SonicWall® SonicOS 6.5 X-Series Solution

Deployment Guide

Contents

1

About the SonicWall X-Series

Topics:

SonicWall X-Series: a Unified Approach

Critical network elements, such as a firewall and switch, need to be managed, usually individually. The SonicWall® SonicOS 6.5 X-Series Solution allows unified management of the firewall and a Dell X-Series switch using the firewall management interface (UI) and GMS.

In certain deployments, the number of ports required might easily exceed the maximum number of interfaces available on the firewall. For example, the maximum number of interfaces available on SonicWall TZ firewalls range from 5 (TZ300) to 10 (TZ600); see Interfaces per firewall.

Interfaces per firewall

Firewall model	Available interfaces
SM 9600	20 (4 10 GbE SFP+, 8 1 GbE SFP, 8 1GE copper), 1 GbE Management, and 1 Console
SM 9400	20 (4 10 GbE SFP+, 8 1 GbE SFP, 8 1GE copper), 1 GbE Management, and 1 Console
NS*a* 9650	28 (10 10 GbE SFP+, 2 10 GbE, 8 2.5 GbE, 8 1 GbE) LCD Display, LCD Controls, 1 GbE Management, Dual USB Ports, and 1 Console
NS*a* 9450	
NS*a* 9250	28 (10 10 GbE SFP+, 2 10 GbE, 8 2.5 GbE, 8 1 GbE) LCD Display, LCD Controls, 1 GbE Management, Dual USB Ports, and 1 Console
SM 9200	20 (8 1 GbE SFP, 8 1GE copper, 4 10 GbE SFP+), 1 GbE Management, and 1 Console
NSA 6650	24 (6 10 GbE SFP+, 2 10 GbE, 4 2.5 GbE SFP, 8 2.5 GbE, 8 1 GbE,) 1 GbE Management, Dual USB Ports, and 1 Console
NSA 6600	20 (4 10 GbE SFP+, 8 1 GbE SFP, 8 1GE copper), 1 GbE Management, and 1 Console
NSA 5600	18 (2 10 GbE SFP+, 4 1 GbE SFP, 12 1GE copper) and 1 Management
NSA 5650	10 (2 10 GbE SFP+, 2 10 GbE, 4 2.5 GbE SFP, 4 2.5 GbE SFP, 16 1 GbE), 1 GbE Management, Dual USB Ports, and 1 Console
NSA 4650	10 (2 10 GbE SFP+, 4 2.5 GbE SFP, 4 2.5 GbE, 16 1 GbE), 1 GbE Management, Dual USB Ports, and 1 Console

Interfaces per firewall

Firewall model	Available interfaces
NSA 4600	18 (2 10 GbE SFP+, 4 1 GbE SFP, 12 1GE copper) and 1 GbE Management
NSA 3650	4 (2 10 GbE SFP+, 8 2.5 GbE SFP, 4 2.5 GbE, 12 1 GbE), 1 GbE Management, Dual USB Ports, and 1 Console
NSA 3600	18 (2 10 GbE SFP+, 4 1 GbE SFP, 12 1GE copper) and 1 Management
NSA 2650	4 (4 2.5 GbE SFP, 4 2.5 GbE, 12 1 GbE), 1 GbE Management, Dual USB Ports, and 1 Console
TZ600	10 GbE
TZ500 Series	8 GbE
TZ400 Series	7 GbE
TZ350 Series	5 GbE
TZ300P Series	5 GbE
TZ300 Series	5 GbE

With the SonicWall X-Series, ports on a Dell X-Series switch are viewed as extended interfaces of the firewall, thereby increasing the number of interfaces available for use up to 192, depending on the X-Series switch. These extended ports can be portshielded and/or configured for high availability and treated as any other interface on the firewall.

NOTE: X-Series switch, X-Switch, and extended switch are used interchangeably.

The TZ Series firewalls support a maximum of two X-Series switches. The SonicWall firewalls shown in X-Series switches supported by SonicWall firewalls support the listed X-Series switches. A SonicWall firewall can provision up to four X-Series switches.

NOTE: For complete information about X-Series switches, see the *Dell™ Networking™ X1000 and X4000 Series Switches User Guide* and the *Dell™ Networking™ X1000 and X4000 Series Switches Getting Started Guide*.

X-Series switches supported by SonicWall firewalls

These SonicWall firewalls

- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- TZ600
- TZ500/TZ500W
- TZ400/TZ400W
- TZ300/TZ300W

Support these X-Series switches (ports)

- X1008 (8 10/100/1000Base-T GbE)
- X1008P (8 10/100/1000Base-T GbE, 2 1GbE SFP fiber, 8 PoE up to 123 W total)
- X1018 (16 10/100/1000Base-T GbE, 2 1GbE SFP fiber)
- X1018P (16 10/100/1000Base-T GbE, 2 1GbE SFP fiber, 16 PoE up to 246W total)
- X1026 (24 10/100/1000Base-T GbE, 2 1GbE SFP fiber)
- X1026P (24 10/100/1000Base-T GbE, 2 1GbE SFP fiber, 24 PoE/12 PoE+ up to 369W total)
- X1052 (48 10/100/1000Base-T GbE, 2 10GbE SFP/SFP+ fiber)
- X1052P (48 10/100/1000Base-T GbE, 24 PoE/12 PoE+ up to 369W total)
- X4012 (12 10GbE SFP/SFP+ fiber)

NOTE: The SonicOS 6.5 X-Series is not supported on the SM 9800, NSA 2600, or SOHO W firewalls.

Terminology

HA High Availability

IDV Interface Disambiguation via VLAN – The reconfiguring of ports, portshielded to firewall interfaces, on the extended switch as access ports of the VLAN corresponding to the PortShield VLAN.

PoE Power over Ethernet – A system than passes electrical power along with data on Ethernet cabling, which allows a single cable to provide both data connection and electrical power to devices. PoE is the 802.3af IEEE standard with 15.4W per port.

PoE+ Power over Ethernet Plus – An enhanced version of PoE that provides more power than PoE. PoE+ is the 802.3at IEEE standard with 25.5W per port.

SFP Small form-factor pluggable – A compact, hot-pluggable transceiver used for both telecommunication and data communications applications and supports 1Gb fiber modules.

SFP+ Enhanced small form-factor pluggable – An enhanced version of SFP that supports 10 Gb fiber modules.

SPM Single Point Management

STP Spanning Tree Protocol – A network protocol that ensures a loop-free topology for Ethernet networks and allows redundant (spare) links to provide backup paths if an active link fails.

Performance Requirements

With SonicOS 6.5, X-Series switch integration functionality has been extended from just TZ Series firewalls to include both SM Series and NSA Series firewalls. A SonicOS firewall can now:

- Be provisioned for a maximum of four X-Series switches.
- Manage an increased number of ports.
- Be connected in daisy chain mode. The firewall is connected to one X-series switch, which in-turn is connected to another X-series switch.

Features Provided by the SonicWall X-Series

Key features supported by the SonicWall X-Series are:

- Provisioning an X-Series switch as an extended switch – Up to four X-Series switches can be provisioned as an extended switch on a SonicWall firewall. When provisioned, the ports on the X-Series switch are managed as are the other ports of the firewall.
- PortShield functionality – Ports on the X-Switch are viewed as “extended” interfaces of the firewall and can join PortShield Groups. For further information, see PortShield Functionality and X-Series Switches on page 7.
- Configuring the extended switch Interface settings – The switch interface settings are configured as regular interface settings through the SonicOS GUI.
- Managing the basic extended switch global parameters using GMS:
    - **STP Mode** – By default, STP mode is set to **Rapid** on the extended switch.

    - **STP State** – By default, STP is **Enabled** globally on the extended switch.

      ⓘ **NOTE:** The following PoE parameters are available only on PoE-capable extended switches.

    - **PoE Alert Usage Threshold** – By default, the threshold is set to **95**% on the extended switch.
    - **PoE Traps** – By default, traps are **disabled** globally on the extended switch.
    - **PoE Power Limit Mode** – By default, the mode is set to **Port limit** (default)
- Managing the extended switch using GMS – The X-Series switch integration feature allows unified management of both the firewall and the switch using the SonicOS management interface and SonicWall GMS version 8.1 SP1 or higher. GMS supports all configuration operations, such as provisioning of an extended switch, configuration of extended switch interface settings, and manageability of extended switch global parameters.

  For information about managing extended switches with GMS, refer to the latest *SonicWall 6.5 System Setup Administration Guide*.
- High Availability (HA) with PortShield functionality – Extended switches can be added to firewalls in an HA configuration with PortShield functionality.
- Diagnostics support for the extended switch:
    - Retrieving statistics of extended switch ports: the firewall polls the extended switch ports periodically and displays the statistics on the **External Switch Diagnostics** tab of the **Network > PortShield Groups** page.
    - Clearing statistics of extended switch ports
    - Upgrading of the firmware image, or boot image, on the extended switch
    - Restarting the extended switch
- Support for VLANs in a dedicated or common uplink configuration – VLAN is supported on extended switches with these caveats:
    - Overlapping VLANs cannot exist under firewall interfaces configured as dedicated uplinks to the same switch because the VLAN space is global on the X-Series switch. For example, if X3 and X5 are configured for dedicated uplinks, VLAN 100 cannot be present under both X3 and X5. Such a configuration is rejected. If X3 and X5 are dedicated uplinks to different X-Series switches, however, then the configuration is accepted.
    - Overlapping VLANs cannot exist under common uplink interfaces. For example, if X3 is set up as a common uplink to an X-Series switch and VLAN 100 exists under X3, another interface—X4, which is configured as a common uplink to a second X-Series switch, cannot have a VLAN 100 subinterface.

  For further information about VLAN support, see Configuring VLAN(s) With Common or Dedicated Uplink(s).
- SPM (Single Point of Management) support removes the need for a dedicated uplink for VLAN interfaces. SPM support allows a common uplink for VLAN interfaces, thereby allowing a single link between the firewall and the X-Switch to carry:
    - Management traffic of the firewall managing the X-Switch.
    - PortShield traffic for the IDV VLANs corresponding to the firewall interfaces.
    - Traffic for the VLAN subinterfaces present under the common uplink interface.

  For further information about SPM support, see Configuring a Common Uplink for VLAN(s) With SPM on page 48.
- X-Switch-related features conflict with other switching features on SM Series and NSA series firewalls, such as wiremode, port redundancy, link aggregation, and mirroring. For example, if an interface is

configured for wiremode, the interface cannot be configured as a firewall uplink to an X-Series switch and vice versa. If such a conflict occurs, the second configuration is rejected.

- PoE/PoE+ and SFP/SFP+ functionality for SonicWall firewalls by certain X-Series switches – For X-Switches that provide PoE/PoE+ functionality, see PoE/PoE+ and SFP/SFP+ Support on page 7.
- Batching configuration messages – To facilitate faster programming of X-Series switches, configuration messages can be batched before being sent to an X-Series switch.
- Dell TZ-X Daisy Chaining solution enables integration of the Firewall with Dell X-Series Switches connected in Daisy Chain mode. The feature is supported on GEN6 TZ wired, wireless platforms and on NSA and SM platforms. The feature is not be supported on NSA 2600 and SM 9800 platforms. Integration with all X-Series Switch Models such as X1008/X1008P, X1018/X1018P, X1026/X1026P, X1052/X1052P and X4012 is supported in Daisy Chain mode.

PortShield Functionality and X-Series Switches

PortShield architecture allows configuration of firewall ports into separate security zones, thereby allowing protection of a deep-packet inspection firewall for traffic between devices across zones. For more information about PortShield functionality and how to manage PortShield Groups with X-Series switches, see the *SonicOS 6.5 System Setup Administration Guide*.

Portshield Interfaces

The SonicOS 6.5 X-Series allows support for portshielding interfaces on the extended switch to firewall interfaces. X-Series switches are L2 switches, and by default, all ports on the extended switch are configured as access ports of the default VLAN 1. When ports of the extended switch are portshielded to firewall interfaces, the ports are reconfigured as access ports part of the VLAN corresponding to the PortShield VLAN, also known as the IDV VLAN of the PortShield host interface.

Portshield Traffic

Traffic between network devices connected to the ports on the extended switch:

- That are part of the same Portshield group are switched automatically by the extended switch.
- And devices connected to ports on the firewall that are part of the same Portshield group are switched by the internal switch on the firewall.
- Destined to firewall interfaces are handled by the data-path in software. Such traffic may be subjected to firewall security services such as access rules, deep packet inspection, and intrusion prevention.
- And devices connected to ports on the firewall that are part of different zone or part of a different Portshield group are forwarded by the data-path in software. Such traffic is subjected to firewall security services in software.

PoE/PoE+ and SFP/SFP+ Support

SonicWall firewalls do not support PoE/PoE+, but this functionality can be added with certain X-Series switches, as shown in X-Series switch PoE/PoE+ and SFP/SFP+ support. This additional functionality enhances SonicPoint usage by the SonicWall firewalls, especially for new SonicPoints supporting 802.11ac (802.11ac supports up to 30W maximum power; 802.11a/b/g/h supports up to 15.4 W maximum power). For further information about which ports on which models are PoE/PoE+ capable, see the *Dell™ Networking™ X1000 and X4000 Series Switches Getting Started Guide*.

Some X-Series switches also support SFP/SFP+, as shown in X-Series switch PoE/PoE+ and SFP/SFP+ support. SFP/SFP+ ports are not PoE capable, so port-based PoE settings are not available on SFP/SFP+ ports.

X-Series switch PoE/PoE+ and SFP/SFP+ support

This X-Series switch	Supports
X1008	1 PoE PD port; by default, port 8 is the PD port
X1008P	8 PoE ports, up to 123W total; by default, ports 1 through 8 support PoE
X1018	2 1GbE SFP ports; by default, ports 17 and 18 support SFP
X1018P	16 PoE ports, up to 246W total; by default, ports 1 through 16 support PoE 2 1GbE SFP ports; by default, ports 17 and 18 support SFP
X1026	2 1GbE SFP ports; by default, ports 25 and 26 support SFP
X1026P	24 PoE/12 PoE+ ports, up to 369W total; by default: • Ports 1 through 12 support PoE+ • Ports 13 through 24 support PoE 2 1GbE SFP ports; by default, ports 25 and 26 support SFP
X1052	4 10GbE SFP+ ports; by default, ports 49 through 52 support SFP+
X1052P	24 PoE/12 PoE+ ports, up to 369W total; by default: • Ports 1 through 12 support PoE+ • Ports 13 through 24 support PoE • Ports 25 through 48 support neither PoE nor PoE+ 4 10GbE SFP+ ports; by default, ports 49 through 52 support SFP+
X4012	12 10GbE SFP+ ports; by default, ports 1 through 12 support SFP+

> ⓘ **IMPORTANT:** A SonicPoint AC without an external power source must be portshielded through ports 1 through 12 on an X1026P or X1052P X-Series switch.
>
> Any non-SonicPoint AC model without an external power source can be portshielded through ports 1 through 8 (X1008P), 1 through 16 (X1018P), or 1 through 24 (X1026P and X1052P).
>
> Any SonicPoint with an external power source (AC power supply or power adapter) can be portshielded to any Ethernet port.

Configuration of the PoE/PoE+ ports on the X-Series switch is managed from the UI of the X-Series switch and the **MANAGE | System Setup| Network > Portshield Groups** page on the firewall.

SonicOS 6.5 X-Series and SonicPoints

Ports on an extended switch can be portshielded to the WLAN zone of a SonicWall firewall, and SonicPoint access points can be connected to these ports. When connecting SonicPoint access points to an X-Series switch, it is important to consider the SonicPoint's power requirements. A SonicPoint ACe/ACi/N2 access point requires a minimum of 25.5 watts. If your X-Series switch does not support PoE+, you must use a SonicPoint power injector. For which switches support PoE+, see PoE/PoE+ and SFP/SFP+ Support on page 7. For more information about managing SonicPoint access points, see the Knowledge Base article, *SonicWall TZ Series and SonicWall X-Series Solution managing SonicWall access points*.

Recommended Reading

For the SonicOS 6.5 X-Series:	*SonicWall X-Series Solution Overview* *SonicWall X-Series Solution: SonicWall integration with I X-Series Switches FAQ* *How to provision X-Series switches on SonicWall TZ series firewalls* *How to provision X-Series Switches on a SonicWall TZ High Availability pair* *How to manage X-Series switch's admin credentials and management IP through the UI and in CLI* *SonicWall X-Series Solution: Which models of X-Switches has support for POE+* *SonicWall X-Series Solution - Support for SonicWall Virtual Interfaces (VLANs)* *SonicWall TZ Series and SonicWall X-Series solution managing SonicWall access points* *SonicWall X-Series Solution– How to backup and restore X-Series switches (189204)*
For SonicOS and PortShield:	*SonicOS 6.5 System Setup Administration Guide*
For managing X-Series switches with GMS:	*SonicWall GMS OS Administration Guide*
For Dell X-Series switches:	*Dell™ Networking™ X1000 and X4000 Series Switches Getting Started Guide* *Dell™ Networking™ X1000 and X4000 Series Switches User Guide*

2

Provisioning an X-Switch on a SonicWall Appliance

ⓘ **IMPORTANT:** A firewall can be connected to one X-Series switch, which in turn can be connected to another X-Series switch in daisy chain mode.

ⓘ **IMPORTANT:** When an extended switch has been powered off and then the firewall is restarted (rebooted), it may take up to 5 minutes before the firewall discovers the extended switch and reports the **Status** of the switch as **Connected**.

When configuring extended switches in a PortShield group, it may take up to 5 minutes for the configuration to be displayed on the **MANAGE | System Setup |Network > PortShield Groups** page.

ⓘ **IMPORTANT:** By default, SSH is disabled on the management interface. You must enable SSH on the management interface to allow remote log in.

Provisioning Through the Firewall User Interface

Further information about provisioning switches can be found in:

- *How to provision X-Series switches on SonicWall TZ series firewalls*
- *How to provision X-Series Switches on a SonicWall TZ High Availability pair*
- *How to manage X-Series switch's admin credentials and management IP through the UI and in CLI*

For information about adding a default gateway through the switch’s UI, see Adding a Default Gateway Through the Firewall UI on page 18.

To provision the X-Series switch on a SonicWall firewall through the switch’s user interface:

1. On the X-Series switch, locate the white label containing the default IP address, Network Mask, user ID, and password.

Record this information as you will need it when configuring the switch on the firewall.

