

# SonicWall<sup>®</sup> SonicOS 6.5 X-Series/N-Series Solution

Deployment Guide

SONICWALL<sup>®</sup>

# Contents

<b>About the SonicWall SonicOS 6.5 X-Series/N-Series Solution</b> .....	<b>3</b>
SonicWall SonicOS 6.5 X-Series/N-Series Solution: a Unified Approach .....	3
Performance Requirements .....	5
Features Provided by the SonicWall SonicOS 6.5 X-Series/N-Series Solution .....	5
PortShield Functionality and X-Series/N-Series Switches .....	7
Portshield Interfaces .....	7
Portshield Traffic .....	7
PoE/PoE+ and SFP/SFP+ Support .....	7
SonicOS 6.5 X-Series/N-Series and SonicPoints .....	8
Recommended Reading .....	9
<b>Provisioning an X-Series/N-Series Switch on a SonicWall Appliance</b> .....	<b>10</b>
Provisioning Through the Firewall User Interface .....	10
Interface Settings .....	13
Portshield Wizard .....	16
Show Portshield Interfaces .....	17
Interface Traffic Statistics .....	17
Adding a Default Gateway Through the Firewall UI .....	18
Provisioning Through the CLI .....	19
<b>Adding the X-Series/N-Series Switch to SonicOS</b> .....	<b>20</b>
Adding an Extended Switch .....	20
Adding an Extended Switch in Daisy Chain Mode .....	22
Deleting an Extended Switch .....	26
Replacing an Extended Switch .....	26
<b>Configuring the SonicOS 6.5 X-Series/N-Series Switch in Various Topologies</b> .....	<b>27</b>
About Topologies .....	27
Connecting the X-Series/N-Series Switch Management Port to a SonicWall Firewall .....	28
Configuring the Different Topologies .....	29
Configuring a Common Uplink .....	29
Configuring a Dedicated Uplink .....	32
Configuring a Hybrid System With Common and Dedicated Uplink(s) .....	38
Configuring Isolated Links for Management and Data Uplinks .....	39
Configuring HA and PortShield With Dedicated Uplink(s) .....	42
Configuring HA and PortShield With a Common Uplink .....	45
Configuring VLAN(s) With Common or Dedicated Uplink(s) .....	46
Configuring a Dedicated Link for SonicPoint Access .....	52

<b>SonicWall Support</b> .....	<b>55</b>
About This Document .....	56

# About the SonicWall SonicOS 6.5 X-Series/N-Series Solution

## Topics:

- [SonicWall SonicOS 6.5 X-Series/N-Series Solution: a Unified Approach](#) on page 3
- [Performance Requirements](#) on page 4
- [Features Provided by the SonicWall SonicOS 6.5 X-Series/N-Series Solution](#) on page 4
- [PortShield Functionality and X-Series/N-Series Switches](#) on page 6
- [PoE/PoE+ and SFP/SFP+ Support](#) on page 7
- [SonicOS 6.5 X-Series/N-Series and SonicPoints](#) on page 7
- [Recommended Reading](#) on page 8

## SonicWall SonicOS 6.5 X-Series/N-Series Solution: a Unified Approach

Critical network elements, such as a firewall and switch, need to be managed, usually individually. The SonicWall® allows unified management of the firewall and the switches using the firewall management interface 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 ranges from 5 (TZ300) to 10 (TZ600).

This feature is supported on all SonicWall firewalls running SonicOS 6.5 or SonicOS 6.2.7 and higher, except for the following:

- NSsp 12000 series
- SuperMassive 9800
- NSA 2600

**NOTE:** The switches are also supported on SOHOW platforms for the SonicOS 6.5.3.2 release.

With the SonicWall SonicOS 6.5 X-Series/N-Series Solution, switch ports are viewed as extended interfaces of the firewall, thereby increasing the number of interfaces available for use up to 192, depending on the switches. These extended ports can be portshielded and/or configured for high availability and treated as any other interface on the firewall.

The TZ Series firewalls support a maximum of two switches. A SonicWall firewall can provision up to four switches.

**NOTE:** For complete information about X-Series/N-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, Dell EMC Networking N-Series N1100-ON, N1500, N2000, N2100-ON, N3000, N3000-ON, N3100-ON, and N4000 Switches User's Configuration Guide*.

<b>HA</b>	High Availability
<b>IDV</b>	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.
<b>PoE</b>	Power over Ethernet – A system that 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.
<b>PoE+</b>	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.
<b>SFP</b>	Small form-factor pluggable – A compact, hot-pluggable transceiver used for both telecommunication and data communications applications and supports 1Gb fiber modules.
<b>SFP+</b>	Enhanced small form-factor pluggable – An enhanced version of SFP that supports 10 Gb fiber modules.
<b>SPM</b>	Single Point Management
<b>STP</b>	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, 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 switches.
- Manage an increased number of ports.
- Be connected in daisy chain mode. The firewall is connected to a switch, which in-turn is connected to another switch.

## Features Provided by the SonicWall SonicOS 6.5 X-Series/N-Series Solution

Key features supported by the SonicWall SonicOS 6.5 X-Series/N-Series Solution are:

- Provisioning a switch as an extended switch – Up to four switches can be provisioned as an extended switch on a SonicWall firewall. When provisioned, the switch ports are managed as are the other ports of the firewall.
- PortShield functionality – Switch ports are viewed as “extended” interfaces of the firewall and can join PortShield Groups. For further information, see [PortShield Functionality and X-Series/N-Series Switches](#) on page 6.
- Configuring the extended switch interface settings – The switch interface settings are configured as regular ones 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 switch integration feature allows unified management of 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 [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 switch. For example, if X3 and X5 are configured for dedicated uplinks, VLAN 100 cannot be present under X3 and X5. Such a configuration is rejected. If X3 and X5 are dedicated uplinks to different 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 a switch and VLAN 100 exists under X3, another interface—X4, which is configured as a common uplink to a second switch, cannot have a VLAN 100 subinterface.

For more 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 switch to carry:
  - Management traffic of the firewall managing the switch.
  - PortShield traffic for the IDV VLANs corresponding to the firewall interfaces.
  - Traffic for the VLAN subinterfaces present under the common uplink interface.

For more information about SPM support, see [Configuring a Common Uplink for VLAN\(s\) With SPM](#) on page 47.

- 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 a 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 switches.
- Batching configuration messages – To facilitate faster programming of switches, configuration messages can be batched before being sent to a switch.
- Switch Daisy Chaining solution enables integration of the firewall with the 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 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/N-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/N-Series switches, see the [SonicOS 6.5 System Setup Administration Guide](#).

### Portshield Interfaces

The SonicOS 6.5 X-Series/N-Series Solution allows support for portshielding interfaces on the extended switch to firewall interfaces. X-Series/N-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 switches. 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 more information about which ports on which models are PoE/PoE+ capable, see the [Dell™ Networking™ X1000 and X4000 Series Switches Getting Started Guide](#).

**NOTE:** For complete information about X-Series/N-Series PoE and SFP support, see the [Dell Networking X1000 and X4000 Series Switches User Guide](#) and the [Dell EMC Networking N-Series N1100-ON, N1500, N2000, N2100-ON, N3000, N3000-ON, N3100-ON, and N4000 Switches User's Configuration Guide](#).

**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 switches is managed from the UI of the switches and the **MANAGE | System Setup | Network > Portshield Groups** page on the firewall.

## SonicOS 6.5 X-Series/N-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 the 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 switch does not support PoE+, you must use a SonicPoint power injector. 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

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

# Provisioning an X-Series/N-Series Switch on a SonicWall Appliance

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

**IMPORTANT:** When an extended switch has been powered off and the firewall is restarted (rebooted), it may take up to five 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](#) on page 10
- [Interface Settings](#) on page 13
- [Interface Traffic Statistics](#) on page 16
- [Adding a Default Gateway Through the Firewall UI](#) on page 18

## Provisioning Through the Firewall User Interface

More 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 a switch on a SonicWall firewall through the switch's user interface:

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

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

**i** **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 switch directly via its GUI/console. To do so results in the firewall being out of sync with the configuration state of the switch.

- 2 Ensure the switch is in Managed Mode.

