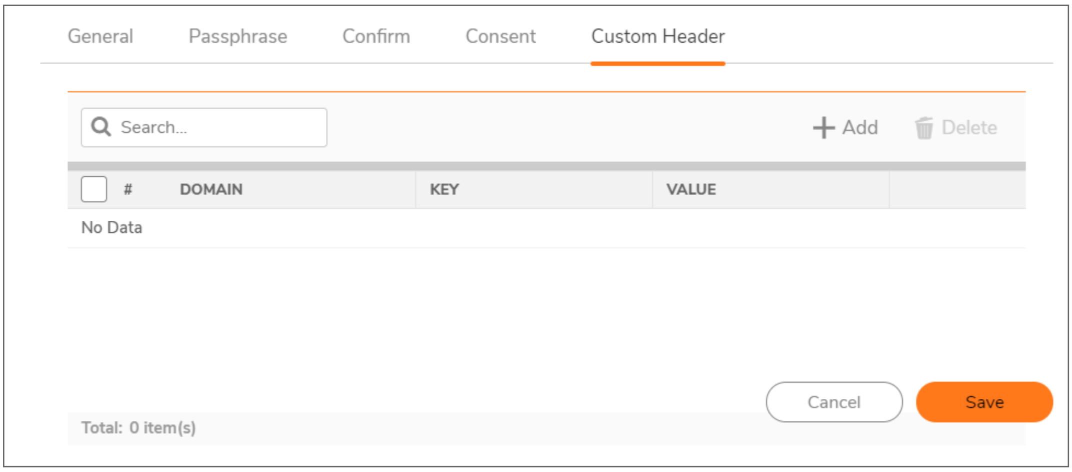
You can configure the firewall as a web proxy server to control web service, such as preventing users from signing in to some web services using any accounts other than the accounts provided, or restricting the content viewable by users. The web proxy server adds a custom header to all traffic matched by the Content Filtering policy, and the header identifies the domains whose users can access the web services or the content that users can access. Encrypted HTTPS traffic is supported if DPI-SSL is enabled.

This feature requires the following:

- Content Filter Service is enabled.
- Custom header insertion is enabled in the matched CFS profile object.
- DPI-SSL is enabled for custom header insertion with encrypted HTTPS requests.

To configure a CFS custom header and enable custom header insertion:

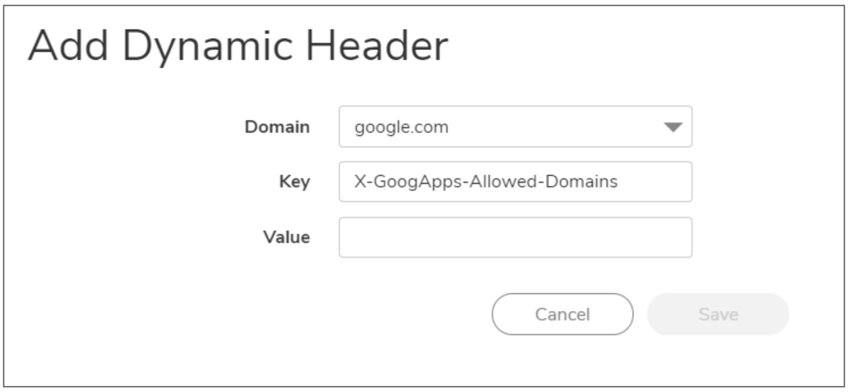
1. Navigate to **OBJECT | Action Profiles > Security Action Profile**. Click **+Add/Edit** and click the **Content Filter** tab.
2. Scroll to the **Custom Header** tab.



□	#	DOMAIN	KEY	VALUE
No Data				

Total: 0 item(s)

3. Click **+Add** to configure the **Domain**, **Key**, and **Value** for the custom Dynamic Header entry.



Add Dynamic Header

Domain: google.com

Key: X-GoogApps-Allowed-Domains

Value:

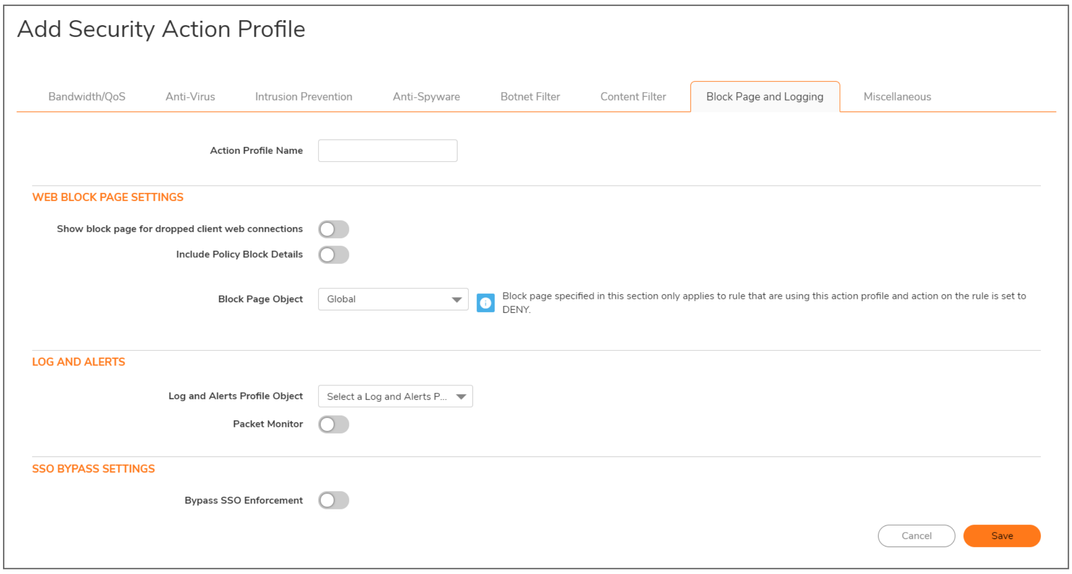
4. Click **Save**. The Header appears in the Custom Header list.
5. Click **Save**.

Block Page and Logging

In this section you can create Block Page and Reporting Action objects that utilize the Profiles you established in **OBJECT | Profile Objects > Block Page**.

To configure the Block Page and Logging Security Action Profile:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Click **+Add** or click the **Edit** icon from the **Configure** column for the Action you would like to modify.
3. Click the **Block Page and Logging** tab.



Add Security Action Profile

Action Profile Name

WEB BLOCK PAGE SETTINGS

Show block page for dropped client web connections ○

Include Policy Block Details ○

Block Page Object: Global

Block page specified in this section only applies to rule that are using this action profile and action on the rule is set to DENY.

LOG AND ALERTS

Log and Alerts Profile Object: Select a Log and Alerts P...