> ⓘ **IMPORTANT:** Apart from the initial IP address, username/password configuration, which is on a white label on the switch, no other configuration is recommended to be performed on the X-Series switch directly via the switch's GUI/console. To do so results in the firewall being out of sync with the configuration state of the X-Series switch.

2 Ensure the switch is in Managed Mode.

> ⓘ **NOTE:** If the X-Switch is not in Managed Mode, then it cannot be managed with SonicOS on the firewall. If the X-Switch is in Managed Mode, the MGMT LED is on; in Unmanaged Mode, the MGMT LED is off.

> ⓘ **TIP:** X1052/X1052P switches are delivered from the factory in Managed Mode. All other switches are delivered from the factory in Unmanaged Mode to avoid unauthorized access to the switch. For further details, see the *Dell™ Networking™ X1000 and X4000 Series Switches User Guide*.

If the switch is:

- In Managed Mode, go to Step 3.
- Not in Managed Mode, enable managed mode by inserting a paperclip into the Managed Mode opening and pressing the Managed Mode button for 7 seconds. The Managed Mode button is a small button located on the:
  - Right side of the rear panel on X1008/X1008 X-Switches.
  - Left side of the rear panel on all other X-Switches.

  Use a straightened paper clip to press the button.

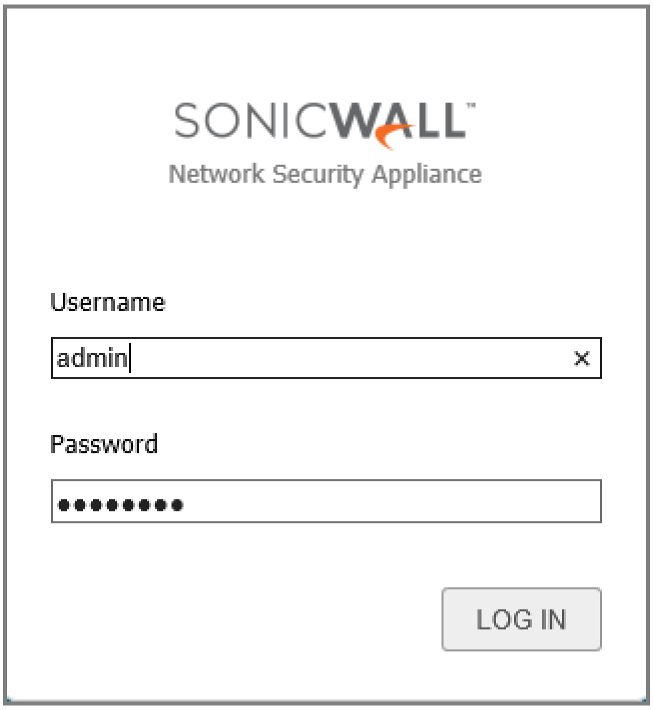
  After 7 seconds, the X-Switch reboots to change to Managed mode.

3 Connect the X-Switch console:

- By an RJ45 cable to a PC in the same subnet as the X-Switch if configuring through the switch’s GUI.
- Through Telnet (9600 baud) if configuring through the CLI.

4 Power on the X-Series switch.

5 In your PC browser, go to IP address https://10.206.53.87. The login screen for the firewall displays.



Username

admin

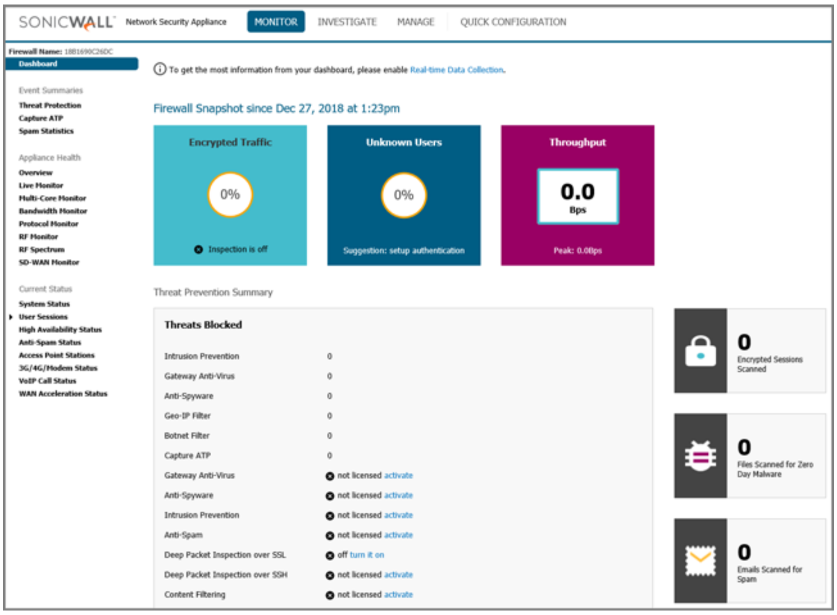
Password

••••••••

6 Log in to the firewall web-based graphical user interface (UI).

ⓘ **NOTE:** The username is **admin** and the password is **password**.

The **Initial Setup** page displays.



Firewall Name: 18B1690C26DC

ⓘ To get the most information from your dashboard, please enable Real-time Data Collection.

Firewall Snapshot since Dec 27, 2018 at 1:23pm

Encrypted Traffic: 0% — Inspection is off

Unknown Users: 0% — Suggestion: setup authentication

Throughput: 0.0 Bps — Peak: 0.0Bps

Threat Prevention Summary

Threats Blocked

Intrusion Prevention	0
Gateway Anti-Virus	0
Anti-Spyware	0
Geo-IP Filter	0
Botnet Filter	0
Capture ATP	0
Gateway Anti-Virus	not licensed activate
Anti-Spyware	not licensed activate
Intrusion Prevention	not licensed activate
Anti-Spam	not licensed activate
Deep Packet Inspection over SSL	off turn it on
Deep Packet Inspection over SSH	not licensed activate
Content Filtering	not licensed activate

0 Encrypted Sessions Scanned

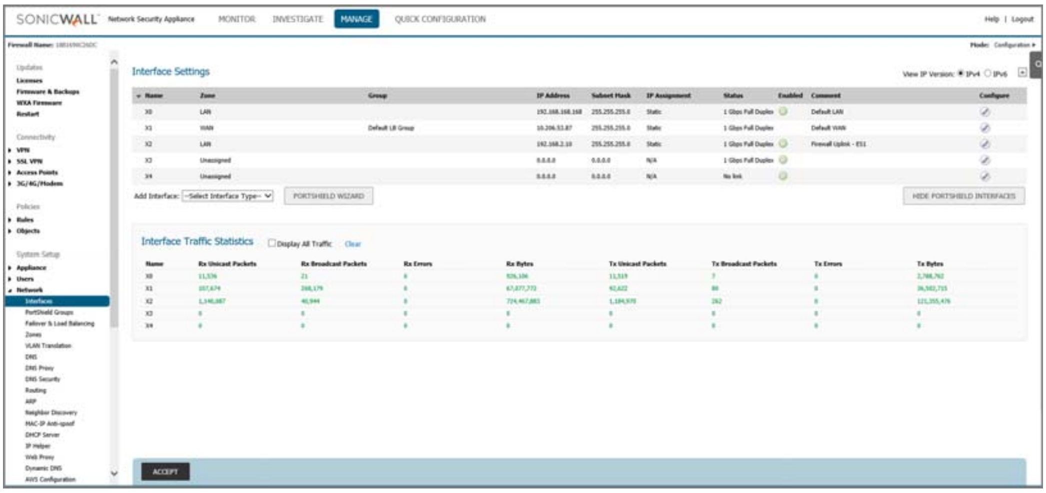
0 Files Scanned for Zero Day Malware

0 Emails Scanned for Spam

7 If you have not recorded the switch’s information in Step 1, do so now.

Interface Settings

1 Navigate to **MANAGE | System Setup | Network > Interfaces**.



Interface Settings

View IP Version: ● IPv4 ○ IPv6

Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Enabled	Comment	Configure
X0	LAN		192.168.168.168	255.255.255.0	Static	1 Gbps Full Duplex	●	Default LAN	✎
X1	WAN	Default LB Group	10.206.53.87	255.255.255.0	Static	1 Gbps Full Duplex		Default WAN	✎
X2	LAN		192.168.2.10	255.255.255.0	Static	1 Gbps Full Duplex	●	Firewall Uplink - ES1	✎
X3	Unassigned		0.0.0.0	0.0.0.0	N/A	1 Gbps Full Duplex	●		✎
X4	Unassigned		0.0.0.0	0.0.0.0	N/A	No link	●		✎

Add Interface: --Select Interface Type-- PORTSHIELD WIZARD HIDE PORTSHIELD INTERFACES

Interface Traffic Statistics □ Display All Traffic Clear

Name	Rx Unicast Packets	Rx Broadcast Packets	Rx Errors	Rx Bytes	Tx Unicast Packets	Tx Broadcast Packets	Tx Errors	Tx Bytes
X0	11,536	21	0	926,106	11,319	7	0	2,788,762
X1	107,674	268,179	0	67,077,772	92,622	80	0	36,582,715
X2	1,146,887	40,944	0	724,467,883	1,184,970	262	0	121,355,476
X3	0	0	0	0	0	0	0	0
X4	0	0	0	0	0	0	0	0

2 At the top right corner, **Mode** can be in either the **Configuration** or **Change Mode** setting. Click on the right arrow key.

3 To ensure the IP address of the firewall does not change dynamically when the DHCP server is enabled on the firewall by default, ensure **Static** is selected in the **IP Assignment** column.

NOTE: Selecting **Static** requires that you must specify a default gateway.

4 Under **Interface Settings**, choose the X-Series switch port you want and decide whether you wish to administratively shutdown the port for the X-switch under the **Enabled** column.

5 On the far right of the table, choose whether you want to **Configure** the firewall. Make sure either the **View IP Version IPv4** or **IPv6** is on. Refer to the following table for more information on the **Interface Settings**:

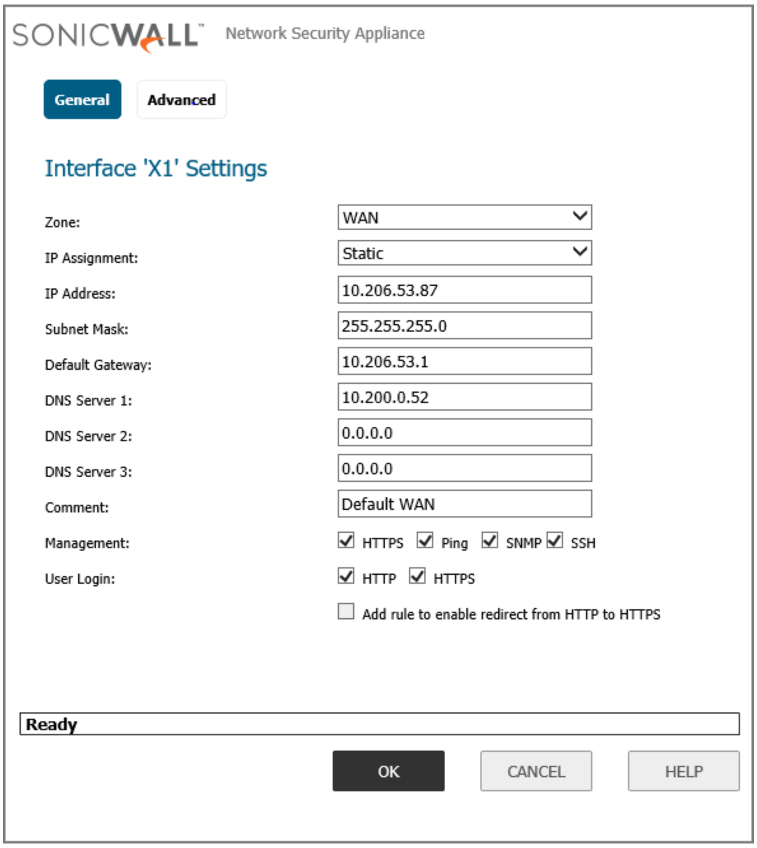
Settings	Definition
Name	The designation of the firewall
Zone	The properties of the firewall, its security type, member interfaces, interface trust, anti-virus, SEC, DPI-SSL Enforcement, and GSC
Group	Whether the firewall belongs to the Default LB Group
IP Address	The numeric address of the firewall
Subnet Mask	The numeric subdivision of the IP address
IP Assignment	The setting of the IP address, whether it is static or dynamic
Status	Whether the firewall is one gigabit port in full duplex and is able to receive one gigabit per second in both directions
Enabled	Indicates the firewall is active. Clicking on the small white checkmark inside the green circle asks you if you want to administratively shutdown a port.

Settings	Definition
Comment	Whether the default local area network (**Default LAN**) is being used or the connection is being made from the firewall (**Firewall UPlink**)
Configure	The details needed to make your firewall work properly

6 **Select Interface Type** by At the bottom of the **Interface Settings** table, click on the drop-down menu icon next to **Add Interface** to **Select Interface Type.** Refer to the following table for more information on the interface choices:

Interface Type	Definition
Virtual Interface	A software-based interface created in the memory of the firewall
VPN Tunnel Interface	A virtual private network interface on a security gateway that connects to a remote peer
WLAN Tunnel Interface	A wireless local area network (WLAN) interface on a security gateway that connects to a remote peer
4to6 Tunnel Interface	Tunneling of IPv4 in an IPv6 only network

7 On the far right of the table, under the **Configure** column, click the small pencil inside the circle icon to set up your firewall. The dialog box below appears.



Interface 'X1' Settings

Zone:	WAN
IP Assignment:	Static
IP Address:	10.206.53.87
Subnet Mask:	255.255.255.0
Default Gateway:	10.206.53.1
DNS Server 1:	10.200.0.52
DNS Server 2:	0.0.0.0
DNS Server 3:	0.0.0.0
Comment:	Default WAN
Management:	☑ HTTPS ☑ Ping ☑ SNMP ☑ SSH
User Login:	☑ HTTP ☑ HTTPS
	□ Add rule to enable redirect from HTTP to HTTPS

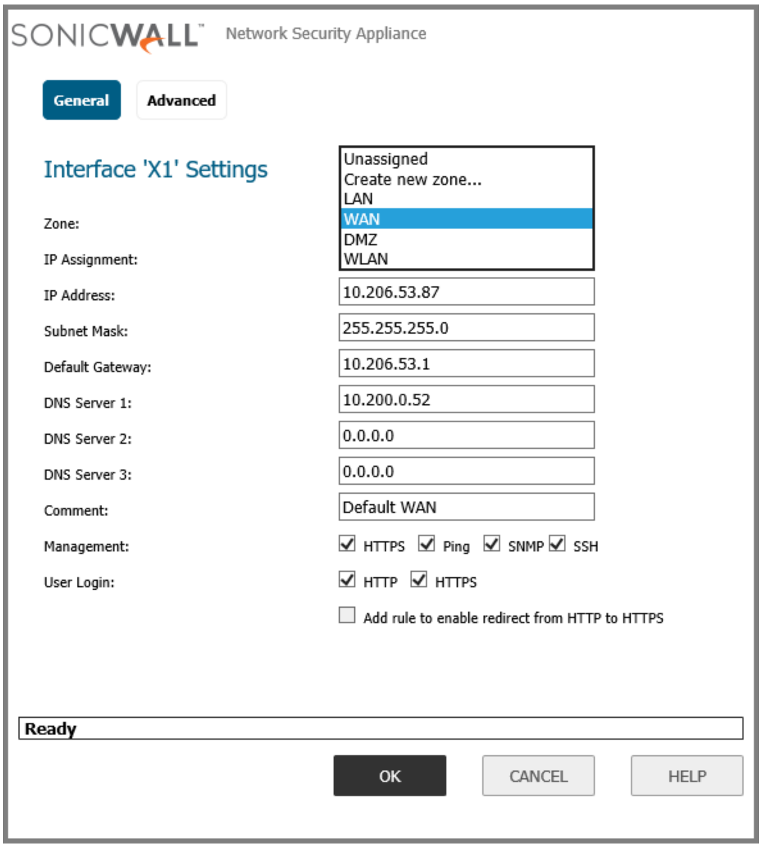
Ready

8 Click **OK.**

Configuring the firewall Zone:

1 The **Zone** configuration is displayed in the pop-up dialog (see below image) of the firewall.

2 Configure the interface as **WAN**, which is the default.



Interface 'X1' Settings

Zone: WAN

IP Assignment:

IP Address: 10.206.53.87

Subnet Mask: 255.255.255.0

Default Gateway: 10.206.53.1

DNS Server 1: 10.200.0.52

DNS Server 2: 0.0.0.0

DNS Server 3: 0.0.0.0

Comment: Default WAN

Management: ☑ HTTPS ☑ Ping ☑ SNMP ☑ SSH

User Login: ☑ HTTP ☑ HTTPS

□ Add rule to enable redirect from HTTP to HTTPS

Ready

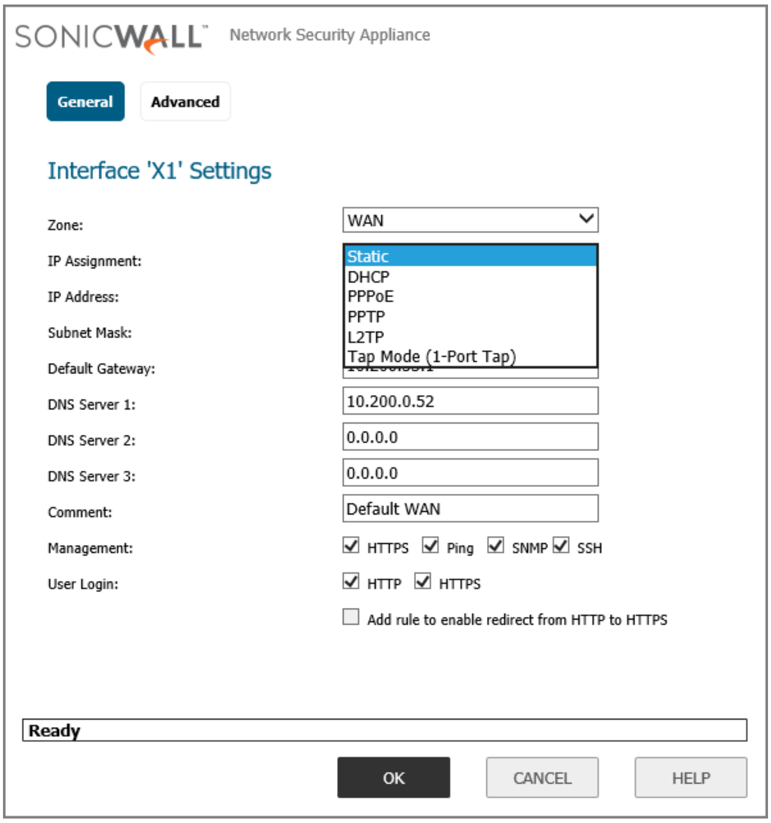
3 Refer to the following table for more information on the Configuration zones available from the drop-down menu:

Zone	Definition
Unassigned	An interface without a link that's disabled
Create new zone	Connecting a serial cable directly to the firewall or via SSH
LAN	Local Area Network
DMZ	The demilitarized zone, perimeter network or screened subnetwork
WLAN	Wireless Local Area Network

Configuring the firewall IP Assignment:

1 The **IP Assignment** configuration is displayed in the pop-up dialog (see below image) of the firewall.

2 Configure the interface as **Static,** which is the default.



SONICWALL Network Security Appliance

General | Advanced

Interface 'X1' Settings

Zone: WAN

IP Assignment: Static

IP Address:

Subnet Mask:

Default Gateway:

DNS Server 1: 10.200.0.52

DNS Server 2: 0.0.0.0

DNS Server 3: 0.0.0.0

Comment: Default WAN

Management: ☑ HTTPS ☑ Ping ☑ SNMP ☑ SSH

User Login: ☑ HTTP ☑ HTTPS

□ Add rule to enable redirect from HTTP to HTTPS

Ready

3 Refer to the following table for more information on the Configuration **IP Assignments** from the drop-down menu:

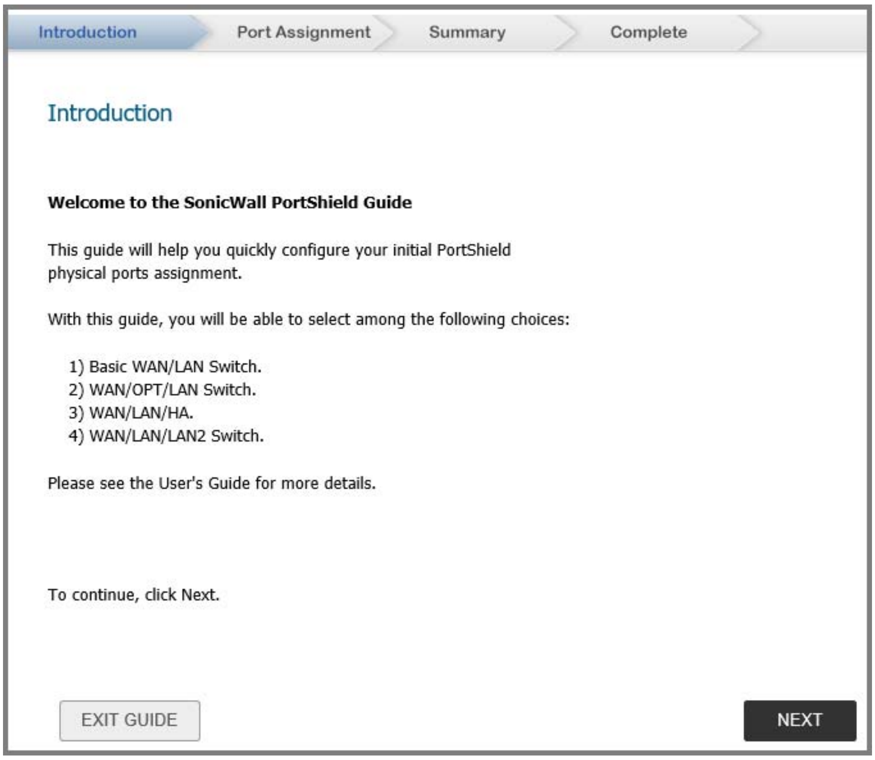
IP Assignment	Definition
Static	A fixed Internet Protocol (IP) address number assigned to the network device by an administrator
DHCP	A Dynamic Host Configuration Protocol used by the server to dynamically assign an IP address to the network device
PPPoE	Point-to-Point Protocol over Ethernet
L2TP	Layer 2 Tunneling Protocol over an IP network
Tap Mode (1 Port Tap)	Deployment option also known as wire mode that does not take any IP address and it typically configured as a bridge between a pair of interfaces

Portshield Wizard

1 Click the **PORTSHIELD WIZARD** button at the bottom of the **Interface Settings** table to display the popup **SonicWall Portshield Guide** to learn about several common Portshield group configurations.

2 The Guide is made up of four sections: **Introduction**, **Port Assignment**, **Summary**, and **Complete**. Click the **NEXT** button at the bottom right of the guide to move through the sections.

3 Click the **EXIT GUIDE** button at the bottom left to leave the guide. A message from the webpage will appear informing you that if you exit the guide your changes will not be saved. Click **OK** or **Cancel**.



Introduction

Welcome to the SonicWall PortShield Guide

This guide will help you quickly configure your initial PortShield physical ports assignment.

With this guide, you will be able to select among the following choices:

1) Basic WAN/LAN Switch.
2) WAN/OPT/LAN Switch.
3) WAN/LAN/HA.
4) WAN/LAN/LAN2 Switch.

Please see the User's Guide for more details.

To continue, click Next.

Show Portshield Interfaces

1 Click the **SHOW PORTSHIELD INTERFACES** button at the bottom right of the **Interface Settings** table to display the Portshield interfaces. The Portshield interfaces are shown.

2 Click the **HIDE PORTSHIELD INTERFACES** button at the bottom right of the **Interface Settings** table to hide the Portshield interfaces. The Portshield interfaces are hidden.

Interface Traffic Statistics

The Interface Traffic Statistics table lists, for each interface, received and transmitted information for all configured interfaces, including VLAN sub-interfaces.

1 Check the box next to **Display All Traffic** to see the transmitted and received bytes over all interfaces.

2 Click the **Accept** button at the bottom of the table.

3 Click **Clear** to clean the transmitted and received bytes over all interfaces.

4 Click the **Accept** button at the bottom of the table. Refer to the following table for more information on the Interface Traffic Statistics:

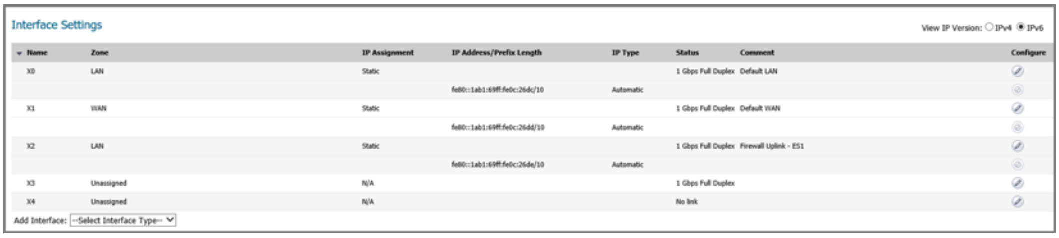
Interface Traffic Statistics	Definition
Name	The name of the firewall you want to display information for
RX Unicast Packets	Indicates the number of point-to-point communications received by the interface
Rx Broadcast Packets	Indicates the number of multi-point communications received by the interface

Interface Traffic Statistics	Definition
Rx Errors	Indicates the number of error packets received on the selected interface
Rx Bytes	Indicates the volume of data, in bytes, received by the interface
Tx Unicast Packets	Indicates the number of point-to-point communications transmitted by the interface
Tx Broadcast Packets	Indicates the number of multipoint communications transmitted by the interface
Tx Errors	Indicates the number of error packets transmitted on the selected interface
Tx Bytes	Indicates the volume of data, in bytes, transmitted by the interface

Adding a Default Gateway Through the Firewall UI

To add a default gateway to a firewall through its UI:

1 In the firewall UI, go to **View IP Version** in the top right corner above the table. Click on either **IPv4** or **IPv6**.



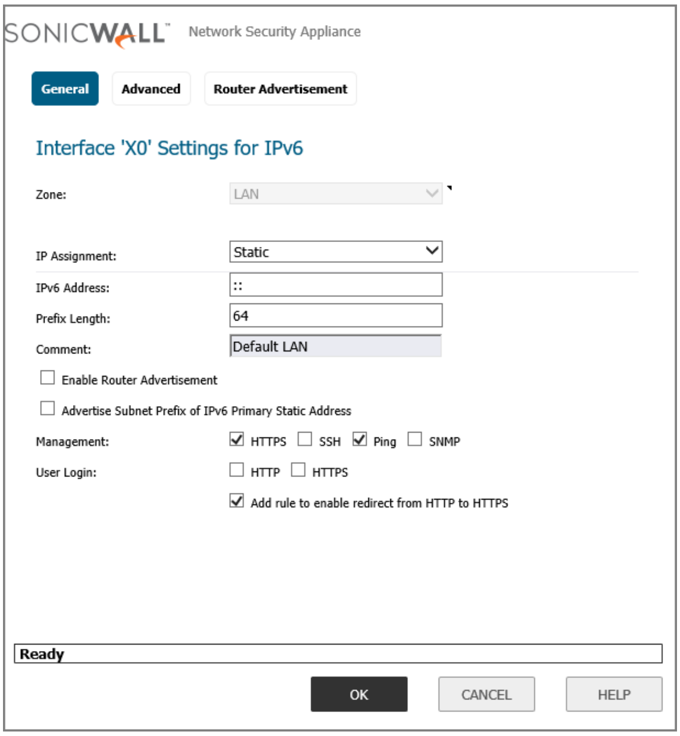
Interface Settings

View IP Version: ○ IPv4 ● IPv6

Name	Zone	IP Assignment	IP Address/Prefix Length	IP Type	Status	Comment	Configure
X0	LAN	Static			1 Gbps Full Duplex	Default LAN	
			fe80::1ab1:69ff:fe0c:26dc/10	Automatic			
X1	WAN	Static			1 Gbps Full Duplex	Default WAN	
			fe80::1ab1:69ff:fe0c:26dd/10	Automatic			
X2	LAN	Static			1 Gbps Full Duplex	Firewall Uplink - ES1	
			fe80::1ab1:69ff:fe0c:26de/10	Automatic			
X3	Unassigned	N/A			1 Gbps Full Duplex		
X4	Unassigned	N/A			No link		

Add Interface: --Select Interface Type--

2 Click on the **Configure** edit button, with the small pencil inside it, in the far right to enter the default gateway IP address in the **IPv6 Address** field.



Interface 'X0' Settings for IPv6

Zone: LAN

IP Assignment: Static

IPv6 Address: ::

Prefix Length: 64

Comment: Default LAN

☐ Enable Router Advertisement

☐ Advertise Subnet Prefix of IPv6 Primary Static Address

Management: ☑ HTTPS ☐ SSH ☑ Ping ☐ SNMP

User Login: ☐ HTTP ☐ HTTPS

☑ Add rule to enable redirect from HTTP to HTTPS

Ready

3 Enter the default gateway IP address in the **IPv6 Address** field.

4 Click **OK**.

Provisioning Through the CLI

Topics:

- Provisioning Without a Default Gateway on page 19
- Provisioning With a Default Gateway on page 20

Provisioning Without a Default Gateway

ⓘ | **IMPORTANT:** This is the recommended way.

To provision the X-Series switch on a SonicWall firewall without a default gateway:

1 Provision the X-Series switch by performing Step through Step 6 in Provisioning Through the Firewall User Interface on page 10.

2 Enter the following CLI commands:

```
console#configure terminal
console(config)#username admin <password>
console(config)#interface vlan 1
console(config-if)#ip address 192.168.2.2
console(config-if)#end
console#write memory
```

3 Ensure the firewall can reach the X-Series switch by pinging the switch from the firewall before provisioning/managing the switch from the firewall.

Provisioning With a Default Gateway

To provision the X-Series switch on a SonicWall firewall with a default gateway:

1 Provision the X-Series switch by performing Step through Step 6 in Provisioning Through the Firewall User Interface on page 10.

2 Enter the following CLI commands:

```
console#configure terminal
console(config)#username admin <password>
console(config)#interface vlan 1
console(config-if)#ip address 192.168.2.3
console(config-if)#exit
console(config)#ip default-gateway 192.168.2.2
console(config)#end
console#write memory
```

3 Ensure the firewall can reach the X-Series switch by pinging the switch from the firewall before provisioning/managing the switch from the firewall.

3

Adding the X-Series Switch to SonicOS

Adding an Extended Switch

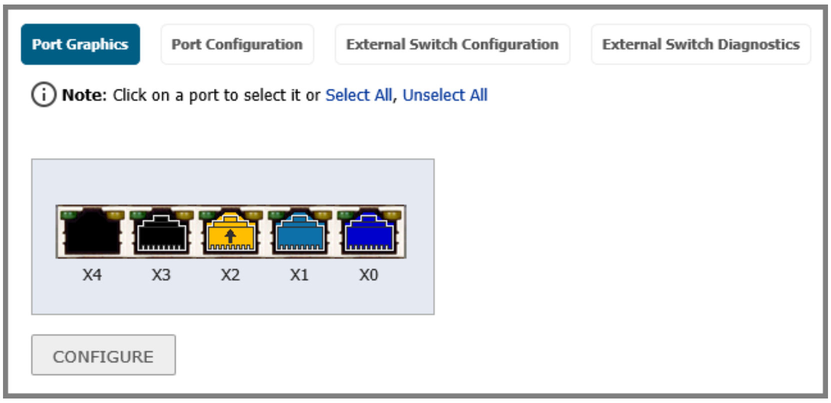
> ⓘ **NOTE:** To manage the X-Series switch from the firewall, one of the interfaces of the firewall needs to be in the same subnet as the X-Series switch. For example, to manage an X-Series switch with a default IP of `192.168.2.3`, an interface of the firewall needs to be configured in the `192.168.2.0` subnet and connected to the X-Series switch.

To add an extended switch:

1 Set up the switch as described in Provisioning Through the Firewall User Interface on page 10.

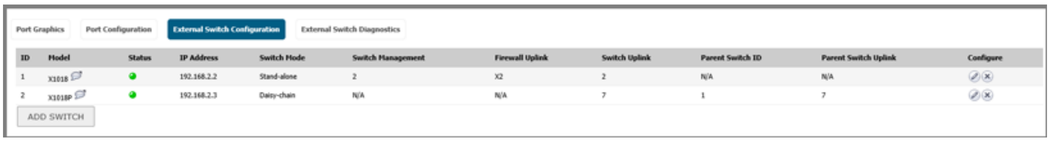
2 Ping the switch to ensure the firewall can interact with the switch.

3 Navigate to **MANAGE |System Setup | Network > PortShield Groups** page.



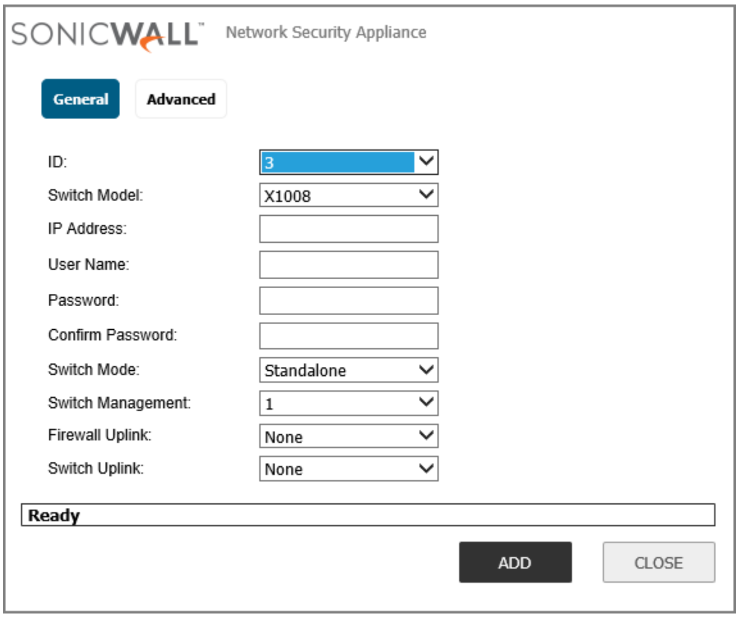
ⓘ **Note:** Click on a port to select it or Select All, Unselect All

4 Click **External Switch Configuration**.



ID	Model	Status	IP Address	Switch Mode	Switch Management	Firewall Uplink	Switch Uplink	Parent Switch ID	Parent Switch Uplink	Configure
1	X1018	●	192.168.2.2	Stand-alone	2	X2	2	N/A	N/A	
2	X1018P	●	192.168.2.3	Daisy-chain	N/A	N/A	7	1	7	

5 Click the **ADD SWITCH** button. The **Add External Switch** dialog displays.



ID: 3
Switch Model: X1008
IP Address:
User Name:
Password:
Confirm Password:
Switch Mode: Standalone
Switch Management: 1
Firewall Uplink: None
Switch Uplink: None

Ready

6 From the **ID** drop-down menu, select the ID of the switch. The default is **1**.

7 From the **Switch Model** drop-down menu, select the model of the external switch. The default is **X1008**.

8 In the **IP Address** field, enter the IP address of the switch obtained from the label on the switch.

9 In the **User Name** field, enter the user ID obtained from the label on the switch.

10 In the **Password** field, enter either the password obtained from the label on the switch or the one you gave when installing the switch.

11 In the **Confirm Password** field, enter the password a second time.

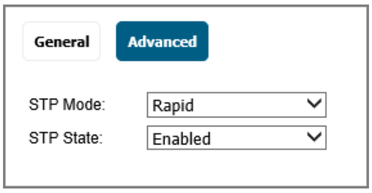
> ⓘ **TIP:** For how to configure the **Switch Management**, **Firewall Uplink**, and **Switch Uplink** options, see the subsection for your topology in Configuring the SonicOS 6.5 X-Series in Various Topologies on page 28.

12 From the **Switch Management** drop-down menu, select the port on the extended switch to be used for management traffic. The default is **1**.

13 From the **Firewall Uplink** drop-down menu, select the port on the firewall to be used as the uplink port. The default is **None**.

14 From the **Switch Uplink** drop-down menu, select the port on the extended switch to be used as the uplink port. The default is **None**.

