Release Notes

SonicOS

SonicOS 6.2.0.0 Release Notes

Contents

Release Purpose

SonicOS 6.2.0.0 is an early release that introduces support for IPv6, 3G/4G Wireless WAN, Jumbo Frames, Advanced Switching, and more on the latest generation of Dell SonicWALL SuperMassive and NSA series appliances.

Platform Compatibility

The SonicOS 6.2.0.0 release is supported on the following Dell SonicWALL appliances:

- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2600

Note: *The NSA 2600 does not support Jumbo Frames, PortShield, or Switching.*

The Dell SonicWALL WXA series appliances (WXA 6000 Software, WXA 500 Live CD, WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are supported for use with Dell SonicWALL NSA security appliances running SonicOS 6.2. The recommended WXA firmware version is WXA 1.3 or higher.

Upgrading Information

Preferences import from SonicOS version 5.9.0.x (minimum 5.9.0.4) to 6.2.0.x (minimum 6.2.0.0) is supported.

For information about obtaining the latest firmware, upgrading the firmware image on your Dell SonicWALL appliance, and importing configuration settings from another appliance, refer to the *SonicOS 6.2 Upgrade Guide* available on MySonicWALL with the firmware.

Browser Support

SonicOS uses advanced browser technologies such as HTML5, which are supported in most recent browsers. Dell SonicWALL recommends using the latest Chrome, Firefox, Internet Explorer, or Safari browsers for administration of SonicOS. This release supports the following Web browsers:

- Chrome 18.0 and higher (recommended browser for dashboard real-time graphics display)
- Firefox 16.0 and higher
- Internet Explorer 8.0 and higher (do not use compatibility mode)
- Safari 5.0 and higher

Mobile device browsers are not recommended for Dell SonicWALL appliance system administration.

New Features

SonicOS 6.2.0.0 includes the following new features for Dell SonicWALL NSA and SuperMassive series appliances:

Note: For detailed information about these features, see the SonicOS 6.2 Administrator's Guide, which can be downloaded at www.mysonicwall.com, on the same page that has the SonicOS 6.2 firmware.

Supported/Unsupported IPv6 Features

This section summarizes the key SonicOS 6.2 features that are, or are not, available with IPv6.

SonicOS Features Available with IPv6

- 6 to 4 tunnel (allows IPv6 nodes to connect to outside IPv6 services over an IPv4 network)
- Access Rules
- Address Objects
- Anti-Spyware
- Application Firewall
- Attack prevention:
  - Land Attack
  - Ping of Death
  - Smurf
  - SYN Flood
- Connection Cache
- Connection Limiting for IPv6 connections
- Connection Monitor
- Content Filtering Service
- DHCP
- DHCP Prefix Delegation
- DNS client
- DNS lookup and reverse name lookup
- Dynamic Routing (RIPng and OSPFv3)
- EPRT
- EPSV
- FTP
- Gateway Anti-Virus
- High Availability:
  - Connection Cache
  - FTP
  - IPv6 management IP address
  - NDP
  - SonicPoint
- HTTP/HTTPS management over IPv6
- ICMP
- IKEv2
- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
- Intrusion Prevention Service
- IP Spoof Protection
- IPv4 Syslog messages, including messages with IPv6 addresses
- IPv6 BGP
- IPv6 for Backend Servers
- IPv6 Rapid Deployment (6rd)
- Layer 2 Bridge Mode
- Logging IPv6 events
- Login uniqueness
- Multicast Routing with Multicast Listener Discovery
- NAT
- Neighbor Discovery Protocol
- NetExtender connections for users with IPv6 addresses

- Packet Capture
- Ping
- Policy Based Routing
- Remote management
- Security services for IPv6 traffic with DPI
- Site-to-site IPv6 tunnel with IPsec for security
- SonicPoint IPv6 support
- SNMP
- SSL VPN
- Stateful inspection of IPv6 traffic
- User status
- Visualization
- VLAN interfaces with IPv6 addresses
- VPN policies
- Wireless
- WireMode

SonicOS Features Not Available with IPv6

- Anti-Spam
- Command Line Interface
- DHCP over VPN
- DHCP Relay
- Dynamic Address Objects for IPv6 addresses
- Dynamic DNS
- FQDN
- Global VPN Client (GVC)
- GMS
- H.323
- High Availability:
  - Multicast
  - Oracle SQL/Net
  - RTSP
  - VoIP
- IKEv1
- IPv6 Syslog messages
- L2TP
- LDAP
- MAC-IP Anti-Spoof
- NAT between IPv6 and IPv4 addresses
- NAT High Availability probing
- NAT load balancing
- NetBIOS over VPN
- NTP
- QoS Mapping
- RADIUS
- RAS Multicast Forwarding
- Route-based VPNs
- Single Sign On
- SIP
- SMTP Real-Time Black List (RBL) Filtering

- SSH
- Transparent Mode
- ViewPoint
- Virtual Assistant
- Web proxy

IPv6 Visualization

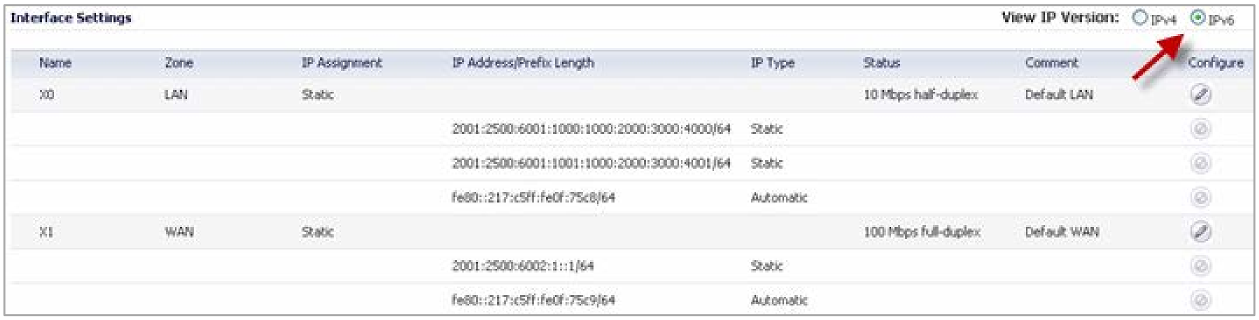
IPv6 Visualization for the App Flow Monitor and Real-Time Monitor is an extension of the IPv4 Visualization, providing real-time monitoring of interface/application rates and visibility of sessions in the management interface.

With the visualization dashboard monitoring improvements for IPv6, administrators are able to respond more quickly to network security vulnerabilities and network bandwidth issues. Administrators can see what websites their employees are accessing, what applications and services are being used in their networks and to what extent, in order to police content transmitted in and out of their organizations.

The App Flow Monitor page has two new options for the View IP Version selection. These options allow you to monitor IPv6 only or IPv4 only traffic. The Real-Time Monitor page has the same two new options under the Interface drop-down menu in the Applications and Bandwidth panels. App Flow Monitor and Real-Time Monitor Visualization is configured the same in IPv6 and IPv4.

IPv6 Interface Configuration

IPv6 interfaces are configured on the **Network** > **Interfaces** page by clicking the **IPv6** option for the **View IP Version** radio button at the top right corner of the page. IPv6 can be enabled or disabled on each interface.



Interface Settings

View IP Version: ○ IPv4 ● IPv6

Name	Zone	IP Assignment	IP Address/Prefix Length	IP Type	Status	Comment	Configure
X0	LAN	Static			10 Mbps half-duplex	Default LAN	
			2001:2500:6001:1000:1000:2000:3000:4000/64	Static			
			2001:2500:6001:1001:1000:2000:3000:4001/64	Static			
			fe80::217:c5ff:fe0f:75c8/64	Automatic			
X1	WAN	Static			100 Mbps full-duplex	Default WAN	
			2001:2500:6002:1::1/64	Static			
			fe80::217:c5ff:fe0f:75c9/64	Automatic			

By default, all IPv6 interfaces appear as routed with no IP address. Multiple IPv6 addresses can be added on the same interface. Auto IP assignment can only be configured on WAN interfaces.

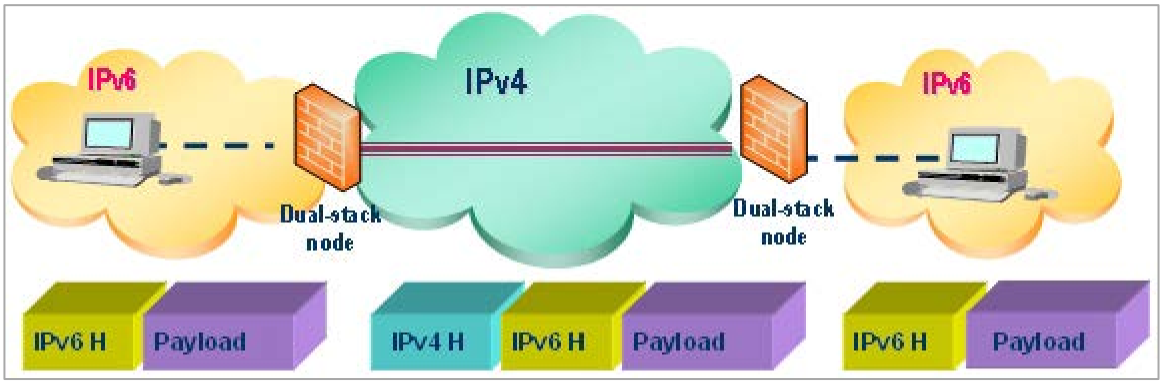
Each interface can be configured to receive router advertisement or not.

IPv6 Tunnel Interfaces

IPv6 tunnel interfaces transport IPv4 packets through IPv6 networks and IPv6 packets through IPv4 networks. For instance, in order to pass IPv6 packets through the IPv4 network, the IPv6 packet will be encapsulated into an IPv4 packet at the ingress side of a tunnel. When the encapsulated packet arrives at the egress of the tunnel, the IPv4 packet will be de-capsulated.

Tunnels can be either automatic or manually configured. A configured tunnel determines the endpoint addresses by configuration information on the encapsulating node. An automatic tunnel determines the IPv4 endpoints from the address of the embedded IPv6 datagram. IPv4 multicast tunneling determines the endpoints through Neighbor Discovery.

The following diagram depicts an IPv6 to IPv4 tunnel.



IPv6 Access to the SonicOS Management Interface

After IPv6 addressing has been configured on the firewall, the SonicOS management interface can be accessed by entering the IPv6 address of the firewall in your browser's URL field.

IPv6 System Diagnostics and Monitoring

SonicOS provides the following diagnostic tools for IPv6:

- Packet Capture on the System > Packet Monitor page
- IPv6 Ping on the System > Diagnostics page
- IPv6 DNS Name Lookup on the System > Diagnostics page
- Reverse Name Resolution on the System > Diagnostics page

Packet Capture

Packet Capture fully supports IPv6. IPv6 keywords can be used to filter the packet capture.

