finjan®
Vital Security™
securing your web

Technical Brief

Bypass Adapter

Vital Security 9.2

Copyright

For additional information, please visit www.finjan.com or contact one of our regional offices:

US & Canada 2025 Gateway Place Suite 180 San Jose, CA 95110, USA Toll Free: 1 888 FINJAN 8 Tel: +1 408 452 9700 Fax: +1 408 452 9701 salesna@finjan.com	**UK & Ireland** 4 th Floor, Westmead House, Westmead, Farnborough, GU14 7LP, UK Tel: +44 (0)1252 511118 Fax: +44 (0)1252 510888 salesuk@finjan.com
Israel/APAC & India Hamachshev St. 1, New Industrial Area Netanya, Israel 42504 Tel: +972 (0)9 864 8200 Fax: +972 (0)9 865 9441 salesint@finjan.com	**Central & Eastern Europe** Alte Landstrasse 27, 85521 Ottobrun, Germany Tel: +49 (0)89 673 5970 Fax: +49 (0)89 673 597 50 salesce@finjan.com
General Information Email: support@finjan.com Internet: www.finjan.com	**Benelux & Nordic** Printerweg 56 3821 AD Amersfoort, Netherlands Tel: +31 334 543 555 Fax: +31 334 543 550 salesne@finjan.com

Catalog name: BA1.0

Table of Contents

1. Overview

The Finjan Bypass Adapter enables bypassing a failed system and provides maximum up time for the network. Finjan's adapters are designed to improve the dependability of internet accessibility in the event of host system failure, a power outage, or software request. In Bypass mode, when configured by the administrator as Fail Open, the connections of the Ethernet network ports are disconnected from the interfaces and switched over to another port, and create a connection back between Ethernet ports. In Bypass (Fail Open) mode, all packets received from one port are transmitted to the other port and vice versa. In Fail Close mode, no packets will be transmitted in either direction.

The Bypass Adapter feature is supported by Finjan's NG-5000 and NG-6000 series hardware only.

1.1 Supported Protocols

The Scanning Server supports HTTP, HTTPS, and FTP in Bridge mode and scans those protocols according to the configured policies.

NOTE: Non-HTTP traffic over port 80 is blocked! System administrators must use the `config_exclude` command to bypass specific hosts.

1.2 Fail Open and Fail Close

Fail Open (open to all traffic with a direct connection) is the ability of the scanning server to forward traffic in case of server failure, reboot, loss of power, or any reason that prevents the scanning server from scanning the traffic. Fail Close, configured by the administrator, is the ability of the scanning server to close the server entirely to all traffic.

For new hardware, which includes the internal bypass Network Interface Card (NIC), the administrator will be able to enable or disable the Fail Open status.

NOTE: Fail Open is the default setting.

1.3 Bridge Mode

When working in Bridge mode, the ports used to forward the traffic are pre-configured and cannot be changed by the user. During set-up configured by the administrator, Eth0 will be assigned automatically.The Scanning Server will use the assigned IP address when it retrieves content from the internet. Additionaly, the user may configure an additional IP address on another interface.

1.3.1 Basic bridging mode

The diagram below shows the basic topology of Bridge mode (where only a single appliance exists in the topology).

1.4 Bypass Server Card

The 1 Gigabit Ethernet Bypass adapters offer stability and increased performance for environments with multiple networks, networking applications and servers. The Bypass adapter card is a 100/1000 dual port Ethernet adapter that provides an effective bypass solution. When installed on the NG-5000 or NG-6000 appliance, the system detects the bypass card during installation and allows the configuration to enable Bridge mode. The two Ethernet ports serve as bridge ports. The bridge will Fail Open automatically, by default, if the NG appliance experiences a failure such as a power outage. The Web traffic then passes from one Ethernet port to the other, without interruption, but does not route through the appliance.

The 1 Gigabit Ethernet Bypass server adapters are PCI Express network interface cards that contain two independent Gigabit ports on one PCI Express adapter.

2. Bypass Adapter Installation

1. Turn off the NG appliance.
2. Remove the top cover.
3. Remove the existing Ethernet card (s).
4. Insert the Bypass card in the available slot.
5. Replace the top cover.
6. Re-image the appliance and run Limited Shell set-up.
7. Navigate to the **Management Console** → **Administration** → **Updates** → **Update Management** and click **Retrieve Updates**.
8. Ensure that the **9.2.0-M01** Maintenance Package is listed in the **Available Updates** window.
9. Install the Maintenance Package.
10. Run `config_bridge` from the Limited Shell.

3. Configuration

Use the commands listed below to configure and review the Bypass adapter:

- config_bridge
- show_bridge
- config_excludes

3.1 config_bridge

The user must enable transparency in the Policy Server after enabling the Bridge support.

Configuring the status of the bridging mode is done via a new Limited Shell command: `config_bridge`.

To run `config_bridge` connect via the Limited Shell**.** Type `config_bridge`.

Three `config_bridge` options are available:

1. Bridge Enabled/Disabled: enables or disables the By Pass Adapter
   The default mode is: *Disabled*
2. Set mode to Fail Open/Fail Close:
   The default mode is: *Fail Open*

   Fail Open –causes the adapter to enter bypass mode forwarding all traffic without scanning.

