Hardware Bypass

This chapter contains the following sections:

Overview

The ISA 3000 is able to operate in bypass mode for ASA or Firepower Threat Defense. Bypass mode is defined as the copper ports are able to continue with an end to end connection, bypassing the Cisco ISA 3000 in the event of loss of power. This functionality is programmable. The Software will be responsible for turning off bypass mode once the system has booted up.

The hardware bypass feature lets traffic pass freely between the following interface pairs in the event of a power outage:

- Gigabitethernet 1/1 and 1/2
- Gigabitethernet 1/3 and 1/4

Note The Hardware Bypass feature is only available on the copper ports.

You can configure the hardware bypass behavior for each pair of interfaces for the following events:

- Power down
- Power up to system operational

Power down means reloading or restarting the Cisco ISA 3000 via power cycle or a complete loss of power. This will bypass the ISA data ports if it has been configured to do so. If you configure the hardware bypass to continue after power up, all the traffic can pass from the internal port to the external port and vice versa. When power is restored, the system software will monitor the boot up progress and only disable the bypass when the system is ready (Firewall is ready to process packets).

Power up means after power is restored, the system will continue in bypass mode in the data ports according to the user configuration. All the traffic can pass from internal port to external port and vice versa until the user manually disables the bypass. An event/trap will be sent to the management system to indicate the system still continues in bypass mode after power is restored.

If you manually enable hardware bypass, the system will enable bypass mode and all Firewall/VPN or IPS function will not take effect until the user issues a command to disable the bypass. A critical event will be sent to the management system to indicate no protection will be provided by the system. The user has to consider whether bypass feature is enabled or not while configuring other features.

For configuration information, please see all of the software guides for Firepower Threat Defense and ASA here:https://www.cisco.com/c/en/us/support/security/industrial-security-appliance-isa/products-installation-and-configuration-guides-list.html

Port Bypass LEDs

Each port is equipped with a bi-colored (Green and Amber) LED which indicates the port status. The LED states are shown below:

Table 1: LED Descriptions

LED	Activity	Description
Ethernet Ports	Bypass Mode Indicator	Off — No link Green Steady on — Link is up Green Flashing — Transmitting and Receiving data Amber — Fault, implies no link Port 1&2 or 3&4 LEDs flashing amber together — Those two ports are in bypass mode and the system is up.