Packet Monitor ○

SSO BYPASS SETTINGS

Bypass SSO Enforcement ○

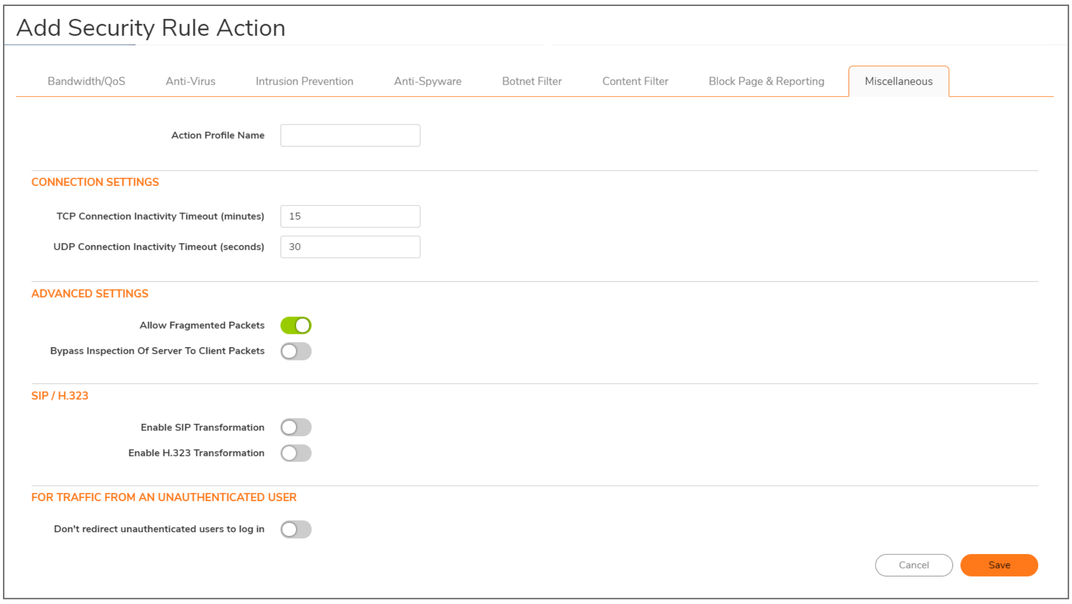
4. Enter a friendly **Action Profile Name**.
5. Under **Web Block Page Settings**, enable **Show block page for dropped client web connections** to show a Global, Default, or custom Block Page you created in Profiles for dropped client web connections.
6. Enable **Include Policy Block Details** if you would like to include an explanation as to the reason the page was blocked.
7. Select a Reporting Object Block Page from the **Block Page Object** drop-down menu. You can use the **Global** page, a **Default Block Page**, or a custom Block Page that you create in **OBJECT | Profiles > Block Page**.
8. Under **Reporting Profile**, select a Reporting Profile Object from the **Reporting Profile Object** drop-down menu. You can use the **Global** page, a **Default Block Page**, or a custom Block Page that you create in **OBJECT | Profile Objects > Block Page**.
9. Enable or disable **Flow Reporting** and **Packet Monitor**.
10. Click **Save**.

Miscellaneous

In this section you can enable and disable additional settings in relation to your profiles and action objects.

To modify Miscellaneous settings:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.
2. Click **+Add** or click the **Edit** icon from the **Configure** column for the Action you would like to modify.
3. Click the **Miscellaneous** tab.



Action Profile Name

CONNECTION SETTINGS

TCP Connection Inactivity Timeout (minutes) 15

UDP Connection Inactivity Timeout (seconds) 30

ADVANCED SETTINGS

Allow Fragmented Packets ●

Bypass Inspection Of Server To Client Packets ○

SIP / H.323

Enable SIP Transformation ○

Enable H.323 Transformation ○

FOR TRAFFIC FROM AN UNAUTHENTICATED USER

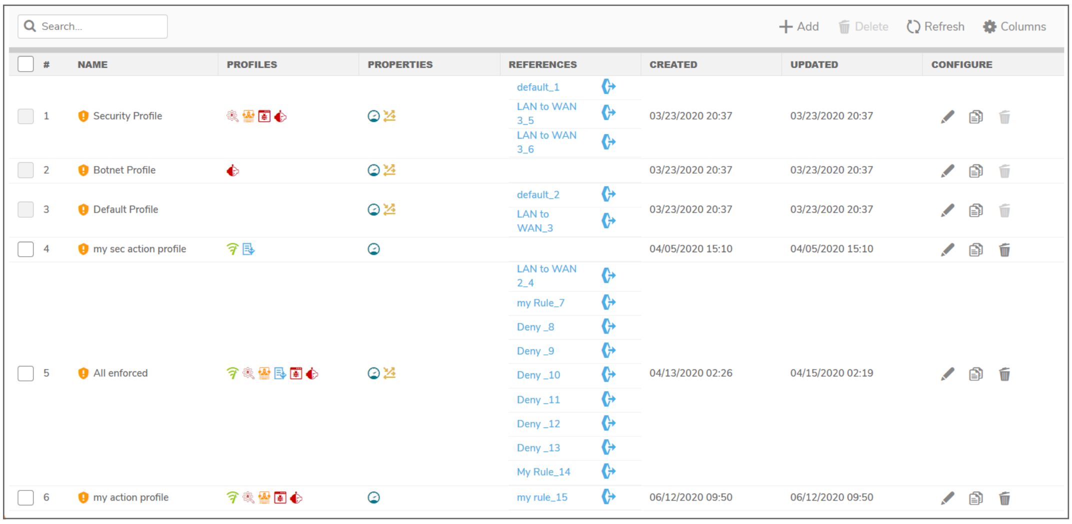
Don't redirect unauthenticated users to log in ○

4. Enter a friendly **Action Profile Name**.
5. Modify **Connection Settings**, **Advanced Settings**, **SIP/H.323 Transformation settings**, and so on.
6. Click **Save**.

Editing Security Action Profiles

To edit an existing Security Action Profile:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.



□	#	NAME	PROFILES	PROPERTIES	REFERENCES	CREATED	UPDATED	CONFIGURE
□	1	Security Profile			default_1 LAN to WAN 3_5 LAN to WAN 3_6	03/23/2020 20:37	03/23/2020 20:37	
□	2	Botnet Profile				03/23/2020 20:37	03/23/2020 20:37	
□	3	Default Profile			default_2 LAN to WAN_3	03/23/2020 20:37	03/23/2020 20:37	
□	4	my sec action profile				04/05/2020 15:10	04/05/2020 15:10	
□	5	All enforced			LAN to WAN 2_4 my Rule_7 Deny _8 Deny _9 Deny _10 Deny _11 Deny _12 Deny _13 My Rule_14	04/13/2020 02:26	04/15/2020 02:19	
□	6	my action profile			my rule_15	06/12/2020 09:50	06/12/2020 09:50	

2. Click the Security Rule Action Object you would to edit one time and in the right **Configure** column, click the **Edit** icon for the Security Action Profile.

   This opens the **Edit Security Action Profile** page, which you can modify or update.