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

**i** **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 more information, 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 paper clip into the Managed Mode opening and pressing the Managed Mode button for seven seconds. The Managed Mode button is a small button located on the:
  - Right side of the rear panel on X1008/X1008 X-Series/N-Series Switches.
  - Left side of the rear panel on all other switches.

Use a straightened paper clip to press the button.

After seven seconds, the switch reboots to change to Managed Mode.

- 3 Connect the switch console:
  - By an RJ45 cable to a PC in the same subnet as the switch, if configuring through its GUI.
  - Through Telnet (9600 baud, if configuring through the CLI).
- 4 Power on the switch.

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



SONICWALL™  
Network Security Appliance

Username  
admin

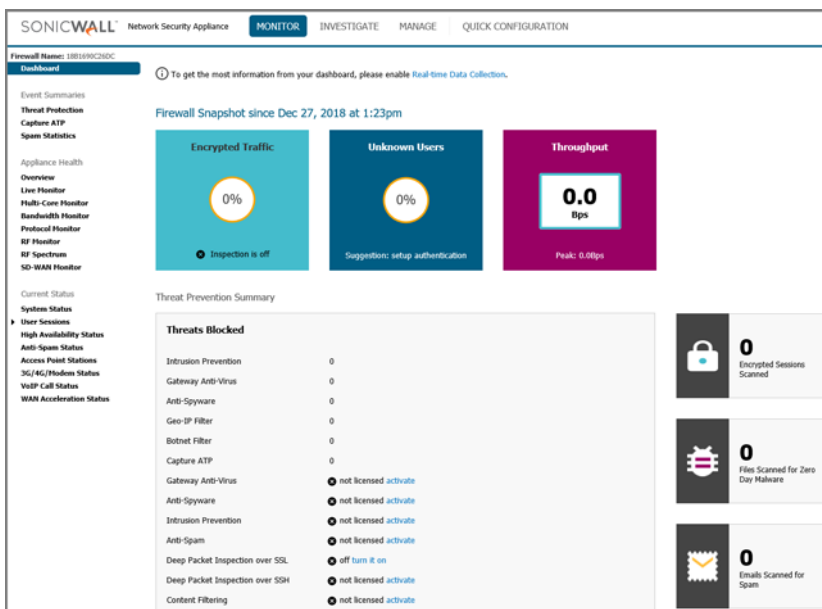
Password  
●●●●●●●●

LOG IN

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


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

The **MONITOR > Dashboard** page displays.



SONICWALL™ Network Security Appliance MONITOR INVESTIGATE MANAGE QUICK CONFIGURATION

Firewall Name: 188169C2NDG

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

Event Summaries  
Threat Protection  
Capture ATP  
Spam Statistics

Appliance Health  
Overview  
Live Monitor  
Hub-Core Monitor  
Bandwidth Monitor  
Protocol Monitor  
RF Monitor  
RF Spectrum  
SD-WAN Monitor

Current Status  
System Status  
User Sessions  
High Availability Status  
Anti-Spam Status  
Access Point Stations  
3G/4G/Proton Status  
VoIP Call Status  
WAN Acceleration Status

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

Encrypted Traffic: 0%  
Unknown Users: 0%  
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 <a href="#">activate</a>
Anti-Spyware	● not licensed <a href="#">activate</a>
Intrusion Prevention	● not licensed <a href="#">activate</a>
Anti-Spam	● not licensed <a href="#">activate</a>
Deep Packet Inspection over SSL	● off <a href="#">turn it on</a>
Deep Packet Inspection over SSH	● not licensed <a href="#">activate</a>
Content Filtering	● not licensed <a href="#">activate</a>

0 Encrypted Sessions Scanned

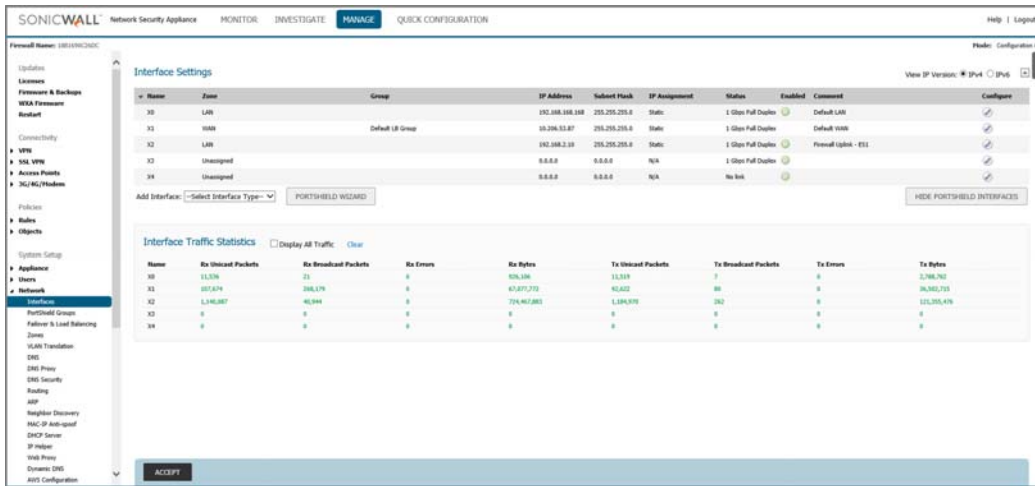
0 Files Scanned for Zero Day Malware

0 Emails Scanned for Spam

- If you have not recorded the switch's information in [Step 1](#), do so now.

# Interface Settings

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



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

- Under **Interface Settings**, choose the switch port you want and decide whether you wish to administratively shut down the port for the switch under the **Enabled** column.
- 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
<b>Name</b>	The designation of the firewall
<b>Zone</b>	The properties of the firewall, its security type, member interfaces, interface trust, anti-virus, SEC, DPI-SSL Enforcement, and GSC
<b>Group</b>	Whether the firewall belongs to the Default LB Group
<b>IP Address</b>	The numeric address of the firewall
<b>Subnet Mask</b>	The numeric subdivision of the IP address
<b>IP Assignment</b>	The setting of the IP address, whether it is static or dynamic
<b>Status</b>	Whether the firewall is one gigabit port in full duplex and can receive one gigabit per second in both directions
<b>Enabled</b>	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
<b>Comment</b>	Whether the default local area network ( <b>Default LAN</b> ) is being used or the connection is being made from the firewall ( <b>Firewall UPLink</b> )
<b>Configure</b>	The details needed to make your firewall work properly

- 6 Select **Interface Type** at the bottom of the **Interface Settings** table and 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
<b>Virtual Interface</b>	A software-based interface created in the memory of the firewall
<b>VPN Tunnel Interface</b>	A virtual private network interface on a security gateway that connects to a remote peer
<b>WLAN Tunnel Interface</b>	A wireless local area network (WLAN) interface on a security gateway that connects to a remote peer
<b>4to6 Tunnel Interface</b>	Tunneling of IPv4 in an IPv6 only network

- 7 On the far right of the table, under the **Configure** column, click the **Edit** icon to set up your firewall. The pop-up dialog box below appears.

SONICWALL™ Network Security Appliance

General Advanced

### Interface 'X1' Settings

Zone:

IP Assignment:

IP Address:

Subnet Mask:

Default Gateway:

DNS Server 1:

DNS Server 2:

DNS Server 3:

Comment:

Management:  HTTPS  Ping  SNMP  SSH

User Login:  HTTP  HTTPS

Add rule to enable redirect from HTTP to HTTPS

Ready

OK CANCEL HELP

- 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.

