Achieving rapid success with WCCP and Web Security Gateway

October 2011 Webinar Q/A

1. **What if you are already using WCCP for Cisco waas on the same routers that you need to use WCCP for websense?**

   Using WCCP for multiple services on the same redirection device is common; the key is not designing a solution where the same interface and direction is used for multiple service groups. This is due to WCCP being limited to redirecting traffic to one service group per direction, per interface. WCCP establishes a hierarchy (service group priority) in the service groups when first negotiated. By default the Websense Content Gateway is designed to hold highest priority for service ID 0 (TCP 80, HTTP).

2. **Are explicit proxy connections also affected by the ARM config?**

   ARM is configured by default to redirect TCP 8080 for HTTP & TCP 8070 for HTTPS; which are considered standard TCP ports for explicit proxy requests.

3. **How can I check if looping occurs using WCCP with Cisco ASA?**

   The easiest way to identify a looping condition is to perform a packet capture of traffic between the proxy and ASA. What you will look for are repeating SYNs until the TTL decrements to 0, and then repeats again.

4. **Can we set up WCCP to more than a single interface (say to eth0 and eth1) for port redundancy?**

   It's not recommended to configure WCCP to redirect a service group to more than one interface on the same proxy. Our V10000 appliance has redundant interfaces to allow port redundancy technologies such as etherchannel to manage connectivity to the proxy.

5. **Could you talk about HASH VS MASK? I was told MASK is better because it does "load distribution" rather than "load balancing.**

   We want to avoid the term "load balancing". WCCP does not perform intelligent load balancing similar to what you would get with an actual load balancer. By default, we utilize destination IP for the load distribution calculation, however this is configurable and is sometimes needed in some specific situations. We wouldn't necessarily think that one assignment method is better than the other, but more along the lines of what your specific hardware/software platform supports and which is optimal in that instance.

6. **How would you recommend a multiple datacenter deployment of WCCP?**

   There are many factors to consider when designing a large distributed deployment. Understanding these details and the scope of the project would be required before making a

recommendation. We would recommend calling our Sales Engineering team to initiate the discussion.

7. **With WCCP can you force all traffic from devices to go through the web filtering gateway without having to do any client side configuration?**

   Absolutely; that is one of the big benefits of WCCP, and a down side as well. Once you have WCCP in place, it will redirect any traffic destined for the ports defined in the service group, requiring no configuration on the client side, hence the term "transparent". This can be a challenge however when an application that tunnels traffic over port 80 does not work well with a proxy.

8. **If we need to bypass proxies for certain destinations, do we need to do it at the router with ACL or something else?**

   You have two options to implement a bypass; either through a deny statement in the redirect list ACL used for WCCP, or a bypass configured within the ARM module of the WCG. My personal opinion is to configure this within the redirect list ACL as I like to avoid turning the WCG into an unnecessary additional router, but at the same time you want to avoid your ACL becoming too large and complex.

9. **What ports are defaulted to the WCG via WCCP?**

   There are no ports defaulted to the WCG via WCCP in v7.6; just what you configure in the WCG itself. Saying that though, you are normally only going to configure the standard ports for HTTP, HTTPS, and FTP if desired. In version 7.5, these standard ports were hard-coded.

10. **Any limitations for WCCP on ASA ios 8.2.2**

    Please review the ASA configuration guide for WCCP limitations on 8.2 here.

11. **We have to two switch redundant setup with P1 connected to switch A and E1 connected to switch B. With P1 and E1 bonding, is WCCP processing active/active?**

    Our Gen2 V10000 appliances have expansion interfaces (E1 & E2) that can be bonded in either Active/Standby or Load balancing mode. It wasn't intended to have the P1/E1 or P2/E2 interfaces on separate redirection devices when bonded. However I don't see why the proxy wouldn't process requests to either interface when in the load balance bonded mode.

12. **We're planning to use IP spoofing. What does the WCCP setup look like to route the traffic back to the V10Ks?**

    IP Spoofing can be a tricky topic, but at a high level, you have to control traffic in both directions so that all parts of the web request are returned to the proxy. This means that a standard service group has to be configured, and a "reverse" service group. Reverse service groups key off of source port instead of destination port, to catch the return traffic from a web server. This

also means that you need an additional redirect list ACL for this reverse service that is a mirror of the redirect list ACL utilized to perform the initial redirection from your users. For example:

```
ip access-list extended wccp_redirect
permit ip 10.0.0.0 0.255.255.255 any
permit ip 192.168.10.0 0.0.0.255 any
ip access-list extended wccp_reverse_redirect
permit ip any 10.0.0.0 0.255.255.255
permit ip any 192.168.10.0 0.0.0.255
```

This also requires that the user traffic, WCG, and WCCP Server reside on three separate legs, or subnets. You would configure the standard service group on the aggregation interface where your user traffic resides, and the reverse service group on the interface where your web server traffic is returned to.