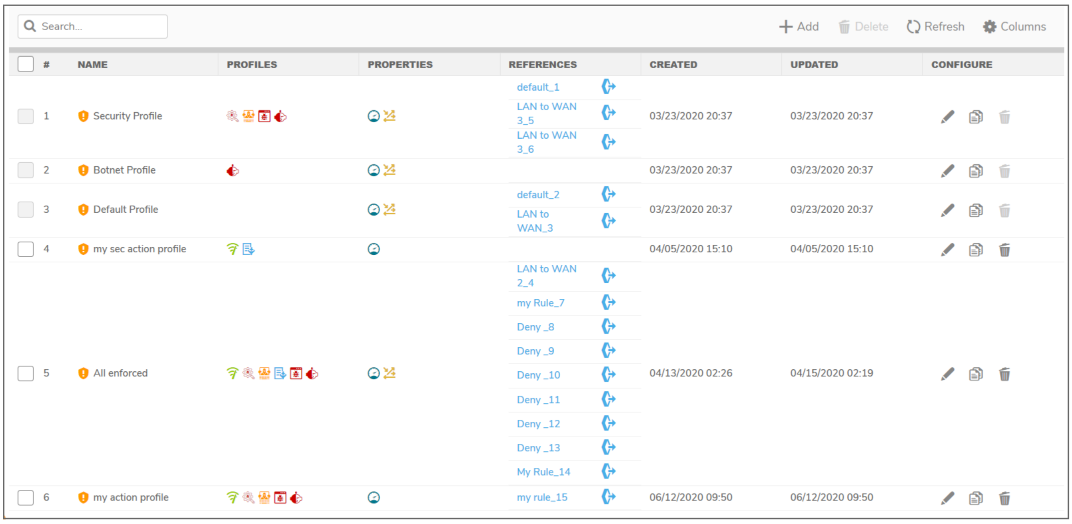
3. Make changes to the **Edit Security Action Profile** page.

4. Click **Save**.

Cloning Security Action Profiles

To clone an existing Security Action Profile:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.



□	#	NAME	PROFILES	PROPERTIES	REFERENCES	CREATED	UPDATED	CONFIGURE
□	1	Security Profile			default_1 LAN to WAN 3_5 LAN to WAN 3_6	03/23/2020 20:37	03/23/2020 20:37	
□	2	Botnet Profile				03/23/2020 20:37	03/23/2020 20:37	
□	3	Default Profile			default_2 LAN to WAN_3	03/23/2020 20:37	03/23/2020 20:37	
□	4	my sec action profile				04/05/2020 15:10	04/05/2020 15:10	
□	5	All enforced			LAN to WAN 2_4 my Rule_7 Deny _8 Deny _9 Deny _10 Deny _11 Deny _12 Deny _13 My Rule_14	04/13/2020 02:26	04/15/2020 02:19	
□	6	my action profile			my rule_15	06/12/2020 09:50	06/12/2020 09:50	

2. Click the Security Rule Action Object you would to clone one time and in the right **Configure** column, click the **Clone** icon for the Security Action Profile.

   This creates a duplicate of the page, which allows you the basis to create a new Security Action Profile using the similar content.

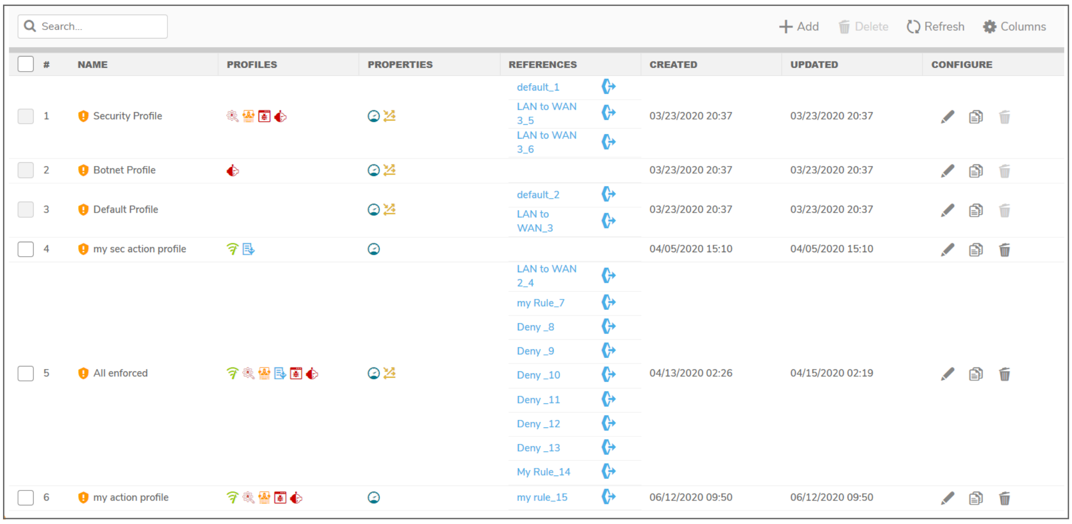
3. Make changes to the **Clone Security Action Profile** page.

Deleting Security Action Profiles

> ⓘ **NOTE:** Only custom Security Action Profiles can be deleted. You cannot delete the Default Security Action Profile page.

To delete a custom Security Rule Action page message:

1. Navigate to **OBJECT | Action Profiles > Security Action Profile**.



□	#	NAME	PROFILES	PROPERTIES	REFERENCES	CREATED	UPDATED	CONFIGURE
□	1	Security Profile			default_1 LAN to WAN 3_5 LAN to WAN 3_6	03/23/2020 20:37	03/23/2020 20:37	
□	2	Botnet Profile				03/23/2020 20:37	03/23/2020 20:37	
□	3	Default Profile			default_2 LAN to WAN_3	03/23/2020 20:37	03/23/2020 20:37	
□	4	my sec action profile				04/05/2020 15:10	04/05/2020 15:10	
□	5	All enforced			LAN to WAN 2_4 my Rule_7 Deny _8 Deny _9 Deny _10 Deny _11 Deny _12 Deny _13 My Rule_14	04/13/2020 02:26	04/15/2020 02:19	
□	6	my action profile			my rule_15	06/12/2020 09:50	06/12/2020 09:50	

2. Click the Security Rule Action Object Page you would to delete one time and in the right **Configure** column, click the Trash can icon.

   A confirmation message appears.

3. Click **OK** or **Cancel**.

To delete ALL custom Security Action Profile pages, click the top box to the left of the **Security Action Profile** page names and click the **Trash** icon from the top toolbar.

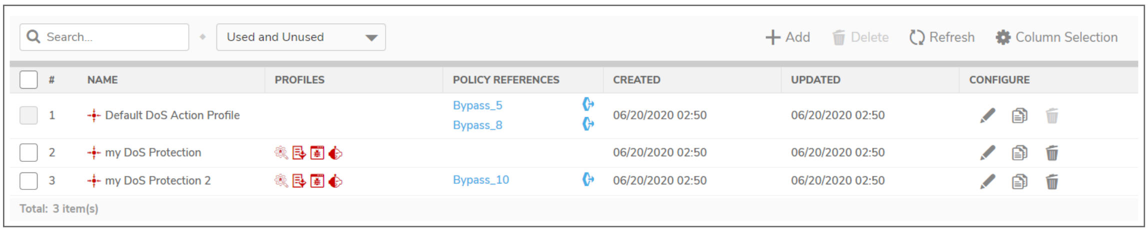
2

DoS Action Profile

DoS Action Profiles are Action profiles that can be established to Protect DoS related activity such as:

- Flood Protection
- DDoS Protection
- Attack Protection
- Connection Limiting

These action objects can all be tracked in the DoS Rule Action table located at **OBJECT | Action Profiles > DoS Action Profile**.



