WCCP on ASA: Concepts, Limitations, and Configuration

Document ID: 116046

Contributed by Sourav Kakkar, Cisco TAC Engineer.
May 31, 2013

Contents

Introduction
Prerequisites
- Requirements
- Components Used
- Conventions

WCCP and ASA Overview
WCCP Redirection
WCCP Service Groups
Configure
Verify
Troubleshoot
Related Information

Introduction

This document describes concepts, limitations, and configuration of the Web Cache Coordination Protocol (WCCP) on a Cisco Adaptive Security Appliance (ASA). WCCP is a method by which the ASA can redirect traffic to a WCCP caching engine through a generic routing encapsulation (GRE) tunnel.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Web Cache Communications Protocol (WCCP) version 2 (v2)
- Cisco Adaptive Security Appliances (ASA)
- Cisco Adaptive Security Appliance (ASA) Software; read Configuration Guides for compatibility
- Proxy caching
- Redirection

Cisco also recommends that you understand the limitations of WCCP configuration on the ASA, as explained in these documents:

- Cisco ASA 5500 Series Configuration Guide using the CLI, 8.2: Configuring Web Cache Services Using WCCP: Guidelines and Limitations
- Cisco ASA Series CLI Configuration Guide, 9.0: Configuring Web Cache Services Using WCCP

Components Used

The information in this document is based on the Web Cache Communications Protocol (WCCP) version 2 (V2).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for information on document conventions.

WCCP and ASA Overview

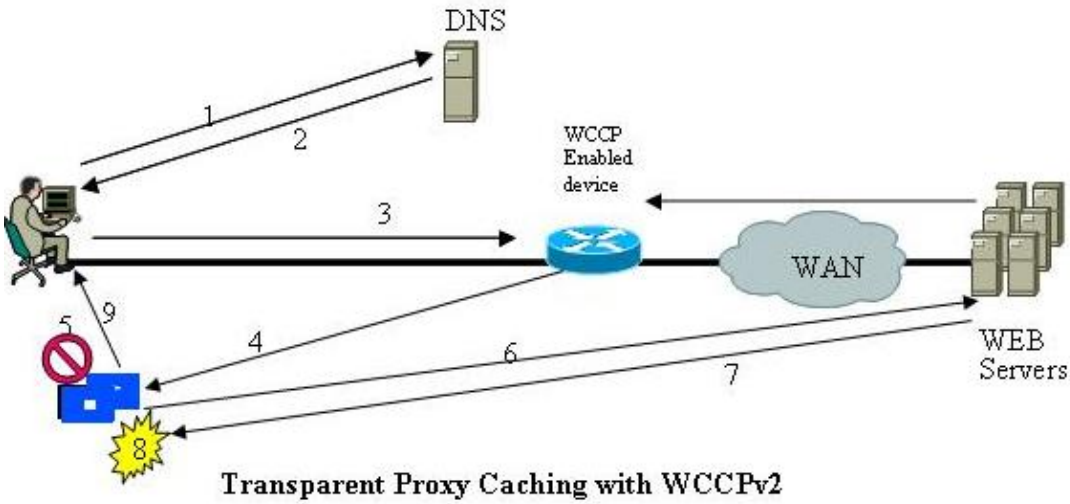
The WCCP specifies interactions between one or more routers and one or more web caches. The purpose of the interaction is to establish and maintain the transparent redirection of selected types of traffic that flow through a group of routers. The selected traffic is redirected to a group of web caches in order to optimize resource usage and lower response times.

For WCCP, the ASA chooses the highest IP address configured on an interface and uses that as the router ID. This is exactly the same process that Open Shortest Path First (OSPF) follows for the router ID. When the ASA redirects packets to the cache engine (CE), the ASA sources the redirect from the router ID IP address (even if it is sourced out a different interface) and encapsulates the packet in a GRE header.

The GRE connection is unidirectional. The ASA encapsulates redirected packets in GRE and sends it to the caching engine. The ASA does not process any GRE−encapsulated responses from the CE. The CE needs to communicate directly to the inside host.

