



securing your web



Setup and Configuration Guide

Vital Security Version 9.2



CONTENTS

1. Introduction	1
Finian Overview	1
About This Manual	2
2. Finjan Appliances	3
Vital Security Appliance Series NG-8000	3 4
NG-8000 Rear Panel	6
NG-8000 Hardware Specifications	7
Vital Security Appliance Series NG-6000	9
NG-6000 Front Panel	9
NG-6000 Rear Panel	0
NG-6000 Hardware Specifications1	2
Vital Security Appliance Series NG-50001	3
NG-5000 Front Panel	3
NG-5000 Rear Panel. 1	4
NG-5000 Hardware Specifications1	5
3. Configuring the Vital Security Appliance 1	7
Management Console System Requirements 1	7
Operating Systems 1	7
Software Requirements	7
Connecting your Vital Security Appliance (NG-5000/6000/8000)1	8
Limited Shell Connection Procedure 1	8
Using an Ethernet Cable 1	8
Using a Serial Cable	9
Initial Setup of your Vital Security Appliance using Limited Shell	0
Initial Setup	1
Running the Setup 2 Limited Shell commande 2	1
Limited Shell Configuration Commands	2
access list	ך ג
change nassword 2	2
config 2	л Л
\mathcal{O}	+



config_network	34
config_time	39
config_psweb	39
disable	40
disable_service_snmpd4	40
disable_service_ssh	40
enable	40
enable_service_snmpd	41
enable_service_ssh	41
ethconf	41
flush_dnscache	42
reset_config	43
Limited Shell Monitoring Commands	43
arp	43
df	43
ifconfig	44
ip2name	44
iptraf	45
last	46
name2ip	46
netstat	47
ping	47
poweroff.	48
reboot	48
restart role	48
save support logs	48
setun	10 49
show	10
show config	τ) 50
show_coning	50
show_network	51
show dbsize	52
show route	52
show_time	53
supersh	53
tcpdump	53
top	54
traceroute	54
uptime	55



vmstat	55
W	56
wget	56
First Login to the Management Console	56
Update Mechanism.	57
Installing Updates	58
Configuring Next Proxy for Updates	58
Configuring the Firewall for Automatic Updates	58
Offline Updates	58
Routing Traffic through the Appliance	59
Configuring Workstations for Routing Traffic through the Appliance .	59
Transparent Proxy	59
Working with HTTP	61
HTTP Proxies	61
Working with Caching Proxies	61
Downstream	61
Upstream	62
HTTP Authentication	62
Working with ICAP	62
Why work with ICAP?	63
Vital Security as an ICAP Server	63
REQMOD – RESPMOD Deployment	63
ICAP Clients	
A Configuring ICAD Clients	65
	03
Network Appliance NetCache Series (NetApp)	65
Blue Coat	69
A Installation Details	79
Installing your Vital Security Appliance	79
Remote Installation on NG-8000	
Post-Installation Bonding Script on NG-8000	86
	_
B. Post-Installation System Hardening	87
System Hardening	
Policy Server	87



Management Access List	. 87
Management Console Password.	. 88
Default SNMP v2 Community String	. 88
User Access to the Scanning Servers	. 88
Scanning Servers	. 89
Proxy IP Address	. 89
Management Access List	. 89
Nortel Switches (Applicable only to NG-8000 Series)	. 90
Defaults SNMP Community String	. 90
Telnet and HTTP Access to the Switch	. 90
Default User and password.	. 90



Vital Security™ Appliance Series NG-5000/NG-6000/NG-8000 Setup and Configuration Guide

© Copyright 1996 - 2008. 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, Window-of-Vulnerability and RUSafe are trademarks or registered trademarks of Finjan. Sophos and Websense are registered trademarks of Sophos plc. McAfee is a registered trademark of McAfee Inc. Kaspersky is a registered trademark of Kaspersky Lab. IBM Proventia Web Filter is a registered trademark of IBM Corporation. SurfControl and Websense are registered trademarks of Websense, Inc. Microsoft and Microsoft Office are registered trademarks of Microsoft Corporation. All other trademarks are the trademarks of their respective owners.

For additional information, please contact one of our regional offices:

USA	UK
2025 Gateway Place Suite 180 San Jose,	4th Floor, Westmead House,
CA 95110, USA	Westmead,
Toll Free: 1 888 FINJAN 8	Farnborough, GU14 7LP, UK
Tel: +1 408 452 9700 Fax: +1 408 452 9701	Tel: +44 (0)1252 511118
salesna@finian.com	Fax: +44 (0)1252 510888
	salesuk@finjan.com
Israel/Asia Pacific	Germany
Hamachshev St. 1,	Alte Landstrasse 27, 85521
New Industrial Area Netanya, Israel 42504	Ottobrun, Germany
Tel: +972 (0)9 864 8200	Tel: +49 (0)89 673 5970
Fax: +972 (0)9 865 9441	Fax: +49 (0)89 673 597 50
salesint@finjan.com	salesce@finjan.com
Cananal	Netherlands
General	Printerweg 56
Email: info@finian.com	3821 AD° Amersfoort
Lindii. <u>Into(a) Infancoin</u>	Netherlands
Internet: <u>www.finjan.com</u>	Tel: +31 334 543 555
	Fax: +31 334 543 550
	salosno@finian.com
	saleshe@inijan.com

Catalog number: SACG-9.0-01

Email:<u>support@finjan.com</u> Internet:www.finjan.com



C H A P T E R

INTRODUCTION

1 Finjan Overview

Cyber-threats are fast increasing and pose a serious and growing problem for corporate networks, appearing in different forms and using a variety of tactics – viruses, worms, Trojans, and more. New, ultra-fast viruses can infect your system within seconds, long before traditional signature-based solutions can protect you. While waiting for anti-virus companies to release a new virus signature, thousands of unprotected computers may have already been infected, leaving no alternative other than to shut down the corporate network.

Finjan's real-time web security solutions provide zero-hour protection against known and unknown web attacks without requiring immediate signature or patch updates. Powered by our Vital Security[™] Web Appliances and utilizing patented real-time content inspection technologies, Finjan's proven security solutions effectively combat a wide array of web threats, including Spyware, Phishing, Trojans, obfuscated malicious code and other types of malware.

Finjan's unique and patented proactive behavior-inspection technology at the gateway offers instant protection against new virus, worm and malicious mobile code outbreaks without time-sensitive signature-file updates, thus closing the **Window-of-Vulnerability**[™] and providing networks with true zero-day protection. By detecting and stopping all such attacks before they enter the corporate network, our solutions help to ensure continuous business operations and save the time and money associated with security incidents.

Vital Security - Finjan's Integrated Security Platform - is a complete and integrated **Secure Content Management** solution in which individual best-of-breed security applications work together in concert to respond proactively to the changing security threats of both today and tomorrow.

Finjan's integrated "all-in-one" security appliances provide proactive, layered protection against complex threats and vulnerabilities. Centralized management and reporting enables IT managers to set organization-wide security policies, safeguard confidential data and generate detailed reports as required for regulatory compliance.



2 About This Manual

Chapter	Description
Chapter 1	Finjan Overview - An introduction to Finjan's Vital Security.
Chapter 2	Finjan Appliances - An introduction to Finjan's Vital Security Appliances, including a brief description of the Vital Security Appliances NG-8000/NG-6000/NG-5000.
Chapter 3	Getting Started – This chapter details everything you need to know about getting started and lists the necessary steps to be taken when installing and working with your appliance. This includes: System requirements (hardware and software) Information on supported protocols (HTTP and ICAP) Configuration of end-user machines Transparent proxy configuration Connecting – describing the steps to be taken prior to accessing the web-based Management Console. This includes the Limited Shell.
Chapter 4	Configuring the ICAP Clients – This chapter discusses configuration of Network Appliance (NetApp) and Blue Coat
Appendix A	Installation Details - using USB Disk-On-Key
Appendix B	System Hardening (Post Installation)





FINJAN APPLIANCES

This manual deals with the following Vital Security appliances:

- NG-8000
- NG-6000
- NG-5000

Each **Vital Security** appliance is supplied with a default IP address, and can be remotely accessed for initial setup by any PC in the same subnet. **Vital Security** uses a secure ssh connection to a command-line interface for first time setup, as well as for https connection for ongoing management.

NOTE: Pictures of appliances displayed in this chapter are for general reference only and may differ from the specific appliances you receive.

1 Vital Security Appliance Series NG-8000

This appliance is a specially configured chassis containing multiple hot swappable blades, with redundant power supplies, disks, blowers and switches, etc. The **Vital Security** Operating System (VSOS) is preinstalled and preconfigured.

The **Vital Security Appliance NG-8000** is supplied as one or more separate blades. You can assign system roles according to your requirements using each blade as a separate server, or activate more than one service on a single blade.





Figure 2-1: NG-8000 Superformance Appliance

1.1 NG-8000 Front Panel



Figure 2-2: NG-8000 Front Panel



The following table describes the NG-8000 Front Panel:

No	Description
1	Information - When this amber LED is lit, a non- critical event has occured that requires attention, such as the wrong I/O module inserted in a bay or power demands that exceed the capacity of power modules currently installed.
2	Over-temperature LED - When lit, has exceeded the temperature limits, or a blade server reports an over-temperature condition. The NG-8000 might already have taken corrective action such as increasing the blower speed. This LED turns off automatically when there is no longer an over- temperature condition.
3	Location LED - When this blue LED is lit or flashing, it has been turned on by the system administrator to aid in visually locating the NG-8000 unit. If a blade server requires attention, the location LED on the blade server will usually also be lit. After the NG-8000 has been located, you can turn off the location LED.
4	Power on LED - When this green LED is lit, the NG- 8000 is powered on. When the LED is off, the power subsystem, the ac power, or the LED has failed, else the management module is not present or not functioning.
5	System Error - When this amber LED is lit it indicates that a system error has occured such as a failed module or a system error in the blade server. An LED on one of the components or on a blade server is also lit to further isolate the problem.
6	USB Connector
7	DVD Drive
8	Floppy Disk Drive



1.2 NG-8000 Rear Panel



Figure 2-3: NG-8000 Rear Panel

The following table describes the NG-8000 Rear Panel:

No	Description	
Blow	Blower Module	
1/15	Blower Error LED - This amber LED is lit and stays lit when an error has been detected in the blower. The system error LED on the NG-8000 system LED is also lit.	
Power Module		
2	Power Connector	
3	DC Power LED - When this LED is lit, the DC output from the power module to the other components and blade servers is present and within specifications. During typical operation this LED is lit.	



No	Description
4	AC Power LED - When this LED is lit, AC input to the power module is present and within specifications. During typical operation this LED is lit.
Mana	gement Module
5	Power on LED - When this green LED is lit, the management module has power.
6	Active LED - When this green LED is lit it indicates that the managemnt module is actively controlling the NG-8000.
7	Management Module Error LED - When this amber LED is lit it indicates that an error has been detected somewhere on the management module. In addition, when this LED is lit then the system error LED on each of the NG-8000 system LED panels is also lit.
8	Ethernet Link LED - When this green LED is lit, there is an active connection through the port to the network.
9	Network Port
10	Ethernet Activity LED - When this green LED is flashing it indicates that there is activity through the port over the network link.
11	Serial Connector
12	Mouse PS2 Connector
13	Keyboard PS2 Connector
14	IP Reset Button

1.3 NG-8000 Hardware Specifications

The following table contains the hardware specifications for the NG-8000 appliance:

Component	Specification
Memory	2 GB
Hard Drive	73 GB SAS (Web appliance)
	2 x 146 GB SAS (RAID 1) (Policy Server)
CPU	Xeon D 2 x 2.0GHz
Gigabit Ethernet NIC	4
Rack Space (7U)	444 x 711.2 x 304.2 mm (WxDxH) 17.5 x 28 x 12 inches (WxDxH)
Heat Output (max)	Four 2000W power supplies 11111BTU (3256 W)



Component	Specification
Environment	Air Temperature: BladeCenter unit on: 10° to 35°C (50° to 95°F), Altitude: 0 to 194m (2998.69 ft) BladeCenter unit on: 10° to
	32°C (50° to 95°F), Altitude: 194m to 2134m (2998.69 to 7000ft)
	BladeCenter unit off: -40° to 60°C (-40° to 140°F)
	Humidity: Server on/off 8 % to 80%
Weight	Fully configured with modules and blades: approx 108.86 kg (240 lb)
	Fully configured without blades: approx 44.91 kg (99lb)



2 Vital Security Appliance Series NG-6000

This appliance is typically deployed to include multiple appliances, each running the **Vital Security** Operating System (VSOS). It can, however, also be deployed as an All-in-one, using a single appliance.

The different services running on each appliance can be configured according to your organization's network requirements.

Figure 2-4: NG-6000 Superformance Appliance

2.1 NG-6000 Front Panel



Figure 2-5: NG-6000 Front Panel

The following table describes the NG-6000 Front Panel:

No	Description
1	Power Control Button - Press this button to turn the server on and off manually. A power control button shield comes installed on the server to prevent the server from being turned off accidentally.
2	Power on LED - When this LED is lit and not flashing it indicates that the server is turned on. When the LED is flashing it indicates that the server is turned off and still connected to an AC power source. When this LED is off it indicates that AC power is not present or the power supply or the LED itself has failed.
3	Hard disk drive activity LED - When this LED is flashing it indicates that the hard disk drive is in use.
4	System locator LED - When this LED is lit or flashing, it has been turned on by the system administrator to aid in visually locating the NG-6000 unit.