15 Optionally, click the **Advanced** tab. The options on the tab depend on the extended switch you are adding:



STP Mode: Rapid

STP State: Enabled

16 From the **STP Mode** drop-down menu, select:

- **Classic**
- **Rapid** (default)
- **Multiple**

17 From the **STP State** drop-down menu, select:

- **Disabled**
- **Enabled** (default)

Adding an Extended Switch in Daisy Chain Mode

You can connect extended TZ-300 X-Series switches in daisy chain mode. The feature allows the integration of the firewall with the switches. The feature is supported on GEN6 TZ wired, wireless platforms and on NSA and SM platforms.

To add an extended switch in daisy chain mode:

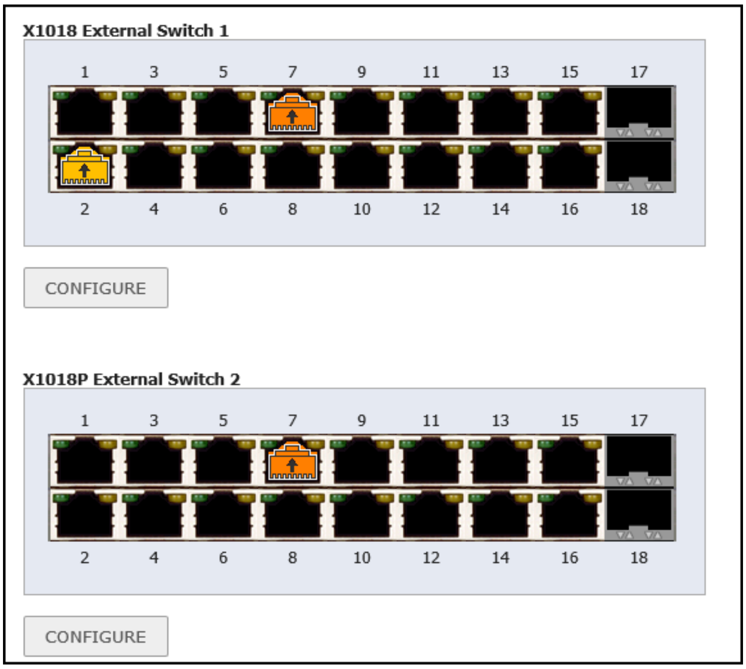
1 Log in using the X1 interface by going to the web user interface IP address https://10.206.53.87.

2 Enter the user name **admin** and the password **password**.

3 See the daisy chain X-switch configuration in the **MANAGE |System Setup | Network > PortShield Groups** page.

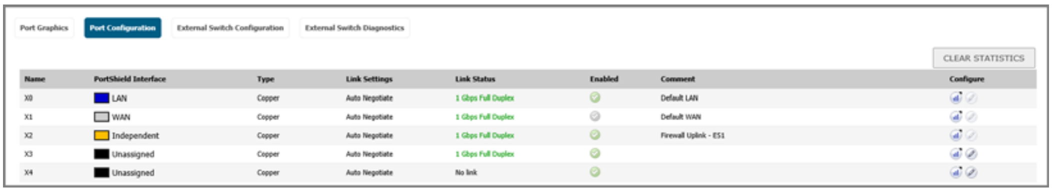
4 Click **Port Graphics** to see the **X1018 External Switch 1 (ES1)** and the **X1018P External Switch 2 (ES2)** connected to each other on **port 7** of both switches in daisy chain mode. They are designated as ES1:7 and ES2:7:

- **Port 2** of **X1018 of ES1** is the **Switch MGMT/Uplink** to **X2**.
- **Port 7** of **X1018 ES1** is the **Parent Switch Uplink to Child Switch ES2:7**.
- **Port 7** of **X1018P ES2** is the **Child Switch Uplink to Parent Switch ES1:7**. This is the one connected in daisy chain mode.



5 Click **Port Configuration** to identify your switch. Refer to the following table for more information on the **Port Configuration** settings:

Settings	Definition
Name	The designation of the X-switch
PortShield Interface	The virtual interface with a set of ports assigned to it.
Type	Whether it is copper or fiber optics
Link Settings	Auto negotiate is the default
Link Status	Whether it is 1Gbps Full Duplex or no link
Enabled	The setting of the IP address, whether it is static or dynamic
Comment	Any user-defined comments
Configure	The details needed to make your X-switch work properly



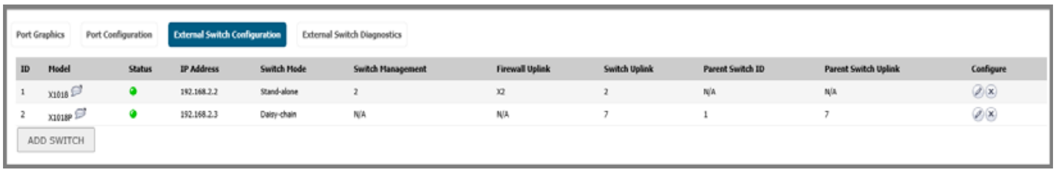
Name	PortShield Interface	Type	Link Settings	Link Status	Enabled	Comment	Configure
X0	LAN	Copper	Auto Negotiate	1 Gbps Full Duplex	✓	Default LAN	
X1	WAN	Copper	Auto Negotiate	1 Gbps Full Duplex	○	Default WAN	
X2	Independent	Copper	Auto Negotiate	1 Gbps Full Duplex	✓	Firewall Uplink - ES1	
X3	Unassigned	Copper	Auto Negotiate	1 Gbps Full Duplex	✓		
X4	Unassigned	Copper	Auto Negotiate	No link	✓		

NOTE: Use the **CLEAR STATISTICS** button at the top right corner of the **Port Configuration** table to clear the data, if desired.

6 Click **External Switch Configuration** to identify and configure your switch. Refer to the following table for more information on the **External Switch Configuration** settings:

Settings	Definition
ID	The designation of the X-switch
Model	The product detail information, name, and interfaces.

Settings	Definition
Status	Displays a green circle when the switch is on. Displays a red circle when the switch is not reachable from the SonicWall appliance.
IP Address	The numeric address of the computer on the Internet to access the switch
Switch Mode	Whether the switch is connected as a stand alone or in daisy chain mode
Switch Management	How many switches are being managed from a remote location using protocols such as VLAN
Firewall Uplink	Whether the default local area network (**Default LAN**) is being used or the connection is being made from the firewall (**Firewall UPlink**)
Switch Uplink	Need help with this definition.
Parent Switch ID	The identification of the main switch
Parent Switch Uplink	The identification of the that the main switch is using from the firewall
Configure	The details needed to make your X-switch work properly



ID	Model	Status	IP Address	Switch Mode	Switch Management	Firewall Uplink	Switch Uplink	Parent Switch ID	Parent Switch Uplink	Configure
1	X1018	●	192.168.2.2	Stand-alone	2	X2	2	N/A	N/A	
2	X1018P	●	192.168.2.3	Daisy-chain	N/A	N/A	7	1	7	

7 Click **External Switch Diagnostics** for testing purposes or to check the hardware functionality while it is connected to the network.

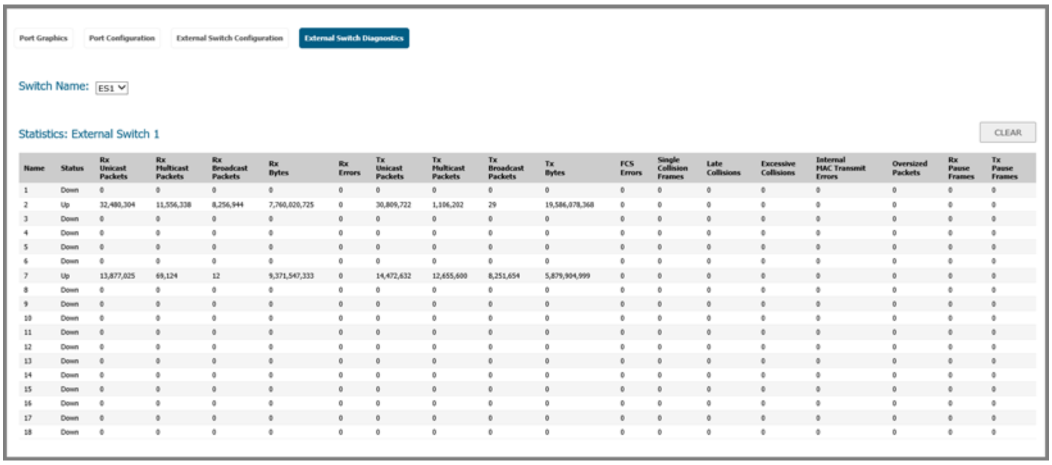
8 Go to the **Switch Name** drop-down menu, on the top left above the table, to choose the switch you want.

- **ES1** and **ES2** will display.

9 The **Statistics** table displays data depending on the switch you choose. Refer to the following table for more information on the **External Switch Diagnostics** settings.

Settings	Definition
Name	Port name, 1 - n.
Status	Whether the port is **Up** or **Down**
Rx Unicast Packets	Indicates the number of point-to-point communications received by the interface.
Rx Multicast Packets	Indicates the number of good multicast packets received on the selected interface.
Rx Broadcast Packets	Indicates the number of multi-point communications received by the interface.
Rx Bytes	Indicates the volume of data, in bytes, received by the interface.
Rx Errors	Indicates the number of error packets received on the selected interface.
Tx Unicast Packets	Indicates the number of multi-point communications received by the interface
Tx Multicast Packets	Indicates the number of multicast packets transmitted from the selected interface.

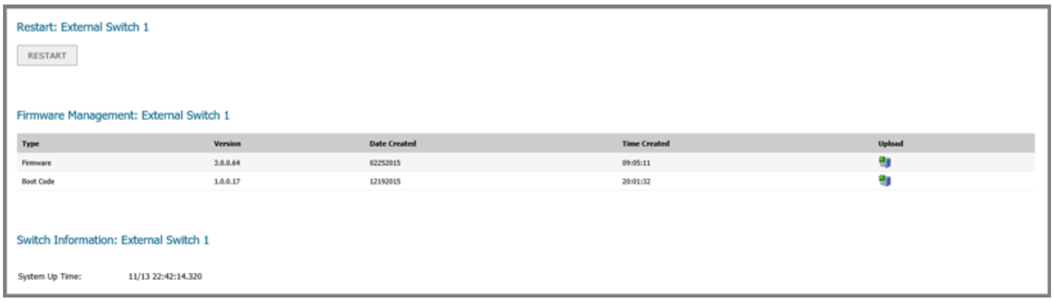
Settings	Definition
Tx Broadcast Packets	Indicates the number of multi-point communications transmitted by the interface.
Tx Bytes	Indicates the volume of data, in bytes, transmitted by the interface.
FCS Errors	A frame check sequence (FCS) error-detecting code added to a frame in a communications protocol.
Single Collision Frames	Two devices on the same Ethernet network attempting to transmit data at the same time.
Late Collisions	Any collision that occurs after 512 bits of the frame have been transmitted.
Excessive Collisions	Number of frame collisions detected that exceeded the number of retries on the port.
Internal MAC Transmit Errors	Number of non-collision transmission errors detected on the port.
Oversized Packets	Number of received packets larger than the port was expecting.
Rx Pause Frames	Number of pause frames received by the port.
Tx Pause Frames	Number of pause frames sent by the port.



Switch Name: ES1

Statistics: External Switch 1

Name	Status	Rx Unicast Packets	Rx Multicast Packets	Rx Broadcast Packets	Rx Bytes	Rx Errors	Tx Unicast Packets	Tx Multicast Packets	Tx Broadcast Packets	Tx Bytes	FCS Errors	Single Collision Frames	Late Collisions	Excessive Collisions	Internal MAC Transmit Errors	Oversized Packets	Rx Pause Frames	Tx Pause Frames
1	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Up	32,480,304	11,556,338	8,256,944	7,760,020,725	0	30,809,722	1,106,202	29	19,586,078,368	0	0	0	0	0	0	0	0
3	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	Up	13,877,025	69,124	12	9,371,547,333	0	14,472,632	12,655,600	8,251,654	5,879,904,999	0	0	0	0	0	0	0	0
8	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0



Restart: External Switch 1

Firmware Management: External Switch 1

Type	Version	Date Created	Time Created	Upload
Firmware	3.0.0.64	02252015	09:05:11	
Boot Code	1.0.0.17	12192015	20:01:32	

Switch Information: External Switch 1

System Up Time: 11/13 22:42:14.320

10 Under **Restart: External Switch 1**, click the **RESTART** button to restart the switch. A popup dialog will appear asking if you are sure you want to start again. Click **OK** or **Cancel**.

11 The **Firmware Management: External Switch 1** table displays five columns: **Type**, **Version**, **Date Created**, **Time Created**, and **Upload**.

- Two types of switches appear under **Type**: **Firmware** and **Boot Code**.

- Click **Upload** to transfer your switch data to the server.

12 Under **Switch Information: External Switch 1** you can see the **System Up Time**.

Deleting an Extended Switch

To delete an extended switch:

1 Navigate to the **MANAGE | System Setup | Network > PortShield Groups** page.

2 Click **External Switch Configuration**.

3 Find the switch by its name under the gray Product Details bar that shows its name and model.

4 Under the Product Details bar on the far right, below **Configure**, click the **x** inside the circle to delete the switch.

ⓘ **IMPORTANT:** A popup dialog box appears with a message from the web page asking you if you are sure you wish to delete the switch.

5 Click **OK**.

Replacing an Extended Switch

Navigate to **MANAGE | System Setup | Network > PortShield Groups** page and replace the extended switch by following one of the two steps described below.

1 Delete the switch from the firewall UI by following the instructions on Deleting an Extended Switch. Physically replace the switch and configure the new switch with a static IP address. Then, re-provision the switch on the firewall UI.

2 Without deleting the switch from the firewall UI, physically replace the switch, configure the new switch with the same static IP address as the replacement switch, connect the switch to the firewall and reboot the firewall.

ⓘ **NOTE:** The firewall already has the switch provisioned in its settings and should reprogram the switch based on its configuration.

4

Configuring the SonicOS 6.5 X-Series in Various Topologies

ⓘ **IMPORTANT:** Before setting up the interface between the SonicWall firewall and the X-Series switch, set up the switch as described in Provisioning an X-Switch on a SonicWall Appliance on page 10.

ⓘ **IMPORTANT:** When an extended switch has been powered off and then the firewall is restarted (rebooted), it may take up to 5 minutes before the firewall discovers the extended switch and reports the **Status** of the switch as **Connected**.

When configuring extended switches in a PortShield group, it may take up to 5 minutes for the configuration to be displayed on the **MANAGE | System Setup | Network > PortShield Groups** page.

About Topologies

The key supported topologies for the SonicOS 6.5 X-Series are:

- Common uplink configuration
- Dedicated uplink configuration
- Hybrid configuration with common and dedicated uplink(s)
- Isolated links configuration for management and data traffic
- HA and PortShield configurations with dedicated uplink(s)
- HA and PortShield configurations with common uplink(s)

- VLAN(s) with dedicated uplink(s) configuration
- SonicPoints with dedicated uplink configuration

About Links

A common link carries data and management traffic. Common links carry all PortShield traffic and all the PortShield groups.

A dedicated link can carry only one PortShield group, and that group must be portshielded to the dedicated port on the SonicWall firewall.

An isolated link can carry management traffic OR data traffic, but not both at the same time. Isolated links usually have separate connections between the firewall and the X-Switch for management traffic and data traffic.

About Uplink Interfaces

Uplink interfaces can be viewed as "trunk" ports set up to carry tagged/untagged traffic. When an extended switch is added with firewall uplink and X-Switch uplink options, the port on the firewall configured as the firewall uplink and the port on the extended switch configured as the switch uplink are set up automatically to receive/send tagged traffic for all IDV VLANs. The IDV VLAN of the tagged traffic allows the firmware to derive the PortShield host interface for the traffic.

Criteria for Configuring an Uplink Interface

- The interface must be a physical interface; virtual interfaces are not allowed.
- The interface must be a switch interface. (On some platforms, some firewall interfaces are not connected to the switch. Such interfaces are not allowed.)
- The interface cannot be a PortShield host (some other firewall interface cannot be portshielded to it) or a PortShield group member (cannot be portshielded to another firewall interface).
- The interface cannot be a bridge primary or bridge secondary interface.
- The interface cannot have any children (it cannot be a parent interface for other child interfaces).

Connecting the X-Series Switch Management Port to a SonicWall Firewall

The interface connected to the management port of the X-Switch must have an IP address from the same subnet as the switch. For example, if the management connection between the switch and the firewall is through X2, then X2 must have an IP address from the same subnet, such as `192.168.2.10.` The default switch IP address is `192.168.2.1.`

All port-based configuration operations are disabled on the X-Switch port designated as the switch management and switch uplink ports. This action ensures that configuration operations on these critical ports do not lead to switch-reachability issues jeopardizing the integration solution.

Configuring the Different Topologies

ⓘ **NOTE:** For a complete description of creating PortShield groups, see the *SonicOS 6.5 System Setup Administration Guide* and Adding an Extended Switch on page 21. The following sections describe only those steps required for the various topologies.

Topics:

Configuring a Common Uplink

X-Series switches can be managed by the firewall, thereby providing a unified management option for managing critical network elements such as the firewall/switch. This configuration allows a single link between the firewall and the X-Series switch to be designated as the uplink that carries all PortShield traffic, both management and data. Both the firewall and switch ports are configured as trunk ports for carrying tagged traffic for VLANs corresponding to all the firewall interfaces. The VLAN tag of the traffic is used to associate the traffic to the PortShield group to which it belongs.

The advantage of such a deployment option is a separate set of firewall/switch ports are not being used for management traffic. The disadvantage is that a high amount of data traffic can penalize forwarding of management traffic as the same link is shared for both types of traffic.

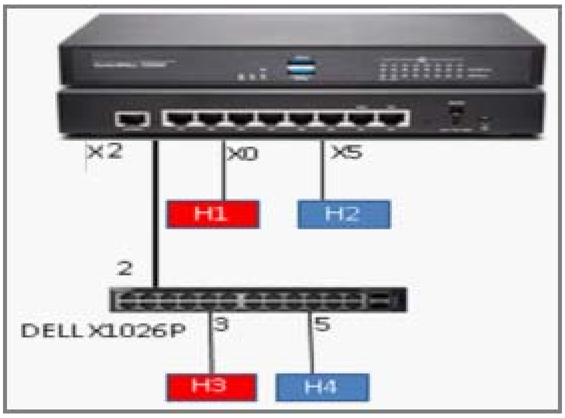
Common Uplink Topology shows a typical integration topology of a TZ500 firewall with an X1026P switch:

- The firewall uplink interface is X3.
- The X-Series switch uplink interface is 2.

