SonicOSX 7
Profile Objects

Administration Guide

Contents

Endpoint Security

With Endpoint Security, you can manage logs for your product subscriptions and licensed security products in one location. Security products include Capture Client, Content Filtering, Intrusion Prevention, App Control, Botnet/GeoIP Filtering, and Gateway Anti-Virus/Anti Spyware/Capture ATP.

When enabled, Capture Client leverages cloud sandbox file testing, comprehensive reporting, and enforcement for endpoint protection, while providing consistent assurance of client security, with easy-to-use and actionable intelligence and reporting.

Endpoint Security can secure your endpoints no matter where they are located and help you keep them clean of malware while enforcing access and content rules.

For configuring Endpoint Security, refer *Policy* > *Endpoint Security* section of SonicOS.

A default Endpoint Security Profile, **Endpoint Enforcement Default Profile**, is created by SonicOS. You can configure and edit this Endpoint Security profile, but you cannot delete it.

To add an Endpoint Security profile:

1. Navigate to **Object > Profile Objects > Endpoint Security** page.
2. Click **Add** icon on the top of the page.
3. Enter the name of the Endpoint Security Profile in the **Name** field.
4. Toggle the **Bypass Guest Endpoint Security Service** option to enable it. Enabling this option bypasses guest check for Endpoint Security when guest service is enabled on matched zone.
5. Toggle the **Capture Client Endpoint Security** option to enable it.
6. Click **Save**. The Endpoint Security profile is created.

To delete an Endpoint Security profile:

1. Navigate to **Object > Profile Objects > Endpoint Security** page.
2. Select the check box of an Endpoint Security profile which you want to delete and click **Delete** icon on the top of the page.

   OR

   Hover on the Endpoint Security profile and click **Delete** icon.

2

Bandwidth

Topics:

Understanding Bandwidth Profiles

Bandwidth management (BWM) is a means of allocating bandwidth resources to critical applications on a network through the use of an established use profile.

SonicOS offers an integrated traffic shaping mechanism through its outbound (Egress) and inbound (Ingress) BWM interfaces. Egress BWM can be applied to traffic sourced from Trusted and Public zones traveling to Untrusted and Encrypted zones. Ingress BWM can be applied to traffic sourced from Untrusted and Encrypted zones traveling to Trusted and Public zones.

The SonicWall security appliance uses BWM to control ingress and egress traffic. BWM allows network administrators to guarantee minimum bandwidth and prioritize traffic based on policies created in the **OBJECT | Profiles > Bandwidth** page of the management interface. By controlling the amount of bandwidth to an application or user, you can prevent a small number of applications or users to consume all available bandwidth. Balancing the bandwidth allocated to different network traffic and then assigning priorities to traffic can improve network performance.

ⓘ **NOTE:** Although BWM is a fully integrated Quality of Service (QoS) system, wherein classification and shaping is performed on the single SonicWall appliance, effectively eliminating the dependency on external systems thereby obviating the need for marking, it is possible to concurrently configure **BWM** and **QoS** (layer 2 and/or layer 3 marking) settings on a single Access Rule. This allows those external systems to benefit from the classification performed on the firewall even after it has already shaped the traffic. For BWM QoS details, refer to *Managing Quality of Service*.

BWM Traffic Priority Queues lists the SonicOS traffic priority queues.

BWM TRAFFIC PRIORITY QUEUES

0 – Realtime	3 – Medium High	6 – Low
1 – Highest	4 – Medium	7 – Lowest
2 – High	5 – Medium Low	

Various types of bandwidth management are available and can be selected on the **OBJECT | Profiles > Bandwidth** page.

BANDWIDTH MANAGEMENT TYPES

BWM Type	Description
Advanced	Enables Advanced Bandwidth Management. Maximum egress and ingress bandwidth limitations can be configured on any interface, per interface, by configuring bandwidth objects, access rules, and application policies and attaching them to the interface.
Global	All zones can have assigned guaranteed and maximum bandwidth to services and have prioritized traffic. When global BWM is enabled on an interface, all of the traffic to and from that interface is bandwidth managed according to the priority queue. Default Global BWM queues: • 2 — High • 4 — Medium • 6 — Low 4 Medium is the default priority for all traffic that is not managed by an Access rule or an Application Control Policy that is BWM enabled. For traffic more than 1 Gbps, maximum bandwidth is limited to 1 Gbps because of queuing, which may limit the number of packets processed.
None	(Default) Disables BWM.

If the bandwidth management type is **None**, and there are three traffic types that are using an interface, if the link capacity of the interface is 100 Mbps, the cumulative capacity for all three types of traffic is 100 Mbps.

When **Global** bandwidth management is enabled on an interface, all traffic to and from that interface is bandwidth managed. If the available ingress and egress traffic is configured at 10 Mbps, then by default, all three traffic types are sent to the medium priority queue. The medium priority queue, by default, has a guaranteed bandwidth of 50 percent and a maximum bandwidth of 100 percent. If no **Global** bandwidth management policies are configured, the cumulative link capacity for each traffic type is 10 Mbps.

ⓘ **NOTE:** BWM rules each consume memory for packet queuing, so the number of allowed queued packets and rules on SonicOS is limited by platform (values are subject to change).

Global uses the unused guaranteed bandwidth from other queues for maximum bandwidth. If there is only default or single-queue traffic and all the queues have a total of 100% allocated as guaranteed, **Global** uses the unused global bandwidth from other queues to give you up to maximum bandwidth for the default/single queue.

Bandwidth Profiles

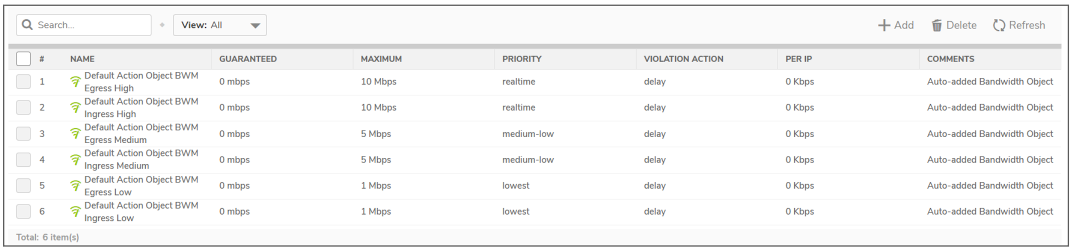
Bandwidth profiles are based on policies that specify bandwidth limitations for traffic classes. A complete bandwidth management policy consists of two parts: a classifier and a bandwidth rule.

A classifier specifies the actual parameters, such as priority, guaranteed bandwidth, and maximum bandwidth, and is configured in a bandwidth object. Classifiers identify and organize packets into traffic classes by matching specific criteria.

To configure a Bandwidth Profile:

1. Navigate to **OBJECT | Profiles > Bandwidth**.

   The **Bandwidth** page appears.



□	#	NAME	GUARANTEED	MAXIMUM	PRIORITY	VIOLATION ACTION	PER IP	COMMENTS
□	1	Default Action Object BWM Egress High	0 mbps	10 Mbps	realtime	delay	0 Kbps	Auto-added Bandwidth Object
□	2	Default Action Object BWM Ingress High	0 mbps	10 Mbps	realtime	delay	0 Kbps	Auto-added Bandwidth Object
□	3	Default Action Object BWM Egress Medium	0 mbps	5 Mbps	medium-low	delay	0 Kbps	Auto-added Bandwidth Object
□	4	Default Action Object BWM Ingress Medium	0 mbps	5 Mbps	medium-low	delay	0 Kbps	Auto-added Bandwidth Object
□	5	Default Action Object BWM Egress Low	0 mbps	1 Mbps	lowest	delay	0 Kbps	Auto-added Bandwidth Object
□	6	Default Action Object BWM Ingress Low	0 mbps	1 Mbps	lowest	delay	0 Kbps	Auto-added Bandwidth Object

Total: 6 item(s)

Topics:

- Configuring Bandwidth Object Settings
- Configuring BWM in a Security Rule Action
- Configuring BWM on an Interface

Configuring Bandwidth Object Settings

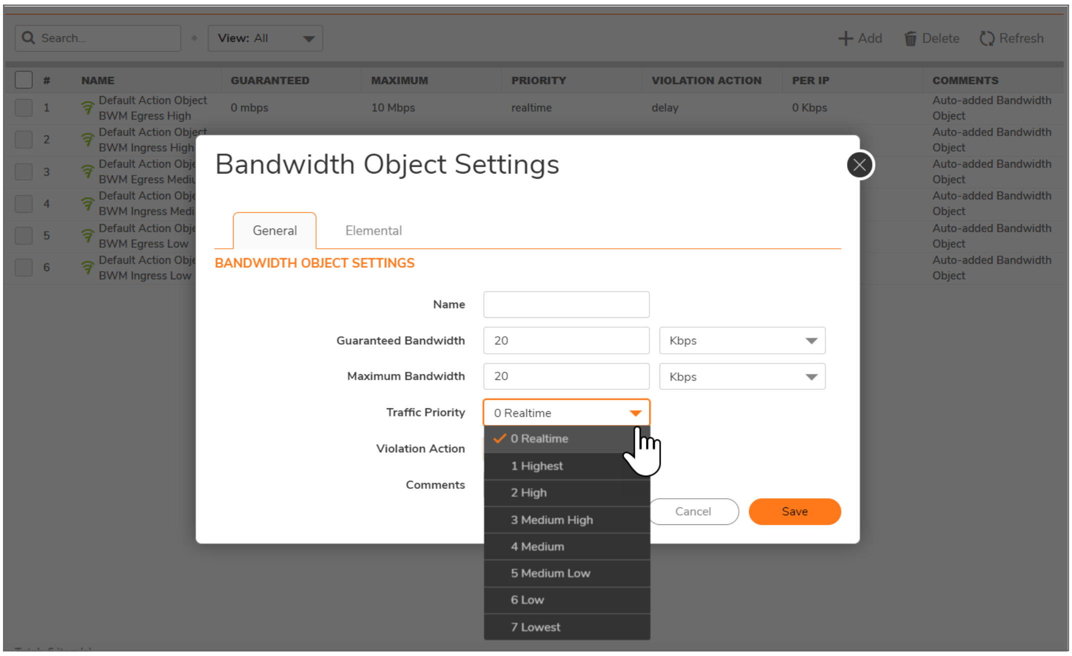
BWM works by first enabling bandwidth management in the **OBJECT | Profiles > Bandwidth** page, enabling BWM on an interface/firewall/app rule, and then allocating the available bandwidth for that interface on the ingress and egress traffic. It then assigns individual limits for each class of network traffic. By assigning priorities to network traffic, applications requiring a quick response time, such as Telnet, can take precedence over traffic requiring less response time, such as FTP.

To view the BWM configuration:

1. Navigate to the **OBJECT | Profiles > Bandwidth** page.

   > ⓘ **NOTE:** The default settings for this page consists of three priorities with preconfigured guaranteed and maximum bandwidth. The medium priority has the highest guaranteed value as this priority queue is used by default for all traffic not governed by a BWM-enabled policy.

   > ⓘ **NOTE:** The defaults are set by SonicWall to provide BWM ease-of-use. It is recommended that you review your specific bandwidth needs and enter the values on this page accordingly.



	#	NAME	GUARANTEED	MAXIMUM	PRIORITY	VIOLATION ACTION	PER IP	COMMENTS
□	1	Default Action Object BWM Egress High	0 mbps	10 Mbps	realtime	delay	0 Kbps	Auto-added Bandwidth Object
□	2	Default Action Object BWM Ingress High						Auto-added Bandwidth Object
□	3	Default Action Obje BWM Egress Mediu						Auto-added Bandwidth Object
□	4	Default Action Obje BWM Ingress Medi						Auto-added Bandwidth Object
□	5	Default Action Obje BWM Egress Low						Auto-added Bandwidth Object
□	6	Default Action Obje BWM Ingress Low						Auto-added Bandwidth Object

Bandwidth Object Settings

BANDWIDTH OBJECT SETTINGS

Name

Guaranteed Bandwidth: 20 Kbps

Maximum Bandwidth: 20 Kbps

Traffic Priority: 0 Realtime

Violation Action

Comments

2. Click **+Add**.
3. For **Guaranteed Bandwidth**, enter the bandwidth that is guaranteed to be provided for a particular traffic class.
4. For **Maximum Bandwidth**, enter the maximum bandwidth that a traffic class can utilize.
5. In the **Traffic Priority**: field(s), enter the priority level from 0 for **Realtime** to 7 for **Lowest**. The priority levels are **1 Highest**, **2 High**, **3 Medium High**, **4 Medium**, **5 Medium Low**, **6 Low**, and **7 Lowest**.
6. For Violation Action, The firewall action that occurs when traffic exceeds the maximum bandwidth.
    - **Delay** – packets are queued and sent when possible.
    - **Drop** – packets are dropped immediately.
7. Click **Save**.

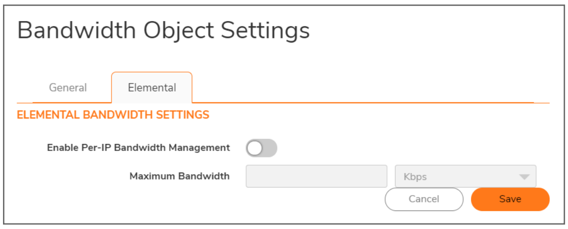
Elemental Bandwidth Object Settings

Elemental bandwidth object settings provide a method of allowing a single BWM rule to apply to the individual elements of that rule. Per-IP Bandwidth Management is an “Elemental” feature that is a sub-option of **Bandwidth Object Settings**. When Per-IP BWM is enabled, the elemental bandwidth settings are applied to each individual IP under its parent rule.

The Elemental Bandwidth Object Settings feature enables a bandwidth object to be applied to individual elements under a parent traffic class. Elemental Bandwidth Object Settings is a sub-option of **OBJECT | Profiles > Bandwidth**, the parent rule or traffic class.

To display the Elemental Bandwidth Object Settings dialog:

1. Click **+Add** to see **Bandwidth Object Settings**.
2. Click **Elemental**.



Bandwidth Object Settings

ELEMENTAL BANDWIDTH SETTINGS

Enable Per-IP Bandwidth Management ○

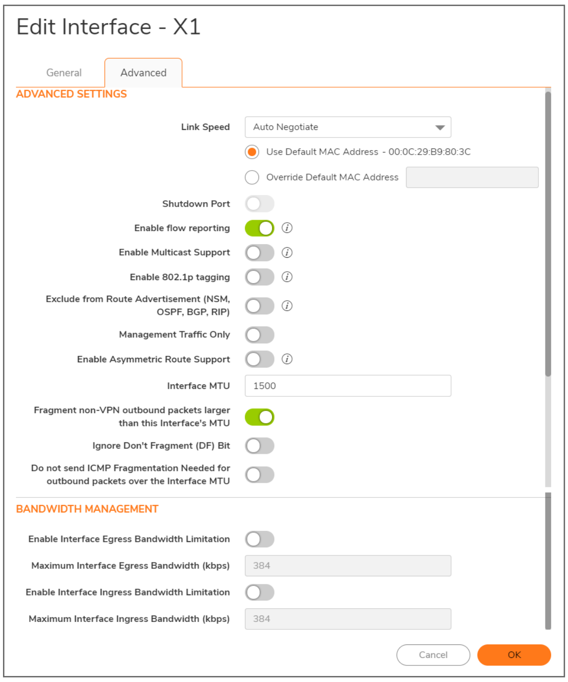
Maximum Bandwidth: Kbps

3. Click the checkbox next to **Enable Per-IP Bandwidth Management**.
4. Enter the **Maximum Bandwidth** in either kbps (default) or Mbps from the drop-down.
5. Click **Save**.

Configuring BWM on an Interface

To configure BWM on an interface:

1. Navigate to **NETWORK | System > Interfaces**.
2. In the **Interface Settings** table, click **Edit the Interface** under the **Configure** column for the appropriate interface. The **Edit Interface** dialog displays.
3. Click **Advanced**.



Edit Interface - X1

ADVANCED SETTINGS

Link Speed: Auto Negotiate

● Use Default MAC Address - 00:0C:29:B9:80:3C

○ Override Default MAC Address

Shutdown Port: off

Enable flow reporting: on

Enable Multicast Support: off

Enable 802.1p tagging: off

Exclude from Route Advertisement (NSM, OSPF, BGP, RIP): off

Management Traffic Only: off

Enable Asymmetric Route Support: off

Interface MTU: 1500

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

Ignore Don't Fragment (DF) Bit: off

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

BANDWIDTH MANAGEMENT

Enable Interface Egress Bandwidth Limitation: off

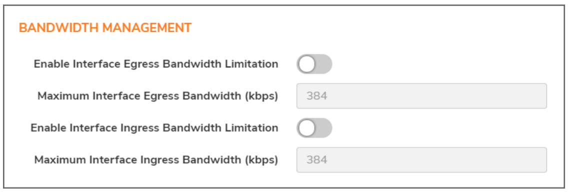
Maximum Interface Egress Bandwidth (kbps): 384

Enable Interface Ingress Bandwidth Limitation: off

Maximum Interface Ingress Bandwidth (kbps): 384

ⓘ | **NOTE:** Displayed options might differ depending on how the interface is configured.

4. Scroll to **Bandwidth Management**.



BANDWIDTH MANAGEMENT

Enable Interface Egress Bandwidth Limitation	○
Maximum Interface Egress Bandwidth (kbps)	384
Enable Interface Ingress Bandwidth Limitation	○
Maximum Interface Ingress Bandwidth (kbps)	384

5. Select either or both **Enable Interface Egress Bandwidth Limitation** and **Enable Interface Ingress Bandwidth Limitation**. These options are not selected by default.

   When either or both of these options are selected, if a there is not a corresponding Access Rule or App Rule, the total egress traffic on the interface is limited to the amount specified in the **Enable Interface Ingress Bandwidth Limitation (kbps)** field.

   When neither option is selected, no bandwidth limitation is set at the interface level, but egress traffic can still be shaped using other options.
6. In the **Maximum Interface Egress/Ingress Bandwidth (Kbps)** field(s), enter the total bandwidth available for all egress/ingress traffic in Kbps. The default is **384.000000** Kbps.
7. Click **OK**.

Configuring BWM in a Security Rule Action

> **IMPORTANT:** BWM must be enabled on **OBJECT | Actions > Security Rule | Bandwidth/QoS** first, as described in *Configuring Bandwidth Management*.

