2016 Release 2 Notes for Forcepoint Cloud Web Protection Solutions

Cloud Web Protection Solutions | 20-May-2016

2016 Release 2 of our web protection products offers new features and product corrections:

What's new in 2016 Release 2?

Cloud Web Protection Solutions | 20-May-2016

File Sandbox reporting options

For organizations whose accounts include the Web Sandbox Module, a new attribute is available in the Report Builder and Transaction Viewer. In addition, 2 new sandboxing reports have been added to the Report Catalog.

Report Builder and Transaction Viewer

File Sandbox Status, found under **Security** in the Attributes list, can be used to find information about files submitted for sandboxing analysis. There are 3 possible status values:

- **Malicious** indicates that sandbox analysis detected potentially damaging, malicious behavior.
- **No threat detected** indicates that sandbox analysis did not detect any malicious behavior.
- **Pending** indicates that a file has been submitted to the sandbox and is queued for analysis.

When sandboxing analysis is performed for one or more files associated with a transaction, the Transaction Details pane in the Transaction Viewer includes a **File Sandbox** tab. The tab lists each file submitted for sandbox analysis, as well as its status. If one or more of the files associated with the transaction is found to be malicious, the File Sandbox tab label is displayed in red.

Report Catalog

The **Web > Security** folder in the Report Catalog contains two new reports:

- **Detailed File Sandboxing Report** provides details about files downloaded by end users that were sent for sandbox analysis in the last 7 days.
- **Top File Sandboxing Results** gives an overview of the top results returned by sandbox analysis in the last 7 days.

Firewall redirect supports HTTPS and non-proxied destinations

The Firewall Redirect connection method can be used to transparently redirect web traffic from offices to the cloud service. This feature has been enhanced to support:

- HTTPS traffic
- Non-proxied destinations configured both on the **Web** > **Bypass Settings** > **Proxy Bypass** page, and within web security policies

Administrators in environments that use firewall redirect can now configure domains (such as those used by Windows Update) to bypass filtering.

Important

Currently, the firewall redirect feature does not provide automatic data center failover. Where transparent redirect and automatic failover is required, please use the IPsec VPN connection method. Contact Technical Support for details.

Resolved and known issues

Cloud Web Protection Solutions | 20-May-2016

Resolved issues

- The cloud service now accepts **.online** as a valid top-level domain.
- The EPS (Encapsulated PostScript) format has been reclassified as an image file type. It will no longer be blocked when executable file blocking is enabled.
- The **Web > Policies > Time Access Exceptions** page in the cloud portal now links to the correct Help page.

Known issues

The following are known issues in this version of the cloud web protection products:

IPsec tunneling

- For SSL decryption to work with IPsec tunneling, SSLv3 must be disabled in Internet Explorer.
- Basic authentication does not work for iTunes with IPsec tunneling.
- Using authentication bypass settings to force NTLM, basic authentication, or the welcome page does not work with IPsec tunneling if a URL condition is present.
- Cisco ASA firewalls earlier than version 9.1 with multiple security contexts enabled cannot use IPsec tunneling.
- NTLM for non-domain users is not supported.
- Some web pages do not load properly in Safari after successful user authentication. The workaround for this is to ensure the Block cookies option is set to Never in Safari's privacy preferences.

Authentication

- If an end user is browsing with Internet Explorer and their system clock is set to a future time or date, session-based authentication fails and is repeatedly requested because IE considers the session cookie to be expired. To avoid this, ensure the system clock is set correctly.
- If a roaming user authenticates using single sign-on with Oracle Identity Federation, the secure authentication form is intermittently displayed if the session times out.

- Firefox sometimes fails to load the page correctly when an end user re-authenticates after session timeout. This occurs only if the session timeout is set to a very short time period.
- The New Tab page in Chrome displays “Internal Server Error” when a user authenticates using a cookie-based method (secure form authentication or single sign-on). To work around this, open a new tab in the browser and re-authenticate to browse successfully.
- If a roaming user authenticates using single sign-on with a supported provider, and their policy also mandates an Acceptable Use Policy (AUP), the compliance page appears only on the second site they browse to, and not on the first site which triggered their authentication.
- This issue relates to the cloud and hybrid proxy. When using Internet Explorer, users may receive the welcome page for basic authentication instead of the welcome page for secure form-based authentication after the secure form-based authentication session expires. They can either restart the browser or browse to a different site.

i-Series appliances

- In cases where the appliance self-signed certificate is used or when the CA certificate is not loaded on clients, Chrome blocks the connection and displays an error page.