No	Description
5	Information LED - When this LED is lit it indicates that a non-critical event has occured. An LED on the light path diagnostics panel is also lit to help isolate the error.
6	System error LED - When the LED is lit it indicates that a system error has occured. An LED on the light path diagnostics panel is also lit to help isolate the error.
7	Release latch
8	USB Connector
9	USB Connector
10	Serial Connector

2.2 NG-6000 Rear Panel



Figure 2-6: NG-6000 Rear Panel

The following table describes the NG-6000 Rear Panel:

No	Description
1	Power Supply 1
2	Power-Cord Connector
3	AC Power LED - When lit, this indicates that sufficient power is coming into the power supply through the power cord. During typical operation this LED is lit.
4	DC Power LED - When lit, this indicates that the power supply is supplying adequate DC power to the system. During typical operation this LED is lit.
5	Power Supply 2
6	SAS (serial Attached SCSI) Connector



No	Description
7	Systems Management Ethernet Connector - This connector is used to connect the server to the network for systems management information control. This connector is active only if you have installed a Remote Supervisor Adapter II SlimLine - not supplied by Finjan (and is used only by this).
8	Serial Connector
9	Power On LED - When this LED is lit and not flashing, it indicates that the server is turned on. When this LED is flashing, it indicates that the server is turned off but still connected to an AC power source. When this LED is off, it indicates that AC power is not present, or the power supply or LED itself has failed.
10	System Locator LED - When this LED is lit or flashing, it has been turned on by the system administrator to aid in visually locating the NG-6000 unit.
11	System Error LED - When this LED is lit, it indicates that a system error has occured. An LED on the light path diagnostics panel is also lit to help isolate this error.
12	Video Connector
13	USB 1 Connector
14	USB 2 Connector
15	Ethernet Activity LED - When this LED is lit it indicates that the server is transmitting to or receiving signals from the Ethernet LAN that is connected to the Ethernet port.
16	Ethernet Connector (GE1)
17	Ethernet Connector (GE0)
18	Ethernet Link LED - When this LED is lit, it indicates that there is an active link connection on the 10BASE-T, 100BASE-TX or 1000BASE-TX interface for the Ethernet port.
19	USB 3 Connector
20	USB 4 Connector
21	Ethernet Connector (GE3)
22	Ethernet Connector (GE2)



2.3 NG-6000 Hardware Specifications

The following table contains the hardware specifications for the NG-6000 appliance:

Component	Specification
Memory	2GB
Hard Drive	2 x 73 GB SAS (RAID 1)
CPU	Intel Xeon dual core x 2.0 GHz
Rack space (2U)	445 x 705 x 86 mm
	(WxDxH)
	17.5 x 27.5 x 3.4 inches
	(WxDxH)
Gigabit Ethernet NIC	4
Power Supply	2 Fully Redundant
Environment	Air Temperature: Server on -
	10° to 35°C (50° to 95°F),
	Server off - 10° to 43°C (50° to
	109.4°F), Shipment -40° to 60°C (-40° to 140°F)
	Humidity: Server on/off 8 % to
	80%, Shipment 5% to 100%
Weight	30kg
Heat Output (max)	Minimum configuration - 1230
	BTU per hour (360 watts)
	Maximum configuration - 3390
	BTU per hour (835 watts)



3 Vital Security Appliance Series NG-5000

This appliance is typically deployed to include multiple appliances, each running the **Vital Security** Operating System (VSOS). It can, however, also be deployed All-in-one, using a single appliance.

The different services running on each appliance can be configured according to your organization's network requirements.



Figure 2-7: NG-5000 Superformance Appliance

3.1 NG-5000 Front Panel



Figure 2-8: NG-5000 Front Panel

The following table describes the NG-5000 Front Panel:

No	Description
1	LCD Display
2	Menu Display Buttons (up/down)



No	Description
3	Menu Display Buttons (Esc/ Enter)
4	Network / Ethernet Connectors (GE0-GE3)
5	Power ON LED
6	Hard Disk LED
7	LED - Not in use
8	LED - Not in use
9	Serial Connector
10	RS232 Connector
11	USB Connectors

3.2 NG-5000 Rear Panel



Figure 2-9: NG-5000 Rear Panel

The following table describes the NG-5000 Rear Panel:

No	Description
1	Power Connector
2	On / Off Switch



3.3 NG-5000 Hardware Specifications

The following table contains the hardware specifications for the NG-5000 appliance.

Component	Specification
Memory	2GB
Hard Drive	160GB SATA2
CPU	Pentium D 3.4 GHz dual core
Flash Card	1024 MB
Rack space (1U)	429 x 382 x 44 mm (WxDxH)
	16.9 x 15.0 x 1.8 inches
Cigobit Ethernet NIC	
Gigabit Ethernet Nic	4
Built-in LCD display	1
Weight	11.5 kg
Power (max)	350W
Heat Output (max)	335 BTU

The NG-5000 has an LCD display which enables system administrators to display the software version, CPU, power off the appliance or restore the default IP address of interface GE3. This will restore the IP address of interface Ge3 to 10.0.3.1 with subnet mask 255.255.255.0.

NOTE: For information on older appliances not listed here, please contact Finjan Support.







CONFIGURING THE VITAL SECURITY APPLIANCE

This section contains the following topics:

- <u>Management Console System Requirements</u>
- <u>Connecting your Vital Security Appliance (NG-5000/6000/8000)</u>
- Limited Shell Configuration Commands
- <u>Update Mechanism</u>
- <u>Routing Traffic through the Appliance</u>
- Working with HTTP
- Working with ICAP

1 Management Console System Requirements

1.1 Operating Systems

The following operating systems are supported for the web browser:

- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Server
- Microsoft Windows XP Professional
- Microsoft Windows 2003 Server

1.2 Software Requirements

The following software is required:

- Microsoft Internet Explorer 6.0 (or higher) for accessing the Management Console.
- SSH Client to connect to the Limited Shell.
- An SFTP application for downloading files from the Appliance.



 Terminal application (such as Microsoft Hyper Terminal) - for accessing the serial console (as well as serial cable)

2 Connecting your Vital Security Appliance (NG-5000/6000/8000)

This section includes the following:

- Limited Shell Connection Procedure
- Initial Setup of your Vital Security Appliance using Limited Shell

NOTE: For instructions on how to install Software Version 9.0 on the appliance, please refer to Installation Details.

2.1 Limited Shell Connection Procedure

There are three different ways to connect to the Limited Shell:

- <u>Using an Ethernet Cable</u>
- Using a keyboard and monitor
- Using a Serial Cable

2.1.1 Using an Ethernet Cable

- To connect to the Limited Shell using an Ethernet cable (for NG-5000/NG-6000):
 - 1. Plug in the power cable and switch the appliance on.
 - Connect a PC directly to the appliance's GE0 port or via a switch (for NG-6000, see <u>NG-6000 Rear Panel</u>) using a standard (8 thread) Ethernet cable. CAT5e cables (or better) are recommended.
 - **3.** The default IP of the GE0 interface is 10.0.0.1, and its default netmask is 255.255.255.0. Configure the TCP/IP settings of your PC so that it is on the same logical network subnet as the appliance's GE0 interface. For example, configure the IP on the PC as 10.0.0.101 and the PC's netmask as 255.255.255.0



IMPORTANT: Do not set the PC's IP to 10.0.0.1, as this will result in an IP conflict with the appliance.

4. Continue with Initial Setup of your Vital Security Appliance using Limited Shell.

To connect to the Limited Shell using an Ethernet cable (for NG-8000):

The following initial procedure is the same for all the blades irrespective of the intended network role (except for the Load Balancer).



- **1.** Plug in the power cables.
- 2. Configure the network settings of any PC to match those of the appliance (IP address and subnet mask).
 - IP address in the same subnet e.g. 10.0.0.101
 - Subnet mask 255.255.255.0
- **3.** Connect your PC to one of the ports on the Gigabit Ethernet switch in I/O switch module Bay 1 on the appliance using a ethernet cable.
- 4. Power up the blades one by one.
 - **To power up the blades one by one:**
 - a Press the **Console Select** button so that the VGA screen attached to the chassis displays output from the blade being powered up.
 - **b** Press the **Power** button until the blade turns on. After the blade finishes booting, a login prompt is displayed.
 - c Continue with <u>Initial Setup of your Vital Security Appliance using Limited</u> <u>Shell</u>



d Repeat this procedure from step a) for each blade.

Figure 3-1: Blade

5. Continue with Initial Setup of your Vital Security Appliance using Limited Shell.

NOTE: For more information on setting up the NG-8000, please contact your *Finjan representative.*

2.1.2 Using a Serial Cable

- To connect to the Limited Shell using a serial cable (for NG-5000/NG-6000):
 - 1. Connect the PC to the appliance's Serial Console, using the serial cable.
 - 2. Using the Hyper Terminal application, enter the appropriate settings"



Baud rate: 19,200
Parity: No
Stop bits:1
Word: 8

Bits per second:	19200	
Data bits:	8	•
Parity:	None	•
Stop bits:	1	-
Flow control:	Hardware	•
Flow control:	Hardware	<u> </u>

Figure 3-2: Hyper Terminal COM1 Properties

2.2 Initial Setup of your Vital Security Appliance using Limited Shell

The Limited Shell feature enables monitoring and viewing the appliance's configuration remotely via an SSH connection, or a Serial port connection or by connecting a keyboard to the appliance's USB port and a monitor to the appliance VGA port. The default username and password for the shell (command line) is **admin** and **finjan** respectively.

SSH access is enabled by default.

No other user can log in directly to the system. Privileged access (root level) is achieved only after logging in as Super Administrator from the Limited Shell (this is for Finjan support purposes only).

A timeout mechanism is activated such that idle connections are disconnected after 5



minutes.

After first login to the Limited Shell, only the **setup** command is available (see <u>Initial</u> <u>Setup</u>). This command lets you run the configuration setup (wizard). After completing the setup, enter **help** to view a list of commands that the shell user can run and their use.

To configure the Appliance, use the configuration commands described in <u>Limited Shell</u> <u>Configuration Commands</u>.

NOTE: The default action for when the user is prompted to select between [y/N] is the option indicated with a capital letter. This means that if you press Enter, the default "no" answer is selected. This is true for all [y/N] prompts in the Limited Shell.

2.2.1 Initial Setup

The Setup guides you step by step through the initial configuration process. Use this setup to configure the following:

- An appliance with one active Ethernet interface with an IP that you have set (all other interfaces will be deactivated).
- Your selected network settings Default gateway, Hostname, and so on.
- Time and date settings that you have manually configured.
- Active appliance roles that work according to the Ethernet interface and IP that you have selected.
- A new password of your choice for the initial setup Web interface **admin** user (the password cannot be finjan or an empty string).

2.2.2 Running the Setup

- **To run the Setup:**
 - 1. Log in to the Limited Shell from a remote machine using an SSH client, serial cable or by connecting a keyboard to the appliance's USB port and a monitor to the appliance VGA port. The default username and password for the shell (command line) is **admin** and **finjan** respectively.
 - 2. After you log in to the Limited Shell, type help to show list of available commands.

Use	"help"	to	show	list	of	available	commands,	"quit'	'to exit.
> he	≘lp								
seti	ap					== R	un configu	ration	setup.
>									

Figure 3-3: After first login screen



3. Enter the **setup** command. The current configuration is then displayed.



NOTE: During each step of the Setup, the Current Configuration settings are updated accordingly. To go back a step, enter **B**; to accept default value press **Enter** and to quit the setup, enter **Q**.

After successful completion of the Setup, all other commands in the limited shell will become enabled.

Configuration stat	usaati
Role	: None
Time Zone	: None
Current date and time	: 2008-03-05 08:58
Interface	: None
IP Address	: None
Default gateway	: None
Hostname	: None
DNS server	: None
DNS search	: None
(B - go back, Enter - a	ccept default values, Q - exit from setup)
Set Role	
1. All in One (Default)	
2. VS Remote Device	
3. VS Policy Server	
>	

Figure 3-4: Setup - Set Role

- **4.** Each appliance can take on a different role within the deployment. Select the required role (1-3) for this appliance. The following roles can be selected:
 - 1. All In One (Default) Selecting the All in One appliance provides management, reporting and scanning services.
 - 2. VS Remote Device
 Select the Vital Security Remote Device if you want to
 activate this appliance for scanning or authentication, while another appliance
 is providing the management and reporting services.
 - 3. VS Policy Server Selecting the Vital Security Policy Server provides only management and reporting services, and requires an additional appliance for scanning.

After entering the required role, the following is displayed:



IMPORTANT: In order to change the device role from Remote Device to Policy Server or All in One device, the administrator must go through the Setup command in the Limited Shell.



