WHITE PAPER

McAfee
Together is power.

High-Performance Inbound SSL Inspection for McAfee Network Security Platform

High-Performance Inbound SSL Inspection for McAfee Network Security Platform

Encrypted Web Traffic: Security and Threats

As the amount of encrypted web traffic continues to increase, so should the level of security. However, encryption can also make it more difficult for network inspection devices to identify and prevent hidden malware and other types of attacks.

According to industry analyst Gartner:

- Through 2019, more than 80% of enterprises' web traffic will be encrypted.[1]
- By 2020, encrypted traffic will carry more than 70% of web malware,[2] *and more than 60% of organizations will fail to decrypt HTTPS efficiently, missing most targeted web malware.*[3]

The McAfee® Network Security Platform utilizes a patent-pending solution that enables enterprise organizations to quickly and efficiently decrypt and inspect inbound secure sockets layer (SSL) traffic to help keep networks and data secure.

Secure Sockets Layer

Security—represented by the triad of confidentiality, integrity, and availability—is vital to protecting ecommerce websites and transactions completed across the public internet. SSL is the standard for establishing an encrypted link between a web server and a browser[4] and the technology most used to address confidentially and integrity.

SSL is most commonly implemented in the form of secure hypertext transport protocol (HTTPS). This secure link ensures that data passed between the web server and the browser is private. Encrypted internet traffic utilizes SSL or transport layer security (TLS). The current recommended Internet Engineering Task Force (IETF) standard is TLS version 1.3.[5] Depreciated versions include SSL 1.0, 2.0, 3.0 and TLS 1.0, 1.1 and 1.2.

As the use of the internet has exploded and become more pervasive, the knowledge and understanding of its users has also increased. Concerns about privacy are top of mind, leading to the use of SSL to protect not only financial transactions but also news, social media, search results, and everyday web browsing.

Threats Hiding in SSL Traffic

While the use of SSL can improve privacy, unfortunately, advanced threats can also be found lurking in encrypted traffic. The protocol is a target for bad actors trying to steal data and, in addition, the encryption of web traffic creates an opportunity to deliver malicious payloads while hampering the ability of security tools to identify, inspect, and prevent these threats.

Connect With Us

Of particular interest is SSL decryption of inbound traffic that originates outside of your network and is targeted at your secure web service. This channel can be used to mask attacks against your public-facing websites and potentially lead to compromise, website defacement, or data loss. To effectively detect and prevent these attacks, organizations need a fast and efficient method to inspect network traffic.

Traditional Decryption Methods and Limitations

The most common approaches used to inspect encrypted traffic utilize "man-in-the-middle" (MITM) and "known key" methodologies. While these methods could be used for nefarious purposes, they are also used by security practitioners to decrypt and inspect SSL traffic before it is delivered to its final destination.

The MITM method uses a network sensor as a proxy that accepts the inbound connections from the client and negotiate an SSL connection. Once the SSL connection is set up, the sensor makes a connection to the web server on behalf of the client, again negotiating another SSL connection. Using this method, the actual client never communicates directly with the web server. While this approach provides decryption for most flows, it can also significantly decrease performance. In general, the overhead is twofold since MITM requires the network appliance to completely decrypt and then re-encrypt traffic during processing.

Another common method utilizes a "known key" approach, which supports RSA-based key exchange using the server's public/private key that is shared with the network sensor appliance. This method relies on the user, usually a web server administrator, to manage the configurations. The encryption key is made available to the network sensor appliance during the configuration and setup of the appliance, and, using this shared key, the appliance is usually able to decrypt and analyze the network packets before forwarding them to the web server. This method provides significant improvements over the MITM approach, since the appliance sensor is not required to re-encrypt traffic (Figure 1).

