Brian May
3/13/19

SSL Decryption How, When, and Why

Prior to diving into why, how, and when Secure Socket Layer (SSL) decryption should be deployed in your enterprise environment, next generation firewalls (NGFW) must first be explained. In short a NGFW is a network appliance that packages together multiple security functions that range from firewall, IPS/IDS, URL filtering, spam filtering, antivirus, anti-spyware, VPN gateway, etc. The key feature that separates NGFW from legacy port based firewalls is that the network traffic is inspected at the application layer. Traditional port based firewalls could only apply security policies based on source, destination, and common port or port range. NGFW can identify applications such as DNS, Facebook, Teamviewer, or Netflix and apply policy to the identified application or group of applications based on the organizations network acceptable use policy. Subscriptions are paid to the vendor annually to provide continued support as the security landscape changes. For instance, it would be nearly impossible to known all new applications created daily and the security vulnerabilities of these apps. The NGFW vendor analyzes the application, assigns a threat rating, and creates a signature so the NGFW can identify the application in real time. For example, an administrator may choose to block any application with a threat level 5. The NGFW vendor writes a signature automatically updating the application list without intervention from the firewall administrator to block new applications with a threat level 5. Based on the current threats and abilities to port hop, it is in this author's opinion all organizations should have an application based NGFW. While I will not pitch a certain NGFW vendor, I will

recommend you research, compare, and demo the NGFW that best suits your enterprise environment. As of March 14, 2019, 49% of websites use SSL encryption via https w3techs.com, w3techs.com is keeping a live tally of this trend. Palo Alto Networks reports that Gartner predicts 80% of network traffic by the end 2019 will be encrypted via SSL ("Decryption Best Practices," 2018). This trend to encrypt all web traffic has its pros and cons, as I will explain later.

When determining how to implement SSL decryption the NGFW would need to integrate with an internal public key infrastructure (PKI) infrastructure to assist with SSL decryption. An internal certificate authority or PKI infrastructure is configured for domain PCs to trust the NGFW. After that the NGFW has a PEM file uploaded to establish the trust between the NGFW and CA. From front to back the SSL decryption connection flows as follows: The user requests an SSL connection via the browser. The browser trusts the NGFW via the internal CA and PKI infrastructure, then the NGFW reaches out to the https source to establish the secure encrypted connection. If the server certificate is signed by a CA that the firewall trusts and meets the policies and profiles you configure, the firewall generates an SSL Forward Trust copy of the server certificate and sends it to the client. Palo Alto Networks a NGFW vendor explain the PKI infrastructure as follows: *"If the server certificate is signed by a CA that the firewall does not trust, the firewall generates an SSL Forward Untrust copy of the server certificate and sends it to the client. The certificate copy the firewall generates and sends to the client contains extensions from the original server certificate and is called an impersonation certificate because it is not the server's actual certificate. If the firewall does not trust*

the server, the client sees a block page warning message that the site they're attempting to connect to is not trusted" ("SSL Forward Proxy," 2019). As you are deploying SSL decryption it is recommended to monitor and record baseline CPU statistics for your NGFW, and then deploy SSL decryption slowly to different networks to test the CPU load from decryption. Some vendors include an SSL decryption exclusion list that is predefined and updated automatically from the vendor, similar to a URL database update. The exclusion list includes site decryption commonly used sites that break decryption because of technical reasons such as pinned certificates and mutual authentication ("Palo Alto Networks Predefined Decryption Exclusions," 2019). Deploying SSL decryption may seem like a daunting task initially but if done methodically and with involvement of upper management you will greatly increase your chances of success.

SSL encryption is a great security measure for most cases as it secures your email login credentials, bank login sessions, online purchasing, etc. The major problem is cyber criminals are starting to use SSL decryption to their benefit to push malicious traffic across an SSL tunnel to compromise a victim. Ethics, accountability, and transparency should be taken into account when deploying an SSL decryption policy. Network traffic that should be decrypted would be presented for review, critique, and publically available for all users via a published policy. A presentation should be put together to include all URL categories that will not be decrypted and those that will be decrypted and presented to upper management for approval. Upper management could include but is not limited to Human Resources, Chief Information Officer, Public Information Officer, CEO, and possibly board

