



SonicOS 7.0

Network Firewall

Administration Guide

SONICWALL®

# Contents

<b>About Firewall</b> .....	<b>4</b>
Firewall Workflow .....	5
<b>Advanced</b> .....	<b>7</b>
Changing Between SonicOS .....	7
Changing From Classic to Policy Mode .....	8
Changing From Policy to Classic Mode .....	9
Detection Prevention .....	10
Dynamic Ports .....	11
Source Routed Packets .....	13
Internal VLAN .....	13
Access Rule Options .....	14
IP and UDP Checksum Enforcement .....	14
Jumbo Frame .....	15
Connections .....	15
Control Plane Flood Protection .....	17
IPv6 Advanced Configuration .....	17
TCP .....	19
TCP Settings .....	20
Layer 3 SYN Flood Protection- SYN Proxy .....	21
Layer 2 SYN/RST/FIN Flood Protection - MAC Blacklisting .....	23
WAN DDOS Protection (Non-TCP Floods) .....	24
TCP Traffic Statistics .....	26
UDP .....	30
UDP Settings .....	30
UDP Flood Protection .....	31
UDP Traffic Statistics .....	32
UDPV6 Traffic Statistics .....	33
ICMP .....	34
ICMP Flood Protection for IPv4 version .....	34
ICMP Traffic Statistics .....	35
ICMP Flood Protection for IPv6 version .....	36
ICMPv6 Traffic Statistics .....	37
<b>Flood Protection</b> .....	<b>39</b>
<b>SSL Control</b> .....	<b>40</b>

Key Features of SSL Control .....	42
Key Concepts to SSL Control .....	43
Caveats and Advisories .....	47
Configuring SSL Control .....	48
General Settings .....	48
Action .....	49
Configuration .....	49
Custom List .....	50
Enabling SSL Control on Zones .....	52
SSL Control Events .....	53
<b>Cipher Control .....</b>	<b>54</b>
TLS Ciphers .....	54
Blocking/Unblocking Ciphers .....	55
Filtering Ciphers .....	56
SSH Ciphers .....	61
<b>Real-Time Black List (RBL) Filter .....</b>	<b>62</b>
Configuring the RBL Filter .....	63
Enabling RBL Blocking .....	63
Adding RBL Services .....	64
Configuring User-Defined SMTP Server Lists .....	64
Testing SMTP IP Addresses .....	66
<b>SonicWall Support .....</b>	<b>67</b>
About This Document .....	68

# About Firewall

The **Firewall** section allows you to perform the following:

- Configure the advanced firewall settings to do the following:
  - Selection of or changing between Classic and Policy modes for NSv series, which provides a unified policy configuration workflow combining Layer 2 to Layer 7 policy enforcement for security policies and optimizing the workflow for other policy types.
  - Configure Detection and prevention in order to prevent threats, and detect them in real time.
  - Configure the dynamic port numbers using the internet's Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP).
  - Configure IP Source Routing allows the sender of a packet to specify which route the packet should take on the way to its destination.
  - Configure the access rule options to control the flow of inbound and outbound Internet traffic from the local network to the public Internet. Both routers and firewalls use access rules to control traffic and verify the source and destination addresses are permitted to send and receive traffic on the local network.
  - Configure the IP and UDP Checksum Enforcement to check a simple error-detection scheme in which each transmitted message that results in a numerical value based on the value of the bytes in a message. and to determine the integrity of the data transmitted over a network respectively.
  - Configure the Control Plane Flood Protection to prevent 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.
  - Configure various IPv6 advanced configurations.
- Manage TCP, UDP and ICMP flood protection and view the traffic statistics through the security appliance.
  - Transmission Control Protocol (TCP) is used for organizing data in a way that ensures the secure transmission between the server and client. It guarantees the integrity of data sent over the network, regardless of the amount. For this reason, it is used to transmit data from other higher-level protocols that require all transmitted data to arrive.
  - User datagram protocol (UDP) operates on top of the Internet Protocol (IP) to transmit datagrams over a network. UDP does not require the source and destination to establish a three-way handshake before transmission takes place. Additionally, there is no need for an end-to-end

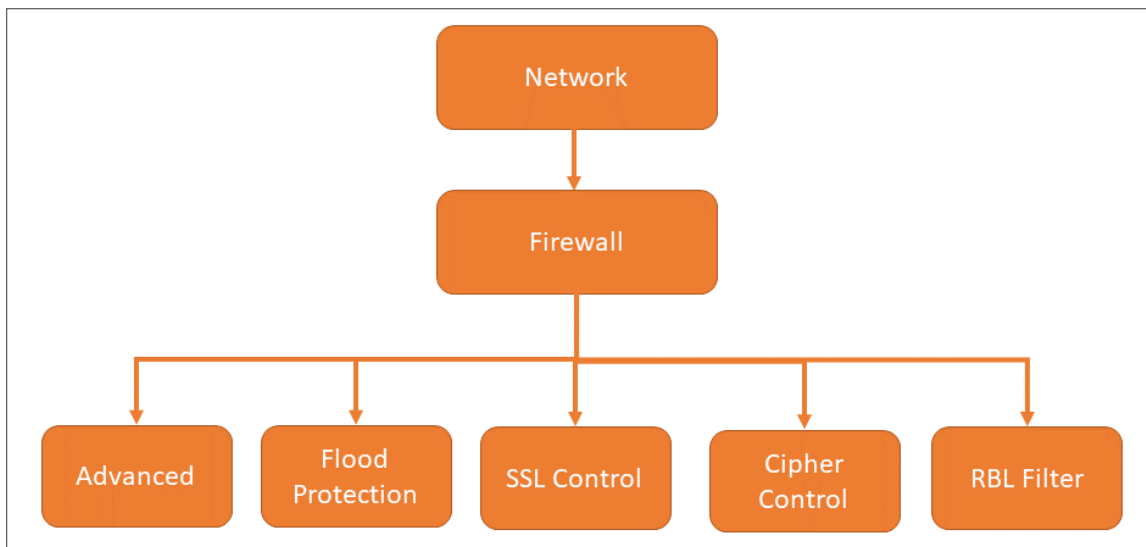
connection.

- Internet Control Message Protocol (ICMP) is used by a device, like a router, to communicate with the source of a data packet about transmission issues. For example, if a datagram is not delivered, ICMP might report this back to the host with details to help discern where the transmission went wrong.
- Configure SSL policies to control the establishment of SSL connections.
  - Configure SSL control system to construct policies and establishment of SSL connections.
- Allow or block the TLS and SSH ciphers in SonicOS.
  - SSL (Secure Sockets Layer) encryption, and its more modern and secure replacement, TLS (Transport Layer Security) encryption, protect data sent over the internet or a computer network. SSL/TLS encrypts communications between a client and server, primarily web browsers and web sites or applications.
- Use RBL filters to block SMTP emails to look up in the database of suspected spammers, and malicious / open mail relays.

### Topics:

- [Firewall Workflow](#)

## Firewall Workflow



## Topics:

- [Advanced](#)
- [Flood Protection](#)
- [SSL Control](#)
- [Cipher Control](#)
- [Real-Time Black List \(RBL\) Filter](#)

# Advanced

This section provides information on how to configure the advanced firewall settings. To configure, navigate to the **Network > Firewall > Advanced** page.

## Topics:

- [Changing Between SonicOS](#)
- [Detection Prevention](#)
- [Dynamic Ports](#)
- [Source Routed Packets](#)
- [Access Rule Options](#)
- [IP and UDP Checksum Enforcement](#)
- [Connections](#)
- [IPv6 Advanced Configuration](#)
- [Control Plane Flood Protection](#)

## Changing Between SonicOS

SonicWall NSv series firewalls support both SonicOS. SonicOS is also known as **Classic** mode, and SonicOS is known as **Policy** mode. Selection of or changing between Classic and Policy modes is supported on NSv series starting in SonicOS 7.0.1 with the following use cases:

- Fresh deployments of SonicOS or SonicOS
- Upgrading an existing deployment from SonicOS 7.0.0 to SonicOS 7.0.1
- Upgrading an existing deployment from SonicOS 6.5.4.v to SonicOS 7.0.1
- Changing an existing deployment from SonicOS 7.0.1 to SonicOS 7.0.1 (from Classic mode to Policy mode)
- Changing an existing deployment from SonicOS 7.0.1 to SonicOS 7.0.1 (from Policy mode to Classic mode)

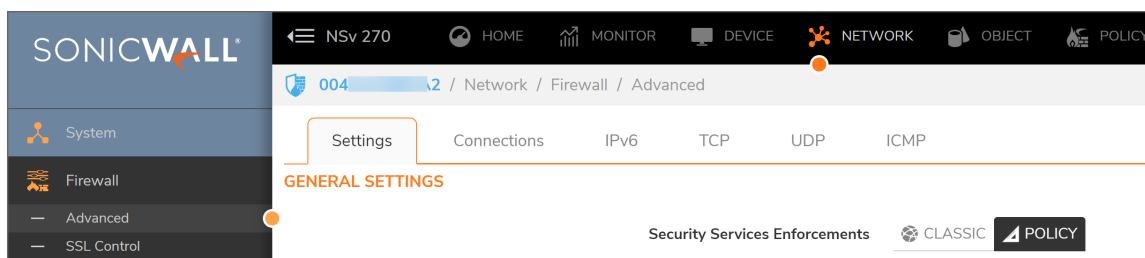
If you have existing NSv deployments running SonicOS 6.5.4.v and plan to continue using NSv on SonicOS 7.0, the ability to change modes provides flexibility to upgrade seamlessly into Classic mode while evaluating or preparing for the move to Policy mode.

Closed-network NSv deployments also support Classic and Policy modes. In a closed network, the lack of internet access prevents the NSv from communicating with the SonicWall License Manager, so the Manual Keyset option is used to apply the security services and other licensing on the firewall. You can select the mode when obtaining the license keyset in MySonicWall. If you switch between modes, you will need to obtain and apply a new license keyset for your NSv.

For more information on the supported modes that can be used on the different SonicOS firewalls see the table in [About SonicOS](#).

The **CLASSIC** and **POLICY** mode switching option is only visible in SonicOS after it is enabled in MySonicWall. Log into your MySonicWall account and enable Firewall Mode Switching for the respective firewall serial number.

The **Settings** screen on the **NETWORK | Firewall > Advanced** page displays the **CLASSIC** and **POLICY** options for **Security Services Enforcements**.



The current mode is indicated by the black button. These buttons are used to initiate the mode change.

For more information, refer to:

- [Changing From Policy to Classic Mode](#)
- [Changing From Classic to Policy Mode](#)

## Changing From Classic to Policy Mode

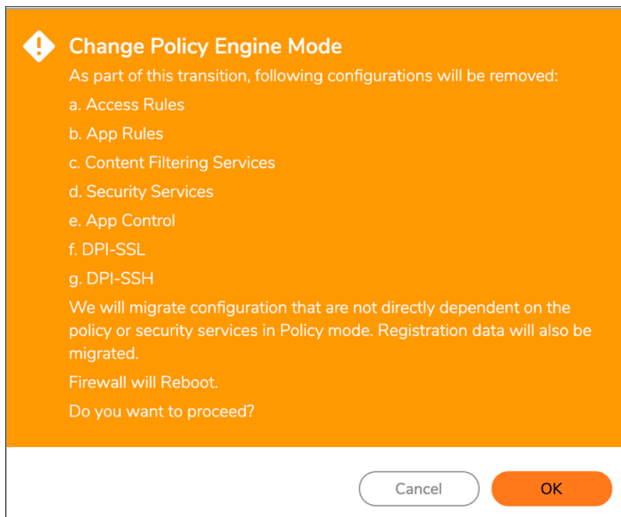
This section describes how to change from Classic mode (SonicOS) to Policy mode (SonicOS) on an existing NSv deployment. After this change, some of the current configuration settings might not be available in Policy mode. The list of configuration settings that will not be available in policy mode is shown in the popup screen when you click the **POLICY** button.

### **To change from Classic mode to Policy mode:**

1. Navigate to the **NETWORK > Firewall > Advanced** page.
2. On the **Settings** screen next to **Security Services Enforcements**, click the **POLICY** button.



3. Read the popup notifications.



4. Click **OK** to proceed with the mode change or click **Cancel** to cancel the mode change.

The NSv reboots and comes up in Policy mode. You must manually reconfigure any settings that were removed during the mode change. These can include configuration settings involving:

- Access Rules
- App Rules
- Content Filtering Service (CFS)
- Security Services
- App Control
- DPI-SSL
- DPI-SSH

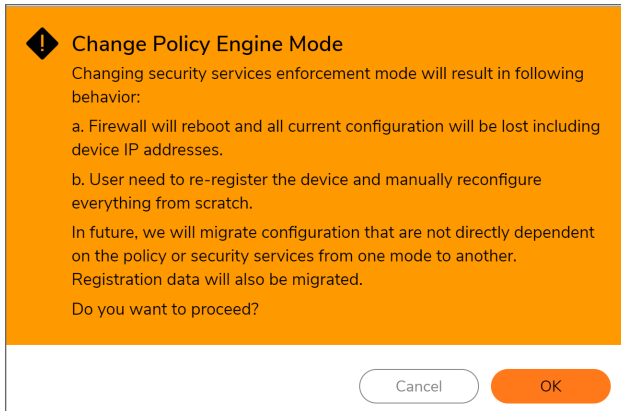
## Changing From Policy to Classic Mode

This section describes how to change from Policy mode (SonicOS) to Classic mode (SonicOS) on an existing NSv deployment. After this change, all of the current configuration settings will be lost and the NSv will reboot with factory default settings. A warning to this effect is shown in the popup screen when you click the **CLASSIC** button.

