Questions Log from January Webinar

Q: Will enabling SSL Decryption increase the amount of logging data going to the database?

A: Yes, it may increase the log records as one HTTPS secure session may have multiple URLS inside the stream, which will result in more log records being inserted into the database

Q: If I have SSL Decryption disabled, will Blocking the Social Networking category still block a user from visiting https://www.facebook.com, for example?

A: Yes, it will still block users from accessing the HTTPS version of a website within the Social Networking category, however the user may receive a 'page cannot be displayed' message rather than the normal Websense block page due to the modern security restrictions as discussed in the Webinar.

Q: Is there any way for Websense to inspect Skype encrypted traffic to see potentially malicious content/files?

A: This will be covered later on but the problem with Skype is that whilst it says it uses SSL it does not conform to the usual SSL RFC's and does not negotiate a SSL channel with proper SSL handshakes where certificates are exchanged. This means that when Skype is used with SSL decryption (as you can imagine using a SSL engine that abides by the SSL RFC standards) that Skype then fails to connect. We have a tunnel Skype option but this means that this bypasses the SSL decryption but allows Skype to connect. At the moment there is not anything that can be done about this due to the way that Skype works

Q: What if the remote website presents an error related to a possible man-in-the-middle attack when using an internal SSL cert with Websense?

A: When using SSL decryption there are essentially two connections, client to proxy and then proxy to site. The self-signed certificate is only used between client and proxy. Similar to internet explorer the WCG has a list of trusted root certificates. These are used when talking to the end site. The self-signed certificate or your sub CA cert is never presented to the end website.

Q: What can we do with non-browser applications that fail even when tunneled, bypassed, etc, but work when going direct (bypassing the proxy)?

A: If adding them correctly to SSL Decryption Bypass or an SSL Incident tunnel does not resolve the issue, and you can find nothing to explain why in the Websense online resources, analyzing a packet capture of the traffic on the Content Gateway in Wireshark, along with log information, can help determine the cause. If you are still unable to resolve the issue, you can open a Support case and one of our engineers will be happy to provide assistance.

Q: Have you had any Defense agencies using SSL decryption?

A: As with public and private companies, government departments around the world use Websense products. While intended to provide security for users within networks, Websense has a strict policy regarding the use of its products for government-led censorship. More information on this policy can be found at http://www.websense.com/content/censorship-policy.aspx

Q: Is the SSL Incident option only available within WCG 7.7?

A: SSL incidents and validation are available in all supported versions

Q: Can WCG certificates be installed on mobile devices?

A: Yes, providing your mobile device operating system allows installation of third-party *.cer certificates. Websense's TRITON Mobile Security (TMS) is designed for managing mobile devices:
http://www.websense.com/content/Regional/UnitedKingdom/triton-mobile-security-features.aspx

Q: Is there any drawback if we enable CVE?

A: The Certificate Verification Engine (CVE) should be enabled when SSL decryption is being used. It does not place an unnecessary burden on WCG.

Q: What are the pros and cons of using internal certificates versus using a third-party certificate?

A: With SSL decryption if you use a self-signed Certificate such as the one that comes with the default WCG installation you then have to deploy this out to all of your client machines. When using a SUB CA all of your client machines already trust your top level domain CA therefore once installed onto your WCG you do not need to deploy the certificate to your clients

Q: If CVE is not enabled on the WCG, is there any type of CRL performed at all or not?

A: No if the CVE is disabled the CRL checking is not performed

Q: When iTunes tries to download an application from Akamai, it fails. We can't put an IP or URL in bypass usually because it changes so much.

A: There are some Hotfixes that address this issue, related to TLS versions. Please check the Hotfixes you have installed.

Q: What is the risk with Subordinate CA with Microsoft CA?

A: The risk of using a sub CA (a CSR signed by Microsoft Certificate Services, as demonstrated in the webinar) is similar to using any other certificate. The main difference is how far up the certification chain the signing goes.

Q: Does the content gateway support SSL bypass based on browser type? If not, can this be submitted as an enhancement?

A: Currently no, this is not a feature that is present in the WCG proxy. If your organization would like this, please open a support case asking to have a Feature Request (FR) raised for this feature.

Q: Is it possible to use my own network CA certificate on my WCG?

A: According to best practices, we recommend that you create a Subordinate CA off of your top level root CA so that you can revoke the certificate if ever needed

Q: With SSL Decryption disabled, if a website is in a category that is Blocked will the website still be blocked?

A: Yes, with SSL Decryption disabled the user will get blocked but the client may receive a ‘page cannot be displayed’ message rather than the block page