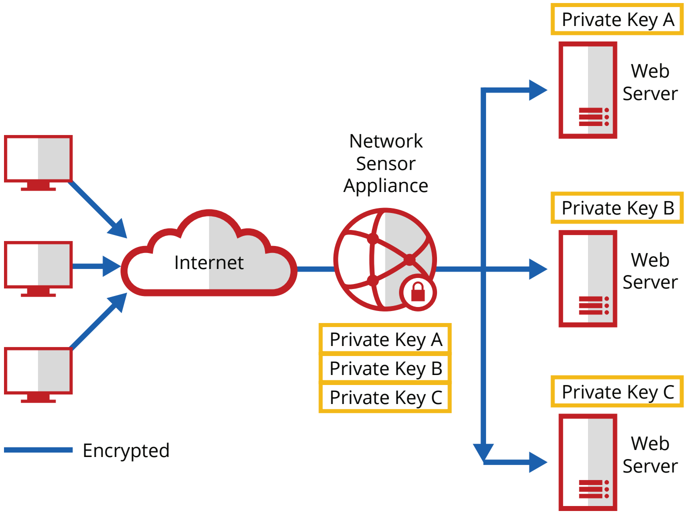


Figure 1. Known key decryption method.

A third method of inspecting traffic is to terminate all SSL/TLS connections from the client on a server load balancer. The server load balancer will then send client communications to the server, usually without encryption. A network sensor appliance can then be placed between the server load balancer and the web servers to inspect and analyze any traffic for anomalies or malicious content. This allows for analysis and inspection, but, since the final connection between the load balancer and the web server is unencrypted, this introduces additional security concerns and may allow unauthorized devices to access sensitive content. As a result, this method of inspection is not suitable for public or hybrid cloud environments.

As approaches to security change, decryption methods must also evolve. For example, a recently introduced method requires more frequent changes to server decryption keys. However, it can be impractical for web server or network security administrators to frequently change or install new keys on all network appliance sensors across the organization. But without the correct keys, network traffic cannot be inspected for malicious threats.

New Ciphers Enhance Security

Standards for SSL/TLS protection provide support for a suite of public key cryptographic algorithms that are used for security. However, existing inbound SSL (IBSSL) only supports the RSA algorithm. While widely adopted, weaknesses in the RSA algorithm have contributed to the development of even stronger ciphers with keys that change more frequently. In addition, TLS version 1.3 removes support for many less secure ciphers and algorithms, including RC4, RSA Key transport, MD5, SHA1, DES, and 3DES.[6]

To address the weaknesses associated with RSA algorithms, a more modern key exchange protocol is required. The recommended replacement utilizes the ephemeral Diffie-Hellman (DHE) or ephemeral Elliptic Curve Diffie-Hellman (ECDHE) key exchange methods. The benefits of DHE/ECDHE include support for Perfect Forward Secrecy (PFS). PFS provides the assurance that session keys are not compromised if the private key of the server is compromised, and also provides protection for past sessions against future compromises.[7]

Performance enhancements are also achieved by using DHE/ECDHE, since Elliptical Curve Cryptography (ECC) key lengths are shorter compared to those created using RSA methods. For example, for 128-bit security an RSA key length of 3,072-bits is required, while ECC only requires a 256-bit key. And for 256-bit security, an RSA key length of 15,360-bits is required, while ECC only requires a 512-bit key. As a result, the ECC algorithm can significantly increase web server performance by requiring shorter keys, which consume fewer compute cycles and less memory. This enables servers to process more simultaneous requests and load web pages much faster.

While DHE/ECDHE provides enhanced performance, it is also resistant to MITM attacks because the session key is created using the known public keys of each party rather than shared over the network. However, since the session key is not transferred across the network, it is difficult (or nearly impossible) to inspect when using shared key methods. To meet existing and future needs, enterprise organizations require a better solution without sacrificing security, performance, and scalability.

McAfee Solution Increases Performance and Security

The McAfee patent-pending solution utilizes an agent-based "key interception" approach that enables the McAfee Network Security Platform to quickly and efficiently decrypt and analyze inbound SSL traffic encrypted with DHE/ECDHE ciphers.

A lightweight agent is installed on the web servers that need protection. The agent then hooks or intercepts function calls to the SSL shared library, a DSO on Linux or DLL on Windows[8] to obtain the encryption keys (Figure 2).

