

Layer 2 Bridge Bypass

Document Scope

This solutions document describes how to configure and manage the Layer 2 Bridge Bypass feature in SonicOS Enhanced 5.5.

This document contains the following sections:

- [“Feature Overview” section on page 1](#)
- [“Prerequisites for Layer 2 Bridge Bypass” section on page 3](#)
- [“Configuring Layer 2 Bridge Bypass” section on page 3](#)

Feature Overview

This section provides an introduction to the Layer 2 Bridge Bypass feature. This section contains the following subsections:

- [“What is Layer 2 Bridge Bypass?” section on page 1](#)
- [“Benefits of Layer 2 Bridge Bypass” section on page 2](#)
- [“How Does Layer 2 Bridge Bypass Work?” section on page 2](#)
- [“Platforms” section on page 3](#)

What is Layer 2 Bridge Bypass?

Layer 2 Bridge Bypass is a physical X0-X1 interface bypass relay currently implemented on the SonicWALL NSA E7500. This feature is sometimes known as “fail to wire”, meaning that the LAN-WAN connection reverts to a straight-through connection if the SonicWALL appliance experiences a hardware or software failure. When the bypass relay is closed, network traffic flows unimpeded between the X0 and X1 interfaces. When the bypass relay is open, network traffic is handled by SonicOS Enhanced running on the SonicWALL appliance. The bypass relay can be opened or closed on demand by software. Low-level logic controlling the relay can also be programmed by the firmware to open or close the relay in the event of a power failure.

The bypass relay state is affected by specific system events in association with the bypass relay configuration options. Configuration is performed in the SonicOS Enhanced Web-based management interface.

Benefits of Layer 2 Bridge Bypass

Enabling the Layer 2 Bridge Bypass feature allows network access to remain open between your local network and the Internet even if your SonicWALL appliance fails due to a hardware or software problem.

How Does Layer 2 Bridge Bypass Work?

The state of the bypass relay changes only upon specific system events. The decision to close or open the bypass relay for each of these events may, or may not, depend on the state of the **Engage physical bypass on malfunction** option at the time of the system event. Each system event is described below, along with how the bypass relay is changed for each event depending on the L2 Bridge bypass option:

1. Power applied – The SafeMode firmware will initially open the bypass relay. If the **Engage physical bypass on malfunction** option is selected and the unit has SafeMode version 5.0.3.3 or later, the bypass relay will close again shortly afterward and will remain closed. If the unit has older SafeMode firmware, the bypass relay will remain open until the SonicOS firmware begins initialization.
2. Beginning of SonicOS firmware startup/initialization – Bypass relay is closed if the **Engage physical bypass on malfunction** option is enabled.
3. End of SonicOS firmware startup/initialization and start of normal operation – Bypass relay is always opened.
4. Beginning of software initiated reboot – If the **Engage physical bypass during soft reboot** option is selected, the bypass relay is closed.
5. Software exception or watchdog timeout – If the **Engage physical bypass on malfunction** option is selected, the bypass relay is closed.
6. Power loss – If the **Engage physical bypass on malfunction** option is selected, the bypass relay is closed.
7. Fail-back to SafeMode – If the **Engage physical bypass on malfunction** option is selected, the bypass relay is closed (requires SafeMode version 5.0.3.3 or later). With older SafeMode versions, the bypass relay is always opened.
8. User-initiated entry into SafeMode by pressing the reset button – The bypass relay is always opened.

SafeMode Dependencies

Fully functional L2 Bridge bypass modes require a revised version of the SafeMode firmware. The required Safemode version is 5.0.3.3 or greater. If an older revision of Safemode is present, the user will be notified with the following warning message when configuring either bypass mode: “Full support of this option may require a ROM upgrade. Please contact your SonicWall support representative for more information.”

The power loss scenario is handled correctly with existing SafeMode firmware, but packet loss will occur during fail-back to SafeMode. The revised version of SafeMode firmware is required to handle these system events without packet loss.

When the upgraded SafeMode version is present, and a fail-back to SafeMode occurs, the bypass relay will remain closed if the **Engage physical bypass on malfunction** option is selected. With the relay closed, the normal Web management interface access through 192.168.168.168 on X0 will not be available. In this case, you can press the reset button on the appliance to perform a user-initiated entry into Safemode. A user-initiated entry into SafeMode by pressing the reset button will always open the bypass relay, regardless of the SafeMode version. This allows X0 to be used as the configuration interface.

Platforms

Layer 2 Bridge Bypass is available on the SonicWALL NSA E7500 running SonicOS Enhanced 5.5 and higher.

