

**finjan**<sup>®</sup>  
Vital Security™

securing your web

## Technical Brief



## Bypass Adapter

VITAL SECURITY 9.2

## Copyright

© Copyright 1996-2009. Finjan Software Inc. and its affiliates and subsidiaries ("Finjan"). All rights reserved.

All text and figures included in this publication are the exclusive property of Finjan and are for your personal and non-commercial use. You may not modify, copy, distribute, transmit, display, perform, reproduce, publish, license, create derivative works from, transfer, use or sell any part of its content in any way without the express permission in writing from Finjan. Information in this document is subject to change without notice and does not present a commitment or representation on the part of Finjan.

The Finjan technology and/or products and/or software described and/or referenced to in this material are protected by registered and/or pending patents including European Patent EP 0 965 094 B1 and U.S. Patents No. 6092194, 6154844, 6167520, 6480962, 6209103, 6298446, 6353892, 6804780, 6922693, 6944822, 6993662, 6965968, 7058822, 7076469, 7155743, 7155744, 7185358, 7418731 and may be protected by other U.S. Patents, foreign patents, or pending applications.

Finjan, Finjan logo, Vital Security, Vulnerability Anti.dote and Window-of- Vulnerability, SecureBrowsing are trademarks or registered trademarks of Finjan. Sophos is a registered trademark of Sophos plc. McAfee is a registered trademark of McAfee Inc. Kaspersky is a registered trademark of Kaspersky Lab. Websense® is a registered trademark of Websense, Inc. IBM® Proventia® Web Filter is a registered trademark of IBM Corporation. Microsoft and Microsoft Office are registered trademarks of Microsoft Corporation. All other trademarks are the trademarks of their respective owners.

For additional information, please visit [www.finjan.com](http://www.finjan.com) or contact one of our regional offices:

<p><b>US &amp; Canada</b> 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 <a href="mailto:salesna@finjan.com">salesna@finjan.com</a></p>	<p><b>UK &amp; Ireland</b> 4 th Floor, Westmead House, Westmead, Farnborough, GU14 7LP, UK Tel: +44 (0)1252 511118 Fax: +44 (0)1252 510888 <a href="mailto:salesuk@finjan.com">salesuk@finjan.com</a></p>
<p><b>Israel/APAC &amp; India</b> Hamachshev St. 1, New Industrial Area Netanya, Israel 42504 Tel: +972 (0)9 864 8200 Fax: +972 (0)9 865 9441 <a href="mailto:salesint@finjan.com">salesint@finjan.com</a></p>	<p><b>Central &amp; Eastern Europe</b> Alte Landstrasse 27, 85521 Ottobrun, Germany Tel: +49 (0)89 673 5970 Fax: +49 (0)89 673 597 50 <a href="mailto:salesce@finjan.com">salesce@finjan.com</a></p>
<p><b>General Information</b> Email: <a href="mailto:support@finjan.com">support@finjan.com</a> Internet: <a href="http://www.finjan.com">www.finjan.com</a></p>	<p><b>Benelux &amp; Nordic</b> Printerweg 56 3821 AD Amersfoort, Netherlands Tel: +31 334 543 555 Fax: +31 334 543 550 <a href="mailto:salesne@finjan.com">salesne@finjan.com</a></p>

Catalog name: BA1.0

## Table of Contents

<b>1. Overview</b>	<b>1</b>
1.1 Supported Protocols	1
1.2 Fail Open and Fail Close	1
1.3 Bridge Mode	2
1.4 Bypass Server Card	2
<b>2. Bypass Adapter Installation</b>	<b>3</b>
<b>3. Configuration</b>	<b>3</b>
3.1 config_bridge	3
3.2 Show _bridge	5
3.3 config_excludes	6
3.4 config_network	6
3.5 Known Limitations	6

## 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. Additionally, 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 Bypass 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.

```
---Bridge configuration status---  
  
Bridge settings:           Enabled  
Bypass settings:          Fail Open  
Watchdog time out:        10  
  
Would you like to change configuration? [y/N] █
```

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:

```
---Bridge configuration status---  
  
Bridge settings:           Enabled  
Bypass settings:          Fail Open  
Watchdog time out:        10  
Bypass status:            type=none, enabled, off  
Bridge monitor status:    (pid 3196) is running...  
Bypass watchdog status:   (pid 3139) is running...  
  
> █
```

### 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.