BIZCOMMUNITY

Encrypted traffic: making what's vulnerable more visible

By Simon McCollough

31 Oct 2018

Dealing with encrypted traffic can be complex, costly, and disruptive. The problem escalates immeasurably if you are operating blind to cyber threats, which is basically what businesses are doing without a comprehensive SSL/TLS strategy in place.

Regrettably, too many still misplace their trust in inadequate security solutions, often leaving IT departments with an unenviable choice: let the traffic go uninspected or suffer extreme application performance losses.

In the new age of digital consent and compliance, can you afford to expose vulnerable data to high risk due to operational myopia, which will damage your brand reputation and lose customer trust?

Simon McCollough is major channel account manager, F5 Networks

Bypassing traditional security

Encrypting data-in-transit with SSL/TLS is already standard practice. Important security initiatives, such as built-in web browser warnings and the EU General Data Protection Regulation (GDPR), have significantly improved privacy awareness and helped mitigate data breach magnitudes.

While this is all good news, cybercriminals will always find a way to hide threats within encrypted payloads or use encrypted channels to propagate malware and exfiltrate data. Traditional security inspection solutions are becoming an increasingly easy challenge to overcome.

Ostensibly, gaining full visibility into encrypted traffic is never easy. Most organisations typically lack a central control to implement decryption policies across the multiple security inspection devices commonly found in the security chain. Consequently, security teams resort to daisy-chaining devices or tedious manual configurations to support inspection activities, increasing latency, complexity, and risk. All too often, the provisioning of network and security services, such as firewalls and security gateways, can turn into a time-intensive and error-prone process if SSL inspections are in the mix.

What is encryption, how does it work and why is it important?

Carey van Vaanderen 6 Mar 2017

At the same time, eavesdropping and man-in-the-middle hijacks will continue to rise due to superannuated transport layer encryption standards still being in use, even though they have been officially retired as “broken”.

Many are also struggling to get the most out of the technology or understand how to best deploy it. Recent research from F5 Labs reveals that while 63% of surveyed business respondents use SSL/TLS encryption for their web applications, only 46% use it for the majority of their applications.

Furthermore, 47% of organisations said they use self-signed certificates, which reduces application trustworthiness. This is unacceptable. Security teams need to ensure all applications are running suitable levels of encryption and have adequate third-party signed certificates in place.

There is far too much confusion and bad practice out there. It’s high time businesses get their heads around growing SSL/TLS complexities, not to mention the associated impacts on data breaches, compliance, and privacy.

Improving your cryptographic posture

Fortunately, it is not all opaque doom and gloom. With the right encryption orchestrator solution, it is now possible to dramatically reduce the risk of encrypted attacks through dynamic service-chaining, which enables automatic insertion of physical or virtual security service appliances.

It is important to note that the best tools always balance app performance and risk mitigation, giving security teams all-encompassing visibility into encrypted traffic. This allows them to effectively manage and quickly respond to previously invisible threats. In addition, improved threat detection and attack remediation capabilities can improve overall operational efficiency across your entire application security infrastructure.

As a rule of thumb, your SSL/TLS strategy should be able to:

- Defend against encrypted threats by scaling SSL across multiple security devices blind to encrypted traffic

- Prevent data loss and ensure compliance by gaining visibility into all data connection points (inbound and outbound traffic)

- Have a single point of control across multiple security tools for greater efficiencies

- Prevent attacks by reducing risks of selective blind spots

- Reduce latency with high-performance decryption and encryption of inbound and outbound SSL/TLS traffic

- Leverage policy-based service chaining to drive greater efficiencies within your security stack

- Load balance between devices to minimise bottlenecks

- Reduce the administrative burden with centralised key management, saving considerable time and money by offloading SSL instead of terminating on the device itself

Securing tomorrow

The ultimate goal is to simplify the SSL/TLS management process, keeping data secure and gaining full visibility into encrypted traffic without compromising application speed or availability.

To do this, businesses need the ability to properly scan inbound and outbound traffic. Crucially, they have to vividly visualise and analyse the nature of today’s attacks vectors in order to secure their applications, which are by far the most valuable, data-laden assets at stake. Remember, there’s nowhere to hide when it comes to the cybercriminals’ encryption corruption. Now is the time to future-proof yourself against tomorrow’s threats.

ABOUT THE AUTHOR

Simon McCollough is major channel account manager, F5 Networks