Cisco ASA WCCP Traffic Redirection Guide

First Published: 2014-07-24

Cisco ASA WCCP Traffic Redirection Guide

This guide describes how to redirect traffic to a device using the Web Cache Communication Protocol (WCCP). You would do this only if you install a WCCP-enabled device and you want to apply the services provided by that device to traffic that flows through the Cisco ASA.

About WCCP

WCCP is a content routing protocol that allows you to transparently redirect traffic to a WCCP-enabled device. The device can then apply its services to the redirected traffic.

For example, the Cisco Web Security Appliance (WSA) can apply application filtering, URL filtering, malware prevention, and other services to the redirected traffic.

The specific services that can be applied to traffic can vary based on the WCCP-enabled device. See the documentation for the device for detailed information about configuring services on that device.

When you redirect traffic using WCCP, keep the following behavior in mind:

- The ASA selects the highest IP address configured on any interface as the WCCP router ID. This address is used to establish a GRE tunnel with the device. When the ASA redirects packets to the WCCP-enabled device, 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. For WCCP to work, the interface whose IP address is chosen as the router ID must be in the UP state and there must be a route to the device.
- An inbound access rule always takes higher priority over WCCP. For example, if an interface ACL does not permit a client to communicate with a server, then the matching traffic is simply dropped, it is not redirected.
- TCP intercept, authorization, URL filtering, inspection engines, and IPS features are not applied to a redirected flow of traffic.
- When a device cannot service a request and returns a packet to the ASA, then the contents of the traffic flow is subject to all the other configured features of the ASA.
- 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 through all service groups.

Guidelines for WCCP

Supported Features

- WCCP version 2 only.

- Redirection of multiple TCP and UDP port-destined traffic.
- Authentication for WCCP-enabled devices in a service group.
- Multiple devices in a service group.
- GRE encapsulation.

Unsupported Features

- Multiple routers in a service group.
- Multicast WCCP.
- The Layer 2 redirect method.
- WCCP source address spoofing.
- WAAS devices.
- AAA for network access does not work in combination with WCCP.

Failover

Supports Active/Active and Active/Standby failover with the following restrictions:

- WCCP redirect tables are not replicated to standby units. After a failover, packets are not redirected until the tables are rebuilt.
- Sessions redirected before failover are usually reset by the web server.

IPv6 Guidelines

Does not support IPv6 traffic for redirection.

Additional Guidelines

- When the ASA determines that a packet needs redirection, it ignores TCP state tracking, TCP sequence number randomization, and NAT on these traffic flows.
- WCCP does not support ACLs that include a user, user group, service group, or a fully qualified domain name object.
- The maximum number of services, including those specified with a dynamic service identifier is 256.

Redirect Traffic with WCCP (CLI)

To redirect traffic to a Web Security Appliance (WSA) or other device that uses WCCP redirection,perform the following procedure.

Before you begin

Install the WCCP-enabled device, such as the WSA. You can either configure WCCP attributes on the WSA first and use those values in the ASA configuration, or configure WCCP on the ASA and use them in the WSA configuration.

See the documentation for your WCCP-enabled device for information on any network topology limitations for the device in relationship to the ASA.

Procedure

Step 1 Enable a WCCP service group and identify the service to be redirected:

wccp { **web-cache** | *service_number* } [**redirect-list** *access_list*] [**group-list** *access_list*] [**password** *password*]

Example:

```
ciscoasa(config)# wccp web-cache password w0lfPe0ple
```

The standard service is **web-cache**, which intercepts TCP port 80 (HTTP) traffic and redirects that traffic to the WCCP-enabled device, but you can instead identify a dynamic service number between 0 and 254. The WCCP-enabled device defines the services associated with this dynamic service number; on the ASA, you are simply associating the number with this group. See the device documentation for details about service numbers. You can specify multiple **wccp** commands if you have more than one dynamic service.

The **redirect-list** *access_list* argument identifies traffic that is redirected to this service group. The permit ACEs in the ACL define the redirected traffic.

The **group-list** *access_list* argument determines which web cache IP addresses are allowed to participate in the service group. The permit ACEs in the ACL define the server addresses or subnets.

