Configuring WCCP v2 with Websense Content Gateway – the Web proxy for Web Security Gateway
December 14, 2011 - Q&A

Q. Is there any other port number which could be used instead on 8070, or it is the one to be used for HTTPS?

- Since v7.5 you can use port 8080 to send both http and https to the proxy.

Q. Are the 'deny ip' statements the IP addresses that we are not redirecting?

- This is correct. The deny IP address statements specify traffic not to be redirected to the proxy via WCCP.

Q. We have two v10K appliances. Is a second standard ACL required on the router? Or is the solution to use the existing standard ACL?

- A second ACL is not necessary. You may use the existing standard ACL group list. Identify both your v10k proxies in this single standard ACL. This ACL affords you an additional level of security.

Q. What is the password in the global ip wccp 0 config for?

- Entering the global WCCP password provides additional security. Proxies requesting to join the WCCP service group must provide the correct password.

Q. If I have one or two appliances, then the correct configuration is use only one standard ACL for the P1 interfaces.

- Correct. You may use the single ACL presented in the demonstration for one or more proxies.

Q. If we have field offices that come to our central office before passing to the Internet how should wccp be set up to redirect those packets to our content gateway that is only located in our central office? The field office connections are joined to an mpls vrf outside of our control and then come in to our central office via a Cisco ASA.

- If you only have the Cisco ASA, WCCP will only work for redirect in and only for internal clients on the same inside interface.

Q. Is eth0 is the P1 interface?

- Yes, that is correct.

Q. Could you please explain extended ACL and why you deny all the private IP address? Our internet network is 10.x.x.x.

- The deny statements prevent internal traffic destined for internal destinations from being redirected. These commands are not necessary for all network architectures. If internal traffic does not pass the router interface where the WCCP redirection is applied, then the commands are not needed.

Q. There was a statement in there for Permit. Do you know what that for?

- The permit statements are for the clients that we want redirected. In our demonstration, we used a single IP address to redirect our test client machine. Alternatively, you may use a network IP range.

Q. Do I have to permit all my internal network on that extended list?

- If you want to redirect all internal network traffic to the Content Gateway, then yes.

Q. First I am denying 10.x.x.x and then I am allowing 10.x.x.x. I do not understand?

- As shown in the demonstration:
    - deny any 10.x.x.x
        - We deny any (source IP) traffic going to the 10.x.x.x network (destination IP).
        - Deny means traffic is not redirected to the proxy.
    - permit 10.x.x.x any
        - We permit only the 10.x.x.x network (source IP) going anywhere (destination IP).
        - Permit means traffic is redirected to the proxy.
        - This makes more sense if you think of the command in a "<permit> <source_IP> <destination_IP>" structure.
- ACLs are processed from top down. When an ACL rule matches the traffic, then that rule applies and the remaining rules are skipped. Such that, all internal traffic is not be redirected. Only traffic destined to a non-internal network address is redirected.

Q. Why did you use GRE instead of L2? When should use one be used over the other, and how is L2 configured?

- The router we are using only negotiates GRE. Generally, you can use L2/Mask/L2 for Cisco 6509 switches. Note that L2 incurs less to processing. Therefore, if you experience high CPU usage, you can test with L2 if your device supports it, and you are layer-two adjacent.

Q. The block page appears from the C interface.

- Correct. On the Websense V-Series appliance, the block page is sent from the C interface.

Q. Are there any additional steps for setting up L2 when compared to GRE?

- Setting up L2 is the same as GRE. Just select L2 and your device must be L2 adjacent. If you have GRE already negotiated, then to successfully start using L2, the WCCP tunnel must be disabled and then re-enabled.

Q. How do you enable WCCP again?

- Within the device the command is:
  - ip wccp version 2
  - ip wccp <service ID>

Q. Will this presentation be available offline?

- The webinar recording and presentation slides will be posted on the support website by end of the today. Q/A will be posted within a week from today. Please check http://www.websense.com/content/SupportWebinars.aspx and click on Archived Webinars.

Q. Can we get a copy of the slides?

- See answer to previous question.

Q. For the ACL, why not permit WCCP traffic and then deny any any?

- For an ACL, there is no need for an explicit deny any any. This is implied at the end of the ACL. Please check with Cisco on known bugs for the "deny any any" statement depending on your IOS version.

