Quick Start 3: Installing and configuring Websense Web Security Gateway v7.7

Date: February 20, 2013 at 8:30AM PST (GMT-8)

Q: Does WCG support centos Linux?
A: Yes, CentOS is officially supported as a software installation for Websense v7.7. However, Websense suggests using Red Hat Enterprise because of the availability server OS support.

Q: If we install it on RHEL 5.8, is that ok? Or is it not at all recommended?
A: Installing Websense v7.7 on Red Hat 5.8 is not supported. The Installation and Deployment Center displays supported Red Hat operating system versions for specific Websense versions. Click here for system requirement details.

Q: If you have the Websense v5000 v2, the Content Gateway is already installed on the appliance, correct?
A: There are two V5000 installation types. One mode includes just the Websense security services without the Content Gateway. The other V-Series appliances mode included the Content Gateway. You can verify your appliance mode type via the Appliance manager. If you do not have the Content Gateway product, contact sales to obtain a Websense Security Gateway subscription key and then re-image your appliance with the Security Gateway image.

Q: Is it ok to comment/remove the last line ::1 localhost?
A: Usually items are not removed. This line is essential if you are using IPv6. It defines the loopback IPv6 address. I would assume you could safely comment out the line if you are also disabling the IPv6 TCP stack on the server.

Q: Disabling the SELinux and stopping the IPTables are still best security practices before installing the WWS/WCG, correct?
A: Before installing Content Gateway, it is important to ensure SELinux is not active. You may either set it to permissive or disable it entirely. If you are not familiar with IPTables, it is far easier to stop the service. By default, when running, the firewall blocks ports Websense requires for installation and operations. However, after installing, best practice is having a firewall to protect your server. The firewall was disabled for use in the Webinar, but you should just allow the Websense ports within IPTables. The deployment guide has a list of ports which you can allow. Also, the "How do I configure IPTables to harden the Content Gateway host system?" article will be very helpful.

Q: Is it ok to enable SELinux after installing? If yes, is there any impact in functionality?
A: To avoid any issues, I leave SELinux disabled after installation. This is typically recommended. We have seen cases in tech support where the Content Gateway manager pages could not be displayed due to this feature being enabled.

Q: For v7.7.3 and explicit proxy, is it best practice to use IP Address or DNS name for Proxy Server?
A: Either one can be used and will work correctly. However, there are pros and cons for using one over the other. A DNS name allows you flexibility, for instance, when migrating between Websense installations, etc. However, a DNS entry needs to be resolved and you are dependent on DNS to return the IP address. Since most administrators push out the setting via a GPO, pushing out a VIP address that represent multiple Content Gateways in my preferred suggestions.

February Webinar Question Log 2013

Q: Since we are able to get the block page pop-up for Remote Filtering Client for HTTPS request, is there a way to get the HTTPS block page without enabling the SSL Manager and without using the Network Agent?
A: Network Agent cannot deliver a block page; however, the Remote Filtering Client software does send a generic block message for HTTPS. The SSL manager needs to be enabled, within the Content Gateway, for the HTTPS block page to display. This is a known behavior and feature requests have been submitted. When an end user is in a secure (HTTPS) Web connection, it is impossible to inject a block page unless it originates from a proxy that is performing SSL inspection. It would be a serious security flaw if an outside service could information into a secure connection. When you use a proxy, and SSL inspection is enabled, then when a block page is necessary, the proxy sends it. This is possible because it is acting as a man-in-the-middle and has sight into the secure connection.

Q: In my organization I do not have direct internet connection for WCG so I need to upstream it through another proxy, how do you do the upstream for WCG?
A: No problem, Content Gateway can act as a parent/child proxy. More information can be found here:

- Can WCG forward traffic to a parent proxy or other upstream device?
- WCG as child proxy passing credentials to parent proxy.

Q: For clustering, is the multicast route really required for V5K/V10K appliances?
A: Yes the multicast route is required. You can cluster via a crossover cable over the P2 interfaces.

Q: Can you demonstrate the VIP by stopping the WCG service in one of the Proxy to understand better?
A: Good suggestion. Sorry I did not have time to demonstrate your request during the presentation. Rest assured, in preparing for my demonstration, I did test your scenario by stopping one proxy. My first step was to determine which proxy was actually doing the work. Recall, VIP allows for fail over, not load balancing. Once I located the active proxy, I stopped it. The remaining proxy picked up filtering obligation with an issue. It worked great. Therefore, essentially, if the primary Content Gateway goes down, then it can take a minute for connections to go through the secondary Content Gateway. Clients are still pointed to the VIP, so they will be redirected to the secondary proxy. Therefore a VIP failover occurs.

Q: Can we view this presentation again?
A: Yes, the Webinar presentation will be posted within two hours (Click here). In roughly a week from today, we will post the answers to questions asked in the Webinar.

Q: Some of the configurations replicated in cluster. And some (ARM) are not. Need clarity?
A: Correct, not all configurations are replicated (e.g. ARM, joining domain in IWA) within the management cluster. This is by design. Some settings need to be isolated to the particular proxy. Other settings, such as VIP, fully replicate across all proxies in the cluster. See the specific feature you are interested in enabling. The help guide for Content Gateway provides details about what is replicated.

Q: Can we cluster two WCG across to different sites. Meaning both WCGs would be in two different subnets? For instance, your primary site and DR site?
A: Our recommendation is the WCGs need to be layer 2 adjacent. This may not be the case if they are located in two different sites as you may be traversing through a mesh of routers (e.g. MPLS network). It has been seen where special configurations have been done in order to get this working, but the results were inconclusive.