The flow of work for redirection has these steps:

1. The host uses the default gateway of the ASA in order to open the HTTP connection.
2. The ASA redirects the packet (encapsulated in GRE) to the CE.
3. The CE verifies or updates the cache for the requested site.
4. The CE replies directly to the host.
    - ♦ All outbound packets from the host are redirected from the ASA to the CE.
    - ♦ All inbound packets from the server to the host are directed from the CE to the host.



Transparent Proxy Caching with WCCPv2

The ASA implements WCCP V2. If the server supports WCCP V2, it should be compatible.

WCCP Redirection

WCCP V2 defines mechanisms that allow one or more routers enabled for transparent redirection to discover, verify, and advertise connectivity to one or more web caches. These are the steps in WCCP redirection:

1. The user enters a URL into a browser.
2. The URL is forwarded to Domain Name System (DNS) for address resolution.
3. The URL is resolved to the IP address of the web server.
4. The client initiates a connection to the server with a SYN request.
5. On the active router, the WCCP web cache service intercepts the HTTP request (TCP port 80) and redirects the request to caches based on the configured load distribution:
    - ♦ If there is a cache hit, the CE responds to the original GET with the requested content and uses the source IP address of the origin server in the response pack.
    - ♦ If the requested content is not already stored on the CE, there is a cache miss:
        1. The CE establishes a connection to the origin server, uses its own IP address as the source, and sends the HTTP GET.
        2. The server responds to CE with content.
        3. The CE writes a copy of the cacheable content to the disk.

WCCP Service Groups

Once connectivity is established, the routers and web caches form service groups in order to handle the redirection of traffic whose characteristics are part of the service group definition.

A web cache transmits a WCCP2_HERE_I_AM message to each router in the group at HERE_I_AM_T (10) second intervals in order to join and maintain its membership in a service group. The message may be by unicast to each router or by multicast to the configured service group multicast address.

- The Web−Cache Identity Info component in the WCCP2_HERE_I_AM message identifies the web cache by IP address.

- The Service Info component of the WCCP2_HERE_I_AM message identifies and describes the service group in which the web cache wishes to participate.

Service Group	***Type***	***Description***
Service 0	Web−cache	Web caching service that permits the ASA to redirect HTTP traffic to the CE.
Service 53	DNS	DNS caching service that permits the ASA to redirect DNS client requests transparently to the client engine.
Service 60	FTP−native	Caching service that permits the ASA to redirect FTP native requests transparently to a single port on the content engine.
Service 70	https−cache	Caching service that permits the ASA to intercept port 443 TCP traffic and redirect this HTTPS traffic to the content engine.
Service 80	rtsp	Media streaming service that permits the ASA to redirect Real Time Streaming Protocol (RTSP) client requests to a single port on the content engine.
Service 81	mmst	Media caching service that permits the ASA to use TCP−based Microsoft Media Server (MMST) redirection in order to route Windows Media Technology (WMT) client requests to TCP port 1755 on the content engine.
Service 82	mmsu	Media caching service that permits the ASA to use User Datagram Protocol (UDP)−based Microsoft Media Server (MMSU) redirection in order to route WMT client requests to UDP port 1755 on the content engine.
Service 83	wmt−rtsp	Media streaming service that allows the ASA to redirect RTSP requests from Windows Media Service 9 clients to UDP port 5005 on the the CE.
Service 90−97	user configurable	User−defined WCCP services that support up to eight ports for each WCCP service. When you configure these user−defined services, you must specify whether to redirect the traffic to the HTTP caching application, to the HTTPS application, or to the streaming application on the content engine.
Service 98	custom−web−cache	Caching service that permits the ASA to transparently redirect HTTP traffic to the content engine on multiple ports other than port 80.
Service 99	reverse−proxy	Caching service that permits the ASA to redirect HTTP reverse proxy traffic to the content engine on port 80.