### ***To change from Policy mode to Classic mode:***

1. Navigate to the **NETWORK > Firewall > Advanced** page.
2. On the **Settings** screen next to **Security Services Enforcements**, click the **CLASSIC** button.

3. Read the popup notifications.



4. Click **OK** to proceed with the mode change or click **Cancel** to cancel the mode change. The NSv reboots and comes up in Classic mode.
5. Log into the NSv using the default credentials, *admin / password*.
6. Configure the network settings to allow your NSv to connect to your local network and to the internet for access to MySonicWall and the SonicWall licensing server. For more information, refer to the *NSv Series 7.0 Getting Started Guide* for your platform (Azure, AWS, VMware, Hyper-V or KVM). The NSv Getting Started guides are available on the SonicWall technical documentation portal at [NSv 7.0 Getting Started Guides](#).
7. Register the NSv to enable full functionality. The **Register Device** button is available on the **HOME | Dashboard > System** pages.

At this point you can manually reconfigure the NSv or import a configuration settings file previously exported from one of the following:

- An NSv running SonicOS 7 (in Classic mode)
- An NSv running SonicOS 6.5.4.v

## Detection Prevention

To enable detection prevention:

1. Navigate to **Network > Firewall > Advanced**.
2. Scroll to **Detection Prevention**.



3. By default, the security appliance responds to incoming connection requests as either blocked or open. To ensure your security appliance does not respond to blocked inbound connection requests, select **Enable**

**Stealth Mode.** Stealth Mode makes your security appliance essentially invisible to hackers. This option is not selected by default.

4. To prevent hackers using various detection tools from detecting the presence of a security appliance, select **Randomize IP ID**. IP packets are given random IP IDs, which makes it more difficult for hackers to “fingerprint” the security appliance. This option is not selected by default.
5. 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. To decrease the TTL value for packets that have been forwarded and, therefore, have already been in the network for some time, select **Decrement IP TTL for forwarded traffic**. This option is not selected by default.

When you select this option, the following option becomes available.

6. The firewall generates Time-Exceeded packets to report when a packet its dropped because its TTL value has decreased to zero. To prevent the firewall from generate these reporting packets, select **Never generate ICMP Time-Exceeded packets**. This option is not selected by default.
7. Click **Accept**.

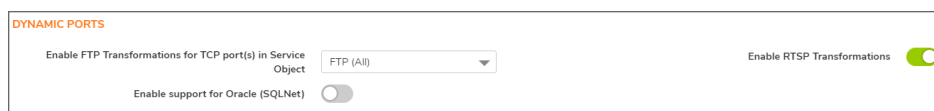
## Dynamic Ports

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.

To configure dynamic ports:

1. Navigate to **Network > Firewall > Advanced**.
2. Scroll to **Dynamic Ports**.



3. From **Enable FTP Transformations for TCP port(s) in Service Object**, select the service group to enable FTP transformations for a particular service object. By default, service group **FTP (All)** is selected.
4. On the **Object > Match Objects > Addresses** page, create an **Address Objects** for the private IP address of the FTP server with the following values:
  - **Name:** FTP Server Private
  - **Zone Assignment:** LAN
  - **Type:** Host

- **IP Address:** 192.168.168.2

- On the **Object > Match Objects > Services** 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

- On the **Policy > Rules and Policies > NAT Policy** page, create a NAT Policy:
- On the **Policy > Rules and Policies > Security Policy** page, create the Access Rule:
- On the **Network > Firewall > Advanced > Dynamic Ports** page, from **Enable FTP Transformations for TCP port(s) in Service Object**, select the **FTP Custom Port Control** Service Object.

- If you have Oracle9i or earlier applications on your network, select **Enable support for Oracle (SQLNet)**. This option is not selected by default.

① | **NOTE:** 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 SonicOS, 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.

6. To support on-demand delivery of real-time data, such as audio and video, select **Enable RTSP Transformations**. RTSP (Real Time Streaming Protocol) is an application-level protocol for control over delivery of data with real-time properties. This option is selected by default.
7. Click **Accept**.

## Source Routed Packets

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.

To configure source-routed packets:

1. Navigate to **Network > Firewall > Advanced**.
2. Scroll to **Source Routed Packets**.
3. Ensure the **Drop Source Routed IP Packets** option is selected. This option is selected by default.  
**TIP:** If you are testing traffic between two specific hosts and you are using source routing, deselect this option.
4. Click **Accept**.



## Internal VLAN

The Internal VLAN section allows you to specify the starting VLAN ID. Every single interface on the firewall is separated by using VLANs internally. By default, it starts at 2. In SonicOS 7, the default vlan id starts at 3968. If you are configuring/using VLAN sub-interfaces on the switch directly connected to the firewall using the same Internal VLAN ID, it might cause unexpected issues. This feature is available only in classic mode.

To change the internal VLAN ID:

1. Navigate to **Network > Firewall > Advanced** page.
2. Scroll to the **Internal VLAN** section.

INTERNAL VLAN

Starting VLAN ID 3968

3. Enter the VLAN ID in the **Starting VLAN ID** field. The default ID is 3968.
4. Click **Accept**.

## Access Rule Options

To configure Access Rule options:

1. Navigate to **Device > Firewall Settings > Advanced**.
2. Scroll to **Access Rule Options**.

ACCESS RULE OPTIONS

Force inbound and outbound FTP data connections to use the default port: 20

Apply firewall rules for intra-LAN traffic to/from the same interface

Always issue RST for discarded outgoing TCP connections

Enable ICMP Redirect on LAN zone

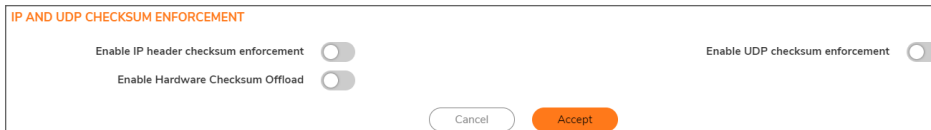
Drop packets which source IP is subnet broadcast address

3. The default configuration allows FTP connections from port 20, but remaps outbound traffic to a port such as 1024. To enforce any FTP data connection through the security appliance must come from port 20 or the connection is dropped, select **Force inbound and outbound FTP data connections to use default port 20**. If the option is selected, the event is then logged as a log event on the security appliance. This option is not selected by default.
4. To apply firewall rules received on a LAN interface and destined for the same LAN interface, select **Apply firewall rules for intra-LAN traffic to/from the same interface**. Typically, this is only necessary when secondary LAN subnets are configured. This option is not selected by default.
5. To send an RST (reset) packet to drop the connection for discarded outgoing TCP connections, select **Always issue RST for discarded outgoing TCP connections**. This option is selected by default.
6. To redirect ICMP packets on LAN zone interfaces, select **Enable ICMP Redirect on LAN zone**. This option is selected by default.
7. To drop packets when the detected IP address is recognized as the one by the subnet, select **Drop packets which source IP is subnet broadcast address**. This option is not selected by default.
8. Click **ACCEPT**.

## IP and UDP Checksum Enforcement

To configure IP and UDP checksum enforcement:

1. Navigate to **Network > Firewall > Advanced**.
2. Scroll to **IP and UDP Checksum Enforcement**.



3. To drop packets with incorrect checksums in the IP header by enforcing IP header checksums, select **Enable IP header checksum enforcement**. This option is not selected by default.
4. To drop packets with incorrect checksums in the UDP header by enforcing UDP header checksums, select **Enable UDP checksum enforcement**. This option is not selected by default.
5. To get data about the hardware checksum offload support, select **Enable Hardware Checksum Offload**.  
① | **NOTE:** This option is available only in SonicOS NSv series firewall platform.
6. Click **ACCEPT**.

## Jumbo Frame

By enabling the Jumbo Frame option you increase throughput and reduces the number of Ethernet frames to be processed. Throughput increase may not be seen in some cases. However, some improvement in throughput if the packets traversing really are jumbo sized.

① | **NOTE:** This option is not available in SonicOS TZ series firewall platform.

To enable Jumbo Frame support:

1. Navigate to **Network > Firewall > Advanced**.



2. Scroll down to the **Jumbo Frame** section.
3. Click the **Enable Jumbo Frame** support switch to green.
4. Click **Accept**.

## Connections

① | **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.

① **TIP:** A hardware platform may differ from another in the amount of memory available, which corresponds to the number of connections.

For specific SPI and DPI connection count maximums, refer to the latest SonicWall datasheet for your firewall platform:

- NSa Series - Datasheet at SonicWall NSa Series
- TZ Series - Datasheet at SonicWall TZ Series
- SuperMassive Series - Datasheet at SonicWall SuperMassive Series

Refer to the SonicWall resources page for more information about our Product Series. Search for high-end, mid-range, entry level, and virtual firewall details, such as Maximum connections (DPI SSL), from the **By Product Series** drop-down menu.

The maximum number of connections depends on the physical capabilities of the particular model of SonicWall security appliance. Flow Reporting does not reduce the connection count on NSa Series, NSA Series, and SuperMassive Series firewalls.

A table with the maximum number of connections for your specific SonicWall security appliance for the various configuration permutations is displayed below the **Connections** group.

#	APPFLOW	EXTERNAL COLLECTOR	MAXIMUM SPI CONNECTIONS	MAXIMUM DPI CONNECTIONS	DPI CONNECTIONS
1	Yes	Yes	2250000	1500000	1500000
2	No	No	3000000	2000000	2000000
3	Yes	No	2250000	1500000 (current)	1500000
4	No	Yes	2400000	1600000	1600000

To configure connection services:

1. Navigate to **Network > Firewall > Advanced**.
2. Scroll to **Connections**.

**CONNECTIONS**

Maximum SPI Connections (DPI services disabled)  
 Maximum DPI Connections (DPI services enabled)  
 DPI Connections (DPI services enabled with additional performance optimizations)

#	APPFLOW	EXTERNAL COLLECTOR	MAXIMUM SPI CONNECTIONS	MAXIMUM DPI CONNECTIONS	DPI CONNECTIONS
1	Yes	Yes	2250000	1500000	1500000
2	No	No	3000000	2000000	2000000
3	Yes	No	2250000	1500000 (current)	1500000
4	No	Yes	2400000	1600000	1600000

3. Choose the type services to be enabled/disabled. 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 recommended setting for most SonicWall network security appliance deployments. This option is selected by default.



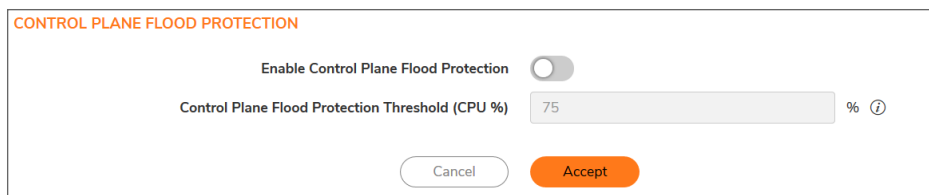
- **DPI Connections (DPI services enabled with additional performance optimization)** - This option is intended for performance critical deployments. This option trades off the number of maximum DPI connections for an increased firewall DPI inspection throughput.

① **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.

## Control Plane Flood Protection

To configure control plane flood protection:

1. Navigate to **Network > Firewall > Advanced > Connections**.
2. Scroll to **Control Plan Flood Protection**.



The screenshot shows a configuration dialog box titled "CONTROL PLANE FLOOD PROTECTION". It contains a toggle switch for "Enable Control Plane Flood Protection" which is currently turned off. Below the toggle is a text input field for "Control Plane Flood Protection Threshold (CPU %)" with the value "75" and a percentage sign and an information icon. At the bottom of the dialog are two buttons: "Cancel" and "Accept".

3. 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 specified threshold, select **Enable Control Plane Flood Protection**, and then specify the threshold in now available **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.

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

4. Click **Accept**.

## IPv6 Advanced Configuration

To configure advanced IPv6:

1. Navigate to **Network > Firewall > Advanced**.
2. Go to **IPv6**.

## IPv6 ADVANCED CONFIGURATIONS

Disable all IPv6 traffic processing on this firewall	<input type="checkbox"/>	<i>i</i>
Drop IPv6 Routing Header type 0 packets	<input checked="" type="checkbox"/>	<i>i</i>
Decrement IPv6 hop limit for forwarded traffic	<input type="checkbox"/>	<i>i</i>
Drop and log network packets whose source or destination address is reserved by RFC	<input type="checkbox"/>	<i>i</i>
Never generate IPv6 ICMP Time-Exceeded packets	<input checked="" type="checkbox"/>	<i>i</i>
Never generate IPv6 ICMP destination unreachable packets	<input checked="" type="checkbox"/>	<i>i</i>
Never generate IPv6 ICMP redirect packets	<input checked="" type="checkbox"/>	<i>i</i>
Never generate IPv6 ICMP parameter problem packets	<input checked="" type="checkbox"/>	<i>i</i>
Allow to use Site-Local-Unicast Address	<input checked="" type="checkbox"/>	<i>i</i>
Enforce IPv6 Extension Header Validation	<input type="checkbox"/>	<i>i</i>
Enforce IPv6 Extension Header Order Check	<input type="checkbox"/>	<i>i</i>
Enable NetBIOS name query response for ISATAP	<input type="checkbox"/>	<i>i</i>

3. To disable IPv6 completely on the firewall, select **Disable all IPv6 traffic processing on this firewall**. When enabled, this option takes precedence over the other IPv6 options in this section. This option is not selected by default.
4. To prevent a potential DoS attack that exploits IPv6 Routing Header type 0 (RH0) packets, select **Drop IPv6 Routing Header type 0 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. This option is selected by default. For more information, see <http://tools.ietf.org/html/rfc5095>
5. To drop a packet when the hop limit has been decremented to 0, select **Decrement IPv6 hop limit for forwarded traffic**; this is similar to IPv4 TTL. This option is not selected by default.
6. 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, select **Drop and log network packets whose source or destination address is reserved by RFC**. This option is not selected by default.
7. 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. To disable this function so the SonicWall appliance does not generate these packets, select **Never generate IPv6 ICMP Time-Exceeded packets**. This option is selected by default.
8. By default, the SonicWall appliance generates IPv6 ICMP destination unreachable packets. To disable this function so the SonicWall appliance does not generate these packets, select **Never generate IPv6 ICMP destination unreachable packets**. This option is selected by default.

