SonicWall® Management Services Firewall Settings Security Administration
# Contents

## Configuring Advanced Firewall Settings
- Detection Prevention .......................................................... 4
- Dynamic Ports .................................................................. 5
- Source Routed Packets ..................................................... 6
- Connections .................................................................... 6
- Dynamic Connection Sizing ............................................. 7
- Access Rule Service Options ........................................... 7
- IP and UDP Checksum Enforcement ................................. 8
- Jumbo Frame .................................................................. 8
- IPv6 Advanced Configuration ........................................... 8
- Control Plane Flood Protection ......................................... 9

## Configuring Bandwidth Management
- Understanding Bandwidth Management .......................... 10
- Configuring the Bandwidth Management Settings .......... 12
- Global Bandwidth Management ........................................ 14
  - Configuring Bandwidth Management ................................ 14
  - Configuring Global BWM on an Interface ......................... 15
  - Configuring Global BWM in an Access Rule .................... 15
  - Configuring Global BWM in an Action Object ................. 16
  - Configuring Application Rules ...................................... 16
- Advanced Bandwidth Management ..................................... 17
  - Elemental Bandwidth Settings ....................................... 19
  - Zone-Free Bandwidth Management ................................. 19
  - Weighted Fair Queuing .................................................. 19
- Configuring Bandwidth Management ..................................... 20
  - Enabling Advanced Bandwidth Management .................... 20
  - Configuring Bandwidth Policies ..................................... 21
  - Setting Interface Bandwidth Limitations with Advanced BWM ................................................................. 24
  - Setting Interface Bandwidth Limitations with Global BWM ................................................................. 25
- Upgrading to Advanced Bandwidth Management ................. 25

## Configuring Flood Protection Settings
- Configuring the TCP Settings ............................................. 27
- Configuring Layer 3 SYN Flood Protection ......................... 28
- Configuring Layer 2 SYN/RST/FIN/TCP Flood Protection – MAC Blacklisting ......................................................... 30
- WAN DDOS Protection (Non-TCP Floods) ............................ 30
  - Threshold for WAN DDOS protection (Non-TCP Packets / Sec) ............................................................... 31
  - WAN DDOS Filter Bypass Rate (every n packets) ......................... 31
  - WAN DDOS Allow List Timeout ...................................... 32
  - Enable DDOS protection on WAN interfaces .................... 32
- Configuring UDP Flood Protection Settings ......................... 32
- Configuring ICMP Flood Protection Settings ......................... 33
Contents

Configuring Firewall Multicast Settings ............................................. 34
  Multicast Snooping ................................................................. 34
  Multicast Policies ................................................................. 35
  IGMP State Table .................................................................... 35
    Enabling Multicast on LAN-Dedicated Interfaces ......................... 36
    Enabling Multicast Through a VPN ......................................... 37

Managing Quality of Service ......................................................... 39
  Classification ........................................................................ 39
  Marking ................................................................................ 40
  Conditioning ........................................................................... 40
    Site to Site VPN over QoS Capable Networks ......................... 41
    Site to Site VPN over Public Networks ................................ 41
  802.1p and DSCP QoS .............................................................. 42
    Enabling 802.1p ................................................................ 42
    DSCP Marking .................................................................... 45
  Bandwidth Management ............................................................ 51
  Glossary .................................................................................. 51

Configuring SSL Control ............................................................... 55
  About SSL Control .................................................................. 55
    Key Features of SSL Control .................................................. 57
    Key Concepts to SSL Control ............................................... 58
    Caveats and Advisories ......................................................... 61
  SSL Control Configuration ....................................................... 62
    General Settings .................................................................. 62
    Action ................................................................................ 62
    Configuration ...................................................................... 62
    Custom Lists ...................................................................... 64
  Enabling SSL Control on Zones .................................................. 65
  SSL Control Events .................................................................. 65

SonicWall Support ........................................................................ 67
  About This Document .............................................................. 68
Configuring Advanced Firewall Settings

This section provides advanced firewall settings for configuring detection prevention, dynamic ports, source routed packets, connection selection, and access rule options. To configure advanced access rule options, select Firewall Settings > Advanced Settings.

The Firewall Settings > Advanced Settings page includes the following firewall configuration option groups:

- Detection Prevention
- Dynamic Ports
- Source Routed Packets
- Connections
- Dynamic Connection Sizing
- Access Rule Service Options
- IP and UDP Checksum Enforcement
- Jumbo Frame
- IPv6 Advanced Configuration
- Control Plane Flood Protection

Detection Prevention

- Enable Stealth Mode - By default, the security appliance responds to incoming connection requests as either “blocked” or “open.” If you enable Stealth Mode, your security appliance does not respond to blocked inbound connection requests. Stealth Mode makes your security appliance essentially invisible to hackers.

- Randomize IP ID - Select Randomize IP ID to prevent hackers using various detection tools from detecting the presence of a security appliance. IP packets are given random IP IDs, which makes it more difficult for hackers to “fingerprint” the security appliance.

- Decrement IP TTL for forwarded traffic - Time-to-live (TTL) is a value in an IP packet that tells a network router whether or not the packet has been in the network too long and should be discarded. Select this option to decrease the TTL value for packets that have been forwarded and, therefore, have already been in the network for some time.

- Never generate ICMP Time-Exceeded packets - The firewall generates Time-Exceeded packets to report when it has dropped a packet because its TTL value has decreased to zero. Select this option if you do not want the firewall to generate these reporting packets.
**Dynamic Ports**

- **Enable FTP Transformations for TCP port(s) in Service Object** - Select from the service group drop-down menu to enable FTP transformations for a particular service object. By default, service group **FTP (All)** is selected.

  FTP operates on TCP ports 20 and 21, where port 21 is the Control Port and 20 is Data Port. When using non-standard ports (for example, 2020, 2121), however, SonicWall drops the packets by default as it is not able to identify it as FTP traffic. The **Enable FTP Transformations for TCP port(s) in Service Object** option allows you to select a Service Object to specify a custom control port for FTP traffic.

  To illustrate how this feature works, consider the following example of an FTP server behind the SonicWall listening on port 2121:

  a. On the **Firewall > Address Objects** page, create an **Address Object** for the private IP address of the FTP server with the following values:
     - **Name**: FTP Server Private
     - **Zone**: LAN
     - **Type**: Host
     - **IP Address**: 192.168.168.2
  
  b. On the **Firewall > Service Objects** page, create a custom Service for the FTP Server with the following values:
     - **Name**: FTP Custom Port Control
     - **Protocol**: TCP(6)
     - **Port Range**: 2121 - 2121
  
  c. On the **Network > NAT Policies** page, create a NAT Policy.
  
  d. On the **Firewall > Access Rules** page, create the Access Rule.
  
  e. On the **Firewall Settings > Advanced Settings** page, from the **Enable FTP Transformations for TCP port(s) in Service Object** drop-down menu, select the **FTP Custom Port Control** Service Object.

- **Enable support for Oracle (SQLNet)** - Select this option if you have Oracle9i or earlier applications on your network. For Oracle10g or later applications, it is recommended that this option not be selected.

  For Oracle9i and earlier applications, the data channel port is different from the control connection port. When this option is enabled, a SQLNet control connection is scanned for a data channel being negotiated. When a negotiation is found, a connection entry for the data channel is created dynamically, with NAT applied if necessary. Within Management Service, the SQLNet and data channel are associated with each other and treated as a session.

  For Oracle10g and later applications, the two ports are the same, so the data channel port does not need to be tracked separately; thus, the option does not need to be enabled.

- **Enable RTSP Transformations** - Select this option to support on-demand delivery of real-time data, such as audio and video. RTSP (Real Time Streaming Protocol) is an application-level protocol for control over delivery of data with real-time properties.
Source Routed Packets

- **Drop Source Routed IP Packets** - (Enabled by default.) Clear this checkbox if you are testing traffic between two specific hosts and you are using source routing.

  IP Source Routing is a standard option in IP that allows the sender of a packet to specify some or all of the routers that should be used to get the packet to its destination.

  This IP option is typically blocked from use as it can be used by an eavesdropper to receive packets by inserting an option to send packets from A to B via router C. The routing table should control the path that a packet takes, so that it is not overridden by the sender or a downstream router.

Connections

**IMPORTANT:** Any change to the Connections setting requires the SonicWall security appliance be restarted for the change to be implemented.

The Connections section provides the ability to fine-tune the firewall to prioritize for either optimal throughput or an increased number of simultaneous connections that are inspected by Deep-Packet Inspection (DPI) services. See Connection count.

### Connection count

<table>
<thead>
<tr>
<th>Platform</th>
<th>SPI connections</th>
<th>Maximum connections</th>
<th>DPI Performance optimized</th>
</tr>
</thead>
<tbody>
<tr>
<td>SuperMassive 9600</td>
<td>10,000,000</td>
<td>2,000,000</td>
<td>1,750,000</td>
</tr>
<tr>
<td>SuperMassive 9400</td>
<td>7,500,000</td>
<td>1,500,000</td>
<td>1,250,000</td>
</tr>
<tr>
<td>SuperMassive 9200</td>
<td>5,000,000</td>
<td>1,500,000</td>
<td>1,250,000</td>
</tr>
<tr>
<td>NSA 6600</td>
<td>2,000,000</td>
<td>1,000,000</td>
<td>750,000</td>
</tr>
<tr>
<td>NSA 5600</td>
<td>2,000,000</td>
<td>1,000,000</td>
<td>750,000</td>
</tr>
<tr>
<td>NSA 4600</td>
<td>1,000,000</td>
<td>500,000</td>
<td>375,000</td>
</tr>
<tr>
<td>NSA 3600</td>
<td>750,000</td>
<td>375,000</td>
<td>250,000</td>
</tr>
<tr>
<td>NSA 2600</td>
<td>500,000</td>
<td>250,000</td>
<td>125,000</td>
</tr>
<tr>
<td>TZ600</td>
<td>150,000</td>
<td>125,000</td>
<td>125,000</td>
</tr>
<tr>
<td>TZ500/TZ500 W</td>
<td>125,000</td>
<td>100,000</td>
<td>100,000</td>
</tr>
<tr>
<td>TZ400/TZ400 W</td>
<td>100,000</td>
<td>90,000</td>
<td>90,000</td>
</tr>
<tr>
<td>TZ300/TZ300 W</td>
<td>50,000</td>
<td>50,000</td>
<td>50,000</td>
</tr>
<tr>
<td>SOHO W</td>
<td>10,000</td>
<td>10,000</td>
<td>10,000</td>
</tr>
</tbody>
</table>

Only one option can be chosen. There is no change in the level of security protection provided by the DPI Connections settings.

- **Maximum SPI Connections (DPI services disabled)** - This option (Stateful Packet Inspection) does not provide SonicWall DPI Security Services protection and optimizes the firewall for maximum number of connections with only stateful packet inspection enabled. This option should be used by networks that require only stateful packet inspection, which is not recommended for most SonicWall network security appliance deployments.
• **Maximum DPI Connections (DPI services enabled)** - This is the default and recommended setting for most SonicWall network security appliance deployments.

• **DPI Connections (DPI services enabled with additional performance optimization)** - This option is intended for performance critical deployments. This option trades off the number of maximum DPI connections for an increased firewall DPI inspection throughput.

  **NOTE:** If either DPI Connections option is chosen and the DPI connection count is greater than 250,000, you can have the firewall resize the DPI connection and DPI-SSL counts dynamically. For more information, see Dynamic Connection Sizing.

The maximum number of connections depends on the physical capabilities of the particular model of SonicWall security appliance as shown in **Connection count**. Flow Reporting does not reduce the connection count on NSA Series and SM Series firewalls.

Mousing over the **Question Mark** icon next to the **Connections** heading displays a pop-up table of the maximum number of connections for your specific SonicWall security appliance for the various configuration permutations. The table entry for your current configuration is indicated in the popup table.

### Dynamic Connection Sizing

  **NOTE:** Dynamic connection sizing is supported on NSA 3600 Series (and higher) and SuperMassive Series network security appliances.

If either Maximum DPI Connections (DPI services enabled) or DPI Connections (DPI services enabled with additional performance optimization) is selected for Connections and the DPI connection count is greater than 250,000, the **Dynamic Connection Sizing** section displays. Configuring this option allows you to have the firewall increase the number of DPI-SSL connections by 750 by reducing the number of DPI connections by 1250000 dynamically.

- **DPI Connections** – Allows you to choose the maximum number of DPI connections, in increments of 125,000. Changing this count changes the value in the **DPI-SSL Connections** drop-down menu.

- **DPI-SSL Connections** – Allows you to choose the maximum number of DPI-SSL Connections, in increments of 750. Changing this count changes the value in the **DPI-SSL Connections** drop-down menu.

For example, if the number of DPI connections selected in the **DPI Connections** drop-down menu is **1250000**, the number of DPI-SSL connections in the **DPI-SSL Connections** drop-down menu is **165000**. If you select **1000000** from the **DPI Connections** drop-down menu, the number of DPI-SSL connections changes to **180000**. If you select **12000** from the **DPI-SSL Connections** drop-down menu, the number of DPI connections changes to **2000000**.

### Access Rule Service Options

- **Force inbound and outbound FTP data connections to use default port 20** - The default configuration allows FTP connections from port 20, but remaps outbound traffic to a port such as 1024. If the checkbox is selected, any FTP data connection through the security appliance must come from port 20 or the connection is dropped. The event is then logged as a log event on the security appliance.

- **Apply firewall rules for intra-LAN traffic to/from the same interface** - Applies firewall rules that are received on a LAN interface and destined for the same LAN interface. Typically, this only necessary when secondary LAN subnets are configured.

- **Always issue RST for discarded outgoing TCP connections** – Sends an RST (reset) packet to drop the connection for discarded outgoing TCP connections. This option is selected by default.
• **Enable ICMP Redirect on LAN zone** – Redirects ICMP packets on LAN zone interfaces. This option is selected by default.

• **Drop packets which source IP is subnet broadcast address** – Drops packets when the detected IP address is recognized as the one by the subnet.

### IP and UDP Checksum Enforcement

• **Enable IP header checksum enforcement** - Select this to enforce IP header checksums. Packets with incorrect checksums in the IP header are dropped. This option is disabled by default.

• **Enable UDP checksum enforcement** - Select this to enforce UDP packet checksums. Packets with incorrect checksums are dropped. This option is disabled by default.

### Jumbo Frame

- **Enable Jumbo Frame support** – Enabling this option increases throughput and reduces the number of Ethernet frames to be processed. Throughput increase may not be seen in some cases. However, there will be some improvement in throughput if the packets traversing are really jumbo size.

  - **NOTE:** Jumbo frames are supported on NSA 3600 and higher appliances.

  - **NOTE:** Jumbo frame packets are 9000 kilobytes in size and increase memory requirements by a factor of 4. Interface MTUs must be changed to 9000 bytes after enabling jumbo frame support as described in *SonicWall SonicOS 6.5 System Setup*.

### IPv6 Advanced Configuration

• **Drop IPv6 Routing Header type 0 packets** – Select this to prevent a potential DoS attack that exploits IPv6 Routing Header type 0 (RH0) packets. When this setting is enabled, RH0 packets are dropped unless their destination is the SonicWall security appliance and their Segments Left value is 0. Segments Left specifies the number of route segments remaining before reaching the final destination. Enabled by default. For more information, see [http://tools.ietf.org/html/rfc5095](http://tools.ietf.org/html/rfc5095).