A service group is identified by Service Type and Service ID. There are two types of service groups:

- Well−known services
- Dynamic services

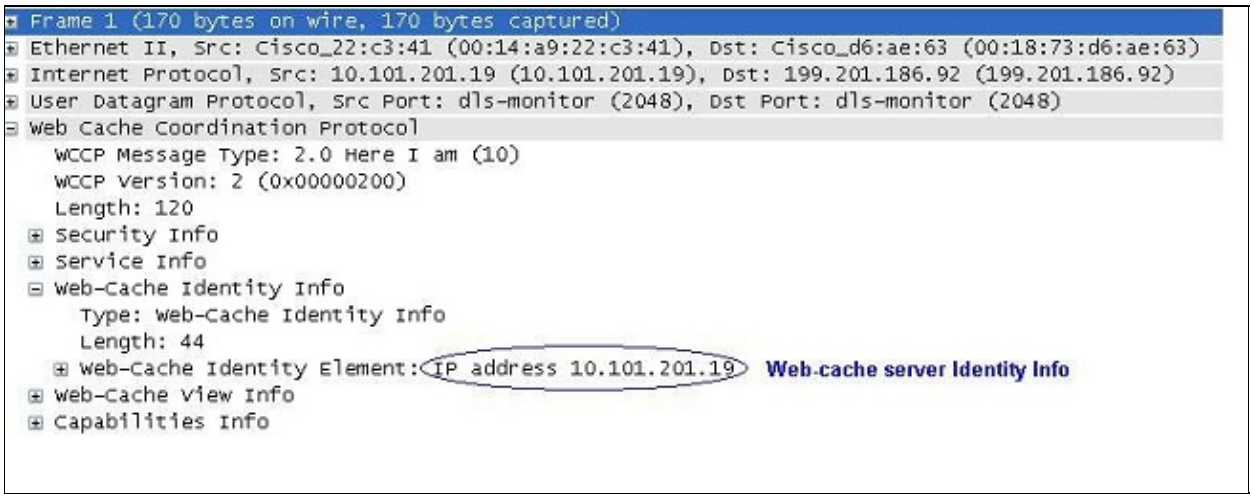
Well−known services are known by both ASA and web caches and do not require a description other than a Service ID.

In contrast, dynamic services must be described to an ASA. The ASA may be configured to participate in a particular dynamic service group, identified by Service ID, without any knowledge of the characteristics of the traffic associated with that service group. The traffic description is communicated to the ASA in the WCCP2_HERE_I_AM message of the first web cache in order to join the service group. A web cache uses the Protocol, Service Flags, and Port fields of the Service Info component in order to describe a dynamic service. Once a dynamic service has been defined, the ASA discards any subsequent WCCP2_HERE_I_AM message that contains a conflicting description. The ASA also discards a WCCP2_HERE_I_AM message that

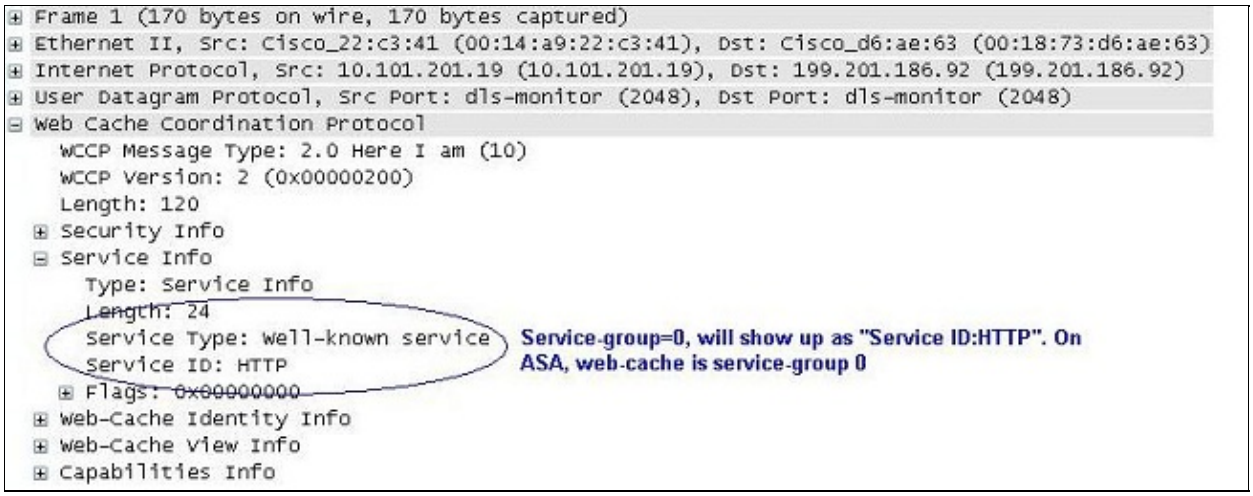
describes a service group for which it has not been configured.