9. By default, the SonicWall appliance generates redirect packets. To disable this function so the SonicWall appliance does not generate redirect packets, select **Never generate IPv6 ICMP redirect packets**. This option is selected by default.
10. By default, the SonicWall appliance generates IPv6 ICMP parameter problem packets. To disable this function; so the SonicWall appliance does not generate these packets, select **Never generate IPv6 ICMP parameter problem packets**. This option is selected by default.
11. To allow Site-Local Unicast (SLU) address, the default SonicWall appliance behavior, select **Allow to use Site-Local-Unicast Address**. This option is selected by default.  
As currently defined, SLU addresses are ambiguous and can represent multiple sites. The use of SLU addresses may adversely affect network security through leaks, ambiguity, and potential misrouting. To avoid the issue, deselect the option to prevent the appliance from using SLU addresses.
12. To have the SonicWall appliance check the validity of IPv6 extension headers, select **Enforce IPv6 Extension Header Validation**. This option is not selected by default.  
When this option is selected, the **Enforce IPv6 Extension Header Order Check** option becomes available. (You may need to refresh the page.)
  - To have the SonicWall appliance check the order of IPv6 Extension Headers, select **Enforce IPv6 Extension Header Order Check**. This option is not selected by default.
13. To have the SonicWall appliance generate a NetBIOS name in response to a broadcast ISATAP query, select **Enable NetBIOS name query response for ISATAP**. This option is not selected by default.  
① | **IMPORTANT:** Select this option only when one ISATAP tunnel interface is configured.
14. Click **Accept**.

## TCP

This **TCP** section allows you to manage the TCP (Transmission Control Protocol) traffic settings such as Layer 2/Layer3 flood protection, WAN DDOS protection and view TCP traffic statistics.

① | **NOTE:** In **Classic** mode to configure **TCP Settings** and **TCP Traffic Statistics**, navigate to **Network > Firewall > Flood Protection > TCP** page.

### Topics:

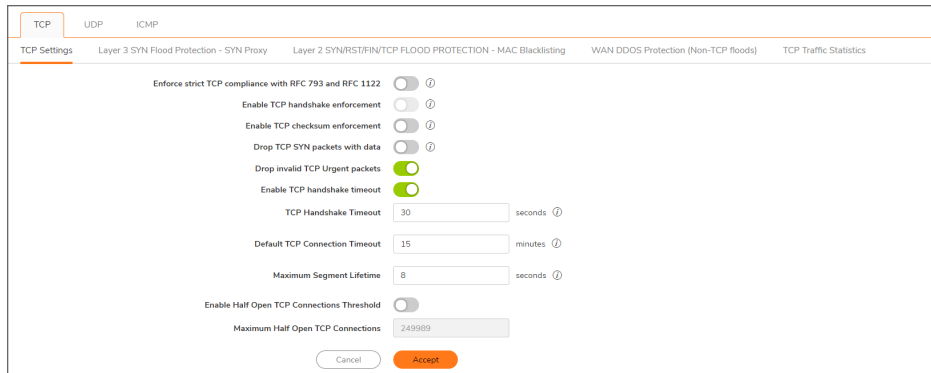
- [TCP Settings](#)
- [TCP Traffic Statistics](#)

The following three tabs are available only in **Policy** mode under **Network > Firewall > Flood Protection**.

- [Layer 3 SYN Flood Protection- SYN Proxy](#)
- [Layer 2 SYN/RST/FIN Flood Protection - MAC Blacklisting](#)
- [WAN DDOS Protection \(Non-TCP Floods\)](#)

# TCP Settings

To configure TCP Settings, navigate to **Network > Firewall > Flood Protection > TCP** page.



- **Enforce strict TCP compliance with RFC 793 and RFC 1122** – This setting ensures strict compliance with several TCP timeout rules. This setting maximizes TCP security, but it might cause problems with the Window Scaling feature for Windows Vista users. This option is not selected by default.
- **Enable TCP handshake enforcement** – This option requires a successful three-way TCP handshake for all TCP connections. It is available only if the **Enforce strict TCP compliance with RFC 793 and RFC 1122**, is selected.
- **Enable TCP checksum enforcement** – If an invalid TCP checksum is calculated, the packet is dropped. This option is not selected by default.
- **Drop TCP SYN packets with data** - This option allows the system to drop TCP SYN packets with data. This option is not selected by default.
- **Drop invalid TCP Urgent packets** - This option allows the system to drop invalid TCP urgent packets. This option is selected by default.
- **Enable TCP handshake timeout** – This selection 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** – This is the maximum time a TCP handshake has to complete the connection. The default is 30 seconds. This option is only available if **Enable TCP Handshake Timeout** is selected.
- **Default TCP Connection Timeout** – This is the 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.

① **NOTE:** Setting an excessively long connection time-out slows the reclamation of stale resources, and in extreme cases, could lead to exhaustion of the connection cache.

- **Maximum Segment Lifetime** – This setting 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** – This option denies new TCP connections if the threshold 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** – This option specifies the maximum number of half-open TCP connections. The default maximum is half the number of maximum connection caches. It is only available if the **Enable Half Open TCP Connections Threshold** is selected.
- Click **Accept**.

## Layer 3 SYN Flood Protection- SYN Proxy

**NOTE:** This tab is available only in **Policy** mode under **Network > Firewall > Flood Protection > TCP > Layer 3 SYN Flood Protection- SYN Proxy**.

A SYN Flood Protection mode is the level of protection that you can select to protect your network against half-opened TCP sessions and high frequency SYN packet transmissions. This feature is enabled and configured on the **Network > Firewall > Flood Protection > TCP > Layer 3 SYN Flood Protection- SYN Proxy** tab.

To configure Layer 3 SYN Flood Protection features:

- In the **SYN Flood Protection Mode** drop-down menu, select a protection mode.
  - **Watch and Report Possible SYN Floods** – The device monitors SYN traffic on all interfaces and logs suspected SYN flood activity that exceeds a packet-count threshold. This option does not actually turn on the SYN Proxy on the device, so the device forwards the TCP three-way handshake without modification.  
This is the least invasive level of SYN Flood protection. Select this option if your network is not in a high-risk environment.  
**IMPORTANT:** When this protection mode is selected, the **SYN-Proxy** options are not available.
  - **Proxy WAN Client Connections When Attack is Suspected** – The device enables the SYN Proxy feature on WAN interfaces when the number of incomplete connection attempts per second exceeds a specified threshold. This method ensures that the device continues to process valid traffic during the attack, and that performance does not degrade. Proxy mode remains enabled

until all WAN SYN flood attacks stop occurring, or until the device blacklists all of them using the SYN Blacklisting feature.

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

- **Always Proxy WAN Client Connections** – This option sets the device to always use SYN Proxy. This method blocks all spoofed SYN packets from passing through the device. This is an extreme security measure, which directs the device to respond to port scans on all TCP ports. The SYN Proxy feature forces the device to respond to all TCP SYN connection attempts, which can degrade performance and generate false positive results. Select this option only if your network is in a high-risk environment.

## SYN Attack Threshold

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.



SYN ATTACK THRESHOLD

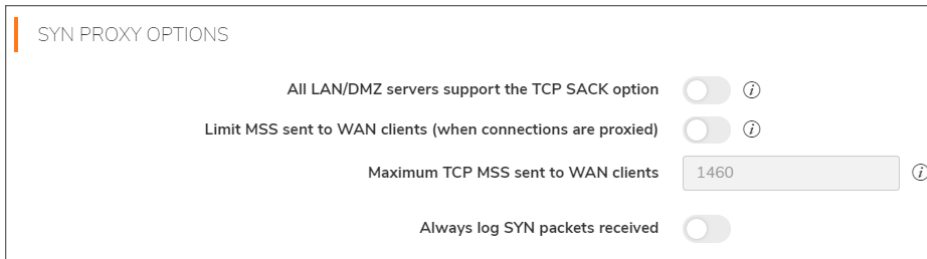
Suggested value calculated from gathered statistics 300

Attack threshold  incomplete connection attempts / second ⓘ

- **Suggested value calculated from gathered statistics** - This is a read-only field provided by the system. After you select the level of protection, the appliance gathers statistics on current WAN TCP connections, keeping track of the maximum, average maximum, and incomplete WAN connections per second. These calculations provide support for a suggested value for the SYN Attack threshold.
- **Attack Threshold** - 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 by the appliance.

## SYN Proxy Options

If one of the higher levels of SYN Protection is selected, SYN-Proxy options can be selected to provide more control over what is sent to WAN clients when in SYN Proxy mode. When the device applies a SYN Proxy to a TCP connection, it responds to the initial SYN packet with a manufactured SYN/ACK reply, waiting for the ACK in response before forwarding the connection request to the server. Devices attacking with SYN Flood packets do not respond to the SYN/ACK reply. The firewall identifies them by their lack of this type of response and blocks their spoofed connection attempts. SYN Proxy forces the firewall to manufacture a SYN/ACK response without knowing how the server responds to the TCP options normally provided on SYN/ACK packets.



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

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

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

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

① **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 continue during an attack.

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

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

① **NOTE:** This tab is available only in **Policy** mode under **Network > Firewall > Flood Protection > TCP > Layer 2 SYN/RST/FIN Flood Protection - MAC Blacklisting**.

The SYN/RST/FIN Blacklisting feature lists devices that exceeded the SYN, RST, and FIN Blacklist attack threshold. The firewall device drops packets sent from blacklisted devices early in the packet evaluation process,

enabling the firewall to handle greater amounts of these packets, providing a defense against attacks originating on local networks while also providing second-tier protection for WAN networks.

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

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

Enable SYN/RST/FIN/TCP flood blacklisting on all interfaces  ⓘ

Never blacklist WAN machines  ⓘ

Always allow SonicWall management traffic  ⓘ

Threshold for SYN/RST/FIN/TCP flood blacklisting  Packets / Sec ⓘ

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

## WAN DDOS Protection (Non-TCP Floods)

① **NOTE:** This tab is available only in **Policy** mode under **Network > Firewall > Flood Protection > TCP > 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.

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



**WAN DDOS PROTECTION (NON-TCP FLOODS)**

Enable DDOS protection on WAN interfaces

Always allow SonicWall management traffic

Always allow VPN negotiation traffic

Threshold for WAN DDOS protection  Non-TCP Packets / Sec ⓘ

WAN DDOS Filter Bypass Rate  every n packets ⓘ

WAN DDOS Allow List Timeout  ⓘ

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

Enabling **WAN DDOS Protection on WAN interfaces** option enables the rest of the options in this section.

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

- Source IP address is on the Allow list
- Packet is SonicWall management traffic, and **Always allow SonicWall management traffic** is selected
- 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 nth packet matching the value specified for **WAN DDOS Filter Bypass Rate (every n packets)**

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

- **Always allow SonicWall management traffic** - This field is available when Enable DDOS protection on WAN interfaces is selected. Select this field so that traffic needed to manage your SonicWall appliances is allowed to pass through your WAN gateways, even when the appliance is under a non-TCP DDOS attack. This option is disabled by default.
- **Always allow VPN negotiation traffic** - This field is available when Enable DDOS protection on WAN interfaces is selected. Select this field so that all VPN negotiation packets are allowed to pass through, even though other traffic is blocked.
- **Threshold for WAN DDOS protection** - The option to set this threshold is available when Enable DDOS protection on WAN interfaces is selected. It specifies the maximum number of non-TCP packets allowed per second to be sent to a host, range, or subnet. Exceeding this threshold triggers WAN DDOS flood protection. The default number of non-TCP packets is 1000. The minimum number is 0, and the maximum number is 10,000,000.

- **WAN DDOS Filter Bypass Rate** - This option can be set when Enable DDOS protection on WAN interfaces is selected. The default value of the WAN DDOS Filter Bypass Rate is 0. This default rate prevents all packets passing through unless the device from which they originate is on the Allow List. This can be an appropriate choice for some deployments.

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

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

- **WAN DDOS Allow List Timeout** - This field is available when Enable DDOS protection on WAN interfaces is selected. If a non-zero Allow List Timeout is defined by the user, entries in the Allow List expire in the configured time. If the Allow List Timeout is zero, they never expire. In either case, the least-recently-used entry in a particular group can be replaced by a new entry, if no unused entry is available in the list.
- Click **Accept**

Using Geo-IP filtering you can block connections coming to or from a geographic location. Refer to the [Using geo-ip filtering](#) article for configuring **Geo-IP** filtering option using SonicOS 7.x.

## TCP Traffic Statistics

You can view the TCP Traffic Statistics on the **Network > Firewall > Flood Protection > TCP > TCP Traffic Statistics** tab.