Configuration state	us
Role	: All in One
Time Zone	: None
Current date and time	: 2008-03-05 02:47
Interface	: None
IP Address	: None
Default gateway	: None
Hostname	: None
DNS server	: None
DNS search	: None
(B - go back, Enter - ad	ccept default values, Q - exit from setup)
Set Time Zone	
The current time zone is Would you like to change	s: US/Eastern e this? [y/N]

Figure 3-5: Set Time Zone

The current timezone is displayed. To change this timezone, select y, else select N.The following is displayed:

Configuration statu	8
Role	: All in One
Time Zone	: US/Eastern
Current date and time	: 2008-03-05 02:50
Interface	: None
IP Address	: None
Default gateway	: None
Hostname	: None
DNS server	: None
DNS search	: None
(B - go back, Enter - ac	cept default values, Q - exit from setup)
Set Time/Date	
The current date and tim Would you like to change	e is: 2008-03-05 02:50 ? [v/N]

Figure 3-6: Set Time/Date

6. The current date and time is displayed. To change this, select y and enter the correct date and time (YYY- MM-DD HH:mm), else select N to display the following:



Configuration status	
Role	: All in One
Time Zone	: US/Eastern
Current date and time	: 2008-03-05 02:01
Interface	: None
IP Address	: None
Default gateway	: None
Hostname	: None
DNS server	: None
DNS search	: None
(B - go back, Enter - acc Set Interface	ept default values, Q - exit from setup)
<pre>1. eth0 (Default) 2. eth1 3. eth2 4. eth3 ></pre>	

Figure 3-7: Set Interface

7. Select the network interface to be used as the Policy/Scanning Server (1-5) for this appliance.

The following table describes the Network Interface for NG-5000/NG-6000:

Network Interfaces for NG-5000 /NG-6000 Appliances	Description
GE0 (eth0): 1GB - Auto-negotiation enabled - Recommended!	Allows communication at a speed of up to 1GB with Auto-Negotiation enabled. Auto- negotiation enables simple, automatic connection of devices by taking control of the cable when a connection is established to a network device that supports a variety of modes from a variety of manufacturers. The device is able to automatically configure the highest performance mode of interoperation.
GE1 (eth1): 1GB - Auto-negotiation enabled	Allows communication at a speed of up to 1GB with Auto-Negotiation enabled.
GE2 (eth2): 1GB - Auto-negotiation enabled	Allows communication at a speed of up to 1GB with Auto-Negotiation enabled.
GE3 (eth3) 1GB - Auto-negotiation enabled	Allows communication at a speed of up to 1GB with Auto-Negotiation enabled.





IMPORTANT: If you want to change the network interface auto negotiation settings for the NG-5000 /NG-6000, you must do so using the <u>ethconf</u> command.

After entering the required interface, the following is displayed:

Configuration stat	us
Role	: All in One
Time Zone	: US/Eastern
Current date and time	: 2008-03-05 02:03
Interface	: ethO
IP Address	: None
Default gateway	: None
Hostname	: None
DNS server	: None
DNS search	: None
(B - go back, Enter - a Set IP Address	ccept default values, Q - exit from setup)
Current IP address:	192.168.120.29/24
Insert new IP address i	n format
IP/[netmask prefix] or	Enter to default:

Figure 3-8: Set IP Address

8. Enter the IP address and netmask for the selected interface as IP/(netmask/ prefix), or press Enter to accept the defaul settings. The following is displayed:



Configuration status	3
Role	: All in One
Time Zone	: US/Eastern
Current date and time	: 2008-03-05 02:04
Interface	: ethO
IP Address	: 192.168.120.29/24
Default gateway	: None
Hostname	: None
DNS server	: None
DNS search	: None
(B - go back, Enter - acc Set Default Gateway	ept default values, Q - exit from setup).
Current gateway configurs Insert IP address of the or press Enter to accept	ation: 192.168.120.254 default gateway current settings

Figure 3-9: Set Default Gateway

9. Enter the Default Gateway IP address and press Enter. The following is displayed:

Configuration stat	us
Role	: All in One
Time Zone	: US/Eastern
Current date and time	: 2008-03-05 03:00
Interface	: ethO
IP Address	: 192.168.120.29/24
Default gateway	: 192.168.120.254
Hostname	: vs-29.finjan.com
DNS server	: None
DNS search	: None
(B - go back, Enter - a	ccept default values, Q - exit from setup)
Set Hostname	
The current hostname is	: vs-29.finjan.com
Type in a new hostname	or press
Enter to accept current	settings

Figure 3-10: Set Hostname

10. Enter the new hostname or press **Enter** to accept the current settings. The following is displayed:



Configuration stat	us
Role	: All in One
Time Zone	: US/Eastern
Current date and time	: 2008-03-05 03:01
Interface	: ethO
IP Address	: 192.168.120.29/24
Default gateway	: 192.168.120.254
Hostname	: vs-29.finjan.com
DNS server	: None
DNS search	: None
(B - go back, Enter - a	ccept default values, Q - exit from setup)
Set DNS Server	
The current DNS configu	ration is: 10.194.0.2
Type in DNS server IPs	separated by a space _
or Enter to accept curr	ent settings

Figure 3-11: Set DNS Server

11. Enter the IP address for the DNS Server or press **Enter** to accept the current DNS configuration settings. Note that the DNS configuration setting is mandatory. The following is displayed:

Configuration stat	us
Role	: All in One
Time Zone	: US/Eastern
Current date and time	: 2008-03-05 03:02
Interface	: ethO
IP Address	: 192.168.120.29/24
Default gateway	: 192.168.120.254
Hostname	: vs-29.finjan.com
DNS server	: 10.194.0.2
DNS search	: None
(B - go back, Enter - a Set DNS search list	ccept default values, Q - exit from setup)
The current DNS search Type in DNS domain name	list is: finjan.com s separated by a space





12. Enter the DNS domain names separated by a space or else just press **Enter** to accept the current settings. The following is displayed:



Figure 3-13: Change Password

X7

NOTE: For any device other than remote devices, password changes are *performed via the Management Console.*

Configuration stat	us
Role	: All in One
Time Zone	: US/Eastern
Current date and time	: 2008-03-05 03:17
Interface	: ethO
IP Address	: 192.168.120.29/24
Default gateway	: 192.168.120.254
Hostname	: vs-29.finjan.com
DNS server	: 10.194.0.2
DNS search	: finjan.com
(B - go back, Enter - a Apply Configuration	ccept default values, Q - exit from setup)
Would you like to save	current configuration? [y/N] 🗧

Figure 3-14: Save Configuration



13. To save the current configuration, select y. This will apply the configuration settings. The appliance's IP will change to the IP you just entered. Note that you will need to wait for up to ten minutes. If you are connected to the appliance via SSH, you should restore your PC's original TCP/IP settings at this point. If you connected your PC directly to the appliance's GE0 port, you can now plug the appliance and your PC into the corporate network.

NOTE: Applying configuration settings might take up to 10 minutes.

--Apply Configuration--

Would you like to save current configuration? [y/N] y Applying configuration, please wait. This may take up to 10 minutes During this period of time all appliance components might be inaccessible.

Note: Some network configuration changes may make the appliance inaccessible. If changes have been made, once you have clicked Apply, try to connect using the new configuration settings.

Deconfiguring network interfaces...done. Configuring network interfaces...done.

Figure 3-15: Applying Configuration


3 Limited Shell commands

After using the Initial Setup to configure the appliance, the Limited Shell can be used to manage the functionality of the appliance, as well as monitoring it closely. Each appliance will have different configuration needs. Therefore, after completing the Initial Setup, the Limited Shell enables you to access each configuration option as required, and configure it to match the system needs.

The following monitoring and configuration commands are available:

```
Use "help" to show list of available commands, "quit" to exit.
 help
Available commands:
access list
                               Enable/Disable Access List.
                                   Display arp table.
arp
                               Change password.
change password
                               config
                               Network or service configuration.
df
                               ==
                                   Display disk usage.
disable
                               Disable service.
enable
                               ___
                                   Enable service.
ethconf
                                   Menu interface to ethtool.
                               flush dnscache
                                   Flush dnscache.
                               ifconfig
                                   Display NIC configuration and statistics.
                               ip2name
                                   Resolve IP to hostname. Usage: ip2name ip.
                               iptraf
                               ____
                                   Interactive IP LAN Monitor.
                                   Display last logins.
last
                               Resolve hostname to IP. Usage: name2ip name.
name2ip
                               netstat
                                   Display network statistics.
                               ping
                                   Send ICMP ECHO REQUEST to network hosts. Usag
                               e: ping IP/Hostname.
poweroff
                               Power off the system.
                                   Reboot the system.
reboot
                               Sending full configuration
reset config
                               ---Press Enter for next page---
restart role
                               Restart role
save support logs
                               Save support logs.
setup
                               Run configuration setup.
show
                                   Show system or service status.
                               ==
                               Access to privileged shell.
supersh
tcpdump
                               Dump traffic on a network.
top
                               ==
                                   Display linux tasks.
                                   Print the route packets take to network host. Usage:
traceroute
                               ==
uptime
                                   Display uptime.
                               Reports information about system usage. Usage: vmsta
vmstat
                               ==
                               ==
                                   Show who is logged on.
                                   Wget retrieves files using HTTP, HTTPS and FTP.
wget
                               ==
```

Figure 3-16: Limited Shell commands



Command	Description
access_list	Enables/disables access list
<u>arp</u>	Displays arp table
change_password	Change password
config	Network or service configuration.
	Double tab to view the config_network, config_time and
	config_psweb commands.
<u>df</u>	Displays disk usage
<u>disable</u>	Disables service
<u>enable</u>	Enables service
<u>ethconf</u>	Menu interface to ethtool
flush_dnscache	Flushes the dns cache
ifconfig	Displays NIC configuration and statistics
<u>ip2name</u>	Resolves ip to hostname (usage: ip2name ip)
<u>iptraf</u>	Interactive IP LAN Monitor
last	Displays last login
name2ip	Resolves hostname to ip (usage: name2ip name)
<u>netstat</u>	Displays network statistics
ping	Sends ICMP ECHO_REQUEST to network hosts (usage:
	ping IP/Hostname)
<u>poweroff</u>	Powers off the system
reboot	Reboots the system
reset_config	Sends full configuration to device
<u>restart_role</u>	Restarts the role
save_support_logs	Saves support logs
<u>setup</u>	Runs configuration setup
show	Shows system or service status.
	Double tab to view the show_dbsize, show_network,
	show_route, show_service and show_time commands
supersh	Provides access to privileged shell
<u>tcpdump</u>	Dumps traffic on a network.
	Results files will be under sftp chroot/tcpdump_captures.
	Files can be downloaded using any sttp client
top	Displays linux tasks
traceroute	Prints the route packets taken to network host (traceroute IP)
<u>uptime</u>	Displays uptime
vmstat	Reports information about system usage (usage: vmstat, CTRL-C to stop)
W	Shows who is logged on
wget	Retrieves files using HTTP, HTTPS and FTP



For more information on configuring the system, refer to <u>Limited Shell Configuration</u> <u>Commands</u>

For further in-depth analysis and diagnostics of the system, refer to <u>Limited Shell Monitoring</u> <u>Commands</u>.



4 Limited Shell Configuration Commands

The Limited Shell configuration commands enable you to define the role the appliance takes, the security, access and time settings, and also carry out routine maintenance operations. The configuration commands are also used to define how the network works, and how the appliance communicates with the network.

4.1 access_list

The Access List feature is configured from the Management Console. The administrator can define a range of IP addresses to access Management applications on predefined ports (such as the Management Console, SNMP, SSH) or User applications on predefined ports (such as HTTP, FTP, ICAP) or System ports (internal ports). Any IP address not defined in the IP range will then be blocked from accessing these applications on the ports defined by Finjan.

The access_list command is used to enable or disable the Access List and is useful for situations when due to a mistaken configuration, or other circumstances, you cannot access the Management Console, and want to disable the Access List feature.

Enter the access_list command and choose enable or disable.



Figure 3-17: access_list

4.2 change_password

The change_password command allows system administrators to change the Limited Shell's password. For security reasons, it is recommended to choose a password which contains both characters (higher case and lower case) and digits. It is also recommended to change the password frequently.

Enter the change_password command and confirm current and new passwords.

> change_password Changing password for admin (current) UNIX password: Enter new UNIX password: Retype new UNIX password: passwd: password updated successfully

Figure 3-18: change_password



4.3 config

The config command enables network, service and Policy Server configuration. Press the tab button twice to display the config_network, config_time and config_psweb commands.



Figure 3-19: config

4.3.1 config_network

The config_network command allows system administrators to configure network parameters, such as the IP address(es), routing information, DNS parameters.

Enter the config_network command.



Figure 3-20: config_network

The current network configuration is displayed (i.e. the DNS Search Domain, nameserver and and Host name configuration). A Name Server is a network server that provides a naming, or directory service. A prompt is displayed asking you if you would like to change the configuration.

Enter **y** to change the network configuration. Select an option from the following commands:



oose an	optic	on	
View			
Interfa	ace		
Gateway	Y		
DNS			
Hostnam	ne		
Hosts			
pe Q to	exit	to	shell
tconf >			
	oose an View Interfa Gateway DNS Hostnan Hosts pe Q to tconf >	Dose an optic View Interface Gateway DNS Hostname Hosts pe Q to exit tconf >]	oose an option View Interface Gateway DNS Hostname Hosts pe Q to exit to tconf >

Figure 3-21: config_network menu

 View: This command allows you to view the current network configuration: The IP address assigned to each interface, the current DNS configuration and the current hostname configuration.

```
netconf > 1
Currently the following interfaces are defined:
ethO
      Enabled
        address 192.168.120.23/24
eth1
      Disabled
        address 192.168.120.23/24
        gateway 192.168.120.254
eth2
      Disabled
        address 10.0.2.1/24
      Disabled
eth3
        address 10.0.3.1/24
eth4
      Disabled
        address 10.0.4.1/24
eth5
      Disabled
        address 10.0.5.1/24
Current DNS configuration:
DNS cache:
            Enabled
nameserver 10.194.0.2
nameserver 10.194.0.5
Current Hostname configuration:
vs-23.finjan.com
Press [Enter] to continue
```

Figure 3-22: config_network - view



 Interface: Allows system administrators to modify interface related parameters such as: Add, Remove or Change an IP address from a physical interface; Add, Remove or Change routing information; Enable or Disable a physical interface.