□	#	NAME	PROFILES	POLICY REFERENCES	CREATED	UPDATED	CONFIGURE
□	1	Default DoS Action Profile		Bypass_5 Bypass_8	06/20/2020 02:50	06/20/2020 02:50	
□	2	my DoS Protection			06/20/2020 02:50	06/20/2020 02:50	
□	3	my DoS Protection 2		Bypass_10	06/20/2020 02:50	06/20/2020 02:50	

Total: 3 item(s)

Topics:

- Adding DoS Action Profiles
- Editing DoS Action Profiles
- Cloning DoS Action Profiles
- Deleting DoS Action Profiles

Adding DoS Action Profiles

SonicOSX defends against UDP/ICMP flood attacks by monitoring IPv6 UDP/ICMP traffic flows to defined destinations. UDP/ICMP packets to a specified destination are dropped if one or more sources exceeds a configured threshold.

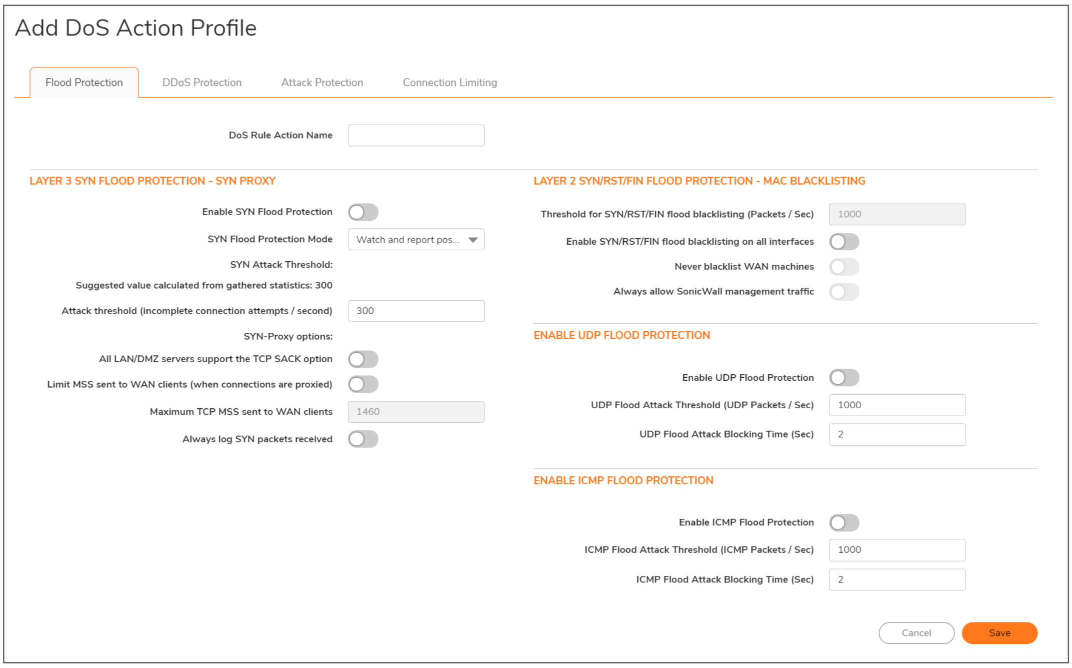
Flood Protection

The **OBJECT | Action Profiles > DoS Action Profile | Flood Protection** tab allows you to:

- Manage:
  - TCP (Transmission Control Protocol) traffic settings such as Layer 2/Layer3 flood protection, WAN DDOS protection
  - UDP (User Datagram Protocol) flood protection
  - ICMP (Internet Control Message Protocol) or ICMPv6 flood protection.
- View statistics through the security appliance:
  - TCP traffic
  - UDP traffic
  - ICMP or ICMPv6 traffic

To configure the Flood Protection DoS Rule Action:

1. Navigate to **OBJECT | Action Profiles > DoS Action Profile**.
2. Click **+Add** or click the **Edit** icon from the **Configure** column.
3. The **Add DoS Action Profile** page open on the **Flood Protection** tab.



Add DoS Action Profile

DoS Rule Action Name:

LAYER 3 SYN FLOOD PROTECTION - SYN PROXY

Enable SYN Flood Protection ○
SYN Flood Protection Mode: Watch and report pos...
SYN Attack Threshold:
Suggested value calculated from gathered statistics: 300
Attack threshold (incomplete connection attempts / second): 300
SYN-Proxy options:
All LAN/DMZ servers support the TCP SACK option ○
Limit MSS sent to WAN clients (when connections are proxied) ○
Maximum TCP MSS sent to WAN clients: 1460
Always log SYN packets received ○

LAYER 2 SYN/RST/FIN FLOOD PROTECTION - MAC BLACKLISTING

Threshold for SYN/RST/FIN flood blacklisting (Packets / Sec): 1000
Enable SYN/RST/FIN flood blacklisting on all interfaces ○
Never blacklist WAN machines ○
Always allow SonicWall management traffic ○

ENABLE UDP FLOOD PROTECTION

Enable UDP Flood Protection ○
UDP Flood Attack Threshold (UDP Packets / Sec): 1000
UDP Flood Attack Blocking Time (Sec): 2

ENABLE ICMP FLOOD PROTECTION

Enable ICMP Flood Protection ○
ICMP Flood Attack Threshold (ICMP Packets / Sec): 1000
ICMP Flood Attack Blocking Time (Sec): 2

4. Enter a friendly **DoS Rule Action Name**.

Layer 3 SYN Flood Protection- SYN Proxy

To configure Layer 3 SYN Flood Protection features:

1. Click **Enable Syn Flood Protection**.
2. In the **SYN Flood Protection Mode** drop down menu, select a protection mode.
    - **Watch and Report Possible SYN Floods** – The device monitors SYN traffic on all interfaces and logs suspected SYN flood activity that exceeds a packet-count threshold. This option does not actually turn on the SYN Proxy on the device, so the device forwards the TCP three way handshake without modification.

    This is the least invasive level of SYN Flood protection. Select this option if your network is not in a high risk environment.

    When this protection mode is selected, the **SYN-Proxy** options are not available.

    - **Proxy WAN Client Connections When Attack is Suspected** – The device enables the SYN Proxy feature on WAN interfaces when the number of incomplete connection attempts per second exceeds a specified threshold. This method ensures that the device continues to process valid traffic during the attack, and that performance does not degrade. Proxy mode remains enabled until all WAN SYN flood attacks stop occurring, or until the device blacklists all of them using the SYN Blacklisting feature.

    This is the intermediate level of SYN Flood protection. Select this option if your network sometimes experiences SYN Flood attacks from internal or external sources.

