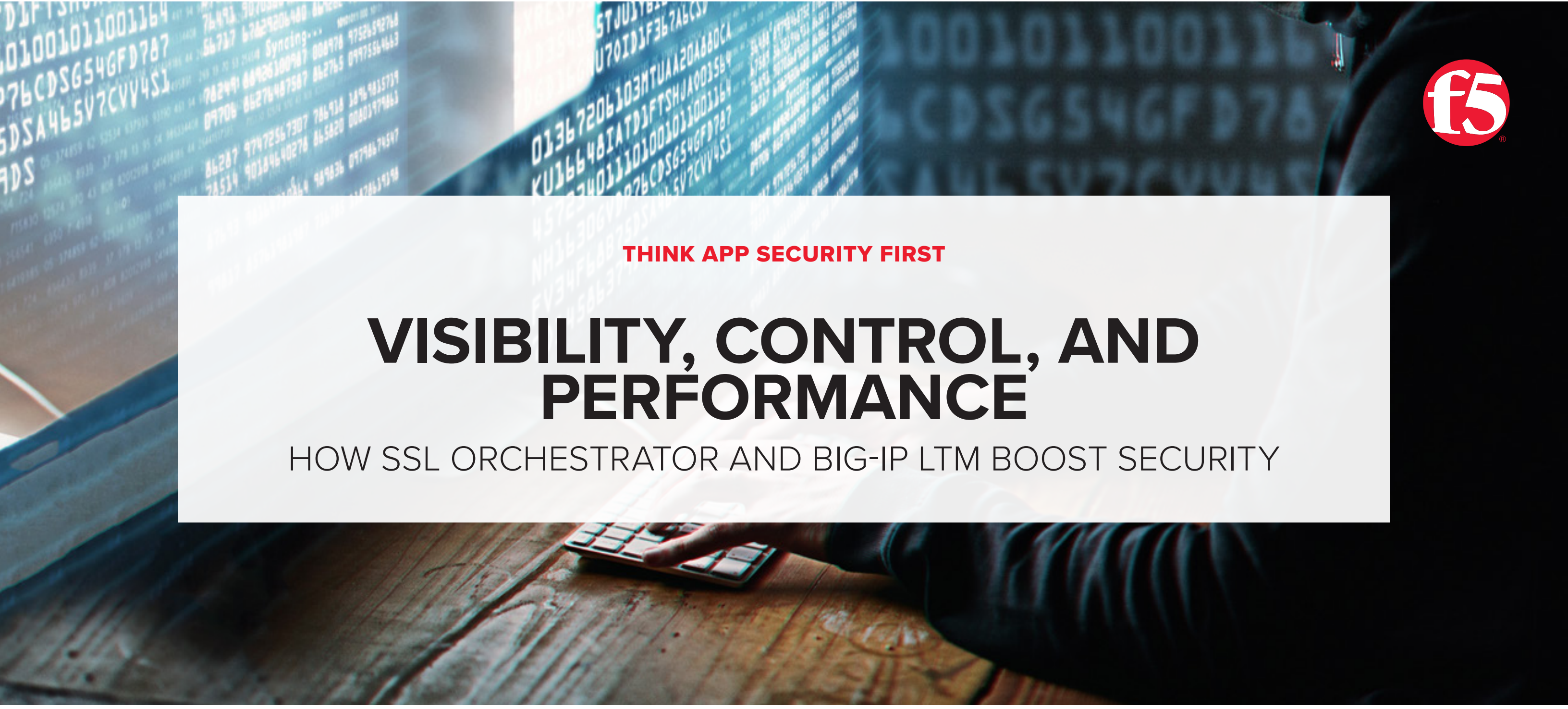


THINK APP SECURITY FIRST

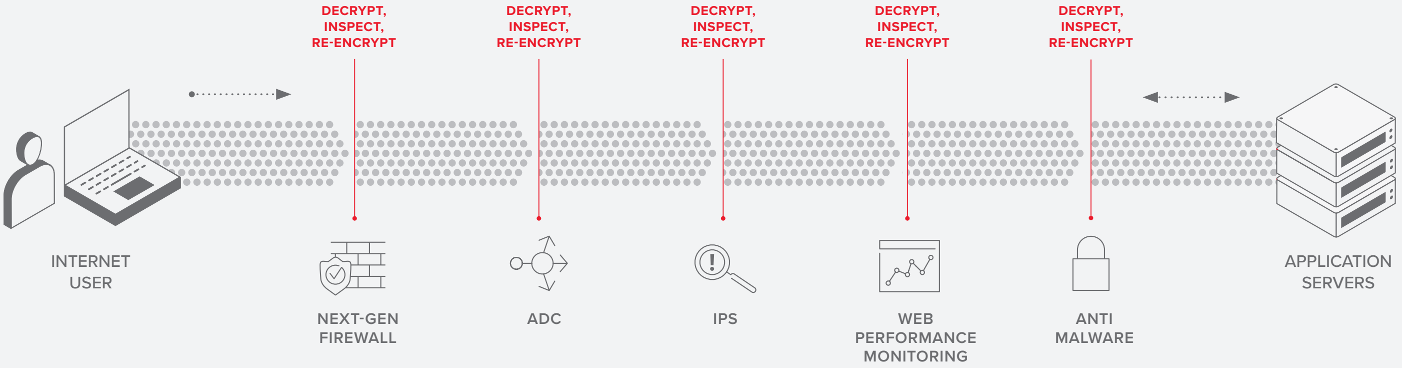
VISIBILITY, CONTROL, AND PERFORMANCE

HOW SSL ORCHESTRATOR AND BIG-IP LTM BOOST SECURITY

INTRODUCTION

The need to inspect traffic with greater scrutiny has grown exponentially as the threat landscape has evolved and encryption has become ubiquitous. Security teams deploy many technologies to detect threats to their applications, including next-generation firewalls (NGFW), web application firewalls (WAF), and intrusion prevention systems (IPS). However, because these technologies do not have visibility into