• **Decrement IPv6 hop limit for forwarded traffic** – Similar to IPv4 TTL, when selected, the packet is dropped when the hop limit has been decremented to 0. Disabled by default.

• **Drop and log network packets whose source or destination address is reserved by RFC** – Select this option to reject and log network packets that have a source or destination address of the network packet defined as an address reserved for future definition and use as specified in RFC 4921 for IPv6. Disabled by default.

• **Never generate IPv6 ICMP Time-Exceeded packets** – By default, the SonicWall appliance generates IPv6 ICMP Time-Exceeded Packets that report when the appliance drops packets due to the hop limit decrementing to 0. Select this option to disable this function; the SonicWall appliance will not generate these packets. This option is selected by default.

• **Never generate IPv6 ICMP destination unreachable packets** – By default, the SonicWall appliance generates IPv6 ICMP destination unreachable packets. Select this option to disable this function; the SonicWall appliance will not generate these packets. This option is selected by default.
• **Never generate IPv6 ICMP redirect packets** – By default, the SonicWall appliance generates redirect packets. Select this option to disable this function; the SonicWall appliance will not generate redirect packets. This option is selected by default.

• **Never generate IPv6 ICMP parameter problem packets** – By default, the SonicWall appliance generates IPv6 ICMP parameter problem packets. Select this option to disable this function; the SonicWall appliance will not generate these packets. This option is selected by default.

• **Allow to use Site-Local-Unicast Address** – By default, the SonicWall appliance allows Site-Local Unicast (SLU) address and this checkbox is selected. As currently defined, SLU addresses are ambiguous and can present multiple sites. The use of SLU addresses may adversely affect network security through leaks, ambiguity, and potential misrouting. To avoid the issue, deselect the checkbox to prevent the appliance from using SLU addresses.

• **Enforce IPv6 Extension Header Validation** – Select this option if you want the SonicWall appliance to check the validity of IPv6 extension headers. By default, this option is disabled.

When both this option and the **Decrement IPv6 hop limit for forwarded traffic** option are selected, the **Enforce IPv6 Extension Header Order Check** option becomes available. (You may need to refresh the page.)

• **Enforce IPv6 Extension Header Order Check** – Select this option to have the SonicWall appliance check the order of IPv6 Extension Headers. By default, this option is disabled.

• **Enable NetBIOS name query response for ISATAP** – Select this option if you want the SonicWall appliance to generate a NetBIOS name in response to a broadcast ISATAP query. By default, this option is disabled.

(1) **NOTE:** Select this option only when one ISATAP tunnel interface is configured.

### Control Plane Flood Protection

• **Enable Control Plane Food Protection** – Select to have the firewall forward only control traffic destined to the firewall to the system Control Plane core (Core 0) if traffic on the Control Plane exceeds the threshold specified in **Control Flood Protection Threshold (CPU %)**. This option is not enabled by default.

To give precedence to legitimate control traffic, excess data traffic is dropped. This restriction prevents too much data traffic from reaching the Control Plane core, which can cause slow system response and potential network connection drops. The percentage configured for control traffic is guaranteed.

• **Control Flood Protection Threshold (CPU %)** – Enter the flood protection threshold as a percentage. The minimum is 5 (%), the maximum is 95, and the default is **75**.
Configuring Bandwidth Management

Bandwidth management (BWM) is a means of allocating bandwidth resources to critical applications on a network.

Management Service 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 travelling to Untrusted and Encrypted zones. Ingress BWM can be applied to traffic sourced from Untrusted and Encrypted zones travelling to Trusted and Public zones.

Topics:
- Understanding Bandwidth Management
- Configuring the Bandwidth Management Settings
- Global Bandwidth Management
- Advanced Bandwidth Management
- Configuring Bandwidth Management
- Upgrading to Advanced Bandwidth Management

Q 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 and thus 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. Refer to Managing Quality of Service for BWM QoS details.

Understanding Bandwidth Management

The SonicWall network security appliance uses BWM to control ingress and egress traffic. BWM allows network administrators to guarantee minimum bandwidth and prioritize traffic based on access rules created in the Policies | Rules > Access Rules 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.

BWM priority queues lists the Management Service priority queues.

<table>
<thead>
<tr>
<th>BWM priority queues</th>
<th>0 – Realtime</th>
<th>1 – Highest</th>
<th>2 – High</th>
<th>3 – Medium High</th>
<th>4 – Medium</th>
<th>5 – Medium Low</th>
<th>6 – Low</th>
<th>7 – Lowest</th>
<th>Lowest</th>
</tr>
</thead>
</table>

Various types of bandwidth management are available and can be selected on the Firewall Settings > BWM page.
Bandwidth management types

<table>
<thead>
<tr>
<th>BWM Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced</td>
<td>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.</td>
</tr>
<tr>
<td>Global</td>
<td>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.</td>
</tr>
<tr>
<td>None</td>
<td>(Default) Disables BWM.</td>
</tr>
</tbody>
</table>

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 Management Service 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.

Glossary

**Bandwidth Management (BWM)**
Any of a variety of algorithms or methods used to shape traffic or police traffic. Shaping often refers to the management of outbound traffic, while policing often refers to the management of inbound traffic (also known as admission control). There are many different methods of bandwidth management, including various queuing and discarding techniques, each with their own design strengths. SonicWall employs a Token Based Class Based Queuing method for inbound and outbound BWM, as well as a discard mechanism for certain types of inbound traffic.

**Guaranteed Bandwidth**
A declared percentage of the total available bandwidth on an interface which is always granted to a certain class of traffic. Applicable to both inbound and outbound BWM. The total Guaranteed Bandwidth across all BWM rules cannot exceed 100% of the total available bandwidth. Management Service 5.0 and higher enhances the Bandwidth Management feature to provide rate limiting functionality. You can create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. The Guaranteed Bandwidth can also be set to 0%.
Configuring Bandwidth Management Settings

BWM works by first enabling bandwidth management in the Firewall Settings > BWM 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, navigate to the Firewall Settings > BWM 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.

- **Bandwidth Management Type** option:

  **IMPORTANT:** When you change the Bandwidth Management Type from:
  - Global to Advanced, the default BWM actions that are in use in any App Rules policies are automatically converted to Advanced BWM settings.
  - Advanced to Global, the default BWM actions are converted to BWM Global-Medium.

  The firewall does not store your previous action priority levels when you switch the Type back and forth. You can view the conversions on the Firewall > App Rules page.
• **Advanced** — Any zone can have guaranteed and maximum bandwidth and prioritized traffic assigned per interface.

• **Global** — All zones can have assigned guaranteed and maximum bandwidth to services and have prioritized traffic. For traffic more than 1 Gbps, maximum bandwidth is limited to 1 Gbps.

• **None** — Disables BWM. This is the default.

• **Interface BWM Settings** — Mousing over the **Question Mark** icon displays a table showing whether the BWM settings are disabled or enabled for ingress and egress on the various interfaces.

• **Global Priority Bandwidth table** — Displays this information about the priorities:

<table>
<thead>
<tr>
<th>Priority</th>
<th>Enable</th>
<th>Guaranteed</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 High</td>
<td>30%</td>
<td></td>
</tr>
<tr>
<td>4 Medium</td>
<td>50%</td>
<td></td>
</tr>
<tr>
<td>6 Low</td>
<td>20%</td>
<td></td>
</tr>
</tbody>
</table>

  > **TIP:** You cannot disable priority 4 Medium, but you can change its percentage.

The sum of all guaranteed bandwidth must not exceed 100%. If the bandwidth exceeds 100%, the **Total** number becomes red. Also, the guaranteed bandwidth must not be greater than the maximum bandwidth per queue.

• **Maximum\Burst** — Enables the maximum/burst rate, as a percentage, for the enabled priority. The corresponding **Enable** checkbox must be checked for the rate to take effect.

### Action Objects

Action Objects define how the App Rules policy reacts to matching events. You can customize an action or select one of the predefined default actions. The predefined actions are displayed in the App Control Policy Settings page when you add or edit a policy from the App Rules page.

Custom BWM actions behave differently than the default BWM actions. Custom BWM actions are configured by adding a new action object from the **Firewall > Action Objects** page and selecting the Bandwidth Management action type. Custom BWM actions and policies using them retain their priority level setting when the Bandwidth Management Type is changed from **Global** to **Advanced**, and from **Advanced** to **Global**.

A number of BWM action options are also available in the predefined, default action list. The BWM action options change depending on the Bandwidth Management Type setting on the **Firewall Settings > BWM** page. If the **Bandwidth Management Type** is set to:

• **Global**, all eight levels of BWM are available.

• **Advanced**, no priorities are set. The priorities are set by configuring a bandwidth object under **Policies | Objects > Bandwidth Objects**.

**Adding a policy: Default actions** lists the predefined default actions that are available when adding a policy.
**Global Bandwidth Management**

Global Bandwidth Management can be configured using the following methods:

- Configuring Bandwidth Management
  - **IMPORTANT:** BWM must be enabled on **Firewall Settings > BWM** first.

- Configuring Global BWM on an Interface
- Configuring Global BWM in an Access Rule
- Configuring Global BWM in an Action Object
- Configuring Application Rules
- Elemental Bandwidth Settings
- Zone-Free Bandwidth Management
- Weighted Fair Queuing
- Enabling Advanced Bandwidth Management
- Configuring Bandwidth Policies
- Setting Interface Bandwidth Limitations with Advanced BWM

**Configuring Bandwidth Management**

*To set the Bandwidth Management type to Global:*

1. Navigate to **Firewall Settings > BWM**.
2. Set the **Bandwidth Management Type** option to **Global**.
3. Enable the priorities that you want by selecting the appropriate checkboxes in the **Enable** column.
   - **NOTE:** You must enable the priorities on this page to be able to configure these priorities in Access Rules, App Rules, and Action Objects.
4. Enter the **Guaranteed** bandwidth percentage that you want for each selected priority. The total amount cannot exceed 100%.
5 Enter the Maximum\Burst bandwidth percentage that you want for each selected priority.
6 Click Accept.

Configuring Global BWM on an Interface

IMPORTANT: Global BWM must be enabled on Firewall Settings > BWM first, as described in Configuring Bandwidth Management.

To configure BWM on an interface:
1 Navigate to Network > Interfaces.
2 Click the Edit button for the appropriate interface. The Edit Interface dialog displays.
3 Click Advanced.

NOTE: Displayed options may differ depending on how the interface is configured.
4 Scroll to Bandwidth Management.
5 Select either or both the Enable Interface Egress Bandwidth Limitation and Enable Interface Ingress Bandwidth Limitation checkbox. These options are not selected by default.

When either or both of these options are selected, if a there isn’t 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 Ingress Bandwidth (Kbps) field(s), enter the total bandwidth available for all ingress traffic in Kbps. The default is 384.000000 Kbps.
7 Click OK.

Configuring Global BWM in an Access Rule

IMPORTANT: Global BWM must be enabled on Firewall Settings > BWM first, as described in Configuring Bandwidth Management.

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

IMPORTANT: Before you can configure any priorities in an Access Rule, you must first enable the priorities that you want to use on the Firewall Settings > BWM page. Refer to the Firewall Settings > BWM page to determine which priorities are enabled. If you select a Bandwidth Priority that is not enabled on the Firewall Settings > BWM page, the traffic is automatically mapped to priority 4 Medium. See Configuring Bandwidth Management.

Priorities are listed in the Access Rules dialog Bandwidth Priority table; see BWM priority queues.

To configure Global BWM in an Access Rule:
1 Navigate to the Firewall > Access Rules page.
2 Click the Edit icon for the rule you want to edit. The Edit Rule dialog displays.
3 Click BWM.
4 Select either or both the Enable Egress Bandwidth Management ('Allow' rules only) checkbox and Enable Ingress Bandwidth Management ('Allow' rules only) checkbox. These options are not selected by default.
   a Select the appropriate bandwidth priority from the Bandwidth Priority drop-down menu. The highest, and default, priority is 0 Realtime. The lowest priority is 7 Lowest.
5 Click OK.

**Configuring Global BWM in an Action Object**

**IMPORTANT:** Global BWM must be enabled on Firewall Settings > BWM first, as described in Configuring Bandwidth Management.

If you do not want to use the predefined Global BWM actions or policies, you have the option to create a new one that fits your needs.

**To create a new Global BWM action object:**
1 Navigate to the Firewall > Action Objects page.
2 Click the Add button at the top of the Action Object table. The Add/Edit Action Object dialog displays.
3 In the Action Name field, enter a name for the action object.
4 In the Action drop-down menu, select Bandwidth Management to control and monitor application-level bandwidth usage. The options on the dialog change.
5 To specify BWM by priority, select either or both the Enable Egress Bandwidth Management checkbox and Enable Ingress Bandwidth Management checkbox. These options are not selected by default.
   a Select the appropriate bandwidth priority from the Bandwidth Priority drop-down menu(s). The highest, and default, priority is 0 Realtime. The lowest priority is 7 Lowest.
6 Click OK.

**Configuring Application Rules**

Configuring BWM in an Application Rule allows you to create policies that regulate bandwidth consumption by specific file types within a protocol, while allowing other file types to use unlimited bandwidth. This enables you to distinguish between desirable and undesirable traffic within the same protocol. Application Rule BWM supports the following Policy Types:

- SMTP Client
- HTTP Client
- HTTP Server
- FTP Client
- FTP Client File Upload
- FTP Client File Download
- FTP Data Transfer
- POP3 Client
- POP3 Server
- Custom Policy
- IPS Content
- App Control Content
- CFS

**NOTE:** You must first enable BWM before you can configure BWM in an Application Rule.

**Before you configure BWM in an App Rule:**
1 Enable the priorities you want to use in Security Configuration | Firewall Settings > BWM. See Configuring Bandwidth Management.
2 Enable BWM in an Action Object. See the Configuring Global BWM in an Action Object.
3 Configure BWM on the Interface. See the Configuring Global BWM on an Interface.
To configure BWM in an Application Rule:

1. Navigate to the Firewall > App Rules page.
2. Under App Rules Policies, select an action type from the Action Type drop-down menu.
3. Click the Edit icon in the Configure column for the policy you want to configure. The App Control Policy Settings dialog displays.
4. In the Action Object drop-down menu, select the BWM action object that you want.
5. Click OK.

Advanced Bandwidth Management

Advanced Bandwidth Management enables you to manage specific classes of traffic based on their priority and maximum bandwidth settings. Advanced Bandwidth Management consists of three major components:

- **Classifier** – classifies packets that pass through the firewall into the appropriate traffic class.
- **Estimator** – estimates and calculates the bandwidth used by a traffic class during a time interval to determine if that traffic class has available bandwidth.
- **Scheduler** – schedules traffic for transmission based on the bandwidth status of the traffic class provided by the estimator.

Advanced Bandwidth Management: Basic concepts illustrates the basic concepts of Advanced Bandwidth Management.

Advanced Bandwidth Management: Basic concepts

Bandwidth management configuration is 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 **bandwidth rule** specifies the actual parameters, such as priority, guaranteed bandwidth, maximum bandwidth, and per-IP bandwidth management, and is configured in a bandwidth object. Bandwidth rules identify and organize packets into traffic classes by matching specific criteria.