    - **Always Proxy WAN Client Connections** – This option sets the device to always use SYN Proxy. This method blocks all spoofed SYN packets from passing through the device. This is an extreme security measure, which directs the device to respond to port scans on all TCP ports. The SYN Proxy feature forces the device to respond to all TCP SYN connection attempts, which can degrade performance and generate false positive results. Select this option only if your network is in a high risk environment.
3. For **SYN Proxy Options**, if one of the higher levels of SYN Protection is selected, SYN Proxy options can be selected to provide more control over what is sent to WAN clients when in SYN Proxy mode. When the device applies a SYN Proxy to a TCP connection, it responds to the initial SYN packet with a manufactured SYN/ACK reply, waiting for the ACK in response before forwarding the connection request to the server. Devices attacking with SYN Flood packets do not respond to the SYN/ACK reply. The firewall identifies them by their lack of this type of response and blocks their spoofed connection attempts. SYN Proxy forces the firewall to manufacture a SYN/ACK response without knowing how the server responds to the TCP options normally provided on SYN/ACK packets.

    The options in this section are not available if **Watch and report possible SYN floods** option is selected for **SYN Flood Protection Mode**.

    - **All LAN/DMZ servers support the TCP SACK option** – Selecting this option enables SACK (Selective Acknowledgment), so that when a packet is dropped, the receiving device indicates which packets it received. This option is not enabled by default. Enable this checkbox only when you know that all servers covered by the firewall that are accessed from the WAN support the SACK option.
    - **Limit MSS sent to WAN clients (when connections are proxied)** – When you choose this option, you can enter the maximum MSS (Minimum Segment Size) value. This sets the threshold for the size of TCP segments, preventing a segment that is too large from being sent to the targeted server. For example, if the server is an IPsec gateway, it might need to

limit the MSS it receives to provide space for IPsec headers when tunneling traffic. The firewall cannot predict the MSS value sent to the server when it responds to the SYN manufactured packet during the proxy sequence. Being able to control the size of a segment makes it possible to control the manufactured MSS value sent to WAN clients. This option is not selected by default.

If you specify an override value for the default of 1460, only a segment that size or smaller is sent to the client in the SYN/ACK cookie. Setting this value too low can decrease performance when the SYN Proxy is always enabled. Setting this value too high can break connections if the server responds with a smaller MSS value.

- **Maximum TCP MSS sent to WAN clients** – This is the value of the MSS. The default is 1460, the minimum value is 32, and the maximum is 1460.

When using Proxy WAN client connections, remember to set these options conservatively as they only affect connections when a SYN Flood takes place. This ensures that legitimate connections can continue during an attack.

- **Always log SYN packets received** – Select this option to log all SYN packets received. This option is only available with higher levels of SYN protection.

Layer 2 SYN/RST/FIN Flood Protection - MAC Blacklisting

The SYN/RST/FIN Blacklisting feature lists devices that exceeded the SYN, RST, and FIN Blacklist attack threshold. The firewall device drops packets sent from blacklisted devices early in the packet evaluation process, enabling the firewall to handle greater amounts of these packets, providing a defense against attacks originating on local networks while also providing second-tier protection for WAN networks.

Devices cannot occur on the SYN/RST/FIN Blacklist and watchlist simultaneously. With blacklisting enabled, the firewall removes devices exceeding the blacklist threshold from the watchlist and places them on the blacklist. Conversely, when the firewall removes a device from the blacklist, it places it back on the watchlist. Any device whose MAC address has been placed on the blacklist will be removed from it approximately three seconds after the flood emanating from that device has ended.

- **Enable SYN/RST/FIN/TCP flood blacklisting on all interfaces** – Enables the blacklisting feature on all interfaces on the firewall. This option is not selected by default. When it is selected, the following options become available.
- **Never blacklist WAN machines** – Ensures that systems on the WAN are never added to the SYN Blacklist. This option is recommended as leaving it cleared may interrupt traffic to and from the firewall's WAN ports. This option is not selected by default.
- **Always allow SonicWall management traffic** – Causes IP traffic from a blacklisted device targeting the firewall's WAN IP addresses to not be filtered. This allows management traffic and routing protocols to maintain connectivity through a blacklisted device. This option is not selected by default.
- **Threshold for SYN/RST/FIN flood blacklisting** – Specifies the maximum number of SYN, RST, FIN, and TCP packets allowed per second. The minimum is 10, the maximum is 800000, and default is 1,000. This value should be larger than the SYN Proxy threshold value because blacklisting attempts to thwart more vigorous local attacks or severe attacks from a WAN network.

Enable UDP Flood Protection

UDP Flood Attacks are a type of denial-of-service (DoS) attack. They are initiated by sending a large number of UDP packets to random ports on a remote host. As a result, the victimized system's resources are consumed with handling the attacking packets, which eventually causes the system to be unreachable by other clients.

SonicWall UDP Flood Protection defends against these attacks by using a "watch and block" method. The appliance monitors UDP traffic to a specified destination. If the rate of UDP packets per second exceeds the allowed threshold for a specified duration of time, the appliance drops subsequent UDP packets to protect against a flood attack.

UDP packets that are DNS query or responses to or from a DNS server configured by the appliance are allowed to pass, regardless of the state of UDP Flood Protection.

The following settings configure UDP Flood Protection:

1. **Enable UDP Flood Protection** – Enables UDP Flood Protection. This option is not selected by default. **Enable UDP Flood Protection** must be enabled to activate the other UDP Flood Protection options.
2. **UDP Flood Attack Threshold** – The maximum number of UDP packets allowed per second to be sent to a host, range, or subnet that triggers UDP Flood Protection. Exceeding this threshold triggers ICMP Flood Protection. The minimum value is 50, the maximum value is 1000000, and the default value is 1000.
3. **UDP Flood Attack Blocking Time** – After the appliance detects the rate of UDP packets exceeding the attack threshold for this duration of time, UDP Flood Protection is activated and the appliance begins dropping subsequent UDP packets. The minimum time is 1 second, the maximum time is 120 seconds, and the default time is 2 seconds.
4. Click **Save**.

Enable ICMP Flood Protection

ICMP Flood Protection functions identically to UDP Flood Protection, except it monitors for ICMPv4/ICMPv6 Flood Attacks. The only difference is that DNS queries are not allowed to bypass ICMP Flood Protection.