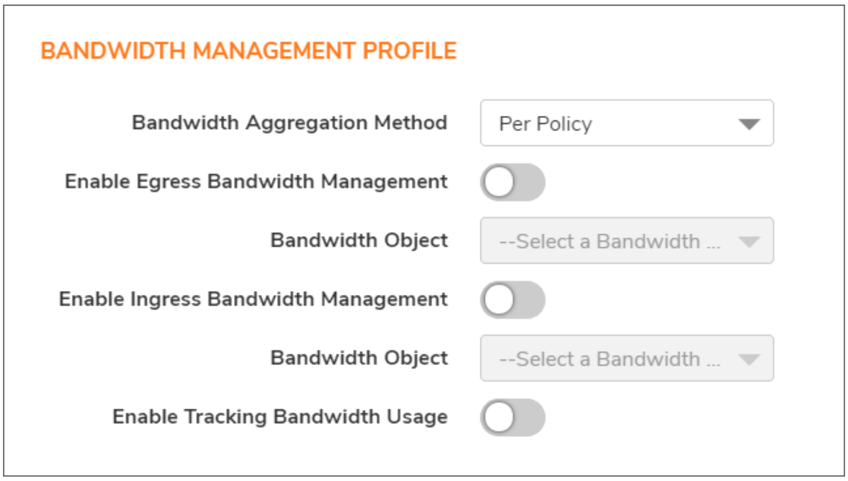
You can configure BWM in each Security Action Rule. This method configures the direction in which to apply BWM and sets the priority queue.

> **IMPORTANT:** Before you can configure any priorities in a Security Action Rule, you must first enable the traffic priorities that you want to use on the **OBJECT | Profiles > Bandwidth** page. Refer to this page to determine which priorities are enabled. If you select a Traffic Priority that is not enabled on the **OBJECT | Profiles > Bandwidth** page, the traffic is automatically mapped to priority **4 Medium**. See *Configuring Bandwidth Management*.

Priorities are listed in the **Bandwidth Object Settings** dialog.

To configure BWM in a Security Rule:

1. Navigate to the **OBJECT | Actions > Security Rule** page.
2. Click the **Edit** icon for the rule you want to edit. The **Edit Security Rule Action** dialog displays.



BANDWIDTH MANAGEMENT PROFILE

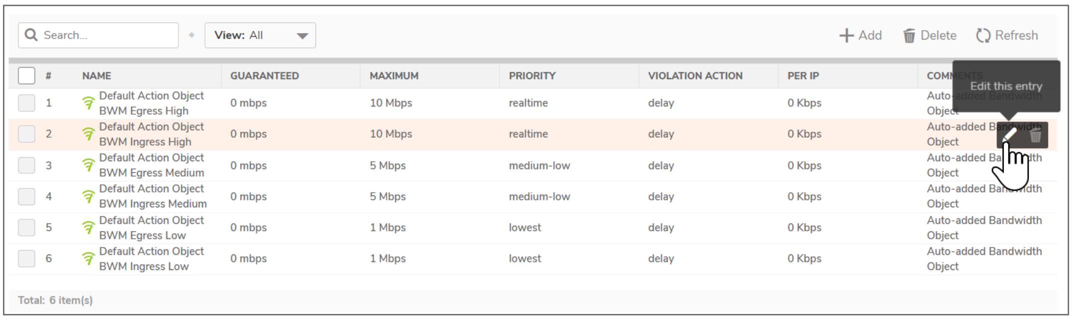
Bandwidth Aggregation Method	Per Policy ▾
Enable Egress Bandwidth Management	○
Bandwidth Object	--Select a Bandwidth ... ▾
Enable Ingress Bandwidth Management	○
Bandwidth Object	--Select a Bandwidth ... ▾
Enable Tracking Bandwidth Usage	○

3. Determine the **Bandwidth Aggregation Method**, whether to aggregate **Per Policy**, or **Per Action**.
4. Select either or both **Enable Egress Bandwidth Management** and **Enable Ingress Bandwidth Management**. These options are not selected by default.
5. Select a **Bandwidth Object** for Ingress or Egress from the drop-down menus.
6. Click **Enable Tracking Bandwidth Usage**.
7. Click **Save**.
8. Navigate to **OBJECT | Profiles > Bandwidth**. See Bandwidth Profiles.

Editing Bandwidth Profiles

To edit the Bandwidth Object Settings configuration:

1. Navigate to the **OBJECT | Profiles > Bandwidth** page.
2. Hover your mouse over the Bandwidth Object you would like to modify.

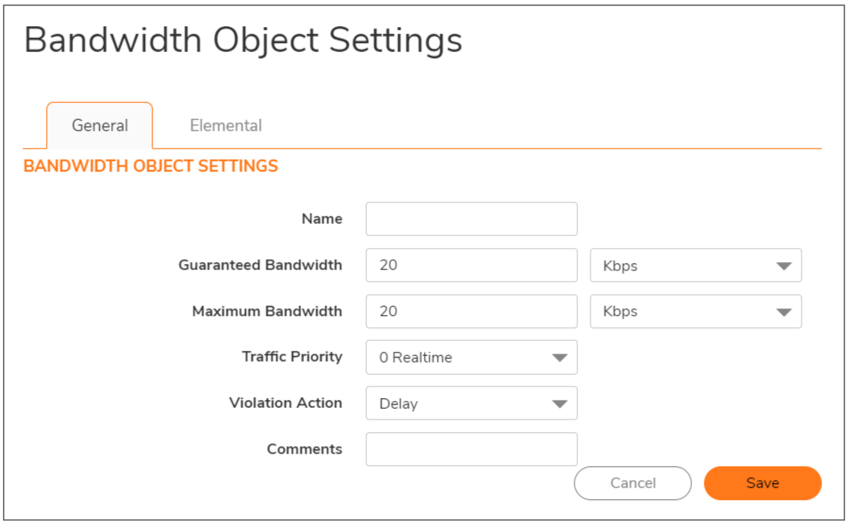


□	#	NAME	GUARANTEED	MAXIMUM	PRIORITY	VIOLATION ACTION	PER IP	COMMENTS
□	1	Default Action Object BWM Egress High	0 mbps	10 Mbps	realtime	delay	0 Kbps	Auto-added Bandwidth Object
□	2	Default Action Object BWM Ingress High	0 mbps	10 Mbps	realtime	delay	0 Kbps	Auto-added Bandwidth Object
□	3	Default Action Object BWM Egress Medium	0 mbps	5 Mbps	medium-low	delay	0 Kbps	Auto-added Bandwidth Object
□	4	Default Action Object BWM Ingress Medium	0 mbps	5 Mbps	medium-low	delay	0 Kbps	Auto-added Bandwidth Object
□	5	Default Action Object BWM Egress Low	0 mbps	1 Mbps	lowest	delay	0 Kbps	Auto-added Bandwidth Object
□	6	Default Action Object BWM Ingress Low	0 mbps	1 Mbps	lowest	delay	0 Kbps	Auto-added Bandwidth Object

Total: 6 item(s)

3. Click the **Edit this entry** icon from the **Configure** pop-up.

   The **Bandwidth Object Settings** page appears.



Bandwidth Object Settings

BANDWIDTH OBJECT SETTINGS

Name		
Guaranteed Bandwidth	20	Kbps
Maximum Bandwidth	20	Kbps
Traffic Priority	0 Realtime	
Violation Action	Delay	
Comments		

4. Change the necessary settings and click **Save**.

Deleting Bandwidth Profiles

ⓘ | **NOTE:** You cannot delete the default Bandwidth Objects.

To delete custom Bandwidth Objects:

1. Navigate to the **OBJECT | Profiles > Bandwidth** page.
2. Select the left checkbox(es) of the custom Bandwidth Object(s) you would like to remove from the Bandwidth Profiles table. You can also select the top left checkbox to remove **ALL** custom Bandwidth Objects.
3. Click **Delete** from the top toolbar. You can also hover over an individual Bandwidth Object and click the **Trash** icon from the **Configure** pop-up.

3

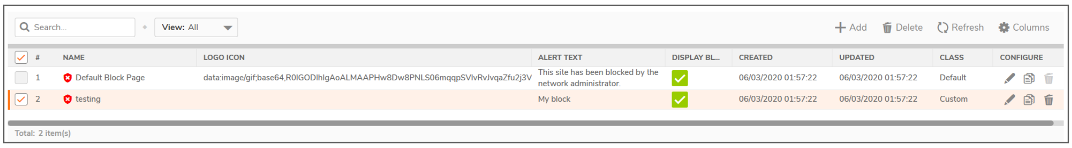
Block Page

You can configure a default message that displays when another user attempts to access a blocked page. You can have the message display detailed information, such as the reason why this IP address was 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.

Customizing Block Page Settings

To create a custom block page message:

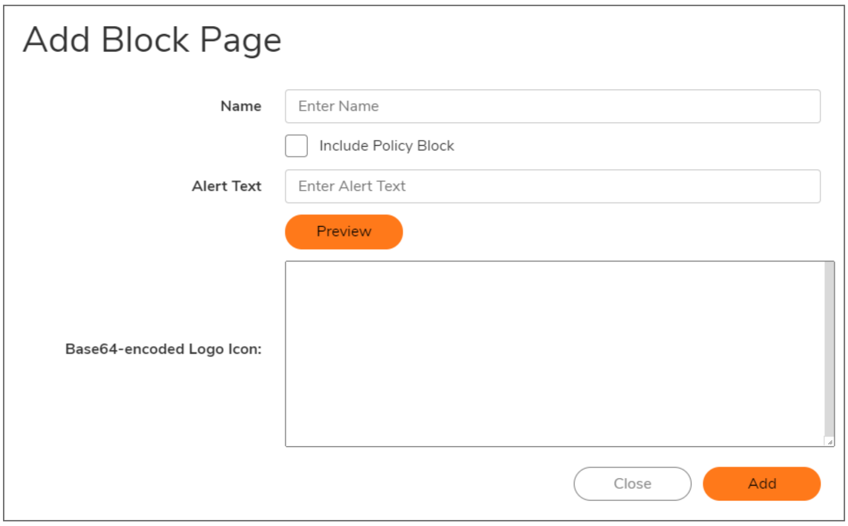
1. Navigate to **OBJECT | Profiles > Block Page**.



☑	#	NAME	LOGO ICON	ALERT TEXT	DISPLAY BL...	CREATED	UPDATED	CLASS	CONFIGURE
□	1	Default Block Page	data:image/gif;base64,R0IGODlhIgAoALMAAPHw8Dw8PNLS06mqqpSVlvRvJvqaZfu2j3V	This site has been blocked by the network administrator.	✓	06/03/2020 01:57:22	06/03/2020 01:57:22	Default	
☑	2	testing		My block	✓	06/03/2020 01:57:22	06/03/2020 01:57:22	Custom	

Total: 2 item(s)

2. Click **+Add**.



Add Block Page

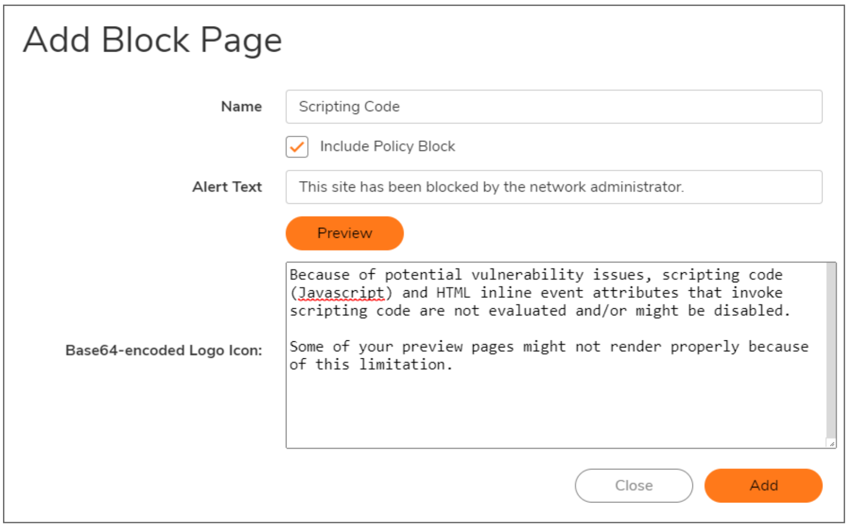
Name: Enter Name

□ Include Policy Block

Alert Text: Enter Alert Text

3. Ensure the **Include Policy Block** option 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:
   - Enter a message to be displayed in the Alert text field, such as `This site has been blocked by the network administrator.`
   - Specify a custom message to be displayed in the **Base64-encoded Logo Icon** page in the 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 instead of the default SonicWall logo.



Add Block Page

Name: Scripting Code

☑ Include Policy Block

Alert Text: This site has been blocked by the network administrator.

Preview

Base64-encoded Logo Icon:

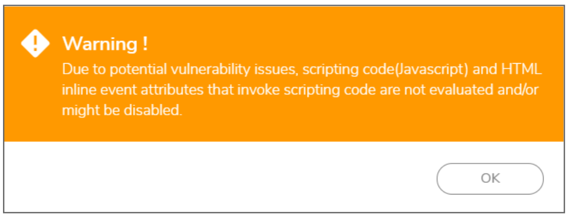
```
Because of potential vulnerability issues, scripting code
(Javascript) and HTML inline event attributes that invoke
scripting code are not evaluated and/or might be disabled.

Some of your preview pages might not render properly because
of this limitation.
```

Close   Add

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.

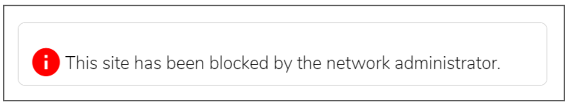


Warning !

Due to potential vulnerability issues, scripting code(Javascript) and HTML inline event attributes that invoke scripting code are not evaluated and/or might be disabled.

OK

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



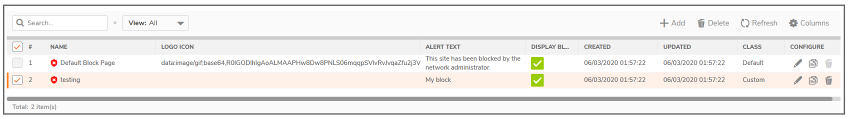
This site has been blocked by the network administrator.

8. Close the **Web Site Blocked** message.
9. Click **Add**.

Cloning Block Pages

To clone an existing custom block page message:

1. Navigate to **OBJECT | Profiles > Block Page**.

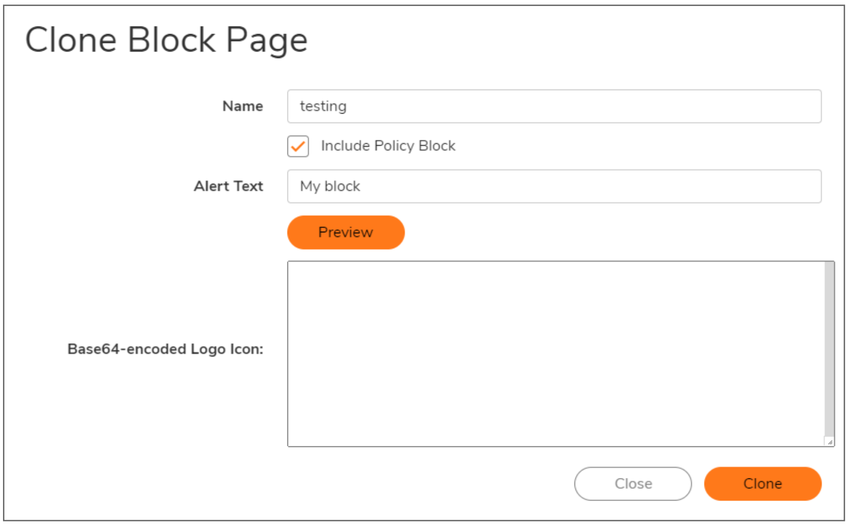


Search... View: All + Add Delete Refresh Columns

☑	#	NAME	LOGO ICON	ALERT TEXT	DISPLAY BL...	CREATED	UPDATED	CLASS	CONFIGURE
□	1	Default Block Page	data:image/gif;base64,R0lGODlhlgAoALMAAPHw8Dw8PNLS06mqqpSVlvRvJvqaZfu2j3V	This site has been blocked by the network administrator.	✓	06/03/2020 01:57:22	06/03/2020 01:57:22	Default	
☑	2	testing		My block	✓	06/03/2020 01:57:22	06/03/2020 01:57:22	Custom	

Total: 2 item(s)

2. Click the Block Page you would to clone one time and in the right **Configure** column, click the **Clone** icon for the Block Page.



Clone Block Page

Name: testing

☑ Include Policy Block

Alert Text: My block

Base64-encoded Logo Icon:

This creates a duplicate of the page, which allows you the basis to create a new Block Page using the similar content.

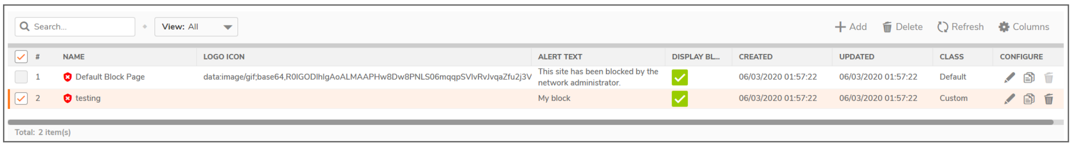
3. Make changes to the **Clone Block Page** form as described in Customizing Block Page Settings.

Deleting Block Pages

ⓘ | **NOTE:** Only custom Block Pages can be deleted. You cannot delete the Default Block Page.

To delete a custom block page message:

1. Navigate to **OBJECT | Profiles > Block Page**.



Search... View: All + Add Delete Refresh Columns

☑	#	NAME	LOGO ICON	ALERT TEXT	DISPLAY BL...	CREATED	UPDATED	CLASS	CONFIGURE
□	1	Default Block Page	data:image/gif;base64,R0lGODlhlgAoALMAAPHw8Dw8PNLS06mqqpSVlvRvJvqaZfu2j3V	This site has been blocked by the network administrator.	✓	06/03/2020 01:57:22	06/03/2020 01:57:22	Default	
☑	2	testing		My block	✓	06/03/2020 01:57:22	06/03/2020 01:57:22	Custom	

Total: 2 item(s)

2. Click the Block 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 Block Pages, click the top box to the left of the Block Page names and click the **Trash** icon from the top toolbar.