TCP TRAFFIC STATISTICS			Clear Statistics
Connections Opened	1066	Max Incomplete WAN Connections / sec	4
Connections Closed	1030	Average Incomplete WAN Connections / sec	0
Connections Refused	2	SYN Floods In Progress	0
Connections Aborted	45	RST Floods In Progress	0
Connection Handshake Errors	0	FIN Floods In Progress	0
Connection Handshake Timeouts	3	TCP Floods In Progress	0
Total TCP Packets	252556	Total SYN, RST, FIN or TCP Floods Detected	0
Validated Packets Passed	252437	TCP Connection SYN-Proxy State (WAN only)	OFF
Malformed Packets Dropped	0	Current SYN-Blacklisted Machines	0
Invalid Flag Packets Dropped	112	Current RST-Blacklisted Machines	0
Invalid Sequence Packets Dropped	25	Current FIN-Blacklisted Machines	0
Invalid Acknowledgement Packets Dropped	22	Current TCP-Blacklisted Machines	0
		Total SYN-Blacklisting Events	0
		Total RST-Blacklisting Events	0
		Total FIN-Blacklisting Events	0
		Total TCP-Blacklisting Events	0
		Total SYN Blacklist Packets Rejected	0
		Total RST Blacklist Packets Rejected	0
		Total FIN Blacklist Packets Rejected	0
		Total TCP Blacklist Packets Rejected	0
		Invalid SYN Flood Cookies Received	0
		WAN DDOS Filter State	Disabled
		WAN DDOS Filter - Packets Rejected	0
		WAN DDOS Filter - Packets Leaked	0
		WAN DDOS Filter - Allow List Count	0

### TCP TRAFFIC STATISTICS

This statistic	Is incremented/displays
Connections Opened	When a TCP connection initiator sends a SYN, or a TCP connection responder receives a SYN.

<b>This statistic</b>	<b>Is incremented/displays</b>
<b>Connections Closed</b>	When a TCP connection is closed when both the initiator and the responder have sent a FIN and received an ACK.
<b>Connections Refused</b>	When a RST is encountered, and the responder is in a SYN_RCVD state.
<b>Connections Aborted</b>	When a RST is encountered, and the responder is in some state other than SYN_RCVD.
<b>Connection Handshake Errors</b>	When a handshake error is encountered.
<b>Connection Handshake Timeouts</b>	When a handshake times out.
<b>Total TCP Packets</b>	With every processed TCP packet.
<b>Validated Packets Passed</b>	When: <ul style="list-style-type: none"> <li>• A TCP packet passes checksum validation (while TCP checksum validation is enabled).</li> <li>• A valid SYN packet is encountered (while SYN Flood protection is enabled).</li> <li>• A SYN Cookie is successfully validated on a packet with the ACK flag set (while SYN Flood protection is enabled).</li> </ul>
<b>Malformed Packets Dropped</b>	When: <ul style="list-style-type: none"> <li>• TCP checksum fails validation (while TCP checksum validation is enabled).</li> <li>• The TCP SACK Permitted option is encountered, but the calculated option length is incorrect.</li> <li>• The TCP MSS (Maximum Segment Size) option is encountered, but the calculated option length is incorrect.</li> <li>• The TCP SACK option data is calculated to be either less than the minimum of 6 bytes, or modulo incongruent to the block size of 4 bytes.</li> <li>• The TCP option length is determined to be invalid.</li> <li>• The TCP header length is calculated to be less than the minimum of 20 bytes.</li> <li>• The TCP header length is calculated to be greater than the packet's data length.</li> </ul>

<b>This statistic</b>	<b>Is incremented/displays</b>
<b>Invalid Flag Packets Dropped</b>	<p>When a:</p> <ul style="list-style-type: none"> <li>• Non-SYN packet is received that cannot be located in the connection-cache (while SYN Flood protection is disabled).</li> <li>• Packet with flags other than SYN, RST+ACK ,or SYN+ACK is received during session establishment (while SYN Flood protection is enabled). <ul style="list-style-type: none"> <li>• TCP XMAS Scan is logged if the packet has FIN, URG, and PSH flags set.</li> <li>• TCP FIN Scan is logged if the packet has the FIN flag set.</li> <li>• TCP Null Scan is logged if the packet has no flags set.</li> </ul> </li> <li>• New TCP connection initiation is attempted with something other than just the SYN flag set.</li> <li>• Packet with the SYN flag set is received within an established TCP session.</li> <li>• Packet without the ACK flag set is received within an established TCP session.</li> </ul>
<b>Invalid Sequence Packets Dropped</b>	<p>When a:</p> <ul style="list-style-type: none"> <li>• Packet within an established connection is received where the sequence number is less than the connection's oldest unacknowledged sequence.</li> <li>• Packet within an established connection is received where the sequence number is greater than the connection's oldest unacknowledged sequence + the connection's last advertised window size.</li> </ul>
<b>Invalid Acknowledgement Packets Dropped</b>	When an invalid acknowledgment packet is dropped.
<b>Max Incomplete WAN Connections / sec</b>	<p>When a:</p> <ul style="list-style-type: none"> <li>• Packet is received with the ACK flag set, and with neither the RST or SYN flags set, but the SYN Cookie is determined to be invalid (while SYN Flood protection is enabled).</li> <li>• Packet's ACK value (adjusted by the sequence number randomization offset) is less than the connection's oldest unacknowledged sequence number.</li> <li>• Packet's ACK value (adjusted by the sequence number randomization offset) is greater than the connection's next expected sequence number.</li> </ul>
<b>Average Incomplete WAN Connections / sec</b>	The average number of incomplete WAN connections per second.
<b>SYN Floods In Progress</b>	When a SYN flood is detected.

<b>This statistic</b>	<b>Is incremented/displays</b>
<b>RST Floods In Progress</b>	When a RST flood is detected.
<b>FIN Floods In Progress</b>	When a FIN flood is detected.
<b>TCP Floods In Progress</b>	When a TCP flood is detected.
<b>Total SYN, RST, FIN or TCP Floods Detected</b>	The total number of floods (SYN, RST, FIN, and TCP) detected.
<b>TCP Connection SYN-Proxy State (WAN only)</b>	For WAN only, whether the TCP connection SYN-proxy is enabled.
<b>Current SYN-Blacklisted Machines</b>	When a device is listed on the SYN blacklist.
<b>Current RST-Blacklisted Machines</b>	When a device is listed on the RST blacklist.
<b>Current FIN-Blacklisted Machines</b>	When a device is listed on the FIN blacklist.
<b>Current TCP-Blacklisted Machines</b>	When a device is listed on the TCP blacklist.
<b>Total SYN-Blacklisting Events</b>	When a SYN blacklisting event is detected.
<b>Total RST-Blacklisting Events</b>	When a RST blacklisting event is detected.
<b>Total FIN-Blacklisting Events</b>	When a FIN blacklisting event is detected.
<b>Total TCP-Blacklisting Events</b>	When a TCP blacklisting event is detected.
<b>Total SYN Blacklist Packets Rejected</b>	The total number of SYN packets rejected by SYN blacklisting.
<b>Total RST Blacklist Packets Rejected</b>	The total number of RST packets rejected by SYN blacklisting.
<b>Total FIN Blacklist Packets Rejected</b>	The total number of FIN packets rejected by SYN blacklisting.
<b>Total TCP Blacklist Packets Rejected</b>	The total number of TCP packets rejected by SYN blacklisting.
<b>Invalid SYN Flood Cookies Received</b>	When a SNY flood cookie is received.
<b>WAN DDOS Filter State</b>	Whether the DDOS filter is enabled or disabled.
<b>WAN DDOS Filter – Packets Rejected</b>	When a WAN DDOS Filter rejects a packet.
<b>WAN DDOS Filter – Packets Leaked</b>	When a WAN DDOS Filter rejects a leaked packet.
<b>WAN DDOS Filter – Allow List Count</b>	When a WAN DDOS Filter processes a packet in the Allow List.

To clear and restart the statistics displayed, click **Clear Statistics** icon.

# UDP

① **NOTE:** In **Classic** mode to configure **UDP Settings**, **UDP Traffic Statistics**, **UDPV6 Traffic Statistics** and **UDP Flood Protection**, navigate to **Network > Firewall > Flood Protection > UDP** page.

This **UDP** section allows you to manage the UDP (User Datagram Protocol) flood protection and view UDP traffic statistics.

## Topics:

- [UDP Settings](#)
- [UDP Flood Protection](#)
- [UDP Traffic Statistics](#)
- [UDPV6 Traffic Statistics](#)

## UDP Settings

### UDP Settings for IPv4 version

To configure UDP Settings for IPv4 version, navigate to **Network > Firewall > Flood Protection > UDP > IPv4** tab.

The screenshot shows the configuration page for UDP Settings for IPv4. At the top, there are three tabs: TCP, UDP (which is selected), and ICMP. Below these, there are two sub-tabs: IPv4 (selected) and IPv6. The main content area is titled "UDP SETTINGS" and contains a single configuration item: "Default UDP Connection Timeout" with a text input field containing the value "30" and the unit "seconds" followed by a help icon.

- **Default UDP Connection Timeout** - The number of seconds of idle time you want to allow before UDP connections time out. This value is overridden by the UDP Connection timeout you set for individual rules. The default timeout time is set as 30 seconds.

### UDP Settings for IPv6 version

To configure UDP Settings for IPv6 version, navigate to **Network > Firewall > Flood Protection > UDP > IPv6** tab.

The screenshot shows the configuration page for UDP Settings for IPv6. At the top, there are three tabs: TCP, UDP (which is selected), and ICMP. Below these, there are two sub-tabs: IPv4 and IPv6 (selected). The main content area is titled "UDP SETTINGS" and contains a single configuration item: "Default UDP Connection Timeout" with a text input field containing the value "30" and the unit "seconds" followed by a help icon.

- **Default UDP Connection Timeout** - The number of seconds of idle time you want to allow before UDP connections time out. This value is overridden by the UDP Connection timeout you set for individual rules. The default timeout time is set as 30 seconds.

## UDP Flood Protection

**NOTE:** This section is available only in **Classic** mode. To configure, navigate to **Network > Firewall > Flood Protection > UDP** page.

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

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

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

**UDP FLOOD PROTECTION**

Enable UDP Flood Protection  ⓘ

UDP Flood Attack Threshold  UDP Packets / Sec ⓘ

UDP Flood Attack Blocking Time  seconds ⓘ

UDP Flood Attack Protected Destination List  ⓘ


### To configure UDP Flood Protection:

1. **Enable UDP Flood Protection** – Enables UDP Flood Protection. This option is not selected by default.
  - ⓘ **NOTE:** Enable UDP Flood Protection must be enabled to activate the other UDP Flood Protection options.
2. **UDP Flood Attack Threshold** – The maximum number of UDP packets allowed per second to be sent to a host, range, or subnet that triggers UDP Flood Protection. Exceeding this threshold triggers ICMP Flood Protection. The minimum value is 50, the maximum value is 1000000, and the default value is 1000.
3. **UDP Flood Attack Blocking Time** – After the appliance detects the rate of UDP packets exceeding the attack threshold for this duration of time, UDP Flood Protection is activated and the appliance begins dropping subsequent UDP packets. The minimum time is 1 second, the maximum time is 120 seconds, and the default time is 2 seconds.
4. **UDP Flood Attack Protected Destination List** – The destination address object or address group that will be protected from UDP Flood Attack.
  - ⓘ **TIP:** Select **Any** to apply the Attack Threshold to the sum of UDP packets passing through the

① | firewall.

5. Click **Accept**.

## UDP Traffic Statistics

UDP TRAFFIC STATISTICS		Clear Statistics
Connections Opened	1215	
Connections Closed	1211	
Total UDP Packets	7724	
Validated Packets Passed	7724	
Malformed Packets Dropped	0	
Average UDP Packet Rate (Packets/Sec)	0	
UDP Floods In Progress	0	
Total UDP Floods Detected	0	
Total UDP Flood Packets Rejected	0	


### UDP TRAFFIC STATISTICS

This statistic	Is incremented/displays
<b>Connections Opened</b>	When a connection is opened.
<b>Connections Closed</b>	When a connection is closed.
<b>Total UDP Packets</b>	With every processed UDP packet.
<b>Validated Packets Passed</b>	When a UDP packet passes checksum validation (while UDP checksum validation is enabled).
<b>Malformed Packets Dropped</b>	When: <ul style="list-style-type: none"><li>• UDP checksum fails validation (while UDP checksum validation is enabled).</li><li>• The UDP header length is calculated to be greater than the packet's data length.</li></ul>
<b>Average UDP Packet Rate (Packets/Sec)</b>	The average number of UDP Packet Rate per second.
<b>UDP Floods In Progress</b>	The number of individual forwarding devices currently exceeding the <b>UDP Flood Attack Threshold</b> .
<b>Total UDP Floods Detected</b>	The total number of events in which a forwarding device has exceeded the <b>UDP Flood Attack Threshold</b> .
<b>Total UDP Flood Packets Rejected</b>	The total number of packets dropped because of UDP Flood Attack detection. Clicking on the <b>Statistics</b> icon displays a pop-up dialog showing the most recent rejected packets.

To clear and restart the statistics displayed, click **Clear Statistics** icon.