SONICWALL™ Network Security Appliance

General Advanced

### Interface 'X1' Settings

Zone: Unassigned  
Create new zone...  
LAN  
WAN  
DMZ  
WLAN

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

OK CANCEL HELP

- 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

OK CANCEL HELP

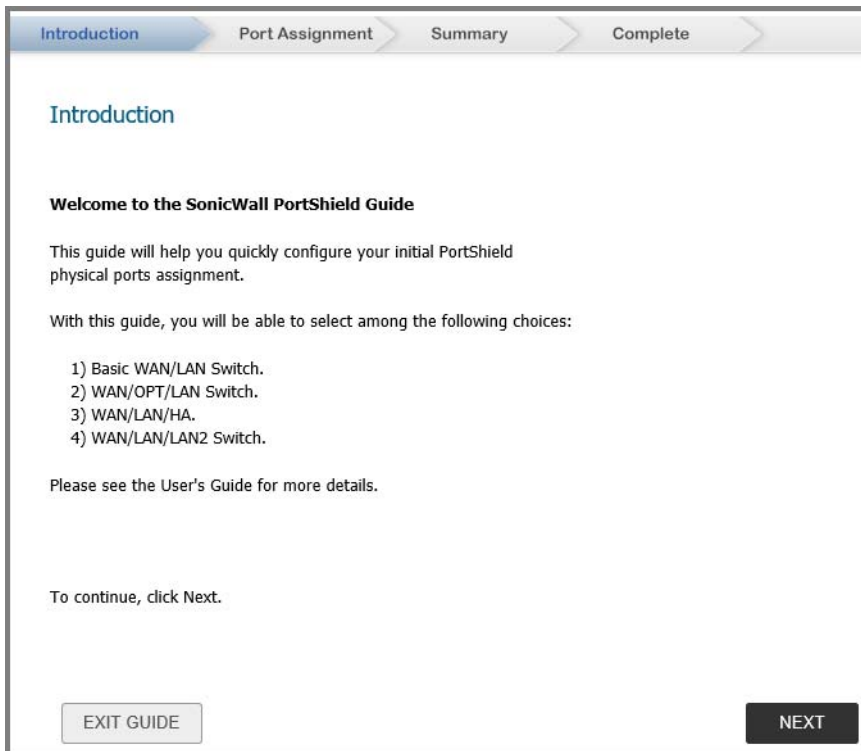
- 3 Refer to the following table for more information on the Configuration **IP Assignments** from the drop-down menu:

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 pop-up **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 appears informing you that if you exit the guide your changes are not be saved. Click **OK** or **Cancel**.





## 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 **ACCEPT**. Refer to the following table for more information on the Interface Traffic Statistics:

Interface Traffic Statistics	Definition
<b>Name</b>	The name of the firewall you want to display information for
<b>RX Unicast Packets</b>	The number of point-to-point communications received by the interface
<b>Rx Broadcast Packets</b>	The number of multi-point communications received by the interface
<b>Rx Errors</b>	The number of error packets received on the selected interface

Interface Traffic Statistics	Definition
Rx Bytes	The volume of data, in bytes, received by the interface
Tx Unicast Packets	The number of point-to-point communications transmitted by the interface
Tx Broadcast Packets	The number of multipoint communications transmitted by the interface
Tx Errors	The number of error packets transmitted on the selected interface
Tx Bytes	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 **IPv4** or **IPv6**.

Name	Zone	IP Assignment	IP Address/Prefix Length	IP Type	Status	Comment	Configure
X0	LAN	Static	fd00:1ab1:69ff:fd0c:264d/10	Automatic	1 Gbps Full Duplex	Default LAN	ⓘ
X1	WAN	Static	fd00:1ab1:69ff:fd0c:264d/10	Automatic	1 Gbps Full Duplex	Default WAN	ⓘ
X2	LAN	Static	fd00:1ab1:69ff:fd0c:264d/10	Automatic	1 Gbps Full Duplex	Firewall Uplink - ES1	ⓘ
X3	Unassigned	N/A			1 Gbps Full Duplex		ⓘ
X4	Unassigned	N/A			No link		ⓘ

- 2 Click the **Edit** icon, under the **Configure** column, and enter the default gateway IP address in the **IPv6 Address** field.

SONICWALL™ Network Security Appliance

General Advanced Router Advertisement

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

OK CANCEL HELP


- 3 Click **OK**.

## Provisioning Through the CLI

### Topics:

- [Provisioning Without a Default Gateway](#) on page 19
- [Provisioning With a Default Gateway](#) on page 19

## Provisioning Without a Default Gateway

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

### *To provision the switch on a SonicWall firewall without a default gateway:*

- 1 Provision the switch by performing the steps in [Provisioning Through the Firewall User Interface](#).
- 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 switch by pinging it from the firewall before provisioning/managing the switch from the firewall.

## Provisioning With a Default Gateway

### *To provision the switch on a SonicWall firewall with a default gateway:*

- 1 Provision the switch by performing the steps in [Provisioning Through the Firewall User Interface](#).
- 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 switch by pinging it from the firewall before provisioning/managing it from the firewall.

# Adding the X-Series/N-Series Switch to SonicOS

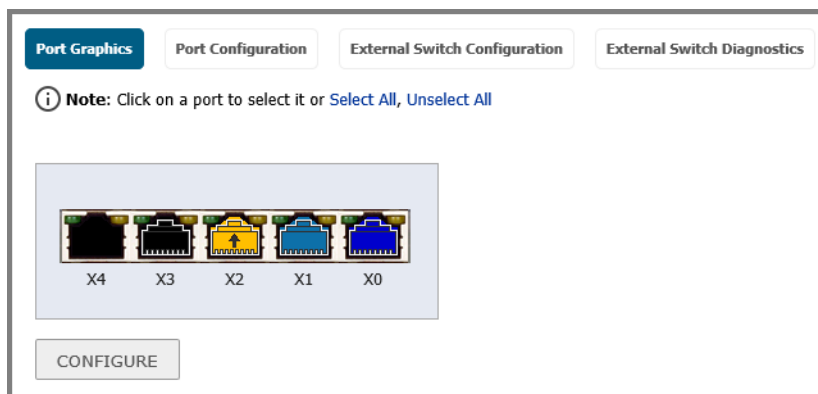
- [Adding an Extended Switch](#) on page 20
- [Adding an Extended Switch in Daisy Chain Mode](#) on page 22
- [Deleting an Extended Switch](#) on page 26
- [Replacing an Extended Switch](#) on page 26

## Adding an Extended Switch

**NOTE:** To manage the switch from the firewall, one of its IP addresses needs to be in the same subnet as the switch. For example, to manage a switch with a default IP address of 192.168.2.3, the interface of the firewall needs to be configured in the 192.168.2.0 subnet and be connected to the 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 it.
- 3 Navigate to **MANAGE | System Setup | Network > PortShield Groups** page.



- 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	⊕ ⊗

ADD SWITCH

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

**SONICWALL™** Network Security Appliance

**General** | **Advanced**

ID:

Switch Model:

IP Address:

User Name:

Password:

Confirm Password:

Switch Mode:

Switch Management:

Firewall Uplink:

Switch Uplink:

**Ready**

**ADD** **CLOSE**

- From the **ID** drop-down menu, select the ID of the switch. The default is **1**.
- From the **Switch Model** drop-down menu, select the model of the external switch. The default is **X1008**.
- In the **IP Address** field, enter the IP address of the switch obtained from the label on the switch.
- In the **User Name** field, enter the user ID obtained from the label on the switch.
- In the **Password** field, enter either the password obtained from the label on the switch or the one you gave when installing the switch.
- In the **Confirm Password** field, enter the password a second time.

**i** **TIP:** For how to configure the **Switch Management**, **Firewall Uplink**, and **Switch Uplink** options, see the subsection for your topology in [Configuring the X-Series/N-Series Switch in Various Topologies](#) on page 27.

- From the **Switch Management** drop-down menu, select the port on the extended switch to be used for management traffic. The default is **1**.
- From the **Firewall Uplink** drop-down menu, select the port on the firewall to be used as the uplink port. The default is **None**.
- 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**.
- Optionally, click the **Advanced** tab. The options on the tab depend on the extended switch you are adding:

The screenshot shows a configuration interface with two tabs: 'General' and 'Advanced'. The 'Advanced' tab is selected. Below the tabs, there are two dropdown menus. The first is labeled 'STP Mode' and has 'Rapid' selected. The second is labeled 'STP State' and has 'Enabled' selected.

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)

18 Click **ADD**.

## Adding an Extended Switch in Daisy Chain Mode

You can connect extended 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 and the password.
- 3 See the daisy chain 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
<b>Name</b>	The designation of the X-switch
<b>PortShield Interface</b>	The virtual interface with a set of ports assigned to it.
<b>Type</b>	Whether it is copper or fiber optics
<b>Link Settings</b>	Auto negotiate is the default
<b>Link Status</b>	Whether it is 1Gbps Full Duplex or no link
<b>Enabled</b>	The setting of the IP address, whether it is static or dynamic
<b>Comment</b>	Any user-defined comments
<b>Configure</b>	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
<b>ID</b>	The designation of the switch
<b>Model</b>	The product detail information, name, and interfaces.
<b>Status</b>	Displays a green circle when the switch is on. Displays a red circle when the switch is not reachable from the SonicWall appliance.