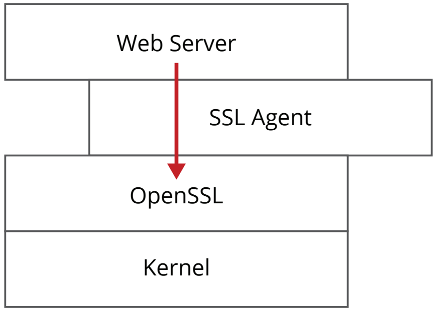
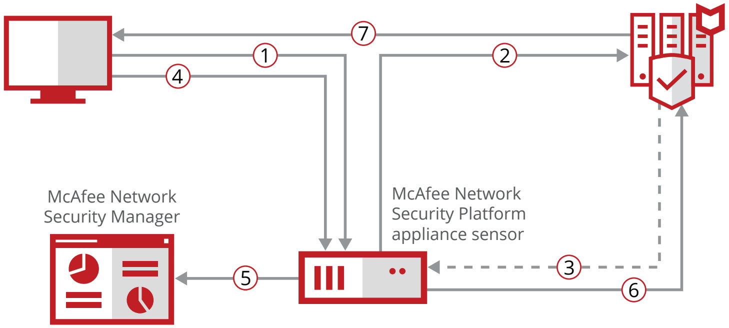


Figure 2. Lightweight agent deployed.

Once the key is intercepted, it is sent through a secure secondary channel to the network security appliance responsible for protecting the corresponding web server. Keys are associated with a specific session using information stored on the network appliance. This allows the appliance to correctly maintain key data for each session, as shown in Figure 3:


7
1
2
4
McAfee Network Security Manager
McAfee Network Security Platform appliance sensor
5
3
6

1. The Sensor intercepts the initial request from the client. (Steps 1, 2, and 3 constitute the handshake process.)
2. The Sensor forwards the request to the web server.
3. The Agent in the web server sends the SSL keys to the Sensor through an encrypted channel.
4. Using the SSL keys received from the Agent, the Sensor decrypts and inspects the subsequent requests from the client.
5. If an attack is detected, the Sensor generates an alert in the Manager.
6. If there are no attacks, the Sensor forwards the request to the web server.
7. The web server responds to the client's request.

Figure 3. McAfee key interception solution.

The McAfee key interception approach provides significant performance and security enhancements compared to traditional decryption methods, including:

- **Faster performance:** While all SSL inspection will impact network security sensors, the McAfee key interception approach provides up to two times faster performance for HTTPS traffic inspection and analysis compared to traditional MITM methods.
- **Removes MITM blind spots:** With the move to modern algorithms and key exchange techniques, an important improvement is the removal of the inspection blind spot created using traditional key-sharing techniques. Given the ephemeral or dynamic nature of DHE/ECDHE (the last "E" stands for "ephemeral"), more and more traffic will bypass inspection and create opportunities for attackers to exploit vulnerabilities or deliver stealth attacks undetected. In cases where agents cannot be installed on servers, only the MITM approach will be available for SSL traffic inspection.
- **More efficient and reliable architecture:** As with any inline inspection approach, MITM requires potentially complex, expensive redundancy and failover (or fail open) architectures. By deploying the agent approach, a listen only architecture (SPAN or TAP) can be used to inspect SSL traffic. This approach reduces complexity and provides fewer points of failure.

Available in the McAfee Network Security Platform,[9] the agent-based key interception methodology from McAfee enables network security sensors to remove traditional inspection blind spots, while providing comprehensive inspection for inbound SSL/TLS traffic that is significantly faster than traditional traffic intercept and decryption methods.

[1] Gartner, Predicts 2017: Network and Gateway Security, December 13, 2016
[2] Ibid.
[3] Gartner, Magic Quadrant for Enterprise Network Firewalls, July 10, 2017
[4] infossl.com: FAQ: What is SSL?
[5] IETF: Transport Layer Security (TLS) Protocol Version 1.3
[6] infossl.com: FAQ: What is SSL?
[7] Wikipedia: Forward secrecy
[8] McAfee support for Microsoft Windows planned for future release
[9] For supported McAfee Network Security Platform models, please visit the McAfee Knowledge Center.

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com