SSL Inspection

What's in your network?

The web is being encrypted at blinding speed as more and more websites are moving to HTTPS. Today more than 70% of all internet traffic is encrypted, helping to keep our data and private information secure. Studies suggest this number will increase to more than 80% by the end of the year; but, **is a "secure" website a "safe" website?**

Encryption does not necessarily mean that content is safe. Threat research shows that 68% of malware uses encryption to hide in the network and one third of malware uses encryption to access and infect the target.

How could this affect you?

If you are not performing SSL inspection or if SSL inspection is implemented improperly, your network security tools are only inspecting 30% of the traffic across your network. This alone is concerning; not to mention, for every malicious event detected by your security tools there are statistically twice as many hidden in SSL/TLS encrypted traffic. Here are a few risks involving SSL/TLS encryption.

- SSL encryption is used to hide dangerous content such as viruses, spyware and other malware.
- Attackers build their own websites with SSL encryption concealing activity within the infected host.
- Attackers inject their malicious content into well-known and trusted SSL-enabled sites.
- SSL can be used to hide data leakage, such as the transmission of sensitive or proprietary information.

Revealing the hidden traffic

AccessIT Group uses SSL inspection to gain visibility into the hidden traffic within your network and identify, classify, and inspect the packets for threats. The process is simple and can be performed by a variety of products like firewalls, Web Gateways, Application security and packet brokers. With a trusted root CA certificate and some extra computing power, you can decrypt the traffic, have it inspected, then re-encrypted before sending it on its way.

Next, we need to examine inbound and outbound traffic. Traditionally inbound traffic could be inspected by an Application Delivery Controller (ADC) and this method is widely used by many organizations as setup is straight forward and involves managing certificates you already own and use. Outbound traffic becomes more challenging as you now must proxy the outbound SSL request and pretend to be the destination to the user and the user to the destination.

Encrypted traffic is in your network.

Do you know what it's doing?

Challenges of SSL inspection

Decrypting and re-encrypting traffic is computationally intensive and many inspection tools are simply unable to decrypt at scale. Overall security appliances suffer a performance decrease of 80% when SSL inspection is enabled. This leads to oversizing a product for your network to handle the extra workload. Every tool that needs to inspect the traffic must be oversized as well as increasing the latency while decrypting and re-encrypting the traffic.

If that's not bad enough, the National Cybersecurity and Communications Integration Center published Technical Alert TA17-075A reporting that 58% of the devices used for SSL decryption have severe vulnerabilities. Many inspection devices do not properly verify the certificate chain of the server before re-encrypting the data, allowing for data intercept; and even more fail to forward certificate chain errors to the client, leaving the client blind about the authenticity of the server.

Now, with the newer TLS 1.3 being release and adopted by websites, older SSL inspection devices can no longer perform properly. TLS 1.3 is a fundamental change in the way HTTPS encryption is handled and Perfect Forward Secrecy (PFS) relies upon the Ephemeral Diffie-Hellman key exchange protocol generating a one-time key for each session. This means that since the exchange of static keys has been removed, passive mode decryption is no longer possible.

Where to decrypt traffic

A few years ago, the Next Generation Firewalls and Web Proxy devices were leading the charge to introduce SSL inspection for outbound traffic while ADC's continued to offer SSL Proxy capabilities for inbound traffic. With increased threats and a growing concern for security, the implementation of multiple security tools has given rise to visibility platforms that can process traffic either inline or from a tap. With their sheer compute and traffic handling capability, these devices can not only direct, route or hand off traffic to security appliances, but they can perform SSL decryption and re-encryption services for those same devices decreasing latency and complexity. Managing SSL encryption processes from a single platform simplifies the complexity of the process, as well as making it easier to implement new security tools to have visibility of that traffic.

So, tell me, what's in your network?

With encrypted traffic increasing at approximately 15% per year and currently approaching 80% of enterprise traffic, it is imperative that security organizations gain visibility into their own forgotten network – the dark space where encryption, once viewed as the best thing for web browsing, is being exploited and used to infiltrate and infect our networks. To ensure the continual protection of your network, embrace the changing technology, rather than employ an "if it's not broke don't fix it" approach. **AccessIT can help you evaluate your SSL inspection tools so that your network is not at risk and your team can rest assured the traffic passing through is safe.**