IPv6 Ping

The ping tool includes a Prefer IPv6 networking option. When pinging a domain name, it uses the first IP address that is returned and shows the actual pinging address. If both an IPv4 and IPv6 address are returned, by default, the firewall pings the IPv4 address. If Prefer IPv6 networking is enabled, the firewall will ping the IPv6 address.

IPv6 DNS Name Lookup and Reverse Name Resolution

You can use IPv6 addresses for DNS Name Lookup or Reverse Name Resolution.

IPv6 Network Configuration

IPv6 can be configured for the following network elements:

- IPv6 DNS
- IPv6 Address Objects
- IPv6 Policy Based Routing
- IPv6 NAT Policies
- IPv6 Neighbor Discovery Protocol
- IPv6 Multicast Routing
- IPv6 DHCPv6 Configuration

IPv6 DNS

DNS for IPv6 is configured using the same method as for IPv4. Click the IPv6 option in the View IP Version radio button at the top left of the **Network > DNS** page.

IPv6 Address Objects

IPv6 address objects or address groups can be added in the same manner as IPv4 address objects. On the **Network > Address Objects** page, the View IP Version radio button has three options: IPv4 only, IPv6 only, or IPv4 and IPv6.

Policy Based Routing

Policy Based Routing is fully supported for IPv6 by selecting IPv6 address objects and gateways for route policies on the **Network > Routing** page. On the **Network > Routing** page, the View IP Version radio button has three options: IPv4 only, IPv6 only, or IPv4 and IPv6. The OSPF feature displays two radio buttons to switch between version 2 and version 3.

IPv6 NAT Policies

NAT policies can be configured for IPv6 by selecting IPv6 address objects on the **Network > NAT Policies** page. On the **Network > NAT Policies** page, the View IP Version radio button has three options: IPv4 only, IPv6 only, or IPv4 and IPv6.

IPv6 Neighbor Discovery Protocol

The Neighbor Discovery Protocol (NDP) is a new messaging protocol that was created as part of IPv6 to perform a number of the tasks that ICMP and ARP accomplish in IPv4. Just like ARP, Neighbor Discovery builds a cache of dynamic entries, and the administrator can configure static Neighbor Discovery entries. IPv6 NDP is configured on the **Network > Neighbor Discovery** page.

Multicast Routing

Multicast Routing is configured on the **Network > Multicast Routing**. The Multicast Proxy feature maintains interoperability between IPv6 and IPv4 networks. The Multicast Listener Discovery (MLD) protocol is used by IPv6 routers to discover multicast listeners that are directly connected to the firewall.

DHCPv6 Configuration

A DHCPv6 server can be configured similar to IPv4 after selecting the IPv6 option in the View IP Version radio button at the top left of the **Network > DNS** page.

IPv6 BGP Support

IPv6 Border Gateway protocol (BGP) communicates IPv6 routing information between Autonomous Systems (ASs). A Dell SonicWALL security appliance with IPv6 BGP support can replace a traditional BGP router on the edge of a network's AS.

IPv6 BGP is enabled on the **Network > Routing** page, but must be configured on the SonicOS Command Line Interface (CLI).

Note*: MPLS/VPN and multicast are not supported for IPv6 BGP in SonicOS 6.2.0.0.*

IPv6 Wire Mode Support

WireMode interfaces in SonicOS 6.2.0.0 are supported for use with IPv6. Wire Mode is a simplified form of Layer 2 Bridge Mode and operates using a bump-in-the-wire implementation. A Wire Mode interface does not take any IP address and it is typically configured as a bridge between a pair of interfaces. No packets received on a Wire Mode interface will be destined to the firewall, they only bridge traffic.

Wire Mode operates in any of four different modes:

- Bypass Mode
- Secure Mode
- Inspect/Scan Mode
- Tap Mode

***Note:** Any WireMode interfaces configured in IPv4 will also be available in IPv6, however they are not editable. WireMode interfaces can only be added, edited, or deleted in IPv4.*

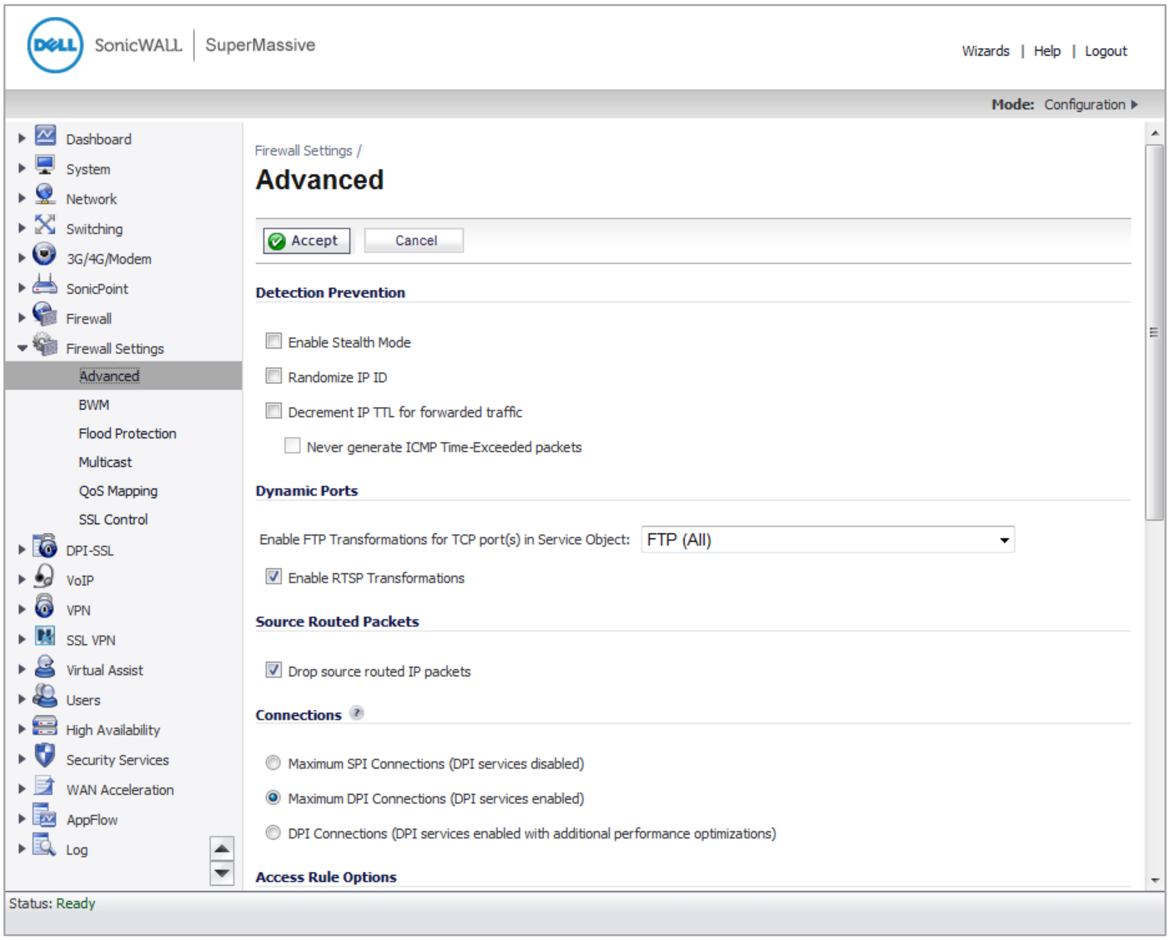
IPv6 Firewall Access Rules Configuration

IPv6 firewall 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 **Firewall > Access Rules** page, the **View IP Version** radio button has three options:

- IPv4 only
- IPv6 only
- IPv4 and IPv6

IPv6 Advanced Firewall Settings

You can configure advanced firewall settings for IPv6, including packet limitations and traffic restrictions on the **Firewall Settings > Advanced** page.



Firewall Settings /
Advanced

Detection Prevention

□ Enable Stealth Mode
□ Randomize IP ID
□ Decrement IP TTL for forwarded traffic
□ Never generate ICMP Time-Exceeded packets

Dynamic Ports

Enable FTP Transformations for TCP port(s) in Service Object: FTP (All)
☑ Enable RTSP Transformations

Source Routed Packets

☑ Drop source routed IP packets

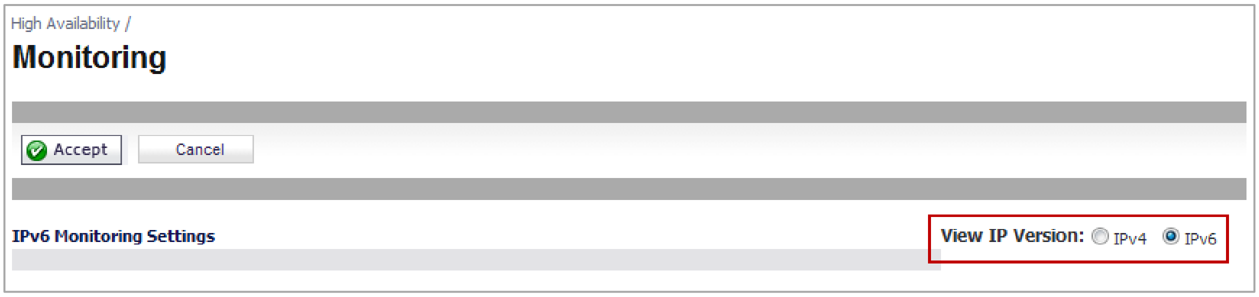
Connections

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

Access Rule Options

IPv6 High Availability Monitoring

IPv6 High Availability (HA) Monitoring is implemented as an extension of HA Monitoring in IPv4. After configuring HA Monitoring for IPv6, both the primary and backup appliances can be managed from the IPv6 monitoring address, and IPv6 Probing is capable of detecting the network status of HA pairs. The IPv4 and IPv6 options can be selected on the **High Availability > Monitoring** page.