A **classifier** is an access rule or application rule in which a bandwidth object is enabled. Access rules and application rules are configured for specific interfaces or interface zones.
The first step in bandwidth management is that all packets that pass through the Management Service firewall are assigned a classifier (class tag). The classifiers identify packets as belonging to a particular traffic class. Classified packets are then passed to the BWM engine for policing and shaping. The Management Service uses two types of classifiers:

- Access Rules
- Application Rules

A rule that has sub elements is known as a parent rule.

**Configuring a bandwidth object: Parameters** shows the parameters that are configured in a bandwidth object:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guaranteed Bandwidth</td>
<td>The bandwidth that is guaranteed to be provided for a particular traffic class.</td>
</tr>
<tr>
<td>Maximum Bandwidth</td>
<td>The maximum bandwidth that a traffic class can utilize.</td>
</tr>
<tr>
<td>Traffic Priority</td>
<td>The priority of the traffic class.</td>
</tr>
<tr>
<td></td>
<td>• 0 – highest priority</td>
</tr>
<tr>
<td></td>
<td>• 7 – lowest priority</td>
</tr>
<tr>
<td>Violation Action</td>
<td>The firewall action that occurs when traffic exceeds the maximum bandwidth.</td>
</tr>
<tr>
<td></td>
<td>• Delay – packets are queued and sent when possible.</td>
</tr>
<tr>
<td></td>
<td>• Drop – packets are dropped immediately.</td>
</tr>
<tr>
<td>Enable Per-IP Bandwidth Management</td>
<td>The elemental feature that enables the firewall to support time-critical traffic, such as voice and video, effectively. When per-IP BWM is enabled, the elemental bandwidth settings are applied to each individual IP under its parent rule.</td>
</tr>
</tbody>
</table>

After packets have been tagged with a specific traffic class, the BWM engine gathers them for policing and shaping based on the bandwidth settings that have been defined in a bandwidth object, enabled in an access rule, and attached to application rules.

Classifiers also identify the direction of packets in the traffic flow. Classifiers can be set for either the egress, ingress, or both directions. For Bandwidth Management, the terms ingress and egress are defined as follows:

- **Ingress** – Traffic from initiator to responder in a particular traffic flow.
- **Egress** – Traffic from responder to initiator in a particular traffic flow.

For example, a client behind Interface X0 has a connection to a server which is behind Interface X1. **Direction of traffic** shows:

- Direction of traffic flow in each direction for client and server
- Direction of traffic on each interface
- Direction indicated by the BWM classifier

**Direction of traffic**

<table>
<thead>
<tr>
<th>Direction of Traffic Flow</th>
<th>Direction of Interface X0</th>
<th>Direction of Interface X1</th>
<th>BWM Classifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client to Server</td>
<td>Egress</td>
<td>Ingress</td>
<td>Egress</td>
</tr>
<tr>
<td>Server to Client</td>
<td>Ingress</td>
<td>Egress</td>
<td>Ingress</td>
</tr>
</tbody>
</table>

To be compatible with traditional bandwidth management settings in WAN zones, the terms inbound and outbound are still supported to define traffic direction. These terms are only applicable to active WAN zone interfaces.

- **Outbound** – Traffic from LAN\DMZ zone to WAN zone (Egress).
- **Inbound** – Traffic from WAN zone to LAN\DMZ zone (Ingress).
Elemental Bandwidth Settings

Elemental bandwidth 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. When Per-IP BWM is enabled, the elemental bandwidth settings are applied to each individual IP under its parent rule.

The Elemental Bandwidth Settings feature enables a bandwidth object to be applied to individual elements under a parent traffic class. Elemental Bandwidth Settings is a sub-option of Firewall > Bandwidth Objects, the parent rule or traffic class. The following table shows the parameters that are configured under Elemental Bandwidth Settings; see SonicWall SonicOS 6.5 Policies.

### Elemental Bandwidth settings: Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Per-IP Bandwidth Management</td>
<td>When enabled, the maximum elemental bandwidth setting applies to each IP address under the parent traffic class, which allows the firewall to support time-critical traffic, such as voice and video, effectively.</td>
</tr>
<tr>
<td>Maximum Bandwidth</td>
<td>The maximum elemental bandwidth that can be allocated to an IP address under the parent traffic class. The maximum elemental bandwidth cannot be greater than the maximum bandwidth of its parent class.</td>
</tr>
</tbody>
</table>

When you enable Per-IP Bandwidth Management, each individual IP under its parent rule will be applied to the elemental bandwidth settings.

### Zone-Free Bandwidth Management

The zone-free bandwidth management feature enables bandwidth management on all interfaces regardless of their zone assignments. Previously, bandwidth management only applied to these zones:

- LAN/DMZ to WAN/VPN
- WAN/VPN to LAN/DMZ

In Management Service 6.2 and above, zone-free bandwidth management can be performed across all interfaces regardless of zone.

Zone-free bandwidth management allows you to configure the maximum bandwidth limitation independently, in either the ingress or egress direction, or both, and apply it to any interfaces using Access Rules and Application Rules.

**NOTE:** Interface bandwidth limitation is only available on physical interfaces. Failover and load balancing configuration does not affect interface bandwidth limitations.

### Weighted Fair Queuing

Traditionally, Management Service bandwidth management distributes traffic to 8 queues based on the priority of the traffic class of the packets. These 8 queues operate with strict priority queuing. Packets with the highest priority are always transmitted first.

Strict priority queuing can cause high priority traffic to monopolize all of the available bandwidth on an interface, and low priority traffic will consequently be stuck in its queue indefinitely. Under strict priority queuing, the scheduler always gives precedence to higher priority queues. This can result in bandwidth starvation to lower priority queues.
Weighted Fair queuing (WFQ) alleviates the problem of bandwidth starvation by servicing packets from each queue in a round robin manner, so that all queues are serviced fairly within a given time interval. High priority queues get more service and lower priority queues get less service. No queue gets all the service because of its high priority, and no queue is left unserviced because of its low priority.

For example, Traffic Class A is configured as Priority 1 with a maximum bandwidth of 400 kbps. Traffic Class B is configured as Priority 3 with a maximum bandwidth of 600 kbps. Both traffic classes are queued to an interface that has a maximum bandwidth of only 500kbps. Both queues will be serviced based on their priority in a round robin manner. So, both queues will be serviced, but Traffic Class A will be transmitted faster than Traffic Class B.

**Shaped bandwidth for consecutive sampling intervals** shows the shaped bandwidth for each consecutive sampling interval:

<table>
<thead>
<tr>
<th>Sampling Interval</th>
<th>Traffic Class A</th>
<th>Traffic Class B</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Incoming kbps</td>
<td>Shaped kbps</td>
</tr>
<tr>
<td>1</td>
<td>500</td>
<td>380</td>
</tr>
<tr>
<td>2</td>
<td>500</td>
<td>350</td>
</tr>
<tr>
<td>3</td>
<td>400</td>
<td>300</td>
</tr>
<tr>
<td>4</td>
<td>600</td>
<td>400</td>
</tr>
<tr>
<td>5</td>
<td>200</td>
<td>180</td>
</tr>
<tr>
<td>6</td>
<td>200</td>
<td>200</td>
</tr>
</tbody>
</table>

**Configuring Bandwidth Management**

**Topics:**
- Enabling Advanced Bandwidth Management
- Configuring Bandwidth Policies
- Setting Interface Bandwidth Limitations with Advanced BWM

**Enabling Advanced Bandwidth Management**

**To enable Advanced bandwidth management:**

1. On the firewall, navigate to the **Firewall Settings > BWM** page.
2. Set the **Bandwidth Management Type** option to **Advanced**.
3. Click **Accept**.

**NOTE:** When Advanced BWM is selected, the priorities fields are disabled and cannot be set here. Under Advanced BWM, the priorities are set in bandwidth policies. See Configuring Bandwidth Policies.
Configuring Bandwidth Policies

Topics:

- Configuring a Bandwidth Object
- Enabling Elemental Bandwidth Management
- Enabling a Bandwidth Object in an Access Rule
- Enabling a Bandwidth Priority in an Access Rule
- Enabling a Bandwidth Object in an Action Object
- Enabling a Bandwidth Priority and Bandwidth Objects in an Action Object

Configuring a Bandwidth Object

To configure a bandwidth object:

1. Navigate to the Firewall > Bandwidth Objects page.
2. Do one of the following:
   - Click the Add button to create a new Bandwidth Object.
   - Click the Edit icon of the Bandwidth Object you want to change.
     The Bandwidth Object Settings dialog displays.
3. In the Name field, enter a name for this bandwidth object.
4. In the Guaranteed Bandwidth field, enter the amount of bandwidth that this bandwidth object will guarantee to provide for a traffic class (in kbps or Mbps).
   a. Specify whether the bandwidth is kbps (default) or Mbps from the drop-down menu.
5. In the Maximum Bandwidth field, enter the maximum amount of bandwidth that this bandwidth object will provide for a traffic class.
   a. Specify whether the bandwidth is kbps (default) or Mbps from the drop-down menu.
6. In the Traffic Priority field, enter the priority that this bandwidth object will provide for a traffic class.
   The highest, and default, priority is 0 Realtime. The lowest priority is 7 Lowest.
   When multiple traffic classes compete for shared bandwidth, classes with the highest priority are given precedence.
7. In the Violation Action field, enter the action that this bandwidth object will provide when traffic exceeds the maximum bandwidth setting:
   - Delay – Specifies that excess traffic packets are queued and sent when possible.
   - Drop – Specifies that excess traffic packets are dropped immediately.
8. In the Comment field, enter a text comment or description for this bandwidth object.
9. Click OK.

NOTE: The actual allocated bandwidth may be less than this value when multiple traffic classes compete for a shared bandwidth.
Enabling Elemental Bandwidth Management

Elemental Bandwidth Management enables Management Service to enforce bandwidth rules and policies on each individual IP that passes through the firewall.

To enable elemental bandwidth management in a bandwidth object:

1. Navigate to the Firewall > Bandwidth Objects page.
2. Click the Edit icon of the Bandwidth Object you want to change. The Bandwidth Object Settings dialog displays.
3. Click Elemental.
4. Select the Enable Per-IP Bandwidth Management option. This option is not selected by default. When enabled, the maximum elemental bandwidth setting applies to each individual IP under the parent traffic class.
5. In the Maximum Bandwidth field, enter the maximum elemental bandwidth that can be allocated to a protocol under the parent traffic class.
   a. Specify whether the bandwidth is kbps (default) or Mbps from the drop-down menu.
6. Click OK.

Enabling a Bandwidth Object in an Access Rule

If Advanced BWM is selected, you can enable bandwidth objects (and their configurations) in Rules > Access Rules.

To enable a bandwidth object in an Access Rule:

1. Navigate to the Firewall > Access Rules page.
2. Do one of the following:
   • Click the Add button to create a new Access Rule. The Add Rule dialog displays.
   • Click the Edit icon for the appropriate Access Rule. The Edit Rule dialog displays.
3. Click BWM.
4. To enable a bandwidth object for the egress direction, under Bandwidth Management, select the Enable Egress Bandwidth Management checkbox.
5. From the Select a Bandwidth Object drop-down menu, select the bandwidth object you want for the egress direction.
6. To enable a bandwidth object for the ingress direction, under Bandwidth Management, select the Enable Ingress Bandwidth Management checkbox.
7. From the Select a Bandwidth Object drop-down menu, select the bandwidth object you want for the ingress direction.
8. To enable bandwidth usage tracking, select the Enable Tracking Bandwidth Usage option.
9. Click OK.
Enabling a Bandwidth Priority in an Access Rule

If **Global BWM BWM** is selected, you can enable bandwidth priority in **Firewall > Access Rules**.

**To enable bandwidth priority in an Access Rule:**

1. Navigate to the **Firewall > Access Rules** page.
2. Do one of the following:
   - Click the **Add** button to create a new Access Rule. The **Add Rule** dialog displays.
   - Click the **Edit** icon for the appropriate Access Rule. The **Edit Rule** dialog displays.
3. Click **BWM**.
4. To enable a bandwidth object for the egress direction, under **Bandwidth Management**, select the **Enable Egress Bandwidth Management** checkbox. This option is not selected by default.
5. From the **Bandwidth Priority** drop-down menu, select the bandwidth priority you want for the egress direction. The highest, and default, priority is **0 Realtime**. The lowest priority is **7 Lowest**.
6. To enable a bandwidth object for the ingress direction, under **Bandwidth Management**, select the **Enable Ingress Bandwidth Management** checkbox. This option is not selected by default.
7. From the **Bandwidth Priority** drop-down menu, select the bandwidth priority you want for the ingress direction. The highest, and default, priority is **0 Realtime**. The lowest priority is **7 Lowest**.
8. Click **OK**.

Enabling a Bandwidth Object in an Action Object

If **Advanced BWM** is selected, you can enable bandwidth objects (and their configurations) in **Firewall > Access Rules**.

**To enable a bandwidth object in an action object:**

1. Navigate to the **Firewall > Action Objects** page.
2. Create a new action object by clicking on the **Add** button. The **Action Object Settings** dialog displays.
3. Enter a name for the action object in the **Action Name** field.
4. From the **Action** drop-down menu, select **Bandwidth Management**, which allows control and monitoring of application-level bandwidth usage. The options on the **Action Object Settings** dialog change.
5. In the **Bandwidth Aggregation Method** drop-down menu, select the appropriate bandwidth aggregation method:
   - **Per Policy** (default)
   - **Per Action**
6. To enable bandwidth management in the egress direction, select the **Enable Egress Bandwidth Management** option.
   a. From the **Bandwidth Object** drop-down menu, select the bandwidth object for the egress direction.
7. To enable bandwidth management in the ingress direction, select the **Enable Ingress Bandwidth Management** option.
   a. From the **Bandwidth Object** drop-down menu, select the bandwidth object for the ingress direction.
8 Optionally, to enable bandwidth usage tracking, select the Enable Tracking Bandwidth Usage option. This option is available only if either or both of the Enable Bandwidth Management options are selected.

9 Click OK.

Enabling a Bandwidth Priority and Bandwidth Objects in an Action Object

If Global BWM BWM is selected, you can specify BWM priority and enable bandwidth objects (and their configurations) in Firewall > Access Rules.

To enable bandwidth priority and a bandwidth object in an action object:

1 Navigate to the Firewall > Action Objects page.
2 Create a new action object by clicking on the Add button. The Action Object Settings dialog displays.
3 Enter a name for the action object in the Action Name field.
4 From the Action drop-down menu, select Bandwidth Management, which allows control and monitoring of application-level bandwidth usage. The options on the Action Object Settings dialog change.
5 To enable bandwidth management in the egress direction, select the Enable Egress Bandwidth Management for priority option.
   a From the Bandwidth Priority drop-down menu, select the bandwidth object for the egress direction. The highest, and default, priority is 0 Realtime. The lowest priority is 7 Lowest.
6 To enable bandwidth management in the ingress direction, select the Enable Ingress Bandwidth Management for priority option.
   a From the Bandwidth Priority drop-down menu, select the bandwidth object for the ingress direction. The highest, and default, priority is 0 Realtime. The lowest priority is 7 Lowest.
7 Click OK.

