WCCP with Authentication and Multiple WSAs Causes a Loop (ACL Required to Limit Client Access)

TAC   **Document ID: 118416**

Contributed by Cisco TAC Engineers.

Oct 13, 2014

Contents

Question
Symptoms
Solution

Question

Does WCCP with Authentication and multiple WSAs cause a loop (ACL required to limit client access)?

Symptoms

When using WCCP, Authentication, and at least two WSAs, clients are being redirected when they attempt to access the Transparent Auth Server URL. This appears as severe latency or time outs on the client.

Solution

When authentication is being used with WCCP, the WSA must first redirect the client to itself, before it can perform authentication. This is a necessary step, since authentication cannot be done twice for the same destination.

The problem that is happening is that when the client makes a new request for the WSA, the WCCP router is redirecting this request back through the WCCP pool. This request may be re−proxied through a different WSA, which will cause this second WSA to attempt to fetch the object from the first WSA.

In order to prevent such undesired behavior, an ACL will need to be created on the WCCP router. The ACL should look similar to the following:

ACL line	Purpose
access−list 105 deny ip host <WSA 1> any	Do NOT redirect traffic that originates from WSA 1
access−list 105 deny ip host <WSA 2> any	Do NOT redirect traffic that originates from WSA 2
access−list 105 deny ip host any <WSA 2>	Do NOT redirect any clients going directly to WSA 1 (authentication)
access−list 105 deny ip host any <WSA 1>	Do NOT redirect any clients going directly to WSA 2 (authentication)

This will prevent the clients from being redirected for the proxy authentication requests to the WSAs.

You can also limit which WSAs will be accepted as web–caches by utilizing the group list:

ACL line	Purpose
access–list 15 permit <WSA 1>	Allow this IP to be included in the specified WCCP service ID
access–list 15 permit <WSA 2>	Allow this IP to be included in the specified WCCP service ID

The syntax to implement WCCP with these ACLs is:

ip wccp <service ID> redirect–list 105
ip wccp <service ID> redirect–list 105 group–list 15

NOTE: You will need to add a rule for each WSA that you have. In the above scenario, there were only two WSAs.

Updated: Oct 13, 2014   Document ID: 118416