4

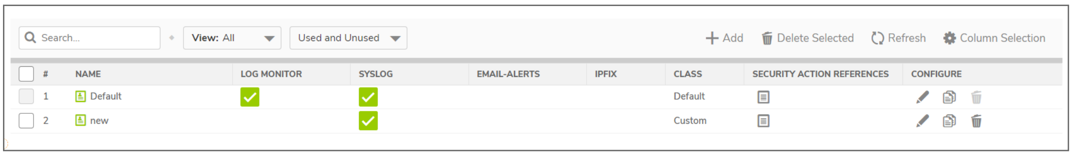
Log and Alerts

Use **Log and Alerts** to filter packets with defined conditions that can be used with corresponding Action applications.

To configure Log and Alerts:

1. Navigate to **OBJECT | Profile Objects > Log and Alerts**.

   The **Log and Alerts** page appears.



□	#	NAME	LOG MONITOR	SYSLOG	EMAIL-ALERTS	IPFIX	CLASS	SECURITY ACTION REFERENCES	CONFIGURE
□	1	Default	✓	✓			Default		
□	2	new		✓			Custom		

Topics:

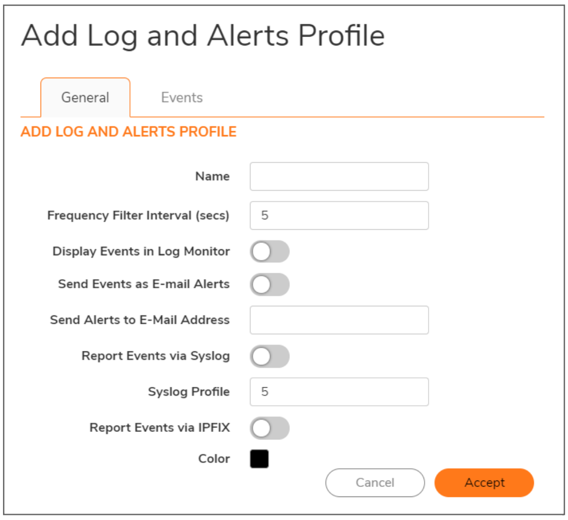
- Adding Log and Alerts Profiles
- Editing Log and Alert Profiles
- Deleting Log and Alert Profiles

Adding Log and Alerts Profiles

To add a Log and Alert Profile:

1. Navigate to **OBJECT | Profile Objects > Log and Alerts**.
2. Click **+Add**.

   The **Add Reporting Profile** dialog appears.


Add Log and Alerts Profile

ADD LOG AND ALERTS PROFILE

Name

Frequency Filter Interval (secs) 5

Display Events in Log Monitor ○

Send Events as E-mail Alerts ○

Send Alerts to E-Mail Address

Report Events via Syslog ○

Syslog Profile 5

Report Events via IPFIX ○

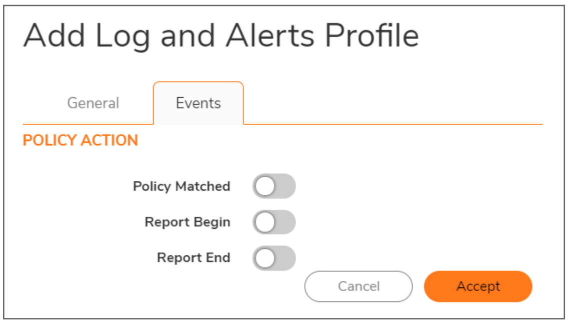
Color ■

3. On the **General** tab, enter a friendly **Name** for your profile.
4. For the **Frequency Filter Interval (secs)** field, enter the number of seconds between reports.

   ⓘ **TIP:** The **Frequency Filter Interval (secs)** field enables you to enter time intervals (in seconds) to avoid duplication of a log message within an interval. The range for these intervals is 0 to 86400 seconds. For Syslog messages, the default interval is 90 seconds. For alert messages, the default interval is 900 seconds.
5. If you want to display the log events in the Log Monitor, select **Enable** for **Display Events in Log Monitor**.
6. If you want to send events as email alerts, select **Enable** for **Send Events as E-mail Alerts** and include the email address as to where to send the alerts.
7. If you want to report events through Syslog, select **Enable** for **Report Events via Syslog**.
8. Indicate the number of the **Sylog Profile** you would like to use.
9. If you would like to report events by way of IPFIX, select **Enable** for **Report Events via IPFIX**.
10. If you want to use a specific color for this Reporting log, click the sample **Color** box. The color selection matrix appears.
11. Click **Accept**.

Events

1. Click the **Events** tab.


Add Log and Alerts Profile

POLICY ACTION

Policy Matched ○

Report Begin ○

Report End ○

2. Enable **Policy Matched** to use the Reporting Profile to search for specific string patterns and highlight matched results.
3. Enable **Report Begin** to place results at the top of the Reporting table.
4. Enable **Report End** to place results at the bottom of the Reporting table.
5. Click **Accept**.

About Event Profiles

By configuring events globally for all Syslog Servers, the events generated from all the modules in the system are reported to all the configured Syslog servers. This generates an enormous amount of Syslog traffic that might cause issues, such as reduced performance or packet loss. Syslog server profiling, known as Event Profiling, allows more granular control by configuring events through the Syslog server instead at the global level. Also, there can be multiple groups of Syslog servers with different events reported to different groups of servers. You can specify up to 24 Event Profiles, with up to seven Syslog servers configured for each Event Profile, for a maximum of 168 Syslog servers per firewall.

ⓘ **IMPORTANT:** A GMS server being used for Syslog must belong to the Profile 0 group. That means the Profile 0 group can have up to eight servers total (seven Syslog servers and one GMS server).

The Event Profile is used, along with the Server Name and Port, to uniquely identify a Syslog server in the Syslog Server table. This allows multiple rows to have the same Name, and Port combination with different Profiles. Therefore, a Syslog server can be a member of more than one Event Profile group.

You can create specific Event Profiles for:

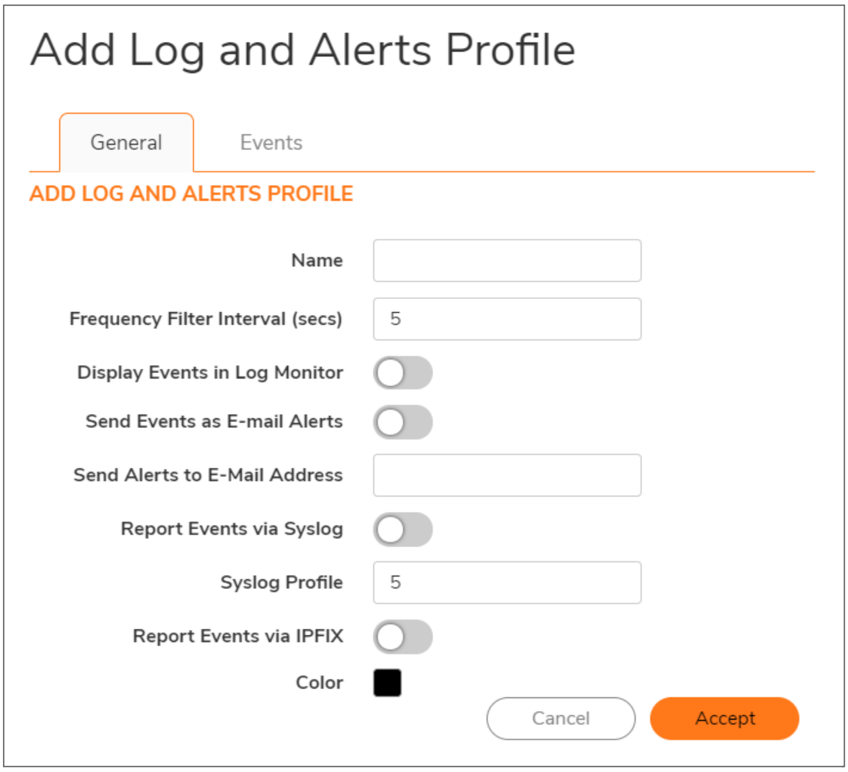
- Endpoint Security
- Bandwidth
- Block Pages
- Log and Alerts
- Intrusion Prevention
- QoS Marking
- DHCP Options
- AWS

Editing Log and Alert Profiles

To edit a Log and Alert Profile:

1. Navigate to **OBJECT | Profile Objects > Log and Alerts**.
2. In the **Configure** column of the profile you would like to modify, click **Edit**.

   The **Add Log and Alerts Profile** dialog appears.



Add Log and Alerts Profile

ADD LOG AND ALERTS PROFILE

Name	
Frequency Filter Interval (secs)	5
Display Events in Log Monitor	○
Send Events as E-mail Alerts	○
Send Alerts to E-Mail Address	
Report Events via Syslog	○
Syslog Profile	5
Report Events via IPFIX	○
Color	■

3. Configure the profile using the same settings as Adding Log and Alerts Profiles.

Deleting Log and Alert Profiles

To delete custom Log and Alert Profiles:

1. Navigate to **OBJECT | Profile Objects > Log and Alerts**.
2. To delete one profile, click the trashcan in the **Configure** column for the profile you would like to remove. Or for multiple profiles, click the checkboxes in the left column for the Log and Alert Profiles you would like removed.
3. Click **Delete Selected** from the top toolbar.
4. A warning message appears. Click **Confirm** or **Cancel**.

   ⓘ | **NOTE:** You cannot delete the **Default** profile.

To delete all custom Log and Alert Profiles:

1. Navigate to **OBJECT | Profile Objects > Log and Alerts**.
2. Click the top checkbox in the left column.

   All custom Log and Alert Profiles are selected.
3. Click **Delete Selected** from the top toolbar.
4. A warning message appears. Click **Confirm** or **Cancel**.

   ⓘ | **NOTE:** You cannot delete the **Default** profile.

5

Intrusion Prevention

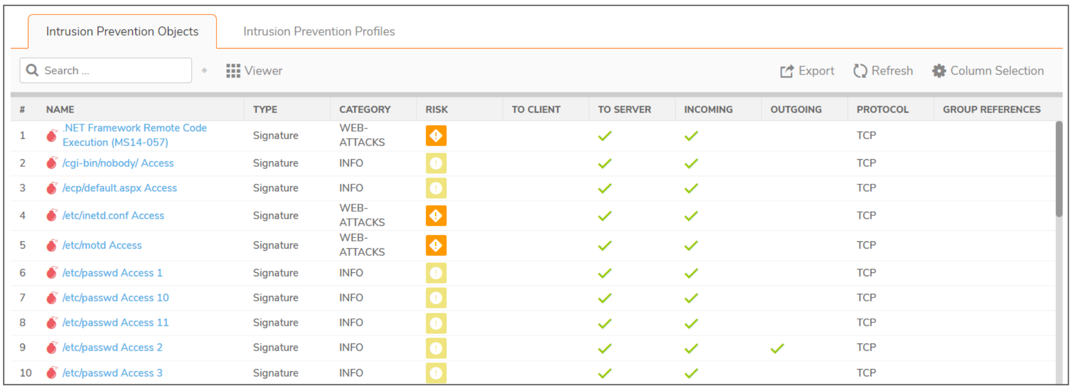
The **Intrusion Prevention Objects** panel allows you to view all SonicWall threat signatures and from the **Intrusion Prevention Profiles** tab you can configure the handling of those signatures by creating category profiles or groups on a signature by signature basis. Intrusion Prevention Profiles are signatures grouped together based on attributes such as types of attack.

Intrusion Prevention Profile objects are created at **OBJECT | Actions > Security Rule**. See the documentation for that feature for more information on setting up your Security Rule Actions.

To view the Intrusion Prevention Objects:

1. Navigate to **OBJECT | Profiles > Intrusion Prevention**.

   The Intrusion Prevention Object page appears.

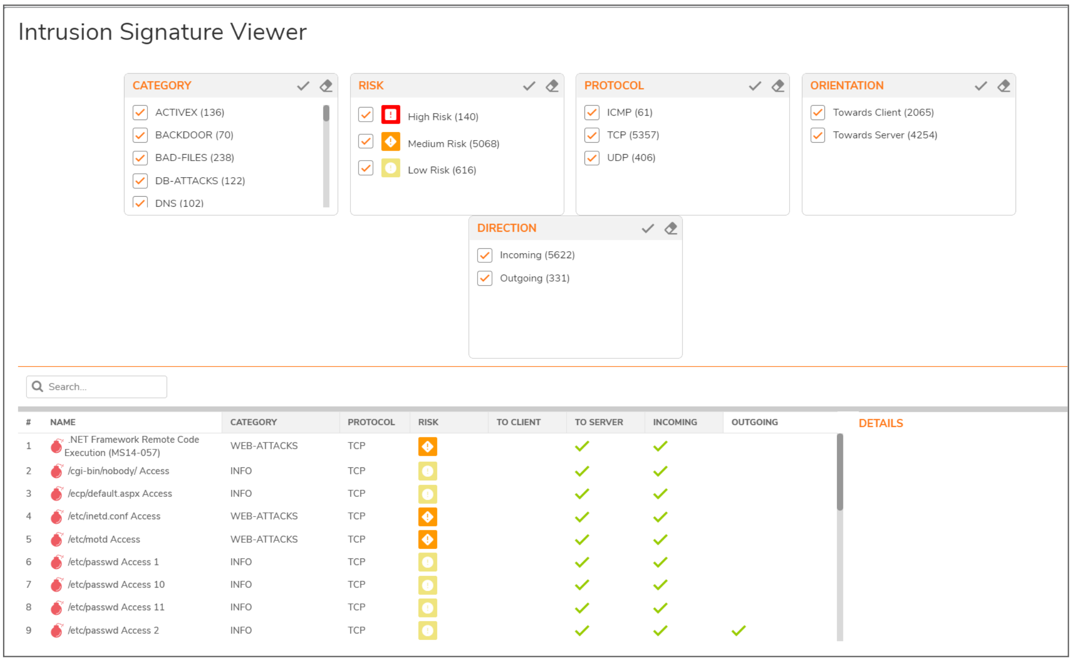


#	NAME	TYPE	CATEGORY	RISK	TO CLIENT	TO SERVER	INCOMING	OUTGOING	PROTOCOL	GROUP REFERENCES
1	.NET Framework Remote Code Execution (MS14-057)	Signature	WEB-ATTACKS	◆		✓	✓		TCP	
2	/cgi-bin/nobody/ Access	Signature	INFO	●		✓	✓		TCP	
3	/ecp/default.aspx Access	Signature	INFO	●		✓	✓		TCP	
4	/etc/inetd.conf Access	Signature	WEB-ATTACKS	◆		✓	✓		TCP	
5	/etc/motd Access	Signature	WEB-ATTACKS	◆		✓	✓		TCP	
6	/etc/passwd Access 1	Signature	INFO	●		✓	✓		TCP	
7	/etc/passwd Access 10	Signature	INFO	●		✓	✓		TCP	
8	/etc/passwd Access 11	Signature	INFO	●		✓	✓		TCP	
9	/etc/passwd Access 2	Signature	INFO	●		✓	✓	✓	TCP	
10	/etc/passwd Access 3	Signature	INFO	●		✓	✓		TCP	

2. Click the **Viewer** to help filter results.

   In the **Viewer**, you can narrow results based on **Category**, **Risk Level**, **Protocol**, **Orientation**, and

Direction. Results of your filtering appear in the lower portion of the **Viewer**.



Intrusion Signature Viewer

CATEGORY
- ☑ ACTIVEX (136)
- ☑ BACKDOOR (70)
- ☑ BAD-FILES (238)
- ☑ DB-ATTACKS (122)
- ☑ DNS (102)

RISK
- ☑ High Risk (140)
- ☑ Medium Risk (5068)
- ☑ Low Risk (616)

PROTOCOL
- ☑ ICMP (61)
- ☑ TCP (5357)
- ☑ UDP (406)

ORIENTATION
- ☑ Towards Client (2065)
- ☑ Towards Server (4254)

DIRECTION
- ☑ Incoming (5622)
- ☑ Outgoing (331)

Search...

#	NAME	CATEGORY	PROTOCOL	RISK	TO CLIENT	TO SERVER	INCOMING	OUTGOING
1	.NET Framework Remote Code Execution (MS14-057)	WEB-ATTACKS	TCP	◆		✓	✓	
2	/cgi-bin/nobody/ Access	INFO	TCP	●		✓	✓	
3	/ecp/default.aspx Access	INFO	TCP	●		✓	✓	
4	/etc/inetd.conf Access	WEB-ATTACKS	TCP	◆		✓	✓	
5	/etc/motd Access	WEB-ATTACKS	TCP	◆		✓	✓	
6	/etc/passwd Access 1	INFO	TCP	●		✓	✓	
7	/etc/passwd Access 10	INFO	TCP	●		✓	✓	
8	/etc/passwd Access 11	INFO	TCP	●		✓	✓	
9	/etc/passwd Access 2	INFO	TCP	●		✓	✓	✓

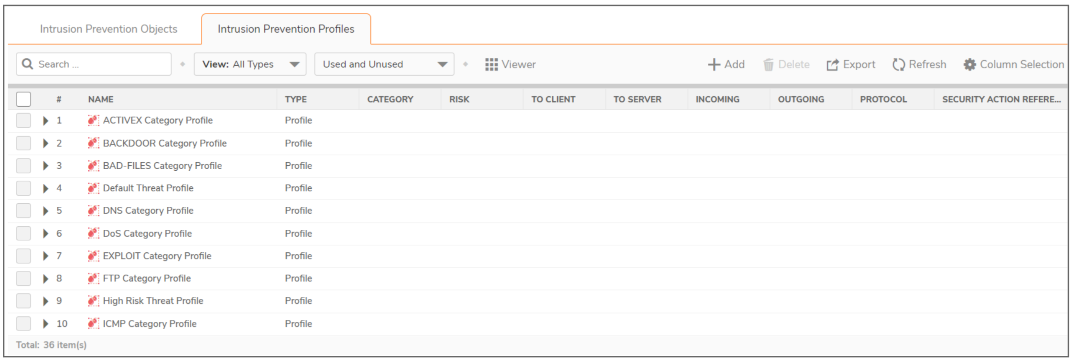
DETAILS

Configuring Intrusion Prevention Profiles

Create Intrusion Prevention Profiles to enforce rules and actions imposed through your Security Rule Actions. Filter your results with the **Intrusion Prevention Profiles Viewer**.