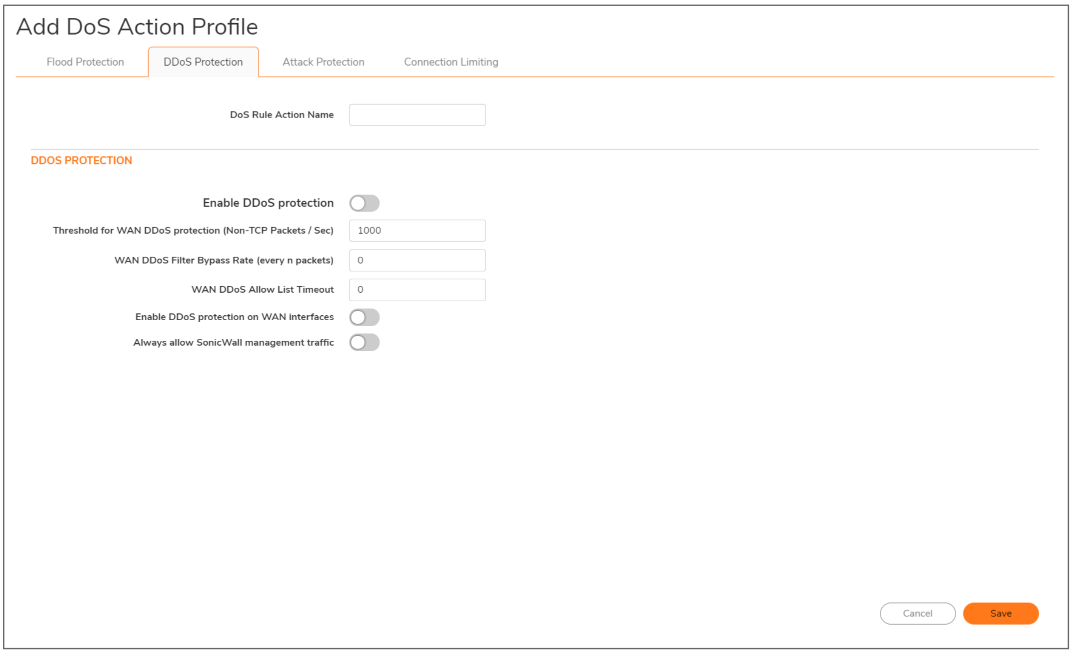
To configure ICMP Flood Protection:

1. **Enable ICMP Flood Protection** – Enables ICMP Flood Protection. **Enable ICMP Flood Protection** must be enabled to activate the other ICMP Flood Protection options.
2. **ICMP Flood Attack Threshold** – The maximum number of ICMP packets allowed per second to be sent to a host, range, or subnet. Exceeding this threshold triggers ICMP Flood Protection. The minimum number is 10, the maximum number is 100000, and the default number is **1000**.
3. **ICMP Flood Attack Blocking Time** – After the appliance detects the rate of ICMP packets exceeding the attack threshold for this duration of time, ICMP Flood Protection is activated, and the appliance begins dropping subsequent ICMP packets. The minimum time is 1 second, the maximum time is 120 seconds, and the default time is **2** seconds.
4. Click **Save**.

DDoS Protection

To configure the DDos Protection portion of the Add DoS Rule Action:

1. Navigate to **OBJECT | Action Profiles > DoS Action Profile**.
2. Click **+Add** or click the **Edit** icon from the **Configure** column.
3. The **Add DoS Action Profile** page opens, click the **DDoS Protection** tab.



Add DoS Action Profile

DoS Rule Action Name

DDOS PROTECTION

Enable DDoS protection

Threshold for WAN DDoS protection (Non-TCP Packets / Sec) 1000

WAN DDoS Filter Bypass Rate (every n packets) 0

WAN DDoS Allow List Timeout 0

Enable DDoS protection on WAN interfaces

Always allow SonicWall management traffic

4. Enter a friendly **DoS Rule Action Name**.
5. Click **Enable DDoS protection**.

- **Threshold for WAN DDOS protection - Non-TCP packets/Second** - The option to set this threshold is available when **Enable DDOS protection on WAN interfaces** is selected. It specifies the maximum number of non-TCP packets allowed per second to be sent to a host, range, or subnet. Exceeding this threshold triggers WAN DDOS flood protection. The default number of non-TCP packets is 1000. The minimum number is 0, and the maximum number is 10,000,000.
- **WAN DOOS Filter Bypass Rate - packets/second** - This rate is available when **Enable DDOS protection on WAN interfaces** is selected. The default value of the WAN DDOS Filter Bypass Rate is 0. This default rate prevents all packets passing through unless the device from which they originate is on the Allow List. This can be an appropriate choice in some deployments.

  When you configure this rate to a non-0 number, some non-TCP packet that would normally be dropped by WAN DDOS Protection are instead passed to the LAN/DMZ network. A non-0 bypass rate allows the risk of a potential attack to be reduced, but not completely blocked. Allowing some packets to pass through (such as every 3rd packet), even though their sources are not on the Allow List, can provide a mechanism by which legitimate WAN-side hosts can get a packet through to the LAN/DMZ side, in spite of the high alert status of the appliance.

  You must determine the appropriate value to set, depending on the capabilities of the potential LAN-side target machines and the nature of the legitimate non-TCP traffic patterns in the network.

- **WAN DDOS Allow List Timeout - seconds** - This field is available when Enable DDOS protection on WAN interfaces is selected. If a non-zero Allow List Timeout is defined by the user, entries in the Allow List expire in the configured time. If the Allow List Timeout is zero, they never expire. In either case, the least-recently-used entry in a particular group can be replaced by a new entry, if no unused entry is available in the list.
- **Enable WAN DDOS Protection on WAN interfaces** - provides protection against non-TCP DDOS attacks, and so should be used in combination with SYN-Flood Protection if TCP SYN-flood attacks are a concern. This feature is not intended to protect a well-known server of non-TCP services on the Internet (such as a central DNS server), but is intended to protect LAN and DMZ networks for which the majority of non-TCP traffic is initiated from the LAN/DMZ side, possibly in combination with limited WAN-initiated traffic.
- Check **Enable WAN DDOS Protection on WAN interfaces** to enable the rest of the options in this section. When WAN DDOS Protection is enabled, it tracks the rate of non-TCP packets arriving on WAN interfaces. When the rate of non-TCP packets exceeds the specified threshold, non-TCP packets arriving on WAN interfaces will be filtered. A non-TCP packet is only forwarded when at least one of the following conditions is met:
  - the source IP address is on the Allow list
  - the packet is SonicWall management traffic, and **Always allow SonicWall management traffic** is selected
  - the packet is an ESP packet and matches the SPI of a tunnel terminating on the network security appliance
  - the packet is the nth packet matching the value specified for **WAN DDOS Filter Bypass Rate (every n packets)**

If none of these conditions are met, the packet is dropped early in packet processing.