Figure 3-23: config_network - Interface

Choose an interface, for example, 1 (eth0). The editing options are displayed.



Figure 3-24: config_network - Interface editing actions

Choose an editing action, for example, 1 (Change IP address).

To add a static route, choose 4 (Add route). The new route must be input as 'IP/via prefix IP'. For example, 1.1.1.1/32 via 10.0.3.3







 Gateway: Allows system administrators to set the default gateway of the appliance. The IP address of the default gateway must be a local IP address. It is mandatory to configure a default gateway to the appliance.

netco	nf > 3
Curre	nt interface configuration:
ethO	Enabled
	address 192.168.120.23/24
eth1	Disabled
	address 192.168.120.23/24
	gateway 192.168.120.254
eth2	Disabled
	address 10.0.2.1/24
eth3	Disabled
	address 10.0.3.1/24
eth4	Disabled
	address 10.0.4.1/24
eth5	Disabled
	address 10.0.5.1/24
Curre	nt gateway configuration:
	gateway 192.168.120.254
To ch	ange type IP address:
netco	nf >

Figure 3-26: config_network - Gateway

To change the current gateway configuration, enter the IP address.

DNS: Allows configuring the DNS servers, which the appliance uses in order to resolve the hostnames to IP addresses. It is also possible to configure a search domain under the DNS settings which allows the appliance to complete the domain name (according to the configured value) in case the host name is not completed. For example, if the search is on http://mize and the search domain is finjan.com, the appliance will try to resolve to http://mize.finjan.com.



IMPORTANT: It is mandatory to configure the DNS Server that has the ability to resolve external IP addresses.



```
netconf > 4
The current DNS configuration is as follows:
search finjan.com
nameserver 10.194.0.2
What would you like to do with it?
1. Change search
2. Add DNS server
3. Remove DNS server
Type Q to quit the menu
netconf ?
```

Figure 3-27: config_network - DNS

The current DNS configuration is displayed. Select an action, for example, 1 (change search).

```
netconf ? 1
Insert a new search line, separating domain names with spaces
```

```
Figure 3-28: config_network - DNS - Change DNS server
```

• **Hostname**: Allows configuring the appliance hostname.



Figure 3-29: config_network - Hostname

• Hosts: Allows configuring the host files.



netconf > 6	
['192.168.120.37	updateng.finjan.com mirror.updateng.finjan.com', '19
2.168.120.37	updateng.finjan.com mirror.updateng.finjan.com']
Default hosts re	cords:
127.0.0.1	localhost
127.0.1.1	vs-126.finjan.com vs-126
Custom hosts rec	ords:
192.168.120.37	updateng.finjan.com mirror.updateng.finjan.com
192.168.120.37	updateng.finjan.com mirror.updateng.finjan.com
Would you like t	o change hosts file? [y/N]

Figure 3-30: config_network - hosts

4.3.2 config_time

The config_time command allows system administrators to set the system date and time, the timezone and also the NTP Server. To change a setting, type \mathbf{y} . Select an option from the menu, else \mathbf{Q} to exit.

Current configuratio	on:
Date:	2008-02-13 11:06
TimeZone	Asia/Jerusalem
NTP Server	None
Would you like to cl	hange? [y/N] y
Time and Date config	guration
1. Date and Time	
2. Timezone	
3. NTP server	
Type Q to quit the r	menu
timecfg > 3	
Type in NTP server o	or Q to exit:

Figure 3-31: config_time

4.3.3 config_psweb

The config_psweb allows you to change the Policy Server management port for enhanced security. To change the Listening port for the Policy Server, add the new Port settings.



> config_psweb Current Policy Server web settings: Listen port - 443 Type in new port settings, or Enter to exit: <mark>-</mark>

Figure 3-32: config_psweb

4.4 disable

The disable command disables the service. The disable command includes the disable_service_snmp and disable_service_ssh commands.



Figure 3-33: disable

4.4.1 disable_service_snmpd

The disable_service_snmpd command disables the snmpd network service.

Enter the disable_service_snmpd command.



Figure 3-34: disable_service_snmpd

4.4.2 disable_service_ssh

The disable_service_ssh command disables the ssh network service. Enter the disable_service_ssh command.



Figure 3-35: disable_service_ssh

4.5 enable

The enable command enables the network service. The enable command includes the



enable_service_snmp and enable_service_ssh commands.



Figure 3-36: enable

4.5.1 enable_service_snmpd

The enable_service_snmpd command enables the snmpd network service.

Enter the enable_service_snmpd command.



Figure 3-37: enable_service_snmpd

4.5.2 enable_service_ssh

The enable_service_ssh command enables the ssh network service.

Enter the enable_service_ssh command.

> enable_ Service s	service sh enab.	_ssh led			
Stopping	OpenBSD	Secure	Shell	server:	sshd.
Starting	OpenBSD	Secure	Shell	server:	sshd.
>					

Figure 3-38: enable_service_ssh

4.6 ethconf

The ethconf command enables configuring the Network Interface parameters.

Enter the ethconf command and choose the required interface. Choose the required speed or select Auto-negotiation to enable the appliance to negotiate its own speed.

Enter the ethconf command and choose the interface, for example, enter 1 (eth1).



Ch	.00	se	the	inte	erface	2:	
0		etł	10				
1		etł	11				
2		etł	12				
3		etł	13				
4		etł	n4				
5		etł	15				
q		Qui	it				
Ту	pe	e i1	nterí	face	numbe	er:	

Figure 3-39: ethconf - interface selection

The settings for the selected interface are displayed.



Figure 3-40: ethconf - adapter configuration

Choose configuration for the adapter and confirm to make the settings permanent.



Figure 3-41: ethconf - ethconf - adapter configuration confirmation

NOTE: According to the IEEE 802.3 standard, when working with 1000Base-T at speed of 1000Mbps, auto-negotiation must be enabled. A fixed speed of 1000Mbps is not supported. For more information, please refer to the 1000BASE-X Auto-Negotiation standard as defined in Clause 37 of the IEEE 802.3 standard.

4.7 flush_dnscache

This command flushes the dns cache.



4.8 reset_config

This command will rebuild the device configuration in extreme situations where the device, for whatever reason, was disconnected for a period of time. This action restarts the devices and may take several minutes.

5 Limited Shell Monitoring Commands

5.1 arp

The Address Resolution Protocol (ARP) is the standard method for finding a host's hardware address when only its network layer address is known.

Enter the arp command to display the appliance's arp table.

Address	HUtype	HWaddress	Flags Mask	Iface
192.168.120.254	ether	00:90:FB:0F:CE:85	с	eth0

5.2 df

The df (disk free) command is a standard Unix command used to display the amount of available disk space for file systems.

Enter the df command to display the disk usage.

Use "help"	to show	list o:	f avail:	able d	comman	ds, "quit" to exit.
> df						
Filesystem		Size	e Vsed	Avail	l Use%	Mounted on
/dev/sda1		7.60	G 916M	6.30	G 13%	7
udev		101	M 44K	101	Y 1%	/dev
devshm		10101	M O	10101	¥ 0%	/dev/shm
/dev/sda5		2.90	G 69M	2.70	; ; ;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;	/img
/dev/sda7		810	G 1.1G	760	G 2%	/opt
/dev/sda3		2.90	G 69M	2.70	G 3%	/tmp
/dev/sda6		560	G 14G	390	G 26%	/var
> 📕						





5.3 ifconfig

The Unix command ifconfig is used to display TCP/IP network interfaces. Enter the ifconfig command to display configuration and statistics.

> ifcon	fig
ethO	Link encap:Ethernet HWaddr 00:1A:64:07:F5:F2 inet addr:192.168.120.91 Bcast:192.168.120.255 Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:96173 errors:0 dropped:0 overruns:0 frame:0 TX packets:3032 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:6574632 (6.2 MiB) TX bytes:357972 (349.5 KiB) Interrupt:3 Memory:ce000000-ce011100
ethl	Link encap:Ethernet HWaddr 00:1A:64:07:F5:F4 inet addr:10.1.1.1 Bcast:10.1.1.3 Mask:255.255.255.252 UP BROADCAST MULTICAST MTU:1500 Metric:1 RX packets:0 errors:0 dropped:0 overruns:0 frame:0 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:0 (0.0 b) TX bytes:0 (0.0 b) Interrupt:10 Memory:ca000000-ca011100
eth2	Link encap:Ethernet HWaddr 00:10:18:2C:A7:12 inet addr:10.0.2.1 Bcast:10.0.2.3 Mask:255.255.255.252 UP BROADCAST MULTICAST MTU:1500 Metric:1 RX packets:0 errors:0 dropped:0 overruns:0 frame:0 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:0 (0.0 b) TX bytes:0 (0.0 b) Interrupt:3
10	Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 UP LOOPBACK RUNNING MTU:16436 Metric:1 RX packets:1878 errors:0 dropped:0 overruns:0 frame:0 TX packets:1878 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:622606 (608.0 KiB) TX bytes:622606 (608.0 KiB)

Figure 3-44: ifconfig

5.4 ip2name

The ip2name command looks up the hostname associated with an IP address entered by the administrator. Enter the ip2name command followed by the IP address to display the associated hostname.







5.5 iptraf

The iptraf command is a Linux network statistics utility. It gathers a variety of parameters such as TCP connection packet and byte counts, interface statistics and activity indicators, TCP/UDP traffic breakdowns, and LAN station packet and byte counts. Enter the iptraf command to display the IP traf options:

- IP traffic monitor
- General Interface Statistics
- Detailed Interface Statistics
- Statistical breakdowns
- LAN station monitor

IP traffic monitor
General interface statistics
Detailed interface statistics Statistical breakdowns
LAN station monitor
Filters
Configure
Exit

Figure 3-46: iptraf

For example, select IP traffic monitor to display the IP traffic monitor details.



IPTraf					
TCP Connections (Source Host:Port)		ackets -	- Bytes	Flags	Iface]
192.168.120.125:22		398	81384	-PA-	eth0
410.194.5.95:4151		201	9476	A	ethO
r192.168.120.125:40259		20	2224	&	10
4192.168.120.125:8000		12	2376	-PA-	10
r127.0.0.1:58998		356	31376	A	10
L127.0.0.1:3050	>	340	82192	$-P\lambda -$	10
r192.168.120.125:8000	>	1	52		10
192.168.120.125:6692	-	0	0		10
r127.0.0.1:3050		1	52		10
4127.0.0.1:56701	-	0	0		10
r192.168.120.125:20910	-	1	52	RESET	10
-192.168.120.125:5222	-	0	0		10
TCP: 6 entries					Active -
Elapsed time: 0:00					
Pkts cantured (all interfaces): 155	58 TC	P flow ra	itet	27.00	kbits/s
Up/Dn/PgUp/PgDn-scroll M-more TCP info	W-chg	actv win	S-sort	TCP	X-exit

Figure 3-47: ip traffic monitor

5.6 last

The last command displays a list of the previous administrators who logged on to the Limited Shell - including those still logged on.

pts/O	ipartouche.finja	Mon	Sep	17	08:07		still	logged in
pts/O	ipartouche.finja	Mon	Sep	17	07:49		08:06	(00:16)
pts/O	ipartouche.finja	Mon	Sep	17	07:22		07:22	(00:00)
pts/O	192.168.120.1	Sun	Sep	16	17:35		17:36	(00:01)
pts/O	192.168.120.1	Sun	Sep	16	17:22		17:28	(00:06)
tty1		Sun	Sep	16	23:14		17:26	(-5:-47)
system boot	2.6.16.53-686	Sun	Sep	16	23:11		08:11	(08:59)
ins Sun Sep 1	6 23:11:28 2007							
	pts/0 pts/0 pts/0 pts/0 pts/0 tty1 system boot ins Sun Sep 1	pts/0 ipartouche.finja pts/0 ipartouche.finja pts/0 ipartouche.finja pts/0 192.168.120.1 pts/0 192.168.120.1 pts/0 192.168.120.1 system boot 2.6.16.53-686 ins Sun	pts/0 ipartouche.finja Mon pts/0 ipartouche.finja Mon pts/0 ipartouche.finja Mon pts/0 192.168.120.1 Sun pts/0 192.168.120.1 Sun tty1 Sun system boot 2.6.16.53-686 Sun ins Sun Sep 16 23:11:28 2007	pts/0 ipartouche.finja Mon Sep pts/0 ipartouche.finja Mon Sep pts/0 ipartouche.finja Mon Sep pts/0 192.168.120.1 Sun Sep pts/0 192.168.120.1 Sun Sep tty1 Sun Sep system boot 2.6.16.53-686 Sun Sep ins Sun Sep 16 23:11:28 2007	pts/0ipartouche.finja Mon Sep 17pts/0ipartouche.finja Mon Sep 17pts/0ipartouche.finja Mon Sep 17pts/0192.168.120.1Sun Sep 16pts/0192.168.120.1Sun Sep 16pts/0192.168.120.1Sun Sep 16system boot2.6.16.53-686Sun Sep 16ins Sun Sep 1623:11:282007	pts/0 ipartouche.finja Mon Sep 17 08:07 pts/0 ipartouche.finja Mon Sep 17 07:49 pts/0 ipartouche.finja Mon Sep 17 07:22 pts/0 192.168.120.1 Sun Sep 16 17:35 pts/0 192.168.120.1 Sun Sep 16 17:22 tty1 Sun Sep 16 23:14 system boot 2.6.16.53-686 Sun Sep 16 23:11 ins Sun Sep 16 23:11:28 2007	pts/0 ipartouche.finja Mon Sep 17 08:07 pts/0 ipartouche.finja Mon Sep 17 07:49 - pts/0 ipartouche.finja Mon Sep 17 07:22 - pts/0 192.168.120.1 Sun Sep 16 17:35 - pts/0 192.168.120.1 Sun Sep 16 17:22 - tty1 Sun Sep 16 17:22 - - system boot 2.6.16.53-686 Sun Sep 16 23:11 - ins Sun Sep 16 23:11:28 2007 - -	pts/0ipartouche.finjaMonSep1708:07stillpts/0ipartouche.finjaMonSep1707:49-08:06pts/0ipartouche.finjaMonSep1707:22-07:22pts/0192.168.120.1SunSep1617:35-17:36pts/0192.168.120.1SunSep1617:22-17:28tty1SunSep1623:14-17:26systemboot2.6.16.53-686SunSep1623:11-08:11

```
Figure 3-48: last
```

5.7 name2ip

The name2ip command displays the IP address associated with a given hostname. Enter the name2ip command followed by a hostname to display the associated IP address.