Q. If you want to redirect 80 and 443, would I have to configure two commands in the router for service group 0 and 70? In this case, would you need to create two service groups within the WSG with these service group numbers?

- Yes, you are correct. For your example, typically service ID 0 is for http and ID 70 is for https. In versions prior to 7.6, you were limited to entering only one port per service group. This required creating two service groups on the router and Content Gateway if you needed to redirect ports 80 and 443. However, in v7.6 you can now enter multiple ports in a single service group. Additionally in v7.6, you are still allowed to create multiple service groups as in previous versions.

Q. If your V5k appliance was down and you are using WCCP, what happens to the clients traffic? Does it ignore the redirect and proceed to the internet or get lost?

- WCCP is a fail open process. If a proxy becomes unavailable, the WCCP server will remove the proxy from the wccp service group and you users will then have direct access to the Internet.

Q. It seems as though you can combine multiple ports into the same service group. All of the best practice documents I have seen separate 80/443/21 into separate service groups... What is the TRUE best practice?

- Yes, you are correct. Version 7.6 now supports entering multiple ports within the same service group. Deciding to employ one or more service groups should be determined as part of your planning process before implementing WCCP. Employing multiple service groups allows for changing entries within on service group without affecting other service groups. However, adding additional service groups increase TCAM entry usage. Devices have a finite number of

ACL TCAM entries available. Having too many service groups can affect performance. Generally, this TCAM usage is not a major factor. Click here to read details on TCAM. http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11-629052.html

Q. How can I load balance all the traffic between two boxes? Do I use he weight value?

- Please see this article: WCCP load distribution
- http://www.websense.com/content/support/library/web/v76/wcg_help/wccp_load.aspx

Q. I have two appliances. What will be the weight value if I want a load balance 50% in one box and other 50%?

- The numbers you enter are relative. For example, you can enter one (1) as weight value in each proxy. The router will add each proxy's weight value (1+1=2) and since the values are 50% of the total (2/1=50%) and only two proxies are involved, then the traffic will be distributed equally between each proxy. However, if you add a third proxy into the example and still enter one (1) as a weight value on each proxy, then the percentage changes to 33.3% (3/1=33%) of traffic. For additional details, see the answer to the previous question.

Q. Is WCCP v2 supported on Brocade/Foundry devices?

- Our Content Gateway supports a wide subset of available WCCP v2 features. See the "WCCP v2 supported features" document for details. http://www.websense.com/content/support/library/web/v76/wcg_help/WCCP.aspx For your device, check the manufacture's web site for WCCP support. The Websense Content Gateway proxy is available a software download for Red hat. You can obtain a test key and confirm how well you non-Cisco device supports WCCP features. Best practice it to ensure your device is running the most current boot version.

Q. What router model and IOS version did you demonstrate?

- Cisco Router 1711 12.3 (7).

Q. Is it possible to implement WCCP without a standard or extended ACLs, or ACLs always necessary?

- You are not required to user either ACL shown. In my demonstration, I proposed using the ACLs because (1) the group=list provides additional security and the (2) redirect-list allows defining the interesting traffic. You will find our documentation available here at Websense for implementing WCCP does not suggest using ACLs. Our documentation provides the minimum configuration requirements.

Customer comment: ACL works from Top to Bottom. If you have a deny statement for example for 10.0.0.0 and at the end you have a permit statement of 10.1.1.0 0.255.255.255. It will deny and not come to permit statement?

- A point in to keep in mind is that the permit and deny statements are formatted as source and destination. The format can be easily misinterpreted. Check the following chart. Take note of the source and destination columns for the statements.

Command	Source IP	Destination IP
deny ip	host 10.212.1.52	any
deny ip	any	10.0.0.0 0.255.255.255
deny ip	any	172.16.0.0 0.15.25.255
deny ip	any	192.168.0.0 0.0.255.255
permit ip	host 10.212.2.215	any

Q. Can you show again the low part of the page wccp configuration please?

```
=============== ENABLE WCCP ========================
!
Enable
config t
!
ip wccp version 2
!
ip access-list standard TST
permit 10.212.1.52
!
ip access-list extended R_TST
deny ip host 10.212.1.52 any
deny ip any 10.0.0.0 0.255.255.255
deny ip any 172.16.0.0 0.15.25.255
deny ip any 192.168.0.0 0.0.255.255
permit ip host 10.212.2.215 any
!
ip wccp 0 group-list TST redirect-list R_TST password tst
!
int vl 10
ip wccp 0 redirect in
end
!
```

Q. I have personally experienced ODD --and undocumented -- issued doing WCCP setup with Cisco router vs. switch vs. ASA_firewall. Based on experience, ASA and router works typically as expected. Why is switch integration so problematic (based on your experience)?