High Availability /

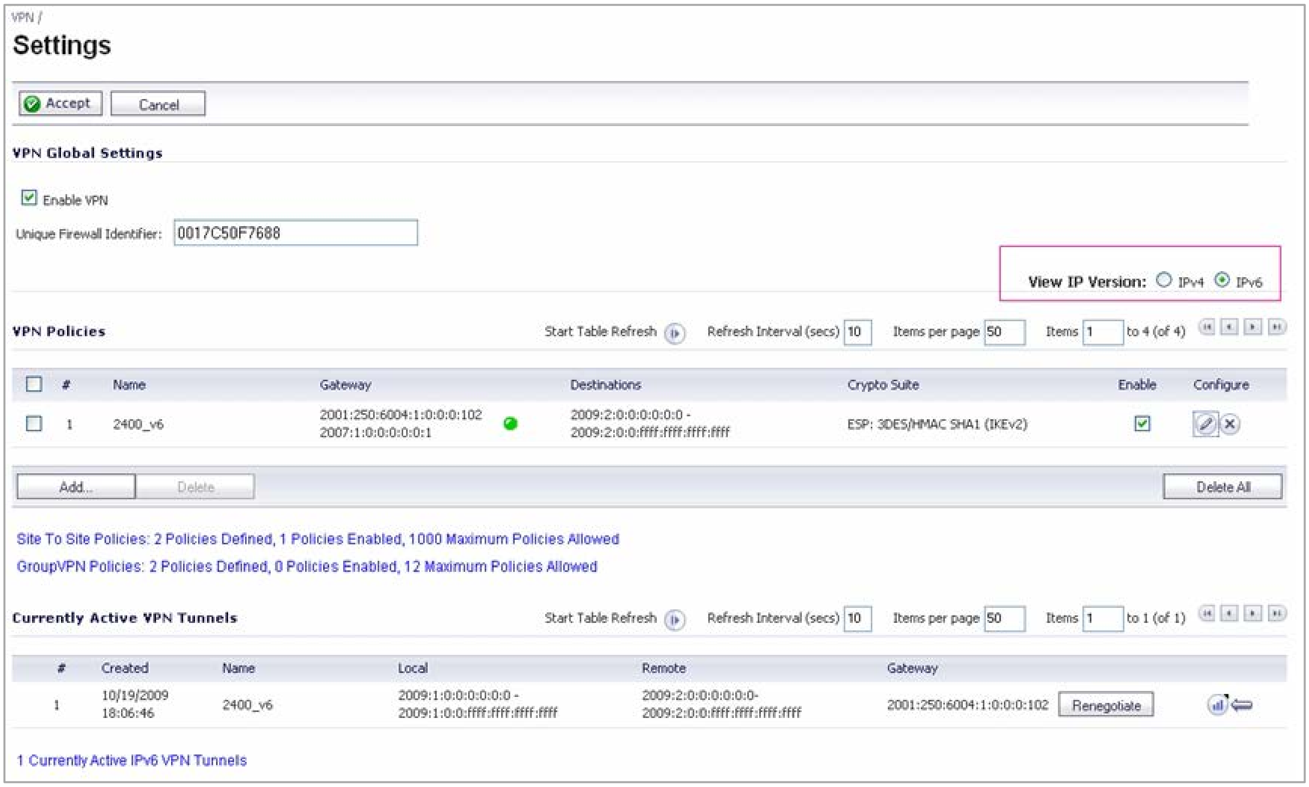
Monitoring

IPv6 Monitoring Settings

View IP Version: ○ IPv4 ● IPv6

IPv6 IPsec VPN Configuration

IPsec VPNs can be configured for IPv6 in a similar manner to IPv4 VPNs after selecting the IPv6 option in the View IP Version radio button at the top left of the **VPN > Settings** page.



VPN /

Settings

VPN Global Settings

☑ Enable VPN

Unique Firewall Identifier: 0017C50F7688

View IP Version: ○ IPv4 ● IPv6

VPN Policies

Start Table Refresh | Refresh Interval (secs) 10 | Items per page 50 | Items 1 to 4 (of 4)

□	#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
□	1	2400_v6	2001:250:6004:1:0:0:0:102 2007:1:0:0:0:0:0:1 ●	2009:2:0:0:0:0:0:0 - 2009:2:0:0:ffff:ffff:ffff:ffff	ESP: 3DES/HMAC SHA1 (IKEv2)	☑	

Site To Site Policies: 2 Policies Defined, 1 Policies Enabled, 1000 Maximum Policies Allowed

GroupVPN Policies: 2 Policies Defined, 0 Policies Enabled, 12 Maximum Policies Allowed

Currently Active VPN Tunnels

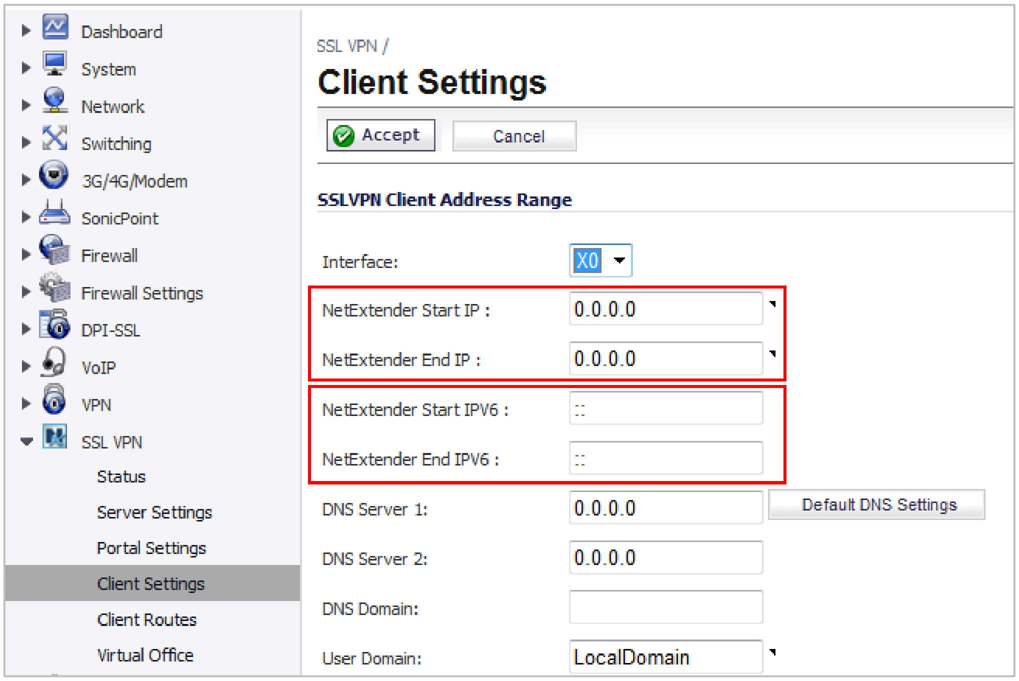
Start Table Refresh | Refresh Interval (secs) 10 | Items per page 50 | Items 1 to 1 (of 1)

#	Created	Name	Local	Remote	Gateway	
1	10/19/2009 18:06:46	2400_v6	2009:1:0:0:0:0:0:0 - 2009:1:0:0:ffff:ffff:ffff:ffff	2009:2:0:0:0:0:0:0- 2009:2:0:0:ffff:ffff:ffff:ffff	2001:250:6004:1:0:0:0:102	Renegotiate

1 Currently Active IPv6 VPN Tunnels

IPv6 SSL VPN Configuration

SonicOS supports NetExtender connections for users with IPv6 addresses. On the **SSLVPN > Client Settings** page, first configure the traditional IPv4 IP address pool, and then configure an IPv6 IP address pool. Clients are assigned two internal addresses: one IPv4 and one IPv6.



Client Settings

SSLVPN Client Address Range

Interface: X0

NetExtender Start IP : 0.0.0.0

NetExtender End IP : 0.0.0.0

NetExtender Start IPV6 : ::

NetExtender End IPV6 : ::

DNS Server 1: 0.0.0.0

DNS Server 2: 0.0.0.0

DNS Domain:

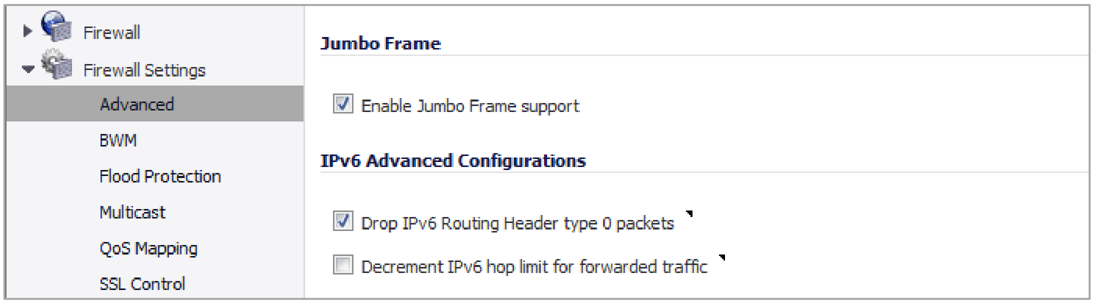
User Domain: LocalDomain

Jumbo Frames

Jumbo Frame support in SonicOS allows the Dell SonicWALL SuperMassive 9000 series and NSA 3600-6600 appliances to process Ethernet frames with payloads ranging from 1500-9000 bytes.

***Note:** Jumbo Frames are not supported on the NSA 2600.*

Jumbo Frame support is enabled on the **Firewall Settings > Advanced** page.



Jumbo Frame

☑ Enable Jumbo Frame support

IPv6 Advanced Configurations

☑ Drop IPv6 Routing Header type 0 packets

☐ Decrement IPv6 hop limit for forwarded traffic

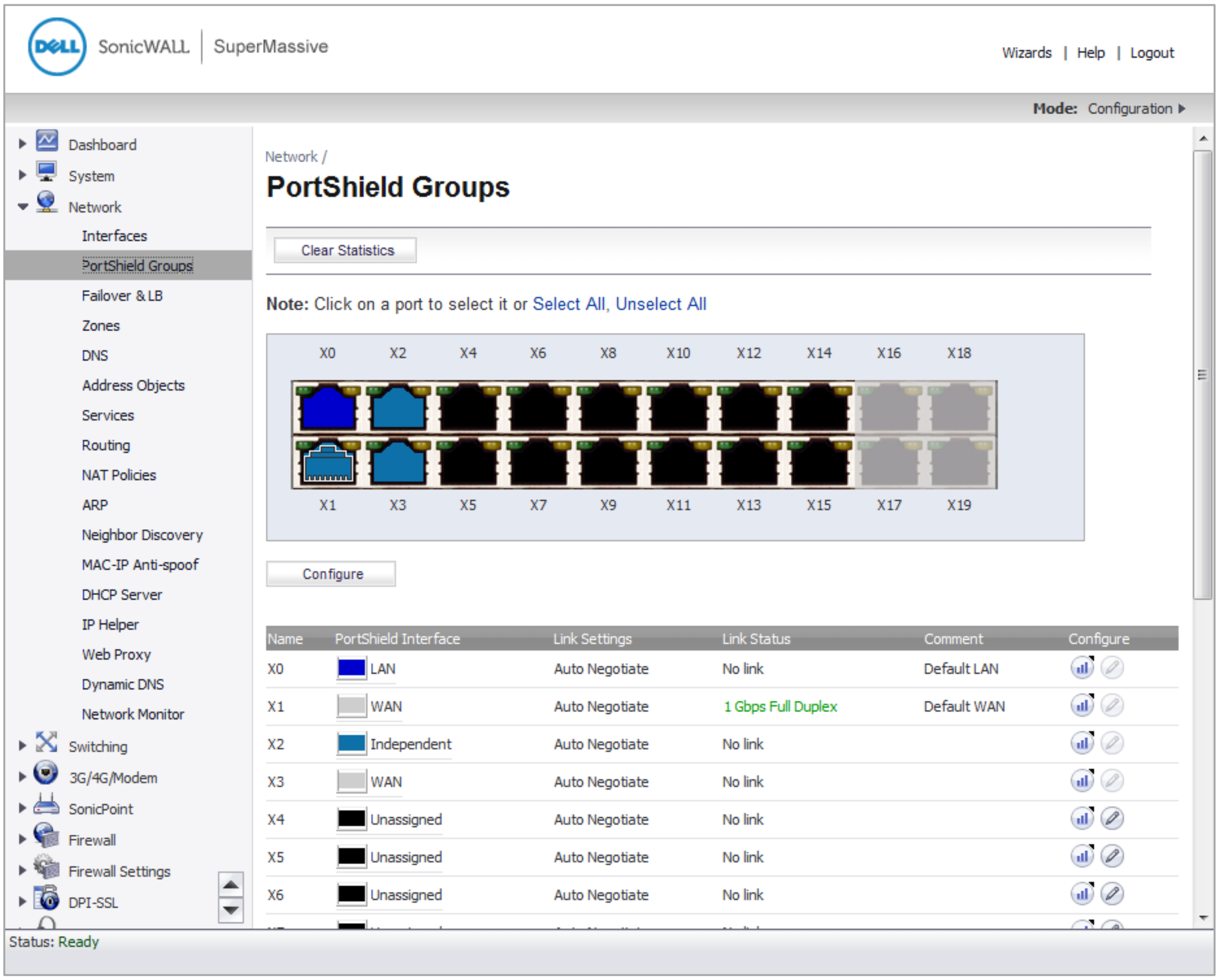
Enable Jumbo Frame support – Enabling this option increases throughput and reduces the number of Ethernet frames to be processed. Throughput increase may not be seen in some cases. However, there will be some improvement in throughput if the packets traversing are really jumbo size.

