finjan®

Vital Security™

securing your web

WCCP

Vital Security 9.2

Copyright

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

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

Catalog name: TB – WCCP 9.2

Table of Contents

1. Introduction 1

2. WCCP Operation 2

2.1 Multiple Routers Support 2

2.2 WCCP Redirection 2

2.3 WCCP and Authentication 3

3. High Availability with WCCP 3

4. Scalability and Load Balancing with WCCP 3

4.1 Hash Assignment 3

4.2 Mask Assignment 4

5. Supported Topologies 4

5.1 Single Router with a single Scanning Server 5

5.2 Single Router with multiple Scanning Servers 5

5.3 Multiple Routers with multiple Scanning Servers 6

5.4 WCCP and Authentication 7

6. Configuration 7

6.1 Scanning Server Configuration 7

6.2 Router Configuration 8

1. Introduction

Web Cache Communication Protocol (WCCP) is a protocol designed and developed by Cisco systems©. Its main purpose is to transparently redirect users to cache servers, without them having to configure proxy settings in their browsers. In Software Release 9.0, Vital Security supports WCCP version 2 and allows WCCP enabled routers and switches to redirect web traffic to the Scanning Servers.

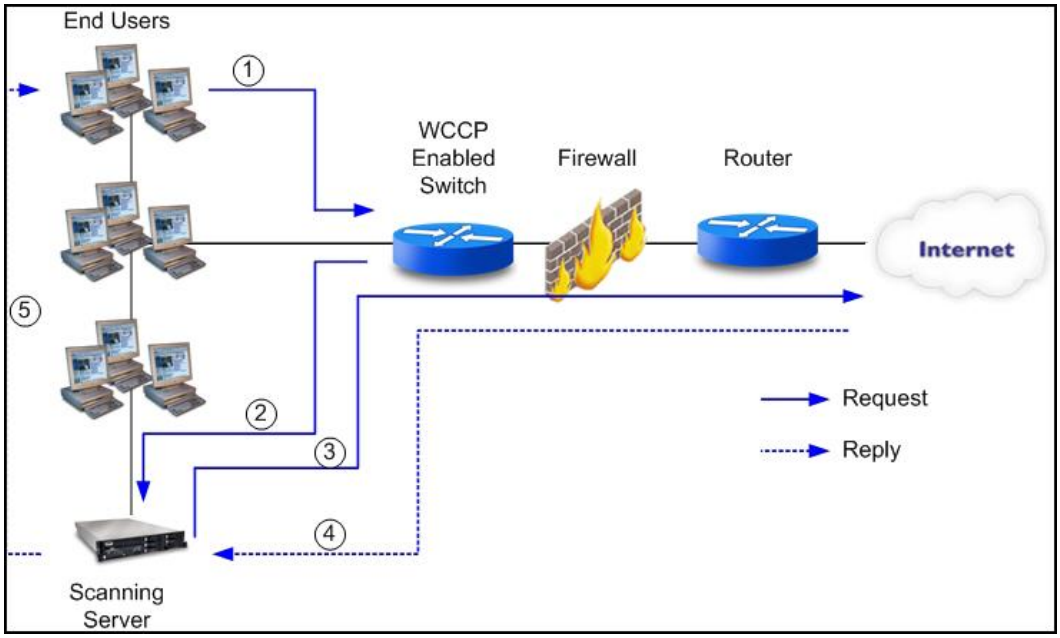

Figure 1: WCCP Enabled Switch

In addition to enabling transparent redirection, WCCP also includes features which enable high availability and scalability:

- **High Availability with WCCP:** in case of Scanning Server failure, the router stops redirecting traffic to the failed Scanning Server, and traffic is either blocked or sent directly to the Internet.
- **Scalability and Load Balancing with WCCP:** WCCP has built-in load sharing capabilities and a WCCP enabled router can distribute traffic among multiple Scanning Servers. With WCCP, it is very simple to add more Scanning Servers. Once a new Scanning Server is added, the WCCP protocol automatically changes the IP assignment.