To configure Intrusion Prevention Profiles:

1. Navigate to **OBJECT | Profiles > Intrusion Prevention**.
2. Click the **Intrusion Prevention Profiles** tab.

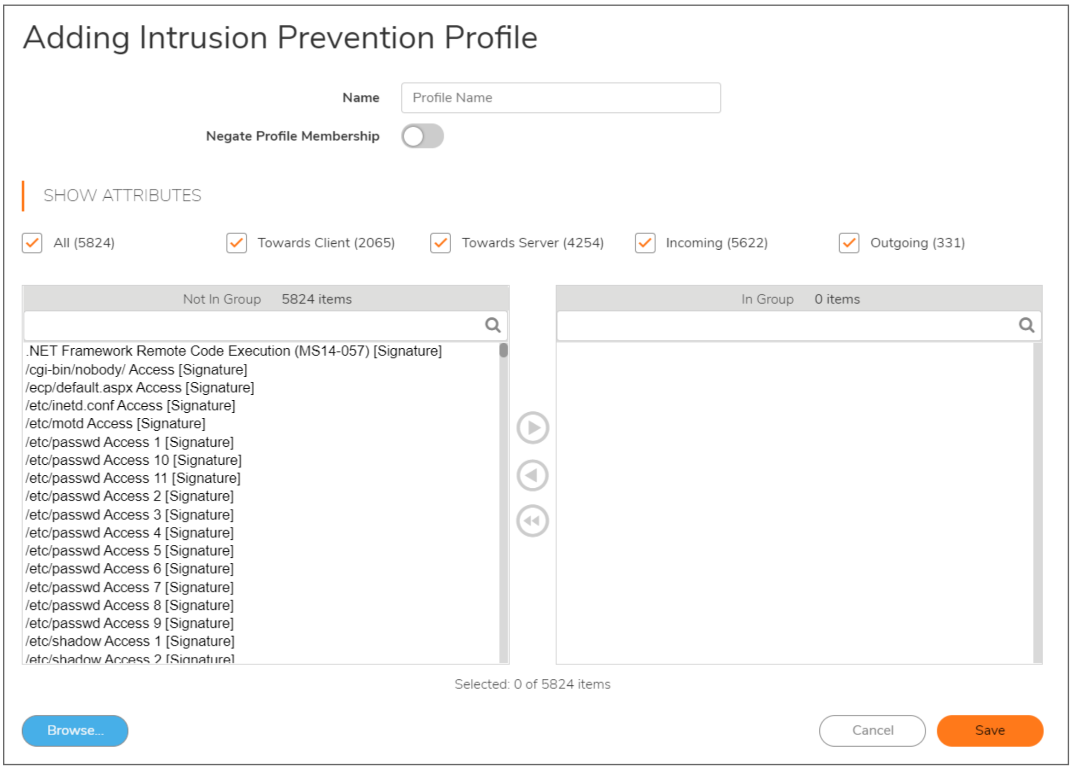


□	#	NAME	TYPE	CATEGORY	RISK	TO CLIENT	TO SERVER	INCOMING	OUTGOING	PROTOCOL	SECURITY ACTION REFERE...
□	1	ACTIVEX Category Profile	Profile								
□	2	BACKDOOR Category Profile	Profile								
□	3	BAD-FILES Category Profile	Profile								
□	4	Default Threat Profile	Profile								
□	5	DNS Category Profile	Profile								
□	6	DoS Category Profile	Profile								
□	7	EXPLOIT Category Profile	Profile								
□	8	FTP Category Profile	Profile								
□	9	High Risk Threat Profile	Profile								
□	10	ICMP Category Profile	Profile								

Total: 36 item(s)

3. Click **+Add**.

The **Adding Intrusion Prevention Profile** page appears.



Adding Intrusion Prevention Profile

Name: Profile Name

Negate Profile Membership: ○

SHOW ATTRIBUTES

☑ All (5824) ☑ Towards Client (2065) ☑ Towards Server (4254) ☑ Incoming (5622) ☑ Outgoing (331)

Not In Group 5824 items

.NET Framework Remote Code Execution (MS14-057) [Signature]
/cgi-bin/nobody/ Access [Signature]
/ecp/default.aspx Access [Signature]
/etc/inetd.conf Access [Signature]
/etc/motd Access [Signature]
/etc/passwd Access 1 [Signature]
/etc/passwd Access 10 [Signature]
/etc/passwd Access 11 [Signature]
/etc/passwd Access 2 [Signature]
/etc/passwd Access 3 [Signature]
/etc/passwd Access 4 [Signature]
/etc/passwd Access 5 [Signature]
/etc/passwd Access 6 [Signature]
/etc/passwd Access 7 [Signature]
/etc/passwd Access 8 [Signature]
/etc/passwd Access 9 [Signature]
/etc/shadow Access 1 [Signature]
/etc/shadow Access 2 [Signature]

In Group 0 items

Selected: 0 of 5824 items

Deleting Intrusion Prevention Profiles

To delete custom Intrusion Prevention Profiles:

1. Navigate to **OBJECT | Profiles > Intrusion Prevention | Intrusion Prevention Profiles**.
2. To delete custom profile(s), click the checkbox(es) in the left column for the Profile(s) you would like to remove.
3. Click **Delete** from the top toolbar.
4. A warning message appears. Click **Confirm** or **Cancel**.

   ⓘ | **NOTE:** You cannot delete **Default** profiles.

To delete all custom Reporting Profiles:

1. Navigate to **OBJECT | Profiles > Intrusion Prevention | Intrusion Prevention Profiles**.
2. Click the top checkbox in the left column.

   All custom Intrusion Prevention Profiles are selected.
3. Click **Delete** from the top toolbar.
4. A warning message appears. Click **Confirm** or **Cancel**.

   ⓘ | **NOTE:** You cannot delete the **Default** profile.

6

QoS Marking

Quality of Service (QoS) refers to a diversity of methods intended to provide predictable network behavior and performance. This sort of predictability is vital to certain types of applications, such as Voice over IP (VoIP), multimedia content, or business-critical applications such as order or credit-card processing. No amount of bandwidth can provide this sort of predictability, because any amount of bandwidth is ultimately used to its capacity at some point in a network. Only QoS, when configured and implemented correctly, can properly manage traffic, and guarantee the desired levels of network service.

Topics:

Classification

Classification is necessary as a first step so that traffic in need of management can be identified. SonicOS uses Access Rules as the interface to classification of traffic. This provides fine controls using combinations of Address Object, Service Object, and Schedule Object elements, allowing for classification criteria as general as **all HTTP traffic** and as specific as **SSH traffic from hostA to serverB on Wednesdays at 2:12am**.

SonicWall network security appliances have the ability to recognize, map, modify, and generate the industry-standard external CoS designators, DSCP and 802.1p (refer to the section *802.1p and DSCP QoS*).

When identified, or classified, traffic can be managed. Management can be performed internally by SonicOS Bandwidth Management (BWM), which is perfectly effective as long as the network is a fully contained autonomous system. Once external or intermediate elements are introduced, such as foreign network infrastructures with unknown configurations, or other hosts contending for bandwidth (for example, the Internet) the ability to offer guarantees and predictability are diminished. In other words, as long as the endpoints of the network and everything in between are within your management, BWM works exactly as configured. Once external entities are introduced, the precision and efficacy of BWM configurations can begin to degrade.

But all is not lost. After SonicOS classifies the traffic, it can **tag** the traffic to communicate this classification to certain external systems that are capable of abiding by CoS tags; therefore, they too can participate in providing QoS.

ⓘ **NOTE:** Many service providers do not support CoS tags such as 802.1p or DSCP. Also, most network equipment with standard configurations are not able to recognize 802.1p tags, and could drop tagged traffic.

Although DSCP does not cause compatibility issues, many service providers simply strip or ignore the DSCP tags, disregarding the code points.

If you wish to use 802.1p or DSCP marking on your network or your service provider's network, you must first establish that these methods are supported. Verify that your internal network equipment can support CoS priority marking, and that it is correctly configured to do so. Check with your service provider – some offer fee-based support for QoS using these CoS methods.

Marking

After the traffic has been classified, if it is to be handled by QoS capable external systems (for example, CoS aware switches or routers as might be available on a premium service provider's infrastructure, or on a private WAN), it must be tagged so that the external systems can make use of the classification, and provide the correct handling and Per Hop Behaviors (PHB).

Originally, this was attempted at the IP layer (layer 3) with RFC791's three Precedence bits and RFC1394 ToS (type of service) field, but this was used by a grand total of 17 people throughout history. Its successor, RFC2474 introduced the much more practical and widely used DSCP (Differentiated Services Code Point) which offered up to 64 classifications, as well as user-definable classes. DSCP was further enhanced by RFC2598 (Expedited Forwarding, intended to provide leased-line behaviors) and RFC2697 (Assured Forwarding levels within classes, also known as Gold, Silver, and Bronze levels).

DSCP is a safe marking method for traffic that traverses public networks because there is no risk of incompatibility. At the very worst, a hop along the path might disregard or strip the DSCP tag, but it rarely mistreats or discards the packet.

The other prevalent method of CoS marking is IEEE 802.1p. 802.1p occurs at the MAC layer (layer 2) and is closely related to IEEE 802.1Q VLAN marking, sharing the same 16-bit field, although it is actually defined in the IEEE 802.1D standard. Unlike DSCP, 802.1p only works with 802.1p capable equipment, and is not universally interoperable. Additionally, 802.1p, because of its different packet structure, can rarely traverse wide-area networks, even private WANs. Nonetheless, 802.1p is gaining wide support among Voice and Video over IP vendors, so a solution for supporting 802.1p across network boundaries (such as WAN links) was introduced in the form of 802.1p to DSCP mapping.

802.1p to DSCP mapping allows 802.1p tags from one LAN to be mapped to DSCP values by SonicOS, allowing the packets to safely traverse WAN links. When the packets arrive on the other side of the WAN or VPN, the receiving SonicOS appliance can then map the DSCP tags back to 802.1p tags for use on that LAN. Refer to *802.1p and DSCP QoS* for more information.

Conditioning

The traffic can be conditioned (or managed) using any of the many policing, queuing, and shaping methods available. SonicOS provides internal conditioning capabilities with its Egress and Ingress Bandwidth Management (BWM), detailed in *Bandwidth Management*. SonicOS's BWM is a perfectly effective solution for fully autonomous private networks with sufficient bandwidth, but can become somewhat less effective as more unknown external network elements and bandwidth contention are introduced. Refer to DSCP marking: Example scenario for a description of contention issues.

Topics:

- Site to Site VPN over QoS Capable Networks
- Site to Site VPN over Public Networks

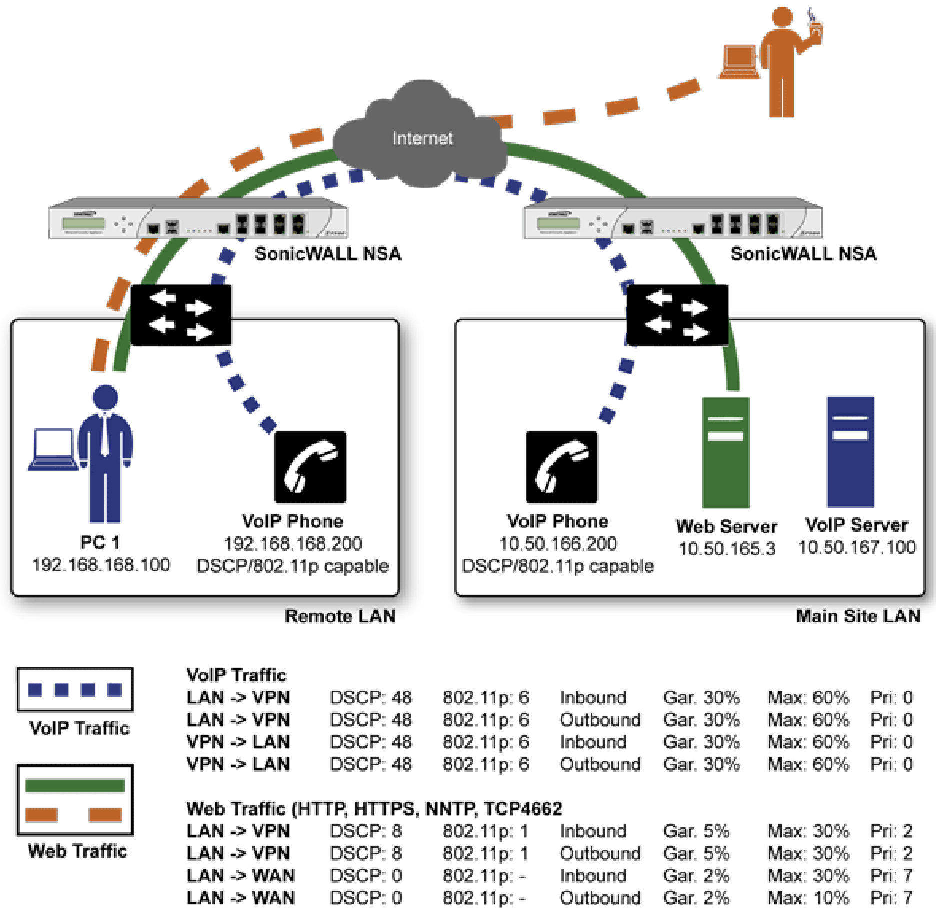
Site to Site VPN over QoS Capable Networks

If the network path between the two end points is QoS aware, SonicOS can DSCP tag the inner encapsulate packet so that it is interpreted correctly at the other side of the tunnel, and it can also DSCP tag the outer ESP encapsulated packet so that its class can be interpreted and honored by each hop along the transit network. SonicOS can map 802.1p tags created on the internal networks to DSCP tags so that they can safely traverse the transit network. Then, when the packets are received on the other side, the receiving SonicWall appliance can translate the DSCP tags back to 802.1p tags for interpretation and honoring by that internal network.

Site to Site VPN over Public Networks

SonicOS integrated BWM is very effective in managing traffic between VPN connected networks because ingress and egress traffic can be classified and controlled at both endpoints. If the network between the endpoints is non QoS aware, it regards and treats all VPN ESP equally. Because there is typically no control over these intermediate networks or their paths, it is difficult to fully guarantee QoS, but BWM can still help to provide more predictable behavior.

SITE TO SITE VPN OVER PUBLIC NETWORKS



VoIP Traffic						
LAN -> VPN	DSCP: 48	802.11p: 6	Inbound	Gar. 30%	Max: 60%	Pri: 0
LAN -> VPN	DSCP: 48	802.11p: 6	Outbound	Gar. 30%	Max: 60%	Pri: 0
VPN -> LAN	DSCP: 48	802.11p: 6	Inbound	Gar. 30%	Max: 60%	Pri: 0
VPN -> LAN	DSCP: 48	802.11p: 6	Outbound	Gar. 30%	Max: 60%	Pri: 0
Web Traffic (HTTP, HTTPS, NNTP, TCP4662						
LAN -> VPN	DSCP: 8	802.11p: 1	Inbound	Gar. 5%	Max: 30%	Pri: 2
LAN -> VPN	DSCP: 8	802.11p: 1	Outbound	Gar. 5%	Max: 30%	Pri: 2
LAN -> WAN	DSCP: 0	802.11p: -	Inbound	Gar. 2%	Max: 30%	Pri: 7
LAN -> WAN	DSCP: 0	802.11p: -	Outbound	Gar. 2%	Max: 10%	Pri: 7

To provide end-to-end QoS, business-class service providers are increasingly offering traffic conditioning services on their IP networks. These services typically depend on the customer premise equipment to classify and tag the traffic, generally using a standard marking method such as DSCP. SonicOS has the ability to DSCP mark traffic after classification, as well as the ability to map 802.1p tags to DSCP tags for external network traversal and CoS preservation. For VPN traffic, SonicOS can DSCP mark not only the internal (payload) packets, but the external (encapsulating) packets as well so that QoS capable service providers can offer QoS even on encrypted VPN traffic.

The actual conditioning method employed by service providers varies from one to the next, but it generally involves a class-based queuing method such as Weighted Fair Queuing for prioritizing traffic, as well a congestion avoidance method, such as tail-drop or Random Early Detection.

802.1p and DSCP QoS

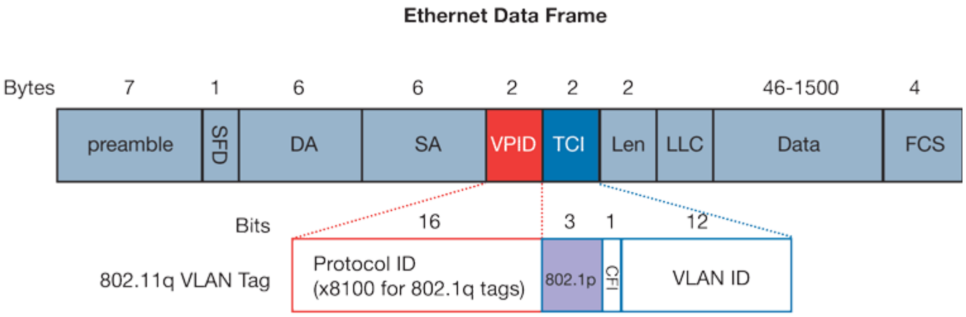
Topics:

- Enabling 802.1p
- DSCP Marking

Enabling 802.1p

SonicOS supports layer 2 and layer 3 CoS methods for broad interoperability with external systems participating in QoS enabled environments. The layer 2 method is the IEEE 802.1p standard wherein 3-bits of an additional 16-bits inserted into the header of the Ethernet frame can be used to designate the priority of the frame, as illustrated in the following figure:

ETHERNET DATA FRAME



- TPID: Tag Protocol Identifier begins at byte 12 (after the 6 byte destination and source fields), is 2 bytes long, and has an Ether type of 0x8100 for tagged traffic.
- 802.1p: The first three bits of the TCI (Tag Control Information – beginning at byte 14, and spanning 2 bytes) define user priority, giving eight (2^3) priority levels. IEEE 802.1p defines the operation for these 3 user priority bits.
- CFI: Canonical Format Indicator is a single-bit flag, always set to zero for Ethernet switches. CFI is used for compatibility reasons between Ethernet networks and Token Ring networks. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port.
- VLAN ID: VLAN ID (starts at bit 5 of byte 14) is the identification of the VLAN. It has 12-bits and allows for the identification of 4,096 (2^12) unique VLAN ID’s. Of the 4,096 possible IDs, an ID of 0 is used to identify priority frames, and an ID of 4,095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

802.1p support begins by enabling 802.1p marking on the interfaces which you wish to have process 802.1p tags. 802.1p can be enabled on any Ethernet interface on any SonicWall appliance.

