Using GREP to filter the access logs

Contents

Question:

Environment: Cisco Web Security Appliance (WSA), all versions of AsyncOS

How can I search the access logs on the S-series appliance?

From the command line interface of the Cisco Web Security Appliance, you can use the **grep** command to filter the access logs and determine what is being blocked. Here is an example to show all that is being blocked:

```
-----------------------------------------
TestS650.wsa.com ()> grep

Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
<...>
18. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs"
Retrieval: FTP Poll

Enter the number of the log you wish to grep.
[]> 1

Enter the regular expression to grep.
[]> BLOCK_

Do you want this search to be case insensitive? [Y]> n

Do you want to tail the logs? [N]> n

Do you want to paginate the output? [N]> n

(entries will be displayed)
-----------------------------------------
```

For the regular expression question, you can enter **BLOCK_** (without the quotes) to show every request that WSA has blocked. (Warning: this list can be very long) .

You can also enter parts of site URL if you want to display access long entries related to a specific site. For example - Entering **windowsupdate** for the regular expression will show you all access log entries containing the Windows Update URL of windowsupdate.microsoft.com.

Getting a little more advanced, if you wanted to display access log entries for a site with windowsupdate in the URL, which were also blocked, you could use the regular expression **windowsupdate.*BLOCK_**.