Settings	Definition
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 ( <b>Default LAN</b> ) is being used or the connection is being made from the firewall ( <b>Firewall Uplink</b> )
Switch Uplink	Whether the switch is connected to the device via a port.
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 switch work properly

ID	Model	Status	IP Address	Switch Mode	Switch Management	Firewall Uplink	Switch Uplink	Parent Switch ID	Parent Switch Uplink	Configure
1	X1010	●	192.168.2.2	Stand-alone	2	X2	2	N/A	N/A	ⓘ ✕
2	X2100	●	192.168.2.3	Daisy-chain	N/A	N/A	7	1	7	ⓘ ✕

ADD SWITCH

- Click **External Switch Diagnostics** for testing purposes or to check the hardware functionality while it is connected to the network.
- Go to the **Switch Name** drop-down menu, on the top left above the table, to choose the switch you want.
  - **ES1** and **ES2** display.
- 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 <b>Up</b> or <b>Down</b>
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.
Tx Broadcast Packets	Indicates the number of multi-point communications transmitted by the interface.



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

Port Graphics   Port Configuration   External Switch Configuration   **External Switch Diagnostics**

Switch Name:

Statistics: External Switch 1 CLEAR

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	11,556,328	8,256,944	2,764,020,725	0	38,809,722	1,106,202	20	15,586,076,368	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	68,124	12	5,371,547,333	0	14,472,632	12,655,600	8,251,654	5,879,804,999	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

- 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**.
- 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.
- 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.

**i** | **IMPORTANT:** A pop-up 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 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.

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

# Configuring the X-Series/N-Series Switch in Various Topologies

- IMPORTANT:** Before setting up the interface between the SonicWall firewall and the switch, set it up as described in [Provisioning an X-Series/N-Series Switch on a SonicWall Appliance](#) on page 10.
- IMPORTANT:** When an extended switch has been powered off and the firewall is restarted (rebooted), it may take up to five 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 five minutes for the configuration to be displayed on the **MANAGE | System Setup | Network > PortShield Groups** page.

- [About Topologies](#) on page 27
  - [About Links](#) on page 28
- [Connecting the X-Series/N-Series Switch Management Port to a SonicWall Firewall](#) on page 28
- [Configuring the Different Topologies](#) on page 29
  - [Configuring a Common Uplink](#) on page 29
  - [Configuring a Dedicated Uplink](#) on page 32
  - [Configuring a Hybrid System With Common and Dedicated Uplink\(s\)](#) on page 38
  - [Configuring Isolated Links for Management and Data Uplinks](#) on page 39
  - [Configuring HA and PortShield With Dedicated Uplink\(s\)](#) on page 42
  - [Configuring HA and PortShield With a Common Uplink](#) on page 45
  - [Configuring VLAN\(s\) With Common or Dedicated Uplink\(s\)](#) on page 46
  - [Configuring a Dedicated Link for SonicPoint Access](#) on page 52

## About Topologies

The key supported topologies for the SonicOS 6.5 X-Series/N-Series Switch 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 switches for management of 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 switch 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 children interfaces).

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

The interface connected to the management port of the 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 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

**i** **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 20. The following sections describe only those steps required for the various topologies.

## Topics:

- [Configuring a Common Uplink](#) on page 29
- [Configuring a Dedicated Uplink](#) on page 32
- [Configuring a Hybrid System With Common and Dedicated Uplink\(s\)](#) on page 38
- [Configuring Isolated Links for Management and Data Uplinks](#) on page 39
- [Configuring HA and PortShield With Dedicated Uplink\(s\)](#) on page 42
- [Configuring HA and PortShield With a Common Uplink](#) on page 45
- [Configuring VLAN\(s\) With Common or Dedicated Uplink\(s\)](#) on page 46
- [Configuring a Dedicated Link for SonicPoint Access](#) on page 52

## Configuring a Common Uplink

X-Series/N-Series switches can be managed by the firewall, thereby providing a unified management option. This configuration allows a single link between the firewall and the 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 that 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 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 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.

**i** **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 39.

## Common Uplink Topology



### To configure a common link:

- 1 Set up the switch as described in [Provisioning an X-Series/N-Series 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.

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	<input checked="" type="checkbox"/>	Default LAN	<a href="#">Configure</a>
X1	WAN	Default LB Group	19.206.53.87	255.255.255.0	Static	1 Gbps Full Duplex	<input checked="" type="checkbox"/>	Default WAN	<a href="#">Configure</a>
X2	LAN		192.168.2.10	255.255.255.0	Static	1 Gbps Full Duplex	<input checked="" type="checkbox"/>	Firewall Uplink - FS1	<a href="#">Configure</a>
X3	Unassigned		0.0.0.0	0.0.0.0	N/A	1 Gbps Full Duplex	<input checked="" type="checkbox"/>		<a href="#">Configure</a>
X4	Unassigned		0.0.0.0	0.0.0.0	N/A	No link	<input checked="" type="checkbox"/>		<a href="#">Configure</a>

Name	Rx Unicast Packets	Rx Broadcast Packets	Rx Errors	Rx Bytes	Tx Unicast Packets	Tx Broadcast Packets	Tx Errors	Tx Bytes
X0	15,763	40	0	867,561	15,757	0	0	2,597,816
X1	75,491	589,702	0	150,886,594	55,844	70	0	25,685,361
X2	1,064,797	38,224	0	677,054,844	1,189,116	236	0	113,454,418
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 **External Switch Configuration**.

7 Click **ADD SWITCH**. The **Add External Switch** dialog displays.

8 Configure the **ID** through **Confirm Password** options as described in [Adding an Extended Switch](#) on page 20.

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.

11 For information about configuring the **Advanced** tab, see [Adding an Extended Switch](#) on page 20.

12 Click **ADD**. The **External Switch Configuration** tab shows the link between X2 and the switch port 2.

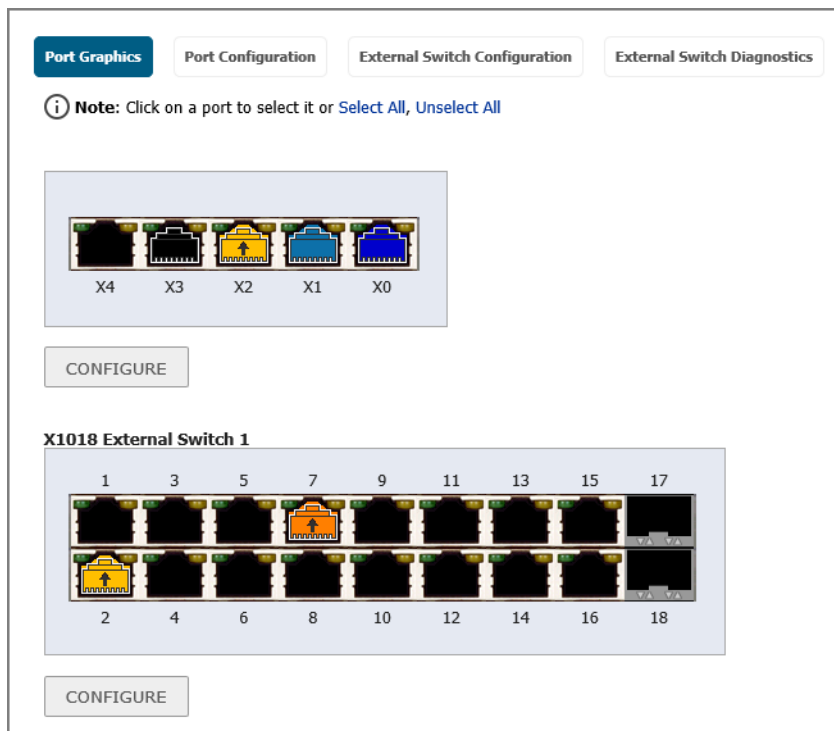
ID	Model	Status	IP Address	Switch Mode	Switch Management	Firewall Uplink	Switch Uplink	Parent Switch ID	Parent Switch Uplink	Configure
1	X2108	Enabled	192.168.2.2	Stand-alone	2	X2	2	N/A	N/A	Configure
2	X2108P	Enabled	192.168.2.3	Daisy-chain	N/A	N/A	2	1	2	Configure

- **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 connected by cable.