The behavior of the 802.1p field within these tags can be controlled by Access Rules. The default 802.1p Access Rule action of None resets existing 802.1p tags to 0, unless otherwise configured (see Managing QoS Marking on page 86 for details).

Enabling 802.1p marking allows the target interface to recognize incoming 802.1p tags generated by 802.1p capable network devices, and also allows the target interface to generate 802.1p tags, as controlled by Access Rules. Frames that have 802.1p tags inserted by SonicOS bears VLAN ID 0.

802.1p tags are only inserted according to Access Rules, so enabling 802.1p marking on an interface does not, at its default setting, disrupt communications with 802.1p-incapable devices.

802.1p requires the specific support by the networking devices with which you wish to use this method of prioritization. Many voice and video over IP devices provide support for 802.1p, but the feature must be enabled. Check your equipment’s documentation for information on 802.1p support if you are unsure. Similarly, many server and host network cards (NICs) have the ability to support 802.1p, but the feature is usually disabled by default. On Win32 operating systems, you can check for and configure 802.1p settings on the Advanced view of the Properties page of your network card. If your card supports 802.1p, it is listed as 802.1p QoS, 802.1p Support, QoS Packet Tagging or something similar.

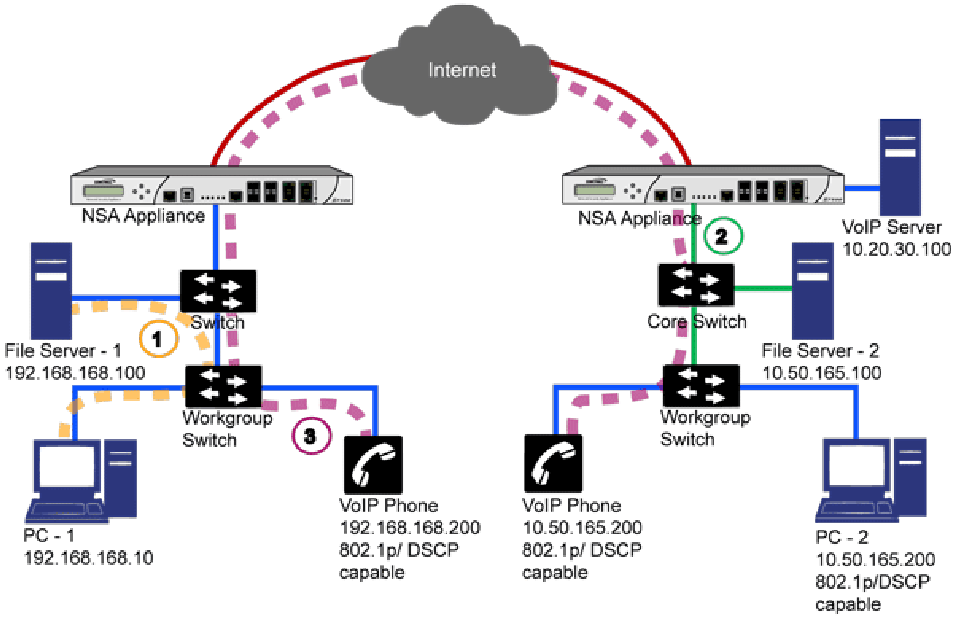
To process 802.1p tags, the feature must be present and enabled on the network interface. The network interface is then able to generate packets with 802.1p tags, as governed by QoS capable applications. By default, general network communications does not have tags inserted so as to maintain compatibility with 802.1p-incapable devices.

If your network interface does not support 802.1p, it is not able to process 802.1p tagged traffic, and ignores it. Make certain when defining Access Rules to enable 802.1p marking that the target devices are 802.1p capable.

It should also be noted that when performing a packet capture (for example, with the diagnostic tool Ethereal) on 802.1p capable devices, some 802.1p capable devices do not show the 802.1q header in the packet capture. Conversely, a packet capture performed on an 802.1p-incapable device almost invariably shows the header, but the host is unable to process the packet.

Before moving on to For more information, see *Managing QoS Marking*, it is important to introduce ‘DSCP Marking’ because of the potential interdependency between the two marking methods, as well as to explain why the interdependency exists.

DSCP MARKING: EXAMPLE SCENARIO



KEY

Blue Lines: 100Mbit links
Green Lines: 1000Mbit links
Red Lines: VPN Tunnel
Orange Line: Line speed data transfer
Plum Line: Voice Media

Remote Site 1	Remote Site 2
X0 (LAN): 192.168.168.168/24 X1 (WAN): 66.182.95.79.30	X0 (LAN): 10.50.165.1/24 X1 (WAN): 67.115.118.80/24 X2 (DMZ): 10.20.30.1/24
VPN Policy 1: ToHQ Local Net: 192.168.168.0/24 Remote Net: 10.50.165.0/24 Remote Net: 10.20.30.0/24	VPN Policy 1: ToRemoteSite1 Local Net: 10.50.165.0/24 Local Net: 10.20.30.x/24 Remote Net: 192.168.168.0/24

In the scenario in DSCP marking: Example scenario, we have Remote Site 1 connected to ‘Main Site’ by an IPsec VPN. The company uses an internal 802.1p/DSCP capable VoIP phone system, with a private VoIP signaling server hosted at the Main Site. The Main Site has a mixed gigabit and Fast-Ethernet infrastructure, while Remote Site 1 is all Fast Ethernet. Both sites employ 802.1p capable switches for prioritization of internal traffic.

1. PC-1 at Remote Site 1 is transferring a 23 terabyte PowerPoint™ presentation to File Server 1, and the 100mbit link between the workgroup switch and the upstream switch is completely saturated.
2. At the Main Site, a caller on the 802.1p/DSCP capable VoIP Phone `10.50.165.200` initiates a call to the person at VoIP phone `192.168.168.200`. The calling VoIP phone 802.1p tags the traffic with priority tag 6 (voice), and DSCP tags the traffic with a tag of 48.
    a. If the link between the Core Switch and the firewall is a VLAN, some switches include the received 802.1p priority tag, in addition to the DSCP tag, in the packet sent to the firewall; this behavior varies from switch to switch, and is often configurable.
    b. If the link between the Core Switch and the firewall is not a VLAN, there is no way for the switch to include the 802.1p priority tag. The 802.1p priority is removed, and the packet (including only the DSCP tag) is forwarded to the firewall.

    When the firewall sent the packet across the VPN/WAN link, it could include the DSCP tag in the packet, but it is not possible to include the 802.1p tag. This would have the effect of losing all prioritization information for the VoIP traffic, because when the packet arrived at the Remote Site, the switch would have no 802.1p MAC layer information with which to prioritize the traffic. The Remote Site switch would treat the VoIP traffic the same as the lower-priority file transfer because of the link saturation, introducing delay—maybe even dropped packets—to the VoIP flow, resulting in call quality degradation.

    So how can critical 802.1p priority information from the Main Site LAN persist across the VPN/WAN link to Remote Site LAN? Through the use of QoS Mapping.

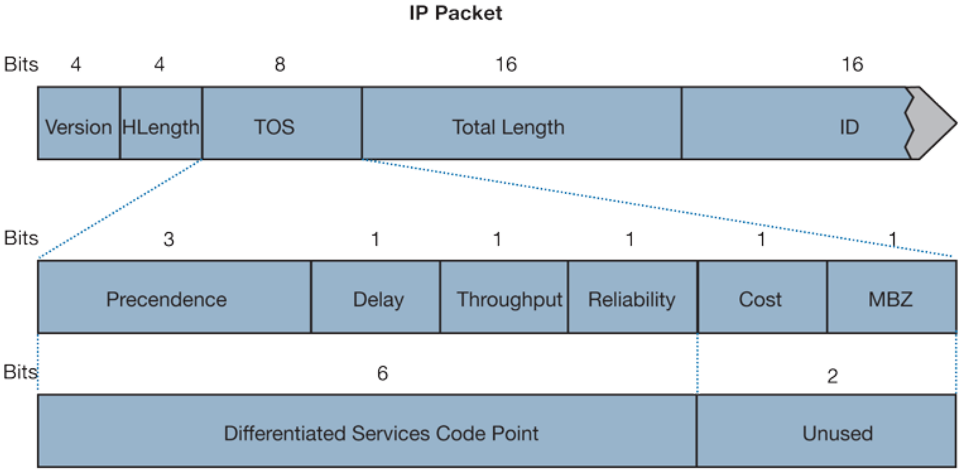
    QoS Mapping is a feature which converts layer 2 802.1p tags to layer 3 DSCP tags so that they can safely traverse (in mapped form) 802.1p-incapable links; when the packet arrives for delivery to the next 802.1p-capable segment, QoS Mapping converts from DSCP back to 802.1p tags so that layer 2 QoS can be honored.

    In our above scenario, the firewall at the Main Site assigns a DSCP tag (for example, value 48) to the VoIP packets, as well as to the encapsulating ESP packets, allowing layer 3 QoS to be applied across the WAN. This assignment can occur either by preserving the existing DSCP tag, or by mapping the value from an 802.1p tag, if present. When the VoIP packets arrive at the other side of the link, the mapping process is reversed by the receiving SonicWall, mapping the DSCP tag back to an 802.1p tag.
3. The receiving SonicWall at the Remote Site is configured to map the DSCP tag range 48-55 to 802.1p tag 6. When the packet exits the firewall, it bears 802.1p tag 6. The Switch recognizes it as voice traffic, and prioritizes it over the file-transfer, guaranteeing QoS even in the event of link saturation.

DSCP Marking

DSCP (Differentiated Services Code Point) marking uses 6-bits of the 8-bit ToS field in the IP Header to provide up to 64 classes (or code points) for traffic. Because DSCP is a layer 3 marking method, there is no concern about compatibility as there is with 802.1p marking. Devices that do not support DSCP simply ignores the tags, or at worst, they reset the tag value to 0.

DSCP MARKING: IP PACKET



DSCP marking: IP packet depicts an IP packet, with a close-up on the ToS portion of the header. The ToS bits were originally used for Precedence and ToS (delay, throughput, reliability, and cost) settings, but were later repurposed by RFC2474 for the more versatile DSCP settings.

DSCP marking: Commonly used code points shows the commonly used code points, as well as their mapping to the legacy Precedence and ToS settings.

DSCP MARKING: COMMONLY USED CODE POINTS

DSCP	DSCP Description	Legacy IP Precedence	Legacy IP ToS (D, T, R)
0	Best effort	0 (Routine – 000)	-
8	Class 1	1 (Priority – 001)	-
10	Class 1, gold (AF11)	1 (Priority – 001)	T
12	Class 1, silver (AF12)	1 (Priority – 001)	D
14	Class 1, bronze (AF13)	1 (Priority – 001)	D, T
16	Class 2	2 (Immediate – 010)	-
18	Class 2, gold (AF21)	2 (Immediate – 010)	T
20	Class 2, silver (AF22)	2 (Immediate – 010)	D
22	Class 2, bronze (AF23)	2 (Immediate – 010)	D, T
24	Class 3	3 (Flash – 011)	-
26	Class 3, gold (AF31)	3 (Flash – 011)	T
27	Class 3, silver (AF32)	3 (Flash – 011)	D
30	Class 3, bronze (AF33)	3 (Flash – 011)	D, T
32	Class 4	4 (Flash Override – 100)	-
34	Class 4, gold (AF41)	4 (Flash Override – 100)	T
36	Class 4, silver (AF42)	4 (Flash Override – 100)	D
38	Class 4, bronze	4 (Flash Override – 100)	D, T

DSCP	DSCP Description	Legacy IP Precedence	Legacy IP ToS (D, T, R)
	(AF43)		
40	Express forwarding	5 (CRITIC/ECP – 101)	-
46	Expedited forwarding (EF)	5 (CRITIC/ECP – 101)	D, T
48	Control	6 (Internet Control – 110)	-
56	Control	7 (Network Control – 111)	-

DSCP marking can be performed on traffic to/from any interface and to/from any zone type, without exception. DSCP marking is controlled by Access Rules, from the QoS view, and can be used in conjunction with 802.1p marking, as well as with SonicOS's internal bandwidth management.

Topics:

- DSCP Marking and Mixed VPN Traffic
- Configure for 802.1p CoS 4 – Controlled Load
- QoS Mapping
- Managing QoS Marking

DSCP Marking and Mixed VPN Traffic

Among their many security measures and characteristics, IPsec VPNs employ anti-replay mechanisms based upon monotonically incrementing sequence numbers added to the ESP header. Packets with duplicate sequence numbers are dropped, as are packets that do not adhere to sequence criteria. One such criterion governs the handling of out-of-order packets. SonicOS provides a replay window of 64 packets, such as whether an ESP packet for a Security Association (SA) is delayed by more than 64 packets, the packet is dropped.

This should be considered when using DSCP marking to provide layer 3 QoS to traffic traversing a VPN. If you have a VPN tunnel that is transporting a diversity of traffic, some that is being DSCP tagged high priority (for example, VoIP), and some that is DSCP tagged low-priority, or untagged/best-effort (for example, FTP), your service provider prioritizes the handling and delivery of the high-priority ESP packets over the best-effort ESP packets. Under certain traffic conditions, this can result in the best-effort packets being delayed for more than 64 packets, causing them to be dropped by the receiving SonicWall's anti-replay defenses.

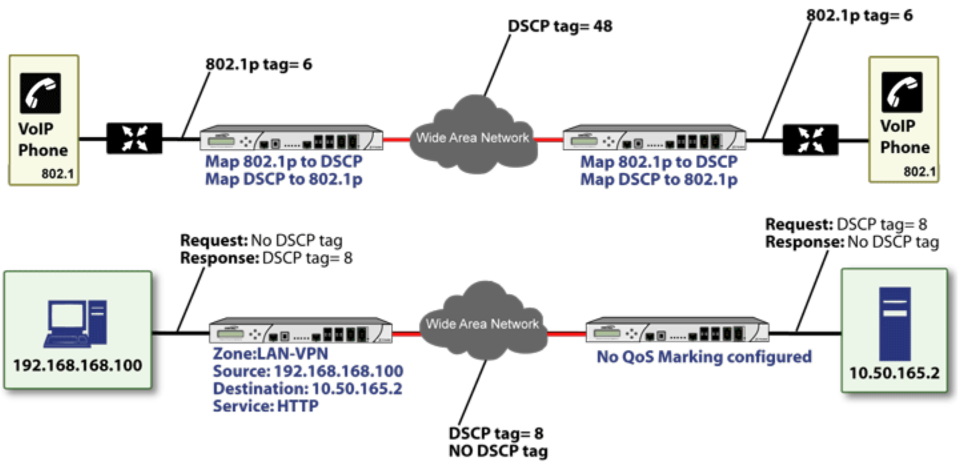
If symptoms of such a scenario emerge (for example, excessive retransmissions of low-priority traffic), it is recommended that you create a separate VPN policy for the high-priority and low-priority classes of traffic. This is most easily accomplished by placing the high-priority hosts (for example, the VoIP network) on their own subnet.

Configure for 802.1p CoS 4 – Controlled Load

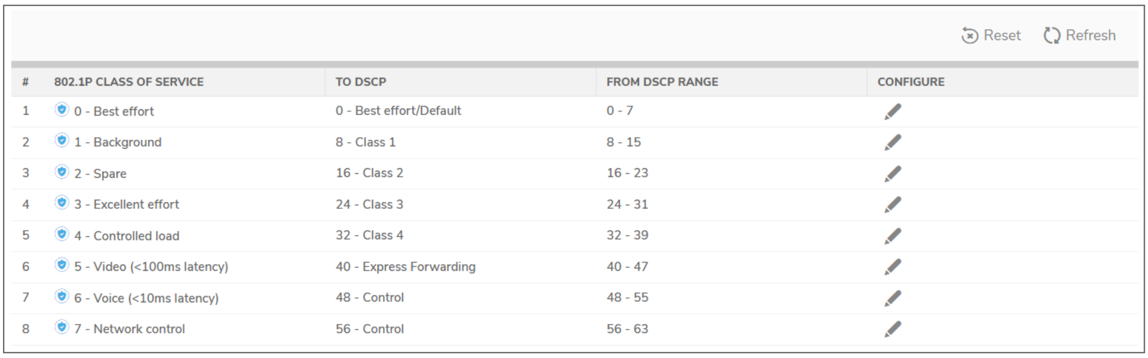
If you want to change the inbound mapping of DSCP tag 15 from its default 802.1p mapping of 1 to an 802.1p mapping of 2, it would have to be done in two steps because mapping ranges cannot overlap. Attempting to assign an overlapping mapping returns the error: "DSCP range already exists or overlaps with another range." First, you have to remove 15 from its current end-range mapping to 802.1p CoS 1 (changing the end-range mapping of 802.1p CoS 1 to DSCP 14), then you can assign DSCP 15 to the start-range mapping on 802.1p CoS 2.

QoS Mapping

The primary objective of QoS Mapping is to allow 802.1p tags to persist across non-802.1p compliant links (for example, WAN links) by mapping them to corresponding DSCP tags before sending across the WAN link, and then mapping from DSCP back to 802.1p upon arriving at the other side, as shown in QoS mapping.



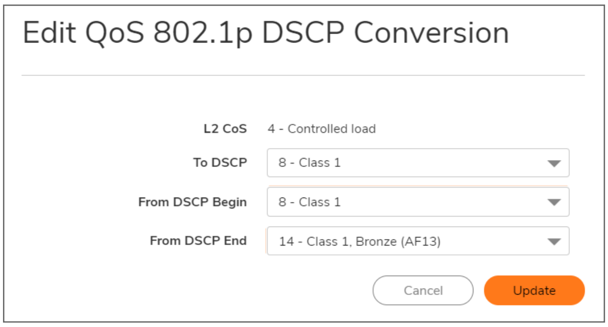
ⓘ **NOTE:** Mapping does not occur until you assign Map as an action of the QoS view of an Access Rule. The mapping table only defines the correspondence that is employed by an Access Rule's Map action.