On the **Network > Interfaces** page for each port, the **Interface MTU** specifies the largest packet size that the interface can forward without fragmenting the packet. You can select the size of the packets that the port will receive and transmit:

- 1500 – Standard packets (default)
- 9000 – Jumbo frame packets

PortShield Groups

PortShield architecture enables you to configure some or all of the LAN ports into separate security contexts, providing protection not only from the WAN and DMZ, but between devices inside your network as well. In effect, each context has its own wire-speed PortShield that provides the protection of a dedicated, deep packet inspection firewall. PortShield configuration is available on the **Network > PortShield Groups** page.



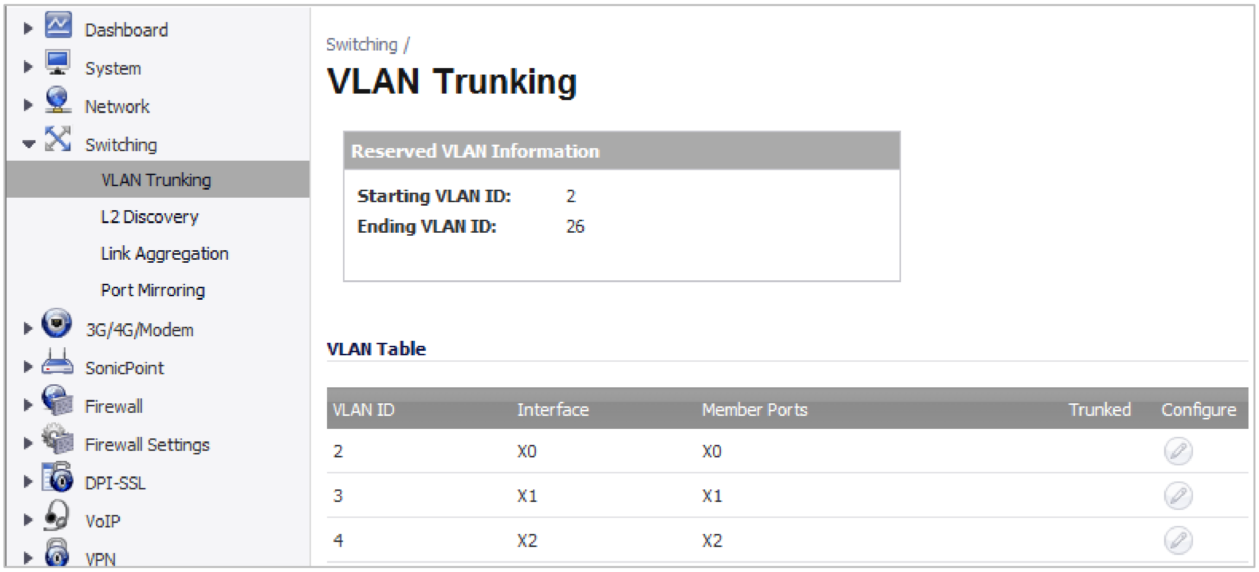
Note: Click on a port to select it or Select All, Unselect All

Name	PortShield Interface	Link Settings	Link Status	Comment	Configure
X0	🟦 LAN	Auto Negotiate	No link	Default LAN	
X1	⬜ WAN	Auto Negotiate	1 Gbps Full Duplex	Default WAN	
X2	🟦 Independent	Auto Negotiate	No link		
X3	⬜ WAN	Auto Negotiate	No link		
X4	⬛ Unassigned	Auto Negotiate	No link		
X5	⬛ Unassigned	Auto Negotiate	No link		
X6	⬛ Unassigned	Auto Negotiate	No link		

***Note:** The PortShield feature is not supported on the NSA 2600.*

Switching

SonicOS 6.2 provides Layer 2 (data link layer) switching functionality.



Switching /

VLAN Trunking

Reserved VLAN Information

Starting VLAN ID: 2
Ending VLAN ID: 26

VLAN Table

VLAN ID	Interface	Member Ports	Trunked	Configure
2	X0	X0		✎
3	X1	X1		✎
4	X2	X2		✎

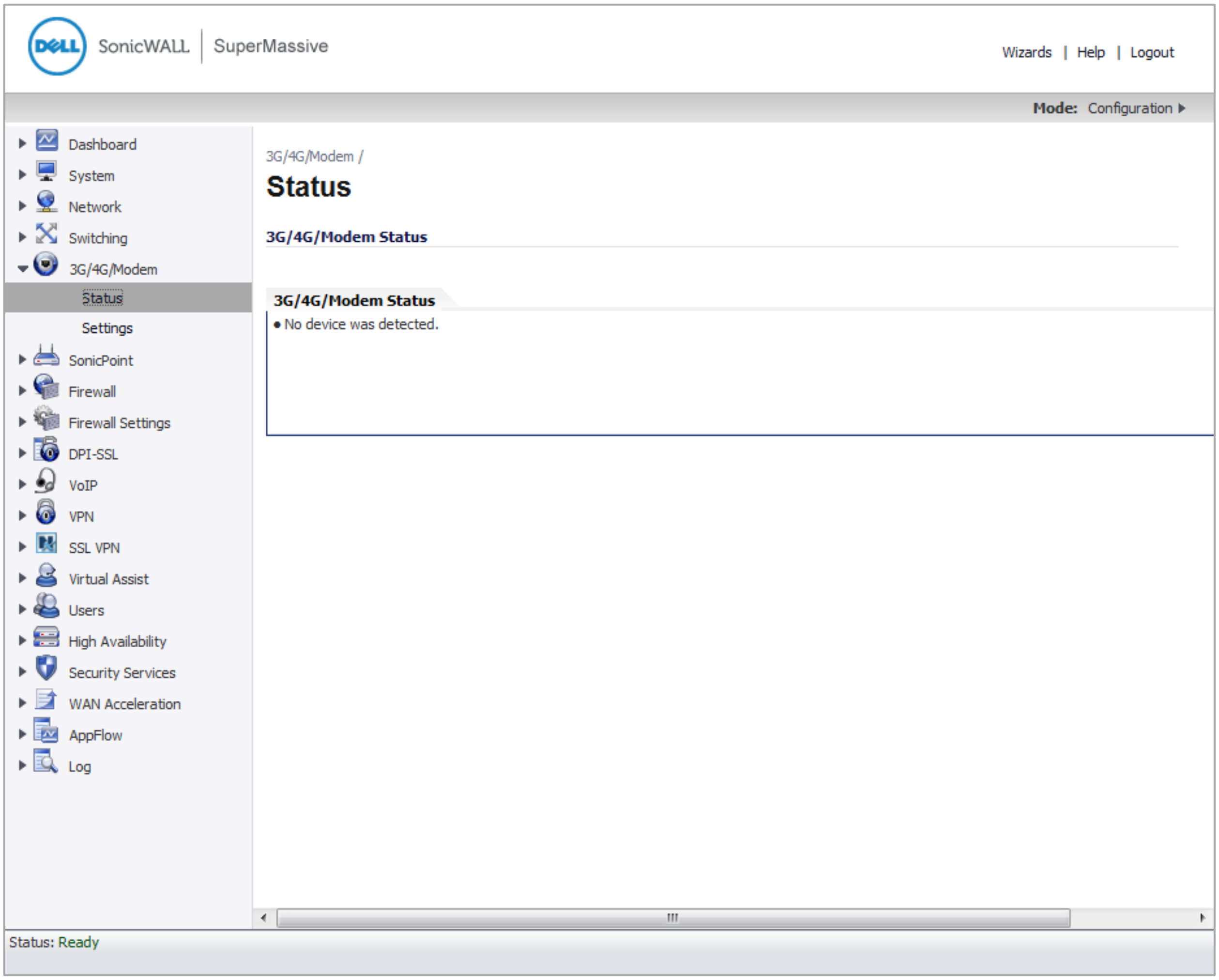
Note: *Switching is not supported on the NSA 2600.*

The Switching functionality provides the following switching features:

- **VLAN Trunking** – Provides the ability to trunk different VLANs between multiple switches.
- **Layer 2 Network Discovery** – Uses IEEE 802.1AB (LLDP) and Microsoft LLTD protocols and switch forwarding table to discover devices visible from a port.
- **Link Aggregation** – Provides the ability to aggregate ports for increased performance and redundancy.
- **Port Mirroring** – Allows the administrator to assign a mirror port to mirror ingress, egress or bidirectional packets coming from a group of ports.
- **Jumbo Frames** – Supporting jumbo frames allows the Dell SonicWALL SuperMassive appliances to process Ethernet frames with payloads ranging from 1500-9000 bytes.

3G/4G/Modem

Dell SonicWALL network security appliances with a USB extension port can support either an external 3G/4G interface or an analog modem interface. When the appliance does not detect an external interface, a **3G/4G/Modem** tab is displayed in the left-side navigation bar.