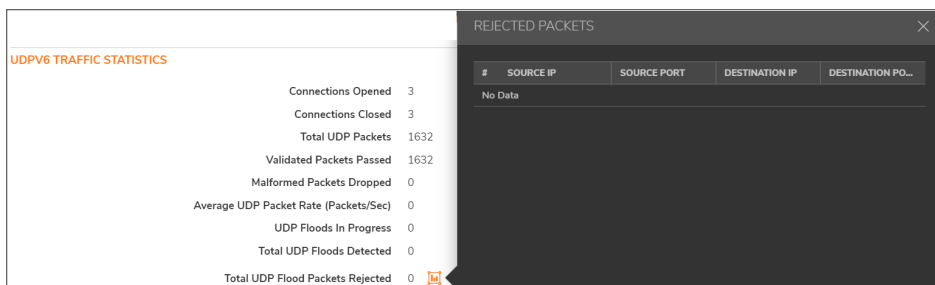


# UDPV6 Traffic Statistics

UDPV6 TRAFFIC STATISTICS		Clear Statistics
Connections Opened	3	
Connections Closed	3	
Total UDP Packets	1630	
Validated Packets Passed	1630	
Malformed Packets Dropped	0	
Average UDP Packet Rate (Packets/Sec)	0	
UDP Floods In Progress	0	
Total UDP Floods Detected	0	
Total UDP Flood Packets Rejected	0	

## UDPV6 TRAFFIC STATISTICS

This statistic	Is incremented/displays
<b>Connections Opened</b>	When a connection is opened.
<b>Connections Closed</b>	When a connection is closed.
<b>Total UDP Packets</b>	With every processed UDP packet.
<b>Validated Packets Passed</b>	When a UDP packet passes checksum validation (while UDP checksum validation is enabled).
<b>Malformed Packets Dropped</b>	When: <ul style="list-style-type: none"> <li>UDP checksum fails validation (while UDP checksum validation is enabled).</li> <li>The UDP header length is calculated to be greater than the packet's data length.</li> </ul>
<b>Average UDP Packet Rate (Packets/Sec)</b>	The average number of UDP Packet Rate per second.
<b>UDP Floods In Progress</b>	The number of individual forwarding devices currently exceeding the UDP Flood Attack Threshold.
<b>Total UDP Floods Detected</b>	The total number of events in which a forwarding device has exceeded the UDP Flood Attack Threshold.
<b>Total UDP Flood Packets Rejected</b>	The total number of packets dropped because of UDP Flood Attack detection. Clicking on the Statistics icon displays a pop-up dialog showing the most recent rejected packets.



The screenshot shows the 'UDPV6 TRAFFIC STATISTICS' table with the following values:

- Connections Opened: 3
- Connections Closed: 3
- Total UDP Packets: 1632
- Validated Packets Passed: 1632
- Malformed Packets Dropped: 0
- Average UDP Packet Rate (Packets/Sec): 0
- UDP Floods In Progress: 0
- Total UDP Floods Detected: 0
- Total UDP Flood Packets Rejected: 0

The 'REJECTED PACKETS' dialog box is open, showing a table with the following headers: #, SOURCE IP, SOURCE PORT, DESTINATION IP, and DESTINATION PORT. The table content is currently empty, displaying 'No Data'.

# ICMP

① **NOTE:** In **Classic** mode to configure **ICMP Flood Protection for IPv4 version**, **ICMP Traffic Statistics**, **ICMPV6 Traffic Statistics** and **ICMP Flood Protection for IPv6 version**, navigate to **Network > Firewall > Flood Protection > ICMP** page.

This **ICMP** section allows you to manage the ICMP (Internet Control Message Protocol) or ICMPv6 flood protection and view ICMP or ICMPv6 traffic.

## Topics:

- [ICMP Flood Protection for IPv4 version](#)
- [ICMP Traffic Statistics](#)
- [ICMP Flood Protection for IPv6 version](#)
- [ICMPv6 Traffic Statistics](#)

## ICMP Flood Protection for IPv4 version

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

To configure ICMP Flood Protection for IPv4 version, navigate to **Network > Firewall > Flood Protection > UDP > ICMP > IPv4** tab.

The screenshot shows the configuration page for ICMP Flood Protection for IPv4. At the top, there are tabs for TCP, UDP, and ICMP, with ICMP selected. Below that, there are tabs for IPv4 and IPv6, with IPv4 selected. The main section is titled "ICMP FLOOD PROTECTION" and contains the following settings:

- Enable ICMP Flood Protection:** A toggle switch is currently turned off.
- ICMP Flood Attack Threshold:** A text input field contains the value "200". To its right, it says "ICMP Packets / Sec" with an information icon.
- ICMP Flood Attack Blocking Time:** A text input field contains the value "2". To its right, it says "seconds" with an information icon.
- ICMP Flood Attack Protected Destination List:** A dropdown menu shows "-- Select an Address Object --" with an information icon.

At the bottom of the configuration area, there are two buttons: "Cancel" and "Accept".

- **Enable ICMP Flood Protection** – Enables ICMP Flood Protection.

① **NOTE:** **Enable ICMP Flood Protection** must be enabled to activate the other ICMP Flood Protection options.

- **ICMP Flood Attack Threshold** – The maximum number of ICMP packets allowed per second to be sent to a host, range, or subnet. Exceeding this threshold triggers ICMP Flood Protection. The minimum number is 10, the maximum number is 100000, and the default number is 200.
- **ICMP Flood Attack Blocking Time** – After the appliance detects the rate of ICMP packets exceeding the attack threshold for this duration of time, ICMP Flood Protection is activated, and the appliance will begin


dropping subsequent ICMP packets. The minimum time is 1 second, the maximum time is 120 seconds, and the default time is 2 seconds.

- **ICMP Flood Attack Protected Destination List** – The destination address object or address group that will be protected from ICMP Flood Attack.

① **TIP:** Select **Any** to apply the Attack Threshold to the sum of ICMP packets passing through the firewall.

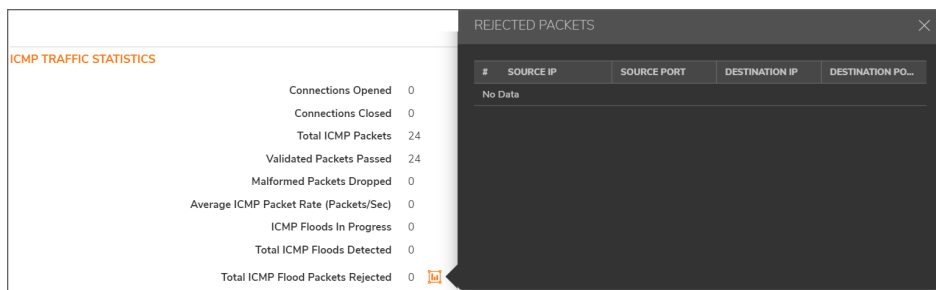
- Click **Accept**.

## ICMP Traffic Statistics

ICMP TRAFFIC STATISTICS		Clear Statistics
Connections Opened	0	
Connections Closed	0	
Total ICMP Packets	24	
Validated Packets Passed	24	
Malformed Packets Dropped	0	
Average ICMP Packet Rate (Packets/Sec)	0	
ICMP Floods In Progress	0	
Total ICMP Floods Detected	0	
Total ICMP Flood Packets Rejected	0	

### ICMP TRAFFIC STATISTICS

This statistic	Is incremented/displays
<b>Connections Opened</b>	When a connection is opened.
<b>Connections Closed</b>	When a connection is closed.
<b>Total ICMP Packets</b>	With every processed ICMPv4 packet.
<b>Validated Packets Passed</b>	When a ICMPv4 packet passes checksum validation (while ICMPv4 checksum validation is enabled).
<b>Malformed Packets Dropped</b>	When: <ul style="list-style-type: none"> <li>• ICMPv4 checksum fails validation (while ICMPv4 checksum validation is enabled).</li> <li>• The ICMPv4 header length is calculated to be greater than the packet's data length.</li> </ul>
<b>Average ICMP Packet Rate (Packets/Sec)</b>	The average number of ICMPv4 Packet Rate per second.
<b>ICMP Floods In Progress</b>	The number of individual forwarding devices currently exceeding the ICMPv4 Flood Attack Threshold.
<b>Total ICMP Floods Detected</b>	The total number of events in which a forwarding device has exceeded the ICMPv4 Flood Attack Threshold.
<b>Total ICMP Flood Packets Rejected</b>	The total number of packets dropped because of ICMPv4 Flood Attack detection. Clicking on the Statistics icon displays a pop-up dialog showing the most recent rejected packets.

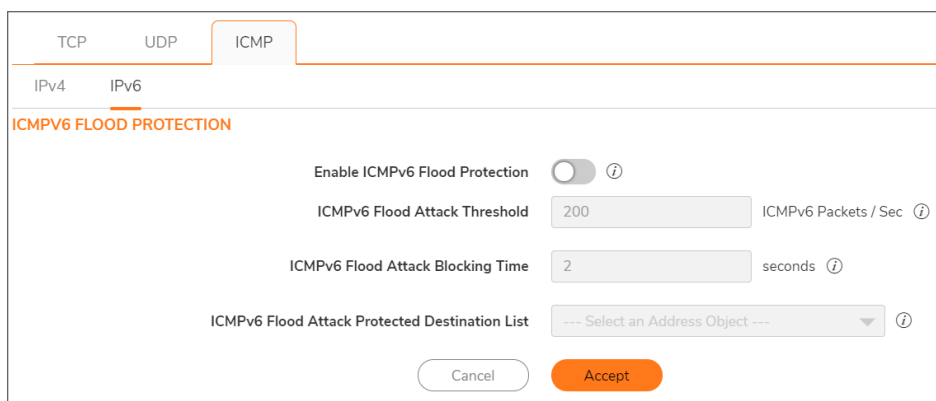


To clear and restart the statistics displayed, click **Clear Statistics** icon.

## ICMP Flood Protection for IPv6 version

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

To configure ICMP Flood Protection for IPv6 version, navigate to **Network > Firewall > Flood Protection > UDP > ICMP > IPv6** tab.



- **Enable ICMPv6 Flood Protection** – Enables ICMPv6 Flood Protection.


ⓘ | **NOTE:** **Enable ICMPv6 Flood Protection** must be enabled to activate the other ICMPv6 Flood Protection options.

- **ICMPv6 Flood Attack Threshold** – The maximum number of ICMPv6 packets allowed per second to be sent to a host, range, or subnet. Exceeding this threshold triggers ICMPv6 Flood Protection. The minimum number is 10, the maximum number is 100000, and the default number is 200.
- **ICMPv6 Flood Attack Blocking Time** – After the appliance detects the rate of ICMPv6 packets exceeding the attack threshold for this duration of time, ICMPv6 Flood Protection is activated, and the appliance will begin dropping subsequent ICMPv6 packets. The minimum time is 1 second, the maximum time is 120 seconds, and the default time is 2 seconds.
- **ICMPv6 Flood Attack Protected Destination List** – The destination address object or address group that will be protected from ICMPv6 Flood Attack.

ⓘ | **TIP:** Select **Any** to apply the Attack Threshold to the sum of ICMPv6 packets passing through the firewall.

- Click **Accept**.

## ICMPv6 Traffic Statistics

ICMPV6 TRAFFIC STATISTICS		Clear Statistics
Connections Opened	1027	
Connections Closed	1027	
Total ICMPv6 Packets	2293	
Validated Packets Passed	2293	
Malformed Packets Dropped	0	
Average ICMP Packet Rate (Packets/Sec)	0	
ICMPv6 Floods In Progress	0	
Total ICMPv6 Floods Detected	0	
Total ICMPv6 Flood Packets Rejected	0	

### ICMP TRAFFIC STATISTICS

This statistic	Is incremented/displays
<b>Connections Opened</b>	When a connection is opened.
<b>Connections Closed</b>	When a connection is closed.
<b>Total ICMPv6 Packets</b>	With every processed ICMPv6 packet.
<b>Validated Packets Passed</b>	When a ICMPv6 packet passes checksum validation (while ICMPv6 checksum validation is enabled).
<b>Malformed Packets Dropped</b>	When: <ul style="list-style-type: none"> <li>• ICMPv6 checksum fails validation (while ICMPv4 checksum validation is enabled).</li> <li>• The ICMPv6 header length is calculated to be greater than the packet's data length.</li> </ul>
<b>Average ICMP Packet Rate (Packets/Sec)</b>	The average number of ICMPv6 Packet Rate per second.
<b>ICMPv6 Floods In Progress</b>	The number of individual forwarding devices currently exceeding the ICMPv6 Flood Attack Threshold.
<b>Total ICMPv6 Floods Detected</b>	The total number of events in which a forwarding device has exceeded the ICMPv6 Flood Attack Threshold.
<b>Total ICMPv6 Flood Packets Rejected</b>	The total number of packets dropped because of ICMPv6 Flood Attack detection. Clicking on the Statistics icon displays a pop-up dialog showing the most recent rejected packets.

The screenshot displays two panels from the SonicOS management interface. On the left, the 'ICMPv6 TRAFFIC STATISTICS' panel shows the following data:

Statistic	Value
Connections Opened	1027
Connections Closed	1027
Total ICMPv6 Packets	2324
Validated Packets Passed	2324
Malformed Packets Dropped	0
Average ICMP Packet Rate (Packets/Sec)	0
ICMPv6 Floods In Progress	0
Total ICMPv6 Floods Detected	0
Total ICMPv6 Flood Packets Rejected	0

On the right, the 'REJECTED PACKETS' window is open, showing a table with the following headers: #, SOURCE IP, SOURCE PORT, DESTINATION IP, and DESTINATION PORT. The table currently contains the text 'No Data'.

To clear and restart the statistics displayed, click **Clear Statistics** icon.