- Switch integration include more options for deployment including redirect in/out and the ability to use L2 or GRE. Depending on the IOS version and/or deployment, more CPU may be used on the switch.
- For additional information, see the answer to the last question presented below.

Q. My Citrix servers are not happy with WCCP. We deployed a v10000 last week and we have some Citrix servers on internet that our users access and with wccp configured all the clients get frequent disconnects ever since we have had wccp configured.

- Your Citrix servers should not be redirected via WCCP. Install the Websense Citrix plugin on your Citrix servers and exclude each Citrix servers from WCCP redirection. This method is far superior—it also provides end user name resolution as well.

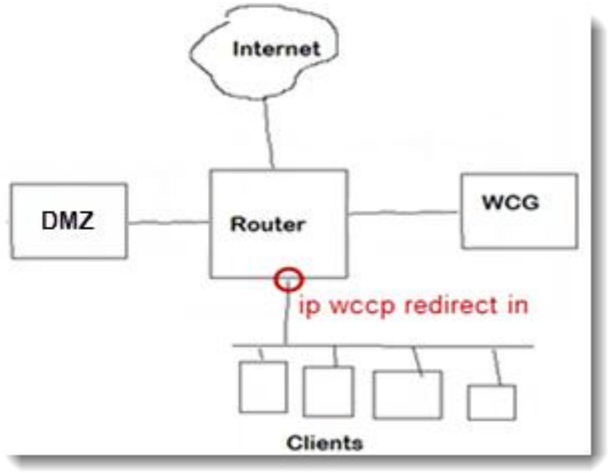
Q. I have Cisco ASA. Did you say that ARM should not be enabled in WCG?

- The ARM module must always be enabled when using WCCP.

Q. Are there any configuration differences between using a Cisco router and a Cisco layer 3 switch for WCCP?

- Configuration for the router and the layer 3 switch is similar.

Q. What is the topology for this practice? Do you have a network map?

- Here is my three-leg router setup.
- 

Q. Have you heard anything about support for WCCP in MPLS/VRF environment?

- As WCCP is not MPLS aware, you should present this question/feature request for Cisco.

Q. What would you use for FTP?

- You can add port 21 as an additional port into the service group created during the demonstration, or create a new server service group specifically for FTP traffic. Service group 5 is a well known ID number for FTP, for example:
  - ip wccp 5 redirect in

Q. Is this for scanning content?

- Yes, the content redirected via WCCP is scanned.

Q. How do the numerous protocols like streaming media, remote access, etc get filtered?

- Websense Network Agent can scan numerous other protocols. Scanning is accomplished via enabling port monitoring.