The **password** *password* argument specifies MD5 authentication for messages that are received from the service group. Messages that are not accepted by the authentication are discarded. You must define this password in the WCCP-enabled device configuration.

Step 2 Identify an interface and enable WCCP redirection on the interface:

wccp interface *interface_name* { **web-cache** | *service_number* } **redirect in**

Example:

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

WCCP redirection is supported only on the ingress of an interface.

Specify **web-cache** or the dynamic service number you configured on the **wccp** command.

Example

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

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

Redirect Traffic with WCCP (ASDM)

To redirect traffic to a Web Security Appliance (WSA) or other device that uses WCCP redirection, perform the following tasks:

Procedure

Step 1 Install the WCCP-enabled device, such as the WSA. You can either configure WCCP attributes on the WSA first and use those values in the ASA configuration, or configure WCCP on the ASA and use them in the WSA configuration.

See the documentation for your WCCP-enabled device for information on any network topology limitations for the device in relationship to the ASA.

Step 2 Create a service group for WCCP, which enables WCCP and identifies the traffic to redirect and theservers to which you are redirecting traffic. See Configuring WCCP Service Groups, on page 4.

Step 3 Identify the interface whose inbound traffic you want to redirect. See Configure WCCP Packet Redirection.

Configuring WCCP Service Groups

To enable WCCP and define a WCCP service group, perform the following steps.

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Advanced** > **WCCP** > **Service Groups**.

Step 2 Do any of the following:

- To add a new service group, click **Add**.
- To edit a service group, select it and click **Edit**.

Step 3 In the Add/Edit Service Group dialog box, configure the following options:

- **Service**—The type of service, one of:
  - **Web Cache**—The standard service, which intercepts TCP port 80 (HTTP) traffic and redirects that traffic to the WCCP-enabled device.
  - **Dynamic Service Number**—The WCCP-enabled device defines the services associated with this dynamic service number (0-254); on the ASA, you are simply associating the number with this group. See the device documentation for details about service numbers. You can create multiple service groups if you have more than one dynamic service.
- **Redirect List**—(Optional.) An ACL whose permit entries define the traffic that should be redirected for this service. Click **Manage** to create new ACLs or to view the contents of an ACL.
- **Group List**—(Optional.) An ACL whose permit entries define the WCCP-enabled devices that can provide this service.
- **Password, Confirm Password**—(Optional.) A password up to seven characters long, which is used for MD5 authentication for messages received from the service group. You must configure the same password on the WCCP-enabled device.

Step 4 Click **OK**.

Step 5 Click **Apply** to save your changes.

Configure WCCP Packet Redirection

To configure packet redirection on the ingress of an interface using WCCP, perform the following steps.

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Advanced** > **WCCP** > **Redirection**.

Step 2 Do any of the following:

- To add redirection for an interface and service group, click **Add**.
- To edit redirection for an interface and service group, select it and click **Edit**.

Step 3 In the Add/Edit WCCP Redirection dialog box, configure the following options:

- **Interface**—The interface whose inbound traffic you want to redirect to the WCCP-enabled device.
- **Service Group**—The WCCP service group for which you are redirecting traffic. Click **New** if you need to create a new group.

Step 4 Click **OK**.

Step 5 Click **Apply** to save your changes.

Monitoring WCCP

You can monitor WCCP using the following commands. In ASDM, enter the commands on **Tools** > **Command Line Interface**.

- **show running-config wccp**

  Shows the current WCCP configuration.

- **show running-config wccp interface**

  Shows the current WCCP interfaces status.

In ASDM, you can also use these options:

- To display configured WCCP service groups, choose **Monitoring** > **Properties** > **WCCP** > **WCCP Service Groups**.
- To display configured WCCP interface statistics, choose **Monitoring** > **Properties** > **WCCP** > **WCCP Redirection**.

History for WCCP

Feature Name	Releases	Feature Information
WCCP	7.2(1)	WCCP specifies interactions between the ASA and external web caches. We introduced the following commands: **wccp** and **wccp interface** We introduced the following screens: **Configuration** > **Device Management** > **Advanced** > **WCCP** > **Service Groups** **Configuration** > **Device Management** > **Advanced** > **WCCP** > **Redirection**