#	802.1P CLASS OF SERVICE	TO DSCP	FROM DSCP RANGE	CONFIGURE
1	0 - Best effort	0 - Best effort/Default	0 - 7	✎
2	1 - Background	8 - Class 1	8 - 15	✎
3	2 - Spare	16 - Class 2	16 - 23	✎
4	3 - Excellent effort	24 - Class 3	24 - 31	✎
5	4 - Controlled load	32 - Class 4	32 - 39	✎
6	5 - Video (<100ms latency)	40 - Express Forwarding	40 - 47	✎
7	6 - Voice (<10ms latency)	48 - Control	48 - 55	✎
8	7 - Network control	56 - Control	56 - 63	✎

For example, according to the default table, an 802.1p tag with a value of **2** is outbound mapped to a DSCP value of **16**, while a DSCP tag of **43** is inbound mapped to an 802.1 value of **5**.

Each of these mappings can be reconfigured. If you wanted to change the outbound mapping of 802.1p tag **4** from its default DSCP value of **32** to a DSCP value of 43, you can click the **Configure** icon for **4 – Controlled load** and select the new **To DSCP** value from the drop-down menu:



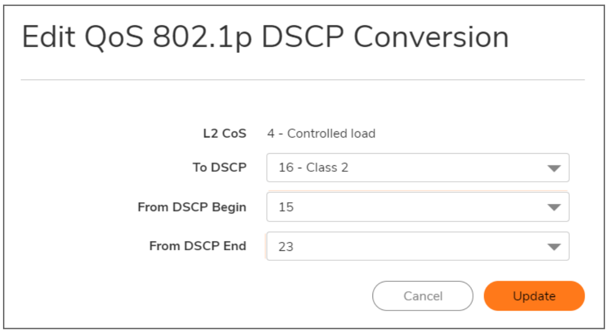
Edit QoS 802.1p DSCP Conversion

L2 CoS 4 - Controlled load

To DSCP 8 - Class 1

From DSCP Begin 8 - Class 1

From DSCP End 14 - Class 1, Bronze (AF13)



Edit QoS 802.1p DSCP Conversion

L2 CoS 4 - Controlled load

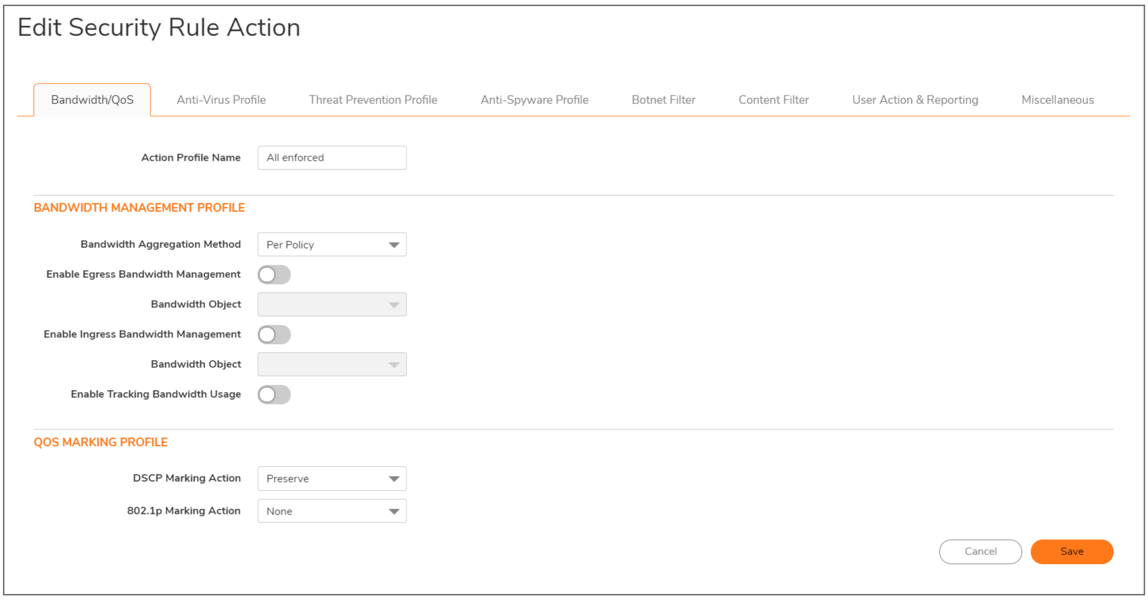
To DSCP 16 - Class 2

From DSCP Begin 15

From DSCP End 23

Managing QoS Marking

The QoS Marking Profile is configured from the Bandwidth/QoS view of the **Add/Edit Security Rule Action** dialog of the **OBJECT | Actions > Security Rule** page:



Edit Security Rule Action

Action Profile Name All enforced

BANDWIDTH MANAGEMENT PROFILE

Bandwidth Aggregation Method Per Policy

Enable Egress Bandwidth Management ○

Bandwidth Object

Enable Ingress Bandwidth Management ○

Bandwidth Object

Enable Tracking Bandwidth Usage ○

QOS MARKING PROFILE

DSCP Marking Action Preserve

802.1p Marking Action None

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

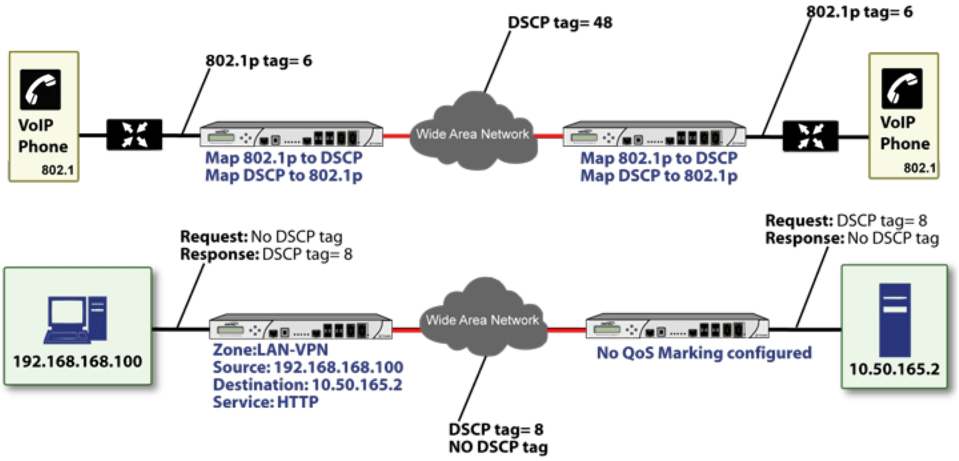
QoS marking: Behavior describes the behavior of each action on both methods of marking:

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 | Actions > Security Rule** page is used to map from a DSCP tag to an 802.1p tag.	The mapping setting defined in the **OBJECT | Actions > Security Rule** 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.

For example, refer to Bi-directional DSCP tag action, which provides a bi-directional DSCP tag action.

BI-DIRECTIONAL DSCP TAG ACTION



HTTP access from a Web-browser on `192.168.168.100` to the Web server on `10.50.165.2` results in the tagging of the inner (payload) packet and the outer (encapsulating ESP) packets with a DSCP value of 8. When the packets emerge from the other end of the tunnel, and are delivered to `10.50.165.2`, they bear a DSCP tag of 8. When 10.50.165.2 sends response packets back across the tunnel to `192.168.168.100` (beginning with the very first SYN/ACK packet) the Security Rule tags the response packets delivered to `192.168.168.100` with a DSCP value of 8.

This behavior applies to all four QoS action settings for both DSCP and 802.1p marking.

One practical application for this behavior would be configuring an 802.1p marking rule for traffic destined for the VPN zone. Although 802.1p tags cannot be sent across the VPN, reply packets coming back across the VPN can be 802.1p tagged on egress from the tunnel. This requires that 802.1p tagging is active of the physical egress interface, and that the [Zone] > VPN Access Rule has an 802.1p marking action other than **None**.

After ensuring 802.1p compatibility with your relevant network devices, and enabling 802.1p marking on applicable SonicWall interfaces, you can begin configuring Security Rules to manage 802.1p tags.

The Remote Site 1 network could have two Access Rules configured as in Remote site 1: Sample access rule configuration.

REMOTE SITE 1: SAMPLE SECURITY RULE CONFIGURATION

Setting	Access Rule 1	Access Rule 2
General View		
Action	Allow	Allow
From Zone	LAN	VPN
To Zone	VPN	LAN
Service	VoIP	VoIP
Source	Lan Primary Subnet	Main Site Subnets
Destination	Main Site Subnets	Lan Primary Subnet
Users Allowed	All	All
Schedule	Always on	Always on

Setting	Access Rule 1	Access Rule 2
General View		
Enable Logging	Enabled	Enabled
Allow Fragmented Packets	Enabled	Enabled
Qos View		
DSCP Marking Action	Map	Map
Allow 802.1p Marking to override DSCP values	Enabled	Enabled
802.1p Marking Action	Map	Map

The first Access Rule (governing **LAN>VPN**) would have the following effects:

- VoIP traffic (as defined by the Service Group) from **LAN Primary Subnet** destined to be sent across the VPN to Main Site Subnets would be evaluated for both DSCP and 802.1p tags.
  - The combination of setting both DSCP and 802.1p marking actions to **Map** is described in the table earlier in Managing QoS Marking.
  - Sent traffic containing only an 802.1p tag (for example, CoS = 6) would have the VPN-bound inner (payload) packet DSCP tagged with a value of 48. The outer (ESP) packet would also be tagged with a value of 48.
  - Assuming returned traffic has been DSCP tagged (CoS = 48) by the firewall at the Main Site, the return traffic is 802.1p tagged with CoS = 6 on egress.
  - Sent traffic containing only a DSCP tag (for example, CoS = 48) would have the DSCP value preserved on both inner and outer packets.
  - Assuming returned traffic has been DSCP tagged (CoS = 48) by the firewall at the Main Site, the return traffic is 802.1p tagged with CoS = 6 on egress.
  - Sent traffic containing only both an 802.1p tag (for example, CoS = 6) and a DSCP tag (for example, CoS = 63) would give precedence to the 802.1p tag and would be mapped accordingly. The VPN-bound inner (payload) packet DSCP would be tagged with a value of 48. The outer (ESP) packet would also be tagged with a value of 48.

Assuming returned traffic has been DSCP tagged (CoS = 48) by the firewall at the Main Site, the return traffic is 802.1p tagged with CoS = 6 on egress.

To examine the effects of the second Security Rule (VPN>LAN), we will look at the Security Rules configured at the Main Site, as shown in Main site: Sample access rule configurations.

MAIN SITE: SAMPLE SECURITY RULE CONFIGURATIONS

Setting	Security Rule 1	Security Rule 2
General View		
Action	Allow	Allow
From Zone	LAN	VPN
To Zone	VPN	LAN
Service	VoIP	VoIP
Source	Lan Subnets	Remote Site 1 Subnets
Destination	Remote Site 1 Subnets	Lan Subnets

Setting	Security Rule 1	Security Rule 2
General View		
Users Allowed	All	All
Schedule	Always on	Always on
Enable Logging	Enabled	Enabled
Allow Fragmented Packets	Enabled	Enabled
Qos View		
DSCP Marking Action	Map	Map
Allow 802.1p Marking to override DSCP values	Enabled	Enabled
802.1p Marking Action	Map	Map

VoIP traffic (as defined by the Service Group) arriving from **Remote Site 1 Subnets** across the VPN destined to **LAN Subnets** on the LAN zone at the Main Site would hit the Access Rule for inbound VoIP calls. Traffic arriving at the VPN zone does not have any 802.1p tags, only DSCP tags.

- Traffic exiting the tunnel containing a DSCP tag (for example, CoS = 48) would have the DSCP value preserved. Before the packet is delivered to the destination on the LAN, it is also 802.1p tagged according to the **QoS Mapping** settings (for example, CoS = 6) by the firewall at the Main Site.
- Assuming returned traffic has been 802.1p tagged (for example, CoS = 6) by the VoIP phone receiving the call at the Main Site, the return traffic is DSCP tagged according to the conversion map (CoS = 48) on both the inner and outer packet sent back across the VPN.
- Assuming returned traffic has been DSCP tagged (for example, CoS = 48) by the VoIP phone receiving the call at the Main Site, the return traffic has the DSCP tag preserved on both the inner and outer packet sent back across the VPN.
- Assuming returned traffic has been both 802.1p tagged (for example, CoS = 6) and DSCP tagged (for example, CoS = 14) by the VoIP phone receiving the call at the Main Site, the return traffic is DSCP tagged according to the conversion map (CoS = 48) on both the inner and outer packet sent back across the VPN.

Configuring QoS Marking

After the traffic has been classified, if it is to be handled by QoS capable external systems (for example, CoS aware switches or routers as might be available on a premium service provider's infrastructure, or on a private WAN), it must be tagged so that the external systems can make use of the classification, and provide the correct handling and Per Hop Behaviors (PHB).

Originally, this was attempted at the IP layer (layer 3) with RFC791's three Precedence bits and RFC1394 ToS (type of service) field, but this was used by a grand total of 17 people throughout history. Its successor, RFC2474 introduced the much more practical and widely used DSCP (Differentiated Services Code Point) which offered up to 64 classifications, as well as user-definable classes. DSCP was further enhanced by RFC2598 (Expedited Forwarding, intended to provide leased-line behaviors) and RFC2697 (Assured Forwarding levels within classes, also known as Gold, Silver, and Bronze levels).

DSCP is a safe marking method for traffic that traverses public networks because there is no risk of incompatibility. At the very worst, a hop along the path might disregard or strip the DSCP tag, but it rarely mistreats or discards the packet.

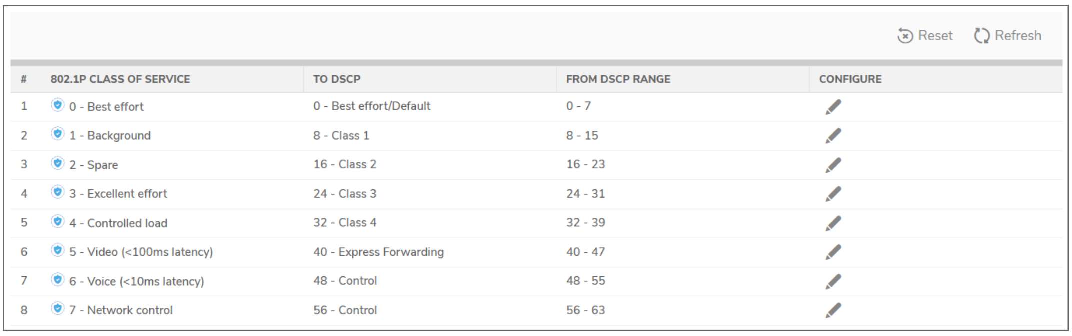
The other prevalent method of CoS marking is IEEE 802.1p. 802.1p occurs at the MAC layer (layer 2) and is closely related to IEEE 802.1Q VLAN marking, sharing the same 16-bit field, although it is actually defined in the IEEE 802.1D standard. Unlike DSCP, 802.1p only works with 802.1p capable equipment, and is not universally interoperable. Additionally, 802.1p, because of its different packet structure, can rarely traverse wide-area networks, even private WANs. Nonetheless, 802.1p is gaining wide support among Voice and Video over IP vendors, so a solution for supporting 802.1p across network boundaries (such as WAN links) was introduced in the form of 802.1p to DSCP mapping.

802.1p to DSCP mapping allows 802.1p tags from one LAN to be mapped to DSCP values by SonicOS, allowing the packets to safely traverse WAN links. When the packets arrive on the other side of the WAN or VPN, the receiving SonicOS appliance can then map the DSCP tags back to 802.1p tags for use on that LAN. Refer to 802.1p and DSCP QoS for more information.

To configure Quality of Service (QoS) Marking packets:

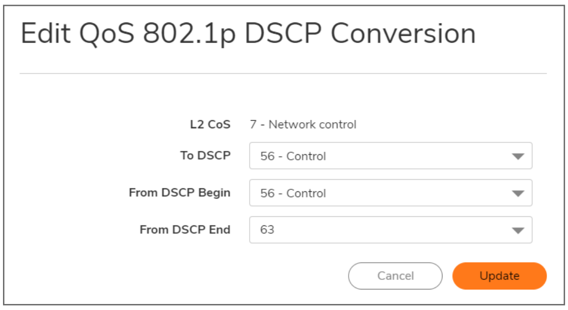
1. You must first setup your QoS Marking profiles in **OBJECT | Actions > Security Rule | Bandwidth/QoS**. See the documentation in that section for more information. After you have established the Action Profile, it should appear as a selection in **OBJECT | Profiles > QoS Marking**

   In the QoS Marking table, select the profile you would like to configure.



#	802.1P CLASS OF SERVICE	TO DSCP	FROM DSCP RANGE	CONFIGURE
1	0 - Best effort	0 - Best effort/Default	0 - 7	✎
2	1 - Background	8 - Class 1	8 - 15	✎
3	2 - Spare	16 - Class 2	16 - 23	✎
4	3 - Excellent effort	24 - Class 3	24 - 31	✎
5	4 - Controlled load	32 - Class 4	32 - 39	✎
6	5 - Video (<100ms latency)	40 - Express Forwarding	40 - 47	✎
7	6 - Voice (<10ms latency)	48 - Control	48 - 55	✎
8	7 - Network control	56 - Control	56 - 63	✎

2. Click the **Edit** icon in the **Configure** column of the profile you would like to modify.



Edit QoS 802.1p DSCP Conversion

L2 CoS: 7 - Network control

To DSCP: 56 - Control

From DSCP Begin: 56 - Control

From DSCP End: 63

3. Complete the form as necessary.
4. Click **Update** to save your settings.

7

DHCP Option

A SonicWall network security appliance includes a DHCP (Dynamic Host Configuration Protocol) server to distribute IP addresses, subnet masks, gateway addresses, and DNS server addresses to your network clients. **Network > DHCP Server** includes settings for configuring the appliance's DHCP server, Lease Scopes, and DHCP Leases.

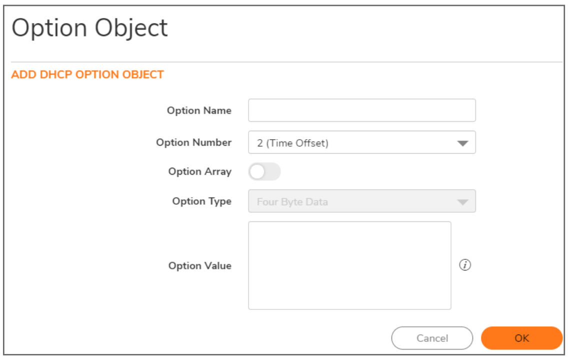
The SonicWall DHCP server Option feature provides support for DHCP Options, also known as vendor extensions, as defined primarily in RFCs 2131 and 2132. DHCP Options allow users to specify additional DHCP parameters in the form of predefined, vendor-specific information that is stored in the options field of a DHCP message. When the DHCP message is sent to clients on the network, it provides vendor-specific configuration and service information. For more information on RFC-Defined DHCP Option Numbers, see:

- IPv4 Options: RFC-Defined DHCPV4 Option Numbers
- IPv6 Options: RFC-Defined DHCPV6 Option Numbers

Configuring DHCP Option Objects

You can create DHCP Option objects in one of these ways:

1. Navigate to **Object > Profile Objects > DHCP Option** page, and click **Add** to create IPv4 and IPv6 DHCP Option Objects. The Add DHCP Option Object dialog displays.