Q. How many is the bandwidth affected after enabling WCCP on the internal network?

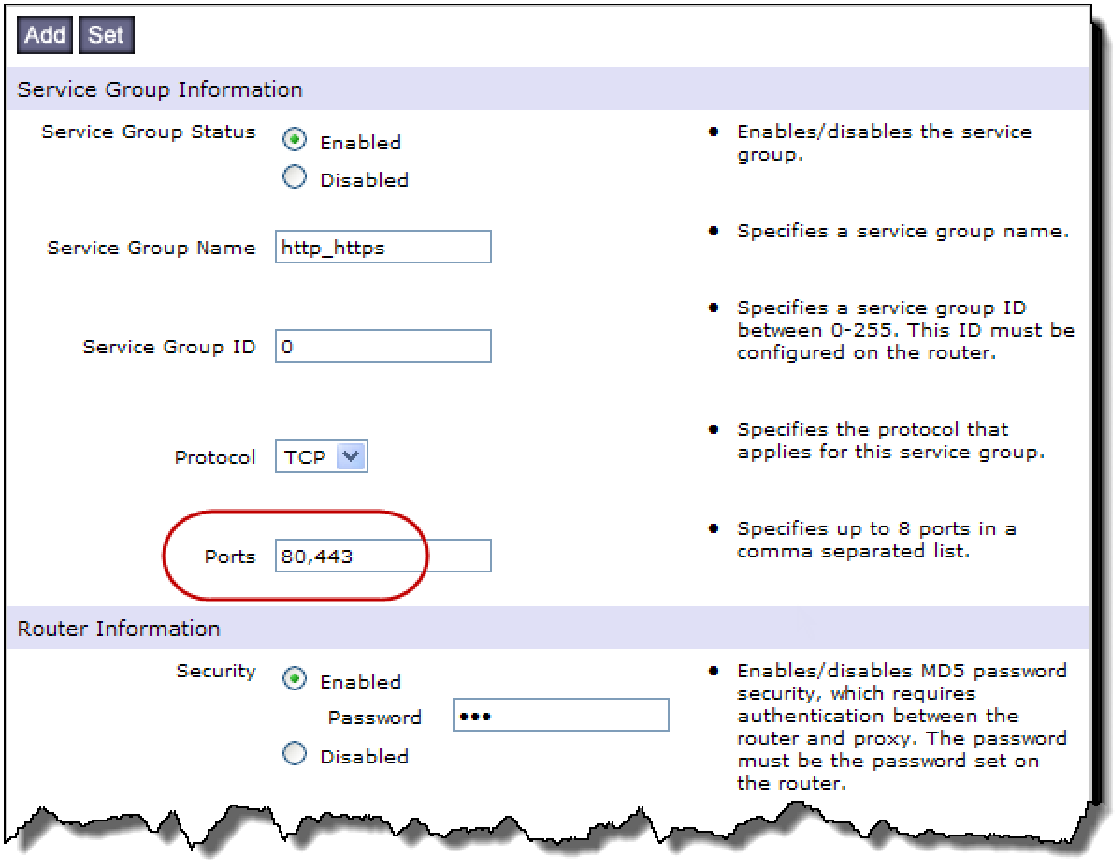
- You should determine this answer as part of your planning process before implementing WCCP. However, typically the increased bandwidth is minimal.

Q. Are there any available tutorials on how to navigate websense console?

- You always have a help option available in each console page. For web filtering, see the following archived Webinars.
    - Jump Start Part 1: Websense Web Security Configuration and Setup
    - Jump Start Part 2: Identifying and Troubleshooting filtering issues for Websense Web Security
    - Jump Start Part 3: Web filtering with the V-Series proxy
    - Jump Start Part 4: Using Reports to Strengthen Filtering Policies

Q. What about service group ID 70. You only setup service group ID 0.

- New to version 7.6, you can add multiple ports when defining a service group in Content Gateway. During the demonstration, I included https traffic (443) in service group 0 as shown below.
- In v7.6, you may still create additional service groups. Service group ID 70 is a well know number for https traffic.

- 

Service Group Information

Service Group Status ● Enabled ○ Disabled
- Enables/disables the service group.

Service Group Name: http_https
- Specifies a service group name.

Service Group ID: 0
- Specifies a service group ID between 0-255. This ID must be configured on the router.

Protocol: TCP
- Specifies the protocol that applies for this service group.

Ports: 80,443
- Specifies up to 8 ports in a comma separated list.

Router Information

Security ● Enabled Password: ••• ○ Disabled
- Enables/disables MD5 password security, which requires authentication between the router and proxy. The password must be the password set on the router.