13. What are the challenges of using WCCP over a PAC file when proxy HTTPS traffic?

This really depends on the PAC file configuration. We utilize PAC files for our hybrid solution where customers enforce transparent redirection (WCCP) when on their network. As long as the traffic flow isn't switching from one to the other, using both features shouldn't be an issue.

14. I have issues configuring wccp on cisco 4500 switch, how I can configure cisco 4500 switch with wccpv2 for a v10000 transparent proxy?

Please review the 4500 switch configuration guide for WCCP on IOS 12.2(31)SG here as an example.

15. What kind of latency can we expect to see utilizing wccp with Websense and our ASA?

Latency is impacted by the traffic volume, the number of security context modes, resource load, and configuration of the firewall. We've observed a lower performance rating with the ASA than larger switch chassis such as the Cisco 6500 series switch.

16. Can you talk a little more about the bypass? Is that setup in the router doing WCCP or is it set on the V10000 appliance? (and if so where?)

Please refer to question 22. This can be situational however depending on the type of deployment you have. Configuring a bypass in the WCG may not be an option if it will cause a redirect loop.

17. Hash and mask in relation to authentication? You have an array of WCG's and dont want the user to be challenged for credentials multiple times? What is better hash or mask?

Proxy authentication is not related to what assignment method you utilize for WCCP. These are two separate functions.

18. **When configured ACL's for redirection and reverse traffic is it better to summarize all the different subnets or specifically set them? We have Nexus 7010's and so far so good, just wondered about the ACLs. We also have IP Spoofing working on the Nexus 7010's**

    In general, it's always more efficient to summarize where you can, however it is important to ensure that either the subnets you're summarizing are contiguous, or that the subnets you are including in the summarization will have no issues with being redirected.

19. **In an active setup, does WCCP or WCG handle load balancing?**

    With WCCP, you are always in an Active/Active setup; this is one of the benefits of WCCP. WCCP handles the load distribution automatically. The WCG with the lowest IP address becomes what is called the "Designated Web Cache", or what we call the "Leader". The Leader controls the service group and handles the redistribution of the assignment method via a "redirect assign" message that is sent by the WCG when there any changes to the service group, such as an addition or loss of a WCG.

20. **Can you talk about the known issues with Active vs. Passive FTP and WCCP redirect? Are only one or the other supported and what if an external site doesn't support that type of FTP?**

    There are known issues with Passive FTP because it utilizes random ports, which almost always results in the appropriate traffic not being redirected. You want to use Active FTP whenever possible. If the destination web site does not support it, you will be forced to implement a bypass.

    Here is a summary of some research I have done on this:
    Active Mode FTP

    Client initiates one connection (CMD); server initiates the other (DATA)

    a. Client opens a random port (N > 1023) and connects to the FTP server on port 21. This is redirected with WCCP.
    b. Client starts listening on N + 1 and then sends a PORT command N + 1 to the FTP server.
    c. FTP server connects to N + 1 from its local DATA port, port 20

    Passive Mode FTP

    Client initiates both connections (CMD + DATA)

    a. Client opens two random ports (N > 1023 and N + 1)
    b. N > 1023 connects to the FTP server on port 21 and issues a PASV command. This is redirected with WCCP
    c. FTP server opens random port (P > 1023) and sends PORT P command back to client.
    d. Client initiates connection from N + 1 to port P to transfer data. **This is *not* redirected with WCCP because the destination port is random**.

    Reference:

http://slacksite.com/other/ftp.html

21. Is it normal not to see redirects incrementing on Cisco if configured on L2 interface?

Depending on your hardware/software version, this can be normal. In the output of some WCCP commands you may not see any redirects incrementing because that output is only displaying redirection performed in software, which is a bad thing with switches utilizing the L2 forwarding method.

22. Can a Cisco 3750 be used for WCCP?

Yes. Check your Cisco documentation for specifics on supported methods and IOS versions required.

23. INCASE OF ASA FAILOVER, would the packet also fail over or dropped?

The ASA must be configured for stateful failover in order for all connections; including proxy connections; to failover to the secondary ASA.

24. Is there a way to bypass local address space with WCCP so it isn't going to WCG?

Absolutely; this is done via deny statements in the redirect list ACL, and this is in my opinion a best practice as we do not want to redirect internal traffic to the proxy.

25. Redirect ACL for WCCP on a client interface is not supported and Incoming traffic redirection on an interface is supported, but outgoing traffic re-direction is not. How to configurate wccpv2 on cisco 4500 switch series release 2.2(54) SG for v10000?