NOTE: The phrase WCCP enabled router also refers to a WCCP enabled switch.

For more information about WCCP and supported IOS and Routers / Switches, please refer to the Cisco Feature Navigator.

2. WCCP Operation

When WCCP is enabled on a Scanning Server, the Scanning Server periodically sends “Here I am” messages to the WCCP enabled router. As a response, the WCCP enabled router replies with “I see you” messages. These two WCCP messages allow the WCCP enabled router to distinguish between the Scanning Servers in the topology. When the WCCP enabled router has “seen” all the Scanning Servers in the topology, it provides all the Scanning Servers with the IP addresses of all the other Scanning Servers present in the topology, such that all Scanning Servers are aware of each other. The WCCP enabled router assigns the Scanning Server with the lowest IP address as the designated Scanning Server. The designated Scanning Server informs the router how to distribute the traffic among all the Scanning Servers and which protocol it supports. Vital Security uses the following service numbers:

1 for HTTP; 2 for HTTPS and 3 for FTP

2.1 Multiple Routers Support

WCCP version 2 supports multiple routers for each Scanning Server. Such a deployment allows multiple routers to use the same Scanning Server. The Scanning Server will reply to the router, which in turn redirects the traffic.

NOTE: Vital Security does not support multicasting with WCCP

2.2 WCCP Redirection

A WCCP enabled router can redirect the traffic to the Scanning Server in one of two ways:

- Generic Router Encapsulation (GRE) protocol - When the Scanning Server is not directly connected to the router or the Scanning Server and the router are on different IP networks, GRE must be used.
- Layer 2 redirect - When a WCCP enabled switch is in use and the Scanning Server is connected directly to the switch, it is more efficient to use Layer 2 forwarding, such that the switch simply re-writes the destination MAC address to the MAC address of the Scanning Server. In terms of performance, Layer 2 forwarding is preferred over GRE.

NOTE: Layer 2 is preferable over GRE redirection since there is no need to encapsulate the packet – an operation which may cause IP fragmentation.

2.3 WCCP and Authentication

WCCP version 2 allows the WCCP enabled router and the Scanning Server to have a shared password. Both the Scanning Servers and the WCCP enabled router must have the same password in order to be able to communicate with each other. Having a password means that unauthorized WCCP servers will not be able to participate in the topology.

3. High Availability with WCCP

WCCP allows for automatic discovery of failed Scanning Servers. The Scanning Servers send “Here I am” message every 10 seconds. Once the Scanning Server stops sending “Here I am” messages, the WCCP enabled Router will wait 30 seconds before it considers the Scanning Server as unavailable, in which case the rest of the available Scanning Servers will then handle the traffic originally handled by the failed Scanning Server. When the failed Scanning Server becomes available once again, it sends a “Here I am” message to the router. The router updates the designated Scanning Server, which in turn updates the load distribution algorithm on the Router.

NOTE: It is possible to configure the router to block all the traffic if there is no available Scanning Server at all, or send the traffic to the Internet unscanned.

4. Scalability and Load Balancing with WCCP

When a single Scanning Server cannot handle the entire load, additional Scanning Servers can easily be added, without the need to change the topology or the configuration of the Scanning Servers. When WCCP is enabled, it simply connects the additional Scanning Servers to the Router. Once the additional Scanning Servers are added, each Scanning Server sends “Here I am” message and the router updates the designated Scanning Server, which in turn updates the router on how to distribute the traffic.

WCCP supports two methods for traffic distribution between the WCCP enabled Router and the Scanning Server:

4.1 Hash Assignment

When Hash Assignment is in use, the WCCP enabled router performs a hash function on the IP address. The result of the hash function can be a value of 0-255. The Routers hold a hash table, which maps the result of

the hash function to one of the Scanning Server. For example, if there are four Scanning Servers, the table will look as follows:

Hash Result	Server
0-63	Scanning Server 1
64-127	Scanning Server 2
128-191	Scanning Server 3
192-255	Scanning Server 4

In case one (or more) Scanning Server fails or a new server is added, the WCCP enabled router recalculates the hash table.