Prerequisites for Layer 2 Bridge Bypass

To use Layer 2 Bridge Bypass, you must configure the X0 and X1 interfaces as a Layer 2 Bridge-Pair.

When the Layer 2 Bridge Bypass relay is closed, the network cables attached to the bypassed interfaces (X0 and X1 on the SonicWALL NSA E7500) are physically connected as if they were a single continuous network cable. The bypass relay options provide the administrator the choice of avoiding disruption of network traffic by bypassing the firewall in the event of a malfunction. This requires the bypassed and non-bypassed states to behave identically for valid traffic, which is only the case when the connected interfaces are configured as a Layer 2 Bridge-Pair, which passes Ethernet frames intact from one network to the other (behaving as a virtual wire). Additional restrictions of the L2 Bridge configuration options are also necessary, as described in the [“Configuration Overview”](#) section on page 3.

Configuring Layer 2 Bridge Bypass

This section contains the following sections:

- [“Configuration Overview”](#) section on page 3
- [“Configuration Procedure”](#) section on page 4
- [“Verifying Administrator Layer 2 Bridge Bypass Configuration”](#) section on page 6

Configuration Overview

Because use of the Layer 2 Bridge Bypass relay is only applicable to interfaces in L2 Bridge mode, the configuration of the bypass relay option appears as an additional configuration option when this mode has been chosen in the Edit Interface popup. This new option is not displayed if a physical bypass relay does not exist between the chosen interfaces of the bridge-pair. One new checkbox will appear in addition to the existing L2 Bridge mode options when L2 Bridge Mode is chosen for a bypass-able pair of interfaces (X0 bridged to X1 on the SonicWALL NSA E7500):

- **Engage physical bypass on malfunction**
 - The bypass relay will be closed for any unexpected anomaly (power failure, watchdog exception, fail-back to SafeMode).
 - On initialization, the bypass relay will remain closed on boot until the end of initialization (requires revised SafeMode firmware), although a small intermittency in the bypass relay may occur during the initial power-up or reboot sequence.

The use of the L2 bypass mode places further restrictions on the L2 Bridge Mode configuration. If **Engage physical bypass on malfunction** is selected, the other L2 Bridge option states are automatically set as follows:

- **Block all non-IPv4 traffic** – Not selected
When this option is selected, non-IPv4 Ethernet frames are blocked by the firmware. This is different than the bypass behavior, so this option must be disabled.
- **Never route traffic on this bridge-pair** – Selected

When selected, this option prevents packets from being routed to a network other than the bridge-pair peer. This is the bypass behavior, so this option must be enabled.

- **Only sniff traffic on this bridge-pair** – Not selected

When enabled, traffic received on a bridge-pair interface is never forwarded. Therefore, this option must be disabled when a bypass option is enabled.

- **Disable stateful-inspection on this bridge-pair** – Not modified

This option is not affected.

When any of the five L2 Bridge options are changed, any interdependent options are changed to a compatible state as well. For instance, if **Never route traffic on this bridge-pair** is unchecked by the administrator, the **Engage physical bypass on malfunction** option will be cleared as well. The same applies to the other option dependencies. This provides immediate feedback to the administrator regarding the option dependencies.

Configuration Procedure

To enable the Layer 2 Bridge Bypass feature, both the X1 and X0 interfaces must be configured, with X1 as the primary interface and X0 as the secondary interface of the Layer 2 Bridge.

Configuring the Primary Interface (X1)

To configure X1 as the primary interface, perform the following steps:

-
- Step 1** Navigate to the **Network > Interfaces** page.
 - Step 2** Click the **Configure** icon in the right column of the X1 (WAN) interface.
 - Step 3** On the General tab in the **Zone** drop-down list, select **WAN**.
 - Step 4** In the **IP Assignment** drop-down list, select **Static**.
 - Step 5** In the **IP Address** field, configure the interface with a static IP address (such as 10.0.56.71).



Note The Primary Bridge Interface must have a Static IP assignment.

- Step 6** In the **Default Gateway** field, enter the IP address of your network default gateway. This is required for the security appliance itself to reach the Internet. (This applies only to WAN interfaces.)
- Step 7** In the **DNS Server** fields, enter the IP addresses of one or more DNS servers. (This applies only to WAN interfaces.)
- Step 8** In the **Comment** field, type a descriptive name for this interface (such as Bridged to X0).
- Step 9** For the **Management** options, select the checkboxes for the desired options (**HTTP, HTTPS, Ping, SNMP, SSH**) to allow management access to the appliance using the selected protocols.
- Step 10** For the **User Login** options, optionally select **HTTP** and/or **HTTPS** to allow users to login on this interface.
- Step 11** If HTTPS is selected without HTTP, select the **Add rule to enable redirect from HTTP to HTTPS** checkbox to allow access to users who type http:// instead of https:// when accessing the appliance management URL.