Please review the 4500 switch configuration guide for WCCP on IOS 12.2(54) SG here.

26. What happens to outgoing traffic if WCCP redirection not working such as V10K is offline?

When the WCG is offline, “Here I Am” messages are no longer sent. Once the WCCP Server stops receiving these, it will send a “Removal Query” message and remove the affected WCG out of the service group. If there is only one WCG within the service group, the service group is disabled and traffic is sent normally. If there are multiple, the Leader WCG will send a “Redirect Assign” message to let the WCCP Server know how to redistribute the traffic. Should the Leader go offline, a new Leader is established and takes control of the service group.

27. We have a WAN setup where unfiltered web traffic is sent to one default gateway through MPLS. This gateway is driven by a FortiGate 300A (FortiGate 3.00 MR7 Patch Release 9 (0753)). Would WCCP be the right option here to capture web traffic here to send it to a V10000G2 appliance?

Provided WCCP is supported by the Fortigate 300A, yes applying WCCP to the incoming traffic on the fortigate seems like the optimal solution.

28. **I thought I heard you say you think it's better to use WCCP on cisco switch/router vs. ASA5540. I didn't understand if that was because of CPU or something else inherent with the switch/router vs. ASA**

    We've seen better performance and throughput when WCCP is configured on a switch with L2 forward and return than on a L3 device such as a router or ASA because the redirection is applied in hardware (ASICs) rather than in software (CPU).

29. **Is the WCCP redirect is best placed before firewalls as redirect out or from the inbound traffic from the network distribution/core without?**

    It would be best to first determine the capabilities of your redirection device(s). Not many devices support WCCP when applied as an out, but keep in mind that when it does, routing and filtering logic is applied prior to determining redirection rules in outbound traffic. This may impact your redirection device resources unnecessarily.

30. **What's best practice to exclude client application traffic that requires port 80 traffic?**

    Unfortunately you can't exclude a specific application's traffic; only the client itself. This is part of the double-edged sword that is transparent proxy that you need to be aware of.

31. **For testing and a phased in approach is it possible to only redirect certain clients/networks, or does WCCP mean all or nothing?**

    Thankfully, WCCP does not mean all or nothing in most deployments. You can specify individual hosts and/or specific subnets via the redirect list ACL used to configure your WCCP Server. However, with some hardware/software platforms there are limitations to what you can use in the ACL, and if you can even use one. Refer to your Cisco documentation for limitations.

32. **Is it common to setup an L3 device only for WCCP - i.e. using a cisco router only for WCCP?**

    I don't know that I would say it's common but I've run across the need to add a device to WCCP redirection. I wouldn't necessarily use a router however as they are a software implementation of WCCP.

33. **What configuration has to happen on the proxy to enable WCCP while testing while the rest of the traffic uses PBR?**

    The important thing is to not have overlap. You want to ensure that you specify deny statements in the ACL used for PBR that you are allowing in the redirection for WCCP.

34. **Which interface of a V10000 use to catch traffic redirected by WCCP on a Cisco 4500 switch?**

    The "P" interfaces on the appliances are tied to the proxy communication.

35. **If the WCG is offline does that mean traffic is passed without filtering? If so, other than open Internet access how would you know WCCP has failed and traffic is open?**

In v7.6 we have developed a proxy assurance agent (PAA) that measures internet performance to determine if the proxy should pull out of WCCP. When the PAA triggers, an alert is sent out. There are external monitor tools that can be leveraged to determine if the proxy is being used also.

36. **How do you (if you even can) "see inside" HTTPS traffic for filtering via WCCP? Doesn't that sort of "break the trust" if you try to see inside the packet for filtering purposes?**

    Like in all HTTPS proxies, a SSL certificate must be deployed to the clients so that we are trusted and can decrypt the traffic for analysis.

37. **I'm getting a login prompt box when I use firefox and IE. I fixed IE by changing the setting in security setting-> internet Zone-> User Authentication to Automactic logon with current user name and password. Firefox does not have this option. Have you seen this issue?**

    We apologize, but this question is not directly related to the presentation content. Please feel free to open a support case to address this issue.

38. **Is L2 recommended over GRE for the WCCP redirect**

    Your network topology and hardware/software limitations will dictate whether L2 is the better choice than GRE. When using switches for WCCP, it is almost always better to use L2 over GRE.

39. **What's the recommended Cisco device for WCCP?**

    We see deployments of WCCP via a switch w/ L2 forward and return redirections as the optimal solution.

40. **Can PBR be a backup to a WCCP policy?**

    Unfortunately due to them both keying off of IP address, I do not see how this could be implemented.