14 To PortShield ports on the firewall and 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 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 switch.
- There is 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).

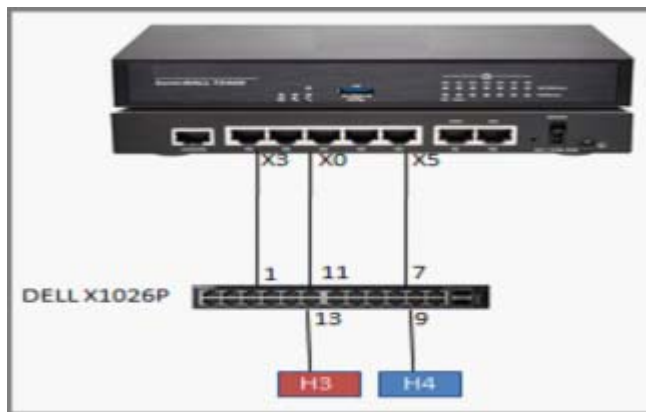
**IMPORTANT:** For the dedicated uplink to work, the physical link must be connected before being configured.



**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 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 33
- [Configuring a Dedicated Uplink With a Common Uplink](#) on page 35

## 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-Series/N-Series Switch on a SonicWall Appliance](#) on page 10.
- 2 Navigate to the **Network > PortShield Groups** page.
- 3 Click **External Switch Configuration**.

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

The screenshot shows the 'Edit External Switch' dialog box with the 'General' tab selected. The fields are as follows:

Field	Value
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

At the bottom of the dialog, there is a 'Ready' status bar, an 'OK' button, and a 'CANCEL' button.

- 5 Configure the **ID** through **Confirm Password** options as described in [Adding an Extended Switch](#) on page 20.
- 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 20.
- 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 **CONFIGURE**.
  - **Port Configuration** tab, click the **Edit** icon of the desired PortShield Interface.

The **Edit Switch Port** dialog displays.

The dialog box shows the following configuration:

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

Status: Ready

Buttons: OK, CANCEL

12 Click **OK**.

## Configuring a Dedicated Uplink With a Common Uplink

*To configure a dedicated uplink topology with a common uplink:*

- 1 Provision the switch as described in [Provisioning an X-Series/N-Series 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 20.

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 **Port Graphics**, the icons for firewall port X3 and switch port 2 are the same color and contain an up arrow.

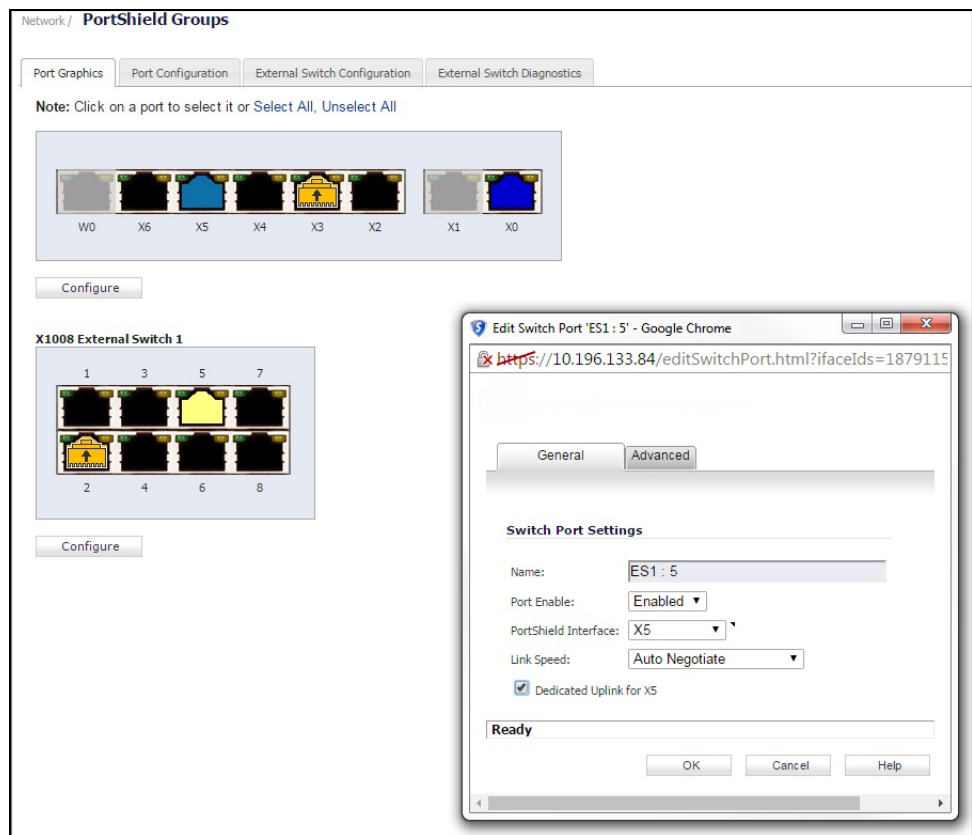


- 3 Click **Port Graphics** or **Port Configuration**.

4 On the:

- **Port Graphics** tab:

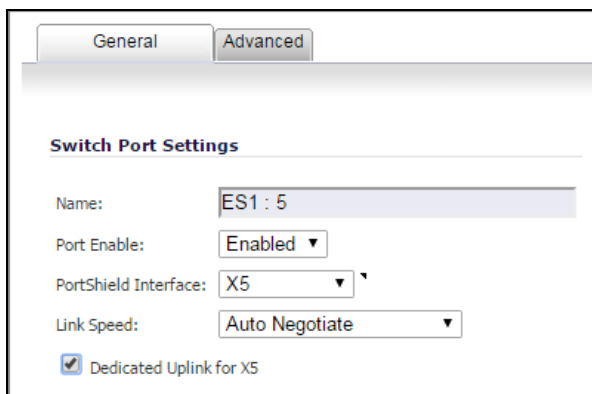
a) Select the desired PortShield Interface(s).



b) Click **Configure**.

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

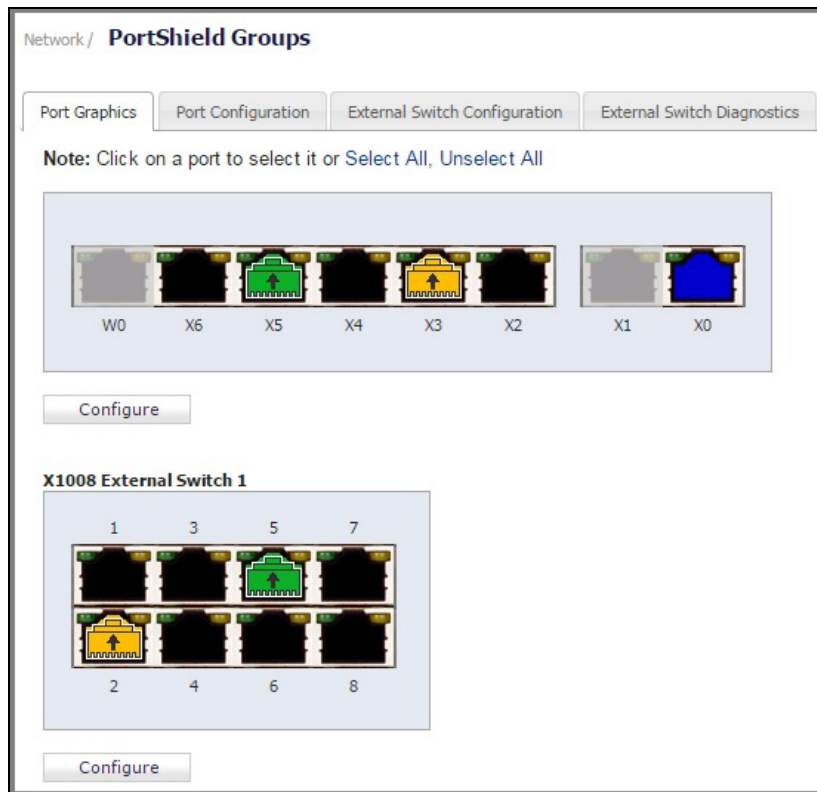
The **Edit Switch Port** dialog displays.