This uplink between X3 on the firewall and port 2 on the extended switch is a common link set up to carry PortShield traffic between H1 and H3 and H2 and H4. The uplink is also the one on which the X-Series switch is managed by the firewall. In such a configuration, X3 is configured in the same subnet as the IP of the switch. Also, X3 is configured as the firewall uplink, and port 2 is configured as the switch management as well as the switch uplink when a switch is provisioned.

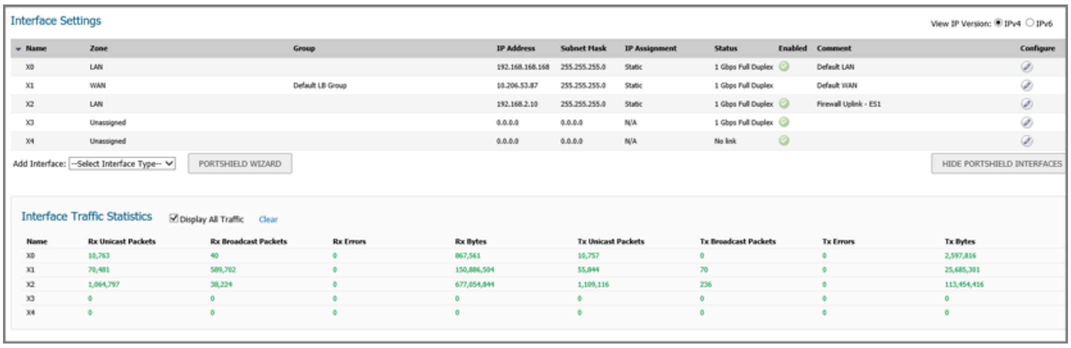
ⓘ **NOTE:** If necessary, you may choose to have different links carry the PortShield traffic and management traffic. For more information, see Configuring Isolated Links for Management and Data Uplinks on page 40.

Common Uplink Topology



To configure a common link:

1. Set up the switch as described in Provisioning an X-Switch on a SonicWall Appliance on page 10.
2. Connect an RJ45 cable between TZ port X0 and X1.
3. Navigate to the **Network > Interfaces** page.



Interface Settings

View IP Version: ● IPv4 ○ IPv6

Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Enabled	Comment	Configure
X0	LAN		192.168.168.168	255.255.255.0	Static	1 Gbps Full Duplex	✓	Default LAN	✎
X1	WAN	Default LB Group	10.206.53.87	255.255.255.0	Static	1 Gbps Full Duplex		Default WAN	✎
X2	LAN		192.168.2.10	255.255.255.0	Static	1 Gbps Full Duplex	✓	Firewall Uplink - ES1	✎
X3	Unassigned		0.0.0.0	0.0.0.0	N/A	1 Gbps Full Duplex	✓		✎
X4	Unassigned		0.0.0.0	0.0.0.0	N/A	No link	✓		✎

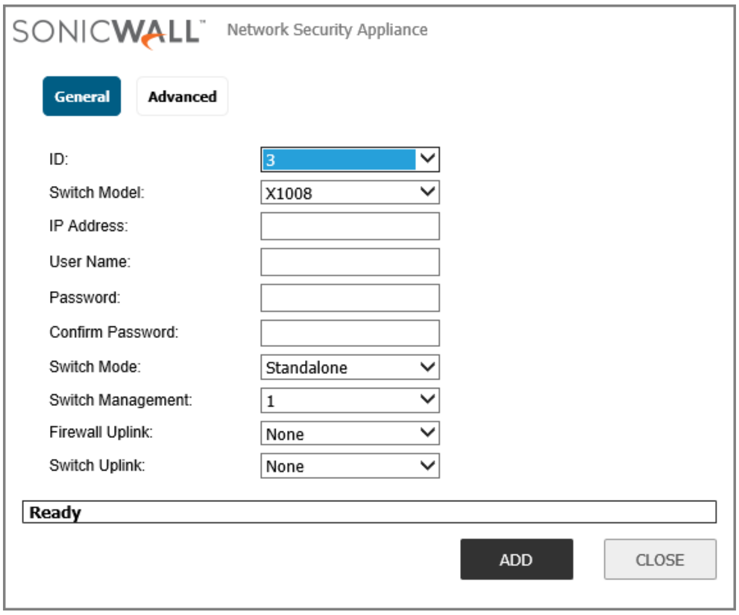
Add Interface: --Select Interface Type-- PORTSHIELD WIZARD HIDE PORTSHIELD INTERFACES

Interface Traffic Statistics ☑ Display All Traffic Clear

Name	Rx Unicast Packets	Rx Broadcast Packets	Rx Errors	Rx Bytes	Tx Unicast Packets	Tx Broadcast Packets	Tx Errors	Tx Bytes
X0	10,763	40	0	867,561	10,757	0	0	2,597,816
X1	70,481	589,702	0	150,886,504	55,844	70	0	25,685,301
X2	1,064,797	38,224	0	677,054,844	1,109,116	236	0	113,454,416
X3	0	0	0	0	0	0	0	0
X4	0	0	0	0	0	0	0	0

4. Ensure that X2 has an IP address in the range `192.168.2.10`
5. Navigate to the **Network > PortShield Groups** page.
6. Click on **External Switch Configuration**.

7 Click the **Add Switch** button. The **Add External Switch** dialog displays.



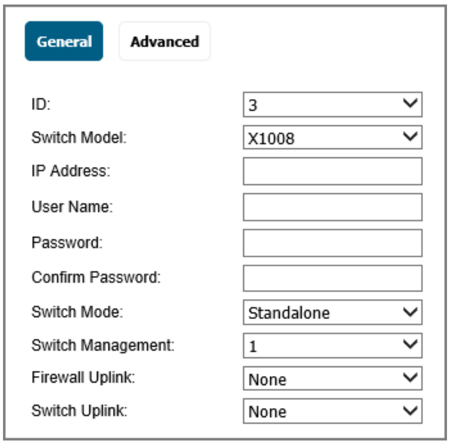
ID:	3
Switch Model:	X1008
IP Address:	
User Name:	
Password:	
Confirm Password:	
Switch Mode:	Standalone
Switch Management:	1
Firewall Uplink:	None
Switch Uplink:	None

Ready

8 Configure the **ID** through **Confirm Password** options as described in Adding an Extended Switch on page 21.

9 Select the port on the switch via which the firewall manages the switch from the **Switch Management** drop-down menu.

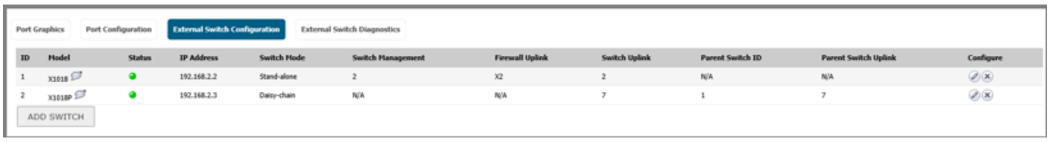
10 Select the **Firewall Uplink** and **Switch Uplink** options from their respective drop-down menus.



ID:	3
Switch Model:	X1008
IP Address:	
User Name:	
Password:	
Confirm Password:	
Switch Mode:	Standalone
Switch Management:	1
Firewall Uplink:	None
Switch Uplink:	None

11 For information about configuring the **Advanced** tab, see Adding an Extended Switch on page 21.

12 Click **Add**. The **External Switch Configuration** tab shows the link between X2 and the X-Switch port 2.



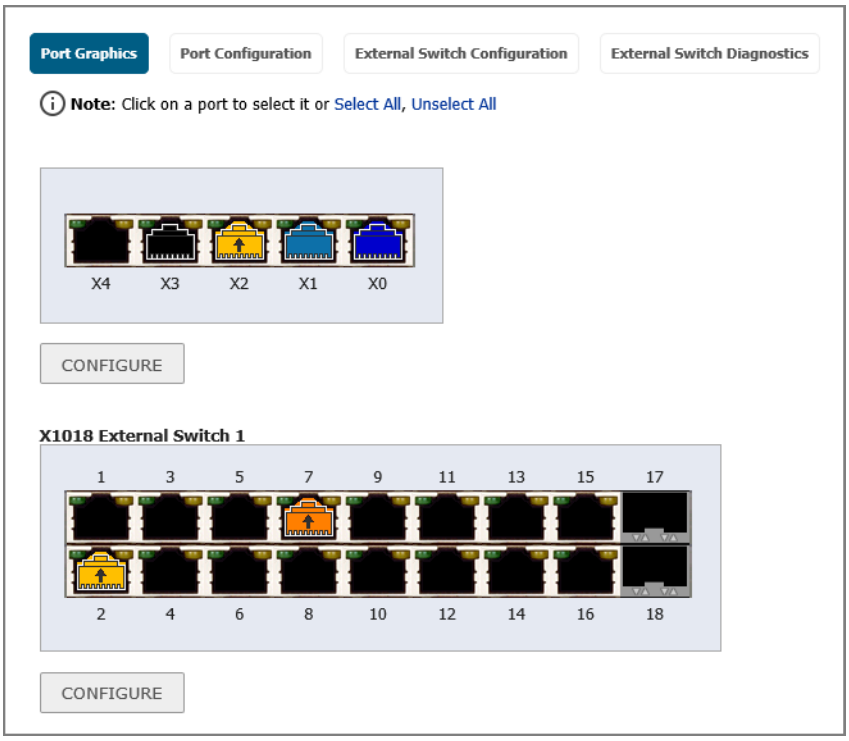
ID	Model	Status	IP Address	Switch Mode	Switch Management	Firewall Uplink	Switch Uplink	Parent Switch ID	Parent Switch Uplink	Configure
1	X1018	●	192.168.2.2	Stand-alone	2	X2	2	N/A	N/A	✎ ☒
2	X1018P	●	192.168.2.3	Daisy-chain	N/A	N/A	7	1	7	✎ ☒

- **Status** – a green **Enabled** icon
- **Switch Management** – port 2
- **Firewall Uplink** – X2

- **Switch Uplink** – port 2

13 Click the **Port Graphics** tab.

The X2 port and X-Switch 1 port 2 have the same color and a small arrow in the middle, which means they are the uplink, that is, connected by cable.



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

X1018 External Switch 1

14 To PortShield ports on the firewall and X-Switch, see the PortShield sections in the *SonicOS 6.5 System Setup Administration Guide*.

Configuring a Dedicated Uplink

This configuration allows a given link between the firewall and the X-Series switch to be designated as the dedicated uplink set up to carry PortShield traffic corresponding to the connected firewall interface. The firewall and switch ports are configured in access mode for the VLAN corresponding to the PortShield VLAN of the firewall interface.

This configuration can be used in deployments where a dedicated 1G link is needed for a particular firewall interface. Cases where this configuration is necessary:

- VLANs are used; for example, another switch behind the X-Switch.
- There will be a large volume of traffic and there needs to be a separate uplink for this traffic.

The risk associated with such a configuration is using up interfaces on the firewall fairly soon.

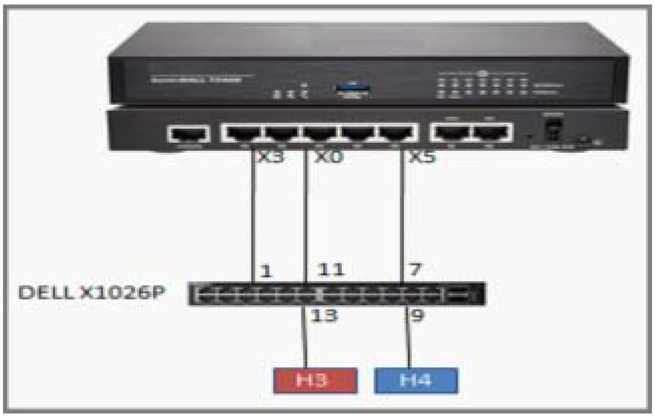
ⓘ **NOTE:** In this example, there is no common uplink to carry the PortShield traffic for the rest of the firewall interfaces (excluding X0 and X5 for which dedicated links are set up).

ⓘ **IMPORTANT:** For the dedicated uplink to work, the physical link must be connected before being configured.

Dedicated Uplink Topology shows a dedicated uplink setup of a TZ500 firewall with an X1026P switch. There are two dedicated uplinks in this scenario:

- The uplink between X2 on the firewall and port 2 on the extended switch is used to manage the switch. In this configuration, X2 is configured in the same subnet as the IP of the X-Series switch.
- In addition, there are two dedicated uplinks:
  - The uplink between X0 on the firewall and port 11 on the extended switch is a dedicated link to carry all PortShield traffic for X0.
  - The uplink between X5 on the firewall and port 7 on the extended switch is a dedicated link to carry all PortShield traffic for X5.

Dedicated Uplink Topology



You can configure a dedicated uplink with or without setting up the common uplink to carry all PortShield traffic for the different firewall interfaces. In both cases, the common uplink is used to manage the extended switch.

Topics:

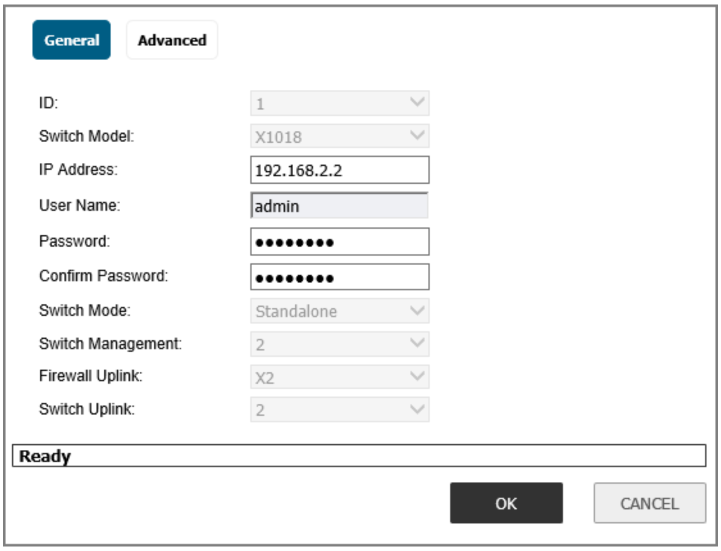
- Configuring a Dedicated Uplink Without a Common Uplink on page 34
- Configuring a Dedicated Uplink With a Common Uplink on page 36

Configuring a Dedicated Uplink Without a Common Uplink

To configure a dedicated uplink topology without an common uplink:

1. Set up the switch as described in Provisioning an X-Switch on a SonicWall Appliance on page 10.
2. Navigate to the **Network > PortShield Groups** page.
3. Click the **External Switch Configuration** tab.

4. Click the **Edit** icon on the far right for an unassigned switch. The **Edit External Switch** dialog displays.



ID:	1
Switch Model:	X1018
IP Address:	192.168.2.2
User Name:	admin
Password:	••••••••
Confirm Password:	••••••••
Switch Mode:	Standalone
Switch Management:	2
Firewall Uplink:	X2
Switch Uplink:	2

Ready

5. Configure the **ID** through **Confirm Password** options as described in Adding an Extended Switch on page 21.

6. Select the port on the switch via which the firewall manages the switch from the **Switch Management** drop-down menu.

7. To provision the extended switch for a dedicated uplink without a common uplink, ensure the **Firewall Uplink** and **Switch Uplink** options are set to **None**.

8. For information about configuring the **Advanced** tab, see Adding an Extended Switch on page 21.

9. Click **Add**. The dialog closes.

10. Click either:

    - **Port Graphics**
    - **Port Configuration**

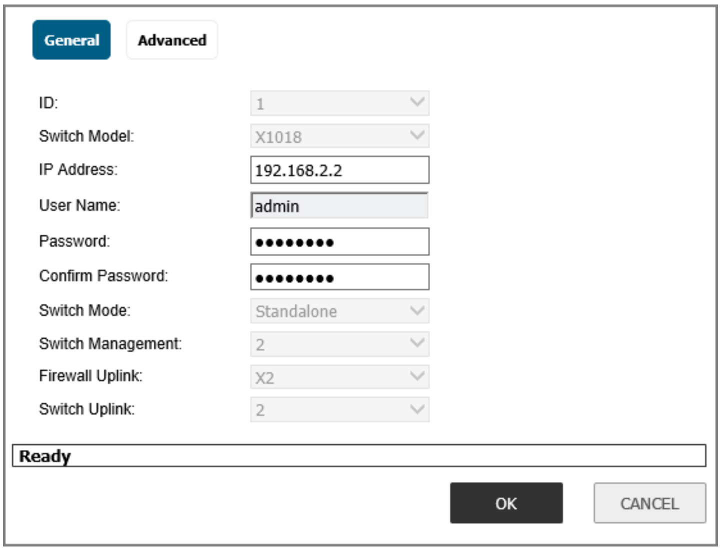
11. On **Port Graphics**:

    a) Select the desired PortShield Interface.

    b) Click the **CONFIGURE** button.

    - **Port Configuration** tab, click the **Edit** icon of the desired PortShield Interface.

The **Edit Switch Port** dialog displays.



ID:	1
Switch Model:	X1018
IP Address:	192.168.2.2
User Name:	admin
Password:	••••••••
Confirm Password:	••••••••
Switch Mode:	Standalone
Switch Management:	2
Firewall Uplink:	X2
Switch Uplink:	2

Ready

12 Click **OK**.

Configuring a Dedicated Uplink With a Common Uplink

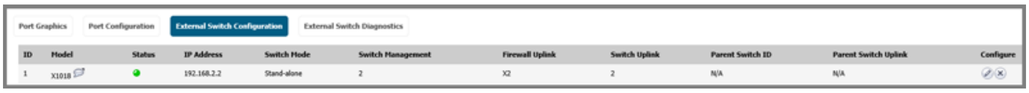
To configure a dedicated uplink topology with an common uplink:

1 Provision the switch as described in Provisioning an X-Switch on a SonicWall Appliance on page 10.

> ⓘ **NOTE:** For this example, a cable is connected to firewall port X2 and switch port 2, which has a human icon in the port icon. This connection is a common link because it carries both management and data traffic.

