



## Vital Security™ NG-8100

### Secure Web Gateway for Large Enterprises

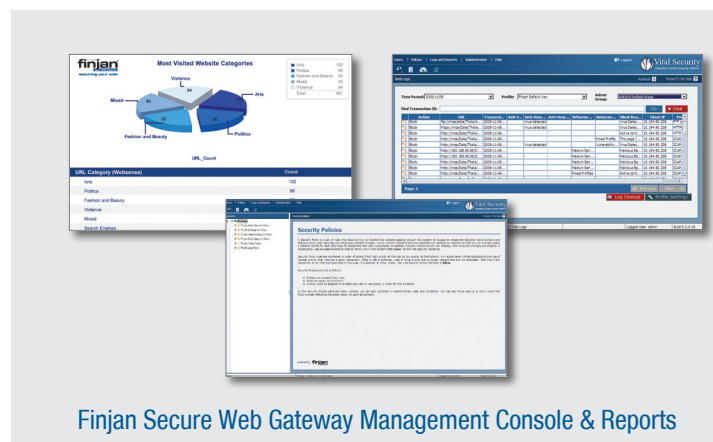
Finjan Secure Web Gateway provides organizations with a unified Web security solution that combines productivity, compliance, liability and bandwidth control as well as multi-layered web security against crimeware and Web 2.0 threats.

NG-8100 is Finjan's Secure Web Gateway for large enterprises recommended for deployments requiring high performance with maximum availability and reliability. This dedicated appliance, running on an IBM blade center platform, is easily managed using the single management console. Hardware, licensing, and power consumption cost reductions, coupled with lower solution and network administration costs, enable low Total Cost of Ownership (TCO).

Finjan Secure Web Gateway NG-8100 provides:

- **Web security** – Anti-malware and Anti-Crimeware via Finjan's patented active real-time content inspection technologies and optional Anti-Virus modules
- **Productivity, liability and bandwidth control** via URL filtering, content caching and applications control technologies
- **Data Leakage Prevention (DLP)** by inspecting outbound communications for sensitive/confidential data, even when hiding in HTTPS/SSL
- **Flexible central management** allows organizations to manage all their actions from the same Web-based console (including monitoring and controlling HTTP, FTP and SSL traffic)
- **Powerful logging and reporting** capabilities, that provide enterprises with clear visibility into the entire organization's Web traffic

NG-8100 utilizes Finjan's patented active real-time content inspection technology that proactively prevents malicious content and data leakage over HTTP/HTTPS/FTP. Its central management and customizable dashboards simplify the administration, control and monitoring of one or more appliances operating in production. Its powerful management capabilities include master policy setting for easier administration.



Finjan Secure Web Gateway Management Console & Reports

NG-8100 is easy to deploy and smoothly integrates into various network topologies and monitoring systems. Interoperability with existing network components and monitoring systems is maintained through the support of Cisco WCCPv2, ICAP, Syslog and SNMP v.3

### Features and Benefits

- Unified Web security solution on a single chassis
- Web security (anti-malware and protection against Web 2.0 threats) in real time
- Patented active real-time content inspection of all HTTP/SSL content
- Intentional and unintentional Data Leakage Prevention (DLP)
- Increased employees' productivity and Web 2.0 control
- Reduction of administration overhead and single point of provisioning via centralized management
- HTTPS/SSL inspection prevents crimeware hiding in SSL traffic; unencrypted traffic does not leave the appliance, therefore reducing eavesdropping risks
- Ensured high availability based on redundant, hot-swappable hardware components
- Low total cost of ownership (TCO) is achieved by utilizing a single chassis that centrally manages all security features, floor space savings of up to 50%, by lower power consumption and hardware-related costs
- Assistance with regulatory compliance such as HIPAA, SOX (COBIT) DS5, PCI DSS 1.1., GLB Act, FISMA, etc.

### Turn Active with Finjan Secure Web Gateway NG-8100

- ✓ URL filtering
- ✓ Anti-Virus
- ✓ Content Caching
- ✓ Web 2.0 Security
- ✓ SSL Inspection
- ✓ Application Control
- ✓ Anti-Malware
- ✓ Data Leakage Prevention
- ✓ Zero-hour Protection