5 Select the **Dedicated Uplink** option.

6 Click **OK**.

The graphics under **Port Graphics** 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.



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

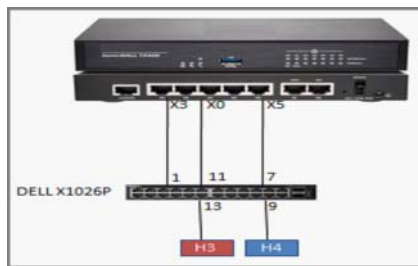
This configuration allows a combination of common and dedicated uplinks to be set up between the firewall and the switch. The dedicated uplinks are used to carry PortShield traffic corresponding to the connected firewall interface. The common uplink is used to carry PortShield traffic for the remaining 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 a 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/N-Series Switch to SonicOS](#) on page 20.
- 2 Configure the uplink as described in [Configuring a Dedicated Uplink With a Common Uplink](#) on page 35.

## Configuring Isolated Links for Management and Data Uplinks

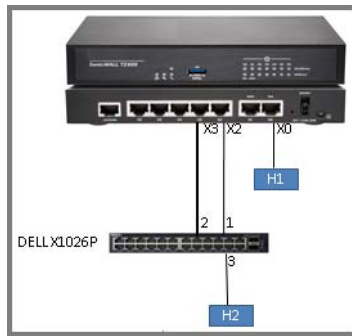
This configuration allows separate links between the firewall and switches to carry management traffic and data traffic. With a common link, the management traffic and data traffic run in the same uplink; if data traffic is congested, so is management traffic, which results in a delay in forwarding management traffic. If data traffic is 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-Series/N-Series Switch on a SonicWall Appliance](#) on page 10.
- 2 Set up the data uplink as described in [Adding an Extended Switch](#) on page 20.
- 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.

The screenshot shows the 'Add External Switch' dialog box with the 'General' tab selected. The fields are as follows:

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 20.
- 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:



General    Advanced

ID:

Switch Model:

IP Address:

User Name:

Password:

Confirm Password:

Switch Management:

Firewall Uplink:

Switch Uplink:

9 Click **ADD**.

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

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	<span style="color: green;">●</span>	192.168.2.1	1	X3	2	

**Port Graphics** displays:

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



# Configuring HA and PortShield With Dedicated Uplink(s)

**IMPORTANT:** To use the switch with HA, you must first create an HA system, and then add the switch.

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

- [Configuring HA Using One Extended Switch Management Port](#) on page 42
- [Configuring HA Using Two Extended Switch Management Ports](#) on page 43

## 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 switch on 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:

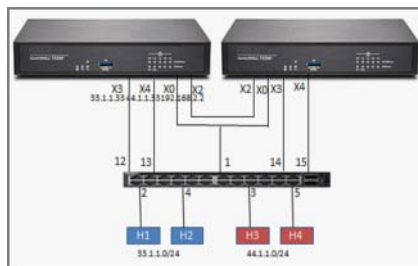
- The firewall interfaces, X3 and X4, on the primary unit are connected to ports 12 and 13 on the switch.
- X3 and X4 are configured as PortShield hosts.
- Similarly, the firewall interfaces X3 and X4 on the secondary unit are connected to ports 14 and 15 on the switch.
- Ports 12 and 14 on the switch 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-Series/N-Series Switch on a SonicWall Appliance](#) on page 10.
- 2 Set up the data uplink as described in [Adding an Extended Switch](#) on page 20.
- 3 Configure the options as described in [Configuring a Common Uplink](#) on page 29 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 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

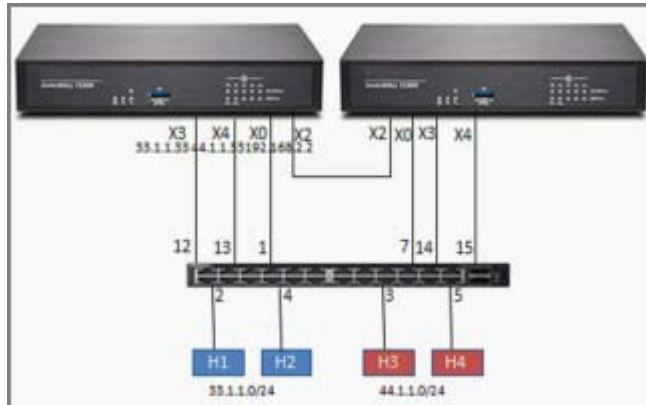
You can connect X0 of the primary and secondary firewalls directly to the ports on the switch. In this case, two switch ports are used on the switch for management traffic.

[HA Pair Using 2 Extended Switch Management Ports Topography](#) shows a 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-Series/N-Series Switch on a SonicWall Appliance](#) on page 10.
- 2 Set up the data uplink as described in [Adding an Extended Switch](#) on page 20.
- 3 Configure the options as described in [Configuring a Common Uplink](#) on page 29 except:
  - a Select the **Primary Switch Management** and **Primary Switch Management** interfaces from their respective drop-down menus:
    - (i) 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**.



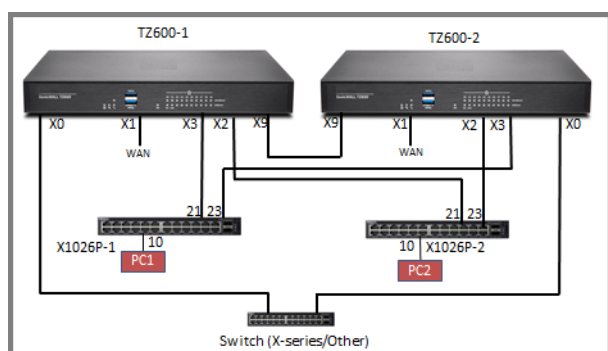
- 4 Click **ADD**.

# 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 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 a switch) and not the same 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-Series/N-Series Switch on a SonicWall Appliance](#) on page 10.
- 2 Set up the data uplink as described in [Adding an Extended Switch](#) on page 20.
- 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 29 except for these ports:

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

The screenshot shows the 'Advanced' configuration page for a switch. The fields are as follows:

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 XO |
|                      | 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 46
- [Configuring a Common Uplink for VLANs](#) on page 47
- [Configuring a Dedicated Uplink for VLANs](#) on page 49

### Prerequisites for VLAN Support

- Support for VLANs is available on 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 switch.
- Overlapping VLANs cannot exist under appliance interfaces configured as dedicated uplinks to the same switch because VLAN space on the switch is global. For example, if X3 and X5 are configured for dedicated uplinks to the same switch, VLAN 100 cannot be present under both X3 and X5. Such a configuration is rejected. If X3 and X5 are dedicated uplinks to different 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 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/N-Series Switch support for VLAN, see [SonicWall SonicOS 6.5 X-Series/N-Series Solution - Support for SonicWall Virtual Interfaces \(VLANs\) \(189771\)](#).

## Configuring a Common Uplink for VLANs

For information about prerequisites and limitationd for VLAN configurations, see [Prerequisites for VLAN Support](#) on page 46.

### Topics:

- [Configuring a Common Uplink for VLAN\(s\) With SPM](#) on page 47
- [Configuring a Dedicated Uplink Plus a Common Uplink for a VLAN](#) on page 49

## Configuring a Common Uplink for VLAN(s) With SPM

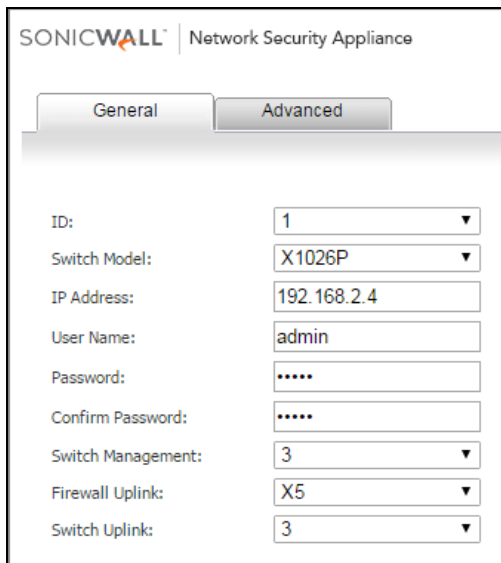
With Single Point of Management (SPM), you can configure a common uplink to carry management traffic of the firewall managing the switches plus PortShield traffic for the IDV VLANs corresponding to the firewall interfaces plus traffic corresponding to the VLAN subinterfaces under the common uplink.