February Webinar Question Log 2013

Q: How does the DNS proxy concept work? Will the proxy stores all the zone files? Or just cached content? How about the zone changes?
A: The DNS proxy is used for caching DNS requests. Essentially, the proxy keep track of A-record request. It retains the results for five minutes before letting the information expire. Here is a good link that explains DNS proxy caching in greater detail: DNS Proxy Caching

Q: Will restarting the Content Gateway in the TAB restart the WCGAdmin service or does it just read the config without interrupting the Internet access?
A: The WCGAdmin service is not restarted, so Internet access is not interrupted. Selecting the Restart button within the Content Gateway manager essentially forces the proxy to re-reads the configuration files.

Q: As my understanding, SSL inspection is inspecting SSL sites. The Websense root-CA certificate needs to be installed in all user machines. If not installed, the WCG will not allow SSL traffic, correct?
A: Yes and no. Let answer you two questions separately.

- The certificate needs to install on all clients in your network. If you have an existing root-CA, you can configure a subCA: SSL SubCA This whole certificate business, of creating a trust between you users and the proxy, has two concepts. First idea is allowing the proxy to act as a middleman, such that it actually makes SSL requests on behalf of your users. Secondly, as is a trusted participant within the SSL connection, it can inspect the traffic for malicious content. Additionally, if you have the Content Verification Engine (CVE) enabled, it will validate certificates it sees coming in from external sites.
- Concerning, your second question, "WCG does not allow SSL traffic when SSL inspection is not enabled". This is not the case. The Content Gateway does allow and it processes HTTPS traffic when SSL inspection not enabled. However, in this condition, the proxy can only inspect the packet header. The secure packet cannot be open to reveal the actual URL. The proxy makes security decisions on the destination IP address in the packet header. As such, the proxy is limited in the depth of analysis it can provide to protect your network. Enabling the SSL engine and deploying a root certificate allows the proxy to fully inspect all SSL traffic.

Q: If you run the filtering and policy services on the same server as the Content Gateway, can you do logging?
A: This placement of Websense components that you describe has no effect on logging. However, it is best practice to install Content Gateway alone—without other Websense components. The reason being, your users will experience quicker browsing if the Content Gateway does not have to contend or share memory and CPU resources. The Content Gateway server is the gateway device in which all your users must pass through to reach the Internet. The quicker the proxy can respond, the happier your end users are.

Q: Can I install WCG with Web Filter?
A: If you are asking a subscription question, then WCG only works with Web Security Gateway subscriptions. If you were asking about installing the WCG component with the Filtering Service component, then look to the previous question for your answer.

Q: When configuring WCCP with clustering and virtual IP, what IP address is configured in the FW? Is it the virtual IP or the individual IPs of the V5Ks?
A: It will be the Virtual IP. However, as an alternative WCCP will recognize both cache engines and if one goes down, traffic will continue to be directed to the working proxy. WCCP was designed for working with cache engines.

February Webinar Question Log 2013

Q: Will you have future broadcast on using PAC files?
A: A presentation on PAC files is not scheduled at this point; however, as I participate in writing and updating knowledge base articles for the department, it is a subject I have schedule to review. In respect to working with PAC files, I will be reviewing, consolidation, and adding information to our knowledge base over the next two months.

Q: Can we get any video about configuration WCG?
A: We have some archived Webinars on various issues working with the Content Gateway. Next month's Webinar will show you more of the interface as I show you how to analyze and troubleshoot proxy issues. While videos are wonderful for seeing the interface, you will find the WCG help guide very informative. Just look up the feature you are interested in, read the material, then jump into the console and see the settings first hand. I use these documents to learn and re-fresh my knowledge on WCG features.

Q: Why would you use the DNS redirect? What is its purpose?
A: This feature provides DNS caching. It is an underemployed option. Not many customers use it. I believe is should be used more. It caches A-records, which results in reducing latency. When filtered via the proxy, your users will see a bit faster response. More information can be found: DNS Proxy Catching

Q: Do I need to enable clustering with two Content Gateways?
A: Clustering is not required if you have multiple Content Gateways. Clustering has benefits. It allows you to manage multiple nodes from a single interface. Most management changes replicate to every node participating in the cluster.

Q: Where is the utility ccleaner available for download?
A: It is free to download. I downloaded it from www.cnet.com. I have been using it for years without an issue. As with any utility, you need to be careful. Originally, I discovered it while working with a customer trying to resolve an issue. When installing it, I deselect the option to install the Google Toolbar.

Q: We need to login on WCG with NT ID for management purposes. How can we configure this?
A: You can log in locally or with a network account.

- Local Login access can be configured under Content Gateway manager under Content Gateway manager > Configure > My Proxy > UI Setup > Login.
- Network accounts can be configured in the TRITON – Manager Settings and be used as a Single Sign-on for Content Gateway manager.

Q: Will WCG support the protocol traffic other than http and https?
A: WCG supports FTP traffic as well. It also accepts DNS traffic, but this is for DNS caching. To control other protocols, your firewall should be configured to deny all traffic with the exception of the Content Gateway. However, in the real world you will have to open some ports for other protocols. Use Websense Network Agent to monitor you non-HTTP traffic. The purpose of Network Agent is to monitor and enforce security policies for non-HTTP protocols.