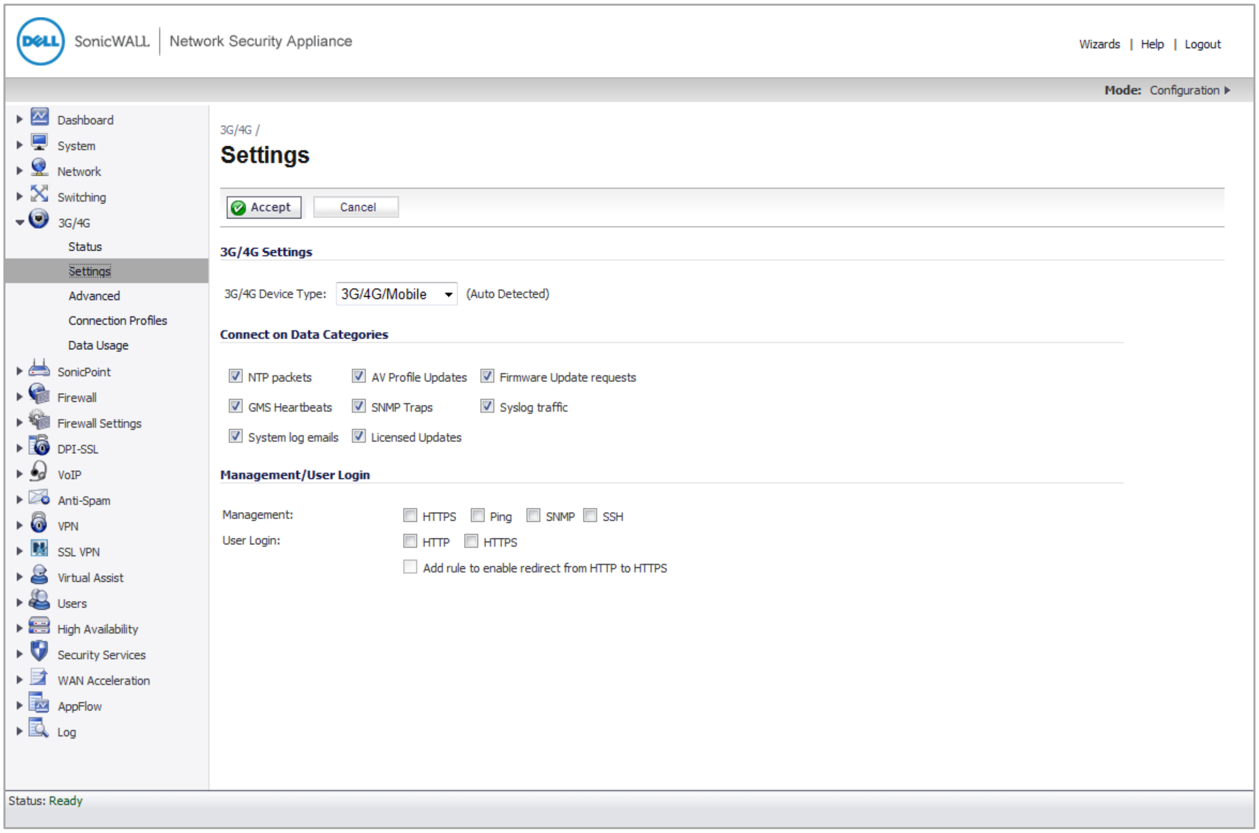
- No device was detected.

Status: Ready

3G/4G

Dell SonicWALL security appliances support 3G/4G Wireless WAN connections that utilize data connections over cellular networks. When a 3G/4G device is connected to the appliance, the left-side navigation pane displays **3G/4G** instead of **3G/4G/Modem**. The 3G/4G connection can be used for:

- WAN failover to a connection that is not dependent on wire or cable
- Temporary networks where a pre-configured connection may not be available, such as at trade-shows and kiosks
- Mobile networks, where the Dell SonicWALL appliance is based in a vehicle
- Primary WAN connection where wire-based connections are not available, but 3G/4G cellular is available



Settings

3G/4G Settings

3G/4G Device Type: 3G/4G/Mobile (Auto Detected)

Connect on Data Categories

☑ NTP packets ☑ AV Profile Updates ☑ Firmware Update requests
☑ GMS Heartbeats ☑ SNMP Traps ☑ Syslog traffic
☑ System log emails ☑ Licensed Updates

Management/User Login

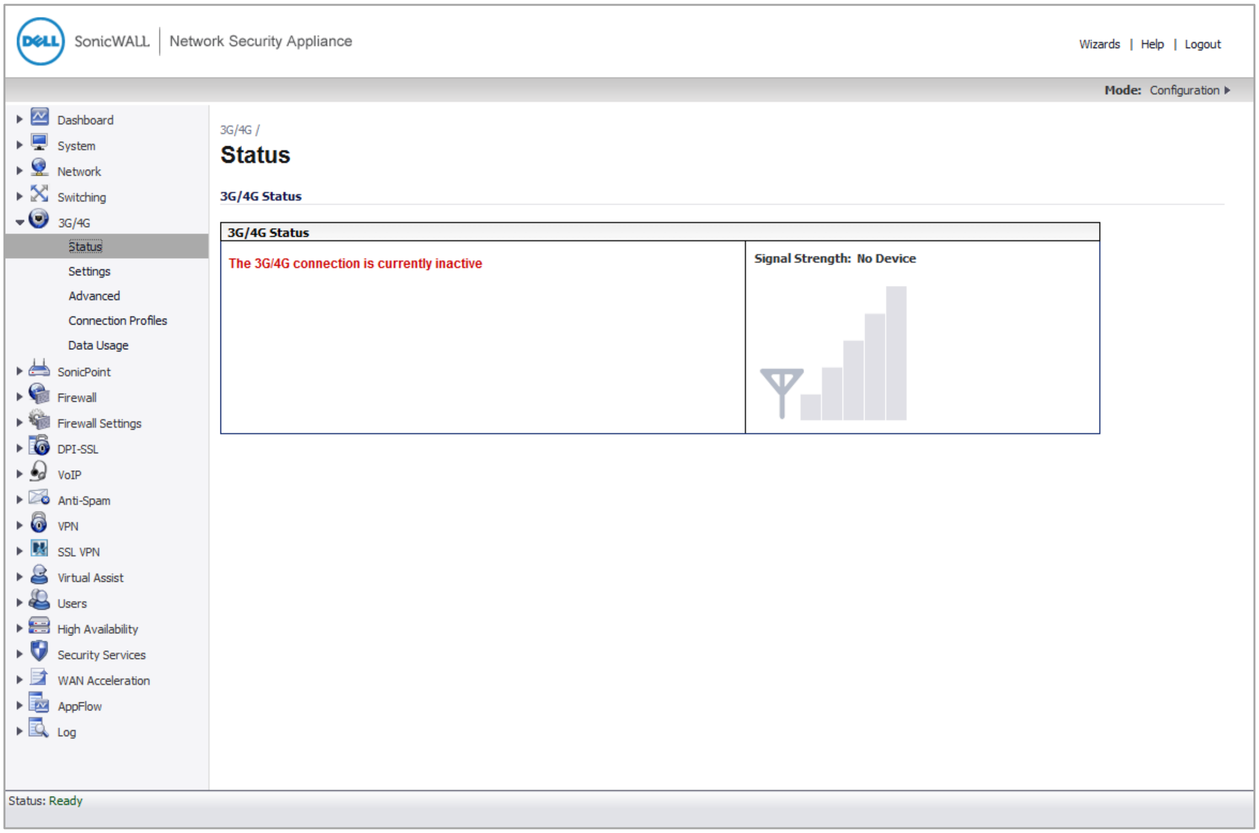
Management: □ HTTPS □ Ping □ SNMP □ SSH
User Login: □ HTTP □ HTTPS
□ Add rule to enable redirect from HTTP to HTTPS

Modem > Status

The **Modem > Status** page displays dialup connection information when the modem is active. You can create modem Connection Profiles in the **Modem Profile Configuration** window, which you access from the **Modem > Connection Profiles** page. In the **Modem Status** section, the following network information from your ISP is displayed when the modem is active:

- WAN Gateway (Router) Address
- WAN IP (NAT Public) Address
- WAN Subnet Mask
- DNS Server 1
- DNS Server 2
- DNS Server 3
- Current Active Dial-Up Profile (id)
- Current Connection Speed

If the modem is inactive, the **Status** page displays a list of possible reasons that your modem is inactive. When the modem is active, the network settings from the ISP are used for WAN access.



3G/4G Status

The 3G/4G connection is currently inactive

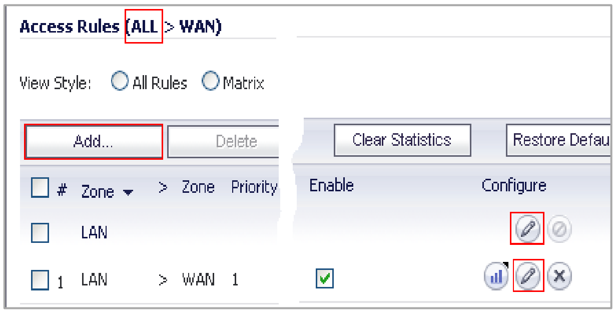
Signal Strength: No Device

Status: Ready

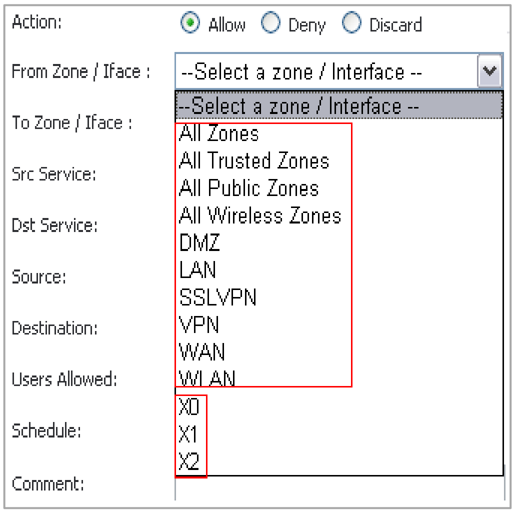
Firewall Access Rules and App Rules Extended Service Lookup

New options have been added to the **Add Rule** dialog of the **Firewall > Access Rules** page and the **Firewall > App Rules** page. Traffic can be controlled by interface and source port now. The Zone menus have been changed to Zone / Interface menus, and a new Source Port menu has been added.

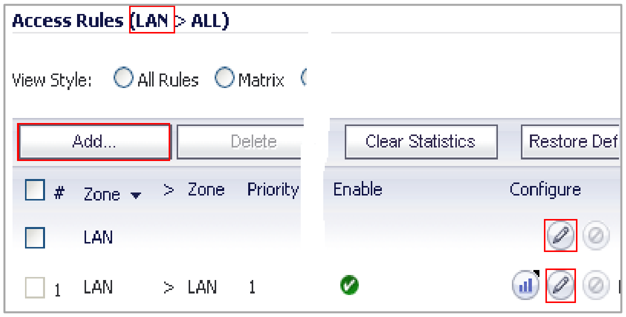
New interface options were added to the Zone / Interface menus. The options that are shown in the Zone and Interface menus depend on the view that is selected on the Access Rules page or the App Rules page. If the selected view is ALL, all zones and assigned interfaces are shown in the menus.