Setting Interface Bandwidth Limitations with Advanced BWM

To set the bandwidth limitations for an interface:

1 Navigate to the Network > Interfaces page.
2 Click the Edit icon for the appropriate interface. The Edit Interface dialog displays.
3 Click Advanced.
4 Scroll to the Bandwidth Management section.
5 Select the Enable Interface Egress Bandwidth Limitation option. This option is not selected by default.
   When this option is:
   • Selected, the maximum available egress BWM is defined, but as advanced BWM is policy based, the limitation is not enforced unless there is a corresponding Access Rule or App Rule.
   • Not selected, no bandwidth limitation is set at the interface level, but egress traffic can still be shaped using other options.
a In the **Maximum Interface Egress Bandwidth (kbps)** field, enter the maximum egress bandwidth for the interface (in kilobytes per second). The default is **384.000000** Kbps.

6 Select the **Enable Interface Ingress Bandwidth Limitation** option. This option is not selected by default. For information on using this option, see **Step 5**.

7 Click **OK**.

### Setting Interface Bandwidth Limitations with Global BWM

**To set the bandwidth limitations for an interface:**

1 Navigate to the **Network > Interfaces** page.
2 Click the **Edit** icon for the appropriate interface. The **Edit Interface** dialog displays.
3 Click **Advanced**.
4 Scroll to the **Bandwidth Management** section.
5 Select the **Enable Interface Egress Bandwidth Limitation** option. This option is not selected by default. When this option is:
   - Selected, the maximum available egress BWM is defined, but as advanced BWM is policy based, the limitation is not enforced unless there is a corresponding Access Rule or App Rule.
   - Not selected, no bandwidth limitation is set at the interface level, but egress traffic can still be shaped using other options.

a In the **Maximum Interface Egress Bandwidth (kbps)** field, enter the maximum egress bandwidth for the interface (in kilobytes per second). The default is **384.000000** Kbps.

6 Select the **Enable Interface Ingress Bandwidth Limitation** option. This option is not selected by default. This option is not selected by default. For information on using this option, see **Step 5**.

7 Click **OK**.

### Upgrading to Advanced Bandwidth Management

Advanced Bandwidth Management uses Bandwidth Objects as the configuration method. Bandwidth objects are configured under **Objects > Bandwidth Objects**, and can then be enabled in **Rules > Access Rules**.

The Advanced Bandwidth Upgrade feature automatically converts all active, valid, traditional BWM configurations to the Bandwidth Objects design model.

In traditional BWM configuration, the BWM engine only affects traffic when it is transmitted through the primary WAN interface or the active load balancing WAN interface. Traffic that does not pass through these interfaces, is not subject to bandwidth management regardless of the **Access Rule** or **App Rule** settings.

Under Advanced Bandwidth Management, the BWM engine can enforce Bandwidth Management settings on any interface.
During the Advanced Bandwidth Management Upgrade process, Management Service translates traditional BWM settings into a default Bandwidth Object and links it to the original classifier rule (Access Rule or App Rule). The auto-generated default Bandwidth Object inherits all the BWM parameters for both the Ingress and Egress directions.

The two following graphics show the traditional BWM settings. The graphic that follows them shows the new Bandwidth Objects that are automatically generated during the Advanced Bandwidth Management Upgrade process.
Configuring Flood Protection Settings

**NOTE:** Control Plane flood protection is located on the Firewall Settings > Advanced page.

**TIP:** You must click Update to activate any settings you select or change.

The Firewall Settings > Flood Protection page allows you to:

- Manage:
  - TCP (Transmission Control Protocol) traffic settings such as Layer 2/Layer 3 flood protection, WAN DDOS protection
  - UDP (User Datagram Protocol) flood protection
  - ICMP (Internet Control Message Protocol) or ICMPv6 flood protection.

- View statistics on traffic through the security appliance:
  - TCP traffic
  - UDP traffic
  - ICMP or ICMPv6 traffic

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

**Topics:**

- Configuring the TCP Settings
- Configuring Layer 3 SYN Flood Protection
- Configuring Layer 2 SYN/RST/FIN/TCP Flood Protection – MAC Blacklisting
- WAN DDOS Protection (Non-TCP Floods)
- Configuring UDP Flood Protection Settings
- Configuring ICMP Flood Protection Settings

### Configuring the TCP Settings

**To configure the TCP Settings:**

1. Navigate to the Firewall Settings > Flood Protection page.
2. Configure the TCP settings you need for your environment:
• **Enforce strict TCP compliance with RFC 793 and RFC 1122** – Ensures strict compliance with several TCP timeout rules. This setting maximizes TCP security, but it may cause problems with the Window Scaling feature for Windows Vista users. This option is not selected by default.
  - **Enable TCP handshake enforcement** – Requires a successful three-way TCP handshake for all TCP connections. This option, available only if the Enforce strict TCP compliance with RFC 793 and RFC 1122, is not selected by default.
• **Enable TCP checksum enforcement** – If an invalid TCP checksum is calculated, the packet is dropped. This option is not selected by default.
• **Enable TCP handshake timeout** – Enforces the timeout period (in seconds) for a three-way TCP handshake to complete its connection. If the three-way TCP handshake does not complete in the timeout period, it is dropped. This option is selected by default.
  - **TCP Handshake Timeout (seconds)** – The maximum time a TCP handshake has to complete the connection. The default is 30 seconds.
• **Default TCP Connection Timeout** – The default time assigned to Access Rules for TCP traffic. If a TCP session is active for a period in excess of this setting, the TCP connection is cleared by the firewall. The default value is 15 minutes, the minimum value is 1 minute, and the maximum value is 999 minutes.
  - **NOTE:** Setting excessively long connection time-outs slows the reclamation of stale resources, and in extreme cases, could lead to exhaustion of the connection cache.
• **Maximum Segment Lifetime (seconds)** – Determines the number of seconds that any TCP packet is valid before it expires. This setting is also used to determine the amount of time (calculated as twice the Maximum Segment Lifetime, or 2MSL) that an actively closed TCP connection remains in the TIME_WAIT state to ensure that the proper FIN / ACK exchange has occurred to cleanly close the TCP connection. The default value is 8 seconds, the minimum value is 1 second, and the maximum value is 60 seconds.
• **Enable Half Open TCP Connections Threshold** – Denies new TCP connections if the high-water mark of TCP half-open connections has been reached. By default, the half-open TCP connection is not monitored, so this option is not selected by default.
  - **Maximum Half Open TCP Connections** – Specifies the maximum number of half-open TCP connections. The default maximum is half the number of maximum connection caches.

**Configuring Layer 3 SYN Flood Protection**

A SYN Flood Protection mode is the level of protection that you can select to defend against half-opened TCP sessions and high-frequency SYN packet transmissions. This feature enables you to set three different levels of SYN Flood Protection.

**To configure SYN Flood Protection features:**

1. Navigate to the Firewall Settings > Flood Protection page.
2. Scroll down to the Layer 3 SYN Flood Protection - SYN Proxy section.
3. From the SYN Flood Protection Mode drop-down menu, select the type of protection mode:
   - **Watch and Report Possible SYN Floods** – Enables the device to monitor SYN traffic on all interfaces on the device and to log suspected SYN flood activity that exceeds a packet count threshold. The feature does not turn on the SYN Proxy on the device so the device forwards the TCP three-way handshake without modification.
This is the least invasive level of SYN Flood protection. Select this option if your network is not in a high-risk environment.

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

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

- **Always Proxy WAN Client Connections** – Sets the device to always use SYN Proxy. This method blocks all spoofed SYN packets from passing through the device.

This is an extreme security measure that directs the device to respond to port scans on all TCP ports because the SYN Proxy feature forces the device to respond to all TCP SYN connection attempts. This can degrade performance and can generate a false positive. Select this option only if your network is in a high-risk environment.

4 Select the **SYN Attack Threshold** configuration options to provide limits for SYN Flood activity before the device drops packets. The device gathers statistics on WAN TCP connections, keeping track of the maximum and average maximum and incomplete WAN connections per second. Out of these statistics, the device suggests a value for the SYN flood threshold.

- **Suggested value calculated from gathered statistics** – The suggested attack threshold based on WAN TCP connection statistics.

- **Attack Threshold (Incomplete Connection Attempts/Second)** – Enables you to set the threshold for the number of incomplete connection attempts per second before the device drops packets at any value between 5 and 200,000. The default is the Suggested value calculated from gathered statistics.

5 Select the **SYN-Proxy options** to provide more control over the options sent to WAN clients when in SYN Proxy mode.

1. **NOTE:** The options in this section are not available if Watch and report possible SYN floods is selected for **SYN Flood Protection mode**.

When the device applies a SYN Proxy to a TCP connection, it responds to the initial SYN packet with a manufactured SYN/ACK reply, waiting for the ACK in response before forwarding the connection request to the server. Devices attacking with SYN Flood packets do not respond to the SYN/ACK reply. The firewall identifies them by their lack of this type of response and blocks their spoofed connection attempts. SYN Proxy forces the firewall to manufacture a SYN/ACK response without knowing how the server will respond to the TCP options normally provided on SYN/ACK packets.

- **All LAN/DMZ servers support the TCP SACK option** – Enables SACK (Selective Acknowledgment) where a packet can be dropped and the receiving device indicates which packets it received. This option is not enabled by default. Enable this checkbox only when you know that all servers covered by the firewall accessed from the WAN support the SACK option.

- **Limit MSS sent to WAN clients (when connections are proxied)** – Enables you to enter the maximum MSS (Minimum Segment Size) value. This sets the threshold for the size of TCP segments, preventing a segment that is too large to be sent to the targeted server. For example, if the server is an IPsec gateway, it may need to limit the MSS it received to provide space for IPsec headers when tunneling traffic. The firewall cannot predict the MSS value sent to the server when it responds to the SYN manufactured packet during the proxy sequence. Being able to control the size of a segment, enables you to control the manufactured MSS value sent to WAN clients. This option is not selected by default.
If you specify an override value for the default of 1460, a segment of that size or smaller is sent to the client in the SYN/ACK cookie. Setting this value too low can decrease performance when the SYN Proxy is always enabled. Setting this value too high can break connections if the server responds with a smaller MSS value.

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

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

- **Always log SYN packets received** – Logs all SYN packets received.

## Configuring Layer 2 SYN/RST/FIN/TCP Flood Protection – MAC Blacklisting

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

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

- **Threshold for SYN/RST/FIN flood blacklisting (SYNs / Sec)**—Specifies the maximum number of SYN, RST, FIN, and TCP packets allowed per second. The minimum is 10, the maximum is 800000, and default is 1,000. This value should be larger than the SYN Proxy threshold value because blacklisting attempts to thwart more vigorous local attacks or severe attacks from a WAN network.

  **NOTE:** This option cannot be modified unless **Enable SYN/RST/FIN/TCP flood blacklisting on all interfaces** has been enabled.

- **Enable SYN/RST/FIN flood blacklisting on all interfaces**—Enables the blacklisting feature on all interfaces on the firewall. This option is not selected by default. When it is selected, these options become available:

  - **Never blacklist WAN machines**—This check box ensures that systems on the WAN are never added to the SYN Blacklist. This option is recommended as leaving it cleared may interrupt traffic to and from the firewall’s WAN ports. This option is not selected by default.

  - **Always allow SonicWall management traffic**—This check box causes IP traffic from a blacklisted device targeting the firewall’s WAN IP addresses to not be filtered. This allows management traffic and routing protocols to maintain connectivity through a blacklisted device. This option is not selected by default.

## WAN DDOS Protection (Non-TCP Floods)

**WAN DDOS Protection** provides protection against non-TCP DDOS attacks and so should be used in combination with SYN-Flood Protection if TCP SYN-flood attacks are a concern. This feature is not intended to protect a well-known server of non-TCP services on the internet (such as a central DNS server), but is intended to protect LAN
and DMZ networks for which the majority of non-TCP traffic is initiated from the LAN/DMZ side, possibly in combination with limited WAN-initiated traffic.

When **WAN DDOS Protection** is enabled, it tracks the rate of non-TCP packets arriving on WAN interfaces. When the rate of non-TCP packets exceeds the specified threshold, non-TCP packets arriving on WAN interfaces will be filtered. A non-TCP packet will only be forwarded when at least one of the following conditions is true:

- the source IP address is on the Allow list
- the packet is SonicWall management traffic, and **Always allow SonicWall management traffic** is selected
- the packet is VPN Negotiation traffic (IKE) and **Always allow VPN negotiation traffic** is selected
- the packet is an ESP packet and matches the SPI of a tunnel terminating on the network security appliance
- the packet is the \( n \)th packet matching the value specified for **WAN DDOS Filter Bypass Rate (every \( n \) packets)**

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

You can configure the **WAN DDOS Protection (Non-TCP Floods)** settings on the **Firewall Settings > Flood Protection** page.

**To configure the WAN DDOS Protection (Non-TCP Floods) settings:**

1. Navigate to the **Firewall Settings > Flood Protection** page.
2. Scroll down to the **WAN DDOS Protection (Non-TCP Floods)** section.

**Threshold for WAN DDOS protection (Non-TCP Packets / Sec)**

**Threshold for WAN DDOS protection** specifies the maximum number of non-TCP packets allowed per second to be sent to a host, range, or subnet. Exceeding this threshold triggers WAN DDOS flood protection. The default number of non-TCP packets is 1000. The minimum number is 0; the maximum number is 10000000.

**WAN DDOS Filter Bypass Rate (every \( n \) packets)**

When the configured Filter Bypass Rate is non-zero, a non-TCP packet that would normally be dropped by WAN DDOS Protection will instead be passed to the LAN/DMZ network. The bypass rate allows a potential attack to be throttled, but not completely blocked. Allowing some packets to pass through even though their sources are not on the Allow List can provide a mechanism by which legitimate WAN side hosts may get a packet through to the LAN/DMZ side, and a response would populate the Allow List so the following non-TCP packets from the legitimate WAN side host would always be forwarded from that point on.

The default value of the Filter Bypass Rate is zero, so the user must modify this value before the heuristic can be attempted. When the Filter Bypass Rate is non-zero, the value determines what proportion of packets are forwarded regardless of the Allow List contents. For example, if the value was set to two, every other packet would be forwarded to the LAN/DMZ networks (assuming they passed policy, etc). If the value were 100, every 100th packet would be forwarded, and so on. The appropriate value is dependent on the capabilities of the potential LAN side target machines and the nature of the legitimate non-TCP traffic patterns in the customer's network.
WAN DDOS Allow List Timeout

If a non-zero Allow List Timeout is defined by the user, entries in the Allow List will expire in the configured time. If the Allow List Timeout is zero, they never expire. In either case, the least-recently-used entry in a particular hash-bucket may be replaced by a new entry if no unused entry is available in the list.

Enable DDOS protection on WAN interfaces

Selecting Enable DDOS protection on WAN interfaces (it is disabled by default) allows you to set two additional options:

Always allow SonicWall management traffic

When Always allow SonicWall management traffic is enabled (it is disabled by default), traffic needed to manage your SonicWall appliances is allowed to pass through your WAN gateways even when the appliance is under a non-TCP DDOS attack.