# Flood Protection

This tab is available under **Network > Firewall > Flood Protection** and is available only **Classic** mode of NSsp, NSa and TZ platforms.

The **Flood Protection** section allows you to:

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

SonicWall 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.

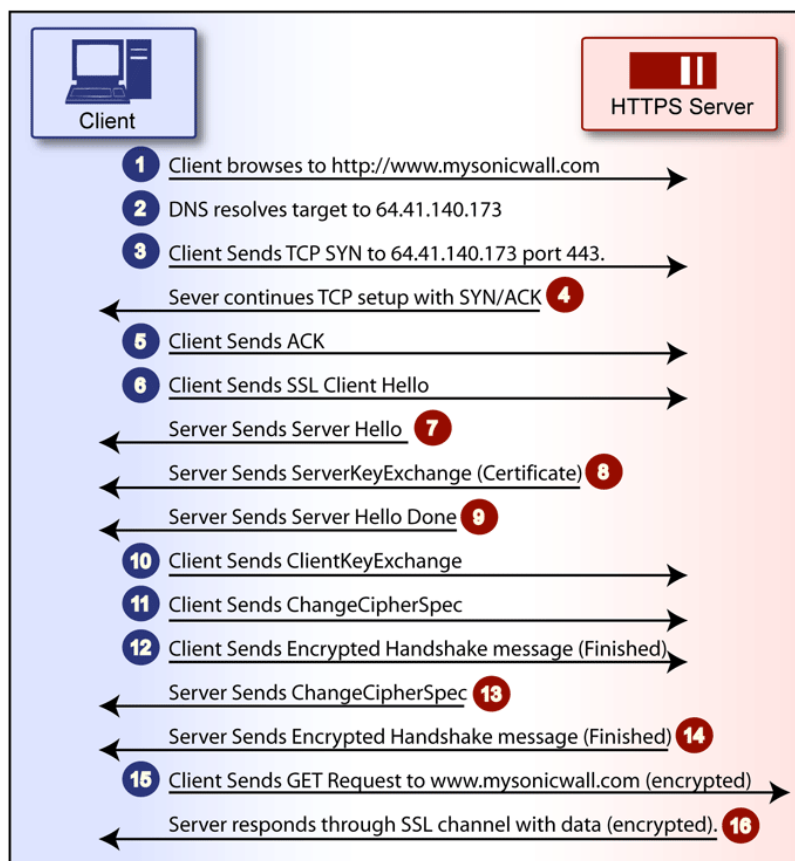
## Topics:

- [TCP](#)
- [UDP](#)
- [ICMP](#)

## SSL Control

SonicOS 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





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 the above image) that the actual target resource ([www.mysonicwall.com](http://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

Feature	Benefit
Common Name-based White and Black Lists	<p>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 <i>prox</i> will match <i>www.megaproxy.com</i>, <i>www.proxify.com</i> and <i>proxify.net</i>. 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.</p> <p>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.</p>
Self-Signed Certificate Control	<p>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.</p> <p>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.</p>
Untrusted Certificate Authority Control	<p>Like the use of self-signed certificates, encountering a certificate issued by an untrusted CA is not an absolute indication of disreputable obscurity, but it does suggest questionable trust.</p> <p>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.</p> <p>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.</p>

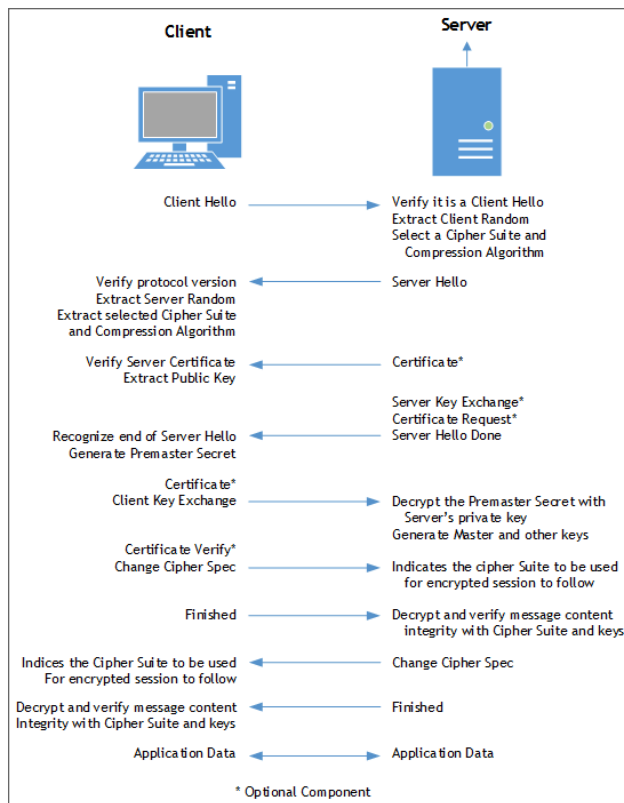
Feature	Benefit
SSL version, Cipher Strength, and Certificate Validity Control	SSL Control provides additional management of SSL sessions based on characteristics of the negotiation, including the ability to disallow the potentially exploitable SSLv2, the ability to disallow weak encryption (ciphers 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.
Zone-Based Application	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.
Configurable Actions and Event Notifications	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.

## Key Concepts to SSL Control

Key concepts to understanding SSL control include

- **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 below.

## 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 below.

### DIFFERENCES BETWEEN SSL AND TLS

SSL	TLS
Uses a preliminary HMAC algorithm	Uses HMAC as described in RFC 2104
Does not apply MAC to version info	Applies MAC to version info
Does not specify a padding value	Initializes padding to a specific value

SSL	TLS
Limited set of alerts and warning	Detailed Alert and Warning messages

① | **NOTE:** SonicOS 7 supports 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 SonicOS trusted store is accessible from the **Device > Settings > Certificates** page. The CA model is built on associative trust, where the client trusts a CA (by having the CAs 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 **Device > Settings > 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. The table below lists common weak ciphers:

#### COMMON WEAK CIPHERS

Cipher	Encryption	Occurs in
EXP1024-DHE-DSS-DES-CBC-SHA	DES(56)	SSLv3, TLS (export)
EXP1024-DHE-CBC-SHA	DES(56)	SSLv3, TLS (export)
EXP1024-RC2-CBC-MD5	RC2(56)	SSLv3, TLS (export)
EDH-RSA-DES-CBC-SHA	DES(56)	SSLv3, TLS
EDH-DSS-DES-CBC-SHA	DES(56)	SSLv3, TLS
DES-CBC-SHA	DES(56)	SSLv2, SSLv3, TLS
EXP1024-DHE-DSS-RC4-SHA	RC4(56)	SSLv3, TLS (export)
EXP1024-RC4-SHA	RC4(56)	SSLv3, TLS (export)

Cipher	Encryption	Occurs in
EXP1024-RC4-MD5	RC4(56)	SSLv3, TLS (export)
EXP-EDH-RSA-DES-CBC-SHA	DES(40)	SSLv3, TLS (export)
EXP-EDH-DSS-DES-CBC-SHA	DES(40)	SSLv3, TLS (export)
EXP-DES-CBC-SHA	DES(40)	SSLv3, TLS (export)
EXP-RC2-CBC-MD5	RC2(40)	SSLv2, SSLv3, TLS (export)
EXP-RC4-MD5	RC4(40)	SSLv2, SSLv3, TLS (export)

## 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 appliances 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 CAs certificate into the **Device > Settings > Certificates** store, particularly if you will be enforcing blocking of certificates issued by untrusted CAs.
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.

# Configuring SSL Control

① **NOTE:** Before configuring SSL Control, ensure your firewall supports IPv6. You can confirm this by using the **IPv6 Advanced Configurations** option under **Network > Firewall > Advanced** page.

SSL Control is located under **Network > Firewall > 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).

The screenshot shows the SSL Control configuration interface. It is divided into three main sections: GENERAL SETTINGS, ACTION, and CONFIGURATION. At the top, there are tabs for 'Settings' and 'Custom List'. In the GENERAL SETTINGS section, there is a toggle for 'Enable SSL Control' which is currently turned off, accompanied by an information icon. The ACTION section contains a radio button selection for 'If an SSL policy violation is detected', with 'Log the event' selected and 'Block the connection and log the event' as an alternative. The CONFIGURATION section lists several detection options, each with a toggle: 'Enable Blacklist' (on), 'Enable Whitelist' (on), 'Detect Weak Ciphers' (off), 'Detect Expired Certificates' (off), 'Detect Weak Digest Certificates' (off), 'Detect Self-Signed Certificates' (on), 'Detect Certificate signed by an Untrusted CA' (on), 'Detect SSLv2' (on), 'Detect SSLv3' (off), and 'Detect TLSv1' (off). At the bottom of the configuration section are 'Cancel' and 'Accept' buttons.

## 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.

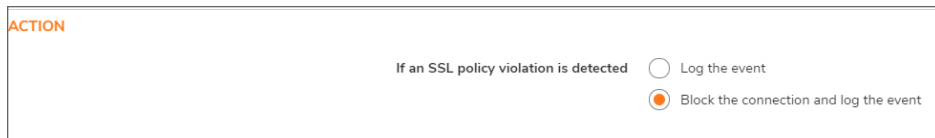
This screenshot shows the 'GENERAL SETTINGS' section of the SSL Control configuration page. It features a single toggle switch for 'Enable SSL Control', which is currently turned off. An information icon is located to the right of the toggle.



# Action

The **Action** section is where you choose 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.



ACTION

If an SSL policy violation is detected

Log the event

Block the connection and log the event

# 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 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 Weak Ciphers** – 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 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 **Device > Settings > Time** page. 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.

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 Self-signed Certificates** – Controls the detection of certificates where the issuer's certificate is not in the firewall's **Device > Settings > Certificates** trusted store. This option is selected by default.

- **Detect Certificates signed by an Untrusted CA** – Controls the detection of certificates where the issuer’s certificate is not in the firewall’s **Device > Settings > 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 obscurity, 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 selected by default. It is also dimmed and cannot be changed.
- **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 List

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:

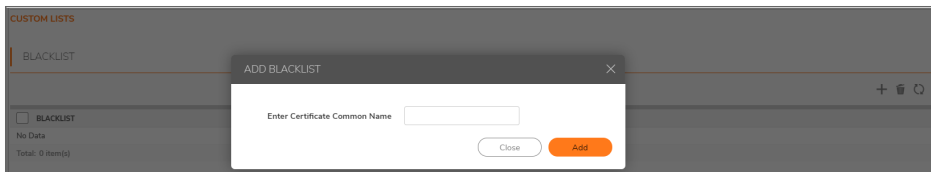
## BLACKLIST AND WHITELIST: PATTERN MATCHING

Entry	Will Match	Will Not Match
sonicwall.com	https://www.sonicwall.com, https://csm.demo.sonicwall.com, https://mysonicwall.com, https://supersonicwall.computers.org, https://67.115.118.87	https://www.sonicwall.de
prox	https://proxify.org, https://www.proxify.org, https://megaproxy.com, https://1070652204	https://www.freeproxy.ru

- 67.115.118.87 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 results in a match to “sonicwall.com” as matching occurs based on the common name in the certificate.
- This is the decimal notation for the IP address 63.208.219.44, whose certificate is issued to *www.megaproxy.com*.
- *www.freeproxy.ru* will not match “prox” as 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 Blacklist:

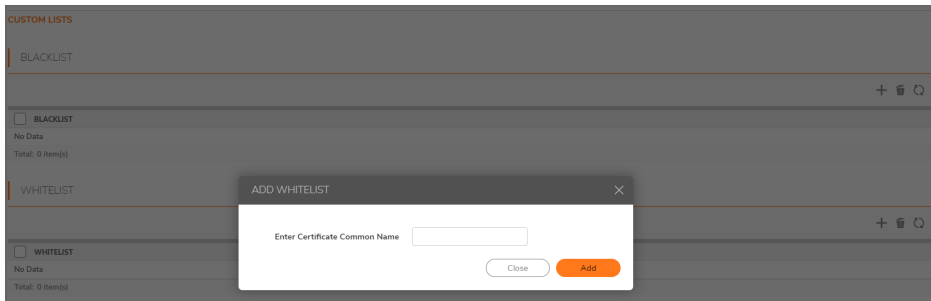
1. Navigate to **Network > Firewall > SSL Control > Custom List > Blacklist**.
2. Click + icon. The **Add Blacklist** dialog displays.



3. Enter the certificate’s name in the **Certificate Common Name** field.  
**TIP:** 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.
4. Click **Add**.  
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.

### To configure the Whitelist:

1. Navigate to **Network > Firewall > SSL Control > Custom List > Whitelist**.
2. Click + icon. The **Add Whitelist** dialog displays.



3. Enter the certificate's name in the **Certificate Common Name** field.
  - ① **TIP:** 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.
4. Click **Add**.

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.

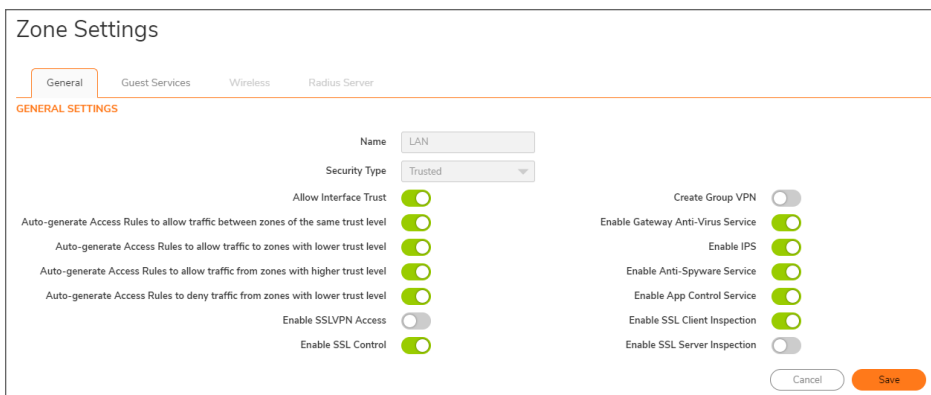
## Enabling SSL Control on Zones

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.