> name2ip www.finjan	.com	
www.finjan.com	А	199.203.243.204
>		

Figure 3-49: name2ip

5.8 netstat

The netstat command is a useful tool for checking your network configuration and activity. It displays the status of network connections on either TCP, UDP, RAW or UNIX sockets to the system.

> netstat
Tcp:
184 active connections openings
184 passive connection openings
O failed connection attempts
O connection resets received
1 connections established
2891 segments received
2608 segments send out
O segments retransmited
O bad segments received.
6 resets sent
Udp:
1819 packets received
48 packets to unknown port received.
O packet receive errors
1880 packets sent

Figure 3-50: netstat

5.9 ping

Use the ping command to check the network connectivity - for example after using netconf.



> ping 10.194.90.233
PING 10.194.90.233 (10.194.90.233) 56(84) bytes of data.
54 bytes from 10.194.90.233: icmp_seq=1 ttl=63 time=4.70 ms
54 bytes from 10.194.90.233: icmp_seq=2 ttl=63 time=0.246 ms
54 bytes from 10.194.90.233: icmp_seq=3 ttl=63 time=0.237 ms
54 bytes from 10.194.90.233: icmp_seq=4 ttl=63 time=0.193 ms
54 bytes from 10.194.90.233: icmp_seq=5 ttl=63 time=0.189 ms
10.194.90.233 ping statistics
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
tt min/avg/max/mdev = 0.189/1.113/4.701/1.794 ms

Figure 3-51: ping

5.10 poweroff

The poweroff command enables you to remotely shut down the appliance.

 \land

IMPORTANT: *Physical access to the appliance is needed to bring the system back online for all models except the NG-8000.*

5.11 reboot

The reboot command enables you to remotely reboot the appliance.

5.12 restart_role

The restart_role command restarts all role services.



Figure 3-52: restart role

5.13 save_support_logs

The save_support_logs command saves support logs in the support directory.



```
> save_support_logs
Collecting support info ...
Compressing data ...
Collecting support info done successfully.
Support info saved in support/info directory
> <mark>_</mark>
```



5.14 setup

The setup command assists you in setting up the device for the first time. It guides you to perform all the necessary steps to establish a working device. You can choose to rerun the Setup command to repeat the initial configuration commands at any time.

```
---Configuration status---
Role
                       : None
Time Zone
                       : None
Current date and time : 2008-04-02 09:47
Interface
                       : None
IP Address
                        : None
Default gateway
                       : None
Hostname
                        : None
DNS server
                        : None
DNS search
                        : None
(B - go back, Enter - accept default values, Q - exit from setup)
  --Set Role--
1. All in One (Default)
2. Vital Security Remote Device
3. Vital Security Policy Server
```



5.15 show

The show command shows system or service status. The show command includes the show_config, show_network, show_service, show_dbsize, show_route, and show_time.



> show_		
show_config	show_network	show_service_
show dbsize	show route	show time
> show		

Figure 3-55: show

5.15.1 show_config

The show_config command shows the current configuration.

Current config-	
Role	: all_in_one
Time Zone	: Asia/Jerusalem
Current date	: 2008-02-13 11:13
Interface	: ethO
IP Address	: 192.168.120.126/24
Default gateway	: 192.168.120.254
Hostname	: vs-126
DNS server	: 10.194.0.2
DNS search	: finjan.com
>	

Figure 3-56: Show_config

5.15.2 show_network

The show_network command shows the current network configuration. This includes: defined interfaces, DNS configuration, DNS cache and current hostname.



```
Currently the following interfaces are defined:
ethO
      Enabled
        address 192.168.120.23/24
eth1 Disabled
       address 192.168.120.23/24
       gateway 192.168.120.254
eth2
     Disabled
        address 10.0.2.1/24
eth3
     Disabled
       address 10.0.3.1/24
eth4
     Disabled
       address 10.0.4.1/24
eth5
     Disabled
        address 10.0.5.1/24
Current DNS configuration:
DNS cache:
           Enabled
nameserver 10.194.0.2
nameserver 10.194.0.5
Current Hostname configuration:
vs-23.finjan.com
```

Figure 3-57: show_network

5.15.3 show_service

The show_service command allows system administrators to view the service configuration status.

Enter the show_service command.



Figure 3-58: show_service

The following commands are available:

 show_service_all: This option displays the service configuration status for all the available services.

Service	Configuration	Status
ssh	enabled	(tcp port 22, pid 10819) is running
snmpd	enabled	(udp port 1556, pid 23504) is running

Figure 3-59: show_service_all

• **show_service_snmpd:** This option displays the service configuration status for snmpd.

> show_serv:	ice_snmpd	
Service	Configuration	Status
snmpd	enabled	(udp port 1556, pid 23504) is running
>		

Figure 3-60: show_service_snmpd

• **show_service_ssh:** This option displays the service configuration status for ssh.

> show servio	e ssh	
Service	Configuration	Status
ssh	enabled	(top port 22, pid 10819) is running
>		

Figure 3-61: show_service_ssh

5.15.4 show_dbsize

The show_dbsize command shows the file size of the databases connected with your appliance.



Figure 3-62: show_dbsize

5.15.5 show_route

The show_route command allows system administrators to view the Kernel IP routing table. Enter the show_route command.



Kernel IP rout	ing table						
Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
10.1.1.0	0.0.0.0	255.255.255.252	U	0	0	0	eth1
10.0.2.0	0.0.0.0	255.255.255.252	U	0	0	0	eth2
172.10.0.0	192.168.120.254	255.255.255.248	UG	0	0	0	ethO
192.168.120.0	0.0.0.0	255.255.255.0	U	0	0	0	ethO
0.0.0.0	192.168.120.254	0.0.0.0	UG	0	0	0	ethO

Figure 3-63: show_route

5.15.6 show_time

The show_time command allows system administrators to view the time, date, time zone ad ntp settings.

Enter the show_time command.

> show_time		
Date:	Mon Sep 17 11:48:27 IST 2007	
FimeZone:	Asia/Tel_Aviv	
NTP server:	192.168.120.21	
>		

Figure 3-64: show_time

5.16 supersh

The supersh command enables root access to the appliance. This command is reserved for Finjan Support only.

5.17 tcpdump

The tcpdump command allows the user to intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. It writes all the information into a tcpdump file. This file can then be downloaded for further analysis. Up to 4 files of 100 MB each are kept. When the fourth file gets full, the first file is deleted (i.e. cyclic progression). SFTP, such as WinSCP, is required in order to download the files.

```
> tcpdump
tcpdump: WARNING: Promiscuous mode not supported on the "any" device
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked), capture size 65535 bytes
Got 45
```

Figure 3-65: tcpdump



5.18 top

The top command displays all the running processes, and updates the display every few seconds, so that you can interactively see what the appliance is doing.

top - 13:57:20 up 7 days, 20:31, 1 user, load average: 8.00, 8.02, 8.00 Tasks: 70 total, 2 running, 67 sleeping, 0 stopped, 1 zombie Cpu(s): 0.3%us, 0.0%sy, 0.0%ni, 99.7%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st Mem: 1027948k total, 894428k used, 133520k free, 48832k buffers											
PID	HSER	DD DD	NT	WIDT	DES	SHD	q	*CPII	SHEN	TINE+	COMMAND
1 10	root	16	0	1948	512	484	S	0.0	0.0	0:00.10	Simile
2	root	RT	0	0	0	0	\$	0.0	0.0	0:00.00	migration/0
3	root	34	19	0	0	0	s	0.0	0.0	0:00.02	ksoftirqd/0
4	root	10	-5	0	0	0	s	0.0	0.0	0:00.11	events/0
5	root	10	-5	0	0	0	s	0.0	0.0	0:00.01	khelper
6	root	10	-5	0	0	0	s	0.0	0.0	0:00.00	kthread
8	root	10	-5	0	0	0	S	0.0	0.0	0:01.37	kblockd/0
69	root	20	-5	0	0	0	s	0.0	0.0	0:00.00	aio/0
68	root	15	0	0	0	0	S	0.0	0.0	0:25.99	kswapd0
654	root	10	-5	0	0	0	s	0.0	0.0	0:00.00	kseriod
707	root	11	-5	0	0	0	S	0.0	0.0	0:00.00	ata/0
719	root	15	0	0	0	0	s	0.0	0.0	0:02.29	kjournald
813	root	13	-4	2176	320	316	s	0.0	0.0	0:00.21	udevd
1510	root	10	-5	0	0	0	S	0.0	0.0	0:00.00	khubd
1849	root	15	0	0	0	0	S	0.0	0.0	0:00.00	kjournald
1851	root	15	0	0	0	0	S	0.0	0.0	0:00.00	kjournald
1853	root	15	0	0	0	0	S	0.0	0.0	0:03.38	kjournald

Figure 3-66: top

5.19 traceroute

The traceroute command displays the route over the network between two systems, listing all the intermediate routers a connection must pass through to get to its destination. It can help you determine why connections to a given server might be poor, and can often help you figure out where exactly the problem is.



```
Enter Destination IP/URL: 87.248.113.14
traceroute to 87.248.113.14 (87.248.113.14), 30 hops max, 40 byte packets
   10.194.0.1 (10.194.0.1) 0.475 ms 0.327 ms 0.324 ms
 1
 2
   finjangw-mered7.ser.netvision.net.il (199.203.92.237)
                                                            26.407 ms
                                                                       5.137 ms
32.805 ms
3
   fa0-1.gw2.hrz.netvision.net.il (212.143.203.91)
                                                      11.665 ms
                                                                 13.838 ms
                                                                            15.17
a
 ms
   tlv-hrz2-ds3.nv.net.il (207.232.0.254) 5.917 ms
 4
                                                      5.599 ms
                                                                 5.446 ms
 5
   pos2-11.brdr1.lnd.nv.net.il (212.143.12.9)
                                                 113.609 ms
                                                             160.331 ms
                                                                         152.772
ns:
 6
   ldn-tch-i1-link.telia.net (213.248.100.101)
                                                  113.521 ms
                                                             87.926 ms
                                                                         85.046 m
 7
   ldn-b1-link.telia.net (80.91.250.209)
                                           81.188 ms
                                                       77.219 ms
                                                                  84.804 ms
 8
   ldn-bb1-link.telia.net (80.91.250.91)
                                           88.319 ms
                                                       93.565 ms
                                                                  96.509 ms
   dln-b1-link.telia.net (80.91.250.85) 103.424 ms
 q
                                                      99.411 ms
                                                                  94.544 ms
  yahoo-115023-dln-b1.c.telia.net (213.155.141.182)
10
                                                        174.147 ms
                                                                    164.375 ms
99.716 ms
11 ge-1-1.bas-b1.ird.yahoo.com (87.248.101.1)
                                                170.895 ms
                                                             170.694 ms ge-1-3.ba
s-b2.ird.yahoo.com (87.248.101.7) 157.647 ms
12
   f1.us.www.vip.ird.yahoo.com (87.248.113.14)
                                                  161.897 ms
                                                              183.232 ms
                                                                          185.604
ms
```

Figure 3-67: traceroute

5.20 uptime

The uptime command produces a single line of output that shows the current time, how long the system has been running (in minutes) since it was booted up, how many user sessions are currently open and the load averages.



Figure 3-68: uptime

5.21 vmstat

The vmstat command reports statistics about kernel threads, virtual memory, disks, traps and CPU activity. Reports generated by the vmstat command can be used to balance system load activity.