Configuring UDP Flood Protection Settings

UDP/UDPv6 Flood Attacks are a type of denial-of-service (DoS) attack. They are initiated by sending a large number of UDP/UDPv6 packets to random ports on a remote host. As a result, the victimized system’s resources are consumed with handling the attacking packets that eventually causes the system to be unreachable by other clients.

SonicWall UDP/UDPv6 Flood Protection defends against these attacks by using a “watch and block” method. The appliance monitors UDP/UDPv6 traffic to a specified destination. If the rate of UDP/UDPv6 packets per second exceeds the allowed threshold for a specified duration of time, the appliance drops subsequent UDP/UDPv6 packets to protect against a flood attack.

UDP/UDPv6 packets that are DNS query or responses to or from a DNS server configured by the appliance are allowed to pass, regardless of the state of UDP/UDPv6 Flood Protection.

The following settings configure UDP/UDPv6 Flood Protection:

- UDP/UDPv6 Flood Attack Threshold (UDP Packets / Sec) – The maximum number of UDP/UDPv6 packets allowed per second to be sent to a host, range, or subnet that triggers UDP/UDPv6 Flood Protection. Exceeding this threshold triggers ICMP Flood Protection. The minimum value is 50, the maximum value is 1000000, and the default value is 1000.
- UDP/UDPv6 Flood Attack Blocking Time (Sec) – After the appliance detects the rate of UDP/UDPv6 packets exceeding the attack threshold for this duration of time, UDP/UDPv6 Flood Protection is activated and the appliance begins dropping subsequent UDP/UDPv6 packets. The minimum time is 1 second, the maximum time is 120 seconds, and the default time is 2 seconds.
- UDP/UDPv6 Flood Attack Protected Destination List – The destination address object or address group that is protected from the UDP/UDPv6 Flood Attack. The default value is Any.

TIP: Select Any to apply the Attack Threshold to the sum of UDP/UDPv6 packets passing through the firewall.
Configuring ICMP Flood Protection Settings

ICMP/ICMPv6 Flood Protection functions identically to UDP Flood Protection, except it monitors for ICMP/ICMPv6 Flood Attacks. The only difference is that there are no DNS queries that are allowed to bypass ICMP/ICMPv6 Flood Protection.

The following settings configure ICMP/ICMPv6 Flood Protection:

- **Enable ICMP Flood Protection** – Enables ICMP/ICMPv6 Flood Protection.
- **ICMP/ICMPv6 Flood Attack Threshold (ICMP Packets / Sec)** – The rate of ICMP/ICMPv6 packets per second sent to a host, range or subnet that triggers ICMP/ICMPv6 Flood Protection.
- **ICMP/ICMPv6 Flood Attack Blocking Time (Sec)** – After the appliance detects the rate of ICMP/ICMPv6 packets exceeding the attack threshold for this duration of time, ICMP/ICMPv6 Flood Protection is activated, and the appliance begins dropping subsequent ICMP/ICMPv6 packets.
- **ICMP/ICMPv6 Flood Attack Protected Destination List** – The destination address object or address group that is protected from the ICMP/ICMPv6 Flood Attack.

**TIP:** Select Any to apply the Attack Threshold to the sum of ICMP/ICMPv6 packets passing through the firewall.
IP multicasting is a method for sending one Internet Protocol (IP) packet simultaneously to multiple hosts. Multicast is suited to the rapidly growing segment of Internet traffic - multimedia presentations and video conferencing. For example, a single host transmitting an audio or video stream and ten hosts that want to receive this stream. In multicasting, the sending host transmits a single IP packet with a specific multicast address, and the 10 hosts simply need to be configured to listen for packets targeted to that address to receive the transmission. Multicasting is a point-to-multipoint IP communication mechanism that operates in a connectionless mode - hosts receive multicast transmissions by “tuning in” to them, a process similar to tuning in to a radio.

The Firewall Settings > Multicast page allows you to manage multicast traffic on the firewall.

Topics:
- Multicast Snooping
- Multicast Policies
- IGMP State Table
- Enabling Multicast on LAN-Dedicated Interfaces
- Enabling Multicast Through a VPN

Multicast Snooping

This section provides configuration tasks for Multicast Snooping.

- **Enable Multicast** - Select this checkbox to support multicast traffic. This checkbox is disabled by default.

- **Require IGMP Membership reports for multicast data forwarding** - Select this checkbox to improve performance by regulating multicast data to be forwarded to only interfaces joined into a multicast group address using IGMP. This checkbox is enabled by default.

- **Multicast state table entry timeout (minutes)** - This field has a default of 5. The value range for this field is 5 to 60 (minutes). Update the default timer value of 5 in the following conditions:
  - You suspect membership queries or reports are being lost on the network.
  - You want to reduce the IGMP traffic on the network and currently have a large number of multicast groups or clients. This is a condition where you do not have a router to route traffic.
  - You want to synchronize the timing with an IGMP router.
Multicast Policies

This section provides configuration tasks for Multicast Policies.

- **Enable reception of all multicast addresses** - This radio button is not enabled by default. Select this radio button to receive all (class D) multicast addresses.
  
  **NOTE:** Receiving all multicast addresses may cause your network to experience performance degradation.

- **Enable reception for the following multicast addresses** - This radio button is enabled by default. In the drop-down menu, select Create a new multicast object or Create new multicast group.
  
  **NOTE:** Only address objects and groups associated with the MULTICAST zone are available to select. Only addresses from 224.0.0.1 to 239.255.255.255 can be bound to the MULTICAST zone.

  **NOTE:** You can specify up to 200 total multicast addresses.

To create a multicast address object:

1. Navigate to the Firewall Settings > Multicast page.
2. Scroll down to the Multicast Snooping section.
3. Select Enable Multicast.
4. Scroll down to the Multicast Policies section.
5. In the Enable reception for the following multicast addresses drop-down menu, select Create new multicast address object. The Add Address Object dialog displays.
6. Configure the name of the address object in the Name field.
7. From the Zone Assignment drop-down menu, select MULTICAST.
8. From the Type drop-down menu, select Host, Range, Network, MAC, or FQDN.
9. Depending on you Type selection, the options on the dialog change. If you selected:
   - Host or Network, the IP Address field displays. Enter the IP address of the host or network. The IP address must be in the range for multicast: 224.0.0.0 to 239.255.255.255.
   - Network, the Netmask field displays. Enter the netmask for the network.
   - Range, the Starting IP Address and Ending IP Address fields display. Enter the starting and ending IP address for the address range. The IP addresses must be in the range for multicast: 224.0.0.1 to 239.255.255.255.
10. Click Update.

IGMP State Table

This section provides descriptions of the fields in the IGMP State Table.

- **Multicast Group Address**—Provides the multicast group address the interface is joined to.
- **Interface / VPN Tunnel**—Provides the interface (such as LAN) for the VPN policy.
- **IGMP Version**—Provides the IGMP version (such as V2 or V3).
- **Time Remaining**—
- **Flush** — Provides an icon to flush that particular entry.
- **Flush** and **Flush All** buttons—To flush a specific entry immediately, check the box to the left of the entry and click **Flush**. Click **Flush All** to immediately flush all entries.

**NOTE:** Receiving all multicast addresses may cause your network to experience performance degradation.

**NOTE:** Only address objects and groups associated with the MULTICAST zone are available to select. Only addresses from 224.0.0.1 to 239.255.255.255 can be bound to the MULTICAST zone.

**NOTE:** You can specify up to 200 total multicast addresses.
Enabling Multicast on LAN-Dedicated Interfaces

Topics:
- Enabling Multicast Support on LAN-dedicated Interfaces
- Enabling Multicast Support for Address Objects Over a VPN Tunnel

Enabling Multicast Support on LAN-dedicated Interfaces

To enable multicast support on the LAN-dedicated interfaces of your firewall:

1. Navigate to the Firewall Settings > Multicast page.
2. Scroll down to the Multicast Snooping section.
3. Select Enable Multicast.
4. Scroll down to the Multicast Policies section.
5. Select Enable the reception of all multicast addresses.
6. Click Update.
7. Navigate to the Network > Interfaces page.
8. Click the Configure button for the LAN interface you want to configure. The Edit Interface dialog displays.
9. Click Advanced.
10. Select Enable Multicast Support.
11. Click Update.

Enabling Multicast Support for Address Objects Over a VPN Tunnel

To enable multicast support for address objects over a VPN tunnel:

1. Navigate to the Firewall Settings > Multicast page.
2. Scroll down to the Multicast Snooping section.
3. Select Enable Multicast.
4. Scroll down to the Multicast Policies section.
5. Select Enable the reception for the following multicast addresses.
6. From the drop-down menu, select Create new multicast address object. The Add Address Object dialog appears.
7. In the Name field, enter a name for your multicast address object.
8. From the Zone Assignment drop-down menu, select a zone: DMZ, LAN, MULTICAST, SSLVPN, VPN, WAN, or WLAN.
When you select a type from the **Type** drop-down menu, the other options change, depending on the selection. If you select:

- **Host**, enter an **IP address** in the **IP Address** field.
- **Range**, enter the starting and ending IP addresses in the **Starting IP Address** and the **Ending IP Address**.
- **Network**, enter the network IP address in the **Netmask** field and a netmask or prefix length in the **Netmask/Prefix Length** field.
- **MAC**, enter the MAC address in the **MAC Address** field and select the **Multi-homed host** checkbox (which is selected by default).
- **FQDN**, enter the FQDN hostname in the **FQDN Hostname** field.

10 Click **Update**.

11 Go to the **VPN > Settings** page.

12 In the **VPN Policies** table, click the **Configure** icon for the Group VPN policy you want to configure. The **VPN Policy** dialog displays.

13 Click **Advanced**.

14 In the **Advanced Settings** section, select **Enable Multicast**.

15 Click **Update**.

### Enabling Multicast Through a VPN

**To enable multicast across the WAN through a VPN:**

1. Enable multicast globally:
   a. Navigate to the **Firewall Settings > Multicast** page.
   b. Check the **Enable Multicast** checkbox.
   c. Click **Update**.
   d. Repeat Step a through Step c for each interface on all participating security appliances.

2. Enable multicast support on each individual interface that will be participating in the multicast network.
   a. Navigate to the **Network > Interfaces** page
   b. Click the **Edit** icon of the participating interface. The **Edit Interface** dialog displays.
   c. Click **Advanced**.
   d. Select the **Enable Multicast Support** checkbox.
   e. Click **Update**.
   f. Repeat Step a through Step e for each participating interface on all participating appliances.

3. Enable multicast on the VPN policies between the security appliances.
   a. Navigate to the **VPN > Base Settings** page.
   b. Click the **Edit** icon of a policy in which include multicasting. The **VPN Policy** dialog displays.
   c. Click **Advanced**.

**NOTE:** The default WLAN’MULTICAST access rule for IGMP traffic is set to DENY. This will need to be changed to ALLOW on all participating appliances to enable multicast if they have multicast clients on their WLAN zones.
d In the Advanced Settings section, select Enable Multicast.

e Click Update.

4 Verify the tunnels are active between the sites.

5 Start the multicast server application and client applications. As multicast data is sent from the multicast server to the multicast group (224.0.0.0 through 239.255.255.255), the firewall queries its IGMP state table for that group to determine where to deliver that data. Similarly, when the appliance receives that data at the VPN zone, the appliance queries its IGMP State Table to determine where it should deliver the data.

The IGMP State Tables (upon updating) should provide information indicating that there is a multicast client on the X3 interface, and across the vpnMcastServer tunnel for the 224.15.16.17 group.

NOTE: By selecting Enable reception of all multicast addresses, you might see entries other than those you are expecting to see when viewing your IGMP State Table. These are caused by other multicast applications that might be running on your hosts.
Managing Quality of Service

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 will ultimately be 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
- Marking
- Conditioning
- 802.1p and DSCP QoS
- Bandwidth Management
- Glossary

Classification

Classification is necessary as a first step so that traffic in need of management can be identified. Management Service 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).

Once identified, or classified, it can be managed. Management can be performed internally by Management Service 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 will work exactly as configured. Once external entities are introduced, the precision and efficacy of BWM configurations can begin to degrade.
But all is not lost. Once Management Service classifies the traffic, it can **tag** the traffic to communicate this classification to certain external systems that are capable of abiding by CoS tags; thus 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 will not be able to recognize 802.1p tags, and could drop tagged traffic.

Although DSCP will not cause compatibility issues, many service providers will 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**

Once 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 will rarely misinterpret or discard 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 will only work 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 (i.e. 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 Management Service, allowing the packets to safely traverse WAN links. When the packets arrive on the other side of the WAN or VPN, the receiving Management Service 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. Management Service provides internal conditioning capabilities with its Egress and Ingress Bandwidth Management (BWM), detailed in the **Bandwidth Management**. Management Service’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 the **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, Management Service 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. Management Service 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

Management Service 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
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. Management Service 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, Management Service 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

Management Service 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 will reset existing 802.1p tags to 0, unless otherwise configured (see Managing QoS Marking for details).

Enabling 802.1p marking will allow the target interface to recognize incoming 802.1p tags generated by 802.1p capable network devices, and will also allow the target interface to generate 802.1p tags, as controlled by Access Rules. Frames that have 802.1p tags inserted by Management Service will bear VLAN ID 0. 802.1p tags will only be inserted according to Access Rules, so enabling 802.1p marking on an interface will 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 will then be able to generate packets with 802.1p tags, as governed by QoS capable applications. By default, general network communications will not have tags inserted so as to maintain compatibility with 802.1p-incapable devices.

**NOTE:** If your network interface does not support 802.1p, it will not be able to process 802.1p tagged traffic, and will ignore 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 will not show the 802.1q header in the packet capture. Conversely, a packet capture performed on an 802.1p-incapable device will almost invariably show the header, but the host will be unable to process the packet.

Before moving on to 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

In the scenario above, 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 will 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.

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 will bear 802.1p tag 6. The Switch will recognize it as voice traffic, and will prioritize 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. Since 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 will simply ignore the tags, or at worst, they will reset the tag value to 0.

### DSCP marking: IP packet

The above diagram 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.

The following table shows the commonly used code points, as well as their mapping to the legacy Precedence and ToS settings.