Option Object

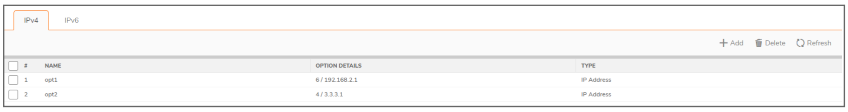
ADD DHCP OPTION OBJECT

Option Name	
Option Number	2 (Time Offset)
Option Array	○
Option Type	Four Byte Data
Option Value	

2. Type a name for the option object in the **Option Name** field.

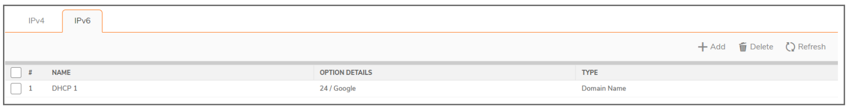
3. From **Option Number**, select the option number that corresponds to your DHCP option. For a list of option numbers, names, and descriptions, refer to:
    - For IPv4, see RFC-Defined DHCPV4 Option Numbers
    - For IPv6, see RFC-Defined DHCPV6 Option Numbers
4. If:
    - Only one option type is available, for example, for **Option Number 2 (Time Offset)**, **Option Array** is dimmed. Go to **Step 7**.
    - There are multiple option types available, for example, for **77 (User Class Information)**, **Option Type** becomes available and lists allowable types of the option, such as **IP Address**, **Two-Byte Data**, **String**, **Boolean**, and so on. Select the option type.
5. Type the option value, for example, an IP address, in the **Option Value** field. If Option Array is checked, multiple values may be entered, separated by a semi-colon (;).
6. Click **OK**. The object displays in the **Option Objects** table.

DHCPV4 OPTION OBJECTS TABLE



□	#	NAME	OPTION DETAILS	TYPE
□	1	opt1	6 / 192.168.2.1	IP Address
□	2	opt2	4 / 3.3.3.1	IP Address

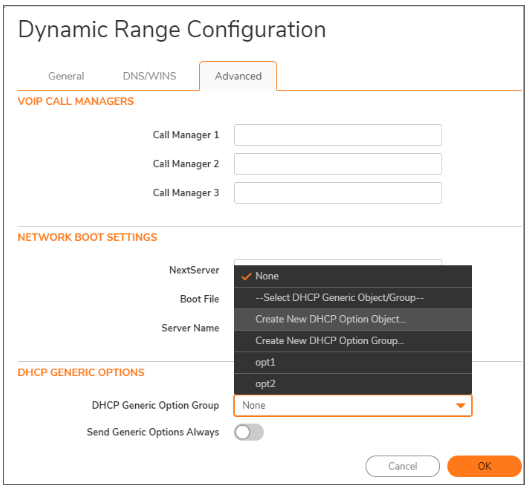
DHCPV6 OPTION OBJECTS TABLE



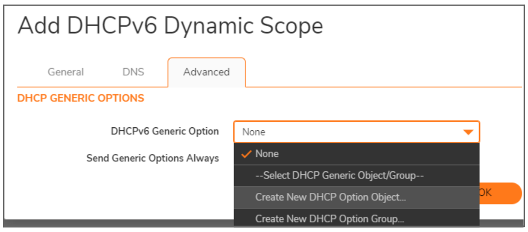
□	#	NAME	OPTION DETAILS	TYPE
□	1	DHCP 1	24 / Google	Domain Name

OR

- Navigate to **Network > DHCP Server > DHCP Server Lease Scopes** tab,
    - To create IPv4 Option object, click **Add Static** or **Add Dynamic** option. In the dialog, click **Advanced** tab and select **Create New DHCP Option Object** from the **DHCP Generic Option Group** drop-down.



- To create IPv6 Option object, select **IPv6** tab and click **Add Static** or **Add Dynamic** option. In the dialog, click **Advanced** tab and select **Create New DHCP Option Object** from the **DHCP Generic Option** drop-down.



Add DHCPv6 Dynamic Scope

DHCP GENERIC OPTIONS

DHCPv6 Generic Option: None

Send Generic Options Always

General
DNS
Advanced
✓ None
--Select DHCP Generic Object/Group--
Create New DHCP Option Object...
Create New DHCP Option Group...
OK

- Follow Steps from 2 through Step 6 from the above section. The object displays in the **Option Objects** table.

RFC-Defined DHCPV4 Option Numbers

Option Number	Name	Description
2	Time Offset	Time offset in seconds from UTC
3	Routers	N/4 router addresses
4	Time Servers	N/4 time server addresses
5	Name Servers	N/4 IEN-116 server addresses
6	DNS Servers	N/4 DNS server addresses
7	Log Servers	N/4 logging server addresses
8	Cookie Servers	N/4 quote server addresses
9	LPR Servers	N/4 printer server addresses
10	Impress Servers	N/4 impress server addresses
11	RLP Servers	N/4 RLP server addresses
12	Host Name	Hostname string, such as (Server Unicast)
13	Boot File Size	Size of boot file in 512-byte chunks
14	Merit Dump File	Client to dump and name of file to dump to
15	Domain Name	DNS domain name of the client
16	Swap Server	Swap server addresses
17	Root Path	Path name for root disk
18	Extension File	Patch name for more BOOTP info
19	IP Layer Forwarding	Enable or disable IP forwarding
20	Src route enabler	Enable or disable source routing
21	Policy Filter	Routing policy filters
22	Maximum DG Reassembly Size	Maximum datagram reassembly size
23	Default IP TTL	Default IP time-to-live

Option Number	Name	Description
24	Path MTU Aging Timeout	Path MTU aging timeout
25	MTU Plateau	Path MTU plateau table
26	Interface MTU Size	Interface MTU size
27	All Subnets Are Local	All subnets are local
28	Broadcast Address	Broadcast address
29	Perform Mask Discovery	Perform mask discovery
30	Provide Mask to Others	Provide mask to others
31	Perform Router Discovery	Perform router discovery
32	Router Solicitation Address	Router solicitation address
33	Static Routing Table	Static routing table
34	Trailer Encapsulation	Trailer encapsulation
35	ARP Cache Timeout	ARP cache timeout
36	Ethernet Encapsulation	Ethernet encapsulation
37	Default TCP Time to Live	Default TCP time to live
38	TCP Keepalive Interval	TCP keepalive interval
39	TCP Keepalive Garbage	TCP keepalive garbage
40	NIS Domain Name	NIS domain name
41	NIS Server Addresses	NIS server addresses
42	NTP Servers Addresses	NTP servers addresses
43	Vendor Specific Information	Vendor specific information
44	NetBIOS Name Server	NetBIOS name server
45	NetBIOS Datagram Distribution	NetBIOS datagram distribution
46	NetBIOS Node Type	NetBIOS node type
47	NetBIOS Scope	NetBIOS scope
48	X Window Font Server	X window font server
49	X Window Display Manager	X window display manager
50	Requested IP address	Requested IP address
51	IP Address Lease Time	IP address lease time
52	Option Overload	Overload “sname” or “file”
53	DHCP Message Type	DHCP message type
54	DHCP Server Identification	DHCP server identification
55	Parameter Request List	Parameter request list
56	Message	DHCP error message
57	DHCP Maximum Message Size	DHCP maximum message size
58	Renew Time Value	DHCP renewal (T1) time
59	Rebinding Time Value	DHCP rebinding (T2) time
60	Client Identifier	Client identifier

Option Number	Name	Description
61	Client Identifier	Client identifier
62	Netware/IP Domain Name	Netware/IP domain name
63	Netware/IP sub Options	Netware/IP sub options
64	NIS+ V3 Client Domain Name	NIS+ V3 client domain name
65	NIS+ V3 Server Address	NIS+ V3 server address
66	TFTP Server Name	TFTP server name
67	Boot File Name	Boot file name
68	Home Agent Addresses	Home agent addresses
69	Simple Mail Server Addresses	Simple mail server addresses
70	Post Office Server Addresses	Post office server addresses
71	Network News Server Addresses	Network news server addresses
72	WWW Server Addresses	WWW server addresses
73	Finger Server Addresses	Finger server addresses
74	Chat Server Addresses	Chat server addresses
75	StreetTalk Server Addresses	StreetTalk server addresses
76	StreetTalk Directory Assistance Addresses	StreetTalk directory assistance addresses
77	User Class Information	User class information
78	SLP Directory Agent	Directory agent information
79	SLP Service Scope	Service location agent scope
80	Rapid Commit	Rapid commit
81	FQDN, Fully Qualified Domain Name	Fully qualified domain name
82	Relay Agent Information	Relay agent information
83	Internet Storage Name Service	Internet storage name service
84	Undefined	N/A
85	Novell Directory Servers	Novell Directory Services servers
86	Novell Directory Server Tree Name	Novell Directory Services server tree name
87	Novell Directory Server Context	Novell Directory Services server context
88	BCMCS Controller Domain Name List	CMCS controller domain name list
89	BCMCS Controller IPv4 Address List	BCMCS controller IPv4 address list
90	Authentication	Authentication
91- 92	Undefined	N/A
93	Client System	Client system architecture
94	Client Network Device Interface	Client network device interface
95	LDAP Use	Lightweight Directory Access Protocol
96	Undefined	N/A
97	UUID/GUID-based Client Identifier	UUID/GUID-based client identifier

Option Number	Name	Description
98	Open Group’s User Authentication	Open group’s user authentication
99 - 108	Undefined	N/A
109	Autonomous System Number	Autonomous system number
110 - 111	Undefined	N/A
112	NetInfo Parent Server Address	NetInfo parent server address
113	NetInfo Parent Server Tag	NetInfo parent server tag
114	URL:	URL
115	Undefined	N/A
116	Auto Configure	DHCP auto-configuration
117	Name Service Search	Name service search
118	Subnet Collection	Subnet selection
119	DNS Domain Search List	DNS domain search list
120	SIP Servers DHCP Option	SIP servers DHCP option
121	Classless Static Route Option	Classless static route option
122	CCC, CableLabs Client Configuration	CableLabs client configuration
123	GeoConf	GeoConf
124	Vendor-Identifying Vendor Class	Vendor-identifying vendor class
125	Vendor Identifying Vendor Specific	Vendor-identifying vendor specific
126 - 127	Undefined	N/A
128	TFTP Server IP Address	TFTP server IP address for IP phone software load
129	Call Server IP Address	Call server IP address
130	Discrimination String	Discrimination string to identify vendor
131	Remote Statistics Server IP Address	Remote statistics server IP address
132	802.1Q VLAN ID	IEEE 802.1Q VLAN ID
133	802.1Q L2 Priority	IEEE 802.1Q layer 2 priority
134	Diffserv Code Point	Diffserv code point for VoIP signalling and media streams
135	HTTP Proxy For Phone Applications	HTTP proxy for phone-specific applications
136 - 149	Undefined	N/A
150	TFTP Server Address, Etherboot, GRUB Config	TFTP server address, Etherboot, GRUB configuration
151 - 174	Undefined	N/A
175	Ether Boot	Ether Boot
176	IP Telephone	IP telephone
177	Ether Boot PacketCable and CableHome	Ether Boot PacketCable and CableHome

Option Number	Name	Description
178 - 207	Undefined	N/A
208	pxelinux.magic (string) = 241.0.116.126	pxelinux.magic (string) = 241.0.116.126
209	pxelinux.configfile (text)	pxelinux.configfile (text)
210	pxelinux.pathprefix (text)	pxelinux.pathprefix (text)
211	pxelinux.reboottime	pxelinux.reboottime
212 - 219	Undefined	N/A
220	Subnet Allocation	Subnet allocation
221	Virtual Subnet Allocation	Virtual subnet selection
222 - 223	Undefined	N/A
224 - 257	Private Use	Private use

RFC-Defined DHCPV6 Option Numbers

Option Number	Name	Description
12	Server Unicast	Hostname string, such as (Server Unicast)
21	SIP Servers Domain Name List	Enables listing of SIP Servers domain names
22	SIP Servers IPv6 Address List	Enables listing of SIP Servers IPv6 Addresses
23	DNS Recursive Name Server	Enables listing of DNS Recursive Name servers
24	Domain Search List	Enables listing of domain names for searching
27	Network Information Service (NIS) Servers	Enables listing of Network Information Service (NIS) servers
28	Network Information Service V2 (NIS+) Servers	Enables listing of Network Information Service V2 (NIS+) servers
29	Network Information Service (NIS) Domain Name	Enables listing of Network Information Service (NIS) domain names
30	Network Information Service V2 (NIS+) Domain Name	Enables listing of Network Information Service V2 (NIS+) domain names
31	Simple Network Time Protocol (SNTP) Servers	Enables listing of Simple Network Time Protocol (SNTP) servers
32	Information Refresh Time	Information refresh time

Editing DHCP Option Objects

Mouse over on the DHCP OptionObject which you want to edit and click **Edit** icon. The Configuration settings are same as the **Add DHCP Option Object** dialog. For more information, see Configuring DHCP Option Objects.

You cannot change the **Name** of the DHCP Option Object.

Deleting DHCP Option Objects

To delete DHCP Option Objects:

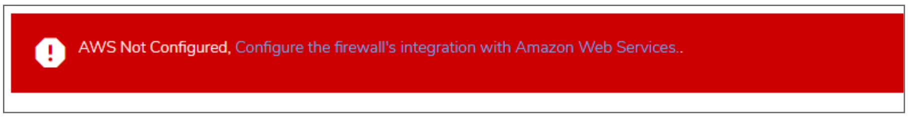
1. Navigate to**Object > Profile Objects > DHCP Option** page.
2. Do one of the following:
    - Mouse over on the DHCP Option which you want to delete and click **Delete** icon.
    - Click the checkbox for one or more objects to be deleted and click **Delete** icon at top of the page.

8

AWS

Before setting up AWS objects or groups, be sure to configure the firewall with the AWS credentials that it needs to use. You can configure these in **Network > System > AWS Configuration** page. In addition, the Test Configuration button is available there to validate the settings before proceeding. See *Configuring AWS Credentials* in the *SonicOS System Setup* administration documentation for more information.

If AWS is not yet configured, the **Object > Profile Objects > AWS** page displays a link to the configuration page. Click on that to open the **Network > System > AWS Configuration** page.



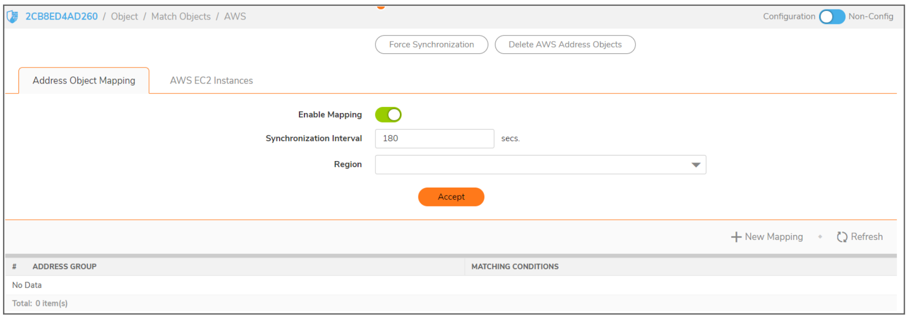
AWS Not Configured, Configure the firewall's integration with Amazon Web Services..

AWS Objects

The **AWS** page is used to map the IP addresses of EC2 Instances running in the AWS Cloud with address objects and address groups configured on the firewall.

New address objects are created for Instance IP addresses, address groups for all addresses of an Instance and those Instance address groups can be added to existing address groups. Those objects, as with any other address objects and address groups, can then be used in firewall policies and features to permit or block access, route traffic and so on.

The **Profile Objects > AWS** page allows a SonicOS administrator to specify sets of EC2 Instance properties. If any of the Instances in one of the monitored regions matches a set of properties, address objects and address groups are created so that, effectively an address group representing the Instance is added to the custom, pre-existing address group specified in the relevant mapping. This address group can be used in firewall policies and, thus, those policies can shape the interaction with EC2 Instances running on AWS.



Enable Mapping: ●

Synchronization Interval: 180 secs.

Region:

#	ADDRESS GROUP	MATCHING CONDITIONS
No Data		

Total: 0 item(s)

Topics:

- About Address Object Mapping with AWS
- Viewing Instance Properties in SonicOSX
- Creating a New Address Object Mapping
- Enable Mapping
- Configuring Synchronization
- Configuring Regions to Monitor
- Verifying AWS Address Objects and Groups

About Address Object Mapping with AWS

EC2 Instances are virtual machines (VMs) running on AWS. Each instance can be one of a number of different available types, depending on the resources required for that instance by the customer. The virtual machine is an instance of a particular Amazon Machine Image (AMI), essentially a template and a specification for VMs that are created from it. All EC2 Instances have a number of properties including:

- Instance type
- AMI used in their creation
- Running state
- ID used for identification
- ID of the Virtual Private Cloud (VPC) where the Instance is located
- A set of user defined tags

You can use any or all of those properties to map matching Instances to address groups that a SonicOS administrator has previously configured on the firewall. Those address groups can be used in Route, VPN and Firewall Policies which can affect how the firewall interacts with AWS hosted machines.

In order to map EC2 Instances to firewall address groups, the Administrator configures any number of mappings between sets of instance properties and pre-existing address groups. If an EC2 Instance, in any of the monitored AWS Regions, matches a set of specified properties, one or more address objects and a single address group are created to represent that Instance and that address group is added to the target address group of the relevant mapping.

