



Field	Definition
Author	Tal Surasky
TW	Sari Klaff
Audience	
Type of doc	Technical Brief
Content Provider	Tal Surasky
Review Group	
Draft Number	
History	
Final Approval by <VP of PM> Date:	
Final Approval by Doc Manager Date:	

**Copyright**

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

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

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

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

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

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

Catalog Name: Integrated Caching version 9.2

## Table of Contents

<b>1.</b>	<b>Introduction</b>	<b>1</b>
<b>2.</b>	<b>HTTP Caching Policies</b>	<b>1</b>
<b>3.</b>	<b>HTTP Caching and Security</b>	<b>1</b>
<b>4.</b>	<b>Upgrades for Existing Vital Security Systems and Cache License</b>	<b>2</b>
<b>5.</b>	<b>Setup and Configuration</b>	<b>3</b>
5.1	Global Configuration	3
5.2	Setting Caching Policy	4
5.3	Flushing the Cache	6

## 1. Introduction

HTTP is one of the most popular communication protocols on the internet. It is used both for browsing the web and running various applications such as web mail and CRM. Using an HTTP caching element in Vital Security system ensures that content delivery to end-users is accelerated. When content is delivered from a local cache after download, there is no need to download identical content for each user's subsequent request; therefore the end-user's response time is reduced. Furthermore, it also reduces the bandwidth used to download multiple copies of the same object. Freeing bandwidth allows the mission critical applications of the organization to run more efficiently.



**NOTE: Due to privacy issues, HTTPS content is not cached. This avoids situations where the secured content of one user is displayed to another user.**

---

## 2. HTTP Caching Policies

As with many other components in Vital Security, system administrators configure the policies by which Vital Security caches HTTP content.

Caching policies consist of both an Action and a Condition.

- ◆ **Action:** The administrator can set the Action to bypass caching according to specific URL or file extension lists, ensuring that specific, non-cacheable URLs or specific file extensions are not cached. System administrators can also cache only specific sites or file extensions.
- ◆ **Condition:** Once an action is set, the administrator can select the criteria to which the rule will or will not match. The condition can be a specific URL list, multiple URL lists, or all lists excluding selected URL lists. Administrators can also select file extensions that Vital Security caches or bypasses.

The Caching policy is a global policy that applies to all users who browse using the system. By default, when caching is enabled, all content is cached. The default policy also contains a rule with two conditions:

- Cache based on URL list
- Cache based on file extension lists

## 3. HTTP Caching and Security

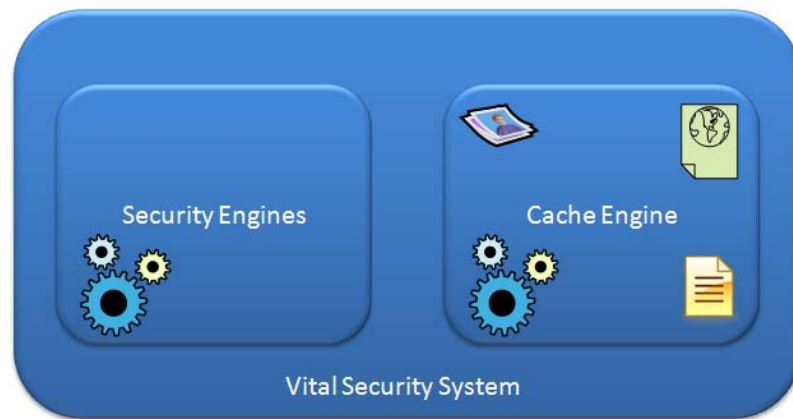
When HTTP Caching is enabled, the cached content is scanned according to the selected security policies, before it is delivered to the end-user. This

ensures a higher level of security given that a newer security update may identify a security threat for a file already in the cache.

Consider the following situation:

- End-user A accesses Website X and downloads the homepage (which includes Java script).
- The Java script is stored in the cache. Security engines scan the Java script for security validations.
- If the script is found to be acceptable, it will be sent to end-user A.

In this same scenario, a newer security update may detect a security validation in the Java script that the previous security update did not identify. By re-scanning the content saved in the cache, Vital Security ensures that all content accessed by the end user is both safe and secure.



**Illustration 1 - Security and Cache Engines**

Vital Security employs another mechanism, which enables it to enhance performance and efficiency. After the content has been scanned by the security engines, the scan results are saved and future requests for the same file are compared with the original scan results. This eliminates the need to re-scan the same file repeatedly. Once a new security update is available, Vital Security flushes its cache and re-scans the content based on the aforementioned process.

#### 4. Upgrades for Existing Vital Security Systems and Cache License

Secured Caching is supported by the NG-6000 and NG-8000 series only and requires special hardware that includes additional memory and hard disks, according to the following specifications:

Appliance	Configuration Without Caching	Configuration With Caching
NG-6000	2GB RAM 2x73GB HDD	4GB RAM 4x73 GB HDD
NG-8000	2GB RAM 1x73GB HDD	4GB RAM 2x73 GB HDD

Existing customers may upgrade their hardware so that Vital Security can run Secured Caching. The upgrade kit includes additional memory and hard disks, as well as a caching license, which enables the activation of the Secured Caching feature.

