Quick Start 4: Identifying and Troubleshooting proxy issues for Websense Web Security Gateway

Date: March 20, 2013 at 8:30 A.M. PST (GMT-8)

Q: How do we perform these commands on the V10K appliances since we don't have actual root access to the directory structure?
A: Use of the Command Line Utility in the Appliance manager.

Q: Is it required to run content_line -x for all config files or is it for only records.config file changes?
A: You need only run the content_line -x command when modifying the records.config file. This command forces the system to re-read changes to the records.config file.

Q: If I am doing changes in filter.config or parent.config, is there any restarting or simply the WCG will re-read the config changes?
A: For the other config files, the GUI will prompt you if need to click on the restart. Note that the restart in Content Gateway manager does not restart the proxy. It forces a re-read of configuration files. It is typically used when making changes to the records.config file.

Q: Is there a way to view WCCP negotiation via the same methodology?
A: Yes, there is a debug tag for WCCP negotiation. It is wccp.*.

Q: When tagging, can you combine with | grep somehow to get the data you are interested in?
A: Yes, use tail or more along with grep to search for of interest.

Q: Is there a way to increase the capture bucket beyond 10000 packets?
A: By default, no limit is set for the amount of packet captures to be captured. You need the -C parameter to set a limit and create rolling packet captures.

Q: Which logging would we use to determine if we need to bypass IWA for specific third party apps' UA?
A: You can use the debug tag win.*|ntlm.* along with the extended.log (transaction logging). In addition, check the messages log. A failed authentication typically logs an entry in the messages log.

Q: If the WCG is deployed as cluster, the logs must be enabled in all nodes? The logs can be viewed from a single location?
A: Yes, if you want to see logs for all proxies, they must be enabled and viewed on that particular proxy. However, you can explicitly run traffic through one proxy to test and enable logging there and then isolate an issue on a single proxy.

Q: Will the rules entered in the filtering section still be logged, such as with IWA? A: If you are creating allow rules for IWA under filter.config, the traffic is still logged. However, no authentication and identification will be occurring.

March Webinar Question Log 2013

Q: How would I go about troubleshooting a site that has videos? The videos do not work, but there is no Websense block message displayed?
A: There are several steps you can take. If transparent, use ACLs to bypass and test the site to see if it plays. Next, try some scanning bypasses under scanning options in the TRITON Web Security management console. I like looking at the extended.log for any error message codes. Packet capture (tcpdump) will give you the most information.

Q: For cert errors - what's the difference between tunnel and allow?
A: With Allow, you still receive a block page. However, you have a button which will allow you to proceed through. If you tunnel, the certificate engine verification is bypassed and no block message is displayed.

Q: For the CIA site, this non-domain machine does not prompt for credentials?
A: The CIA site does not prompt for credentials. To access the site without a certificate error, you have to type www.cia.gov. This matches the common name displayed in the site's certificate. To display the certificate error in my demonstration, I deliberately typed cia.gov as to receive common name mismatch certificate error. The authentication prompt occurred simply because I was access the proxy via a workstation not part of the domain. The CIA site and the authentication prompt you saw are not related issues.

Q: What are the collateral effects if we set a range like 1025 to 65535 into tunnel ports? Can WCG identify the http protocol used into non-standard port and automatically tunnel that traffic?
A: Inputting a full range 1025 to 65535 has not been tested. However, if you enter non-standard ports to tunnel the traffic, WCG can do that.

Q: What is the difference between SSL incidents in WCG vs. SSL Decryption Bypass (Destination URLs) in Triton?
A: They both have similar functions in that decryption is bypassed. With SSL incidents you can add an individual URL to be bypassed, while SSL Decryption Bypass gives you the ability to bypass whole categories such as financial institutions.

Q: How can a customer clear the cache on WCG without requiring tech support access to the DOMs?
A: The cclear command is only available through tech support access to the DOMs. A feature request may be submitted to be added to the Command Line Interface.

Q: Can WCCP be set up to forward traffic for port 8080 to the proxy or will there be any issues? Most malware is starting to use this port to get around a proxy but it needs to be inspected.
A: It is best to block non-standard ports on the firewall. You may also modify the default proxy port.

Q: Logs can grow as you said. How do I reinitialize them/clear/wipe them in one shot?
A: You can remove logs in the Content Gateway manager. Login in and select Configure > My Proxy > Logs > System and remote the select log file to be deleted.

Q: Do you recommend doing the SSL decryption bypass before the SSL incidents in WCG?
A: This depends on what are trying to accomplish. If you have several financial institutions you need to bypass, it is best to use SSL decryption bypass to select the financial institution category. If you want to completely tunnel a specific URL so that it does not go through a Certificate Verification Engine or is not decrypted, then you can use the SSL incidents tunnel.

March Webinar Question Log

2013

Q: Is there a simple way to wipe the content filter database? Just to have it cleared from reports when doing certain testing?

A: Data is logged to SQL partitions. If you are testing don't need the data in the latest partition, you can archive or delete the partition through the TRITON management console under settings > logging. However, it may be easier to simply stop the Log Server service while testing. If Log Server is not running, then no data is captured and sent to SQL Server.

Q: Are there any filters that are setup in WireShark that will help with troubleshooting packet captures

A: The most common filters used for Wireshark are ip.addr, tcp.port, an http contains. Please watch the prior Webinar I referenced in my presentation. I did not mention Wireshark filters because the prior technician covered these details. He also provided debugging examples using another tool, which I did not mention. Please view the other webinar. You will find it very rewarding. Web Security Gateway - What to do when a Web site does not load as expected (November 09, 2011 Webinar)
http://www.websense.com/support/article/webinar/Webinar-Web-Security-Gateway-What-to-do-when-a-Web-site-does-not-load-as-expected

Q: How do you enable button to allow access to cia.gov website?

A: From the Content Gateway console, select Configure > SSL > Validation > Verification Bypass tab.

Q: How do you handle CPU spikes on content gateway software implementation?

A: This depends on what is causing the CPU spike and if it merits creating a hotfix. Is the spike happening during database updates, high production hours, or is there a specific process that is taking up all the memory? We also want to be sure that the server is meeting the minimum requirements. Are you running the latest release? Is your machine sized correctly for your network? If you are having CPU spikes, contact tech support so we can resolve such matters.

Q: Is this presentation available for download?

A: The following link is available to download now and will be available for about a week. It will also be available or our support page later today.

ftp://eng_public:websense@ftp.websense.com/2013_03_20_Mar_Webinar_v20_b.zip

March Webinar Question Log

2013

Q: Where can I get access to other webinars?

A: Please visit our support Web site. As shown below, you have two spots on the page to select Archived Webinars. http://www.websense.com/content/SupportWebinars.aspx#1