4.2 Mask Assignment

Mask Assignment, if supported by the WCCP enabled router, performs a bitwise logical AND operation between each mask value and the content of the packet. After this operation, the WCCP enabled router compares a list of values for each mask. Like the Hash assignment, also with this method, the WCCP enabled router compares the result with a list of values. Based on this list, the WCCP enabled router selects the Scanning Server.

NOTE: When possible, it is recommended to use a combination of Layer 2 redirection with Mask assignment for best performance.

5. Supported Topologies

The introduction of WCCP allows the Vital Security system to support more topologies.

The following topologies are supported with WCCP:

- Single Router with a single Scanning Server
- Single Router with multiple Scanning Servers
- Multiple Routers with multiple Scanning Servers
- WCCP and Authentication

Traffic Flow: As previously mentioned, with WCCP there is no need to configure the end user's browser settings since the redirection is performed by the WCCP enabled router. The end user sends the request to the original server and the WCCP enabled router intercepts the request and redirects it to one of the Scanning Servers. The Scanning Server then scans the traffic and creates a new request (using the Scanning Server IP address as the source IP) and sends it to the original server.

NOTE: A request which arrives from one of the Scanning Servers is not intercepted by the WCCP enabled router.

5.1 Single Router with a single Scanning Server

This topology is the basic WCCP topology. All web traffic is redirected to a single Scanning Server. Based on the router's configuration, traffic will be sent directly to the Internet if the Scanning Server fails.

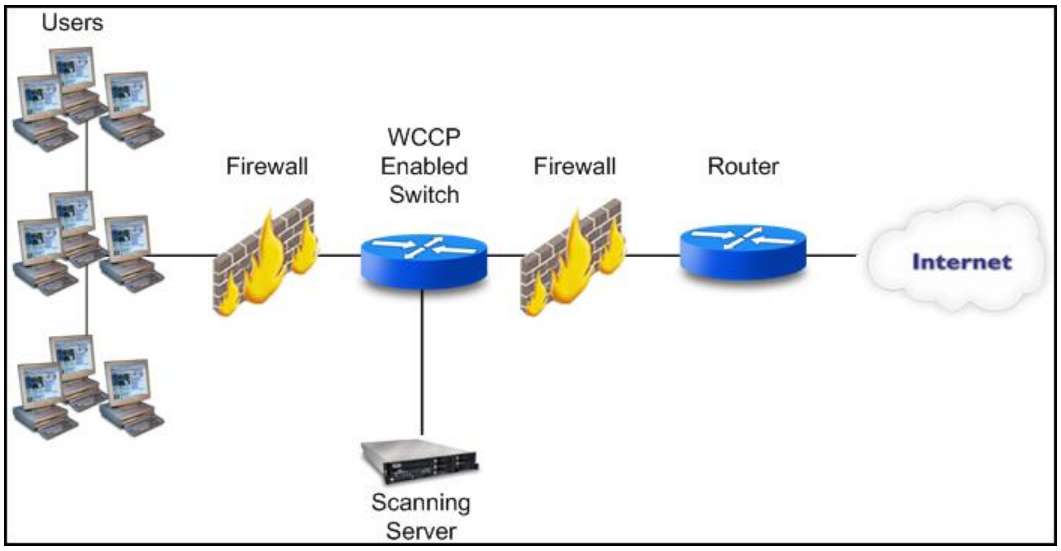

Figure 2: Single Router & Single Scanning Server

5.2 Single Router with multiple Scanning Servers

In this topology, multiple Scanning Servers are connected to a single router and the router load balances traffic (equally) among all the Scanning Servers. Failure in a single Scanning Server does not affect the network since the other Scanning Servers take over and handle the traffic.