# Vital Security™ NG-8100 Main Features

## Security

- Multi-layered web security solution:
  - Integrates Finjan's patented active real-time content inspection technology to prevent crimeware and malware proactively
  - Zero-hour protection (Finjan Vulnerability Anti.dote™), Anti-Spyware and SSL inspection engines
  - Choice of fully integrated Anti-Virus and URL-filtering engines
- Integrated Data Leakage Prevention (DLP) including inspection of HTTP/HTTPS communication and deep analysis of various content types, such as detection of "Trojans phoning home"
- Digital Certificates Validation – verifying that digitally signed code holds valid certificates
- Web 2.0 security and control:
  - Secure inbound and outbound Web 2.0 content traffic to prevent malware and data leakage
  - Enables organizations to control the use of Web 2.0 applications such as Facebook, MySpace or others
- Application control - flexible setting of rules by application type including instant messaging, Skype, and P2P
- Inspected protocols: HTTP, HTTPS, FTP, and FTP over HTTP

## High Performance and Availability

- Secure content caching for accelerated content delivery and enhanced productivity
- Robust Quad-Core server platform for enterprise-grade throughput performance
- Active/Standby Policy Server option

## Manageability

- Centralized management and customized dashboards for simple administration, control and monitoring of Finjan Secure Web Gateway appliances
- Powerful task-based management and granular policy settings
- Policy settings wizard to easily setup and manage security policies with single-click rules refinement
- Reporting and logging provide clear visibility into the entire organization's Web traffic
- Powerful logging and tracking of web security violations, system events and audit trail
- Multi-role management enables multiple administration groups to manage and monitor the system with different authorities
- Master policy enables policy inherency for easier administration
- SNMP support provides "just-in-time" alerts of relevant operational events using SNMP traps, as well as email alerts
- Support of transparent proxy mode
- User authentication/identification is based on Microsoft Active Directory® or other LDAP servers, without the need for any additional software
- Secure LDAP ensures that authentication credentials are transferred securely from the directory server to the appliance
- Supports RADIUS authentication for administrators
- Customizable reports enabling the organization to evaluate productivity, compliance and security using drill-down reports and dashboards are generated by Finjan's Vital Security™ Reporter
- Support of Cisco WCCPv2, ICAP, Syslog and SNMP v3 standards ensures interoperability with various network topologies and caching systems

## Hardware Performance Specifications NG-8100 (per blade)

CPU	2 x Intel Xeon Quad-Core E5506 2.13GHz
Hard Disk	Up to 2x146GB SAS
Memory	4GB DDR3
Gigabit Ethernet NIC	Up to 4

## Caching kit (optional extension to the NG-8100)

Hard disk	73GB SAS
-----------	----------

## IBM eServer® BladeCenter™ Chassis

Max. number of blades	14 hot swappable blade servers
Rack space (7U)	44.4 x 71.1 x 30.4 cm (WxDxH) 17.5 x 28 x 12 inches (WxDxH)
Redundancy	Hot swappable blowers and power supplies
Number of users per deployment	Up to 60,000 per chassis

NG-8100 is an environmental-friendly appliance due to its power consumption savings of up to 35% compared to other rack servers. As all Finjan Secure Web Gateways, NG-8100 also complies with the EU RoHS Directive



In order to provide our customers with a complete best-of-breed content security solution, Finjan teams up with leading AV and URL filtering providers to deliver comprehensive and integrated proactive content security solutions for organizations and enterprises.



### For Additional Information

please visit [www.finjan.com](http://www.finjan.com) or contact our regional offices:

#### US & Canada

Toll Free: 1 888 FINJAN 8 (1 888 346 5268)  
Tel: +1 408 452 9700  
Email: [salesna@finjan.com](mailto:salesna@finjan.com)

#### Mediterranean/APAC & India

Tel: +972 (0)9 864 8200  
Email: [salesis@finjan.com](mailto:salesis@finjan.com)

#### Central & Eastern Europe

Tel: +49 (0)89 673 5970  
Email: [salesce@finjan.com](mailto:salesce@finjan.com)

#### UK & Ireland

Tel: +44 (0)1252 511118  
Email: [salesuk@finjan.com](mailto:salesuk@finjan.com)

#### Benelux & Nordic

Tel: +31 (0)33 454 3555  
Email: [salesne@finjan.com](mailto:salesne@finjan.com)

© Copyright 1996 - 2009. Finjan Inc. and its affiliates and subsidiaries. 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, 6904780, 6922693, 6944822, 6993662, 6965968, 7058822, 7076469, 7155743, 7155744, 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, RUSafe and SecureBrowsing are trademarks or registered trademarks of Finjan Inc., and/or its affiliates and subsidiaries. Sophos is a registered trademark of Sophos plc. McAfee is a registered trademark of McAfee Inc. IBM Proventia Web Filter technology is a registered trademark of IBM Internet Security Systems. Kaspersky is a registered trademark of Kaspersky Lab. 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. Q3 2009.