   Fail Close – shuts down the link on both bridge interfaces and causes the external HA system to stop routing packets to this bridge.

If systems are up again:

In **Fail Open,** traffic is re-directed to the scanner.

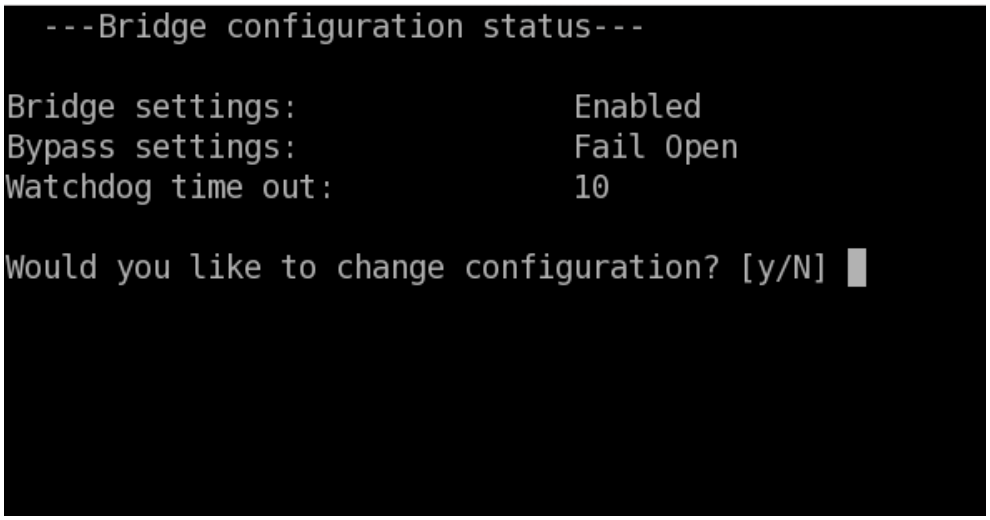
In **Fail Close,** the links are active and traffic is scanned.

3. Configure Watchdog timer
   The default interval is *10* secs. The interval is user-defined.

NOTE: The Watchdog timer is set between 5 and 300 seconds.

To modify the bridge settings, run config_bridge.

The current Bridge status is displayed.



Followed by

```
Would you like to change configuration? [y/N]
```

Type `y` to change an option, then type:

- (1) to Enable/ Disable the Bridge.
- (2) to set the Fail Open / Fail Close mode status
- (3) to set the Watchdog timer
- (Q) to quit the menu

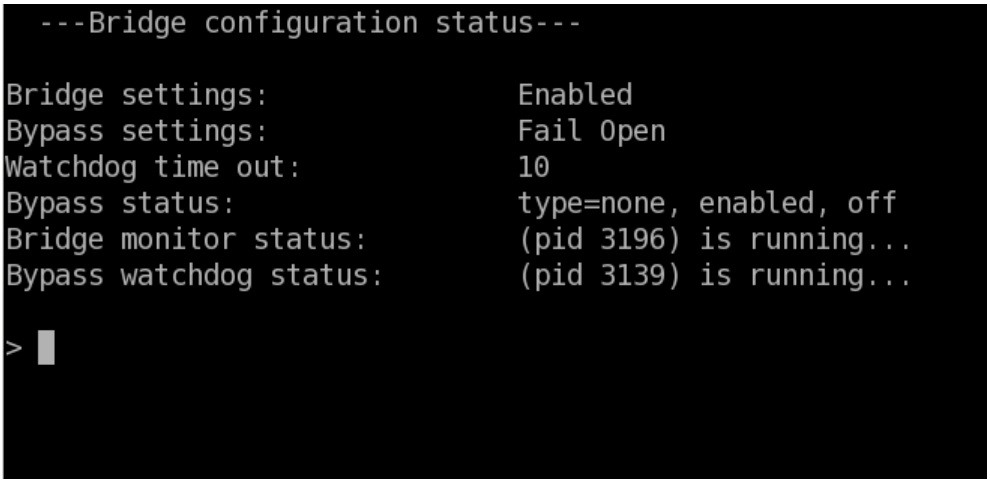
NOTE: This option is available only with the presence of the internal bypass NIC.

The Bypass settings can only be configured after Bridge mode is enabled. If Bridge mode is enabled, the user cannot configure the interfaces. The default interfaces are Eth0 and Eth1.

3.2 Show _bridge

To view the Bridge Configuration status, type `show_bridge`.

The `show_bridge` status is displayed:



3.3 config_excludes

Use the `config_exclude` command to exclude TCP/IP connections from being scanned based on IP addresses and ports.

3.4 config_network

When the bridge is enabled `config_network` prohibits changes such as the IP address in the bridge interfaces configuration. To modify the bridge interfaces configuration these parameters must be removed from the bridge using the `config_bridge` command.

3.5 Known Limitations

- Exclude port 443 traffic using the `config_exclude` command if an SSL license is not installed.
- When the adapter is in Bypass mode, the appliance is not manageable unless a dedicated management port is configured.