- ① **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 **Object > Match Objects > Zones** page.
2. Click **Edit** icon for the desired zone. The **Zone Settings > General** dialog displays.



3. Select the **Enable SSL Control** option.
4. Click **Save**. 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

#	Event Message	Conditions When it Occurs
1	SSL Control: Certificate with Invalid date	The certificate's start date is either before the SonicWall's system time or it's end date is after the system time.
2	SSL Control: Certificate chain not complete	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.
3	SSL Control: Self-signed certificate	The certificate is self-signed (the CN of the issuer and the subject match).  For information about enforcing self-signed certificate controls, see <a href="#">SSL Control Events</a> .
4	SSL Control: Untrusted CA	The certificate has been issued by a CA that is not in the <b>Device &gt; Settings &gt; Certificates</b> store of the firewall.  For information about enforcing self-signed certificate controls, see <a href="#">SSL Control Events</a> .
5	SSL Control: Website found in blacklist	The common name of the subject matched a pattern entered into the blacklist.
6	SSL Control: Weak cipher being used	The symmetric cipher being negotiated was fewer than 64 bits. For a list of weak ciphers, see <a href="#">SSL Control Events</a> .
7	SSL Control: Failed to decode Server Hello	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.
8	SSL Control: Website found in whitelist	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.
9	SSL Control: HTTPS via SSLv2	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.

# Cipher Control

You can allow or block any or all TLS and SSH ciphers in SonicOS. This functionality applies to:

- DPI-SSL (TLS traffic inspected by the firewall)
- https MGMT (TLS sessions accessing the firewall)
- SSL Control (inspect TLS traffic passing through the firewall: non DPI-SSL)

Any change to the TLS ciphers apply to all TLS traffic.

The list of ciphers displayed in the **Network > Firewall > Cipher Control** page are a list of known TLS ciphers. The list of ciphers is a super set of supported ciphers. While this list contains all known ciphers, DPI-SSL and HTTPS MGMT support a much smaller list of ciphers. For example, DPI-SSL and HTTPS MGMT do not yet support TLS 1.3 ciphers or support some weak ciphers that are listed in **Network > Firewall > Cipher Control**.

The ciphers are ordered based on the security strengths, with ciphers on top more secure than the ones below. Both DPI-SSL and HTTPS MGMT implementations use the relative ordering of their supported ciphers based on **Network > Firewall > Cipher Control**; that is, for the DPI-SSL supported ciphers, DPI-SSL orders them based on the ciphers listed in **Network > Firewall > Cipher Control**. The same is true for HTTPS MGMT ciphers.

## TLS Ciphers

TLS Ciphers		SSH Ciphers										
Q Enter Search Text		Action: All	Strength: All	CBC: All	TLS1.0	TLS1.1	TLS1.2	TLS1.3	Block	Unblock	Refresh	Column Configurati
<input type="checkbox"/>	CIPHER NAME	STRENGTH	BLOCKED	IS CBC	TLS1.0	TLS1.1	TLS1.2	TLS1.3	DPI-SSL	HTTPS M		
<input type="checkbox"/>	TLS_AES_128_GCM_SHA256	Recommended										
<input type="checkbox"/>	TLS_AES_256_GCM_SHA384	Recommended										
<input type="checkbox"/>	TLS_CHACHA20_POLY1305_SHA256	Recommended										
<input type="checkbox"/>	TLS_AES_128_CCM_SHA256	Recommended										
<input type="checkbox"/>	TLS_AES_128_CCM_8_SHA256	Recommended										
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Recommended										
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Recommended										
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	Recommended										
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Recommended										
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Recommended										
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Recommended										
<input type="checkbox"/>	TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256	Recommended										
<input type="checkbox"/>	TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384	Recommended										
<input type="checkbox"/>	TLS_ECDHE_PSK_WITH_AES_128_CCM_8_SHA256	Recommended										
<input type="checkbox"/>	TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256	Recommended										
<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Recommended										
<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Recommended										
<input type="checkbox"/>	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	Recommended										
<input type="checkbox"/>	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	Recommended										
<input type="checkbox"/>	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256	Recommended										

<b>Cipher Name</b>	Name of the Cipher
<b>Strength</b>	Strength of the cipher: <ul style="list-style-type: none"> <li>• <b>Recommended</b></li> <li>• <b>Secure</b></li> <li>• <b>Weak</b></li> <li>• <b>Insecure</b></li> </ul>
<b>Blocked</b>	Indicates, with a <b>Blocked</b> icon, whether the cipher has been blocked from being used
<b>Is CBC</b>	Indicates, with an <b>Enabled</b> icon, whether the cipher uses CBC (Cipher-Block Chaining) mode
<b>TLS1.0</b> <b>TLS1.1</b> <b>TLS1.2</b> <b>TLS1.3</b>	Indicates, with an <b>Enabled</b> icon, whether the cipher is used in the TLS (Transport Layer Security) protocol version
<b>DPI-SSL</b>	Indicates the protocols that support the ciphers.
<b>HTTPS management</b>	
<b>SSL control</b>	

#### Topics:

- [Blocking/Unblocking Ciphers](#)
- [Filtering Ciphers](#)

## Blocking/Unblocking Ciphers

### *To block ciphers:*

1. Navigate to **Network > Firewall > Cipher Control**.
2. Click **TLS Ciphers**.
3. Either:
  - Select the cipher(s) to block.
  - Click the checkbox in the table header.
4. Click **Block**. A confirmation dialog is displayed to block the selected ciphers.
5. Click **OK**.  
A **Blocked** icon displays in the Blocked column for each blocked cipher(s).

### *To unblock ciphers:*

1. Navigate to **Network > Firewall > Cipher Control**.
2. Click **TLS Ciphers**.
3. Either:

- Select the cipher(s) to unblock.
  - Click the checkbox in the table header.
4. Click **UnBlock**. A confirmation dialog is displayed to unblock the selected ciphers.
  5. Click **OK**.  
The **Blocked** icon is no longer displayed in the Blocked column for each blocked cipher(s).

## Filtering Ciphers

You can filter ciphers to easily configure which ciphers should be allowed or blocked.

### Topics:

- [Selecting Display Options](#)
- [Displaying Ciphers by Strength](#)
- [Displaying Ciphers by Block/Unblock](#)
- [Displaying Ciphers by CBC Mode](#)
- [Displaying Ciphers by TLS Protocol Version](#)

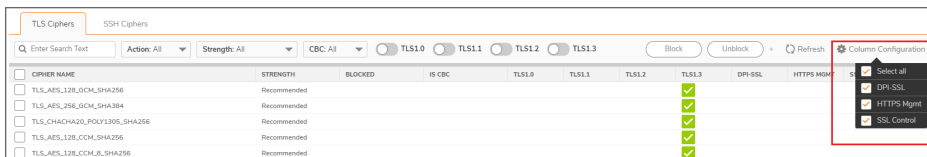
## Selecting Display Options

The **TLS Ciphers** table displays which TLS protocols support which ciphers. You can also display other protocols that support the ciphers:

- DPI-SSL
- HTTPS management
- SSL control

### To filter TLS Ciphers based on its protocols:

1. Navigate to **Network > Firewall > Cipher Control**.
2. Click **TLS Ciphers**.
3. Click **Column Configuration** option. The Select Columns to show/hide drop-down displays.



4. Select the protocol(s) to display:
  - a. **Select All**– This option is selected by default.
  - b. **DPI-SSL** – This option is selected by default.
  - c. **HTTPS MGMT** – This option is selected by default.
  - d. **SSL Control** – This option is selected by default.



## Displaying Ciphers by Strength

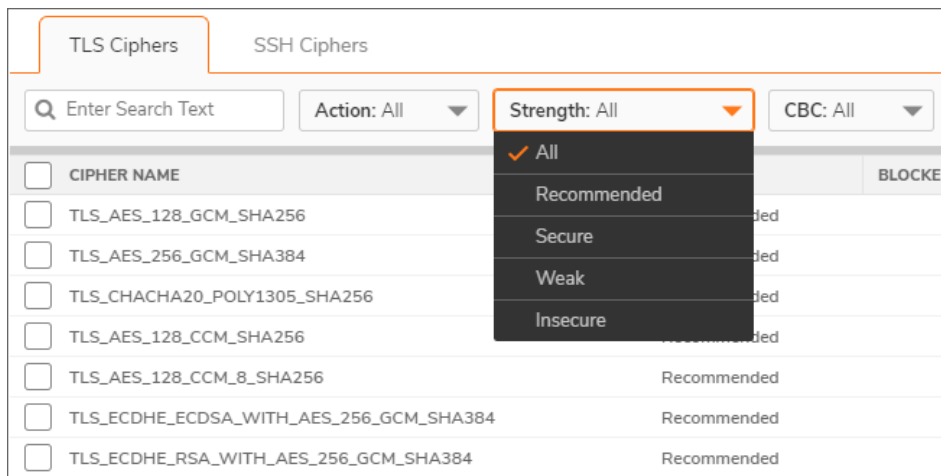
Ciphers are rated according to their strength:

- Recommended
- Secure
- Insecure
- Weak

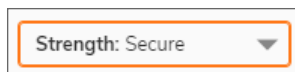
The TLS Ciphers table displays all ciphers of all strengths. You can restrict the TLS Cipher table to display only those ciphers of a particular strength.

### To display ciphers by strength:

1. Navigate to **Network > Firewall > Cipher Control**.
2. Click **TLS Ciphers**.
3. Select the required option from Strength drop-down. The default is **All**.



TLS Cipher table redisplay, showing only those ciphers with the corresponding strength and the Strength drop-down menu reflects the displayed strength.

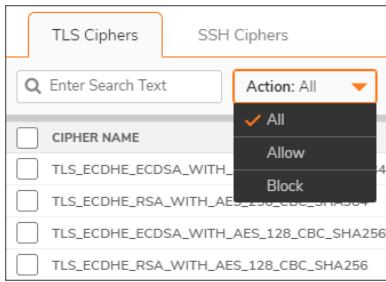


## Displaying Ciphers by Block/Unblock

The TLS Ciphers table displays all blocked and unblocked ciphers. You can restrict the TLS Cipher table to display only those ciphers that are blocked or unblocked.

### To display blocked/unblocked ciphers:

1. Navigate to **Network > Firewall > Cipher Control**.
2. Click **TLS Ciphers**.
3. Select the allow/block action from **Action** drop-down.



- All (default)
- Allow (unblock)
- Block

The TLS Cipher table redisplay, showing only those ciphers with the corresponding action and Action reflects the displayed action.

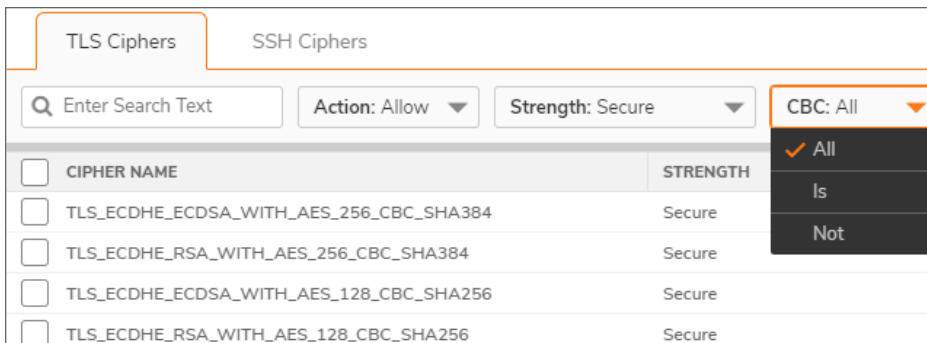


## Displaying Ciphers by CBC Mode

The TLS Ciphers table displays all ciphers for all ciphers regardless of whether they use CBC mode. You can restrict the display to whether a cipher uses CBS mode.

### *To display whether ciphers use CBC mode:*

1. Navigate to **Network > Firewall > Cipher Control**.
2. Click **TLS Ciphers**.
3. Select whether the cipher uses CBC mode from CBC.



- All (default)
- Is (uses CBC mode)
- Not (does not use CBC mode)

The TLS Cipher table redisplay according to the selection, showing an **Enabled** icon in the Is CBC

column for those ciphers using CBC mode and nothing in the CBC column for those that don't.

TLS Ciphers		SSH Ciphers			
<input type="text" value="Enter Search Text"/>	Action: Allow	Strength: Secure	CBC: Is	<input type="checkbox"/> TLS1.0	<input type="checkbox"/> TLS1.1
<input type="checkbox"/> CIPHER NAME	STRENGTH	BLOCKED	IS CBC		
<input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	Secure		<input checked="" type="checkbox"/>		
<input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Secure		<input checked="" type="checkbox"/>		
<input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	Secure		<input checked="" type="checkbox"/>		
<input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Secure		<input checked="" type="checkbox"/>		
<input type="checkbox"/> TLS_RSA_WITH_AES_128_CBC_SHA256	Secure		<input checked="" type="checkbox"/>		
<input type="checkbox"/> TLS_RSA_WITH_AES_256_CBC_SHA256	Secure		<input checked="" type="checkbox"/>		
<input type="checkbox"/> TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	Secure		<input checked="" type="checkbox"/>		
<input type="checkbox"/> TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	Secure		<input checked="" type="checkbox"/>		
<input type="checkbox"/> TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	Secure		<input checked="" type="checkbox"/>		

# Displaying Ciphers by TLS Protocol Version

The TLS Ciphers table displays all ciphers for all TLS protocol versions. You can restrict the display by version of TLS protocol the cipher supports.