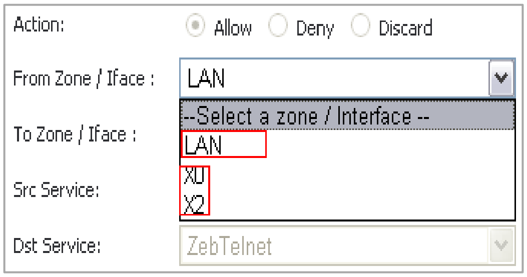


□ #	Zone	>	Zone	Priority	Enable	Configure
□	LAN					
□ 1	LAN	>	WAN	1	☑	



Otherwise, only items specified by the selected view are shown in the menus. For example, the view can also be set to LAN or WAN. If the LAN view is selected, only LAN zones and interfaces are shown in the menus.




Action: ● Allow ○ Deny ○ Discard

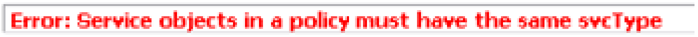
From Zone / Iface : LAN

To Zone / Iface :

Src Service:

Dst Service: ZebTelnet

The options for the Source Port menu will be the same as the options in the Service menu. The Source Port menu and the Service menus should be set to the same service types. Otherwise, the following error message is displayed:


Error: Service objects in a policy must have the same svcType

Per-IP Bandwidth Management

The **Enable Per-IP Bandwidth Management** option enables a bandwidth object to be applied to individual elements under a parent traffic class. The **Enable Per-IP Bandwidth Management** option is under the Elemental tab in the **Edit Bandwidth Object** dialog that is accessed from the **Firewall > Bandwidth Objects** page.

Advanced Bandwidth Management

Bandwidth Management (BWM) allows network administrators to guarantee minimum bandwidth and prioritize traffic. BWM is enabled in the **Firewall Settings > BWM** page. By controlling the amount of bandwidth to an application or user, the network administrator can prevent a small number of applications or users from consuming all available bandwidth. Balancing the bandwidth allocated to different network traffic and then assigning priorities to traffic improves network performance.

Three types of bandwidth management can be enabled on the **Firewall Settings > BWM** page:

- **Advanced** – Enables administrators to configure maximum egress and ingress bandwidth limitations on individual interfaces, per interface, by configuring bandwidth objects, access rules, and application policies.
- **Global** – Allows administrators to enable BWM settings globally and apply them to any interfaces. Global BWM is the default BWM setting.
- **None** – Disables BWM.

Scalability Enhancements

Several enhancements for scalability are provided in SonicOS 6.2:

- Maximum NAT Policies is increased to 1024 on the NSA 2600/3600/4600
- Maximum NAT Policies is increased to 2048 on the NSA 5600/6600 and SuperMassive 9200/9400/9600
- Maximum number of Routes is increased to 1024 on the NSA 6600 and SuperMassive 9200/9400/9600

Single Sign-On scalability enhancements are shown in the table:

	Maximum SSO Users		Maximum Web Users	
Firmware Version	Before 6.2	6.2 and above	Before 6.2	6.2 and above
NSA 2600	250	30,000	250	1,000
NSA 3600	500	40,000	300	1,500
NSA 4600	1,000	50,000	1,000	2,000
NSA 5600	2,500	60,000	1,500	3,000
NSA 6600	4,000	70,000	2,500	5,000
SuperMassive 9200	7,500	100,000	2,500	5,000
SuperMassive 9400	12,000	100,000	3,200	5,000
SuperMassive 9600	20,000	100,000	4,000	5,000

SHA-2 in IPSec

SHA-2 is a set of cryptographic algorithms used to secure IPSec traffic. SHA-2 provides a number of enhancements over its predecessor, SHA-1, to address potential security flaws. Dell SonicWALL has implemented the SHA256 variant of SHA-2.

SHA-2 can be used for Global VPN policies that are configured either manually or through the VPN wizard. If IKE is used for IPSec, SHA256 is available for both IKE and IKEv2.

If the two phases are negotiated successfully, the new algorithms are shown in the log page.

Suite B Cryptography Support

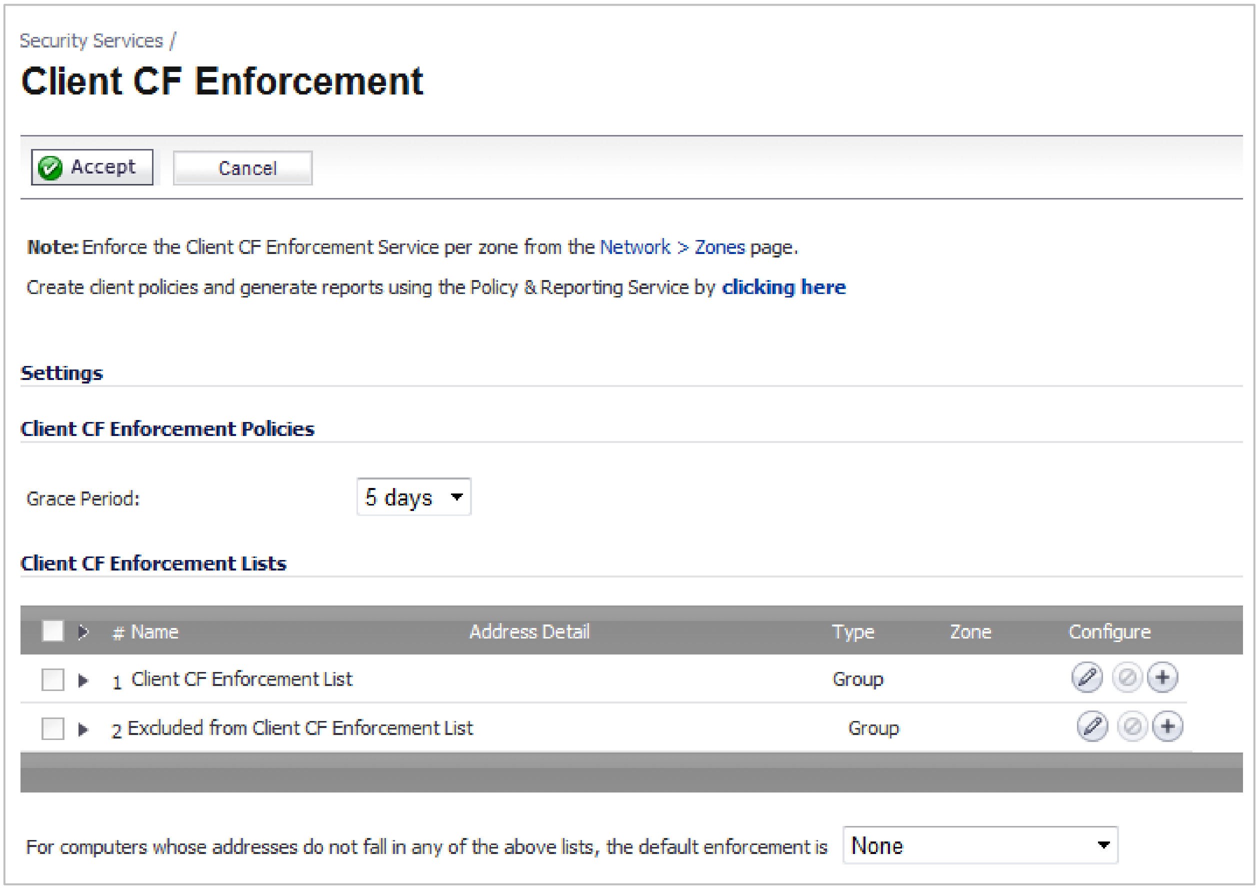
Suite B is a set of cryptographic algorithms promulgated by the National Security Agency as part of its Cryptographic Modernization Program. It is to serve as an interoperable cryptographic base for both unclassified information and most classified information.

Suite B requires a new mode of operations for some components in SonicOS. In SonicOS, SuiteB is supported in the following components:

- Internet Protocol Security (IPsec)
- Secure Shell (SSH)
- Certificates
- VPN–IKE key exchange
- VPN–IKE authentication
- VPN–Encryption/Decryption
- VPN–Digital Signatures

Client Content Filtering Service

The Dell SonicWALL Content Filtering Client service provides protection and policy enforcement for businesses, schools, libraries and government agencies by utilizing a scalable, dynamic database to block objectionable and unproductive Web content. On the **Security Services > Client CFS Enforcement** page, SonicOS provides a way to configure the licensed Content Filtering Client service. You can enforce download of the client software onto any Windows or Mac OS client systems connecting to the Internet through the Dell SonicWALL firewall, by enabling enforcement on a per-zone basis from the **Network > Zones** page.



Note: Enforce the Client CF Enforcement Service per zone from the Network > Zones page.

Create client policies and generate reports using the Policy & Reporting Service by **clicking here**

Settings

Client CF Enforcement Policies

Grace Period: 5 days

Client CF Enforcement Lists

# Name	Address Detail	Type	Zone	Configure
1 Client CF Enforcement List		Group		
2 Excluded from Client CF Enforcement List		Group		

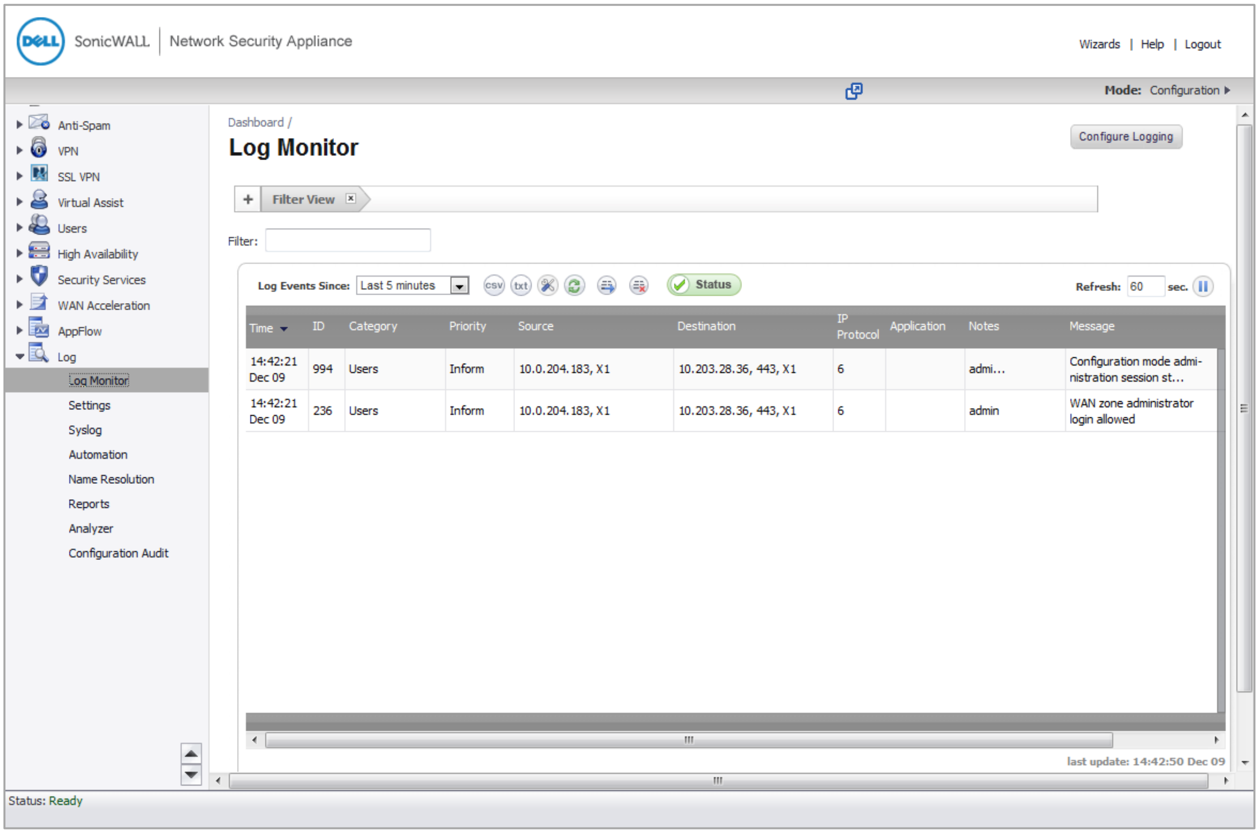
For computers whose addresses do not fall in any of the above lists, the default enforcement is None

The Content Filtering Client prevents individual users from accessing inappropriate content while reducing organizational liability and increasing productivity. Web sites are rated according to the type of content they contain. The Content Filtering Client filters access to these web sites based on their ratings and the administrator's policy settings for a user or group. Once the Content Filtering Client is installed on the machine, it continues to enforce the policy even when the client system accesses the Internet via another gateway.