### DSCP marking: Commonly used code points

<table>
<thead>
<tr>
<th>DSCP</th>
<th>DSCP Description</th>
<th>Legacy IP Precedence</th>
<th>Legacy IP ToS (D, T, R)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Best effort</td>
<td>0 (Routine – 000)</td>
<td>-</td>
</tr>
<tr>
<td>8</td>
<td>Class 1</td>
<td>1 (Priority – 001)</td>
<td>-</td>
</tr>
<tr>
<td>10</td>
<td>Class 1, gold (AF11)</td>
<td>1 (Priority – 001)</td>
<td>T</td>
</tr>
<tr>
<td>12</td>
<td>Class 1, silver (AF12)</td>
<td>1 (Priority – 001)</td>
<td>D</td>
</tr>
<tr>
<td>14</td>
<td>Class 1, bronze (AF13)</td>
<td>1 (Priority – 001)</td>
<td>D, T</td>
</tr>
</tbody>
</table>
**DSCP marking: Commonly used code points**

<table>
<thead>
<tr>
<th>DSCP</th>
<th>DSCP Description</th>
<th>Legacy IP Precedence</th>
<th>Legacy IP ToS (D, T, R)</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>Class 2</td>
<td>2 (Immediate – 010)</td>
<td>-</td>
</tr>
<tr>
<td>18</td>
<td>Class 2, gold (AF21)</td>
<td>2 (Immediate – 010)</td>
<td>T</td>
</tr>
<tr>
<td>20</td>
<td>Class 2, silver (AF22)</td>
<td>2 (Immediate – 010)</td>
<td>D</td>
</tr>
<tr>
<td>22</td>
<td>Class 2, bronze (AF23)</td>
<td>2 (Immediate – 010)</td>
<td>D, T</td>
</tr>
<tr>
<td>24</td>
<td>Class 3</td>
<td>3 (Flash – 011)</td>
<td>-</td>
</tr>
<tr>
<td>26</td>
<td>Class 3, gold (AF31)</td>
<td>3 (Flash – 011)</td>
<td>T</td>
</tr>
<tr>
<td>27</td>
<td>Class 3, silver (AF32)</td>
<td>3 (Flash – 011)</td>
<td>D</td>
</tr>
<tr>
<td>30</td>
<td>Class 3, bronze (AF33)</td>
<td>3 (Flash – 011)</td>
<td>D, T</td>
</tr>
<tr>
<td>32</td>
<td>Class 4</td>
<td>4 (Flash Override – 100)</td>
<td>-</td>
</tr>
<tr>
<td>34</td>
<td>Class 4, gold (AF41)</td>
<td>4 (Flash Override – 100)</td>
<td>T</td>
</tr>
<tr>
<td>36</td>
<td>Class 4, silver (AF42)</td>
<td>4 (Flash Override – 100)</td>
<td>D</td>
</tr>
<tr>
<td>38</td>
<td>Class 4, bronze (AF43)</td>
<td>4 (Flash Override – 100)</td>
<td>D, T</td>
</tr>
<tr>
<td>40</td>
<td>Express forwarding</td>
<td>5 (CRITIC/ECP¹ – 101)</td>
<td>-</td>
</tr>
<tr>
<td>46</td>
<td>Expedited forwarding (EF)</td>
<td>5 (CRITIC/ECP – 101)</td>
<td>D, T</td>
</tr>
<tr>
<td>48</td>
<td>Control</td>
<td>6 (Internet Control – 110)</td>
<td>-</td>
</tr>
<tr>
<td>56</td>
<td>Control</td>
<td>7 (Network Control – 111)</td>
<td>-</td>
</tr>
</tbody>
</table>

1. ECP: Elliptic Curve Group

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 Management Service’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. Management Service provides a replay window of 64 packets, i.e. if an ESP packet for a Security Association (SA) is delayed by more than 64 packets, the packet will be 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 will prioritize 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 will give the error DSCP range already exists or overlaps with another range. First, you will 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:

QoS mapping

NOTE: Mapping will 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 will be employed by an Access Rule’s Map action.

<table>
<thead>
<tr>
<th>802.1p Class Of Service</th>
<th>To DSCP</th>
<th>From DSCP Range</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - Best effort</td>
<td>0 - Best effort/Default</td>
<td>0-7</td>
<td>✔️</td>
</tr>
<tr>
<td>2 - Background</td>
<td>8 - Class 1</td>
<td>8-15</td>
<td>✔️</td>
</tr>
<tr>
<td>3 - Sore</td>
<td>16 - Class 2</td>
<td>16-23</td>
<td>✔️</td>
</tr>
<tr>
<td>2 - Excellent effort</td>
<td>24 - Class 2</td>
<td>24-21</td>
<td>✔️</td>
</tr>
<tr>
<td>4 - Controlled load</td>
<td>32 - Class 4</td>
<td>32-39</td>
<td>✔️</td>
</tr>
<tr>
<td>3 - Video (&lt;100ms latency)</td>
<td>40 - Express forwarding</td>
<td>40-47</td>
<td>✔️</td>
</tr>
<tr>
<td>6 - Voice (&lt;20ms latency)</td>
<td>48 - Control</td>
<td>48-55</td>
<td>✔️</td>
</tr>
<tr>
<td>7 - Network control</td>
<td>56 - Control</td>
<td>56-63</td>
<td>✔️</td>
</tr>
</tbody>
</table>

For example, according to the default table, an 802.1p tag with a value of 2 will be outbound mapped to a DSCP value of 16, while a DSCP tag of 43 will be 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 box.

You can restore the default mappings by clicking the Reset QoS Settings button.
Managing QoS Marking

QoS marking is configured from the QoS view of the Add/Edit Rule dialog of the Firewall > Access Rules page:

Both 802.1p and DSCP marking as managed by Management Service Access 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

<table>
<thead>
<tr>
<th>Action</th>
<th>802.1p (layer 2 CoS)</th>
<th>DSCP (layer 3)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>When packets matching this class of traffic (as defined by the Access Rule) are sent out the egress interface, no 802.1p tag will be added.</td>
<td>The DSCP tag is explicitly set (or reset) to 0.</td>
<td>If the target interface for this class of traffic is a VLAN subinterface, the 802.1p portion of the 802.1q tag will be explicitly set to 0. If this class of traffic is destined for a VLAN and is using 802.1p for prioritization, a specific Access Rule using the Preserve, Explicit, or Map action should be defined for this class of traffic.</td>
</tr>
<tr>
<td>Preserve</td>
<td>Existing 802.1p tag will be preserved.</td>
<td>Existing DSCP tag value will be preserved.</td>
<td></td>
</tr>
<tr>
<td>Explicit</td>
<td>An explicit 802.1p tag value can be assigned (0-7) from a drop-down menu that will be presented.</td>
<td>An explicit DSCP tag value can be assigned (0-63) from a drop-down menu that will be presented.</td>
<td>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.</td>
</tr>
<tr>
<td>Map</td>
<td>The mapping setting defined in the Firewall Settings &gt; QoS Mapping page will be used to map from a DSCP tag to an 802.1p tag</td>
<td>The mapping setting defined in the Firewall Settings &gt; QoS Mapping page will be used to map from an 802.1 tag to a DSCP tag. An additional checkbox will be presented to Allow 802.1p Marking to override DSCP values. Selecting this checkbox will assert 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.</td>
<td>If Map is set as the action on both DSCP and 802.1p, mapping will only occur in one direction: if the packet is from a VLAN and arrives with an 802.1p tag, then DSCP will be mapped from the 802.1p tag; if the packet is destined to a VLAN, then 802.1p will be mapped from the DSCP tag.</td>
</tr>
</tbody>
</table>

For example, refer to Bi-directional DSCP tag action, which provides a 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 will result 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 will 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 Access Rule will tag 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 Access 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 access rule configuration

<table>
<thead>
<tr>
<th>Setting</th>
<th>Access Rule 1</th>
<th>Access Rule 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General View</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Allow</td>
<td>Allow</td>
</tr>
<tr>
<td>From Zone</td>
<td>LAN</td>
<td>VPN</td>
</tr>
<tr>
<td>To Zone</td>
<td>VPN</td>
<td>LAN</td>
</tr>
<tr>
<td>Service</td>
<td>VOIP</td>
<td>VOIP</td>
</tr>
<tr>
<td>Source</td>
<td>Lan Primary Subnet</td>
<td>Main Site Subnets</td>
</tr>
<tr>
<td>Destination</td>
<td>Main Site Subnets</td>
<td>Lan Primary Subnet</td>
</tr>
<tr>
<td>Users Allowed</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Schedule</td>
<td>Always on</td>
<td>Always on</td>
</tr>
<tr>
<td>Enable Logging</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Allow Fragmented Packets</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Qos View
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 will be 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 will be 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 will be 802.1p tagged with CoS = 6 on egress.

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

### Remote site 1: Sample access rule configuration

<table>
<thead>
<tr>
<th>Setting</th>
<th>Access Rule 1</th>
<th>Access Rule 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP Marking Action</td>
<td>Map</td>
<td>Map</td>
</tr>
<tr>
<td>Allow 802.1p Marking to override DSCP values</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>802.1p Marking Action</td>
<td>Map</td>
<td>Map</td>
</tr>
</tbody>
</table>

### Main site: Sample access rule configurations

<table>
<thead>
<tr>
<th>Setting</th>
<th>Access Rule 1</th>
<th>Access Rule 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General View</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Allow</td>
<td>Allow</td>
</tr>
<tr>
<td>From Zone</td>
<td>LAN</td>
<td>VPN</td>
</tr>
<tr>
<td>To Zone</td>
<td>VPN</td>
<td>LAN</td>
</tr>
<tr>
<td>Service</td>
<td>VOIP</td>
<td>VOIP</td>
</tr>
<tr>
<td>Source</td>
<td>Lan Subnets</td>
<td>Remote Site 1 Subnets</td>
</tr>
<tr>
<td>Destination</td>
<td>Remote Site 1 Subnets</td>
<td>Lan Subnets</td>
</tr>
<tr>
<td>Users Allowed</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Schedule</td>
<td>Always on</td>
<td>Always on</td>
</tr>
<tr>
<td>Enable Logging</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Allow Fragmented Packets</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Qos View</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSCP Marking Action</td>
<td>Map</td>
<td>Map</td>
</tr>
</tbody>
</table>
VoIP traffic (as defined by the Service Group) arriving from Remote Site 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 will 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 will also be 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 will be 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 will have 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 will be DSCP tagged according to the conversion map (CoS = 48) on both the inner and outer packet sent back across the VPN.

**Bandwidth Management**

For information on Bandwidth Management (BWM), see Bandwidth management (BWM).

**Glossary**

- **802.1p** – IEEE 802.1p is a Layer 2 (MAC layer) Class of Service mechanism that tags packets by using 3 priority bits (for a total of 8 priority levels) within the additional 16-bits of an 802.1q header. 802.1p processing requires compatible equipment for tag generation, recognition and processing, and should only be employed on compatible networks.

- **Bandwidth Management (BWM)** – Refers to any of a variety of algorithms or methods used to shape traffic or police traffic. Shaping often refers to the management of outbound traffic, while policing often refers to the management of inbound traffic (also known as admission control). There are many different methods of bandwidth management, including various queuing and discarding techniques, each with their own design strengths. SonicWall employs a Token Based Class Based Queuing method for inbound and outbound BWM, as well as a discard mechanism for certain types of inbound traffic.

- **Class of Service (CoS)** – A designator or identifier, such as a layer 2 or layer 3 tag, that is applied to traffic after classification. CoS information will be used by the Quality of Service (QoS) system to differentiate between the classes of traffic on the network, and to provide special handling (for example, prioritized queuing, low latency) as defined by the QoS system administrator.

- **Classification** – The act of identifying (or differentiating) certain types (or classes) of traffic. Within the context of QoS, this is performed for the sake of providing customized handling, typically prioritization or de-prioritization, based on the traffic’s sensitivity to delay, latency, or packet loss. Classification within Management Service uses Access Rules, and can occur based on any or all of the following elements: source zone, destination zone, source address object, destination address object, service object, schedule object.
• **Code Point** – A value that is marked (or tagged) into the DSCP portion of an IP packet by a host or by an intermediate network device. There are currently 64 Code Points available, from 0 to 63, used to define the ascending prioritized class of the tagged traffic.

• **Conditioning** – A broad term used to describe a plurality of methods of providing Quality of Service to network traffic, including but not limited to discarding, queuing, policing, and shaping.

• **DiffServ (Differentiated Services)** – A standard for differentiating between different types or classes of traffic on an IP network for the purpose of providing tailored handling to the traffic based on its requirements. DiffServ primarily depends upon Code Point values marked in the ToS header of an IP packet to differentiate between different classes of traffic. DiffServ service levels are executed on a Per Hop Basis at each router (or other DiffServ enabled network device) through which the marked traffic passes. DiffServ Service levels currently include at a minimum Default, Assured Forwarding, Expedited Forwarding, and DiffServ. Refer to [DSCP Marking](#) for more information.

• **Discarding** – A congestion avoidance mechanism that is employed by QoS systems in an attempt to predict when congestion might occur on a network, and to prevent the congestion by dropping over-limit traffic. Discarding can also be thought of as a queue management algorithm, since it attempts to avoid situations of full queues. Advanced discard mechanisms will abide by CoS markings so as to avoid dropping sensitive traffic. Common methods are:
  - **Tail Drop** – An indiscriminate method of dealing with a full queue wherein the last packets into the queue are dropped, regardless of their CoS marking.
  - **Random Early Detection (RED)** – RED monitors the status of queues to try to anticipate when a queue is about to become full. It then randomly discards packets in a staggered fashion to help minimize the potential of Global Synchronization. Basic implementations of RED, like Tail Drop, do not consider CoS markings.
  - **Weighted Random Early Detection (WRED)** – An implementation of RED that factors DSCP markings into its discard decision process.

• **DSCP (Differentiated Services Code Points)** – The repurposing of the ToS field of an IP header as described by RFC2747. DSCP uses 64 Code Point values to enable DiffServ (Differentiated Services). By marking traffic according to its class, each packet can be treated appropriately at every hop along the network.

• **Global Synchronization** – A potential side effect of discarding, the congestion avoidance method designed to deal with full queues. Global Synchronization occurs when multiple TCP flows through a congested link are dropped at the same time (as can occur in Tail Drop). When the native TCP slow-start mechanism commences with near simultaneity for each of these flows, the flows will again flood the link. This leads to cyclical waves of congestion and under-utilization.

• **Guaranteed Bandwidth** – A declared percentage of the total available bandwidth on an interface which will always be granted to a certain class of traffic. Applicable to both inbound and outbound BWM. The total Guaranteed Bandwidth across all BWM rules cannot exceed 100% of the total available bandwidth. Management Service enhances the Bandwidth Management feature to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic. The Guaranteed Bandwidth can also be set to 0%.

• **Inbound (Ingress or IBWM)** – The ability to shape the rate at which traffic enters a particular interface. For TCP traffic, actual shaping can occur where the rate of the ingress flow can be adjusted by delaying egress acknowledgements (ACKs) causing the sender to slow its rate. For UDP traffic, a discard mechanism is used since UDP has no native feedback controls.

• **IntServ (Integrated Services)** – As defined by RFC1633. An alternative CoS system to DiffServ, IntServ differs fundamentally from DiffServ in that it has each device request (or reserve) its network requirements before it sends its traffic. This requires that each hop on the network be IntServ aware, and it also requires each hop to maintain state information for every flow. IntServ is not supported by Management Service. The most common implementation of IntServ is RSVP.
- **Maximum Bandwidth** – A declared percentage of the total available bandwidth on an interface defining the maximum bandwidth to be allowed to a certain class of traffic. Applicable to both inbound and outbound BWM. Used as a throttling mechanism to specify a bandwidth rate limit. The Bandwidth Management feature is enhanced to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic. The Maximum Bandwidth can be set to 0%, which will prevent all traffic.

- **Outbound (Egress or OBWM)** – Conditioning the rate at which traffic is sent out an interface. Outbound BWM uses a credit (or token) based queuing system with 8 priority rings to service different types of traffic, as classified by Access Rules.

- **Priority** – An additional dimension used in the classification of traffic. Management Service uses 8 priority rings (0 = highest, 7 = lowest) to comprise the queue structure used for BWM. Queues are serviced in the order of their priority ring.