[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**.



SONICWALL Network Security Appliance

General Advanced

ID: 1

Switch Model: X1026P

IP Address: 192.168.2.4

User Name: admin

Password: .....

Confirm Password: .....

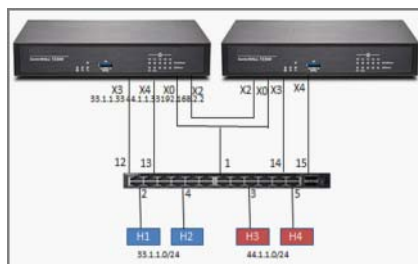
Switch Management: 3

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-Series/N-Series Switch on a SonicWall Appliance](#) on page 10.
- 2 Set up the data uplink as described in [Adding an Extended Switch](#) on page 20.
- 3 Configure the uplinks as described in [Configuring a Common Uplink](#) on page 29.



## 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-Series/N-Series Switch on a SonicWall Appliance](#) on page 10.
- 2 Set up the data uplink as described in [Adding an Extended Switch](#) on page 20.
- 3 Configure the uplinks as described in [Configuring a Hybrid System With Common and Dedicated Uplink\(s\)](#) on page 38.

## Configuring a Dedicated Uplink for VLANs

Topics:

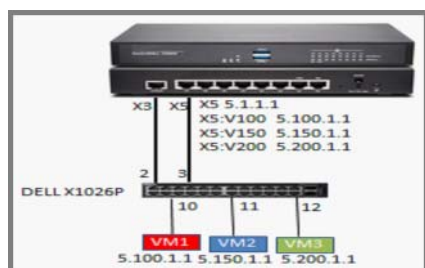
- [Dedicated Uplink for VLAN Topology](#) on page 49
- [Configuring a Dedicated Uplink for a VLAN](#) on page 50

### Dedicated Uplink for VLAN Topology

In a dedicated uplink configuration, a given link between the firewall and the 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

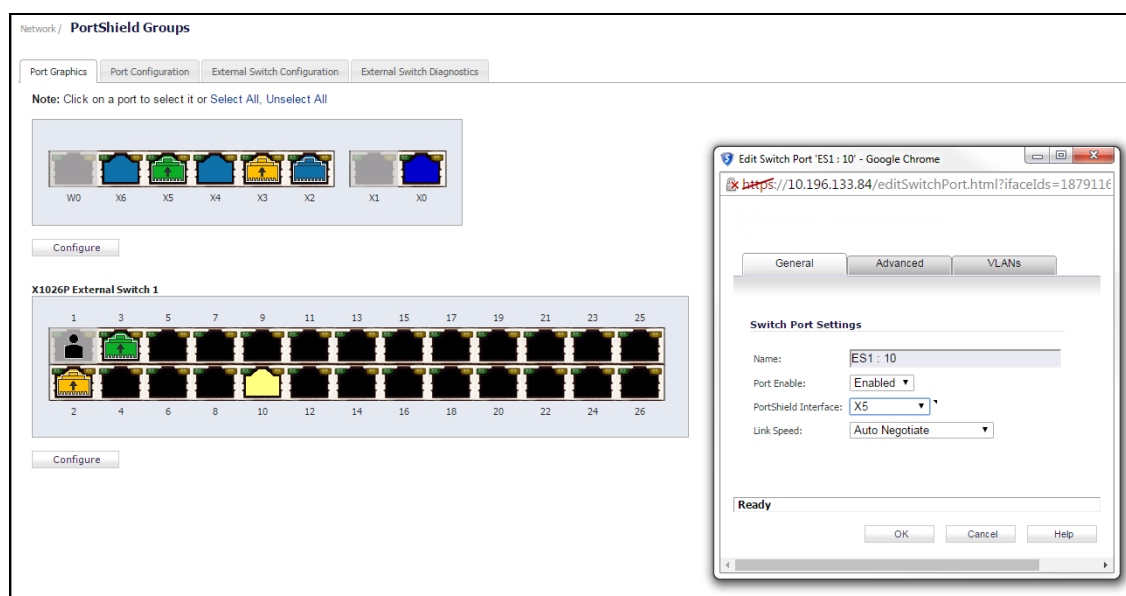
Support for VLAN(s) is achieved in a multi-step configuration process:

- 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 a 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.

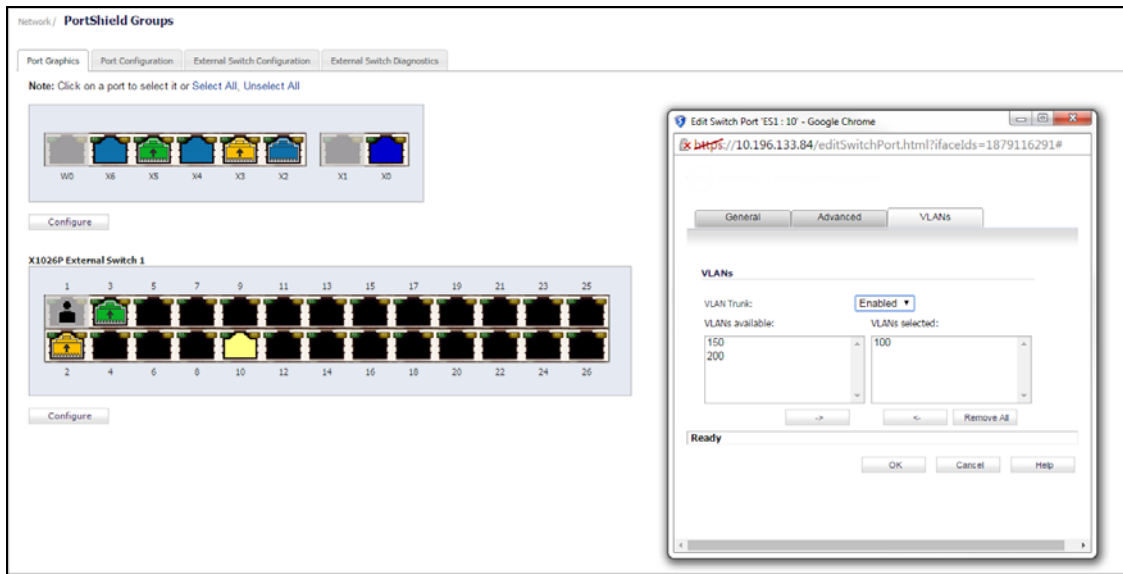
### *To configure a dedicated uplink for VLANs without a common uplink:*

- 1 Provision the switch as described in [Provisioning an X-Series/N-Series Switch on a SonicWall Appliance](#) on page 10.
- 2 Set up the data uplink as described in [Adding an Extended Switch](#) on page 20.
- 3 Configure the options as described in [Configuring a Dedicated Uplink](#) on page 32 except ensure to select the **Dedicated Uplink** option.

