

**Webinar Title:** Jump Start Part 2: Identifying and Troubleshooting filtering issues for Websense Web Security

**Date:** October 27, 2010

- 1. In this instance with an actual IP address that has to be allowed, is there any way to have it perform a reverse lookup and see what the domain name is via that method, then apply the proper category? The concern here is if/when those specific IP addresses change.**

Unfortunately, due to the nature of HTTPS traffic, a Websense installation that is not integrated with a proxy device of some nature will be unable to determine the URL of HTTPS traffic; all re-categorization must be done by IP. Changes to the IP of the origin server would require changing the re-categorization.

- 2. Is there any better way, other than trial and error, to determine the list of IP addresses used by a URL. In other words, can Websense learn the multiple IPs from DNS answers that show the list?**

The TestLogServer tool displays all of the relevant information about a site on one screen; this would be the best way to determine the specific IP being requested for an HTTPS site to facilitate re-categorization.

- 3. The unfiltered URLs/custom categories which are added I assume are added to the policy database, what is the procedure to export this information for backup purposes if a server was needed to be rebuilt?**

The entirety of your policy database can be backed up using the wsbackup utility, and then restored to a new server.

- 4. Can we unblock part of a site - a training video for YouTube but not the whole YouTube site**

As long as Websense can identify the specific URL being requested, we should be able to add specific exceptions to permit one video while denying access to YouTube as a whole.

- 5. Can I report on a policy?**

Websense cannot report on a specific policy. We can run reports on such things as users, groups, Active Directory objects, specific sites, or category disposition (blocked/permitted).

- 6. The "view source" method to find group & policy info seems rather convoluted. Are there plans to make this easier (e.g. a simple link on the page) or can the "more information" page be customized to display this?**

There are no plans to make changes to the "view source" method. There are KBs available to assist in the customization of block pages, but Websense Technicians are unable to assist in this customization.

- 7. In reporting, when I attempt a report on groups, much more than the Client groups appear, ie. Domain User, Administrators, and other security groups. Can I change this to only review the Client Groups?**

Unfortunately not, Websense maintains all the information about the user that was filtered, including any groups they are in, not only the groups that are added to the clients list.

**8. How often does Websense sync with Active Directory in reference to AD groups?**

Websense syncs with Active Directory on user group information every 4 hours.

**9. Can the filtering groups be defined in Active Directory to be used by Websense? In other words, do I need to duplicate group structures in Websense?**

Websense can be configured to be able to browse your tree and use your currently configured user and group information to filter traffic.

**10. What is the purpose of "use most restrictive" filtering?**

The checkbox for "Use most restrictive filtering" changes how Websense will filter traffic for a user that is in 2 different groups, with 2 different policies applied to them.

**11. Can I setup Websense to not filter any traffic to the server that hosts an application?**

Websense can be configured to ignore traffic from any source device on your network. Consult the integration guide or guide on Network Agent for your version of Websense to learn how to do this.

**12. We have an internal application that we use at our firm. It runs as an executable from a mapped network drive. This application locks up for our users when Websense filtering is enabled. Where do I start to troubleshoot this?**

Using the TestLogServer tool or ConsoleClient utility should help shed some light on how this application is getting out of your network. If it makes a GET request to a site on port 80 or 443, there is a chance Websense sees this traffic and could be blocking it.

**13. Does TestLogServer show all protocols that are being passed?**

By default, not all protocols are set to be logged. If a protocol is set to be logged in the protocol filter list, then TestLogServer would see that protocol traffic and display it in the window.

**14. Is it possible to select only some users to be logged by the Log Server?**

No, if a user is being filtered, they will be logged. We can configure specific categories to be not logged, but not usernames.

**15. During a database update, the filter stops filtering. Is there a way to continue the filtering during the load or control when the database updates?**

Database updates, by default, should download very late at night. The database does need to reload, however, any time the Filtering Service is restarted. To prevent incorrect filtering, limit these restarts to times of low activity on your network.

**16. What are your thoughts on using a span port in conjunction with ASA?**

Since integration with an ASA will not provide us with information on the bandwidth being used, nor will it provide us traffic that is not on ports 80 or 443, using a port span in conjunction with an ASA integration helps to ensure we capture and can filter all of your traffic.

**17. Can you apply policy for a computer name instead of IP?**

No, only usernames, groups, IP addresses, or network ranges can have policies applied to them.

**18. When using TestLogServer, does one need to stop any services as one did in previous versions of Websense?**

Yes, stopping the log server is normally required unless following the steps outlined in the Webinar.

**19. What happens when you have a computer that is run using 2 user IDs? The user logs into the computer and performs a "run as" for the Web browser. Our IT staff uses this scenario. If you have different policies for each of the user IDs, which one is used to assign the policy used?**

If the username being used in the 'Run As' window is a domain account, that authentication would trigger a session to be created on the domain controller, which the DC Agent would then pick up and use as the username for policy acquisition.

**20. Will users notice any slowness issues when using integrated mode?**

There would be latency added when using integrated mode when compared to standalone mode, however, unless the integration device is severely overtaxed, the amount of latency should be imperceptible to the end user.

**21. Are sites that are added to the user-defined categories excluded from real-time scanning?**

No, sites going through the Content Gateway proxy would be scanned using Real-Time scanning.

**22. What is the precedence of filtering? In our environment, we have 3 policies that are applied and wondering which one "wins" and is applied. Basically, we have a laptop as a public kiosk for library users. So, there is a user account policy in Websense Manager, an IP-based policy and the laptop is also included in a subnet-based policy.**

Websense first looks at policies applied to usernames, then policies applied to specific IP addresses, then policies applied to network ranges, then policies applied to groups.

**23. Can we customize block pages for multiple languages?**

Yes, there are localization versions of the block page in the C:\Program Files\Websense\Block Pages folder. Each of those can be customized with their own custom block page.