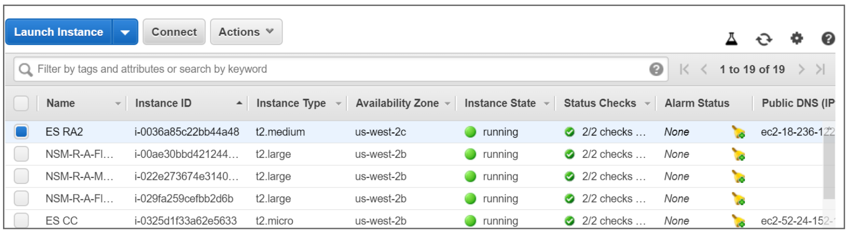
EC2 Instances can have multiple private and public IP addresses depending on the number of virtual network interfaces and the use of Elastic IP Addresses. When an Instance matches the properties specified in a mapping, address objects are created for each of its IP addresses, both public and private. Those address objects are then added into one address group which represents the EC2 Instance as a whole. It is that “Instance address group” that is then added to the mapping's target address group, an existing address group used in the configuration of the various firewall policies. Any one EC2 Instance may match the criteria of more than one mapping, in which case the Instance address group is added to more than one target address group. There are no limits.

Tagging an EC2 Instance on AWS

There are multiple ways to tag an EC2 Instance. This section describes how to do so manually.

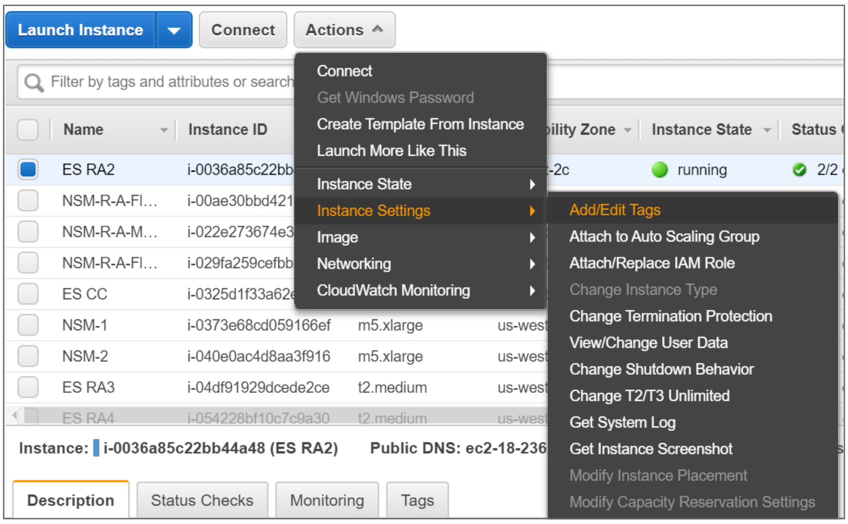
To manually add a tag to an existing EC2 Instance:

1. On the AWS Console, navigate to the EC2 Dashboard and turn to the Instances page.
2. Select the Instance that you wish to tag by selecting the check box in the first column of the table.



□	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IP
☑	ES RA2	i-0036a85c22bb44a48	t2.medium	us-west-2c	● running	✓ 2/2 checks ...	None	ec2-18-236-122
□	NSM-R-A-Fl...	i-00ae30bbd421244...	t2.large	us-west-2b	● running	✓ 2/2 checks ...	None	
□	NSM-R-A-M...	i-022e273674e3140...	t2.large	us-west-2b	● running	✓ 2/2 checks ...	None	
□	NSM-R-A-Fl...	i-029fa259cefbb2d6b	t2.large	us-west-2b	● running	✓ 2/2 checks ...	None	
□	ES CC	i-0325d1f33a62e5633	t2.micro	us-west-2b	● running	✓ 2/2 checks ...	None	ec2-52-24-152-

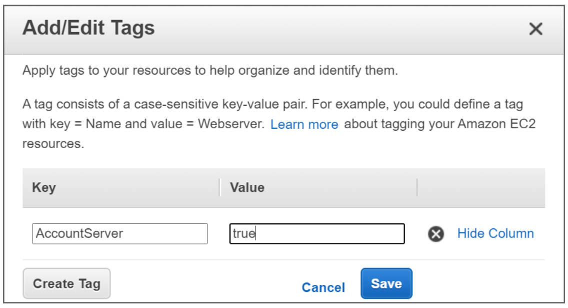
3. With the Instance selected, click on the **Actions** button to launch the popup menu.
4. Select **Instance Settings** and then select **Add/Edit Tags**.



Instance: i-0036a85c22bb44a48 (ES RA2)   Public DNS: ec2-18-236

The **Add/Edit** Tags dialog is displayed.

5. In the **Add/Edit** Tags dialog, enter descriptive values in the **Key** and **Value** fields.

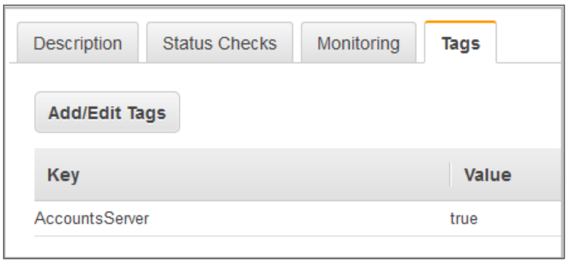


Apply tags to your resources to help organize and identify them.

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. Learn more about tagging your Amazon EC2 resources.

Key	Value
AccountServer	true

6. Click **Save** to tag the Instance with this key and value.
7. Verify the tag on the Instances page under the EC2 Dashboard. With the Instance still selected, view the associated tags by clicking the **Tags** tab in the panel at the bottom of the page. This provides confirmation that the EC2 Instance has been tagged.



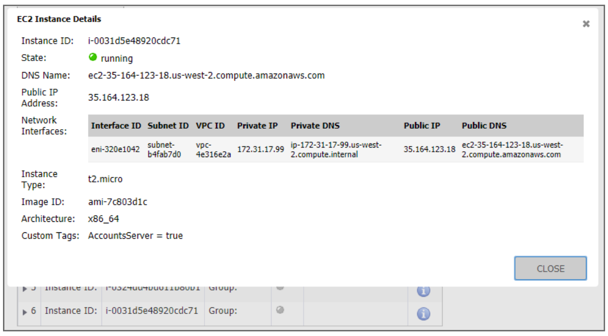
Key	Value
AccountsServer	true

You can now use that tag when defining address object mappings in the SonicOS management interface.

Viewing Instance Properties in SonicOSX

The **Profile Objects > AWS** page provides a way to define mappings between sets of EC2 Instance properties and firewall address groups. Address objects and an address group are created for any EC2 Instance that matches the set of specified properties, and the address group is added to the mapping's targeted address group.

For any EC2 Instance, you can view the values of the different properties that can be used in a mapping by clicking the **Information** button in the row for the Instance. This launches a popup dialog that displays the various properties including the Instance's ID, running state, AMI, type, the VPC ID and the different IP addresses. The user defined or custom tags, and their values, are also listed.



EC2 Instance Details

Instance ID: i-0031d5e48920cdc71

State: ● running

DNS Name: ec2-35-164-123-18.us-west-2.compute.amazonaws.com

Public IP Address: 35.164.123.18

Network Interfaces:

Interface ID	Subnet ID	VPC ID	Private IP	Private DNS	Public IP	Public DNS
eni-320e1042	subnet-b4fab7d0	vpc-4e316e2a	172.31.17.99	ip-172-31-17-99.us-west-2.compute.internal	35.164.123.18	ec2-35-164-123-18.us-west-2.compute.amazonaws.com

Instance Type: t2.micro

Image ID: ami-7c803d1c

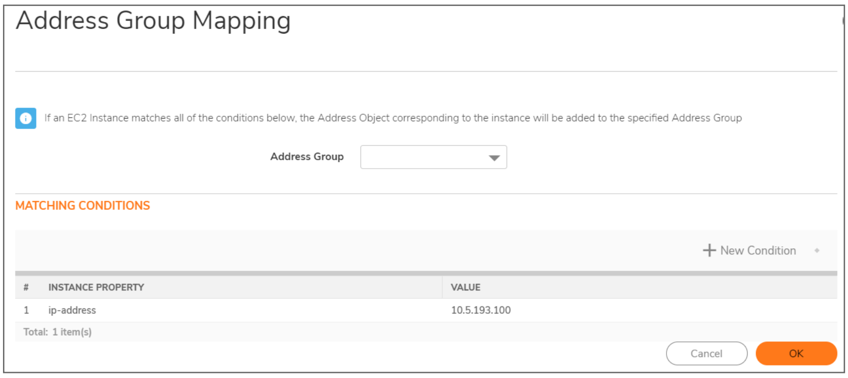
Architecture: x86_64

Custom Tags: AccountsServer = true

Creating a New Address Object Mapping

To create a new address object mapping:

1. Navigate to the **Object > Profile Objects > AWS** page.
2. Click the **New Mapping** button. This pops up a dialog enabling you to specify the details of the mapping.



Address Group Mapping

If an EC2 Instance matches all of the conditions below, the Address Object corresponding to the instance will be added to the specified Address Group

Address Group

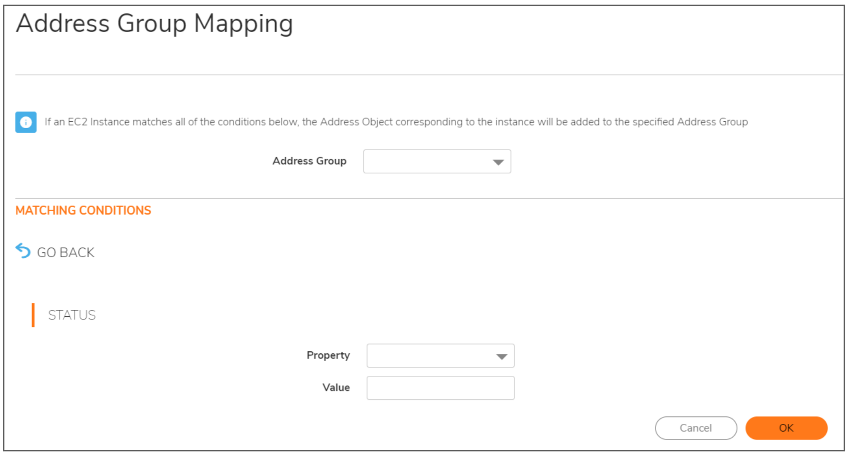
MATCHING CONDITIONS

#	INSTANCE PROPERTY	VALUE
1	ip-address	10.5.193.100

Total: 1 item(s)

3. In the **Address Group** drop-down list, select the existing address group to which the address groups representing any matched EC2 Instances will be added.

   Only custom address groups are shown in the selection control. If you have added a custom tag to an address group, you can use this custom tag to add a new condition to the mapping.
4. Click the **New Condition** button. The Mapping Condition options are displayed.



Address Group Mapping

If an EC2 Instance matches all of the conditions below, the Address Object corresponding to the instance will be added to the specified Address Group

Address Group

MATCHING CONDITIONS

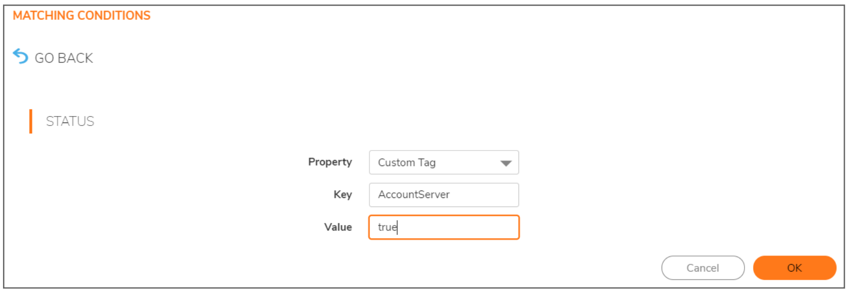
STATUS

Property

Value

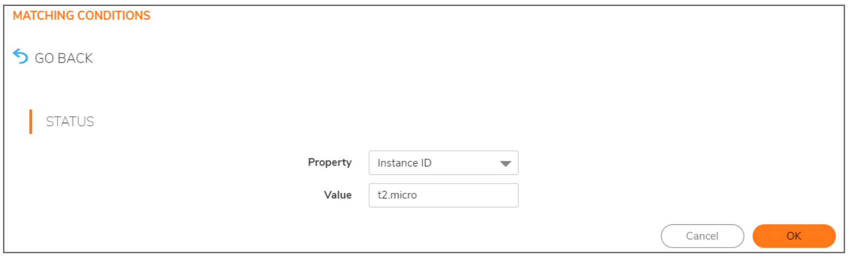
5. Choose the desired property from the **Property** drop-down list. For example, select **Custom Tag**.
6. In the **Key** field, enter the key for the tag.

7. In the **Value** field, enter the value that you wish to match against, such as true.



Property: Custom Tag
Key: AccountServer
Value: true

8. Click **OK**.
9. Back in the **Address Group Mapping** dialog, optionally add another mapping condition by clicking the **New Condition** button again.
10. Select the desired property from the **Property** drop-down list.
11. Fill in the displayed fields as needed.



Property: Instance ID
Value: t2.micro

12. Click **OK**.
13. Back in the **Address Group Mapping** dialog, review the whole mapping condition you are about to create.

    Any EC2 Instance in the regions of interest that match our specified conditions (in this example, having a custom tag of *AccountsServer* = *true* and of type *t2.micro*) will have address objects created for each of their IP addresses. Those address objects are added to an address group, representing the EC2 Instance as a whole and that address group is added to the address group targeted in the mapping. In this example, that is the address group called *AccountsDeptServers*.
14. Optionally edit or delete particular conditions by clicking on the corresponding button in the **Manage** column of the row.
15. When ready, click **OK**.
16. In the **Object > Profile Objects > AWS** page, click **Accept** to save the mapping.

Enable Mapping

You can create any number of address object mappings, however, they will not take effect until you enable mapping.

To enable mapping:

1. On the **Object > Profile Objects > AWS** page, select the **Enable Mapping** option.
2. Click the **Accept** button.

Configuring Synchronization

The **Synchronization Interval** determines how often the firewall should check for changes and make any necessary updates to the relevant address objects and address groups.

Synchronization is needed because the address object mappings and the AWS regions being monitored can be changed or reconfigured at any time, while the IP addresses and running state of the EC2 instances may be changed on AWS.

To configure the Synchronization Interval:

1. On the **Object > Profile Objects > AWS** page, enter the desired number of seconds into the **Synchronization Interval** field.
2. Click **Accept**.

To force synchronization:

1. On the **Object > Profile Objects > AWS** page, click on either the **Force Synchronization** or the **Delete AWS Address Objects** button.

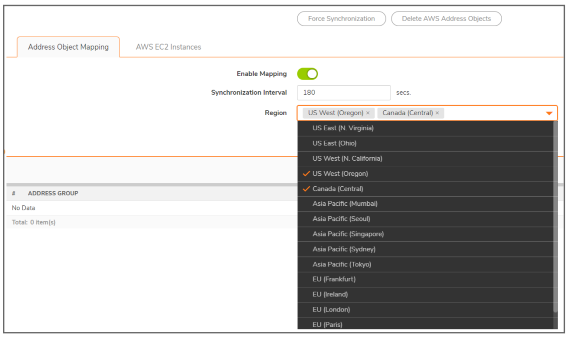
   This is useful if you are aware of changes and in a hurry to see the address objects updated accordingly.
2. Click **Accept**.
3. Click the **Refresh** button so that the page reflects the latest data.

Configuring Regions to Monitor

EC2 Instances are tied to particular AWS Regions. SonicOSX only monitors those AWS regions of particular interest. By default, this setting is initialized to the AWS region chosen as the Default Region during AWS Configuration and used if sending firewall logs to AWS CloudWatch Logs. However, it is possible to select multiple regions to monitor and the mappings will be applied across each of those selected.

To select one or more regions to monitor:

1. On the **Object > Profile Objects > AWS** page, click on the **Region** drop-down list and select the checkbox for each region of interest.



Enable Mapping ●

Synchronization Interval 180 secs.

Region US West (Oregon) × Canada (Central) ×

#	ADDRESS GROUP
No Data	

Total: 0 item(s)

2. Click **Accept**.

Verifying AWS Address Objects and Groups

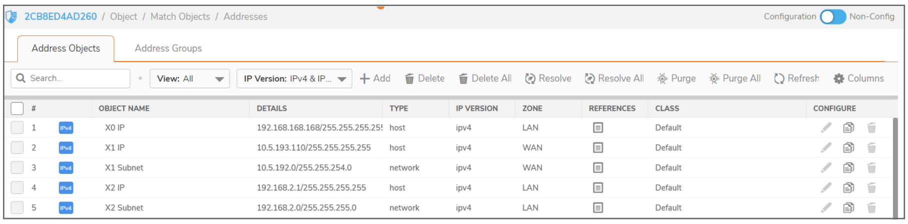
With mappings in place, a **Synchronization Interval** set, **Region** specified and, most importantly, **Mapping** enabled, you can view address objects and address groups representing the matched EC2 Instances and their IP addresses.

For example, on the AWS page itself, the address group and the Mapped address groups are shown in the EC2 Instances table.

Expanding the relevant row reveals the address objects corresponding to an Instance's public and private IP addresses.

Navigating to the **Object > Match Objects > Addresses** page in SonicOS and viewing the Address Object screen shows those same host address objects. VPN is used for the zone of private IP addresses and WAN is used for a public address zone.

A naming convention is used for the Instance address group and the address objects for each of the IP addresses, based on the Instance ID and, for the address objects, a suffix depending on whether the address is public or private.



□	#		OBJECT NAME	DETAILS	TYPE	IP VERSION	ZONE	REFERENCES	CLASS	CONFIGURE
□	1	IPv4	X0 IP	192.168.168.168/255.255.255.25!	host	ipv4	LAN	▤	Default	
□	2	IPv4	X1 IP	10.5.193.110/255.255.255.255	host	ipv4	WAN	▤	Default	
□	3	IPv4	X1 Subnet	10.5.192.0/255.255.254.0	network	ipv4	WAN	▤	Default	
□	4	IPv4	X2 IP	192.168.2.1/255.255.255.255	host	ipv4	LAN	▤	Default	
□	5	IPv4	X2 Subnet	192.168.2.0/255.255.255.0	network	ipv4	LAN	▤	Default	

Viewing the **Address Groups** screen and expanding the rows of interest shows that the original *AccountsDeptServers* address group now has an address group, representing an EC2 Instance, as a member.

The EC2 Instance address group itself contains the address objects that were created for each of its IP addresses.

9

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 Profile Objects Administration Guide
Updated - October 2020
Software Version - 7
232-005342-00 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