> v	ms	tat													
pro	CS		mem	ory		sua	ap	ic)	-syst	em		C]	pu	
r	b	swpd	free	buff	cache	si	30	bi	bo	in	cs	us	sy	id	wa
0	0	501300	126088	52052	323584	1	1	23	63	28	5	2	0	98	0
0	0	501300	126088	52068	323568	0	0	0	84	282	76	0	0	99	0
1	0	501300	126088	52076	323628	0	0	0	7	278	70	0	0	100	0
0	0	501300	126088	52092	323612	0	0	0	31	281	73	0	0	100	0
0	0	501300	126088	52092	323612	0	0	0	0	275	70	0	0	100	0
0	0	501300	125840	52108	323636	9	0	9	16	280	255	3	1	96	0

Figure 3-69: vmstat

5.22 w

The w command shows who is currently logged on and the current command they are running.

08:29:58	up	15:18,	1	user,	load	average:	0.00,	0.00,	0.00	
JSER	TTY	FI	ROM			LOGINO	IDLE	JCPU	PCPU	WHAT
admin	pts/	'0 i;	part	ouche.	finja	08:29	0.00s	0.01s	0.01s	/usr/bin/python

Figure 3-70: w

5.23 wget

The wget command allows you to download web files using HTTP, HTTPS and FTP protocols.



Figure 3-71: wget

6 First Login to the Management Console

When you first log in to the Management Console, you will be directed to the License screen. A single license key can be used for multiple Policy Servers. It can also be re-used for situations where the administrator needs to reinstall the system.

Evaluation License: When entering the Management Console for the first time, an installation Wizard will run and the administrator must enter a license key. An evaluation key entitles you to a 30 day evaluation period with full Vital Security functionality. Once the 30 days evaluation period has passed, Vital Security will start forwarding Internet content through without scanning it. The Management Console will be disabled until the administrator



enters a permanent license key.

NOTE: The Policy Server will update Finjan Headquarters as to the status of the License. This information is confidential and will be kept at the Finjan Financial offices.

Ten days before the evaluation license is about to expire, an informative message will be displayed.

Permanent License: A permanent license is generated by Finjan and sent to the customer. Its expiration date is based on a service agreement with the customer. Starting three months before the expiration date, the administrator will receive notifications that the license needs to be renewed. Once the license has expired, you will be treated to a thirty day grace period where traffic will be scanned but administrators will have very limited access to the Management Console. After the grace period is complete, Vital Security will no longer function as required.

To enter your new License Key:

- 1. Enter the license key provided by Finjan and click **Continue**.
- 2. Read through the EULA agreement and check the I accept checkbox.
- 3. Click OK to finish.

7 Update Mechanism

The **Update** mechanism periodically checks Finjan's Web site and automatically displays any available updates via the Management Console for the administrator. There are three categories of updates:

Security Updates Behavior scanning logic and vulnerability data: These can be configured automatically. Vital Security behavior profiling data and security processors are updated automatically from the Finjan site as soon as new Windows vulnerabilities are discovered. Vulnerability protection typically arrives before viruses that exploit the vulnerability are released.

Finjan Software is a market leader in malicious mobile code. Malicious Code Research Center at Finjan employs dedicated experts who work around the clock to identify new Windows vulnerabilities and exploits, enabling real day-zero protection.

- OS Version updates: Automatic downloading from the Finjan Web site can be enabled/disabled via the Management Console. You will be notified automatically when updates become available so that you can install them and keep your system up-to-date.
- Third-party security engines: Vital Security incorporates best-of-breed third-party engines (anti-virus and URL categorization). These applications rely on frequent and regular updates, and these are downloaded and installed automatically by the autoupdate feature.



7.1 Installing Updates

Updates are installed via the Vital Security Management Console, which runs on the All in One appliance or Policy Server at the default HTTPS port (443). It is recommended to check for updates each time that you use the system, in the event that security and functional updates have been released either since the product was installed or since the last check was performed.

7.1.1 Configuring Next Proxy for Updates

If you are connecting your All-in-One appliance or Policy Server to the Internet via a proxy server, you must configure the proxy in the Proxy Server and Port fields in the Management Console on the Administartion –> Updates –> Updates Configuration tab, and then click Save and Commit Changes to ensure that the change takes effect.

7.1.2 Configuring the Firewall for Automatic Updates

In order to enable Automatic updates for the NG Appliance Series, the Firewall should be opened for the Policy Server, using the HTTPS (port 443) protocol in the outgoing direction.

There are two destination URLs:

https://updateNG.finjan.com/remote_update

https://mirror.updateNG.finjan.com/remote_update

The following table details the ports needed for configuring Automatic Updates:

Description	Port Number				
All in one machine (web traffic)	oorts)				
Only HTTP, FTP and HTTPS from					
LAN to WAN					
Additional ports to open from L	AN to DMZ				
Manager - transfer of policy updates, and other updates	5222				
Manager – secure transfer of policy	5224				
updates, and other updates					
Log traffic (from server)	8000				
Secure Log traffic	8001				
SNMP queries (if enabled)	161 UDP				
Additional ports to open from D	MZ and LAN				
SNMP trap (if enabled and	162 UDP				
configured to send traps to the					
SNMP Manager on the LAN)					

7.1.3 Offline Updates

Customers who are using the appliance in an isolated network that is not connected to the Internet, can download any updates from the Finjan update site. These updates can be



manually downloaded and saved onto a removable media (e.g. CD) which should then be connected to the offline computer where you manage the Policy Server. From the Management Console, you can install the updates using the Import Local Updates option.

This feature requires a special license. Please contact your Finjan representative for further details.

8 Routing Traffic through the Appliance

You can use any of the following proxy setting alternatives, or configure proxy access to be transparent.

8.1 Configuring Workstations for Routing Traffic through the Appliance

Manual Configuration per Individual User

In Internet Explorer, select Tools \rightarrow Internet Options \rightarrow Connections \rightarrow LAN Settings and click the Advanced button in the Proxy Servers area. In the Proxy Settings dialog box, enter the IP address of the Vital Security Scanning Server or Load Balancer in the HTTP field.

Customized Installation of Internet Explorer

Download the Microsoft tool IAEK6 in order to enable customized installation of Internet Explorer for all users.

Group Policy Manager

In the **Microsoft Active Directory**, create a **Group Policy Object** (GPO) that configures which proxy to use per machine or user.

Login Scripts

For older legacy systems such as NT4, you can use login scripts to configure the proxy server.

In Firefox, select Tools → Options and click on the Network tab. Click on the Settings tab, and can manually specify the IP address(es) of the proxy or use automatic proxy settings via a URL.

8.2 Transparent Proxy

Vital Security can be deployed as a transparent proxy - for HTTP, HTTPS and FTP, in conjunction with a third-party content switch or a layer-4 router in the network. This means that all HTTP traffic is routed, at packet level, through the content switch to the Vital Security Appliance. End-users are not aware of this and have the same surfing experience as if they were communicating directly with the Web server.

When deployed as a transparent proxy, there is no need to configure proxy settings of individual end-user browsers. However, because of the transparency, the appliance is not



able to perform proxy-level user authentication.

To enable working in transparent mode:

- 1. In the Vital Security Management Console, navigate to Administration → System Settings → Finjan Devices → Scanning Server.
- 2. In the selected Scanning Server, choose the **General** node.
- 3. Click Edit and select the Enable Transparent Proxy Mode.
- 4. Define the ports to be used for the scanned traffic.

	TLS .		HTTP Ports			
+	From	То	+	From	То	
21		21	80		80	
HTTPS	Ports					
HTTPS	From	То	(

Figure 3-72: Transparent Proxy Mode

5. Click Save and click



The following diagram illustrates the deployment.





Figure 3-73: Transparent Proxy

9 Working with HTTP

In order for browsers or other appliances to be protected by Vital Security, the Vital Security must be configured as the Proxy Server. Working with the Vital Security you can configure your browser for maximum efficiency (number of requests per second) in Microsoft Internet Explorer by selecting **Tools** \rightarrow **Internet Options** \rightarrow **Advanced** and selecting both **Use HTTP 1.1** and **Use HTTP 1.1 through proxy connections**.

9.1 HTTP Proxies

Vital Security can communicate with any RFC-compliant Web proxy.

9.2 Working with Caching Proxies

When a caching proxy is in use, **Vital Security** can be integrated either upstream or downstream from the cache proxy in the network.

9.2.1 Downstream

When Vital Security is positioned downstream of the cache proxy, the cached content is rescanned for every request. This topology clearly works for systems with user/group policies that differentiate between the sites that the different users/groups may visit, as every request is submitted to Vital Security and scanned against the relevant policy.

This means that:



- Every request is scanned with the latest security updates, even if the content was cached before the last update.
- Traffic scanned initially by Vital Security is cached and subsequently forwarded again by the caching proxy in line with additional user requests. Each time this happens, the content is rescanned by Vital Security. The resulting drain on resources should be taken into account regarding performance.
- Every additional request for cached content is subjected to the policy specific to the user making the new request. Policy changes will always be implemented because all content, even if it comes from the cache, is scanned again by Vital Security.
- All accesses to cached content are subject to the logging policy, and are potentially logged by Vital Security.

9.2.2 Upstream

When Vital Security is positioned upstream from the cache, traffic is scanned only once, and is then cached and forwarded directly to the users. This is optimal for organizations that use a single policy for all Internet access, and do not apply different policies to different users/ groups. This is not suitable for per user/group policies that differentiate between the sites visited by users/groups. (In such cases, you may consider working with ICAP.)

This means that:

- Because content is only scanned once, there is less drain on resources, leading to improved performance.
- Cached content is not subject to the latest security updates, nor to policy changes.
- Vital Security cannot log accesses to cached content.

9.3 HTTP Authentication

Authentication enables the following:

- Ensures that only requests from bona-fide users are handled/processed.
- Enables the allocation of different policies to different users and/or groups by matching authentication data to user identifiers in the system.
- Ensures that all logged transactions are attributed to the corresponding user.

Authentication policies are covered in the Policies chapter of the Management Console Reference Guide.

10 Working with ICAP

ICAP stands for Internet **C**ontent **A**daptation **P**rotocol. ICAP is used in conjunction with caching proxies such as Network Appliance NetCache or Blue Coat Proxy SG. ICAP configurations typically require significant tuning to maximize the benefits.



10.1 Why work with ICAP?

One of the reasons is that if you are working with a caching proxy that supports the ICAP protocol, you can achieve significant performance benefits from configuring Vital Security as an ICAP server rather than an HTTP proxy. Working with ICAP means that you don't need to change the topology but rather integrate our product with ICAP. You can configure specific content to be sent for scanning. The default is to scan everything.

10.2 Vital Security as an ICAP Server

When deployed in the ICAP environment, the ICAP client typically provides user credentials and **Vital Security** does not have to authenticate users.



Figure 3-74: Vital Security as an ICAP Server

10.3 REQMOD – RESPMOD Deployment

As an ICAP Server, Vital Security can provide both REQMOD (Request Modification) and RESPMOD (Response Modification) services.

- The service name for REQMOD is **Finjan_REQMOD**.
- The service name for RESPMOD is **Finjan_RESPMOD**.

Vital Security can receive both REQMOD and RESPMOD requests.

Here is an example of an ICAP URL for the REQMOD service:



icap://192.168.2.153:1344/Finjan_REQMOD

NOTE: When working with RESPMOD, REQMOD must be enabled.

Vital Security can also work in REQMOD only, for example, for performing URL filtering, but in this case, the actual incoming content is not scanned.

Configuration of a Vital Security scanning server as an ICAP server is carried out via the Management Console.

NOTE: If there is no direct Internet access, in order to perform pre-fetching of Java classes for Applet scanning, ALL Scanning Servers must have the next proxy configured. If you are using ICAP, ensure that the NG Appliance Scanning Server appears on the Access List.

10.4 ICAP Clients

There are a number of ICAP Clients that support Vital Security:

- Network Appliance NetCache Series
- Blue Coat Proxy SG Series



C H A P T E R

CONFIGURING ICAP CLIENTS

This chapter describes the configuration of the following ICAP clients:

- Network Appliance NetCache Series (NetApp)
- Blue Coat

1 Network Appliance NetCache Series (NetApp)

In order to configure Vital Security to work with NetApp, follow the procedures below in the order given.

To configure NetApp via Vital Security:

- 1. In the Vital Security Management Console, select Administration → System Settings → Finjan Devices.
- 2. In the Devices screen, select the Scanning Server with which you are working, and then select **ICAP**.

Finjan devices	ICAP							
Finjan devices	Device IP: 192.168.120.55 Enable ICAP ICAP Service Options Advanced Access List Headers Listening IP: Listening Port: 1344							
 Policy Server Device Default Values 								

Figure 4-1: Devices - ICAP


- 3. Click on **Edit** in the right hand pane.
- 4. Select Enable ICAP for Device.
- 5. In the Access List tab, click on 🖕 and select Add Row from the drop-down menu.

+	l.	Туре			So	urce IP		Weight
1	NetApp		6	10	• 194	. 78	. 67	100

Figure 4-2: Access List

- 6. Select NetApp from the Type drop-down list.
- 7. Add the **Source IP** address of the ICAP client and add the **weight**. Note that the weight is in percentage. If there is only one ICAP client, enter 100 in the weight field.
- 8. In the ICAP Service tab, enter the IP Address of the Scanning Server.
- 9. Click Save to apply changes, else Cancel. Select Commit changes.