The numbers 0 to 254 are dynamic services, and the web cache service is a standard, or well−known, service. What this means is that when the web cache service is specified, the WCCP V2 protocol has predefined that TCP destination port 80 traffic is to be redirected. For the numbers 0 to 254, each number represents a dynamic service group. The WCCP CEs (such as Bluecoat) are to define a set of protocols and ports that are to be redirected for each service group. Then, when the ASA is configured with that same service group number (wccp 0 ... or wccp 1 ...), the ASA performs redirection on the specified protocols and ports as directed by the Bluecoat device.

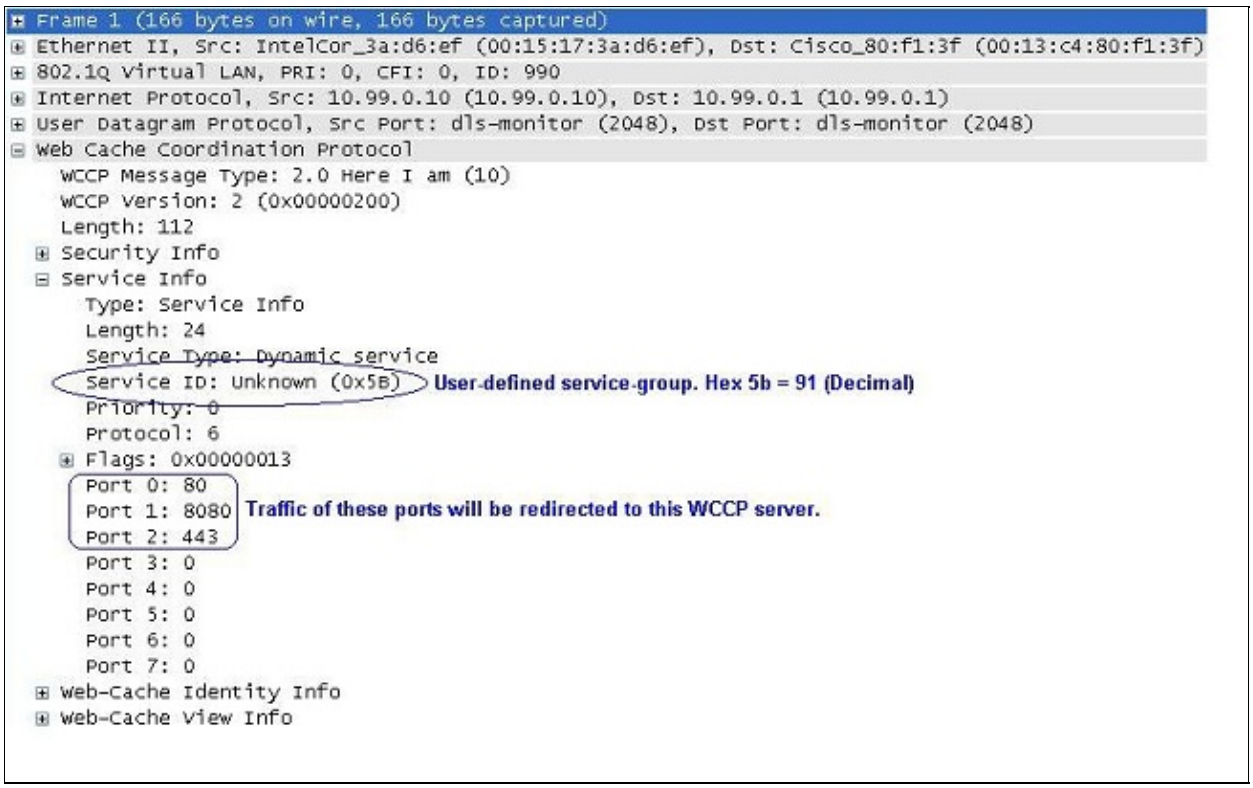
This is an example that shows Web−Cache Identity Info:



This is an example that shows that the web cache is part of service group 0:



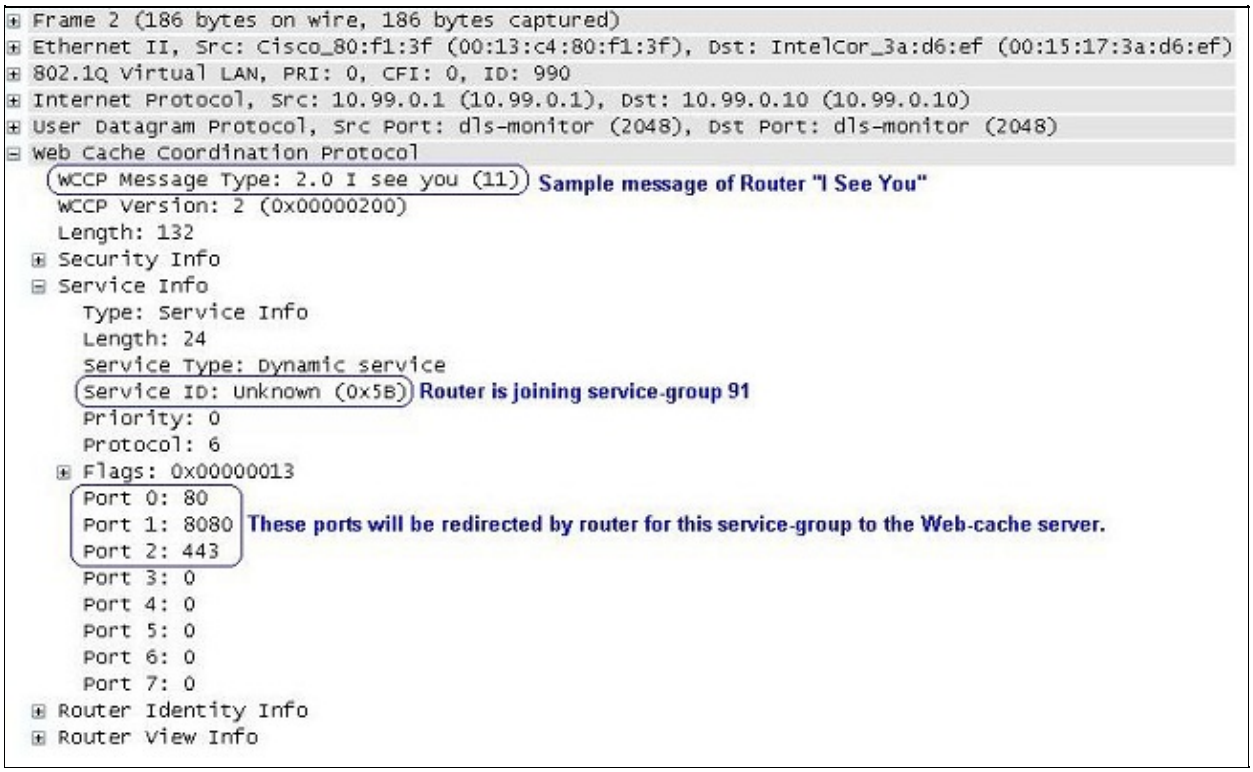
This is an example that shows a web cache server as part of customer service group 91 and the ports whose traffic is redirected to the server:



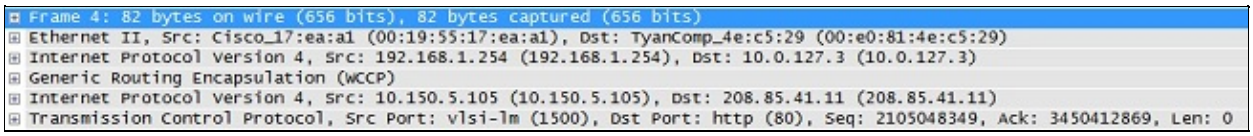
ASA responds to a WCCP2_HERE_I_AM message with a WCCP2_I_SEE_YOU message.

- If the WCCP2_HERE_I_AM message was unicast, the router responds immediately with a unicast WCCP2_I_SEE_YOU message.
- If the WCCP2_HERE_I_AM message was multicast, the router responds with the scheduled multicast WCCP2_I_SEE_YOU message for the service group.

This is an example of the router/ASA 'I See You' message, which shows that the router joins service group 91 and redirects ports 80, 8080, and 443 to the web cache server:



This is an example of a GRE packet:



Configure

Note: In redirect−list, the access list should only contain network addresses. Port−specific entries are not supported.

Note: For more information on the ***wccp*** command, see Cisco ASA 5500 Series Command Reference, 8.2.

This procedure describes how to configure WCCP on an ASA:

1. Enter the ***wccp*** command in order to specify the traffic to redirect:

   ```
   wccp {web−cache | service_number} [redirect−list access_list] [group−list access_list]
   [password password]
   ```
2. Enter the ***wccp*** command in order to specify the interface on which traffic redirection should occur:

   ```
   wccp interface interface_name {web−cache | service_number} redirect in
   ```

Note: WCCP redirect is supported only on the ingress of an interface.

This is an example of an ASA configuration:

```
access−list caching permit ip source_subnet mask any
wccp 90 redirect−list caching
```

```
wccp interface 90 redirect in

Helpful Commands:
show wccp
show wccp 90 service −> this should indicate the ports that are being serviced by this WCCP
server. Without the 'service−flags ports−defined' in the Cache server configuration, the ports
to be redirected are NOT passed to the ASA. Therefore, the traffic will never be redirected.
This will result in 'Unassigned' increases with 'show wccp'.

ASA# show wccp 90 service

WCCP service information definition:
Type:          Dynamic
Id:            90
Priority:      0
Protocol:      6
Options:       0x00000013
−−−−−−−−
Hash:      SrcIP DstIP
Alt Hash:  −none−
Ports:     Destination:: 80 8080 0 0 0 0 0 0

ASA# show wccp 90 view

WCCP Routers Informed of:
X.X.X.X [Higher IP address on the device will be seen here]

WCCP Cache Engines Visible:
Y.Y.Y.Y [IP address of the web−cache server in the service−group 91]
```

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

If redirection does not work as expected, use these outputs in order to troubleshoot. All of these outputs are on ASA.

- ***show tech−support***
- ***show wccp [service|view|hash|bucket|detail]***
- ***show asp table classify***

If the output from these three commands looks valid, you might then need to:

- Review the appropriate syslogs.
- Use the ***capture*** comand in order to investigate captures between the ASA interface and web cache server IP and captures between the client and the web server it is trying to access.

The Output Interpreter Tool (registered customers only) supports certain ***show*** commands. Use the Output Interpreter Tool in order to view an analysis of ***show*** command output.

Related Information

- ***Cisco ASA 5500 Series Next Generation Firewalls Reference Guides***
- ***Cisco ASA 5500 Series Next Generation Firewalls Configuration Guides***
- ***Technical Support & Documentation − Cisco Systems***

Updated: May 31, 2013 Document ID: 116046