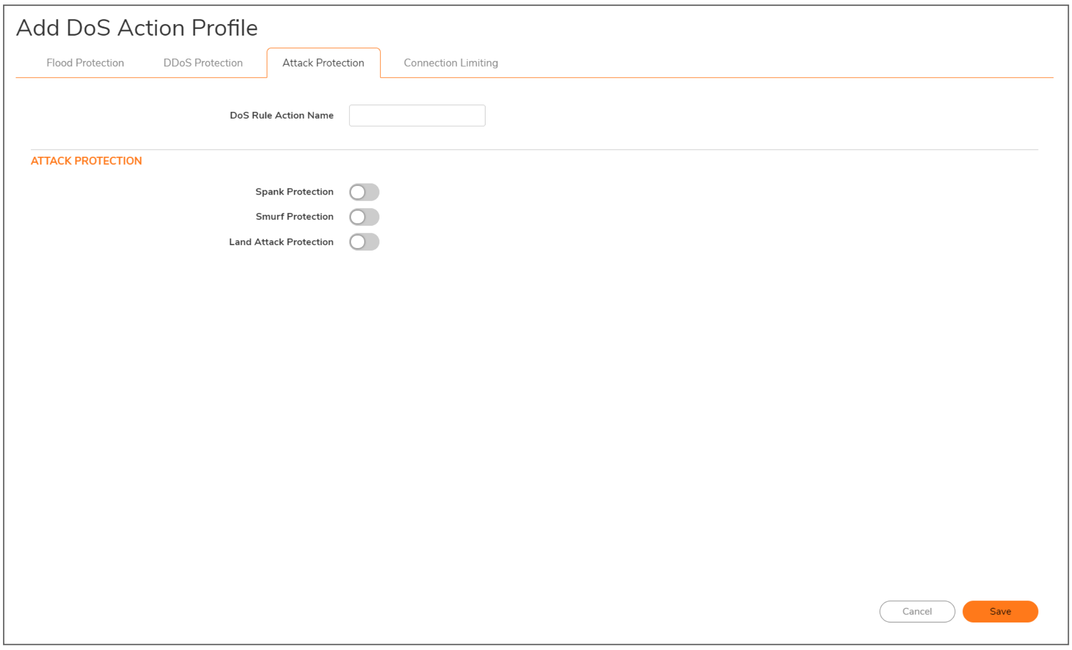
- Always allow SonicWall management traffic - This field is available when **Enable DDOS protection on WAN interfaces** is selected. Select this field so that traffic needed to manage your SonicWall appliances is allowed to pass through your WAN gateways, even when the appliance is under a non-TCP DDOS attack. This option is disabled by default.
- Always allow VPN negotiation traffic - This field is available when **Enable DDOS protection on WAN interfaces** is selected. Select this field so that all VPN negotiation packets are allowed to pass through, even though other traffic is blocked.

6. Click **Save**.

Attack Protection

To configure the Attack Protection portion of the Add DoS Rule Action:

1. Navigate to **OBJECT | Action Profiles > DoS Action Profile**.
2. Click **+Add** or click the **Edit** icon from the **Configure** column.
3. The **Add DoS Action Profile** page opens, click the **Attack Protection** tab.


Add DoS Action Profile

DoS Rule Action Name

ATTACK PROTECTION

Spank Protection ○
Smurf Protection ○
Land Attack Protection ○

4. Enter a friendly **DoS Rule Action Name**.
5. Enable **Spank Protection** to guard against remote host attacks responding to TCP packets that have come from a multicast IP addresses. Attackers exploit this vulnerability by conducting a 'spank' denial of service attack. This results in the host being shut down or the network traffic reaching saturation. Also, this vulnerability can be used by an attacker to conduct stealth port scans against the host.
6. Enable **Smurf Protection** to guard against attacks where LAN Clients are being used as part of an "Amplifier network."
7. Enable **Land Attack Protection** to protect against a Layer 4 Denial of Service (DoS) attack where the attacker resets the source and destination information of a TCP segment to be the same. A vulnerable machine crashes or freezes because the packet is being repeatedly processed by the TCP stack.
8. Click **Save**.

Connection Limiting

The Connection Limiting feature is intended to offer an additional layer of security and control when coupled with such features as SYN Cookies and Intrusion Prevention Services (IPS). Connection limiting provides a means of throttling connections through the firewall using Access Rules as a classifier, and declaring the maximum percentage of the total available connection cache that can be allocated to that class of traffic.

Coupled with IPS, this can be used to mitigate the spread of a certain class of malware as exemplified by Sasser, Blaster, and Nimda. These worms propagate by initiating connections to random addresses at atypically high rates. For example, each host infected with Nimda attempted 300 to 400 connections per second, Blaster sent 850 packets per second, and Sasser was capable of 5,120 attempts per second. Typical, non-malicious network traffic generally does not establish anywhere near these numbers, particularly when it is Trusted > Untrusted traffic (that is, LAN > WAN). Malicious activity of this sort can consume all available connection cache resources in a matter of seconds, particularly on smaller appliances.

In addition to mitigating the propagation of worms and viruses, Connection Limiting can be used to alleviate other types of connection cache resource consumption issues, such as those posed by uncompromised internal hosts running peer to peer software (assuming IPS is configured to allow these services), or internal or external hosts using packet generators or scanning tools.

Finally, Connection Limiting can be used to protect publicly available servers (such as, Web servers) by limiting the number of legitimate inbound connections permitted to the server (that is, to protect the server against the Slashdot effect). This is different from SYN flood protection that attempts to detect and prevent partially open or spoofed TCP connection. This is most applicable for Untrusted traffic, but it can be applied to any zone traffic as needed.

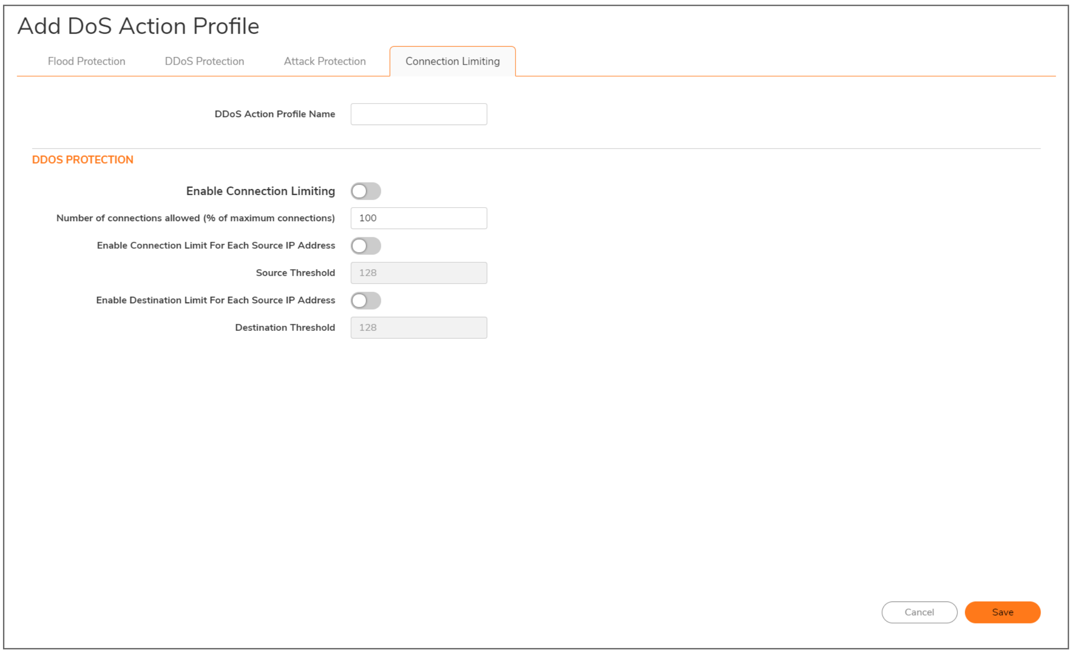
Connection Limiting is applied by defining a percentage of the total maximum allowable connections that might be allocated to a particular type of traffic. The previous figures show the default LAN > WAN setting, where all available resources might be allocated to LAN > WAN (any source, any destination, any service) traffic.