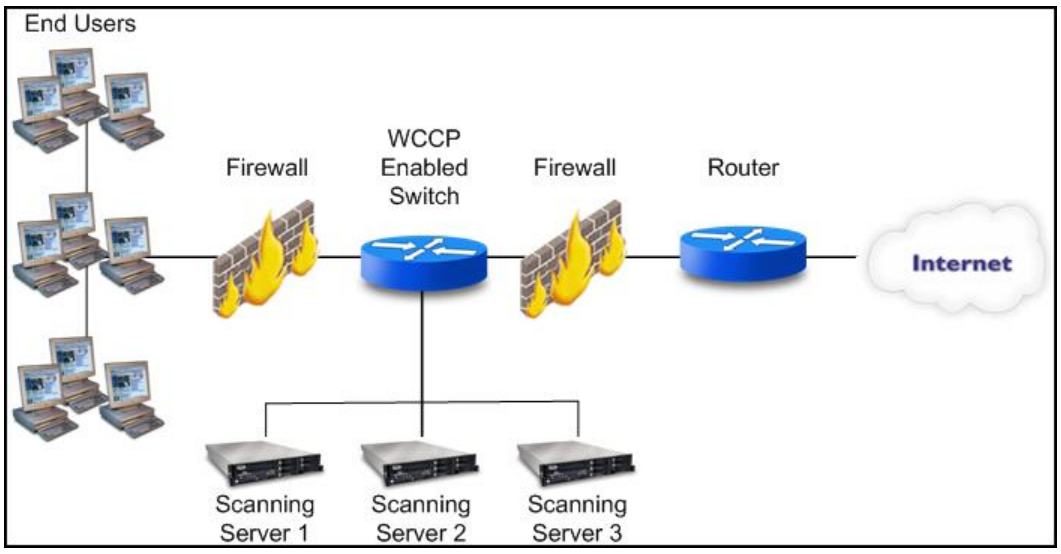

Figure 3: Single Router & Multiple Scanning Servers

In load balancing scenario,

5.3 Multiple Routers with multiple Scanning Servers

In this topology, multiple routers (or switches) are connected to multiple Scanning Servers. Each Scanning Server receives traffic from multiple routers.

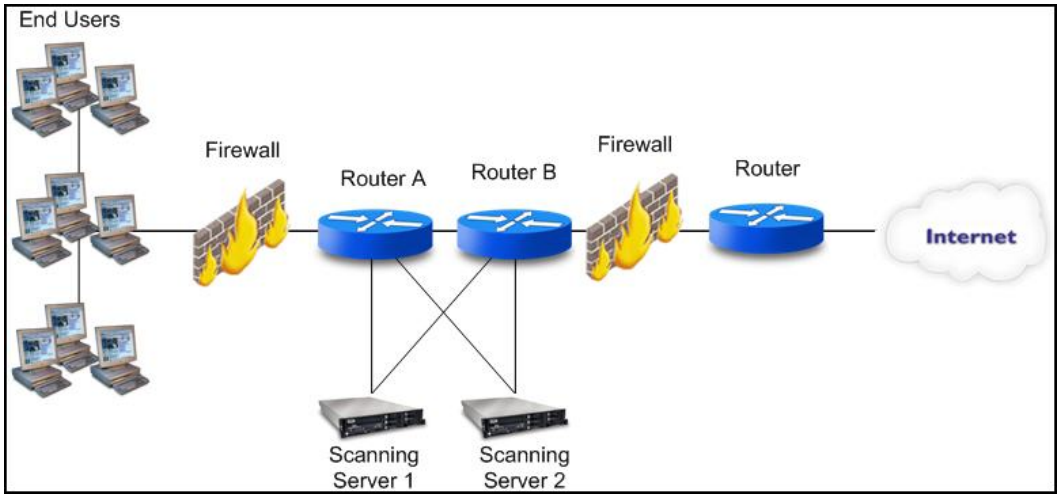

Figure 4: Multiple Routers & Multiple Scanning Servers

5.4 WCCP and Authentication

In this topology traffic intercepted by the WCCP enabled router is redirected to the Scanning Server, which in turn redirects the user to the Authentication device. After the authentication process is completed, the Scanning Server provides the information to the authenticated user.