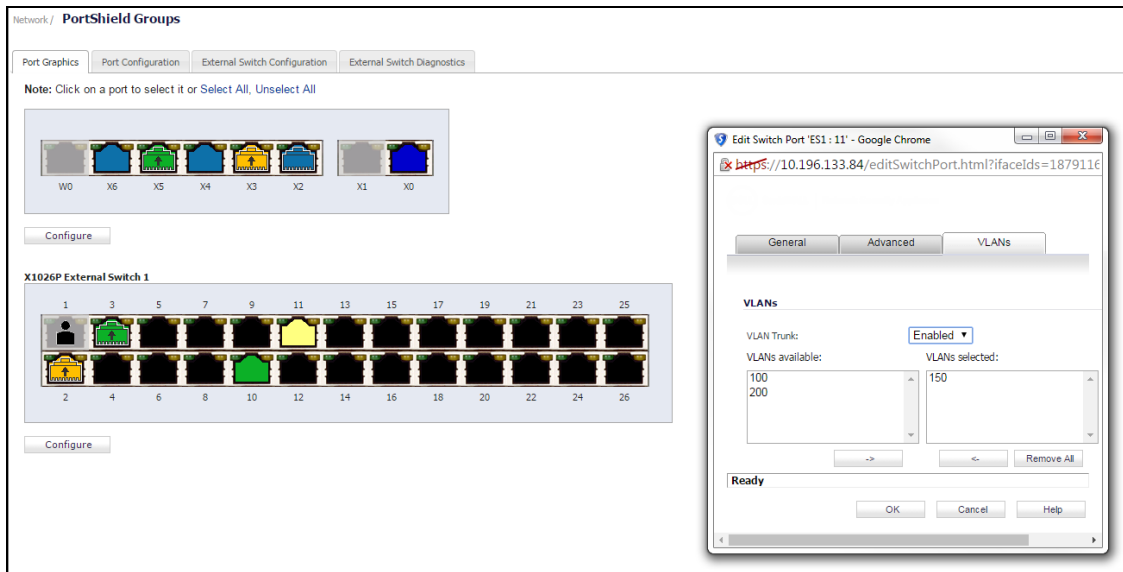
When a dedicated uplink is set up for a given firewall interface, if VLAN(s) exist under the firewall interface, a new tab, **VLANs**, displays on the **Edit Switch Port** dialog when the PortShield Interface is selected:



- 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:



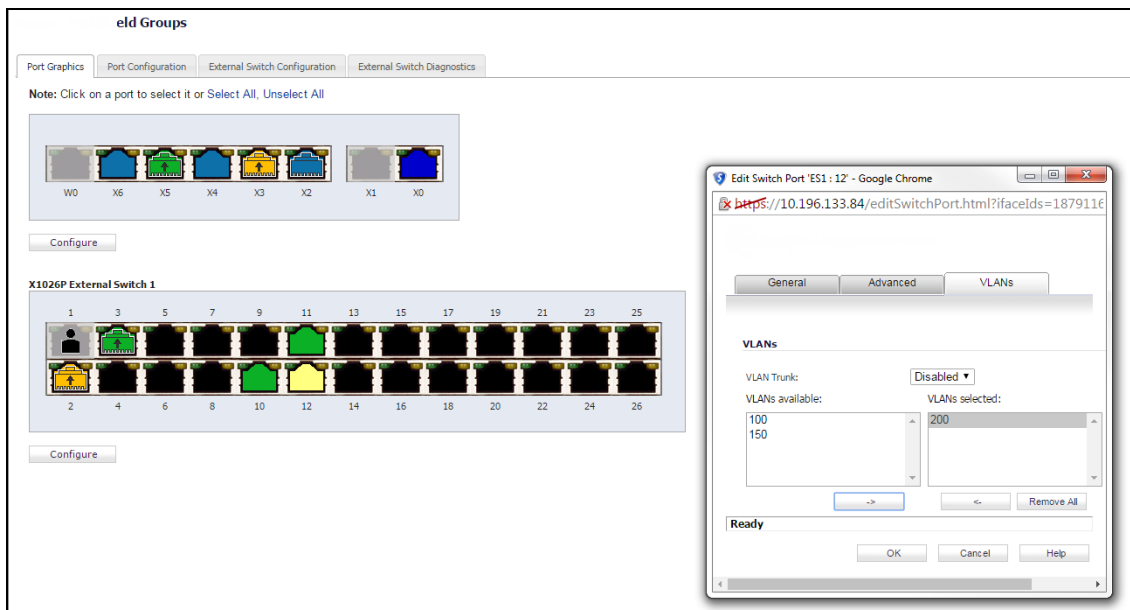
- 5 Similarly, Port 11 is portshielded to X5 and configured as a trunk to carry VLAN 150 by:
  - a Selecting **Enabled** for the **VLAN Trunk** option.
  - b Choosing **VLAN 150** from the available list of VLANs.



- 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.



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 switch to the firewall.

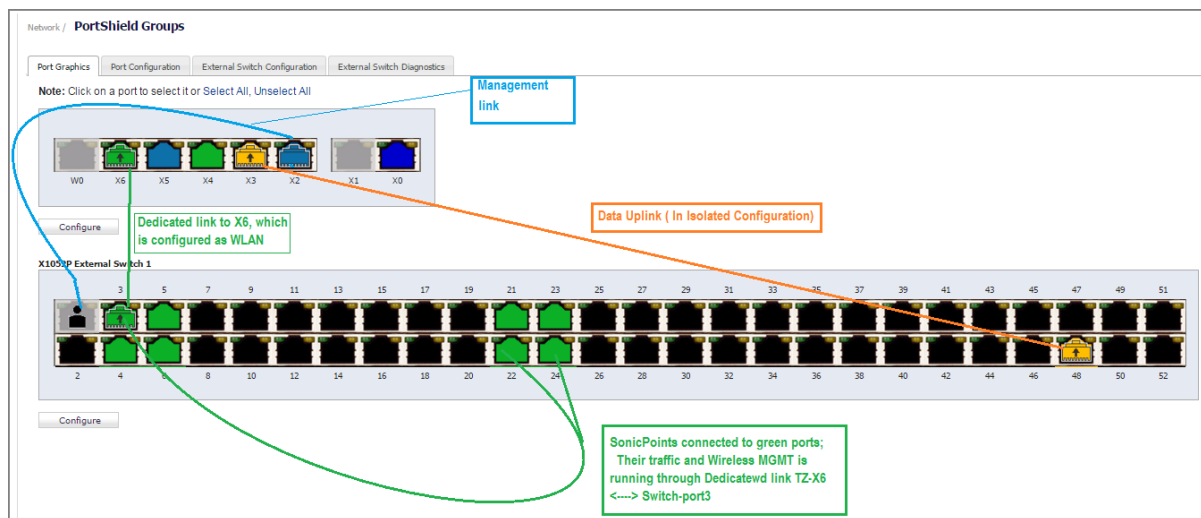
For non-SonicPoint access points and for SonicPoints without particular management, the port in the firewall can be configured as **ANY** (LAN/WAN/DMZ, although usually LAN). In this case, the pair of ports between the firewall and the switch must be configured as a dedicated link. Other ports on the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



For more information about using SonicPoints with switches, see [SonicWall TZ Series and SonicWall X-Series Solution managing SonicPoint access points](#).

#### To configure a dedicated uplink for SonicPoints:

- 1 Provision the switch as described in [Provisioning an X-Series/N-Series Switch on a SonicWall Appliance](#) on page 10.
- 2 Set up the data uplink as described in [Adding an Extended Switch](#) on page 20.
- 3 Configure the uplinks as described in [Configuring a Dedicated Uplink for VLANs](#) on page 49.
- 4 Ensure that all SonicPoints are connected to switchSonicWall SonicOS 6.5 X-Series/N-Series Solution ports configured in the PortShield group of the dedicated link.

## B

- button
  - Managed Mode, 12

## C

- common link, 24

## D

- dedicated link, 24

## E

- extended switch
  - global parameters, 6
  - overview, 5
  - supported topologies, 23

## I

- IDV (Interface Disambiguation via VLAN), 6
- interface
  - uplink, 24
- isolated link, 24

## L

- link
  - common, 24
  - dedicated, 24
  - isolated, 24

## M

- Managed Mode button, 12

## P

- PoE (Power over Ethernet), 6
- PoE+ (Power over Ethernet Plus), 6

## S

- SFP (Small form-factor pluggable), 6
- SFP+ (Enhanced small form-factor pluggable), 6
- SPM (Single Point Management), 6
- STP (Spanning Tree Protocol), 6

- switch, extended
  - See extended switch, 5

## U

- uplink
  - common configuration, 25
  - extended switch, 24
  - firewall, 24
  - interface, 24
  - X-Switch, 24
- uplink interface
  - criteria for configuring, 24



# 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/N-Series Deployment Guide  
Updated - May 2019  
Software Version - 6.5.3  
232-004884-00

## Copyright © 2019 SonicWall Inc. All rights reserved.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners

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

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

## End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/en-us/legal/license-agreements>.

## Open Source Code

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

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