LANCOM SYSTEMS

White Paper

Network visibility through DPI and encryption proxies

Role of encryption

Given that public Internet today is simply not imaginable without proper encryption (98 % of web traffic is encrypted and encrypted communication is the default in modern browsers), it is vital for any application to provide and employ proper encryption technologies. Encryption is necessary to protect the application's assets and its users.

This also explains the long track record of modern encryption, dating back to the inception of SSL 1.0 in 1994 almost 30 years ago. Approximately 20 years ago, AES was introduced into the standard, which dramatically increased the performance and applicability of the protocols. Today's standard is already the sixth iteration of standard, which was renamed from SSL to TLS halfway through.

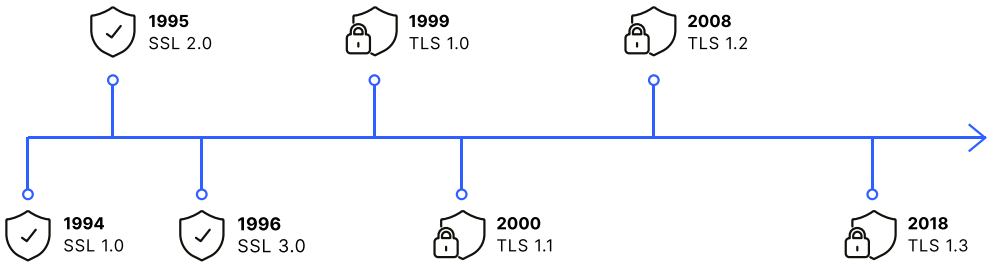

Figure 1:
Development SSL / TLS

Current trend

There are basically two trends in encryption nowadays: On the one hand, the amount of data being encrypted is constantly increasing. Traditionally, the actual data payloads were the main target of encryption, because they naturally held the sensitive data to begin with. Now, the definition of sensitive data has expanded to also include things like meta data of encrypted payloads. Consequently, metadata needs to be encrypted as well, thus spawning new technologies and protocols to support said encryption like TLS 1.3 or DoH.

This clearly indicates that we're headed towards an encrypt-everything society.

The other trend is the advent of quantum computing and the impact it has on current encryption methodologies and algorithms. This jeopardizes the current claim of confidentiality that encryption provides, especially since cryptographic systems are generally reluctant to change and no one can actually predict the evolution speed of quantum computing systems. Current encryption algorithms are vulnerable to quantum decryption techniques like Shor's algorithm as the quantum approach shifts the problem solving domain from the mathematical, prime factoring domain to the physical domain of creating qbits, thus being able to process all possible states simultaneously instead of sequentially.

However, not all is lost, as there are new or adapted traditional algorithms that cannot be broken by quantum approaches and are therefore dubbed post-quantum or quantum-safe encryption.

The positives

Encryption is an essential part of today's applications. Any type of modern communication depends on reliable and strong encryption to ensure the integrity and confidentiality of the information being transmitted. Encryption provides the secure envelope for this and should be considered as default modus operandi. You wouldn't send the information in question by postcard either, would you?

The negatives

Traditionally, middle boxes and technologies such as deep packet inspection (DPI) and application analysis have relied heavily on the meta data of the certificates used in SSL/TLS encrypted connections. With the advent of TLS 1.3, this information is no longer readily available as it is encrypted along with the regular payload, e.g. the SNI (Server Name Identifier) portion of the handshake. Therefore, other technologies are required to continue to provide the information needed for application control and management. These technologies include, for example, behavioral analysis of packet transport such as size, frequency, and timing properties.

Impact on visibility

Network visibility is vital to ensure and optimize the functionality and operation of any network.

This is especially true for financial institutions and other entities that have increased requirements regarding compliance and similar topics. The use of encryption has made all this invisible and inaccessible.

Therefore, the use of application and network proxies has become much more important. The necessary data to resolve the aforementioned tasks can only be obtained by decrypting the packets. On course, this must be done in a very secure and reliable way and requires profound expertise as well as changes to the network architecture, e.g. distribution of internal certificates and chains of trust to enable decryption and encryption at the proxy level.

