Configuring Web Cache Services Using WCCP

This chapter describes how to configure web caching services using WCCP, and includes the following sections:

Information About WCCP

The purpose of web caching is to reduce latency and network traffic. Previously-accessed web pages are stored in a cache buffer, so if a user needs the page again, they can retrieve it from the cache instead of the web server.

WCCP specifies interactions between the ASA and external web caches. The feature transparently redirects selected types of traffic to a group of web cache engines to optimize resource usage and lower response times. The ASA only supports WCCP version 2.

Using a ASA as an intermediary eliminates the need for a separate router to do the WCCP redirect because the ASA takes care of redirecting requests to cache engines. When the ASA knows when a packet needs redirection, it skips TCP state tracking, TCP sequence number randomization, and NAT on these traffic flows.

Guidelines and Limitations

Supported WCCP Features

The following WCCPv2 features are supported with the ASA:

- Redirection of multiple TCP/UDP port-destined traffic.
- Authentication for cache engines in a service group.

Unsupported WCCP Features

The following WCCPv2 features are not supported with the ASA:

- Multiple routers in a service group is not supported. Multiple Cache Engines in a service group is still supported.

- Multicast WCCP is not supported.

- The Layer 2 redirect method is not supported; only GRE encapsulation is supported.

- WCCP source address spoofing is not supported.

- WAAS devices are not supported.

WCCP Interaction With Other Features

In the ASA implementation of WCCP, the following applies as to how the protocol interacts with other configurable features:

- Cut-through proxy will not work in combination with WCCP.

- An ingress access list entry always takes higher priority over WCCP. For example, if an access list does not permit a client to communicate with a server then traffic will not be redirected to a cache engine. Both ingress interface access lists and egress interface access lists will be applied.

- TCP intercept, authorization, URL filtering, inspect engines, and IPS features are not applied to a redirected flow of traffic.

- When a cache engine cannot service a request and packet is returned, or when a cache miss happens on a cache engine and it requests data from a web server, then the contents of the traffic flow will be subject to all the other configured features of the ASA.

- In failover, WCCP redirect tables are not replicated to standby units. After a failover, packets will not be redirected until the tables are rebuilt. Sessions redirected prior to failover will likely be reset by the web server.

- If you have two WCCP services and they use two different redirection ACLs that overlap and match the same packets (with a deny or a permit action), the packets behave according to the first service-group found and installed rules. The packets are not passed thorugh all service-groups.

Enabling WCCP Redirection

There are two steps to configuring WCCP redirection on the ASA. The first involves identifying the service to be redirected with the **wccp** command, and the second is defining on which interface the redirection occurs with the **wccp redirect** command. The **wccp** command can optionally also define which cache engines can participate in the service group, and what traffic should be redirected to the cache engine.

WCCP redirect is supported only on the ingress of an interface. The only topology that the ASA supports is when client and cache engine are behind the same interface of the ASA and the cache engine can directly communicate with the client without going through the ASA.

The following configuration tasks assume you have already installed and configured the cache engines you wish to include in your network.

To configure WCCP redirection, perform the following steps:

	Command	Purpose
Step 1	`wccp {web-cache	service_number}` `[redirect-list access_list] [group-list access_list] [password password]`  **Example:** `hostname(config)# wccp web-cache`	Enables a WCCP service group The standard service is **web-cache**, which intercepts TCP port 80 (HTTP) traffic and redirects that traffic to the cache engines, but you can identify a service number if desired between 0 and 254. For example, to transparently redirect native FTP traffic to a cache engine, use WCCP service 60. You can enter this command multiple times for each service group you want to enable. The **redirect-list** *access_list* argument controls traffic redirected to this service group. The **group-list** *access_list* argument determines which web cache IP addresses are allowed to participate in the service group. The **password** *password* argument specifies MD5 authentication for messages received from the service group. Messages that are not accepted by the authentication are discarded.
Step 2	`wccp interface interface_name {web-cache	service_number} redirect in`  **Example:** `hostname(config)# wccp interface inside web-cache redirect in`	Enables WCCP redirection on an interface. The standard service is **web-cache**, which intercepts TCP port 80 (HTTP) traffic and redirects that traffic to the cache engines, but you can identify a service number if desired between 0 and 254. For example, to transparently redirect native FTP traffic to a cache engine, use WCCP service 60. You can enter this command multiple times for each service group you want to enable.

Examples

For example, to enable the standard **web-cache** service and redirect HTTP traffic that enters the inside interface to a web cache, enter the following commands:

```
hostname(config)# wccp web-cache
hostname(config)# wccp interface inside web-cache redirect in
```

Feature History for WCCP

Table 56-1 lists the release history for this feature.

Table 56-1   Feature History for WCCP

Feature Name	Releases	Feature Information
WCCP	7.2(1)	This feature was introduced.