Step 12 Click **OK**.

The screenshot shows the 'Interface 'X1' Settings' page in the SonicWall Network Security Appliance. The 'General' tab is selected. The configuration includes:

- Zone: WAN
- IP Assignment: Static
- IP Address: 10.0.56.71
- Subnet Mask: 255.255.255.0
- Default Gateway: 10.0.0.2
- DNS Server 1: 10.50.128.52
- DNS Server 2: 0.0.0.0
- DNS Server 3: 0.0.0.0
- Comment: Bridged to X0
- Management: HTTP, HTTPS, Ping, SNMP, SSH
- User Login: HTTP, HTTPS
- Add rule to enable redirect from HTTP to HTTPS

Configuring the Secondary Interface (X0)

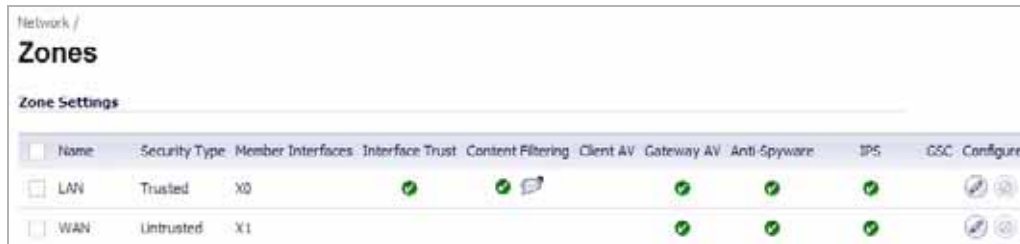
To configure X0 as the secondary interface, perform the following steps:

- Step 1** Navigate to the **Network > Interfaces** page.
- Step 2** Click the **Configure** icon in the right column of the X0 (LAN) interface.
- Step 3** On the General tab in the **IP Assignment** drop-down list, select **Layer 2 Bridged Mode**.
- Step 4** In the **Bridged to** drop-down list, select the **X1** interface.
- Step 5** Select the **Never route traffic on this bridge-pair** checkbox.
- Step 6** Select the **Engage physical bypass on malfunction** checkbox.
- Step 7** In the **Comment** field, type a descriptive name for this interface (such as Bridged to X1).
- Step 8** For the **Management** options, select the checkboxes for the desired options (**HTTP**, **HTTPS**, **Ping**, **SNMP**, **SSH**) to allow management access to the appliance using the selected protocols.
- Step 9** For the **User Login** options, optionally select **HTTP** and/or **HTTPS** to allow users to login on this interface.
- Step 10** If **HTTPS** is selected without **HTTP**, select the **Add rule to enable redirect from HTTP to HTTPS** checkbox to allow access to users who type `http://` instead of `https://` when accessing the appliance management URL.

Step 11 Click **OK**.

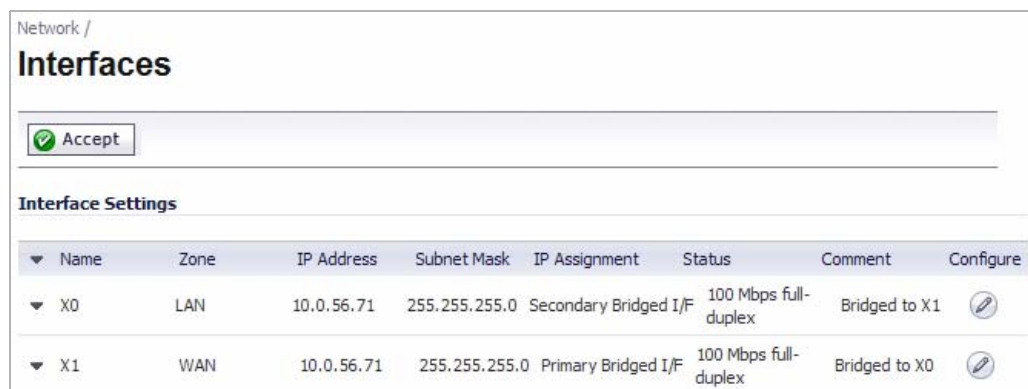


You may now apply security services to the appropriate zones, as desired. In this scenario, they should be applied to the LAN, WAN, or both zones.



Verifying Administrator Layer 2 Bridge Bypass Configuration

The Network > Interfaces page displays the updated configuration.



Solution Document Version History

Version Number	Date	Notes
1	6/19/2009	This document was created by Susan Weigand