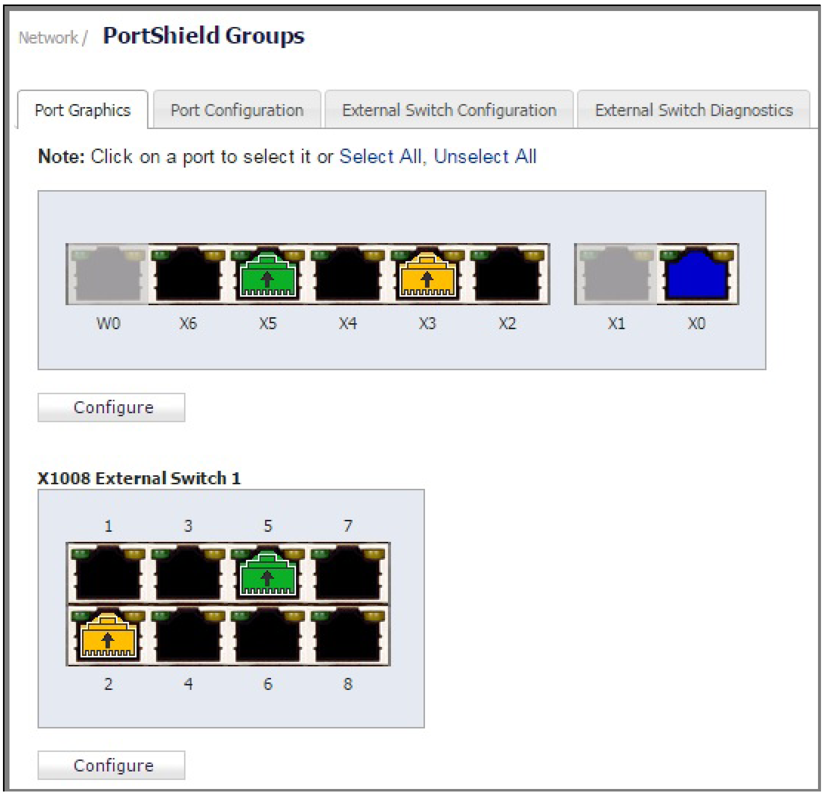
2 Set up the common uplink as described in Adding an Extended Switch on page 21.

The **External Switch Configuration** screen is updated.



ID	Model	Status	IP Address	Switch Mode	Switch Management	Firewall Uplink	Switch Uplink	Parent Switch ID	Parent Switch Uplink	Configure
1	X1018	●	192.168.2.2	Stand-alone	2	X2	2	N/A	N/A	

The **External Switch Configuration** and **Port Graphics** screens are updated. On the **Port Graphics** tab, the icons for firewall port X3 and switch port 2 are the same color and contain an up arrow.



Network / PortShield Groups
Port Graphics
Port Configuration
External Switch Configuration
External Switch Diagnostics
Note: Click on a port to select it or Select All, Unselect All
W0
X6
X5
X4
X3
X2
X1
X0
Configure
X1008 External Switch 1
1
3
5
7
2
4
6
8
Configure

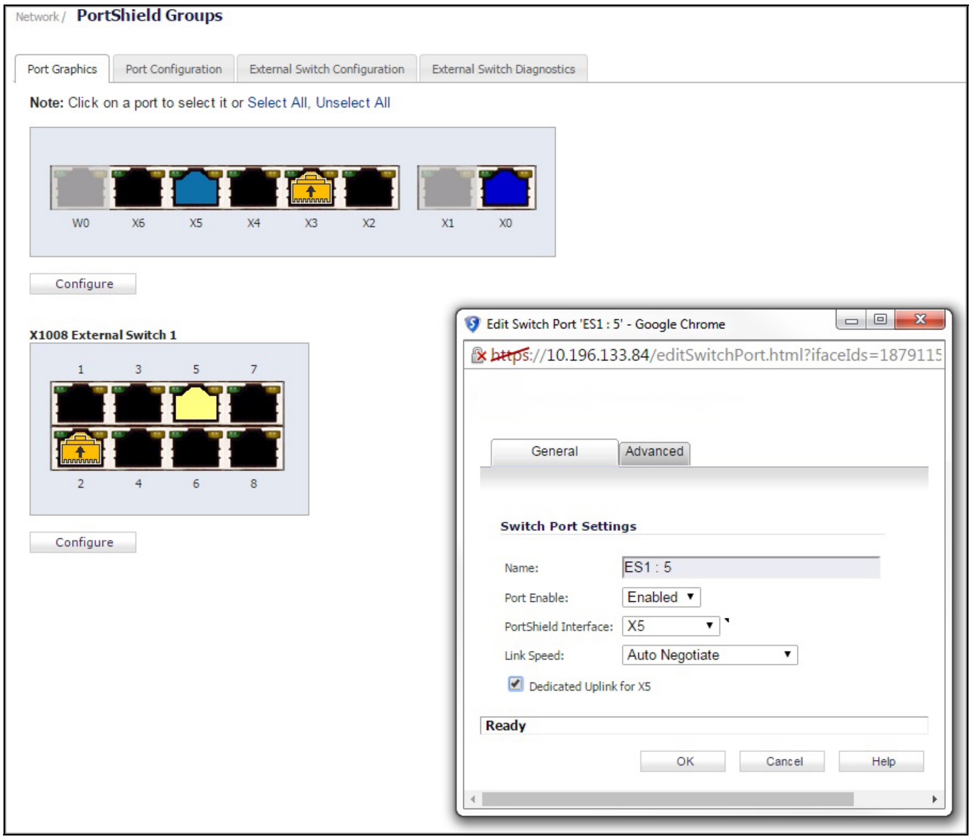
3 Click either the:

- **Port Graphics** tab.
- **Port Configuration** tab.

4 On the:

- **Port Graphics** tab:

  a) Select the desired PortShield Interface(s).



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

Edit Switch Port 'ES1 : 5' - Google Chrome

~~https~~://10.196.133.84/editSwitchPort.html?ifaceIds=1879115

Switch Port Settings

Name: ES1 : 5

Port Enable: Enabled

PortShield Interface: X5

Link Speed: Auto Negotiate

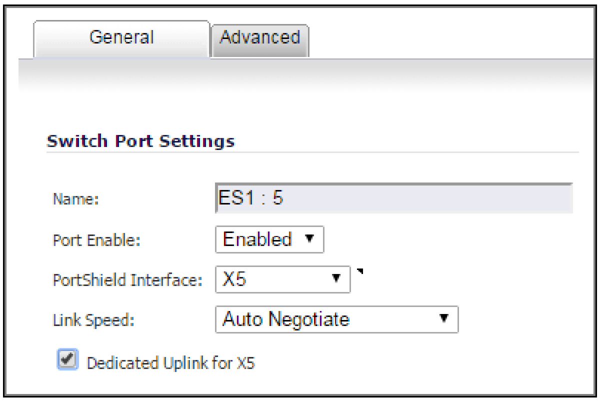
☑ Dedicated Uplink for X5

Ready

  b) Click the **Configure** button.

- **Port Configuration** tab, click the **Edit** icon of the desired PortShield Interface.

The **Edit Switch Port** dialog displays.



Switch Port Settings

Name: ES1 : 5

Port Enable: Enabled

PortShield Interface: X5

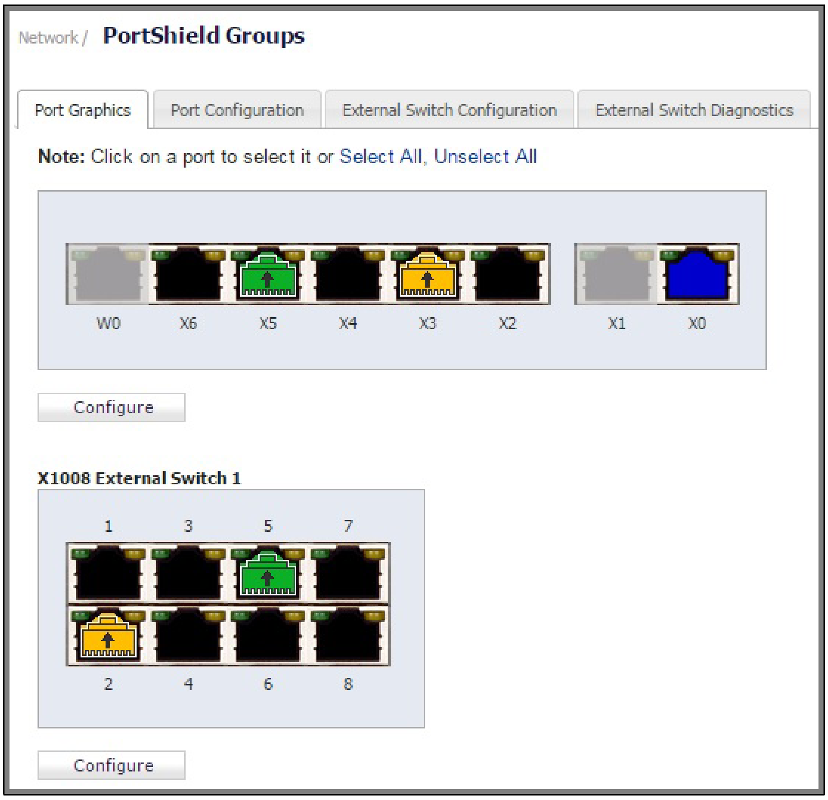
Link Speed: Auto Negotiate

☑ Dedicated Uplink for X5

5 Select the **Dedicated Uplink** option.

6 Click **OK**.

The graphics on the **Port Graphics** tab show the firewall X5 and switch port 5 icons have the same color (green in this example) and an up arrow, which indicates a dedicated link.



Network / PortShield Groups

Port Graphics | Port Configuration | External Switch Configuration | External Switch Diagnostics

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

Configuring a Hybrid System With Common and Dedicated Uplink(s)

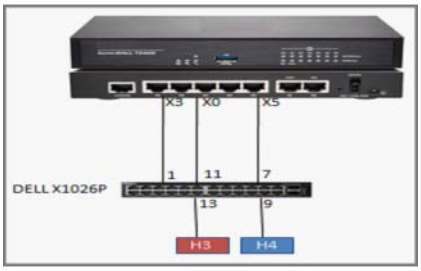
This configuration allows a combination of common and dedicated uplinks to be set up between the firewall and the X-Series switch. The dedicated uplinks are used to carry PortShield traffic corresponding to the connected firewall interface. The common uplink is used to carry PortShield traffic for the remaining firewall interfaces (with no dedicated uplinks).

Hybrid Uplink Topology shows a hybrid uplink integration topology of a TZ400 firewall with an X1026P switch:

- The dedicated uplink between X0 on the firewall and port 11 on the extended switch is set up to carry PortShield traffic for X0.
- The common link between X3 on the firewall and port 2 on the extended switch carries PortShield traffic for firewall interfaces other than X0.
- Ports X0 and 11 for the dedicated uplink are access ports for the VLAN corresponding to X0. Ports X3 and 2 for the common uplink are trunk ports, and VLANs corresponding to all firewall interfaces, except X0, are added as members to this trunk to facilitate carrying the PortShield VLAN-tagged traffic.

In this configuration, the link between X3 and 2 is also used to carry management traffic between the firewall and the switch.

Hybrid Uplink Topology



Setting up a hybrid configuration is done in two steps:

1. Configure an common uplink.
2. Configure the dedicated uplink.

To set up a hybrid configuration with common and dedicated uplinks:

1. Set up the switch as described in Adding the X-Series Switch to SonicOS on page 21.
2. Configure the uplink as described in Configuring a Dedicated Uplink With a Common Uplink on page 36.

Configuring Isolated Links for Management and Data Uplinks

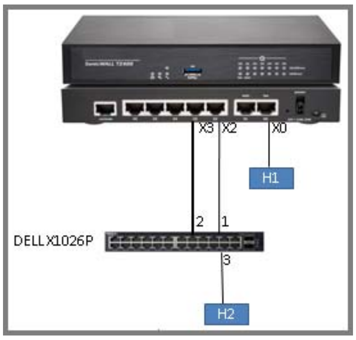
This configuration allows separate links between the firewall and X-Series switch to carry management traffic and data traffic. With a common link, the management traffic and data traffic run in the same uplink; if data traffic is congested, so is management traffic, which results in a delay in forwarding management traffic. If data traffic will be congested, consider configuring separate links for management traffic and data traffic. Although similar to a common link configuration, the isolated management/data configuration runs separate uplinks for management traffic and data traffic. This configuration ensures that even with a high amount of data traffic, management traffic to the switch is forwarded without being delayed.

IMPORTANT: The MGMT port cannot be portshielded.

Isolated Link Topology shows an isolated link setup of a TZ400 firewall with an X1026P switch:

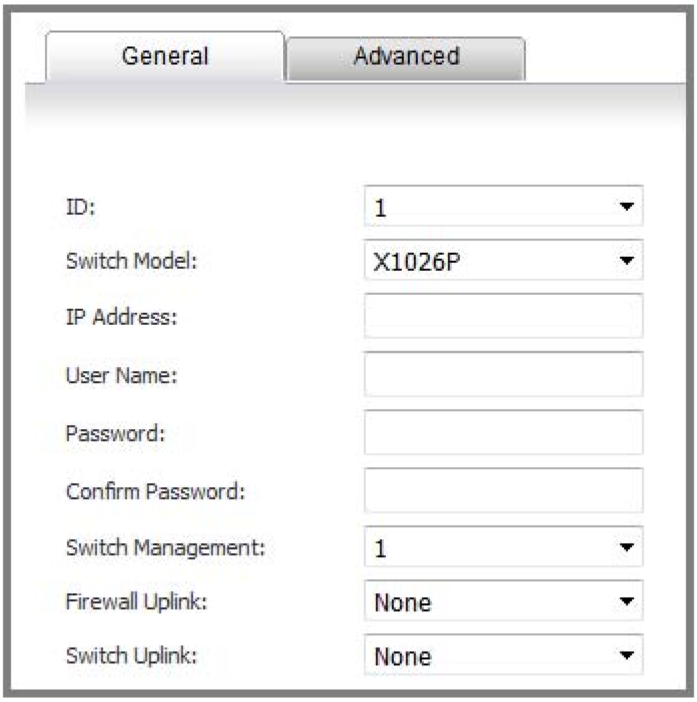
- The link between X2 on the firewall and port 1 on the external switch carries management traffic to the switch. In such a configuration, X2 is configured in the same subnet as the IP of the X-Series switch.
- The link between X3 on the firewall and port 2 on the external switch is the uplink set up to carry PortShield traffic between H1 and H2.
- X3 is configured as the firewall uplink.
- Port 1 is configured as the switch MGMT port.
- Port 2 is configured as the switch data uplink.

Isolated Link Topology



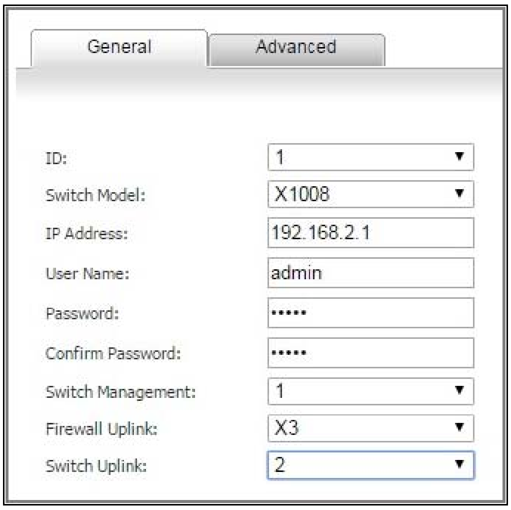
To set up isolated links for management and data traffic:

1. Provision the switch as described in Provisioning an X-Switch on a SonicWall Appliance on page 10.
2. Set up the data uplink as described in Adding an Extended Switch on page 21.
3. Navigate to the **Network > PortShield Groups** page.
4. Click the **External Switch Configuration** tab.
5. Click **Add Switch**. The **Add External Switch** dialog displays.



ID:	1
Switch Model:	X1026P
IP Address:	
User Name:	
Password:	
Confirm Password:	
Switch Management:	1
Firewall Uplink:	None
Switch Uplink:	None

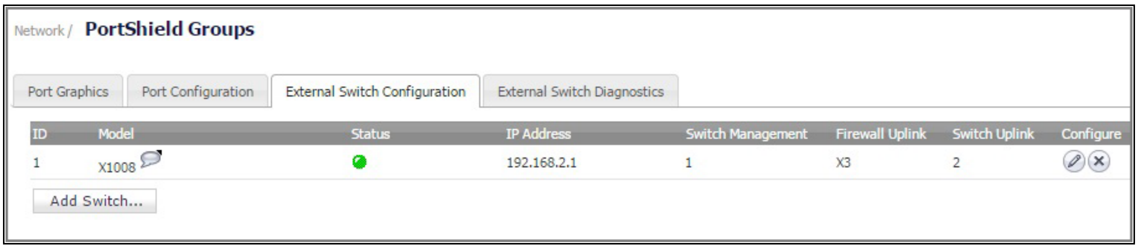
6. Configure the **ID** through **Confirm Password** options as described in Adding an Extended Switch on page 21.
7. To specify the port on the switch via which the firewall manages the switch, select the port from the **Switch Management** drop-down menu.
8. Select the **Firewall Uplink** and **Switch Uplink** options from their respective drop-down menus:



ID:	1
Switch Model:	X1008
IP Address:	192.168.2.1
User Name:	admin
Password:	•••••
Confirm Password:	•••••
Switch Management:	1
Firewall Uplink:	X3
Switch Uplink:	2

9 Click **Add**.

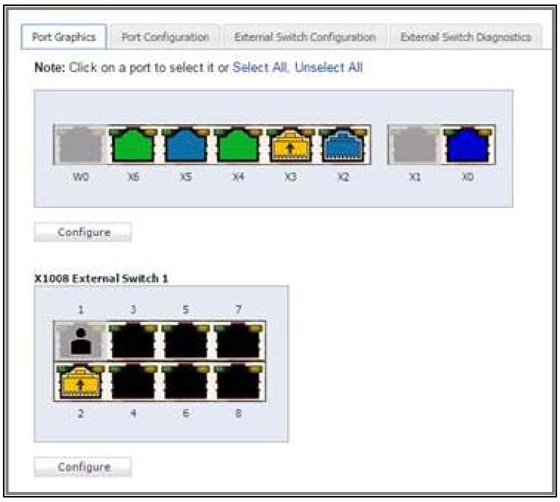
10 The extended switch configuration is displayed on the **Network > PortShield Groups > External Switch Configuration** tab.