### To display ciphers by TLS protocol:

1. Navigate to **Network > Firewall > Cipher Control**.
2. Click **TLS Ciphers**.
3. Click the TLS version(s) for displaying ciphers:



- TLS1.0
- TLS1.1
- TLS1.2
- TLS1.3

The display is restricted to only those ciphers supporting that TLS version.

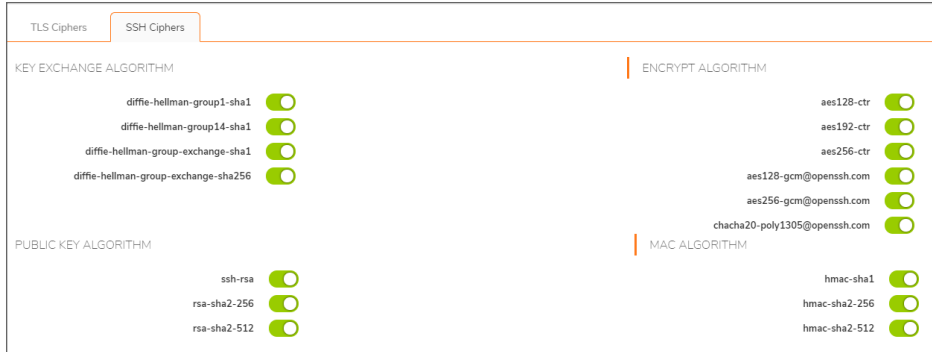
The screenshot shows the 'TLS Ciphers' table with the 'TLS1.2' radio button selected. The table has columns for 'IS CBC', 'TLS1.0', 'TLS1.1', 'TLS1.2', and 'TLS1.3'. The 'IS CBC' column contains green checkmarks for all rows. The 'TLS1.2' column also contains green checkmarks for all rows. The other columns are empty. A 'Block' button is visible in the top right corner of the table area.

	IS CBC	TLS1.0	TLS1.1	TLS1.2	TLS1.3
	✓			✓	
	✓			✓	
	✓			✓	
	✓			✓	
	✓			✓	
	✓			✓	
	✓			✓	
	✓			✓	
	✓			✓	
	✓			✓	
	✓			✓	

**NOTE:** If a cipher supports more than the selected version, the Enabled icon displays for the other supported versions as well.

# SSH Ciphers

The SSH Ciphers page of **Network > Firewall > Cipher Control** allows you to specify which cryptographic SSH ciphers SonicOS uses.



<b>Key Exchange Algorithm</b>	Lists the cryptographic algorithms used to exchange cryptographic keys between two parties
<b>Public Key Algorithm</b>	Lists the asymmetric cryptographic algorithms using pairs of public keys
<b>Encrypt Algorithm</b>	Lists the encryption algorithms used in secure transfers of files, such as FTP transfers
<b>MAC Algorithm</b>	Lists the algorithms using a MAC (message authentication code) value to authenticate messages

To select or deselect SSH ciphers:

1. Navigate to **Network > Firewall > Cipher Control**.
2. Click **SSH Ciphers**.
3. Select the SSH algorithm to use or ignore.

**ⓘ | IMPORTANT:** All SSH ciphers are selected by default.

## Real-Time Black List (RBL) Filter

RBL filters are designed to block SMTP emails based on senders IP addresses where the sender's IP address gets looked up in the database of suspected spammers, malicious/open mail relays, and so on. RBL filters prevents SMTP emails from suspicious email servers.

SMTP Real-Time Black List (RBL) is a mechanism for publishing the IP addresses of SMTP spammers use. There are a number of organizations that compile this information both for free: <http://www.spamhaus.org>, and for profit: <https://ers.trendmicro.com/>.

① **NOTE:** SMTP RBL is an aggressive spam filtering technique that can be prone to false-positives because it is based on lists compiled from reported spam activity. The SonicOS implementation of SMTP RBL filtering provides a number of fine-tuning mechanisms to help ensure filtering accuracy.

RBL list providers publish their lists using DNS. Blacklisted IP addresses appear in the database of the list provider's DNS domain using inverted IP notation of the SMTP server in question as a prefix to the domain name. A response code from 127.0.0.2 to 127.0.0.9 indicates some type of undesirability:

Blocked Response Codes
127.0.0.2 - Open Relay
127.0.0.3 - Dialup Spam Source
127.0.0.4 - Spam Source
127.0.0.5 - Smart Host
127.0.0.6 - Spamware Site
127.0.0.7 - Bad List Server
127.0.0.8 - Insecure Script
127.0.0.9 - Open Proxy Server

For example, if an SMTP server with IP address 1.2.3.4 has been blacklisted by RBL list provider sbl-xbl.spamhaus.org, then a DNS query to 4.3.2.1.sbl-xbl.spamhaus.org will provide a 127.0.0.4 response, indicating that the server is a known source of spam, and the connection will be dropped.

① **NOTE:** Most spam today is known to be sent from hijacked or zombie machines running a thin SMTP server implementation. Unlike legitimate SMTP servers, these zombie machines rarely attempt to retry failed delivery attempts. Once the delivery attempt is blocked by RBL filter, no subsequent delivery attempts for that same piece of spam will be made.

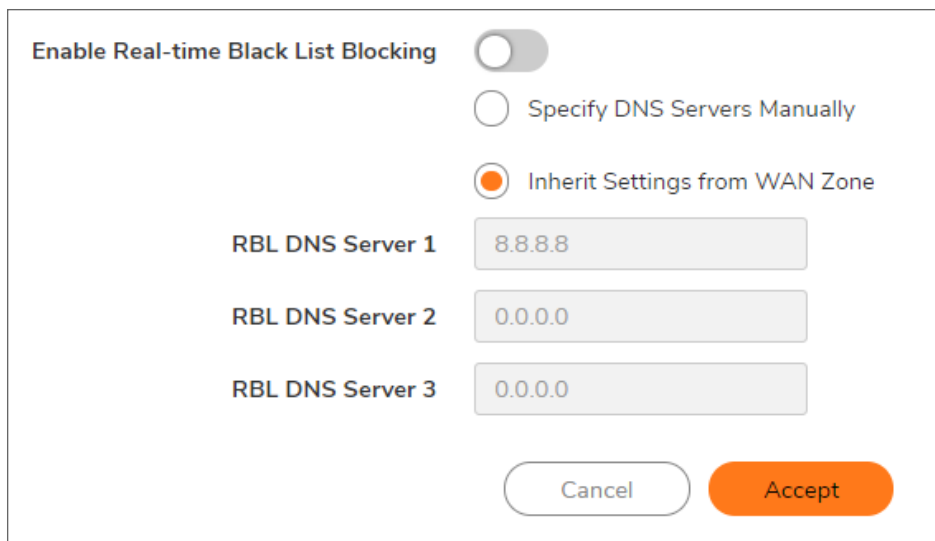
# Configuring the RBL Filter

## Topics:

- [Enabling RBL Blocking](#)
- [Adding RBL Services](#)
- [Configuring User-Defined SMTP Server Lists](#)
- [Testing SMTP IP Addresses](#)

## Enabling RBL Blocking

When **Enable Real-time Black List Blocking** is enabled in the **Real-time Black List Settings** tab on the **RBL Filter** page, inbound connections from hosts on the WAN or outbound connections to hosts on the WAN are checked against each enabled RBL service with a DNS request to the DNS servers configured under **RBL DNS Servers**.



The screenshot shows a configuration window for RBL DNS Servers. At the top, there is a toggle switch for "Enable Real-time Black List Blocking" which is currently turned off. Below the toggle are two radio button options: "Specify DNS Servers Manually" (which is unselected) and "Inherit Settings from WAN Zone" (which is selected). Underneath these options are three input fields for "RBL DNS Server 1", "RBL DNS Server 2", and "RBL DNS Server 3". The first field contains the IP address "8.8.8.8", while the second and third fields contain "0.0.0.0". At the bottom of the window are two buttons: "Cancel" and "Accept".

The RBL DNS Servers menu allows you to specify the DNS servers. You can choose **Inherit Settings from WAN Zone** or **Specify DNS Servers Manually**. If you select **Specify DNS Servers Manually**, enter the DNS server addresses in the **DNS Server** fields.

When you have finished, click **Accept**.

The DNS responses are collected and cached. If any of the queries result in a blacklisted response, the server will be filtered. Responses are cached using TTL values, and non-blacklisted responses are assigned a cache TTL of 2 hours. If the cache fills up, then cache entries are discarded in a FIFO (first-in-first-out) fashion.

The IP address check uses the cache to determine if a connection should be dropped. Initially, IP addresses are not in the cache and a DNS request must be made. In this case the IP address is assumed innocent until proven guilty, and the check results in the allowing of the connection. A DNS request is made and results are cached in a

separate task. When subsequent packets from this IP address are checked, if the IP address is blacklisted, the connection will be dropped.

## Adding RBL Services

You can add additional RBL services in the **Real-time Black List Services** tab.

RBL_SERVICE	RESPONSE CODES	ENABLE	STATISTICS	CONFIGURE
<input type="checkbox"/> sbl-xbl.spamhaus.org		<input checked="" type="checkbox"/>	0	
<input type="checkbox"/> dnsbl.sorbs.net		<input checked="" type="checkbox"/>	0	

To add an RBL service, click the **Add** icon. In the **Add Black-List Service** dialog, you specify the RBL domain to be queried, enable it for use, and specify its expected response codes. Most RBL services list the responses they provide on their Web site, although selecting **Block All Responses** is generally acceptable.

### Add Black-List Service

**RBL DOMAIN SETTINGS**

Enable RBL Domain

RBL Domain

**RBL BLOCKED RESPONSES**

- 127.0.0.2 - Open Relay
- 127.0.0.3 - Dial-up Spam Source
- 127.0.0.4 - Spam Source
- 127.0.0.5 - Smart Host
- 127.0.0.6 - Spamware Site
- 127.0.0.7 - Bad List Server
- 127.0.0.8 - Insecure Script
- 127.0.0.9 - Open Proxy Server
- 127.0.0.10 - PBL ISP
- 127.0.0.11 - PBL GRID
- Block All Responses

The connection details are maintained for each RBL Service in the **RBL Service** table, and can be viewed with a mouseover of the (Information) icon to the right on the service entry.

## Configuring User-Defined SMTP Server Lists

The **User Defined SMTP Server Lists** tab allows for Address Objects to be used to construct a white-list (explicit allow) or black-list (explicit deny) of SMTP servers. Entries in this list will bypass the RBL querying procedure.

#	NAME	ADDRESS DETAIL	TYPE	ZONE	CONFIGURE
1	RBL User White List		Group		+
2	RBL User Black List		Group		+



① **NOTE:** To see entries in the RBL User White List and RBL User Black List, click the arrow to the right of the checkbox for that list.

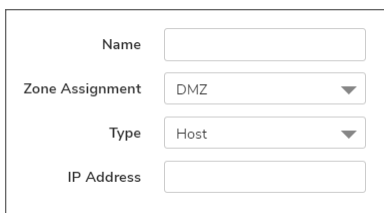
### Topics:

- [Configuring a White List](#)
- [Configuring a Black List](#)

## Configuring a White List

For example, to ensure that you always receive SMTP connections from a partner site's SMTP server:

1. Create an Address Object for the server using the **Add** icon. The **Add User-Defined SMTP Server** dialog appears.

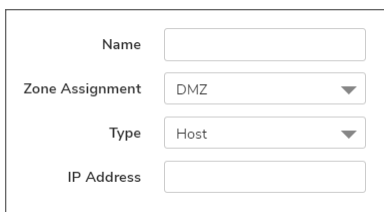


2. Configure the Address Object.
3. Click **OK**. The Address Object is added to the RBL User White List in the User-Defined SMTP Server Lists table.

① **NOTE:** To delete a White List Address Object, click the triangle icon of RBL White List row and click **Delete** icon.

## Configuring a Black List

1. Create an Address Object for the server using the **Add** icon. The **Add User-Defined SMTP Server** dialog appears.



2. Configure the Address Object.
3. Click **OK**. The Address Object is added to the RBL User Black List in the User-Defined SMTP Server Lists table.

① **NOTE:** To delete a Black List Address Object, click the triangle icon of RBL User Black List row and click **Delete** icon.

# Testing SMTP IP Addresses

The **Device > Diagnostics > Real-Time Blacklist** page also provides a Real-time Black List Lookup feature that allows for SMTP IP addresses (or RBL services, or DNS servers) to be specifically tested.

For a list of known spam sources to use in testing, refer to: <http://www.spamhaus.org/sbl/latest/>.

# SonicWall Support

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

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

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at <https://community.sonicwall.com/technology-and-support>.
- View video tutorials
- Access <https://mysonicwall.com>
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

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

# About This Document

SonicOS Network Firewall Administration Guide

Updated - July 2023

Software Version - 7.0

232-005386-10 Rev E

Copyright © 2023 SonicWall Inc. All rights reserved.

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

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

## End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/end-user-product-agreements/>.

## Open Source Code

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

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