In cases where not all of the appliances have been upgraded to support Integrated Caching and the hardware configuration is mixed, caching will work on all the appliances; however, caching will work with limited capabilities on hardware without additional memory and disks.



**NOTE: After installing a Caching Kit, is it mandatory to re-install the Vital Security system. For systems shipped with a Caching Kit, this is not required.**

## 5. Setup and Configuration

Configuring Secured Caching consists of two steps:

- Enabling caching and setting up the global parameters
- Setting the caching policy

### 5.1 Global Configuration

The global configuration of Secured Caching, is performed via **Administration → System Settings → Finjan Devices → Caching**

Enable Caching

Caching Policy:

Max Obj size:  bytes

**Figure 1: Secured Caching Configuration**

After Caching is enabled, the system administrator can configure the following parameters:

- ◆ **Caching Policy:** The Caching Policy can be configured under **Policies → Caching**. The caching policy is a global policy that affects all users who are browsing using the Vital Security system. By default, when the system license includes caching, Caching is enabled and Vital Security caches all cacheable HTTP content.
- ◆ **Maximum Object Size:** HTTP caching is performed for HTTP objects, such as images, scripts, static HTML pages, and so on. The system administrators can set the maximum size of a single object that Vital Security caches.
- ◆ **Export Cache Logs:** When Export Cache Logs is enabled, the log files are saved in W3C format and exported to the same repository as the rest of the system logs. Using Vital Security Reporter, administrators can generate relevant reports for caching. When this option is disabled, logs are not saved.



**NOTE: In case the Vital Security is configured to send traffic to an upstream proxy and the upstream proxy requires NTLM authentication, caching is not supported.**

## 5.2 Setting Caching Policy

Although multiple Caching Policies can be configured, only a single policy can be activated at any single time per Scanning Server, and this policy will be global to all users who are browsing using Vital Security. If there is a need to allow (or disallow) certain users to access particular Websites or to download certain file types, it will be enforced by the Security Policies.

A Caching Policy consists of the following building blocks:

- ◆ **Policy Name:** a descriptive name for the Policy

The screenshot shows a web form for creating a new caching policy. It has two main input fields: 'Policy Name' with the value 'New Caching Policy' and 'Description' with the value 'New Caching Policy Description'. At the bottom right, there are three buttons: 'Edit' (with a pencil icon), 'Save' (with a checkmark icon), and 'Cancel' (with an 'X' icon). The Finjan logo and 'powered by' text are visible in the bottom left corner.

Figure 2: Caching Policy

- ◆ **Rule:** A Caching Policy may contain a single rule or multiple rules. The rules are evaluated according to their order. If there is no match between any of the rules and the traffic, the default action is to cache the traffic. A rule can either be configured to cache the content or to bypass caching.

The screenshot shows a web form for configuring a rule. It includes a 'Rule Name' field with the value 'Bypass caching for on-line banking' and a 'Description' field with the text 'This Rule bypasses caching for certain web sites.'. Below these is a section for 'Enable Rule' which is checked. Underneath, there is an 'Action' dropdown menu currently set to 'Bypass Cache'. At the bottom right, there are three buttons: 'Edit' (grey), 'Save' (green), and 'Cancel' (red). The Finjan logo and 'powered by' text are in the bottom left corner.

Figure 3: Rule Configuration

- ◆ **Condition:** The condition is the actual parameter by which the rules are matched. System administrators can cache content (or bypass caching) according to URL lists or file extension lists. A rule with two conditions will be evaluated with both conditions, where a logical AND combines the two conditions.

Condition Name:

Applies to:

Any of the items selected below  
 Everything except for the items selected below

Select/Deselect all

<input type="checkbox"/>	URL Bypass List (Medium)
<input type="checkbox"/>	URL Bypass List (Strict)
<input checked="" type="checkbox"/>	URL Cache Bypass List
<input type="checkbox"/>	URL White List (Basic)
<input type="checkbox"/>	URL White List (Medium)
<input type="checkbox"/>	URL White List (Strict)

powered by **finjan**

Figure 4: Condition Configuration

### 5.3 Flushing the Cache

Cache Flushing allows system administrators to delete all content from the cache. This operation should not be part of the day-to-day maintenance, as this operation terminates all existing connections. Flushing the cache is available via the Limited Shell using the following command: `flush_webcache` or via the Management Console.

Filename: Integrated Caching.docx  
Directory: C:\Documents and Settings\sklaff\My Documents  
Template: C:\Documents and Settings\sklaff\Application  
Data\Microsoft\Templates\FinjanTemplateMay2008.dot  
Title: Integrated Caching  
Subject: Technical Brief  
Author: sklaff  
Keywords:  
Comments:  
Creation Date: 8/9/2008 8:20:00 AM  
Change Number: 17  
Last Saved On: 18/11/2008 2:42:00 PM  
Last Saved By: sklaff  
Total Editing Time: 313 Minutes  
Last Printed On: 3/3/2009 10:11:00 AM  
As of Last Complete Printing  
Number of Pages: 10  
Number of Words: 1,735 (approx.)  
Number of Characters: 9,892 (approx.)