encrypted traffic, they require SSL/TLS decryption to provide any value in inspection. In a traditional infrastructure, those decryption and re-encryption tasks must be repeated at each point in the inspection chain.

TRAFFIC DECRYPTION AT MULTIPLE POINTS


DECRYPT, INSPECT, RE-ENCRYPT
DECRYPT, INSPECT, RE-ENCRYPT
DECRYPT, INSPECT, RE-ENCRYPT
DECRYPT, INSPECT, RE-ENCRYPT
DECRYPT, INSPECT, RE-ENCRYPT
INTERNET USER
NEXT-GEN FIREWALL
ADC
IPS
WEB PERFORMANCE MONITORING
ANTI MALWARE
APPLICATION SERVERS

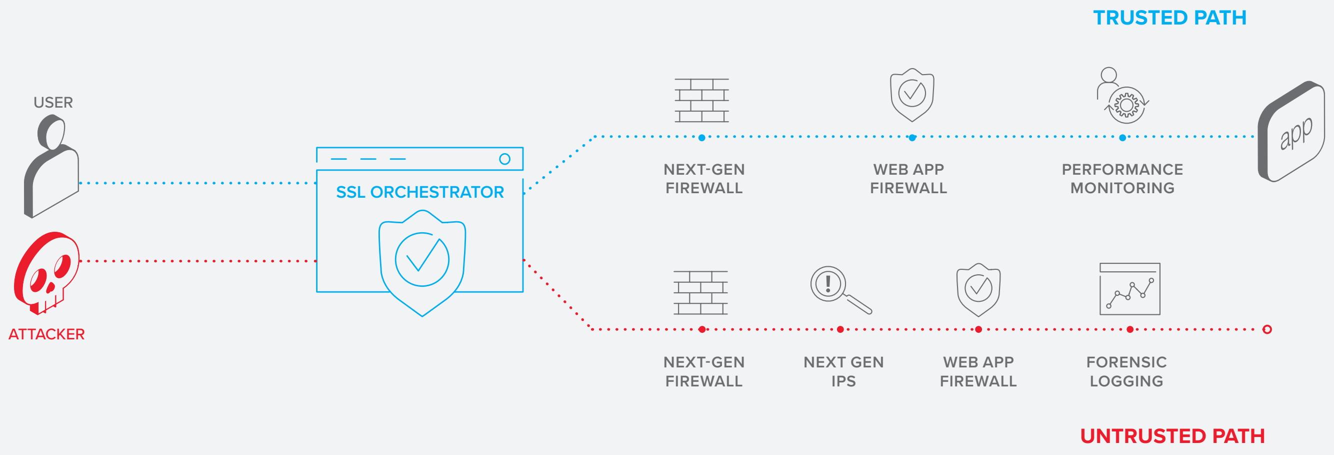
Decrypting at multiple points in a connection flow introduces several problems:

- Additional investment for TLS decryption on each device.
- Additional performance overhead on each decrypting device.
- Multiple points of failure and increased latency on the connection.
- Increased distribution and management of public certificate and key pairs.
- Challenges in scaling each service independently.

Many organizations have responded by creating decryption zones in the DMZ for inspection by multiple devices, but it's usually a static path where all decrypted traffic is inspected by the same chain of devices. While this strategy does boost performance and lower management overhead, it can introduce scaling problems. It may also limit the environment to less secure crypto by restricting the use of the cipher suites required for forward secrecy. Finally, the process can be inefficient because your security devices are inspecting everything instead of identifying and inspecting only the suspicious traffic. Setting up a decryption zone without added intelligence and traffic orchestration clearly isn't the ideal solution to the pressing problem of visibility into encrypted traffic. The good news is that there's a better way.

(MORE) SECURE APPLICATION DELIVERY

With the explosion of HTTPS traffic, decryption has become a requirement to enable application-layer traffic management decisions. Organizations frequently leverage an Application Delivery Controller (ADC) such as BIG-IP Local Traffic Manager (LTM) to provide visibility for other systems beyond the application server. A relatively new challenge is the requirement to provide visibility for multiple third-party inspection technologies on the same application connection.



DYNAMIC SERVICE CHAINING WITH SSL ORCHESTRATOR

Upon its release in 2017, F5 SSL Orchestrator introduced the capability to dynamically chain multiple inspection services together for outbound traffic flows. With TMOS version 14, SSL Orchestrator adds the same capability for inbound traffic flows. This new inbound service chaining capability makes an existing BIG-IP LTM the logical place to add SSL Orchestrator to enable the security inspection today's threat landscape demands.

Consider the scenario in which all decrypted traffic is sent to a performance monitoring system before sending it on to the destination application server. If the source IP address is suspicious, it would be advantageous to send that decrypted traffic to be inspected by the IPS and also to be logged by the performance monitoring system. With SSL Orchestrator, this extra inspection of a suspicious request can happen without complex routing or additional network paths. SSL Orchestrator's unique service-chaining ability enables security operations to create one dynamic configuration adaptable to many different scenarios with multiple associated inspection paths.

SSL ORCHESTRATOR'S UNIQUE SERVICE-CHAINING ABILITY ENABLES SECURITY OPERATIONS TO CREATE ONE DYNAMIC CONFIGURATION.

SSL Orchestrator includes an easy-to-use GUI with workflows that accommodate both new and existing applications. This makes it simple to integrate into existing environments or build new ones. SSL Orchestrator can also be configured as it would be in a standalone architecture to send re-encrypted traffic to another routed destination instead of a pool of application servers.

ARCHITECTURAL CONSIDERATIONS

After passing each inspection device in the decryption zone, the traffic returns to the original BIG-IP device. As a result, traffic and utilization can ramp up quickly. For BIG-IP Cloud Edition deployments, this can entail utilizing larger or more instances. For BIG-IP hardware appliances, this means ensuring a new or existing appliance is specified with enough available capacity. Fortunately, the highly-optimized SSL/TLS stack in TMOS is extremely efficient for both decryption and re-encryption—and on hardware it has the added benefit of dedicated crypto processors.

CONCLUSION

Security is about controlling risk, and control is only possible with visibility. SSL Orchestrator enables security practitioners to add visibility into new and existing traffic flows to maximize the effectiveness of prior security investments. Adding SSL Orchestrator to BIG-IP Local Traffic Manager minimizes the impact to your existing architecture and leverages your ADC as a strategic point of control—which helps boost your security posture while maintaining the performance standards your business requires.

Learn more at f5.com/security.