The Dell SonicWALL Content Filtering Client is available with support in 5 languages including English, Japanese, Simplified Chinese, Korean and Brazilian Portuguese. On system startup, the client automatically detects the host operating system language and switches to that language (if supported). If a language is not supported, the client defaults to English.

Log > Log Monitor

The Dell SonicWALL network security appliance maintains an Event log for tracking potential security threats. This log can be viewed in the **Log > Log Monitor** page or in the **Dashboard > Log Monitor** page. Both pages have identical functionality.



Log Monitor

Filter:

Log Events Since: Last 5 minutes

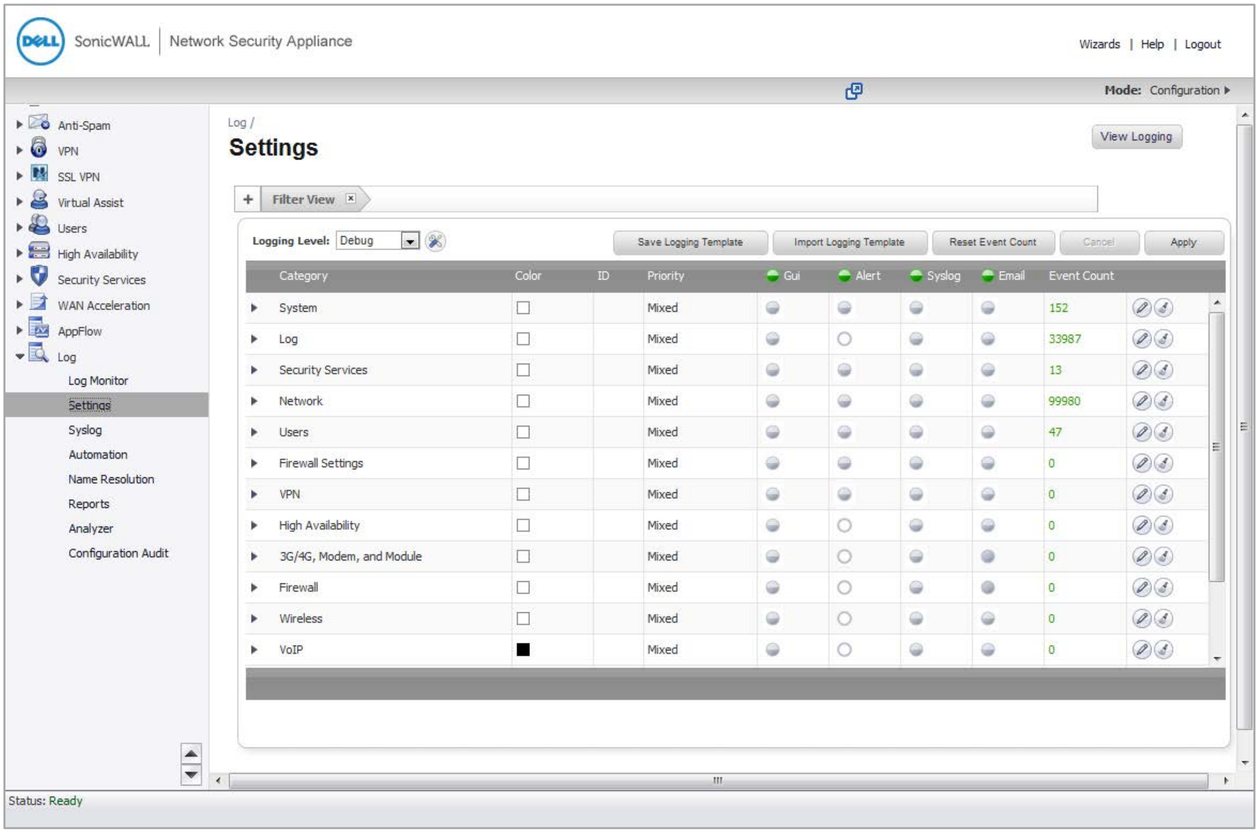
Refresh: 60 sec.

Time	ID	Category	Priority	Source	Destination	IP Protocol	Application	Notes	Message
14:42:21 Dec 09	994	Users	Inform	10.0.204.183, X1	10.203.28.36, 443, X1	6		admi...	Configuration mode administration session st...
14:42:21 Dec 09	236	Users	Inform	10.0.204.183, X1	10.203.28.36, 443, X1	6		admin	WAN zone administrator login allowed

last update: 14:42:50 Dec 09

Log > Settings

The **Log > Settings** page provides configuration tasks to enable you to categorize and customize the logging functions on your Dell SonicWALL security appliance for troubleshooting and diagnostics.

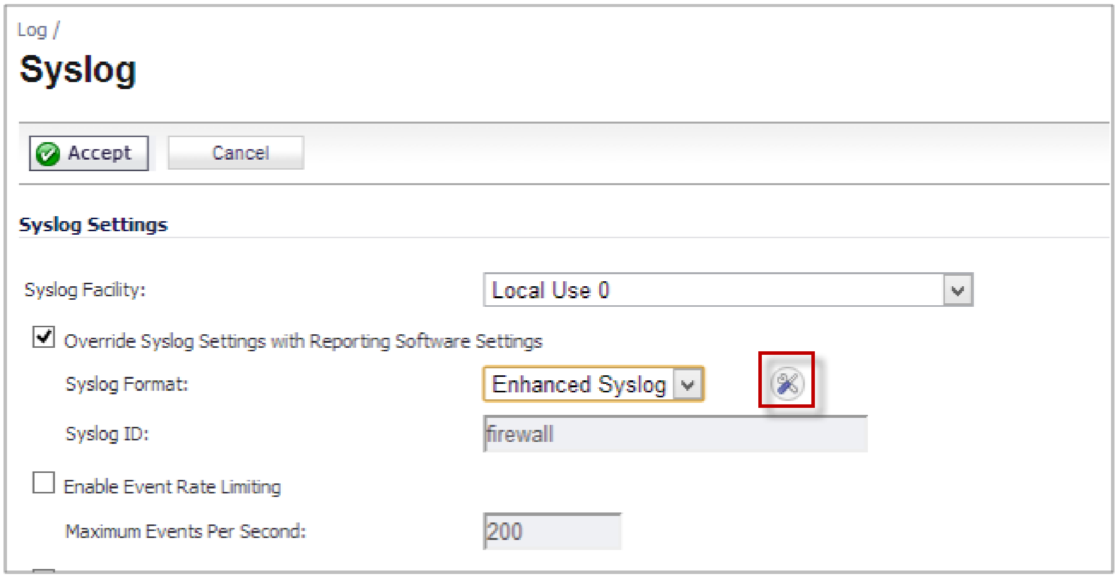


Logging Level: Debug

Category	Color	ID	Priority	Gui	Alert	Syslog	Email	Event Count
System	□		Mixed	●	●	●	●	152
Log	□		Mixed	●	○	●	●	33987
Security Services	□		Mixed	●	●	●	●	13
Network	□		Mixed	●	●	●	●	99980
Users	□		Mixed	●	●	●	●	47
Firewall Settings	□		Mixed	●	●	●	●	0
VPN	□		Mixed	●	●	●	●	0
High Availability	□		Mixed	●	○	●	●	0
3G/4G, Modem, and Module	□		Mixed	●	○	●	●	0
Firewall	□		Mixed	●	○	●	●	0
Wireless	□		Mixed	●	○	●	●	0
VoIP	■		Mixed	●	○	●	●	0

Enhanced Syslog

The Enhanced Syslog option can be selected on the **Log > Syslog** page.



Syslog Settings

Syslog Facility: Local Use 0

☑ Override Syslog Settings with Reporting Software Settings

Syslog Format: Enhanced Syslog

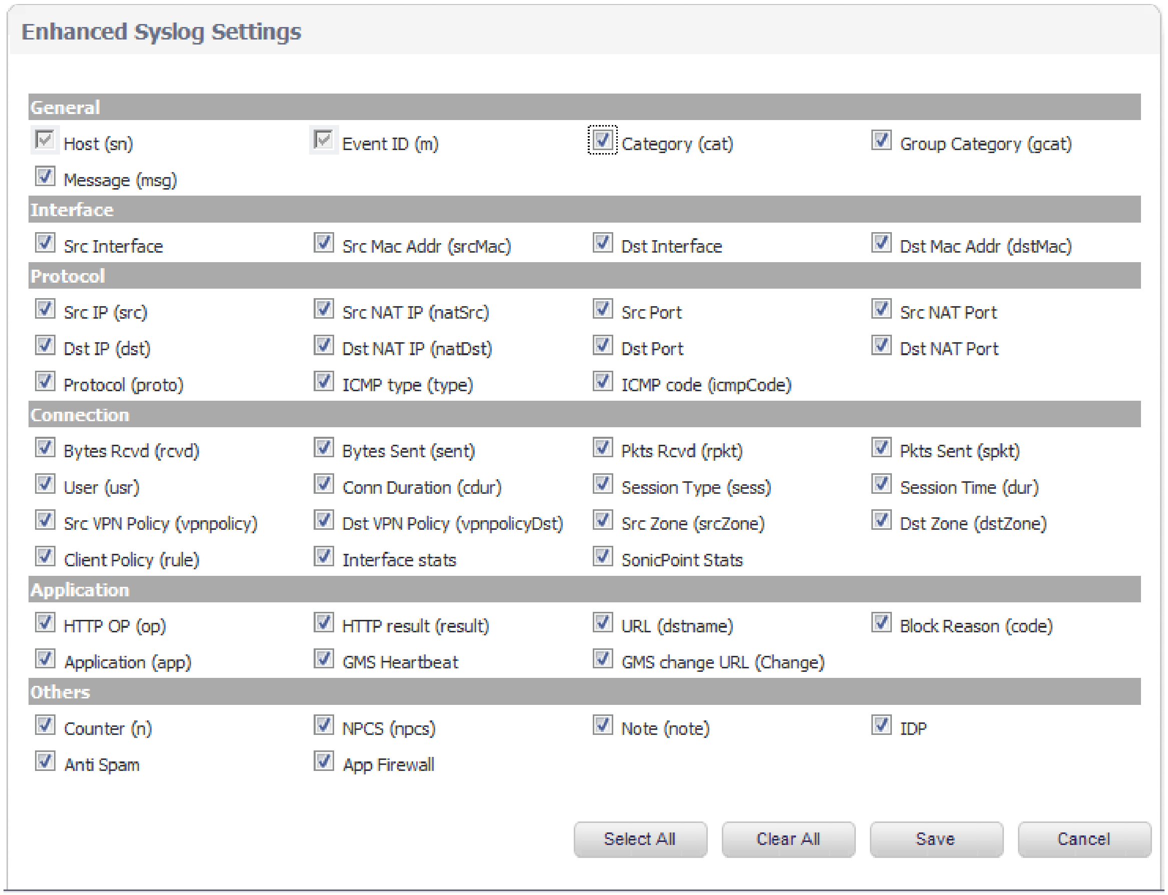
Syslog ID: firewall

□ Enable Event Rate Limiting

Maximum Events Per Second: 200

When you select the **Enhanced Syslog** option from the menu, the Configure icon becomes active. Clicking the configure icon launches the **Enhanced Syslog Settings** dialog.

