THINK APP SECURITY FIRST

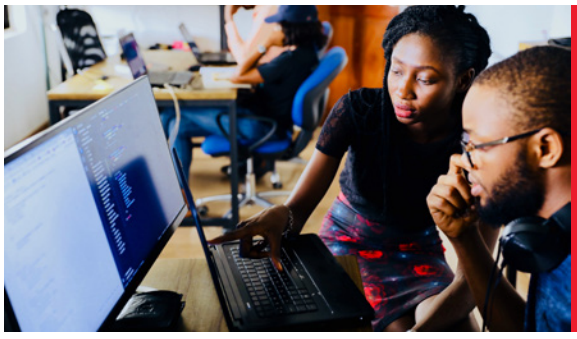
SSL/TLS ORCHESTRATION

DEFENDING AGAINST ENCRYPTED THREATS

ENCRYPTION AND THE CURRENT SECURITY LANDSCAPE

According to research from the F5 Labs threat intelligence team, 80% of page loads on millions of sites sampled are encrypted. Transport Layer Security (TLS) adoption has become the norm for organizations of all sizes and in all industries due to several driving factors: the EU General Data Protection Regulation (GDPR), Google search results ranking preferences, browser warnings for HTTP (cleartext) sites, and the growing importance of privacy, to name just a few.

While this evolution improves security for web traffic, it comes at a price—increased workload demand and the potential hazards of malware cloaked in encrypted traffic. This has placed the burden on organizations to implement an efficient solution that allows their infrastructure to enable speed and availability while also ensuring strong security and privacy.



80% OF PAGE LOADS ON MILLIONS OF SITES SAMPLED ARE ENCRYPTED, BASED ON RESEARCH FROM THE F5 LABS THREAT INTELLIGENCE TEAM.

YOU CAN'T DEFEND AGAINST WHAT YOU CAN'T SEE

Encrypting traffic is great for preventing man-in-the-middle attacks that can potentially allow an attacker to view or alter data; however, encryption can make inspection or analytics devices and services blind to that traffic. Encrypting and decrypting traffic consumes a lot of computational power, so many security inspection solutions like an Intrusion Detection/Prevention System (IDS/IPS), malware sandbox, next-gen firewall (NGFW), and others either don't decrypt at all or take such

a huge performance hit that they pass along encrypted traffic just to keep up. Whether it's traffic coming into your application or internal traffic going out to the Internet, you need all your infrastructure investments to have the visibility they need to fulfill their potential.

Challenges with outbound traffic inspection

Everyone knows that malware is dangerous, but it typically takes a layered defense to identify and stop it from propagating to other users and devices—or from exfiltrating data. Malware can be acquired from several different sources such as malicious web sites or phishing emails, so it's crucial to inspect egress network traffic to ensure no sensitive data is leaving your controlled environment. This becomes a challenge as nearly all attackers are now using encrypted channels to hide their malware's outbound calls to command-and-control servers.

Challenges with inbound traffic inspection

There are also difficulties inspecting inbound traffic. An app or website is often crucial to an organization's business—34% of web apps are reported as being mission critical, according to the F5 Labs 2018 Application Protection Report. And when your application is essential, you'll likely have security solutions like a web application firewall (WAF) or an IDS/IPS to filter out malicious traffic. In addition to security inspection devices, you may need to run app traffic through analytics engines or customer experience solutions. All of these solutions offer unique value—but decryption at scale is not likely one of them.

34%

OF WEB APPS ARE REPORTED AS BEING MISSION CRITICAL, AND THEY'RE AT RISK FROM MALICIOUS TRAFFIC.

THE BENEFITS OF VISIBILITY

Security analysts estimate that all malware now uses encryption to hide its tracks from the security devices designed to identify and neutralize it. When implementing a defense-in-depth strategy, many administrators deploy security solutions in a serial chain to defend against malware. This is incredibly inefficient, and also leaves the door open for malicious traffic to be passed through by an overwhelmed security inspection solution. You need visibility and security, but you can't sacrifice performance.

Malware neutralized

An SSL/TLS solution to decrypt traffic and send to inspection devices is a good first step to mitigating the effects of malware. However, it may introduce unnecessary latency if certain traffic doesn't need to go

through certain inspection devices. For example, if a user's outbound traffic is going to a known good site (or IP address), and the data loss prevention (DLP) solution doesn't detect anything sensitive, does the traffic still need to go through the NGFW or the IDS? Perhaps, but it's important to have the ability to customize the path of your traffic according to your risk tolerance.

HAVING A CENTRALIZED POINT OF CONTROL FOR ALL DECRYPTION AND ENCRYPTION MAKES IT EASIER TO CHANGE CIPHERS AS OLD CIPHERS ARE DEPRECATED.

Perfect forward secrecy and cipher agility

The TLS protocol has a passive surveillance countermeasure called perfect forward secrecy (PFS) protection, which adds an additional exchange to the key establishment protocol between the two sides of the encrypted connection. By generating a unique session key for each session the user initiates, PFS guarantees that an attacker cannot simply recover a single key and decrypt millions of previously recorded conversations.

As PFS becomes the de facto standard—especially as this is the only method allowed within TLS 1.3—you'll need to have a plan for any passive inspection solutions for inbound traffic. Previously, with RSA keys, you would share the key with any of those solutions; however, this is not possible with PFS generating a unique key for each session. F5 SSL Orchestrator can either decrypt and forward cleartext traffic to inspection solutions, or it can decrypt and re-encrypt using TLS 1.2 with RSA. The second option does put the onus back on the inspection devices to decrypt, however the solutions would not be required to be in line with traffic—and thus would not increase latency, nor would there be cleartext data-in-transit within your data center.

F5 SSL ORCHESTRATOR CAN EITHER DECRYPT AND FORWARD CLEARTEXT TRAFFIC TO INSPECTION SOLUTIONS, OR IT CAN DECRYPT AND RE-ENCRYPT USING TLS 1.2 WITH RSA.

No vulnerabilities have yet been found with the elliptical curve ciphers that are mandatory when implementing PFS, but we all know that anything that is secure today won't stay that way forever. Security research and hacking tools continue to advance, as does compute power—and that will inevitably help uncover a vulnerability. Having a centralized point of control for all decryption and encryption makes it easier to change ciphers as old ciphers are deprecated.

VISIBILITY ISN'T ENOUGH—CONTROL THROUGH ORCHESTRATION IS KEY

Having the ability to see inside the packets coming into your applications or going out from your network is a great step, but it's only the first step. Resorting to manual daisy-chaining or configuration to manage decryption/encryption across the entire security stack is tedious. And we all know that any policy that mandates things must be a certain way always come with an exception. F5 SSL Orchestrator delivers visibility at great scale but differentiates itself from the pack with orchestration.

HAVING THE ABILITY TO SEE INSIDE THE PACKETS COMING INTO YOUR APPLICATIONS OR GOING OUT FROM YOUR NETWORK IS A GREAT STEP, BUT IT'S ONLY THE FIRST STEP.

Orchestration provides policy-based traffic steering to a service chain based on risk and dynamic network conditions. Via the virtue of being a full-proxy for both SSL/TLS and HTTP, SSL Orchestrator can make intelligent decisions to steer inbound and outbound traffic to service chains within the security stack. And while most of your traffic is likely HTTPS, SSL Orchestrator allows you to intelligently manage decryption and re-encryption with other traffic types like STARTTLS within FTP, IMAP, POP3, and ICAP. No other product can do all that, which is why no other SSL/TLS solution provides more comprehensive protection for your apps—and your network.

Learn more at
f5.com/security.

DC0618 | ARTICLE-SEC-261249709 | 09.18