Network / PortShield Groups
Port Graphics
Port Configuration
External Switch Configuration
External Switch Diagnostics

ID	Model	Status	IP Address	Switch Management	Firewall Uplink	Switch Uplink	Configure
1	X1008	●	192.168.2.1	1	X3	2	

The **Port Graphics** tab displays:

- The extended switch port 1 is management (it is grey with a human icon in it).
- The data uplink is between X3 and extended port 2.


Port Graphics
Port Configuration
External Switch Configuration
External Switch Diagnostics
Note: Click on a port to select it or Select All, Unselect All
W0
X6
X5
X4
X3
X2
X1
X0
Configure
X1008 External Switch 1
1
3
5
7
2
4
6
8
Configure

Configuring HA and PortShield With Dedicated Uplink(s)

ⓘ **IMPORTANT:** To use the SonicWall X-Series with HA, you must first create an HA system, and then add the X-Switch.

There are two ways to configure HA units with dedicated uplinks:

- Configuring HA Using One Extended Switch Management Port on page 43
- Configuring HA Using Two Extended Switch Management Ports on page 44

Configuring HA Using One Extended Switch Management Port

In this configuration with PortShield functionality in HA mode, firewall interfaces that serve as PortShield hosts should be connected to the X-Series switch on both the active and standby units. The PortShield members should also be connected to ports on the switch. The link between the firewall interface serving as the PortShield host and the switch is set up as a dedicated uplink.

HA Pair Using One Extended Switch Management Port Topography shows a TZ300 HA pair with an X1026 switch and one dedicated link:

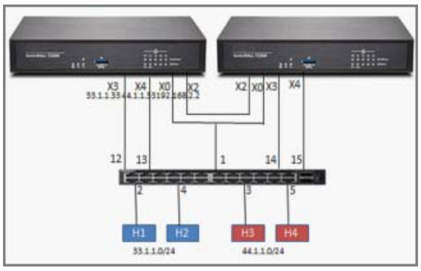
- The firewall interfaces, X3 and X4, on the primary unit are connected to ports 12 and 13 on the X-Series switch.
- X3 and X4 are configured as PortShield hosts.
- Similarly, the firewall interfaces X3 and X4 on the secondary unit are connected to ports 14 and 15 on the X-Series switch.
- Ports 12 and 14 on the switch are portshielded to X3 with the dedicated uplink option enabled.
- Ports 13 and 15 on the switch are portshielded to X4 with the dedicated uplink option enabled.
- Ports 2 and 4 are portshielded to X3.
- Ports 3 and 5 are portshielded to X4.

When the primary unit acts in active HA mode, traffic between H1 and X3 is carried over the dedicated link between X3 and 12 and traffic between H3 and X4 is carried over the dedicated link between X4 and 13.

When the secondary unit acts in active HA mode, traffic between H1 and X3 is carried over the dedicated link between X3 and 14, and traffic between H3 and X4 is carried over the dedicated link between X4 and 15.

The link between the firewall interface, X0, and port 1 on the X-Series switch, carries the management traffic to manage the switch from the firewall. In such a configuration, X0 is configured to be in the same subnet as the switch. Also, X0 on the primary as well as the secondary is ensured to be connected to port 1 of the switch (for example, via a hub) so that when the secondary firewall becomes the active unit, the switch can be managed via the link between the firewall interface X0 on the secondary and port 1 of the switch. In such a configuration, when the switch is provisioned, the Primary Switch Management and Secondary Switch Management are set to 1.

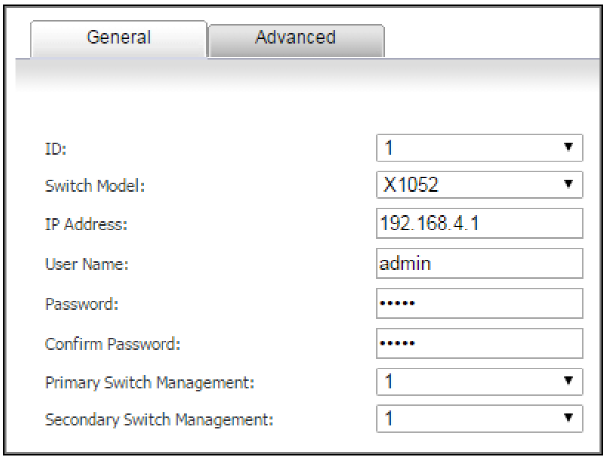
HA Pair Using One Extended Switch Management Port Topography



To set up HA with one dedicated uplink:

1. Provision the switch as described in Provisioning an X-Switch on a SonicWall Appliance on page 10.
2. Set up the data uplink as described in Adding an Extended Switch on page 21.
3. Configure the options as described in Configuring a Common Uplink on page 30 except:
    a. Select the **Primary Switch Management** and **Secondary Switch Management** interfaces from their respective drop-down menus:

        > **NOTE:** The **Firewall Uplink** and **Switch Uplink** options are not relevant for a firewall operating in HA mode. The primary **Firewall Uplink** option and both the primary and secondary **Switch Uplink** options are set to **None**.



ID:	1 ▾
Switch Model:	X1052 ▾
IP Address:	192.168.4.1
User Name:	admin
Password:	•••••
Confirm Password:	•••••
Primary Switch Management:	1 ▾
Secondary Switch Management:	1 ▾

4. Click **ADD**.

Configuring HA Using Two Extended Switch Management Ports

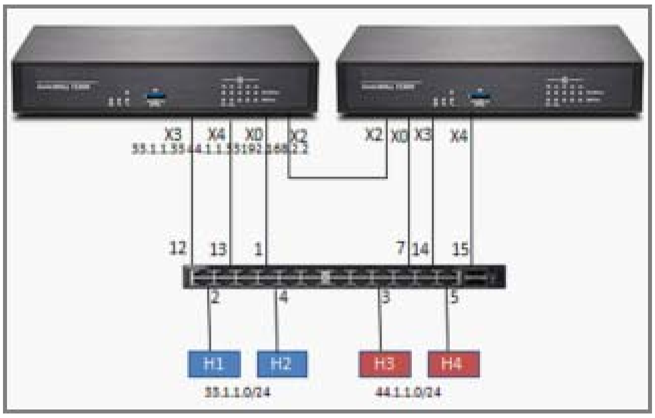
You can connect X0 of the primary and secondary firewalls directly to the ports on the X-Series switch. In this case, two switch ports are used on the switch for management traffic.

HA Pair Using 2 Extended Switch Management Ports Topography shows a a TZ300 HA pair with an X1026 switch and two dedicated links:

- X0 of the primary unit is connected to port 1.
- X0 of the secondary unit is connected to port 7

When the switch is provisioned, **Primary Switch Management** is set to port 1 and **Secondary Switch Management** is set to port 7. When the primary firewall is active, the link between X0 of the primary and port 1 of the switch carry the management traffic. When the secondary firewall is active, the link between X0 of the secondary and port 7 of the switch is used by the firewall to manage the switch.

HA Pair Using 2 Extended Switch Management Ports Topography



To set up HA with two extended switch management ports:

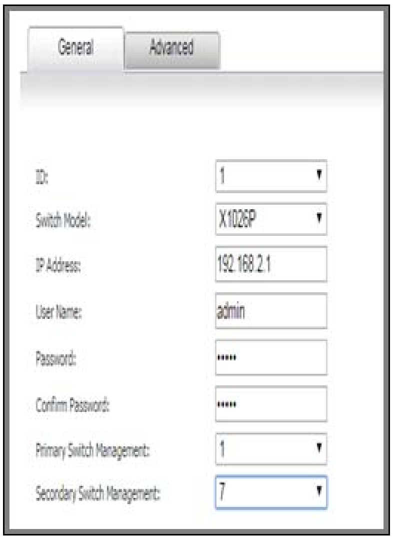
1 Provision the switch as described in Provisioning an X-Switch on a SonicWall Appliance on page 10.

2 Set up the data uplink as described in Adding an Extended Switch on page 21.

3 Configure the options as described in Configuring a Common Uplink on page 30 except:

   a Select the **Primary Switch Management** and **Primary Switch Management** interfaces from their respective drop-down menus:

   > **NOTE:** The **Firewall Uplink** and **Switch Uplink** options are not relevant for a firewall operating in HA mode. The primary **Firewall Uplink** option and both the primary and secondary **Switch Uplink** options are set to **None**.



ID:	1
Switch Model:	X1026P
IP Address:	192 168 2 1
User Name:	admin
Password:	•••••
Confirm Password:	•••••
Primary Switch Management:	1
Secondary Switch Management:	7

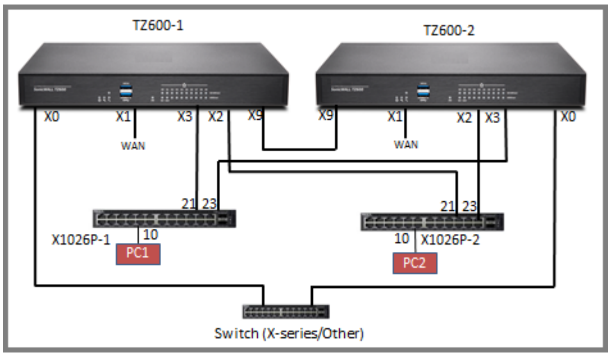
4 Click **ADD**.

Configuring HA and PortShield With a Common Uplink

In this configuration with PortShield functionality in HA mode, a link between the active/standby firewalls and the X-Series switch serves as a common uplink to carry all the portshielded traffic. Firewall interfaces that serve as PortShield hosts are connected to a separate switch (not necessarily an X-Series switch) and not the same X-Series switch connected to the active and standby units. This other switch avoids the looping of packets for the same PortShield VLAN. The PortShield members can be connected to ports on the X-Series switch that is controlled by the active/standby firewalls.

HA Pair Using a Common Switch Topography shows a TZ600 HA pair and two X1026P switches. The link between X3 and X1026P-1 is set up as a common uplink. Similarly, the link between X2 and X1026P-2 is set up as a common uplink. The PortShield hosts' X0 are connected to a different switch (which could be an X-Series switch or any other vendor's switch) to avoid looping of packets. Ports 10 on both X1026P-1 and X1026P-2 are portshielded to X0, and hosts connected to Ports 10 on both switches can communicate using the common uplink.

HA Pair Using a Common Switch Topography



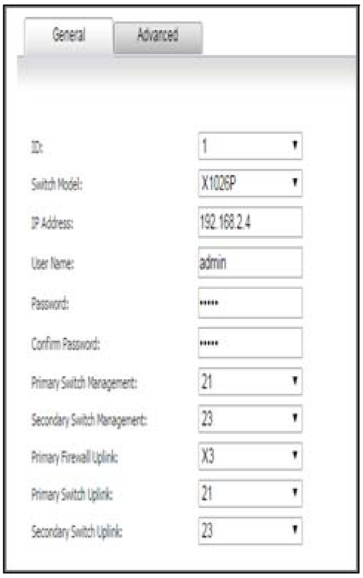
To set up HA with a common uplink:

1. Provision the switch(es) as described in Provisioning an X-Switch on a SonicWall Appliance on page 10.
2. Set up the data uplink as described in Adding an Extended Switch on page 21.
3. On the **Network > Interfaces** page, configure these interfaces for both firewalls:

X0	LAN/PortShield host
X1	WAN
X2	Firewall uplink on the firewall for X1026P-2
X3	Firewall uplink on the firewall for X1026P-1

4 Configure the options as described in Configuring a Common Uplink on page 30 except for these ports:

X1026P-1 Interfaces:	10	Host-facing interface portshielded to X0
	21	Switch uplink for the primary firewall
	23	Switch uplink for the secondary firewall



ID:	1
Switch Model:	X1026P
IP Address:	192.168.2.4
User Name:	admin
Password:	•••••
Confirm Password:	•••••
Primary Switch Management:	21
Secondary Switch Management:	23
Primary Firewall Uplink:	X3
Primary Switch Uplink:	21
Secondary Switch Uplink:	23

X1026P-2 Interfaces:	10	Host-facing interface portshielded to X0
	21	Switch uplink for the primary firewall
	23	Switch uplink for the secondary firewall

Configuring VLAN(s) With Common or Dedicated Uplink(s)

Topics:

- Prerequisites for VLAN Support on page 47
- Configuring a Common Uplink for VLANs on page 48
- Configuring a Dedicated Uplink for VLANs on page 50

Prerequisites for VLAN Support

- Support for VLANs is available on both dedicated and common uplinks.For example, VLANs can be configured under firewall interfaces configured as a dedicated uplink. VLANs also can be configured under the firewall interface provisioned as the common uplink for the X-Series switch.
- Overlapping VLANs cannot exist under appliance interfaces configured as dedicated uplinks to the same switch because VLAN space on the X-Series switch is global. For example, if X3 and X5 are configured for dedicated uplinks to the same X-Series switch, VLAN 100 cannot be present under both X3 and X5. Such a configuration is rejected. If X3 an X5 are X5 are dedicated uplinks to different X-Series switches, however, then such a configuration is accepted

- Overlapping VLANs cannot exist under common uplink interfaces. For example, if X3 is set up as a common uplink to an X-Series switch and VLAN 100 exists under X3, another interface that is configured as a common uplink to a second X-Series switch, for example, X4, cannot have a VLAN 100 sub-interface.
- PortShield of extended switch interfaces to common uplink interfaces without selecting any VLANs for access/trunk configuration is not supported.

For more information about SonicOS 6.5 X-Series support for VLAN, see *SonicWall X-Series - Support for SonicWall Virtual Interfaces (VLANs) (189771)*.

Configuring a Common Uplink for VLANs

For information about prerequisites and limitation for VLAN configurations, see Prerequisites for VLAN Support on page 47.

Topics:

Configuring a Common Uplink for VLAN(s) With SPM

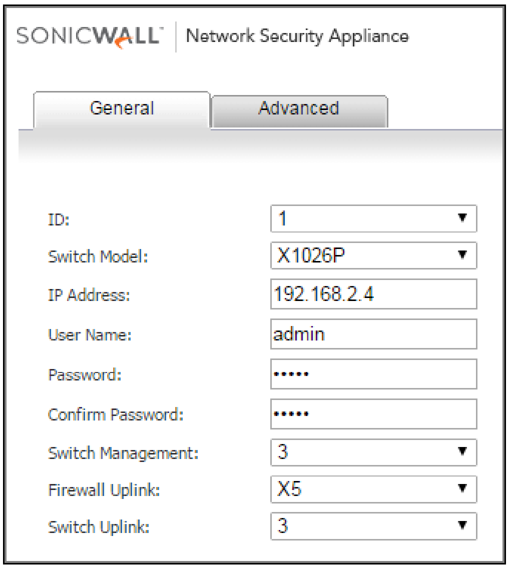
With Single Point of Management (SPM), you can configure a common uplink to carry management traffic of the firewall managing the X-Series switch plus PortShield traffic for the IDV VLANs corresponding to the firewall interfaces plus traffic corresponding to the VLAN subinterfaces under the common uplink.

VLAN With Dedicated Uplink Topology shows a TZ500 with an X1026P switch:

- The link between X5 and port 3 on the extended switch is configured as a common uplink for carrying PortShield traffic for the different firewall interfaces.
- The link between X5 and port 3 is also used by the firewall to manage the switch.
- Interface X5 is configured to be in the same subnet as the IP of the switch. In this configuration example, the switch is first provisioned with the **Firewall Uplink** as X5, **Switch Uplink** as 3, and **Switch Management** as 3.
- There are three VLAN interfaces with VLAN tags 100, 150, and 200 configured under X5.
- The link between X5 on the firewall and port 3 on the extended switch is a common link set up to carry management traffic, PortShield traffic, and traffic tagged with VLANs 100, 150, 200.

Supporting such a topology requires this configuration:

- A switch is provisioned using X5 as the **Firewall Uplink** and 3 as both the **Switch Uplink** and **Switch Management**.



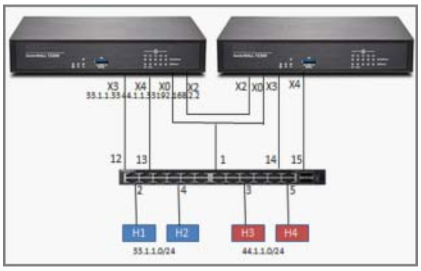
ID:	1
Switch Model:	X1026P
IP Address:	192.168.2.4
User Name:	admin
Password:	•••••
Confirm Password:	•••••
Switch Management:	3
Firewall Uplink:	X5
Switch Uplink:	3

- Port 2 is portshielded to X3 with the dedicated link option.

  NOTE: This configuration is also possible without the presence of the dedicated link and just using the common uplink between X5 and 3.

- Port 3 is portshielded to X5 with dedicated uplink option.
- Port 10 is portshielded to X5 and configured as a trunk to carry VLAN 100.
- Port 11 is portshielded to X5 and configured as a trunk to carry VLAN 150.
- Port 12 is portshielded to X5 and configured as an access to carry VLAN 200

VLAN(s) With Common Uplink Topology



To configure a common uplink for a VLAN:

1. Provision the switch as described in Provisioning an X-Switch on a SonicWall Appliance on page 10.
2. Set up the data uplink as described in Adding an Extended Switch on page 21.
3. Configure the uplinks as described in Configuring a Common Uplink on page 30.

Configuring a Dedicated Uplink Plus a Common Uplink for a VLAN

To configure a dedicated uplink plus a common uplink for a VLAN:

1. Provision the switch as described in Provisioning an X-Switch on a SonicWall Appliance on page 10.

2 Set up the data uplink as described in Adding an Extended Switch on page 21.

3 Configure the uplinks as described in Configuring a Hybrid System With Common and Dedicated Uplink(s) on page 39.

Configuring a Dedicated Uplink for VLANs

Topics:

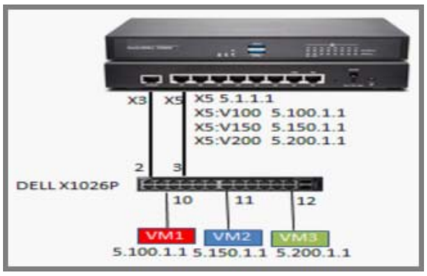
- Dedicated Uplink for VLAN Topology on page 50
- Configuring a Dedicated Uplink for a VLAN on page 50

Dedicated Uplink for VLAN Topology

In a dedicated uplink configuration, a given link between the firewall and the X-Series switch designated as the dedicated uplink is set up to carry traffic for all VLANs configured under the firewall interface plus PortShield traffic corresponding to the firewall interface.

