

Troubleshooting

Realtime Log Viewer

View live filter traffic data on this DrawBridge, system-wide. Use requires `System Owner` or higher permission levels.

Individual Remote device Realtime Logs may be viewed by the `Company Owner` permission-level by visiting the Remote Device record , and clicking **View Realtime Log Lines** in the record hamburger menu. For Local Devices go to the `Content Filter App` , select `Troubleshooting` and then **Realtime Log Viewer**.

Display Filters

- `Userip` applies to the Access Log and TLS Log only
- `Pattern` applies to any of the three logs
- Actions `Allow` , `Block` , `Block Invisible` , and `SSLBump` only apply to the Access Log

Log Types

- **Access Log:** Live web traffic classification activity
- **TLS Log:** Live information TLS sessions handled by the DrawBridge, including errors when the session establishment was not successful. Traffic that is `SSLbypassed` will not be visible here, because the DrawBridge is not intercepting and handling those sessions.
- **Errors Log:** Live errors and remote device authentication data

Explaining the Filter Actions

Filter Action	About
<code>Allow</code>	The DrawBridge allowed the request after analysis
<code>Block</code>	The DrawBridge blocked the request after analysis, and served a block page
<code>Block Invisible</code>	The DrawBridge blocked the request after analysis, and served an invisible pixel (used primarily when blocking advertisements)
<code>SSLBump</code>	The DrawBridge intercepted the initiation of a TLS session and took over as Man-in-the-Middle.

Note for troubleshooting: When diagnosing a strange connection issue with a particular website or service, **be sure** to toggle on the `SSLBump` display filter -- sometimes a web server will abandon a connection when the DrawBridge intercepts the session. In such cases, you'll see one or more `sslbump` loglines, but no subsequent, `allow` or `block` lines as would typically be the case.

If the service *must work*, then the best solution is to put the domain in the **Bypass Filter** policy for the Company in question. Note that this does disable DrawBridge filtering on that domain, so use responsibly.

System Update

Regenerate Config Files

Filter changes are normally saved to disk when clicking the Reload button in the banner in DrawBridge.

Manually running this command should only be done when the filter behavior does not match current settings in DrawBridge, such as when output from the Realtime Log Viewer indicates that policy changes have not yet taken effect.

Restart Redwood

Filter adjustments take effect after clicking the Reload button in DrawBridge. Reloading the config files is significantly faster than restarting the filter process, and does not disrupt active network connections.

Use this option if you've changed the Port number for a Remote Device record, or if there's configuration setting that doesn't seem to match your expectations.

Update Classifier Patterns

Redwood receives periodic classification updates throughout the day to enhance accuracy in filtering and reporting. Click below to manually check for updates. Any available updates will automatically take effect.

This command is useful only if your filter administrator requests that it be run.

Revision #7

Created 15 September 2022 14:17:51 by Marvin M.

Updated 16 April 2024 19:51:57 by jay@compassfoundation.io