The **Enhanced Syslog Settings** dialog enables you to select the specific settings that you want to log, such as which interfaces, protocols, or applications that you want Syslog to log.



Enhanced Syslog Settings

General

☑ Host (sn) ☑ Event ID (m) ☑ Category (cat) ☑ Group Category (gcat)
☑ Message (msg)

Interface

☑ Src Interface ☑ Src Mac Addr (srcMac) ☑ Dst Interface ☑ Dst Mac Addr (dstMac)

Protocol

☑ Src IP (src) ☑ Src NAT IP (natSrc) ☑ Src Port ☑ Src NAT Port
☑ Dst IP (dst) ☑ Dst NAT IP (natDst) ☑ Dst Port ☑ Dst NAT Port
☑ Protocol (proto) ☑ ICMP type (type) ☑ ICMP code (icmpCode)

Connection

☑ Bytes Rcvd (rcvd) ☑ Bytes Sent (sent) ☑ Pkts Rcvd (rpkt) ☑ Pkts Sent (spkt)
☑ User (usr) ☑ Conn Duration (cdur) ☑ Session Type (sess) ☑ Session Time (dur)
☑ Src VPN Policy (vpnpolicy) ☑ Dst VPN Policy (vpnpolicyDst) ☑ Src Zone (srcZone) ☑ Dst Zone (dstZone)
☑ Client Policy (rule) ☑ Interface stats ☑ SonicPoint Stats

Application

☑ HTTP OP (op) ☑ HTTP result (result) ☑ URL (dstname) ☑ Block Reason (code)
☑ Application (app) ☑ GMS Heartbeat ☑ GMS change URL (Change)

Others

☑ Counter (n) ☑ NPCS (npcs) ☑ Note (note) ☑ IDP
☑ Anti Spam ☑ App Firewall

Known Issues

This section contains a list of known issues in the SonicOS 6.2 release.

App Control

Symptom	Condition / Workaround	Tracking Number
An App Control existing signature is not blocking the Psiphon Proxy Access application running in SSH+ mode.	Occurs when App Control is enabled on the zone and configured to block Psiphon signatures with the ID's 7486, 10330, 10517, 5, and 10097. These signatures are blocked with Psiphon running in VPN mode or SSH mode, but are not blocked in SSH+ mode.	151710
App Rules do not filter files properly with the configured Match Object Settings.	Occurs when the Match Object Type is set to File Name and the Match Type is set to Exact Match in the Match Object Settings dialog of the Add New Match Object button on the Firewall > Match Objects page.	150967

High Availability

Symptom	Condition / Workaround	Tracking Number
In an HA pair, a wire mode paired interface link is up on one firewall, but displays “No link” on the other firewall until that firewall is restarted.	Occurs when the HA pair is configured in Active/Standby mode and X0 is configured as a wire mode interface paired to X1. Physical monitoring is enabled for X0 and X1. After connecting a computer to X1 on the secondary unit, the link appears to be up. But when connecting to X1 on the primary unit, “No link” is displayed until the firewall is restarted.	150230

Networking

Symptom	Condition / Workaround	Tracking Number
The WAN Interface gets unassigned after upgrading the firewall and attempting to use the exported settings file from SonicOS 5.9.0.6 or any of the lower 5.9 versions.	Occurs when the WAN Interface MTU is manually changed to a value that is not MTU-20 and a multiple of 8 (for example, 1450 Bytes). The default value for the WAN Interface MTU is 1500 Bytes, and this issue does not occur when the default value is used. **Workaround**: Change the WAN Interface MTU to the default value of 1500 Bytes or to a value that is MTU-20 and a multiple of 8 before upgrading. (For example, change the MTU to 1452 or 1436 Bytes.)	151877
PortShield Groups show all non-defined interfaces as "Independent" and the SonicOS admin cannot edit or modify the settings for any interface in PortShield.	Occurs when an exported settings file containing a Layer 2 Bridge Pair configuration and other settings is imported to the firewall.	151257
The firewall cannot connect to the network for up to 7 minutes.	Occurs when 512 IPv6 VLAN interfaces have been added to the firewall and the firewall is rebooted.	151097
The firewall fails to recognize the OSPF protocol in an OSPF over VPN tunnel.	Occurs when an OSPF over VPN tunnel is configured as an unnumbered tunnel on both sides of the connection between two firewalls, and route advertisement is enabled.	150957
The firewall does not auto-reset the Maximum Transmission Unit (MTU) of an “OSPF over Tunnel” VPN and the MTUs are different on the two sides of the VPN. So, the firewall cannot finish discovering its neighbor relationships.	Occurs when both sides of the VPN have Route Advertisement enabled, and the VPN status is up, and unnumbered tunnel interfaces are configured on both sides of the VPN.	150953
No configured RIPv2 over unnumbered tunnel interface routes are displayed in the routing table or in the Tech Support Report (TSR) on the firewall on one side of the connection.	Occurs when RIPv2 over unnumbered tunnel interface routes are configured on both sides of connected networks. The firewall on one side of the connection is able to learn and display the	150906

Symptom	Condition / Workaround	Tracking Number
	routes, but the firewall on the other side is not able to learn or display these routes, even though these routes can be seen when using the CLI command, “show routing rip database”.	
A virtual sub-interface in WAN PPPoE mode cannot connect to the PPPoE server.	Occurs when the admin uses the Override Default MAC Address option to change the MAC address of the parent physical interface.	150868
The user interface on the firewall stops responding.	Occurs when exporting the configuration settings.	150183
The VLAN ID 4094 is not available for the interface.	Occurs when trying to configure a LAN interface and set the VLAN Tag to 4094 in the Add Interface dialog of the Network > Interfaces page.	147768

Modules

Symptom	Condition / Workaround	Tracking Number
A 3G/4G device is sometimes not detected or activated for WAN access.	Occurs when the Huawei E1750 is inserted into a firewall which has a 3G profile configured with settings for persistence and as the primary WAN. No WAN IP address is configured for X1 (default WAN interface).	150416
A USB Modem connects to the firewall then immediately disconnects and gets removed from the Interface list.	Occurs when the firewall is restarted and the modem dials a connection.	150137

SSL VPN

Symptom	Condition / Workaround	Tracking Number
NetExtender fails to re-establish a connection automatically after the session is administratively disconnected in SonicOS. The default route is deleted on the client computer.	Occurs when using the NetExtender client on a Mac OS computer and connecting from the WAN side to establish a session, and then Tunnel All mode is enabled on the SonicOS SSL VPN > Client Routes page and the current session is disconnected on the SSL VPN > Status page.	151414
The SSL VPN connection disconnects and reconnects while running traffic.	Occurs when a WAN Zone interface is configured as an SSL VPN tunnel, and 100 NetExtender clients are connected via the SSL VPN tunnel.	149480
The SSL VPN server cannot allocate IPv6 addresses to NetExtender. Only the IPv4 addresses are available for use.	Occurs when NetExtender has been configured to use both IPv4 and IPv6 addresses, and a user tries to log in using an IPv6 address.	147897

Switching

Symptom	Condition / Workaround	Tracking Number
PCs cannot be discovered because the Link Layer Discovery Protocol (LLDP) is receiving but not transmitting.	Occurs when the firewall is connected to PCs and is configured for bi-directional (send and receive) LLDP.	149253

Upgrading

Symptom	Condition / Workaround	Tracking Number
The NSA 2600 cannot be accessed on X0 or MGMT after importing configuration settings (prefs) from another appliance.	Occurs when settings from an NSA 240 are imported to the NSA 2600, and X8 on the NSA 240 was bridged to X0. **Workaround**: Change X8 to unassigned before exporting the settings from the NSA 240 for import to the NSA 2600.	148338

Users

Symptom	Condition / Workaround	Tracking Number
A custom user group with an L2TP server configured can be deleted.	Occurs when the user group is configured for an L2TP server and the group is deleted from the Users > Local Groups page. It should not be possible to delete the group while the L2TP server is configured to it.	150224

Visualization Dashboard

Symptom	Condition / Workaround	Tracking Number
Connections that are blocked by the Cloud Anti-Virus service are displayed incorrectly on the AppFlow monitor. The Threat column displays “unspecified”, and the Sessions Flow Table is empty.	Occurs when the Cloud Anti-Virus and Gateway Anti-Virus services are enabled simultaneously, and all signatures have been downloaded.	151000

VPN

Symptom	Condition / Workaround	Tracking Number
The OSPF status changes from FULL to disabled and OSPF cannot be enabled again.	Occurs when OSPF is enabled for a tunnel VPN policy with advanced routing, and both firewalls use X0 as the borrowed interface and then the X0 IP address is changed on the local firewall.	151794
The remote VPN network is not redistributed by OSPF or RIP. The local router does not learn the remote VPN network IP routes.	Occurs when the "Redistribute remote VPN network" option is enabled and the list of Address Objects in a site-to-site VPN policy includes 97 AO's on both the local and remote firewalls, and then is changed to 2 AO's on the remote firewall.	151359

Related Technical Documentation

Dell SonicWALL Release Notes and User Guides are available on the Dell Software Support site:

https://support.software.dell.com/release-notes-product-select

Knowledge articles and links to related community forums and other resources are available on the Dell Software Support site:

https://support.software.dell.com/kb-product-select

Dell SonicWALL instructional videos are available on the Dell Software Support site:

https://support.software.dell.com/videos-product-select

Last updated: 9/23/2014