- **Mapping** – With regard to Management Service’s implementation of QoS, mapping is the practice of converting layer 2 CoS tags (802.1p) to layer 3 CoS tags (DSCP) and back again for preserving the 802.1p tags across network links that do not support 802.1p tagging. The map correspondence is fully user-definable, and the act of mapping is controlled by Access Rules.

- **Marking** – Also known as tagging or coloring – The act of applying layer 2 (802.1p) or layer 3 (DSCP) information to a packet for the purpose of differentiation, so that it can be properly classified (recognized) and prioritized by network devices along the path to its destination.

- **MPLS** (Multi Protocol Label Switching) – A term that comes up frequently in the area of QoS, but which is natively unsupported by most customer premise IP networking devices, including SonicWall appliances. MPLS is a carrier-class network service that attempts to enhance the IP network experience by adding the concept connection-oriented paths (Label Switch Paths – LSPs) along the network. When a packet leaves a customer premise network, it is tagged by a Label Edge Router (LER) so that the label can be used to determine the LSP. The MPLS tag itself resides between layer 2 and layer 3, imparting upon MPLS characteristics of both network layers. MPLS is becoming quite popular for VPNs, offering both layer 2 and layer 3 VPN services, but remains interoperable with existing IPsec VPN implementation. MPLS is also very well known for its QoS capabilities, and interoperates well with conventional DSCP marking.

- **Per Hop Behavior (PHB)** – The handling that will be applied to a packet by each DiffServ capable router it traverses, based upon the DSCP classification of the packet. The behavior can be among such actions as discard, re-mark (re-classify), best-effort, assured forwarding, or expedited forwarding.

- **Policing** – A facility of traffic conditioning that attempts to control the rate of traffic into or out of a network link. Policing methods range from indiscriminate packet discarding to algorithmic shaping, to various queuing disciplines.

- **Queuing** – To effectively make use of a link’s available bandwidth, queues are commonly employed to sort and separately manage traffic after it has been classified. Queues are then managed using a variety of methods and algorithms to ensure that the highest priority queues always have room to receive more traffic, and that they can be serviced (de-queued or processed) before lower priority queues. Some common queue disciplines include:
  - **FIFO** (First In First Out) – A very simple, undiscriminating queue where the first packet in is the first packet to be processed.
  - **Class Based Queuing (CBQ)** – A queuing discipline that takes into account the CoS of a packet, ensuring that higher priority traffic is treated preferentially.
  - **Weighted Fair Queuing (WFQ)** – A discipline that attempts to service queues using a simple formula based upon the packets’ IP precedence and the total number of flows. WFQ has a tendency to become imbalanced when there is a disproportionately large number of high-priority flows to be serviced, often having the opposite of the desired effect.
  - **Token Based CBQ** – An enhancement to CBQ that employs a token, or a credit-based system that helps to smooth or normalize link utilization, avoiding burstiness as well as under-utilization. Employed by Management Service BWM.
• **RSVP** (Resource Reservation Protocol) – An IntServ signaling protocol employed by some applications where the anticipated need for network behavior (for example, delay and bandwidth) is requested so that it can be reserved along the network path. Setting up this Reservation Path requires that each hop along the way be RSVP capable, and that each agrees to reserve the requested resources. This system of QoS is comparatively resource intensive, since it requires each hop to maintain state on existing flows. Although IntServ’s RSVP is quite different from DiffServ’s DSCP, the two can interoperate. RSVP is not supported by Management Service.

• **Shaping** – An attempt by a QoS system to modify the rate of traffic flow, usually by employing some feedback mechanism to the sender. The most common example of this is TCP rate manipulation, where acknowledgements (ACKs) sent back to a TCP sender are queued and delayed so as to increase the calculated round-trip time (RTT), leveraging the inherent behavior of TCP to force the sender to slow the rate at which it sends data.

• **Type of Service (ToS)** – A field within the IP header wherein CoS information can be specified. Historically used, albeit somewhat rarely, in conjunction with IP precedence bits to define CoS. The ToS field is now rather commonly used by DiffServ’s code point values.
Configuring SSL Control

This section describes how to plan, design, implement, and maintain the SSL Control feature.

Topics:
- About SSL Control
- SSL Control Configuration
- Enabling SSL Control on Zones
- SSL Control Events

About SSL Control

Management Service includes SSL Control, a system for providing visibility into the handshake of SSL sessions and a method for constructing policies to control the establishment of SSL connections. SSL (Secure Sockets Layer) is the dominant standard for the encryption of TCP-based network communications, with its most common and well-known application being HTTPS (HTTP over SSL); see HTTP over SSL communication. SSL provides digital certificate-based endpoint identification, and cryptographic and digest-based confidentiality to network communications.

HTTP over SSL communication

1. Client browses to http://www.mysonicwall.com
2. DNS resolves target to 64.41.140.173
3. Client Sends TCP SYN to 64.41.140.173 port 443. Server continues TCP setup with SYN/ACK
4. Client Sends ACK
5. Client Sends SSL Client Hello
6. Server Sends Server Hello
7. Server Sends ServerKeyExchange (Certificate)
8. Server Sends Server Hello Done
9. Client Sends ClientKeyExchange
10. Client Sends ChangeCipherSpec
11. Client Sends Encrypted Handshake message (Finished)
12. Server Sends ChangeCipherSpec
13. Server Sends Encrypted Handshake message (Finished)
14. Client Sends GET Request to www.mysonicwall.com (encrypted)
15. Server responds through SSL channel with data (encrypted)
An effect of the security provided by SSL is the obscuration of all payload, including the URL (Uniform Resource Locator, for example, https://www.mysonicwall.com) being requested by a client when establishing an HTTPS session. This is due to the fact that HTTP is transported within the encrypted SSL tunnel when using HTTPS. It is not until the SSL session is established (see HTTP over SSL communication) that the actual target resource (www.mysonicwall.com) is requested by the client, but as the SSL session is already established, no inspection of the session data by the firewall or any other intermediate device is possible. As a result, URL-based content filtering systems cannot consider the request to determine permissibility in any way other than by IP address.

While IP address based filtering does not work well for unencrypted HTTP because of the efficiency and popularity of host-header-based virtual hosting (defined in Key Concepts to SSL Control), IP filtering can work effectively for HTTPS due to the rarity of host-header-based HTTPS sites. But this trust relies on the integrity of the HTTPS server operator, and assumes that SSL is not being used for deceptive purposes.

For the most part, SSL is employed legitimately, being used to secure sensitive communications, such as online shopping or banking, or any session where there is an exchange of personal or valuable information. The ever decreasing cost and complexity of SSL, however, has also spurred the growth of more dubious applications of SSL, designed primarily for the purposes of obfuscation or concealment rather than security.

An increasingly common camouflage is the use of SSL encrypted Web-based proxy servers for the purpose of hiding browsing details, and bypassing content filters. While it is simple to block well known HTTPS proxy services of this sort by their IP address, it is virtually impossible to block the thousands of privately-hosted proxy servers that are readily available through a simple Web-search. The challenge is not the ever-increasing number of such services, but rather their unpredictable nature. Since these services are often hosted on home networks using dynamically addressed DSL and cable modem connections, the targets are constantly moving. Trying to block an unknown SSL target would require blocking all SSL traffic, which is practically infeasible.

SSL Control provides a number of methods to address this challenge by arming the security administrator with the ability to dissect and apply policy based controls to SSL session establishment. While the current implementation does not decode the SSL application data, it does allow for gateway-based identification and disallowance of suspicious SSL traffic.

Topics:
- Key Features of SSL Control
- Key Concepts to SSL Control
- Caveats and Advisories
# Key Features of SSL Control

**SSL control: Features and benefits**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name-based White and Black Lists</td>
<td>You can define lists of explicitly allowed or denied certificate subject common names (described in Key Concepts). Entries are matched on substrings, for example, a blacklist entry for prox will match <a href="http://www.megaproxy.com">www.megaproxy.com</a>, <a href="http://www.proxify.com">www.proxify.com</a> and “roxify.net. This allows you to easily block all SSL exchanges employing certificates issued to subjects with potentially objectionable names. Inversely, you can easily authorize all certificates within an organization by whitelisting a common substring for the organization. Each list can contain up to 1,024 entries. As the evaluation is performed on the subject common name embedded in the certificate, even if the client attempts to conceal access to these sites by using an alternative hostname or even an IP address, the subject is always detected in the certificate, and policy is applied.</td>
</tr>
<tr>
<td>Self-Signed Certificate Control</td>
<td>It is common practice for legitimate sites secured by SSL to use certificates issued by well-known certificate authorities, as this is the foundation of trust within SSL. It is almost equally common for network appliances secured by SSL (such as SonicWall network security appliances) to use self-signed certificates for their default method of security. So while self-signed certificates in closed environments are not suspicious, the use of self-signed certificates by publicly or commercially available sites is. A public site using a self-signed certificate is often an indication that SSL is being used strictly for encryption rather than for trust and identification. While not absolutely incriminating, this sometimes suggests that concealment is the goal, as is commonly the case for SSL encrypted proxy sites. The ability to set a policy to block self-signed certificates allows you to protect against this potential exposure. To prevent discontinuity of communications to known/trusted SSL sites using self-signed certificates, the whitelist feature can be used for explicit allowance.</td>
</tr>
<tr>
<td>Untrusted Certificate Authority Control</td>
<td>Like the use of self-signed certificates, encountering a certificate issued by an untrusted CA is not an absolute indication of disreputable obscuration, but it does suggest questionable trust. SSL Control can compare the issuer of the certificate in SSL exchanges against the certificates in the firewall’s certificate store. The certificate store contains approximately 100 well-known CA certificates, exactly like today’s Web-browsers. If SSL Control encounters a certificate that was issued by a CA not in its certificate store, it can disallow the SSL connection. For organizations running their own private certificate authorities, the private CA certificate can easily be imported into the firewall’s certificate store to recognize the private CA as trusted. The store can hold up to 256 certificates.</td>
</tr>
<tr>
<td>SSL version, Cipher Strength, and Certificate Validity Control</td>
<td>SSL Control provides additional management of SSL sessions based on characteristics of the negotiation, including the ability to disallow the potentially exploitable SSLv2, the ability to disallow weak encryption (ciphers less than 64 bits), and the ability to disallow SSL negotiations where a certificate’s date ranges are invalid. This enables the administrator to create a rigidly secure environment for network users, eliminating exposure to risk through unseen cryptographic weaknesses, or through disregard for or misunderstanding of security warnings.</td>
</tr>
</tbody>
</table>
SSL control: Features and benefits

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone-Based Application</td>
<td>SSL Control is applied at the zone level, allowing you to enforce SSL policy on the network. When SSL Control is enabled on the zone, the firewall looks for Client Hellos sent from clients on that zone through the firewall, which triggers inspection. The firewall looks for the Server Hello and Certificate that is sent in response for evaluation against the configured policy. Enabling SSL Control on the LAN zone, for example, inspects all SSL traffic initiated by clients on the LAN to any destination zone.</td>
</tr>
<tr>
<td>Configurable Actions and Event Notifications</td>
<td>When SSL Control detects a policy violation, it can log the event and block the connection, or it can simply log the event while allowing the connection to proceed.</td>
</tr>
</tbody>
</table>

Key Concepts to SSL Control

• SSL - Secure Sockets Layer (SSL) is a network security mechanism introduced by Netscape in 1995. SSL was designed to provide privacy between two communicating applications (a client and a server) and also to authenticate the server, and optionally the client. SSL’s most popular application is HTTPS, designated by a URL beginning with https:// rather than simply http://, and it is recognized as the standard method of encrypting Web traffic on the Internet. An SSL HTTP transfer typically uses TCP port 443, whereas a regular HTTP transfer uses TCP port 80. Although HTTPS is what SSL is best known for, SSL is not limited to securing HTTP, but can also be used to secure other TCP protocols such as SMTP, POP3, IMAP, and LDAP. SSL session establishment occurs as shown in Establishing an SSL session:

Establishing an SSL session
• **SSLv2** – The earliest version of SSL still in common use. SSLv2 was found to have a number of weaknesses, limitations, and theoretical deficiencies (comparatively noted in the SSLv3 entry), and is looked upon with scorn, disdain, and righteous indignation by security purists.

• **SSLv3** – SSLv3 was designed to maintain backward compatibility with SSLv2, while adding the following enhancements:
  - Alternate key exchange methods, including Diffie-Hellman.
  - Hardware token support for both key exchange and bulk encryption.
  - SHA, DSS, and Fortezza support.
  - Out-of-Band data transfer.
  - TLS – Transport Layer Security, also known as SSLv3.1, is very similar to SSLv3, but improves upon SSLv3 in the ways shown in Differences between SSL and TLS:

**Differences between SSL and TLS**

<table>
<thead>
<tr>
<th>SSL</th>
<th>TLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uses a preliminary HMAC algorithm</td>
<td>Uses HMAC as described in RFC 2104</td>
</tr>
<tr>
<td>Does not apply MAC to version info</td>
<td>Applies MAC to version info</td>
</tr>
<tr>
<td>Does not specify a padding value</td>
<td>Initializes padding to a specific value</td>
</tr>
<tr>
<td>Limited set of alerts and warning</td>
<td>Detailed Alert and Warning messages</td>
</tr>
</tbody>
</table>

**NOTE:** Management Service 6.2.2.1 and above support TLS 1.1 and 1.2.

• **MAC** – A MAC (Message Authentication Code) is calculated by applying an algorithm (such as MD5 or SHA1) to data. The MAC is a message digest, or a one-way hash code that is fairly easy to compute, but which is virtually irreversible. In other words, with the MAC alone, it would be theoretically impossible to determine the message upon which the digest was based. It is equally difficult to find two different messages that would result in the same MAC. If the receiver’s MAC calculation matches the sender’s MAC calculation on a given piece of data, the receiver is assured that the data has not been altered in transit.

• **Client Hello** – The first message sent by the client to the server following TCP session establishment. This message starts the SSL session, and consists of the following components:
  - **Version** – The version of SSL that the client wishes to use in communications. This is usually the most recent version of SSL supported by the client.
  - **Random** – A 32-bit timestamp coupled with a 28-byte random structure.
  - **Session ID** – This can either be empty if no Session ID data exists (essentially requesting a new session) or can reference a previously issued Session ID.
  - **Cipher Suites** – A list of the cryptographic algorithms, in preferential order, supported by the clients.
  - **Compression Methods** – A list of the compression methods supported by the client (typically null).

• **Server Hello** – The SSL server’s response to the Client Hello. It is this portion of the SSL exchange that SSL Control inspects. The Server Hello contains the version of SSL negotiated in the session, along with cipher, session ID and certificate information. The actual X.509 server certificate itself, although a separate step of the SSL exchange, usually begins (and often ends) in the same packet as the Server Hello.
• **Certificates** - X.509 certificates are unalterable digital stamps of approval for electronic security. There are four main characteristics of certificates:
  - Identify the subject of a certificate by a common name or distinguished name (CN or DN).
  - Contain the public key that can be used to encrypt and decrypt messages between parties
  - Provide a digital signature from the trusted organization (Certificate Authority) that issued the certificate.
  - Indicate the valid date range of the certificate

• **Subject** – The guarantee of a certificate identified by a common name (CN). When a client browses to an SSL site, such as https://www.mysonicwall.com, the server sends its certificate which is then evaluated by the client. The client checks that the certificate’s dates are valid, that it was issued by a trusted CA, and that the subject CN matches the requested host name (that is, they are both www.mysonicwall.com). Although a subject CN mismatch elicits a browser alert, it is not always a sure sign of deception. For example, if a client browses to https://mysonicwall.com, which resolves to the same IP address as www.mysonicwall.com, the server presents its certificate bearing the subject CN of www.mysonicwall.com. An alert will be presented to the client, despite the total legitimacy of the connection.

