Web Security Gateway - What to do when a Web site does not load as expected

November 2011 Webinar Q/A

1. How do you handle the situation where a site produces a blank blockpage and the real-time monitor shows the site is permitted? We have found that there is a redirect but the redirect does not show in the real-time monitor.
    - You can run testlogserver to check what request is actually blocked. OR you can run a packet capture using wireshark to see where the redirect is generated from.

2. Can you specifically allow access to sites like Dropbox, Googledocs or Mediafire, allow downloads, but block uploads?
    - You will only be able to block downloads using file type blocking. In order to block uploads as well you will need to get Data Security Suite.

3. Will there be any file size limit in the WCG log file?
    - There are different log files within the WCG. For the transaction logs which are generated in extended.log file you can configure the file size from the WCG manager.
    - By default this is approx 4.5 GB for the Extended.log and Error.log. When this space is used then the older log files are deleted as required.

4. Does this presentation not apply to Websense Enterprise? My GUI looks nothing like the GUI you are showing.
    - We are working on Websense Content Gateway, which is the proxy product from Websense available with WSG bundle.

5. Is 10 seconds a normal latency for establishing a HTTPS connection?
    - Yes, provided you have SSL decryption enabled. If you think this is consistent you may want to check your DNS.

6. What authentication codes do Kerberos use, instead of NTLM. Or is it still 407 and 502?
    - It will still be a 407 proxy authentication required, but you get just the one 407 instead of the two that you get with NTLM.

7. Why can we get access when a webserver is on a vlan?
    - Which webserver are you referring to? Is the request going via proxy?

8. When I surf to https site, how do I not get certificate errors in Internet Explorer?
    - WCG acts a cert authority for you, so you need to deploy the certificate to the clients. You can do this via group policy and then certificate errors should disappear.

9. Does it support transparent mode?
    - Yes, it supports transparent mode.
    - WCCP or PBR. That doesn't require you to use explicit proxy settings in the browser. This is supported.

10. Can I generate SSL certificate?
    - yes you can, refer to Kbs on the support website.

11. Do you support SSL transparent scan?
    - yes we support this.

12. Can I use wildcards to allow https sites?
    - yes you can.

13. Can I used wildcards to re-categorise URLs for HTTPS connections? I have tried but it only works by IP address.

    - This depends on whether you use Explicit or Transparent proxy configuration. With Explicit, the browser sends the URL hostname to the proxy so you can use URL wildcards, such as *.yahoo.com.
    - If you use Transparent proxy configuration, then the browser only sends the IP address of the site it wants to connect to. In this case you can use IP wildcards, such as 72.30.*.* for filtering.

14. Is it possible to make the NTLM Auth Exceptions for just the Windows Media Content? It was advised that the WMP will not do authentication which is why the pop-up was occurring.
    - In the WCG Access Control menu, you can set NTLM exceptions by “User-Agent”. I believe the Windows Media Player has a User-Agent of “NSPlayer”. This can be used to bypass WMP requests. However, the User-Agent may vary across versions so you should check the HTTP header sent in Wireshark.

15. Can I download trial version? If so, how?
    - Yes you can, please reach out to our sales team or have a look on the website. You can find contact numbers for our sales team. Check out for Websense Security Gateway product or V10000 appliance.

16. Are the Command-line commands, available if I use Putty (SSH) to logon to the appliance? Or must I go through the Appliance Manager GUI?
    - The command line commands are available via ssh however you will not be able to login unless you have authorization to manage the proxy on the appliance version. Usually appliances are managed by Tech support only.

17. Can I use winscp?
    - yes you can to transfer files.

18. Can the error.log and extended.log, be redirected to my syslog (Splunk) server?
    - Yes you can do that, depending on your requirement you may want to do it. You can contact tech support if you have the appliance version to set this up. If you have software version you can look at our KBs.

19. What are the side effects of Authentication Bypass?
    - If you have an authentication bypass, depending on how it is configured it will mean that users will be able to visit the site without authenticating. This also means they will receive an IP-based policy or Default policy, as the username is not known. If not setup correctly you may have users who you may not wish to give access being able to visit the site.

20. What debugging tools work best for resolving client applications that use ports 80 & 443?
    - You could use tcpdump, fiddler and wireshark. They are the best for site access issues.

21. You've showed examples for troubleshooting using explict proxy, how different is the troubleshooting process when using WCCP instead of explict proxy?
    - You can still run wireshark (tcpdump), use fiddler. In addition to that there are some specific debugs for WCCP that can be enabled on the proxy you will need to contact tech support for this.
    - Also, with WCCP the client will send the request to port 80. With explicit the client will send to port 8080 (default proxy port).

22. Do I need to have a V-Series Appliance in order to view/create the extended.log?
    - You need to have either the software version, known as Websense Security Gateway (WSG) or V10k appliance.

23. For an intercepted HTTPS request, what does the verfiy deny depth = 0 error mean and is tunneling/bypassing the only way to avoid it?
    - It means that the certificate verification for the site failed. You can log a case with tech support to investigate if you still need the site to be decrypted.

24. We still use the old feature "testlogserver.exe". Is it still recommended?
    - yep, always useful but that helps more with the filtering requests once they have been passed to the Filtering service running on the Web Security part of the product. If you need proxy specific troubleshooting then use the tools mentioned in this webinar.

25. When we tried to connect to this webinar, websense was blocking us. We have a websense content gateway with wccp. We had to bypass websense to connect. We are experiencing problems with other webinar technologies. Where would we go first to check why it is being blocked?
    - log a case with tech support please

26. Is there a background article available that explains how to enable decryption of https transaction? I don't understand how this is possible (how is it accomplished?). Does it involve a certificate installation on the clients that matches the Websense appliance?
    - WCG will act as a certificate authority for your clients, so you do need to deploy client certificates. Please search our knowledgebase for further information.