Impact on routing, switching, load balancing, network slicing, etc?

Fundamental network functions such as routing and switching should hardly be affected. Of course, higher-level functions that depend on additional information, such

as application-based routing, suffer from the same drawbacks in terms of visibility. This leads to the following: The technology needs to evolve further to enable behavioral analysis, for example.

The impact on other functionalities needs be assessed on a case-by-case basis. For example, the impact on load balancing depends heavily on the technology used for the actual balancing. Round-robin methodologies should not be impacted at all, while methodologies that rely on additional data again suffer from the same consequences.

Security woes

This is again a two-fold situation. On the one hand, encryption significantly increases security by hiding information that can be used by adversaries to find vulnerabilities in the organization and exploit them. Additionally, with proper encryption techniques, it is nearly impossible to inject malicious data into trusted information streams.

On the other hand, the same technology can be used by adversaries to hide malware and malicious communications from scanning and detection systems. For example, a virus downloaded through a compromised server may not be detected by a scan engine if the connection is encrypted.

To counter this, organizations need to take special measures for their network infrastructure to keep their various security systems such as malware scanners, IDS / IPS engine, etc. operational.

What can be enterprises' biggest network-related issues with encrypted traffic?

The loss of visibility described above requires fundamental changes to the network infrastructure to keep services operational and maintain control of the network.

To regain visibility and full scanning potential, encrypted connections must be terminated at dedicated, trusted endpoints where traffic can be decrypted, scanned, and re-encrypted before being forwarded to its final destination.

This presents a challenge for the handling and distribution of the required certificates, especially in BYOD scenarios. Some applications even explicitly protect themselves against these techniques, as from their perspective they are indistinguishable from attacks. In these situations, CISOs and organizations are faced with the tough decision of either blocking the whole application or accepting the inherent dangers of black-box communications. When the choice is to block the application, application management solutions that work with encrypted traffic, e.g. DPI taking behavioral analysis into account, are of course the preferred solution.

The solution

Security solution providers are of course very well aware of the problems and challenges that companies face today. They strive to offer well-tailored solutions for the various encryption scenarios.

One valid solution is to use a state-of-the-art next-generation UTM firewall that features behavioral DPI and the necessary forward and reverse proxies to enable inspection. A comprehensive overview of the different functions and their impact can be found here: www. lancom-systems.com/products/security

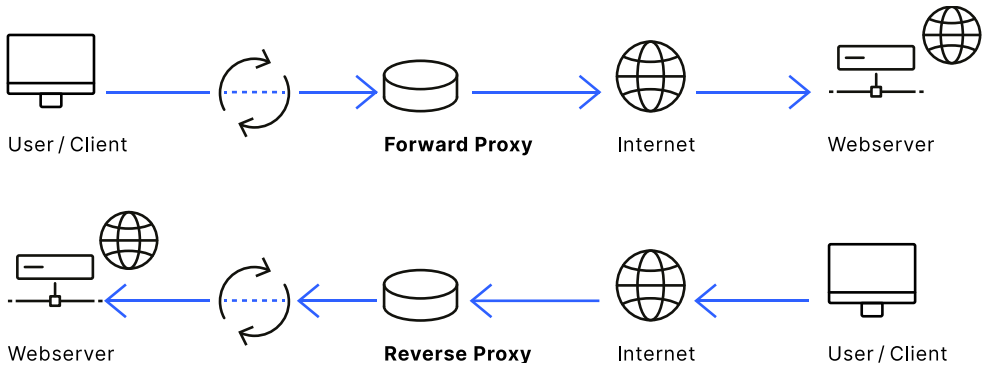

Figure 2:
Forward Proxy vs. Reverse Proxy

Conclusion

To sum up the previous points:

- → Behavioral DPI to regain application visibility
- → Decryption and re-encryption using proxies to detect threats hidden in encrypted communications
- → Asset management infrastructure to manage and monitor certificate infrastructures
- → Network anomaly detection can help in recognizing attacks and finding breaches
- → Employee awareness

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de
www.lancom-systems.com