Q. Can I use WSGA with WCCP and us a simple proxy?

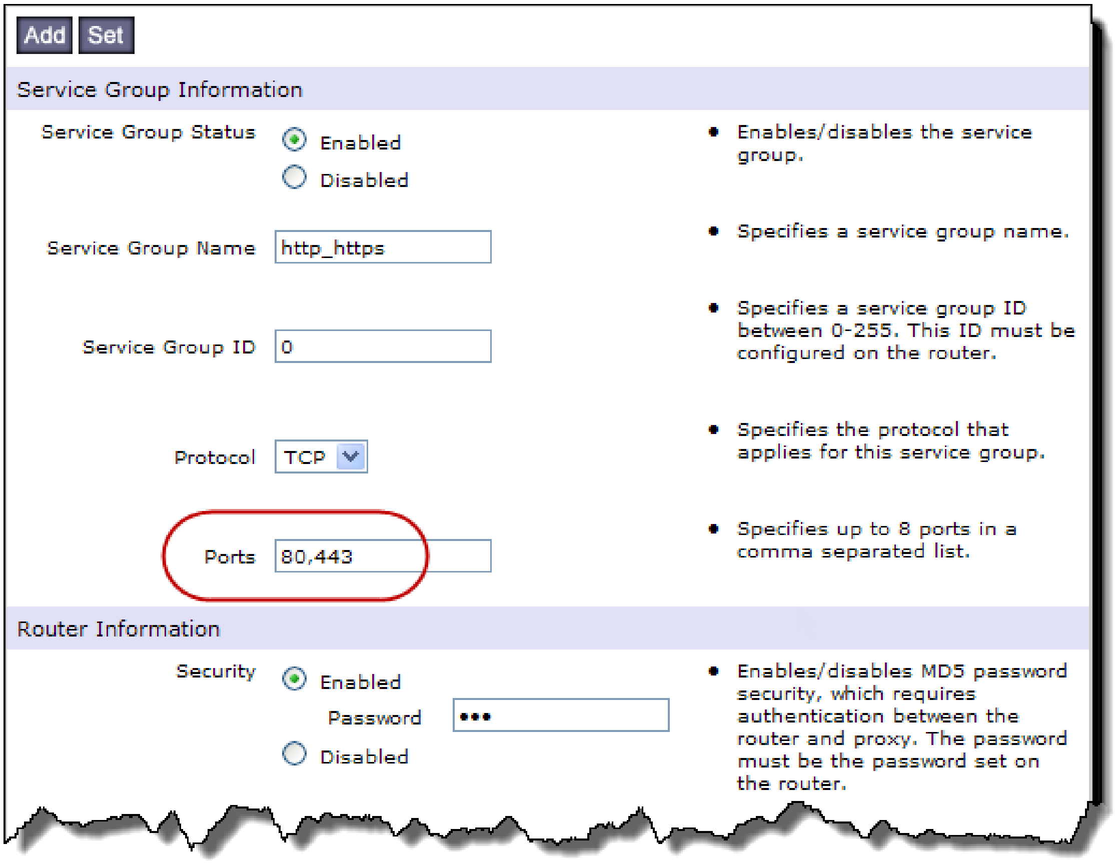
- Yes you can use either WSG or WSGA as a simple proxy. Just point your traffic directly at the proxy as you would in any explicit proxy configuration. For an appliance, point traffic to the P1 interface. You may use port 8080 for both http and https traffic. Since version 7.5, you can send both http and https traffic to the port 8080 on the proxy.

Q. What is the symptom if the ARM is not enabled?

- If ARM is not enabled, then no there will be no NATing on the Websense Content Gateway and it will not be able to redirect the traffic.

Q. I noticed that on the ACL that you used to identify interesting traffic that you specified ALL traffic originating from the host (permit ip host x.x.x.x any). Is there any reason that you specified it this way as opposed to specifying specific traffic such as tcp 80 and 443?

- Excellent question, but there is one item missing in your equation. Since we are using a dynamic service group, the Content Gateway sends the router the data defining the service group. It is in this data that I configured which ports to redirect. See the following screen shot.



Service Group Information

Service Group Status ● Enabled ○ Disabled
- Enables/disables the service group.

Service Group Name http_https
- Specifies a service group name.

Service Group ID 0
- Specifies a service group ID between 0-255. This ID must be configured on the router.

Protocol TCP
- Specifies the protocol that applies for this service group.

Ports 80,443
- Specifies up to 8 ports in a comma separated list.

Router Information

Security ● Enabled Password ••• ○ Disabled
- Enables/disables MD5 password security, which requires authentication between the router and proxy. The password must be the password set on the router.

-
- Within the Here I am packets sent form the WCG to the WCCP Server, the ports to be redirected are specified. For routers and switches, we can safely use simple IP statements in the redirect list. Regardless of the redirect list specifying all IP traffic, only ports 80 and 443 in this example will be redirected.
- Note, it is not recommended to use simple IP statements with ASA as they can produce undesirable results.