VLAN With Dedicated Uplink Topology shows a TZ500 with an X1026P switch:

VLAN With Dedicated Uplink Topology



- The link between X3 and port 1 on the extended switch is used by the firewall to manage the switch.
- Interface X3 is configured to be in the same subnet as the IP of the switch.

  NOTE: In this example, a common uplink is not required, hence, the extended switch is provisioned with the **Firewall Uplink** and **Switch Uplink** options set to **None** and **Switch Management** set to **1**.

- There are three VLAN interfaces with VLAN tags 100, 150, and 200 configured under X5.
- The link between X5 on the firewall and port 3 on the extended switch is a dedicated link set up to carry traffic tagged with VLANs 100, 150, and 200 and untagged traffic for X5.

Supporting such a topology, requires this configuration:

- Port 3 is portshielded to X5 with dedicated uplink option.
- Port 10 is portshielded to X5 and configured as a trunk to carry VLAN 100.
- Port 11 is portshielded to X5 and configured as a trunk to carry VLAN 150.
- Port 12 is portshielded to X5 and configured as an access to carry VLAN 200.

Configuring a Dedicated Uplink for a VLAN

Support for VLAN(s) is achieved in a multi-step configuration process:

1 Provision the switch. The switch can be provisioned with the:

  - Firewall uplink and switch uplink set to **None** if support for VLAN(s) alone is needed.

- Common uplink option if support is needed for an common trunk interface to carry PortShield traffic for other firewall interfaces along with VLAN(s) support.

2 Configure the dedicated link by:

   a Choosing an extended switch port that is connected physically to the firewall interface.

   b Portshielding the port to the firewall interface.

   c Choosing the dedicated link option.

3 Select the extended switch port on which VLAN(s) need to be enabled

4 Portshield the switch port to the firewall interface.

5 Configure the required VLAN(s) under the VLAN tab.

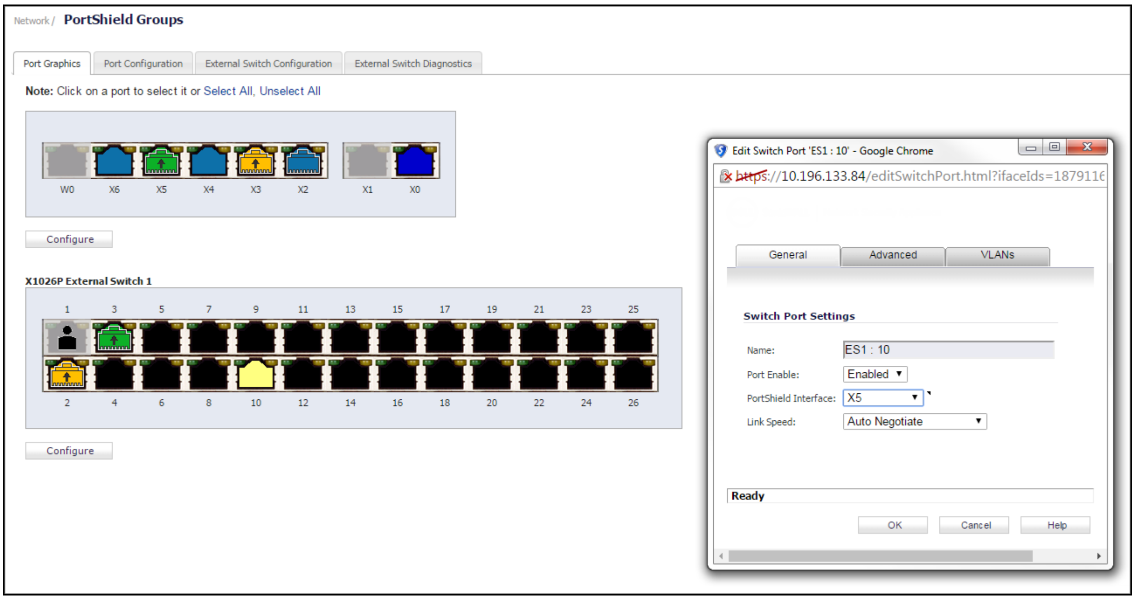
To configure a dedicated uplink for VLANs without a common uplink:

1 Provision the switch as described in Provisioning an X-Switch on a SonicWall Appliance on page 10.

2 Set up the data uplink as described in Adding an Extended Switch on page 21.

3 Configure the options as described in Configuring a Dedicated Uplink on page 33 except ensure to select the **Dedicated Uplink** option.

When a dedicated uplink is set up for a given firewall interface, if VLAN(s) exist under the firewall interface, a new tab, **VLANs**, displays on the **Edit Switch Port** dialog when the PortShield Interface is selected:



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

~~https~~://10.196.133.84/editSwitchPort.html?ifaceIds=187911€

Switch Port Settings

Name: ES1 : 10

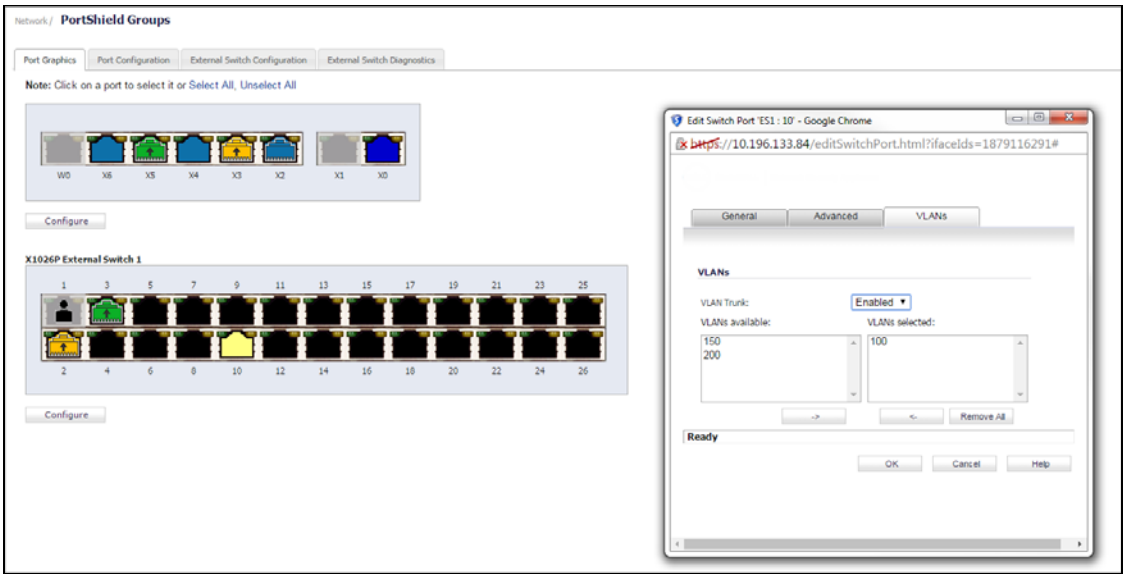
Port Enable: Enabled

PortShield Interface: X5

Link Speed: Auto Negotiate

Ready

4 Use the **VLANs** tab to configure an extended switch port in trunk or access mode. In this example, Port 10 is portshielded to X5 and configured as a trunk to carry VLAN 100 by selecting **Enabled** for the **VLAN Trunk** option and choosing **VLAN 100** from the available list of VLANs:



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

X1026P External Switch 1

Edit Switch Port 'ES1 : 10' - Google Chrome

https://10.196.133.84/editSwitchPort.html?ifaceIds=1879116291#

VLANs

VLAN Trunk: Enabled

VLANs available: 150 200

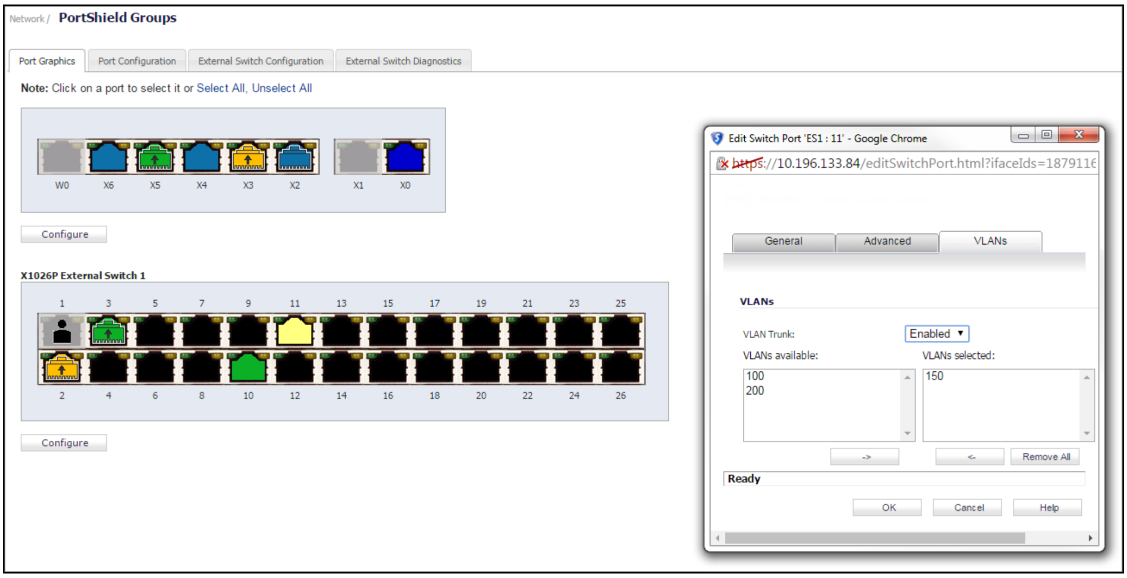
VLANs selected: 100

Ready

5 Similarly, Port 11 is portshielded to X5 and configured as a trunk to carry VLAN 150 by:

a Selecting **Enabled** for the **VLAN Trunk** option.

b Choosing **VLAN 150** from the available list of VLANs.



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

X1026P External Switch 1

Edit Switch Port 'ES1 : 11' - Google Chrome

https://10.196.133.84/editSwitchPort.html?ifaceIds=187911€

VLANs

VLAN Trunk: Enabled

VLANs available: 100 200

VLANs selected: 150

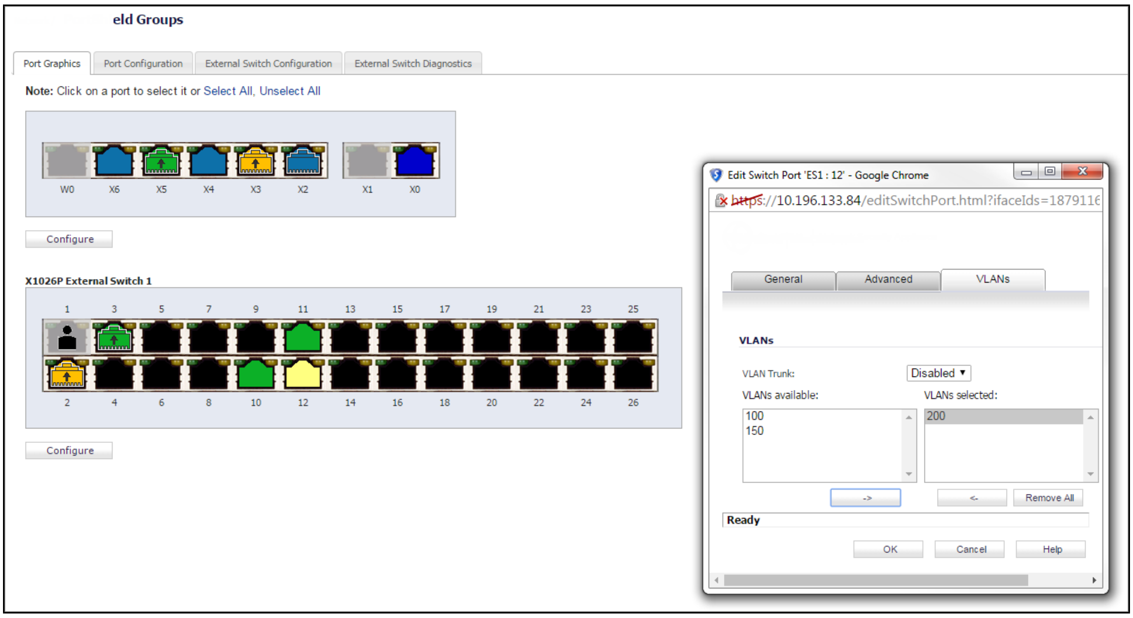
Ready

6 Portshield port 12 to X5 and configure it as an access for VLAN 200 by:

a Selecting **Disabled** for the **VLAN Trunk** option.

b Choosing **VLAN 200** from the available list of VLANs:

> ⓘ **NOTE:** For access, only a single VLAN can be selected from the available list of VLANs, whereas when configured as a trunk, multiple VLANs can be selected for a given port.



eld Groups
Port Graphics
Port Configuration
External Switch Configuration
External Switch Diagnostics
Note: Click on a port to select it or Select All, Unselect All
W0
X6
X5
X4
X3
X2
X1
X0
Configure
X1026P External Switch 1
1
3
5
7
9
11
13
15
17
19
21
23
25
2
4
6
8
10
12
14
16
18
20
22
24
26
Configure
Edit Switch Port 'ES1 : 12' - Google Chrome
https://10.196.133.84/editSwitchPort.html?ifaceIds=187911€
General
Advanced
VLANs
VLANs
->
<-
Remove All
Ready
OK
Cancel
Help

VLAN Trunk: Disabled

VLANs available: 100, 150

VLANs selected: 200

With this configuration, port 3 on the extended switch carries tagged traffic for VLANs 100,150, and 200 and untagged traffic for IDV VLAN 6. Port 10 is a trunk port carrying tagged traffic for VLAN 100, Port 11 is a trunk port carrying tagged traffic for VLAN 150, and Port 12 is an access port carrying untagged traffic for VLAN 200. Ports 10, 11, and 12 are portshielded to X5 through the dedicated link between X5 and port 2.

Configuring a Dedicated Link for SonicPoint Access

It is recommended that SonicPoint access points be connected through dedicated links because SonicPoint access points carry several VLANS, and dedicated links pass through VLAN tunnels. The dedicated links act as trunks passing tagged traffic from the access point through the X-Series switch to the firewall.

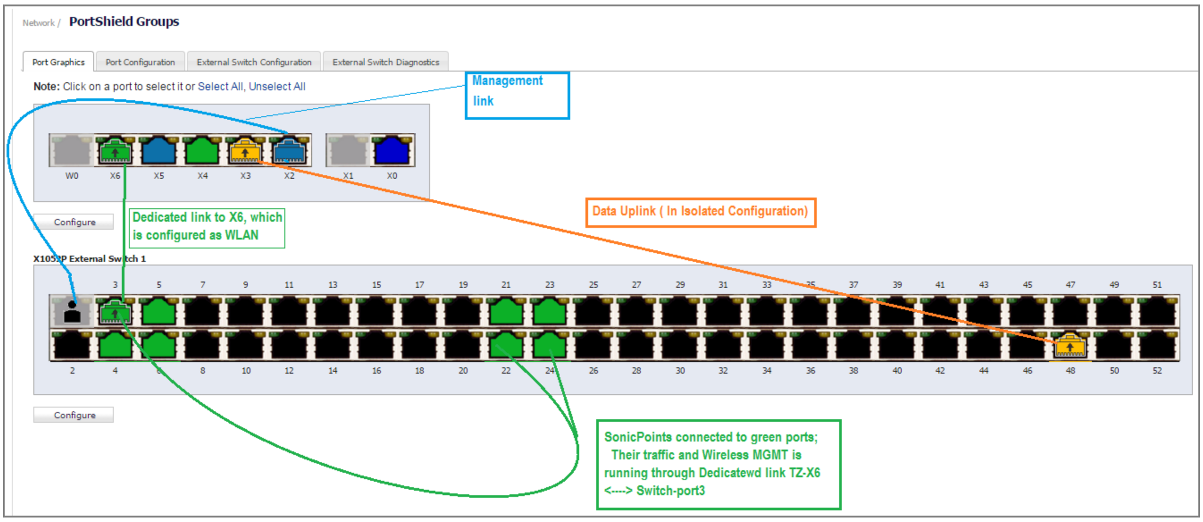
For non-SonicPoint access points and for SonicPoints without particular management, the port in the firewall can be configured as **ANY** (LAN/WAN/DMZ, although usually LAN). In this case, the pair of ports between the firewall and the X-Series switch must be configured as a dedicated link. Other ports on the switch that are expected to connect to access points with RJ45 are portshielded to that dedicated port.

If the SonicPoint access points are behind the firewall and are to be managed, the pair ports on the firewall and the X-Series switch must be configured as a dedicated link. The dedicated port on the firewall must be configured as WLAN. Other ports on the switch that are expected to connect to SonicPoint access points with RJ45 are portshielded to that dedicated port.

> ⓘ **IMPORTANT:** Any SonicPoint with an external power source (AC power supply or power adapter) can be portshielded to any Ethernet port.

When SonicPoints are configured with X-Series switches, the SonicPoints must be portshielded in a group configured to a port of the dedicated link. See SonicPoints And a Dedicated Uplink.

SonicPoints And a Dedicated Uplink



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

Management link

Data Uplink (In Isolated Configuration)

Dedicated link to X6, which is configured as WLAN

SonicPoints connected to green ports; Their traffic and Wireless MGMT is running through Dedicatewd link TZ-X6 <----> Switch-port3

For more information about using SonicPoints with an X-Series switch, see *SonicWall TZ Series and SonicWall X-Series managing SonicPoint ACe/ACi/N2 access points* (SW13970).

To configure a dedicated uplink for SonicPoints:

1. Provision the switch as described in Provisioning an X-Switch on a SonicWall Appliance on page 10.
2. Set up the data uplink as described in Adding an Extended Switch on page 21.
3. Configure the uplinks as described in Configuring a Dedicated Uplink for VLANs on page 50.
4. Ensure that all SonicPoints are connected to X-Switch ports configured in the PortShield group of the dedicated link.

Index

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 6.5 X-Series Deployment Guide
Updated - January 2019
Software Version - 6.5.3
232-004680-00 Rev A

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