

WCCP session to the router/switch up, but browsing not happening due to route issues



Document ID: 118257

Contributed by Bhuiyan Muhaimen and Jai Koolwal, Cisco TAC Engineers.

Aug 12, 2014

Contents

Question:

WCCP session to the router/switch up, but browsing not happening due to route issues

Environment:

Cisco Web Security Appliance
Catalyst Switch, Router, ASA

Symptoms:

WCCP session is up and working but browsing does not work.

In certain circumstances, the Cisco Web Security Appliance can talk to the router but client traffic might not pass. We would see WCCP session is up but still no browsing is happening.

WCCP configuration on the Catalyst switch is minimal (*the redirect-list is not germane to this discussion but reproduced here for the sake of completeness*):

```
ip wccp 91 redirect-list 130 group-list 30
```

```
interface Vlan20
description client vlan 20
ip address 192.168.20.1 255.255.255.0
ip wccp 91 redirect in
```

```
access-list 30 permit 10.66.71.17
access-list 130 permit ip any host 192.168.20.103 log
access-list 130 permit ip host 192.168.20.103 any log
```

We would see WCCP is up:

```
Switch#sh ip wccp 91 d
WCCP Client information:
```

```
WCCP Client ID:    10.66.71.17
Protocol Version:  2.0
State:             Usable
Redirection:       L2
```

Packet Return: L2
Packets Redirected: 0
Connect Time: 00:12:49
Assignment: MASK

But browsing could fail to happen.

The problem lies with the route configuration on the Cisco Web Security Appliance. For example, the Cisco Web Security Appliance might not have a route to get back to VLAN 20. The non-working route configuration is as follows:

Success — Your changes have been committed.

Routes for Management and Data Traffic (Interface M1: 10.66.71.17)

Name	Destination Network	Gateway	<input type="checkbox"/> Delete
Default Route	All Others (Including External)	10.66.71.1	<input type="checkbox"/>
client	192.168.30.0/24	10.66.71.4	<input type="checkbox"/>
wccp	192.168.99.99	10.66.71.4	<input type="checkbox"/>

Copyright © 2003-2009 IronPort Systems, Inc. All rights reserved.

The problem is usually seen if only one interface (M1) is used for the Cisco Web Security Appliance for both management and data traffic. In the above example, we have route to VLAN 30 through the second entry and route to WCCP device through third entry and a default route to 10.66.71.1 for all other networks. However if 10.66.71.1 is the gateway to the Internet but does not know about how to route to 192.168.20.0/24 then routing would fail and client browsers will not be able to browse.

A simple ping test would show whether we have a route back to the client.

```
s650a.lab (SERVICE)> ping 192.168.20.103
```

Press Ctrl-C to stop.

```
PING 192.168.20.103 (192.168.20.103): 56 data bytes
```

```
^C---- 192.168.20.103 ping statistics ----
```

```
17 packets transmitted, 0 packets received, 100% packet loss
```

The solution to this problem is to add in a route on the Cisco Web Security Appliance back to the client VLANs. This can be done by:

WebUI > Network > Route > Add Route

Routes

Success: Your changes have been committed.

Routes for Management and Data Traffic (Interface MI: 10.66.71.17)

Name	Destination Network	Gateway	All Delete
Default Route	All Others (Including External)	10.66.71.1	<input type="checkbox"/>
client	192.168.30.0/24	10.66.71.4	<input type="checkbox"/>
ethernet-vlan20	192.168.20.0/24	10.66.71.4	<input type="checkbox"/>
wccp	192.168.99.99	10.66.71.4	<input type="checkbox"/>

Copyright © 2003-2009 IronPort Systems, Inc. All rights reserved.

After adding this, pings should flow from the Cisco Web Security Appliance to the client and we should see browsing happening on the clients in VLAN 20 (host 192.168.20.103 in this example).

```
s650a.lab (SERVICE)> ping 192.168.20.103
```

```
Press Ctrl-C to stop.PING 192.168.20.103 (192.168.20.103): 56 data bytes
64 bytes from 192.168.20.103: icmp_seq=0 ttl=127 time=0.835 ms
64 bytes from 192.168.20.103: icmp_seq=1 ttl=127 time=0.343 ms
```

```
^C--- 192.168.20.103 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.343/0.589/0.835/0.246 ms
```

Please note that it bares repeating that this is one of the reason that browsing might fail. There could be other reasons why WCCP would be up but browsing would not be working but this is one of the more common problems.