More specific rules can be constructed; for example, to limit the percentage of connections that can be consumed by a certain type of traffic (for example, FTP traffic to any destination on the WAN), or to prioritize important traffic (for example, HTTPS traffic to a critical server) by allowing 100% to that class of traffic, and limiting general traffic to a smaller percentage (minimum allowable value is 1%).

It is not possible to use IPS signatures as a Connection Limiting classifier; only Access Rules (for example, Address Objects and Service Objects) are permissible.

To configure the Connection Limiting portion of the Add DoS Action Profile page:

1. Navigate to **OBJECT | Action Profiles > DoS Action Profile**.
2. Click **+Add** or click the **Edit** icon from the **Configure** column.
3. The **Add DoS Action Profile** page opens, click the **Connection Limiting** tab.



DDoS Action Profile Name

DDOS PROTECTION

Enable Connection Limiting ○

Number of connections allowed (% of maximum connections) 100

Enable Connection Limit For Each Source IP Address ○

Source Threshold 128

Enable Destination Limit For Each Source IP Address ○

Destination Threshold 128

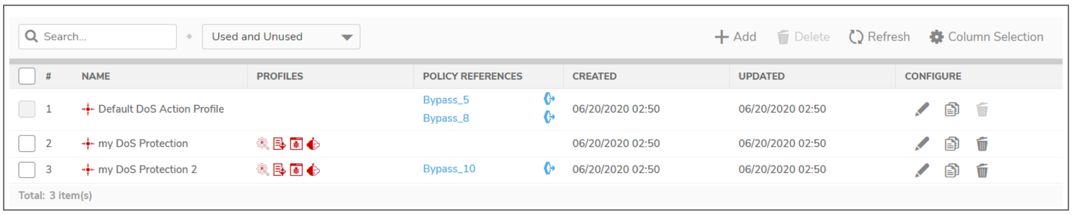
4. Enter a friendly **DoS Rule Action Name**.
5. Enable Connection Limiting.

6. Configure options and thresholds as necessary.
7. Click **Save**.

Editing DoS Action Profiles

To edit an existing DoS Action Profile:

1. Navigate to **OBJECT | Action Profiles > DoS Action Profile**.



□	#	NAME	PROFILES	POLICY REFERENCES	CREATED	UPDATED	CONFIGURE
□	1	Default DoS Action Profile		Bypass_5 Bypass_8	06/20/2020 02:50	06/20/2020 02:50	
□	2	my DoS Protection			06/20/2020 02:50	06/20/2020 02:50	
□	3	my DoS Protection 2		Bypass_10	06/20/2020 02:50	06/20/2020 02:50	

Total: 3 item(s)

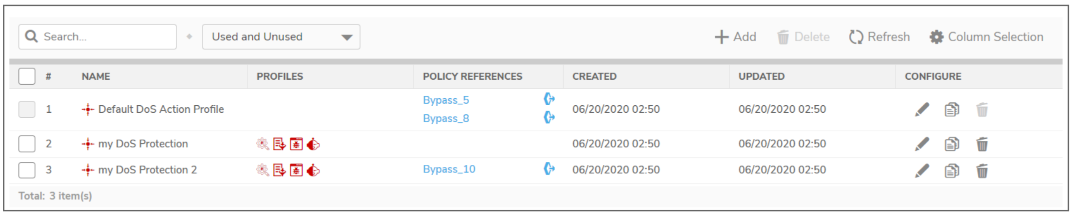
2. Click the DoS Action Profile you would to edit one time and in the right **Configure** column, click the **Edit** icon for the DoS Rule Object.

   This opens the **Edit DoS Action Profile** page, which you can modify or update.
3. Make changes to the **Edit DoS Action Profile** page.
4. Click **Save**.

Cloning DoS Action Profiles

To clone an existing DoS Action Profile:

1. Navigate to **OBJECT | Action Profiles > DoS Action Profile**.



□	#	NAME	PROFILES	POLICY REFERENCES	CREATED	UPDATED	CONFIGURE
□	1	Default DoS Action Profile		Bypass_5 Bypass_8	06/20/2020 02:50	06/20/2020 02:50	
□	2	my DoS Protection			06/20/2020 02:50	06/20/2020 02:50	
□	3	my DoS Protection 2		Bypass_10	06/20/2020 02:50	06/20/2020 02:50	

Total: 3 item(s)

2. Click the DoS Rule Action Object you would to clone one time and in the right **Configure** column, click the **Clone** icon for the DoS Action Object.

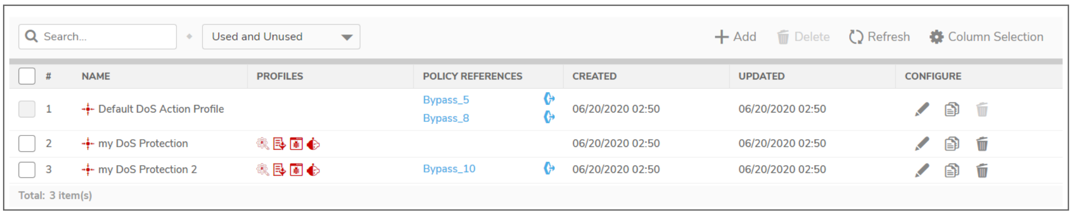
   This creates a duplicate of the page, which allows you the basis to create a new DoS Action Profile using the similar content.
3. Make changes to the **Clone DoS Action Profile** form.

Deleting DoS Action Profiles

ⓘ **NOTE:** Only custom DoS Action Profiles can be deleted. You cannot delete the Default DoS Action Profiles page.

To delete a custom DoS Action Profile page message:

1. Navigate to **OBJECT | Action Profiles > DoS Action Profile**.



□	#	NAME	PROFILES	POLICY REFERENCES	CREATED	UPDATED	CONFIGURE
□	1	Default DoS Action Profile		Bypass_5 Bypass_8	06/20/2020 02:50	06/20/2020 02:50	
□	2	my DoS Protection			06/20/2020 02:50	06/20/2020 02:50	
□	3	my DoS Protection 2		Bypass_10	06/20/2020 02:50	06/20/2020 02:50	

Total: 3 item(s)

2. Click the **DoS Action Profile** page you would to delete one time and in the right **Configure** column, click the **Trash** can icon.

   A confirmation message appears.

3. Click **OK** or **Cancel**.

To delete ALL custom DoS Action Project pages, click the top box to the left of the DoS Action Profile Page names and click the **Trash** icon from the top toolbar.

3

SonicWall Support

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

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 and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access https://mysonicwall.com
- 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

ⓘ | **NOTE:** A NOTE icon indicates supporting information.

ⓘ | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

ⓘ | **TIP:** A TIP icon indicates helpful information.

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

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

SonicOSX Action Profiles Administration Guide
Updated - August 2020
Software Version - 7
232-005324-00 Rev A

The information in this document is provided in connection with SonicWall 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 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. 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 Inc. 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
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035