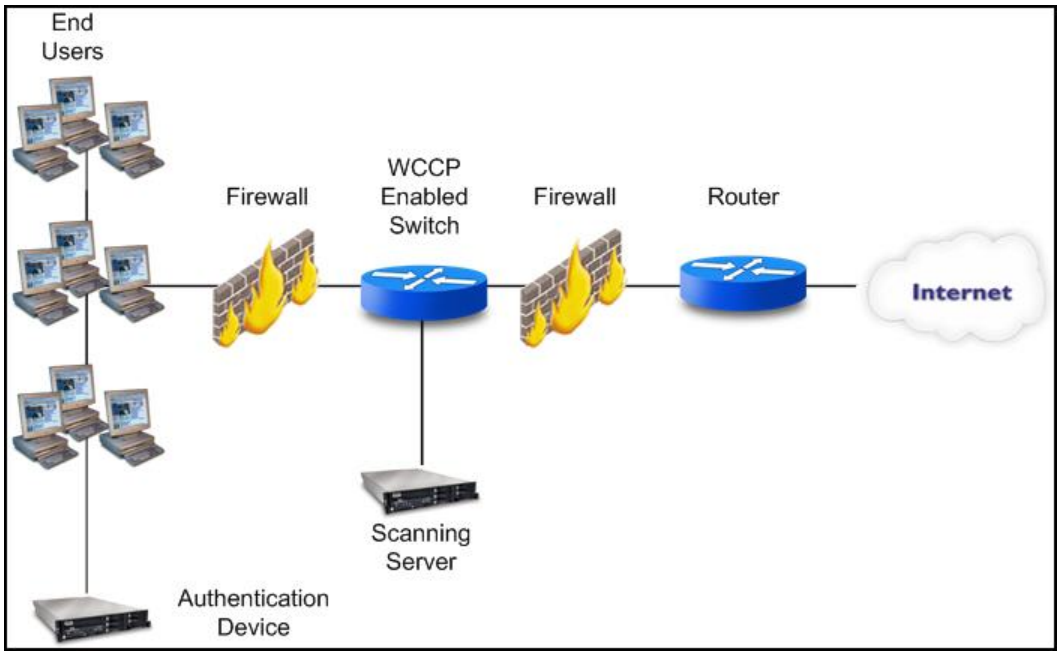

Figure 5: WCCP & Authentication Device

6. Configuration

Configuration of the WCCP requires configuration of the Scanning Servers as well as configuring the WCCP enabled router.

6.1 Scanning Server Configuration

Transparency must be enabled prior to WCCP configuration on the Scanning Server.

⇨ **To enable transparency:**

1. Navigate to **Administration→ System Settings → Finjan Devices**.
2. Click on Scanning Server node in the Devices tree to expand it and then select **General**.
3. Select the **Transparent Proxy Mode** tab on the right hand pane.

4. Click **Edit** and select **Enable Transparent Proxy Mode**. Make sure there are ports defined for each of the sections.
5. Click **Save** and click  .
6. To enable redirect of FTP traffic, select **FTP** option under Scanning Server in the Devices tree.
7. Click **Edit** on right hand pane and select **Enable FTP for Device**.

NOTE: Passive FTP is not supported because the WCCP router does not do layer 7 inspection, nor does it track FTP port changes.

8. Select the **WCCP** option under Scanning Server in the Devices tree.
9. Click **Edit** on right hand pane and select **Enable WCCP V2.**
10. Select the Forwarding method and enter the shared password (if configured on the router).
11. Enter the IP address of the router. If multiple routers exist, click  and enter additional router IP address. Repeat if necessary.
12. Click **Save** and click  .

NOTE: When working with WCCP, up to 8 different TCP ports can be used for each service.

6.2 Router Configuration

To configure Cisco routers and switches, please refer to Configuring Web Cache Services Using WCCP.

Disclaimer

Although WCCP was tested using different Cisco routers and switches, there might be cases where interoperability issues occur. CISCO offers different implementations of the WCCP feature with their routers and switches and Finjan highly recommends testing the future topology in a lab environment before implementing it into production.

Please contact your Finjan representative for more information