members. An initial standard can include but is not limited to excluding decryption of health and financial information. When users think of decryption or SSL inspection the initial knee jerk reaction could constitute invasion of privacy. The policy must be clearly written to explain that decryption is to protect the users, companies systems, and networks by blocking malware, URL, and any threat mitigated by the NGFW. Transparency of policy in a clear language should be presented so a non technical person can understand the reason SSL decryption is beneficial to them to better secure their network connection. BYOD (bring your own device) devices can be decrypted but this would be a more involved process that could include a NAC (network access control) and 802.1x authentication processes along with the CA certification install as an opt-in option for devices not owned by the company. Incorporating BYOD devices in your SSL decryption project could increase liability but cover you for due diligence efforts, so craft your security policy accordingly.

Why should an enterprise decrypt SSL traffic? Without decrypting the SSL session, policy cannot be applied to encrypted traffic. Traditionally, if I want to create a new application or service I would register a system, user, and port with Internet Assigned Numbers Authority (IANA). Port based firewall could allow or restrict traffic based on these common ports. Today, because applications created outpaced the available ports, an application or service can be written to run over any port. Once the SSL encryption takes place a port based or application based NGFW cannot apply security policies to protect the end user from attacks. Links from websites or emails including malware could freely pass through the SSL tunnel.

The remote website or application would be able to attack over the SSL tunnel circumventing the firewall all together. One example of malware using SSL to bypass a NGFW is the banking malware Trickbot. Trickbot uses social engineering and phishing to mimic banking emails with Microsoft office attachments that contain macros that download the Trickbot worm over SSL. Once Trickbot has compromised the machine command and control traffic is sent via SSL and injectDLL module is used to capture banking credentials from a browser. Even the most paranoid user would be unaware this is going on in the background. After a CPU baseline has been established the current CPU load while decrypting traffic may influence types of traffic or networks you choose to decrypt. For example, if the accounting network is more important to your organization than the HR network, you may choose to just decrypt the higher priority network depending on NGFW CPU load. The same can be said for email traffic versus news traffic. The give and take will depend on decryption versus performance and what your organization deems necessary. The performance measure by NSS labs includes the following: "On average, the 7 NGFW devices tested by NSS Labs experienced a performance loss of ~74% with 512b and 1024b (current industry standard) ciphers and ~81% loss with 2048b ciphers, which will become the industry standard by the end of 2013. ("NSS Labs," 2013)"

As the Internet becomes more and more encrypted, the way we secure our enterprise environment will evolve as all technology does. Black hats will not give up their day job finding vulnerabilities in software or network security policies for personal gain. Cybercrime is big business to the tune of 3 trillion globally in 2015 and is expected to rise to 6 trillion in 2021 ("Cybercrime Damages $6 Trillion By

2021," 2019). Please consider upgrading to an application based firewall if you haven't already done so and explore deploying SSL decryption in your environment with the help of your executive leadership. At the end of the day I hope to relay the importance of policy transparency to the end user and the need, not a want, for SSL decryption to better security your enterprise network.

Works Cited

Sanjana Jain, S. (2019, March 19). Why Google is Forcing You To Have SSL Certificates on Your Websites. Retrieved from https://serverguy.com/security/google-forcing-ssl-certificate-websites/

*Palo Alto Networks. (2018, December 11). *Decryption Best Practices*. Retrieved from https://docs.paloaltonetworks.com/best-practices/8-0/decryption-best-practices/decryption-best-practices#

*Palo Alto Networks. (2019, March 1). *Palo Alto Networks Predefined Decryption Exclusions*. Retrieved from https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/decryption/decryption-exclusions/palo-alto-networks-predefined-decryption-exclusions.html#

Cybercrime Damages $6 Trillion By 2021. (2019). Retrieved from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

*NSS Labs. (2019, April 10). NSS Labs Research Finds SSL Traffic Causes Significant Performance Problems for Next Generation Firewalls, Retrieved from http://link.galegroup.com/apps/doc/A333584656/ITBC?u=ncliveecu&sid=ITBC&xid=0cab03fe

*Palo Alto Networks. (2019, March 1). *SSL Forward Proxy*. Retrieved from https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/decryption/decryption-concepts/ssl-forward-proxy#