  To proceed past this error page, ensure the browser page is the active window, and then type **proceed**. For Chrome versions 33 and 34, type **danger**.

  To prevent this issue occurring, end users should not use the appliance self-signed certificate and should load the CA on their clients.
- The YouTube for Schools feature does not work for HTTPS sites. To work around this, you can redirect this traffic to the cloud: ensure you enable SSL decryption in your policy and under SSL Decryption Categories, set the YouTube category to Decrypt.
- The appliance does not currently support authentication decryption bypass for custom categories.
- When using a Windows XP machine with Internet Explorer 8 (or below), HTTPS connections are not supported on i-Series appliances.
- If you add a custom protocol with a name containing non-ASCII characters, an error occurs on the appliance and the new protocol is not added.
- The appliance does not support browsing directly to full URLs (i.e., those including a full path to a specific page) in custom categories for SSL traffic. Using the host name only is supported.
- Google redirect does not work correctly if a user browses to http://www.google.com and Google does not automatically change this to https://www.google.com. In this case, traffic is not redirected to the cloud service and Google applies its own redirect to the appropriate site for the country it detects, rather than the options set in the cloud portal. If the country site selected by Google conflicts with your cloud settings, add “google.com” to the **Always**

analyze list on the Web Content & Security tab to ensure traffic redirection to the cloud.

Endpoint

- When both the Direct Connect and Proxy Connect endpoint clients are enabled for an account, and auto-upgrade is enabled, machines with Direct Connect endpoint client 1.5.8.1.3255 download (but do not install) the latest version of the Proxy Connect endpoint when checking for updates.
- The Endpoint Auditing report has the following known issues:
  - All times in the report are based on the time zone of the machine used to view the report, rather than the end-user machine on which the endpoint is installed.
  - If communication to the endpoint client machine is lost or the machine enters suspend or hibernate mode, this change of state is not reflected in the report.
  - If an end-user machine is shut down, the endpoint is automatically enabled on restart regardless of its previous state, and this is not reflected in the report.
  - If the endpoint is automatically installed from the cloud and then immediately disabled, end user details are not associated with a policy, and the disable action is not reflected in the report until the endpoint is re-enabled and the end user starts browsing.
  - When an endpoint version is upgraded, either manually or via GPO, the endpoint is enabled even if it was previously disabled. This is not reflected in the report.
- When users install an up-to-date version of Windows endpoint, the endpoint summary report shows the Windows endpoint version as outdated, because the Mac endpoint version has a higher number than the Windows version.
- On machines where the Mac endpoint is installed, for certain types of users (e.g., root), it looks like they can edit the network proxies page. However, any changes made here are not saved. The endpoint's resistance to tampering continues to work.
- It is possible to delete the Mac endpoint in the System Preferences pane. This will not affect the operation of the endpoint. If this occurs, use the command line tools instead of the user interface to get the debug logs and to uninstall the endpoint.

  To have the endpoint re-appear in System Preferences, copy "/Library/PreferencePanes/WebsenseEndpoint.prefPane" to the same directory from another machine on which the Mac endpoint is installed.

Policies

- For users whose organizations choose to display the acceptable use policy compliance page, this page appears for each different browser they use within the frequency period selected (1, 7 or 30 days). For example, if they browse using Internet Explorer and Chrome within the same time period, the page appears

twice, and they must agree to accept the page twice. Note that when using the endpoint auto-install feature, this same issue occurs.

- The compliance page appears the first time an end user browses to an HTTP site and does not appear if the user browses to HTTPS or FTP sites. Note that when using the endpoint auto-install feature, this same issue occurs.
- In the File Blocking tab, file extensions for HTTPS remain blocked even if they are set to Allow.
- End users may have to clear their cache for the Google redirect feature to work correctly.