To configure NetApp via the NetApp web interface:

- 1. Log in to the NetApp Web interface. The ICAP Setup window is displayed with the General tab open.
- 2. Click Setup.
- 3. Click ICAP \rightarrow ICAP 1.0 in the left hand pane.
- 4. Select the Enable Version 1.0 option.



Setup	Utilities	`	NetCache Appliance:	C1200-2010326.finjan.com:31 Version: NetApp Release 6.0
				Help () NOW
ICAP - IC	AP 1.0			۲
Use this page Enable boxes,	to view existing ICA click Commit Chan	P service farms, edit their s ges to save your selections	ettings, enable or disable them. After selecting 8.	one or more Del or
General	Service Farms	Access Control Lists	Test ICAP Service	
ICAP 1.0 Enab	le			۲
🔽 Enable I	CAP Version 1.0			
ICAP 1.0 Log	Enable			۲
🔽 Enable t	ne ICAP 1.0 log			
ICAP 1.0 X-CB	ent-IP from X-Forw	arded-For		۲
🗖 Generate	the X-Client-IP ICA	P Header from the X-Forwa	arded-For HTTP Header	
ICAP 1.0 Log	Format			۲
ICAP Det	fault Log Format			

Figure 4-3: ICAP Setup - General

- 5. Open the Service Farms tab.
- 6. Press the New Service Farm button to create a new ICAP Service.

To configure an ICAP Service Farm:

- 1. To set a REQMOD service, ensure that the following conditions are met:
 - In the Vectoring Point field, select **REQMOD_PRECACHE**.
 - In the Services field set the service URL:

icap://[Vital Security's IP]:[ICAP port]/Finjan_REQMOD on

- 2. To set a RESPMOD service, ensure that the following conditions are met:
 - In the Vectoring Point field select respmode_precache
 - In the Services field set the service URL:

icap://[Vital Security's IP]:[ICAP port]/Finjan_RESPMOD on

Several services can be defined in **Services** and load-balanced by NetApp.





New ICAP Service Farm

Edit the ICAP Service Farm Definition. You must Commit Changes for your changes to be saved.

ICAP Service raini Deminuor	ICAP	Service	Farm	Definition
-----------------------------	------	---------	------	------------

Service Farm Name:	V3_REQMOD
ectoring Point	REQMOD_PRECACHE
Order:	2
Service Farm Enable:	
oad Balancing:	Round Robin Based 🛩
Bypass on Failure:	
Consistency:	weak 💌
bw Threshold:	
Services:	icap://10.194.90.157:1344/Finjan_REQMOD
	(Format on each line: icao//10 55 10 43:1344/cervicename on)

Commit Changes

Close

Figure 4-4: New ICAP Service Farm

3. Once the services have been configured in the Service Farms, Access Control List rules should be defined to include these services.



Setup Utilities				
Changes Committed				
ICAP - ICAP 1.0				
Use this page to view existing ICAP service selections. General Service Farms Access	e farms, edit their setti ess Control Lists	ngs, enable or disab Test ICAP Service	le them. After selecting o	one or more Del (
Enable ACLs				
Enable Access Control Lists				
HTTP ACL				
icap (vs_RESPMOD) any icap (vs_REQMOD) any				

Figure 4-5: Access Control Lists

With every ICAP settings change, NetApp sends an OPTIONS request to the relevant ICAP Service.

2 Blue Coat

To configure Vital Security to work with Blue Coat, please follow all the procedures below in the order given.

To configure Blue Coat via Vital Security:

- 1. In the Vital Security Management Console, select Administration → System Settings → Finjan Devices.
- 2. In the Devices screen, select the Scanning Server with which you are working, and then select ICAP.
- 3. Click on Edit in the right hand pane.
- 4. Select Enable ICAP for Device.



5. In the Access List tab, click on 👍 and select Add Row from the drop-down menu.

Weight		neaucis.	Auvanceu Access List	ICAP DEF
the Rest of the Party of the Pa	urce IP	So	Туре	+
45 100	.33 .45	10 . 194	Blue Coat 🛛 💽	1
45 1	•33 •45	10 . 194	Blue Coat 💌	2

Figure 4-6: Blue Coat Configuration

- 6. Select Blue Coat from the Type drop-down list.
- 7. Add the **Source IP** address of the ICAP client and add the **weight**. Note that the weight is in percentage. If there is only one ICAP client, enter 100 in the weight field.
- 8. In the ICAP Service tab, enter the IP Address of the Scanning Server.
- 9. Click Save to apply changes, else Cancel. Select Commit changes.

To configure Blue Coat via the Blue Coat Web interface

1. Log in to the Blue Coat web interface.







2. Navigate to the Management Console.

Blue ®Coat	Management Conse	ole		HOME SUPPORT
192.168.0.30 - Blue Coat St	G800 Series			
	Configuration Mail General Clock Archive Network Services External Services Health Checks Authentication Bandwidth Mgmt. Policy Content Filtering Forwarding SSL Access Logging	Apply	Jc9 biySO Appliance: Blue Coat SO800 Series wySO Appliance: 00152 Cancel	Help

Figure 4-8: Blue Coat Management Console



NOTE: *If, at any time during the session, the Java Plug-in Security Warning appears, select Grant this session to continue.*

To define REQMOD (Request Modification) Service.

- 1. From the Blue Coat Management Console, select External Services → ICAP. The ICAP Services screen is displayed on the right.
- At the bottom of the ICAP Services screen, click New. The Add List Item dialog box is displayed.
- **3.** Enter a name and click **OK**. For instance, Finjan_Reqmod. The External Services window is displayed again with the name you have selected.

Blue ® Coat	Management Console		HOME S	UPPORT DOCUMENTATION LOG OU
10.194.150.166 - Blue Coat	SG800 Series			
Configuration Ma General Identification Clock Archive Network Services External Services ICAP" Websense Service-Oroups Health Checks Authentication Bandwidth Mgmt. Policy Policy Options Policy Files Visual Policy Manager Excentions	Aintenance Statistics ICAP Services ICAP Pable Services: Respmod New	ence Page Serv	ice	Health: OK
 Content Filtering Forwarding SSL Access Logging 	Preview	Apply	Revert	Help



4. Click Edit. The Edit ICAP Services dialog box is displayed.



ICAP version:	10	
Constant LIDI		
Service URL:	icap://10.194.90.10/Fi	njan_REQMOD
Maximum number of connec	tions: 5	
Connection timeout (second	s): 70	
Patience page delay (secon	ds): 10 F	enabled
Notify administrator:	🔲 Virus detected	
□ ICAP v1.0 Options		
Method supported:	C response modification	
	• request modification	
Preview size (bytes):	0	🗖 enabled
Send:	Client address	Server address
	Authenticated user	Authenticated groups
ICAP server tag:		
Sense settings	Get settings from ICAP serv	/er
- Health Check Options	S.	
		NT 1 1

Figure 4-10: Edit ICAP Services



Field Name	Field Data to be entered
ICAP Version	Select 1.0 from the dropdown list
Server Type	Enter the following: icap:// <scanner ip<="" th=""></scanner>
	(ICAP server)>: <scanner port<="" th=""></scanner>
	(default=1344)>/Finjan_REQMOD. For
	example, icap://192.168.90.10:1344/
	Finjan_REQMOD
Method Supported	Click the request modification radio
	button.

The following table describes the field data to be entered:

5. If your Vital Security scanner is up and running, then press the **Sense Settings** button and then **OK**. A confirmation message appears; click **OK** again.

(If, on the other hand, your Vital Security scanner is not yet up and running, then click **OK** only to continue. In this case, you should return to this dialog box later on when Vital Security is up and running in order to select Sense Settings)

- 6. In the Edit ICAP Services box, select the **Authenticated User** checkbox and then click **OK**.
- 7. Click **Apply** in the ICAP Services screen to complete the configuration.

To activate the REQMOD Service:

1. In the Blue Coat Management Console, select Policy → Visual Policy Manager. The Visual Policy Manager is displayed.



Blue ® Coat	Management Con	sole Home i se
192.168.0.30 - Blue Coat S	G800 Series	
•	Configuration M	aintenance Statistics
	General Identification Clock Archive Network Services External Services ICAP Websense Senice-Groups Health Checks Authentication Bandwidth Mgmt. Policy Policy Options Policy Options Policy Files Wisual Policy Manager Exceptions Content Filtering Forwarding SSL Access Logging	Visual Policy Manager

Figure 4-11: Visual Policy Manager Launch

2. Click Launch and the Visual Policy Manager dialog box is displayed.

adtus de/u [Schocho stand [bomoser [bom			
respinoul pypass chacked web Audie	ntication Layer (1)	Forwarding Layer (1)	
No. Destination	Action	Track	Comment
1 Any 🚰 ICAP	Dominal Consist	and the second se	

Figure 4-12: Visual Policy Manager Dialog Box

3. From the Main Menu Bar, select Policy → Add Web Access Layer, and the Add New Layer dialog box is displayed.



×
Cancel

Figure 4-13: Add New Layer Dialog Box

4. Add in the required name and click **OK.** The Visual Policy Manager is displayed with a new Web Access Layer.

Blue Coat Visit File Edit Policy	al Policy Manager Configuration Viev	(10.194.150.168 • Help	5 - Blue Coat S(i800 Series)		>
C Add Rule	Delete F	tule 🔶 🔶	Move Up	🗲 Move Dow	vn 🗎 🔁 In:	stall Policy
Reqmod						
No. Sou	irce Destination	n Service	Time	Action	Track	Comment
					Deny Deny (Content F Set Edit Delete Negate Cut Copy Paste	ilter)

Figure 4-14: Web Access Layer Added

- 5. In the Action column, right-click on **Deny**, and then select **Set**. The **Set Action Object** dialog is displayed.
- 6. Click New.



😺 Se	et Action Object		×	
Exist	ing Action Objects			
Shov	w: All (sort by object-name)		*	
	Allow		<u> </u>	
	Always Verify Block IM Message Encryption			
88	Block Popup Ads			
	Deny			
	Return Exception			
	Return Redirect			
	Send IM Alert			
	Modify Access Logging		-	
	Override Access Log Field			
	Rewrite Host	ve l	Edit	
	Deflect ID			
	Supprace Headard			
	Coptrol Doquest Header	el	Help	
	Control Response Header			
	Netfor Lizer			
	Noti y Oser			
	Strip Active Content			
	Set Client HTTP Compression			
	Set Server HTTP Compression			
	Set HTTP Compression Level			
'ro>	Set SOCKS Compression	-		E
	Manage Bandwidth			
-	Modify IM Message			
	Return ICAP Patience Page			Revert
	Set External Filter Service			
	Set ICAP Request Service			
	Set FTP Connection	Systems, Inc. All righ	ts reserved.	
	Set SOCKS Acceleration			
	Set Streaming Max Bitrate			
	Combined Action Object			

Figure 4-15: Edit ICAP Request Service

7. In the Add ICAP Request Service Object window, select the Use ICAP Request Service checkbox.



🐱 Add ICA	P Request Service Object	×
Name:	ICAPRequestService3	
🛈 Use I	CAP request service finjan_reqmod	
	or handling	
If	an error occurs during ICAP request pro	cessing:
	• Deny the client request (recommer	nded)
	C Continue without further ICAP req	uest processing
C Do no	it use any ICAP request service	
17 ICAP red	juest services configured on ProxySG	
[OK Cancel	Help

Figure 4-16: Add ICAP Request Service Object

- **8.** From the drop-down list, select the REQMOD service you have defined, and click **OK**.
- 9. Go back to the Set Action Object dialog box, and click OK.
- 10. Click the Install Policy button in the Visual Policy Manager.

9

- To define RESPMOD (Response Modification) Service:
 - Carry out the same steps as the above procedure. When adding a new layer to the Blue Coat policy, choose a Add Web Content Layer instead of Add Web Access Layer.
 - Choose Respmod instead of Reqmod where relevant. For example:icap:// 192.168.90.10:1344/Finjan_RESPMOD





INSTALLATION DETAILS

1 Installing your Vital Security Appliance

An update can be performed by restoring the configuration (after fully installing from USB).

- **To install a Release using a USB key on NG-5000:**
 - **1.** Attach a bootable USB flash device, and a USB-keyboard and VGA monitor to the appliance whilst it is still switched off.
 - 2. Power on the appliance. The appliance will read automatically from the USB key.
 - 3. When the Finjan screen appears, type yes to continue with the process.



Finite Security Vital Security

Jital Security is about to be installed. This procedure will initialize (i.e. format, erase) data from the magnetic media on the appliance and install Jersion: 9.0.0, Build: #20, dated: 2008-02-14-2251.

This process should take approximately 10 minutes (20 minutes for NG-8000), assuming you are using a USB2.0 device. If your bios is not configured to use JSB2.0, it is highly recommended to change this setting BEFORE CONTINUING with the setup process.

In order to continue with this process, type 'yes' and press the return key. boot: $_$

Figure A-1: Finjan installation screen

- **4.** Let the installation run it will take approximately 10 minutes. After this time, the appliance will reboot.
- 5. When the Finjan installation screen reappears, remove the USB key. Reboot the appliance by pressing **Ctrl + Alt + Delete**.

Set up the configuration as required via the Limited Shell as described in <u>Initial Setup of your</u> <u>Vital Security Appliance using Limited Shell</u>.