• **Certificate Authority (CA)** - A Certificate Authority (CA) is a trusted entity that has the ability to sign certificates intended, primarily, to validate the identity of the certificate’s subject. Well-known certificate authorities include VeriSign, Thawte, Equifax, and Digital Signature Trust. In general, for a CA to be trusted within the SSL framework, its certificate must be stored within a trusted store, such as that employed by most Web-browsers, operating systems and run-time environments. The Management Service trusted store is accessible from the System > Certificates page. The CA model is built on associative trust, where the client trusts a CA (by having the CA’s certificate in its trusted store), the CA trusts a subject (by having issued the subject a certificate), and therefore the client can trust the subject.

• **Untrusted CA** – An untrusted CA is a CA that is not contained in the trusted store of the client. In the case of SSL Control, an untrusted CA is any CA whose certificate is not present in System > Certificates.

• **Self-Signed Certificates** – Any certificate where the issuer’s common-name and the subject’s common-name are the same, indicating that the certificate was self-signed.

• **Virtual Hosting** – A method employed by Web servers to host more than one website on a single server. A common implementation of virtual hosting is name-based (Host-header) virtual hosting, which allows for a single IP address to host multiple websites. With Host-header virtual hosting, the server determines the requested site by evaluating the “Host:” header sent by the client. For example, both www.website1.com and www.website2.com might resolve to 64.41.140.173. If the client sends a “GET /” along with “Host: www.website1.com”, the server can return content corresponding to that site.

  Host-header virtual hosting is generally not employed in HTTPS because the host header cannot be read until the SSL connection is established, but the SSL connection cannot be established until the server sends its Certificate. Since the server cannot determine which site the client will request (all that is known during the SSL handshake is the IP address) it cannot determine the appropriate certificate to send. While sending any certificate might allow the SSL handshake to commence, a certificate name (subject) mismatch will trigger a browser alert.

• **Weak Ciphers** – Relatively weak symmetric cryptography ciphers. Ciphers are classified as weak when they are less than 64 bits. For the most part, export ciphers are weak ciphers. Common weak ciphers lists common weak ciphers:

  **Common weak ciphers**

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Encryption</th>
<th>Occurs in</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXP1024-DHE-DSS-DES-CBC-SHA</td>
<td>DES(56)</td>
<td>SSLv3, TLS (export)</td>
</tr>
<tr>
<td>EXP1024-DHE-CBC-SHA</td>
<td>DES(56)</td>
<td>SSLv3, TLS (export)</td>
</tr>
</tbody>
</table>
**Caveats and Advisories**

1. **Self-signed and Untrusted CA enforcement** – If enforcing either of these two options, it is strongly advised that you add the common names of any SSL secured network appliances within your organization to the whitelist to ensure that connectivity to these devices is not interrupted. For example, the default subject name of a SonicWall network security appliance is **192.168.168.168**, and the default common name of SonicWall SSL VPN appliances is **192.168.200.1**.

2. If your organization employs its own private Certificate Authority (CA), it is strongly advised that you import your private CA’s certificate into the System > Certificates store, particularly if you will be enforcing blocking of certificates issued by untrusted CAs. Refer to SonicWall SonicOS 6.5 System Setup for more information on this process.

3. SSL Control inspection is currently only performed on TCP port 443 traffic. SSL negotiations occurring on non-standard ports will not be inspected at this time.

4. **Server Hello fragmentation** – In some rare instances, an SSL server fragments the Server Hello. If this occurs, the current implementation of SSL Control does not decode the Server Hello. SSL Control policies are not applied to the SSL session, and the SSL session is allowed.

5. **Session termination handling** – When SSL Control detects a policy violation and terminates an SSL session, it simply terminates the session at the TCP layer. Because the SSL session is in an embryonic state at this point, it is not currently possible to redirect the client or to provide any kind of informational notification of termination to the client.

6. **Whitelist precedence** – The whitelist takes precedence over all other SSL Control elements. Any SSL server certificate which matches an entry in the whitelist will allow the SSL session to proceed, even if other elements of the SSL session are in violation of the configured policy. This is by design.

7. The number of pre-installed (well-known) CA certificates is 93. The resulting repository is very similar to what can be found in most Web-browsers. Other certificate related changes:
   a. The maximum number of CA certificates was raised from 6 to 256.
   b. The maximum size of an individual certificate was raised from 2,048 to 4,096.
   c. The maximum number of entries in the whitelist and blacklist is 1,024 each.
SSL Control Configuration

**NOTE:** Before configuring SSL Control, ensure your firewall supports IPv6. You can confirm this by using the IPv6 Check Network Settings tool on the System > Diagnostics page; see SonicWall SonicOS 6.5 Investigation.

SSL Control is located on the **MANAGE** view, under Security | Firewall Settings > SSL Control. SSL Control has a global setting, as well as a per-zone setting. By default, SSL Control is not enabled at the global or zone level. The individual page controls are as follows (refer Key Concepts to SSL Control for more information on terms used in this section).

Topics:
- General Settings
- Action
- Configuration
- Custom Lists

**General Settings**

The **General Settings** section allows you to enable or disable SSL control:

- **Enable SSL Control** – The global setting for SSL Control. This must be enabled for SSL Control applied to zones to be effective. This option is not selected by default.

**Action**

The **Action** section is where you specify the action to be taken when an SSL policy violation is detected; either:

- **Log the event** – If an SSL policy violation, as defined within the Configuration section below, is detected, the event is logged, but the SSL connection is allowed to continue. This option is not selected by default.
- **Block the connection and log the event** – In the event of a policy violation, the connection is blocked and the event is logged. This option is selected by default.

**Configuration**

The **Configuration** section is where you specify the SSL policies to be enforced:

- **Enable Blacklist** – Controls detection of the entries in the blacklist, as configured in the Custom Lists. This option is selected by default.
- **Enable Whitelist** – Controls detection of the entries in the whitelist, as configured in the Configure Lists section below. Whitelisted entries take precedence over all other SSL control settings. This option is selected by default.
- **Detect Expired Certificates** – Controls detection of certificates whose start date is before the current system time, or whose end date is beyond the current system time. Date validation depends on the firewall’s System Time. Make sure your System Time is set correctly, preferably synchronized with NTP, on the System > Time page. This option is not selected by default.
- **Detect Incomplete Certificates** – Controls detection of certificates that contain incomplete information. This option is not selected by default.
• **Detect Weak Ciphers (<64 bits)** – Controls the detection of SSL sessions negotiated with symmetric ciphers less than 64 bits, commonly indicating export cipher usage. This option is not selected by default.

• **Detect Weak Digest Certificates** – Controls detection of certificates created using MD5 or SHA1. Both MD5 or SHA1 are not considered safe. This option is not selected by default.

• **Detect Self-Signed Certificates** – Controls the detection of certificates where both the issuer and the subject have the same common name. This option is selected by default.

  It is common practice for legitimate sites secured by SSL to use certificates issued by well-known certificate authorities, as this is the foundation of trust within SSL. It is almost equally common for network appliances secured by SSL (such as SonicWall security appliances) to use self-signed certificates for their default method of security. So while self-signed certificates in closed-environments are not suspicious, the use of self-signed certificates by publicly or commercially available sites is. A public site using a self-signed certificate is often an indication that SSL is being used strictly for encryption rather than for trust and identification. While not absolutely incriminating, this sometimes suggests that concealment is the goal, as is commonly the case for SSL encrypted proxy sites. The ability to set a policy to block self-signed certificates allows you to protect against this potential exposure. To prevent discontinuity of communications to known/trusted SSL sites using self-signed certificates, use the whitelist feature for explicit allowance.

• **Detect Certificates signed by an Untrusted CA** – Controls the detection of certificates where the issuer’s certificate is not in the firewall’s System > Certificates trusted store. This option is selected by default.

  Similar to the use of self-signed certificates, encountering a certificate issued by an untrusted CA is not an absolute indication of disreputable obscuration, but it does suggest questionable trust. SSL Control can compare the issuer of the certificate in SSL exchanges against the certificates stored in the SonicWall firewall where most of the well-known CA certificates are included. For organizations running their own private certificate authorities, the private CA certificate can easily be imported into the SonicWall’s whitelist to recognize the private CA as trusted.

• **Detect SSLv2** – Controls detection and blocking of SSLv2 exchanges. SSLv2 is known to be susceptible to cipher downgrade attacks because it does not perform integrity checking on the handshake. Best practices recommend using SSLv3 or TLS in its place. This option is not selected by default.

• **Detect SSLv3** – Controls detection and blocking of SSLv3 exchanges. This option is not selected by default.

• **Detect TLSv1** – Controls the detection and blocking of TLSv1 exchanges. This option is not selected by default.
Custom Lists

The Custom Lists section allows you to configure custom whitelists and blacklists.

- **Configure Blacklist and Whitelist** – Allows you to define strings for matching common names in SSL certificates. Entries are case-insensitive and are used in pattern-matching fashion, as shown in Blacklist and Whitelist: pattern matching:

  **Blacklist and Whitelist: pattern matching**

<table>
<thead>
<tr>
<th>Entry</th>
<th>Will Match</th>
<th>Will Not Match</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="https://mysonicwall.com">https://mysonicwall.com</a>, <a href="https://supersonicwall.computers.org">https://supersonicwall.computers.org</a>,</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="https://67.115.118.87">https://67.115.118.87</a></td>
<td></td>
</tr>
</tbody>
</table>

1. 67.115.118.67 is currently the IP address to which sslvpn.demo.sonicwall.com resolves, and that site uses a certificate issued to sslvpn.demo.sonicwall.com. This will result in a match to "sonicwall.com" since matching occurs based on the common name in the certificate.

2. This is the decimal notation for the IP address 63.208.219.44, whose certificate is issued to www.megaproxy.com.

3. www.freeproxy.ru will not match "prox" since the common name on the certificate that is currently presented by this site is a self-signed certificate issued to "-". This can, however, easily be blocked by enabling control of self-signed or Untrusted CA certificates.

**To configure the Whitelist and Blacklist:**

1. Navigate to the Firewall Settings > SSL Control page.
2. Click the Configure button. The SSL Control Custom Lists dialog displays.
3. To add a certificate to either the Black List or White List table, click Add. The Add Blacklist/Whitelist Domain Entry dialog displays.
4. Enter the certificate’s name in the Certificate Common Name field.

   **NOTE:** List matching is based on the subject common name in the certificate presented in the SSL exchange, not in the URL (resource) requested by the client.

   You can edit and delete certificates with the buttons beneath each list table.
5. Click OK.

   Changes to any of the SSL Control settings do not affect currently established connections; only new SSL exchanges that occur after the change is committed are inspected and affected.
6. Click OK.
7. Click Accept.
Enabling SSL Control on Zones

After SSL Control has been globally enabled, and the desired options have been configured, SSL Control must be enabled on one or more zones. When SSL Control is enabled on the zone, the firewall looks for Client Hellos sent from clients on that zone through the firewall will trigger inspection. The firewall then looks for the Server Hello and Certificate that is sent in response for evaluation against the configured policy. Enabling SSL Control on the LAN zone, for example, will inspect all SSL traffic initiated by clients on the LAN to any destination zone.

**NOTE:** If you are activating SSL Control on a zone (for example, the LAN zone) where there are clients who will be accessing an SSL server on another zone connected to the firewall (for example, the DMZ zone), it is recommended that you add the subject common name of that server’s certificate to the whitelist to ensure continuous trusted access.

**To enable SSL Control on a zone:**

1. Navigate to the **Network > Zones** page.
2. Select the **Configure** icon for the desired zone. The **Edit Zone** dialog displays.
3. Select the **Enable SSL Control** checkbox.
4. Click **OK**. All new SSL connections initiated from that zone are now subject to inspection.

SSL Control Events

Log events include the client’s username in the notes section (not shown) if the user logged in manually or was identified through CIA/Single Sign On. If the user’s identity is not available, the note indicates the user is **Unidentified**.

**SSL control: Event messages**

<table>
<thead>
<tr>
<th>#</th>
<th>Event Message</th>
<th>Conditions When it Occurs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SSL Control: Certificate with Invalid date</td>
<td>The certificate’s start date is either before the SonicWall’s system time or it’s end date is after the system time.</td>
</tr>
<tr>
<td>2</td>
<td>SSL Control: Certificate chain not complete</td>
<td>The certificate has been issued by an intermediate CA with a trusted top-level CA, but the SSL server did not present the intermediate certificate. This log event is informational and does not affect the SSL connection.</td>
</tr>
<tr>
<td>3</td>
<td>SSL Control: Self-signed certificate</td>
<td>The certificate is self-signed (the CN of the issuer and the subject match). <strong>NOTE:</strong> For information about enforcing self-signed certificate controls, see Caveats and Advisories.</td>
</tr>
<tr>
<td>4</td>
<td>SSL Control: Untrusted CA</td>
<td>The certificate has been issued by a CA that is not in the <strong>System &gt; Certificates</strong> store of the firewall. <strong>NOTE:</strong> For information about enforcing self-signed certificate controls, see Caveats and Advisories.</td>
</tr>
<tr>
<td>5</td>
<td>SSL Control: Website found in blacklist</td>
<td>The common name of the subject matched a pattern entered into the blacklist.</td>
</tr>
<tr>
<td>6</td>
<td>SSL Control: Weak cipher being used</td>
<td>The symmetric cipher being negotiated was fewer than 64 bits. For a list of weak ciphers, see Common weak ciphers.</td>
</tr>
<tr>
<td>7</td>
<td>See #2</td>
<td>See #2.</td>
</tr>
</tbody>
</table>
## SSL control: Event messages

<table>
<thead>
<tr>
<th>#</th>
<th>Event Message</th>
<th>Conditions When it Occurs</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>SSL Control: Failed to decode Server Hello</td>
<td>The Server Hello from the SSL server was undecipherable. Also occurs when the certificate and Server Hello are in different packets, as is the case when connecting to a SSL server on a SonicWall appliance. This log event is informational, and does not affect the SSL connection.</td>
</tr>
<tr>
<td>9</td>
<td>SSL Control: Website found in whitelist</td>
<td>The common name of the subject (typically a website) matched a pattern entered into the Whitelist. Whitelist entries are always allowed, even if there are other policy violations in the negotiation, such as SSLv2 or weak ciphers.</td>
</tr>
<tr>
<td>10</td>
<td>SSL Control: HTTPS via SSLv2</td>
<td>The SSL session was being negotiated using SSLv2, which is known to be susceptible to certain man-in-the-middle attacks. Best practices recommend using SSLv3 or TLS instead.</td>
</tr>
</tbody>
</table>
SonicWall Support

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

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

The Support Portal enables you to:

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

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