To install a Release using a USB key on NG-6000/NG-8000:

- 1. Attach a bootable USB flash device, and a USB-keyboard and VGA monitor to the appliance whilst it is still switched off.
- **2.** Power on the appliance.
- **3.** Press F12 to choose the Boot Device Configuration Menu. The boot device menu appears.
- 4. In the Boot Device menu, use the arrow key to select USB Key/Disk and press Enter.
- **5.** In the screen that appears, select the required USB key and press Enter.



- 6. In the next screen, in the Persistent field, ensure that it says **This boot only** and press Enter.
- **7.** In a few minutes, the Finjan screen appears, type yes to continue with this process.
- 8. When the Finjan screen appears, type yes to continue with the process.



This process should take approximately 10 minutes (20 minutes for NG-8000), assuming you are using a USB2.0 device. If your bios is not configured to use JSB2.0, it is highly recommended to change this setting BEFORE CONTINUING with the setup process.

In order to continue with this process, type 'yes' and press the return key. boot: $_$

Figure A-2: Finjan installation screen

- **9.** Let the installation run it will take approximately 20 minutes. After this time, the appliance will reboot.
- **10.** When the Finjan installation screen reappears, remove the USB key. Reboot the appliance by pressing **Ctrl + Alt + Delete**.
- **11.** Set up the configuration as required via the Limited Shell as described in <u>Initial</u> <u>Setup of your Vital Security Appliance using Limited Shell</u>.

NOTE: For information on installing version 9.0 on older appliances, please contact Finjan Support.



1.1 Remote Installation on NG-8000

What you need:

- ◆ Java[™] 6 installed on your computer
- DVD reader
- Internet connection to the BladeCenter Management Module with a valid IP address

To install a Release remotely onto a BladeCenter:

- 1. On your local PC, insert the DVD with the release on it into the DVD slot.
- 2. In your Internet browser, enter the Management Net address. For example, HTTP:// 10.194.150.75
- 3. Enter the user name: USERID and password: PASSW0RD (Note that there is a zero in PASSW0RD.)

Connect to 10.19	94.150.75
R	GA
Local System User name:	🖸 USERID 💌
Password:	Remember my password
	OK Cancel

Figure A-3: Login Screen

4. In the BladeCenter Management Module, on the left-pane, under Blade Tasks, select **Remote Control**. Next, click **Start Remote Control**. A new window opens.



TRM. B	adeCenter, Advanced Management Module	
Bay 1: SN#BM User: USERID	KVM owner: Blade12 - SN#ZJ1ZCC5CP10F since 03/30/2008 09:32:51 Media tray owner: No blade selected. Console redirect: No session in progress.	4
✓ Monitors ▲ System Status Event Log LEDe	Refresh	
Power Management Hardware VPD	Start Remote Control 🥝	
Firmware VPD Remote Chassis ▼Blade Tasks Power/Restart On Demand	Click "Start Remote Control" to control a blade remotely. A new window will appear that provides access to the Remote Console and Remote Disk functionality. On this window, you will have full keyboard and mouse control of the blade which currently owns the KVM. You will also be able to change KVM and media tray ownership.	_
Remote Control Firmware Update Configuration	Note: An Internet connection is required to download the Java Runtime Environment (JRE) if the Java 1.4.2 Plug-in is not already installed. For best results, use Sun JRE 1.4.2_08 or higher.	
Open Eabric Manager	Start Remote Control	

Figure A-4: Remote Control - Start Remote Control

5. In the Remote Control window, select the required Blade from the Media Tray drop-down list. In this example, we are working with Blade 7.

Remote I	Disk				
Media Tray	Blade7 - SN#YK1180668188	Mount Remote Media To:	Chassis KVM Owner 💌	Refresh Lists	
	Available Resources	2	Select	ed Resources	- 51
Select Ima Removable	ge e Drive (A:)	>>> <<	Mount All	Write Protect	
Remote (Console				
Ctrl+Alt.	Alt+Tab				

Figure A-5: Remote Control: Media Tray

6. In the Available Resources window, scroll down and select CD-Rom. Using the arrows, move it right to the Selected Resources window and click **Mount All**.



🕈 Remote I)isk				
Media Tray	Blade7 - SN#YK1180668188	Mount Remote Media To:	Chassis KVM Owner 💌	Refresh Lists	
	Available Resources		Select	ed Resources	
Select Ima	ge		CD-ROM (E:)		
Removable	Drive (A:)				
CD-ROM (2). X	>> <<			
			Mount All	Write Protect	
✓ Remote (Console				
Remote (Console 		PROFIL PRO	1	

- Figure A-6: Selected Resources Mount All
- 7. In the Remote Console section, in the KVM field, scroll down to the Blade7 option (See figure above).
- 8. Switch over from the Remote Control screen to the Main Management Screen and click **Power/Restart** on the left pane. Selct Blade7 and click **Restart Blade**.



User: USERID BI	ade Pow	er / R	estart 🥝				
Monitors A System Status Event Log	Click the c below the t	heckbo table to	exes in the first column to perform the desired action	select o n.	ne or more bl	ades; then,	click one c
Power Management	E	Bay	Name	Pwr	Local Pwr Control	Wake on LAN	Console Redirect
Firmware VPD		1	SN#ZJ1XXW4C912K	On	Enabled	On	
Remote Chassis ade Tasks	E	2	GPC	On	Enabled	On	
Power/Restart	Г	4	SN#ZJ1ZCC5CN1KD	On	Enabled	On	
Remote Control		5	SN#ZK124X61A1MR	On	Enabled	On	
Firmware Update	_	6	SN#VK11806681BN	On	Enabled	On	L
Configuration	6	7	CN#///100000101	0.	Enabled	0.	
Serial Over LAN	$\mathbf{\nabla}$	1	SN#1K110000010D	Un	Enabled	Un	1
Open Fabric Manager		8	SN#ZJ1ZCC5CW1AW	On	Enabled	On	
Admin/Power/Restart		9	SN#ZJ1ZCC5CRR0C	On	Enabled	On	
Configuration		10	SN#ZJ1ZCC5CN1GL	On	Enabled	On	
Firmware Update	Г	11	SN#ZJ1ZCC5CN12M	Off	Enabled	On	
Control		12	SN#71170050010E	00	Enabled	0.0	
General Settings	- And	12	SIMMEDIZCOSCP TOP	On	Linabled	Un	
Alerts Serial Port		14	PRESBRUAPSPHS01	On	Enabled	On	-
Port Assignments Network Interfaces Network Protocols Chassis Internal Networ Security File Management Firmware Update Configuration Mgmt	Powe Powe Shut Resta Enabl Disab Enabl	r On B r Off Bl Down (art Blad le Loca le Loca le Wak	iade ade DS and Power Off Blade e I Power Control al Power Control e on LAN				

Figure A-7: Restart Blade

9. Switch back over to the Remote Control screen, and wait for the Server to boot up from the DVD. Type **yes** to start the installation.



Finite Security" Securing your web

Jital Security is about to be installed. This procedure will initialize (i.e. format, erase) data from the magnetic media on the appliance and install Jersion: 9.0.0, Build: #20, dated: 2008-02-14-2251.

This process should take approximately 10 minutes (20 minutes for NG-8000), assuming you are using a USB2.0 device. If your bios is not configured to use JSB2.0, it is highly recommended to change this setting BEFORE CONTINUING with the setup process.

In order to continue with this process, type 'yes' and press the return key. boot: $_$

Figure A-8: Finjan Vital Security Installation Security

- **10.**Let the installation run it will take approximately 10 minutes. After this time, the appliance will reboot.
- 11. When the Finjan installation screen reappears, remove the DVD. Reboot the appliance by pressing **Ctrl + Alt + Delete**.
- **12.** Set up the configuration as required via the Limited Shell as described in <u>Initial Setup</u> of your Vital Security Appliance using Limited Shell

1.2 Post-Installation Bonding Script on NG-8000

In order to support topologies where switch redundancy is required, a special bonding script (also known as teaming) has been designed for the NG-8000. This should only be run by a Finjan certified engineer. Please contact Finjan Support for details.





POST-INSTALLATION SYSTEM HARDENING

1 System Hardening

After the installation and configuration of the Vital Security system, it is highly recommended to "harden" (tighten up) the Policy Server and Scanning Server in order to prevent unauthorized access to the system.

1.1 Policy Server

The procedures below shows how to harden the Policy Server by denying unauthorized access to it.

1.1.1 Management Access List

Vital Security provides the ability to configure a Management access list from the Management Console. The access list ensures that only restricted IP addresses have access to the system for management. The Access list is not enabled by default since the administrator would not be able to access the system due to the fact that Administrator subnets are not known before the installation. Once the access list is enabled, all access from unknown IPs is disabled.

Configure a Management Access List:

- Navigate to Administration → System Settings → Finjan Devices → <IP Address>
 Access List.
- 2. Click Edit to enable the screen for editing mode.
- 3. Select Use Access List.
- 4. In the **Management Access List**, click on the plus icon and in the row provided enter the relevant IP addresses.
- 5. Click Save and click 🛛 🖄 .



1.1.2 Management Console Password

The default password provided is "finjan". It is recommend to change the default password as soon as possible.



To change the Management Console password:

- 1. Navigate to Administration \rightarrow Administrators \rightarrow admin.
- 2. Click Edit to enable the screen for editing.
- 3. Enter a password in the New Password field and repeat in the Confirm Password field.
- 4. Click Save and click X

1.1.3 Default SNMP v2 Community String

The default SNMP v2 Read-Only community string is 'finjan'. Since most attack tools try to use the default well-known community strings, it is recommended to change it.

To change the SNMPv2 Community String: 3

- 1. Navigate to Administration \rightarrow Alerts \rightarrow SNMP \rightarrow SNMP Version.
- 2. Click Edit to enable the screen for editing.
- 3. In the community field, change the word public.
- 4. Click Save and click



NOTE: *This changes the community string for the Scanning Servers as well.*

1.1.4 User Access to the Scanning Servers

Vital Security provides the ability to configure a Users access list from the Management Console. The access list ensures that only authorized IP addresses are allowed to access the Scanning Servers.

0 To configure a Users Access List:

- 1. Navigate to Administration \rightarrow System Settings \rightarrow Finjan Devices \rightarrow <IP Address> \rightarrow Access List.
- 2. Click Edit to enable the screen for editing mode.
- 3. Select Use Access List.
- 4. In the Users Access List, click on the plus icon and in the row provided enter the relevant IP addresses.
- 5. Click **Save** and click



1.2 **Scanning Servers**

The procedure below shows how to harden the Scanning Servers by denying unauthorized access to them

1.2.1 Proxy IP Address

When the Scanning Server has multiple IP addresses (whether on a single network interface or multiple network interfaces) it is recommended to limit access to the Scanning Server via the interface that is being used by the end-users.

3

To limit access via a single IP address:

- 1. In the Management Console, navigate to Administration \rightarrow System Settings \rightarrow Finjan Devices \rightarrow <IP Address> \rightarrow Scanning Server \rightarrow HTTP \rightarrow Proxy IP and Port.
- 2. Click Edit to enable the screen for editing mode.
- 3. Select Enable HTTP for Device.
- 4. Enter the required IP in the Proxy IP Address field. The Scanning Server will not accept requests from any other IP address.
- 5. Click Save and click

NOTE: If the Scanning Server is also scanning HTTPS traffic, then add the required IP in the HTTPS - Proxy IP Address field.

1.2.2 Management Access List

Vital Security provides the ability to configure a Management access list from the Management Console. The access list ensures that only restricted IP addresses have access to the system for management. The Access list is not enabled by default since the administrator would not be able to access the system due to the fact that Administrator subnets are not known before the installation. Once the access list is enabled, all access from unknown IPs is disabled.

3 To configure a Management Access List:

- 1. In the Management Console, navigate to Administration \rightarrow System Settings \rightarrow Finjan Devices \rightarrow <IP Address> \rightarrow Access List.
- 2. Click Edit to enable the screen for editing mode.
- 3. Select Use Access List.
- 4. In the Management Access List, click on the plus icon and in the row provided enter the relevant IP addresses.



5. Click Save and click 🛛 🖄 .

1.3 Nortel Switches (Applicable only to NG-8000 Series)

Nortel Switch (both Layer 2-3 and Layer 2-7) has to be hardened as well in order to limit unauthorized access to it and also in order to secure the communication between the management station and the switch.

1.3.1 Defaults SNMP Community String

SNMP access to the Nortel switch can be addressed as follows:

- It can be completely disabled by issuing a "/cfg/sys/access/snmp disabled" command or set to read-only with "/cfg/sys/access/snmp read-only".
- The write community strings can be modified using "/cfg/sys/ssnmp/rcom" and "/cfg/sys/ ssnmp/wcomm".

NOTE: Configuring SNMPv3 on the Scanning Servers enables encrypted access and can more precisely limit the objects that may be accessed. However - if SNMPv3 is enabled, the System Dashhboard will not show the relevant information.

1.3.2 Telnet and HTTP Access to the Switch

Telnet and HTTP access to the switch should be disabled in order to prevent management via unsecured communication by enabling SSH access instead. Enabling SSH on the switch means that all switch management will be carried out through SSH and not via the Management module

1.3.3 Default User and password

The default user and password for the Nortel switch is 'admin'. It is highly recommended to

change the default password. In order to do so use the command /cfg/sys/access/user/ admpw

You will be prompted to enter the existing password (default "admin") once and the new password twice. Don't forget to apply and save your settings.