SOLUTION OVERVIEW

Accelerate Encrypted Threat Protection with BIG-IP SSL Orchestrator and AWS Gateway Load Balancer

The ever-increasing volume of SSL/TLS traffic has paved the way for cybercriminals to launch hidden attacks that sneak past even the most advanced security stacks, leaving organizations vulnerable and at risk. Blocking encrypted threats and safeguarding your network requires maximizing infrastructure investment, efficiencies, and security for robust SSL/TLS inspection.

KEY BENEFITS

Gain visibility into encrypted traffic
Expose hidden threats in SSL/TLS traffic with centralized decryption for inspection across existing and new security tools.

Maximize security investment
Optimize performance with efficient management and orchestration of inbound, outbound, and east-west encrypted traffic.

Improve risk management and privacy
Implement policies that effectively balance security and privacy.

Support cloud agility and security
Integrate with cloud native constructs through simple insertion and dynamic security chains.

WHILE BUILDING APPS IN AWS HELPS YOU INNOVATE WITH AN EFFICIENCY-FORWARD MINDSET, IT'S BECOME MORE CHALLENGING AND DISRUPTIVE FOR ORGANIZATIONS TO PROTECT AGAINST THE ESCALATING ENCRYPTED THREAT LANDSCAPE WITHOUT SACRIFICING AGILITY AND COMPLICATING CLOUD ARCHITECTURE.

Battle Between Agility and Security for Ultimate Encrypted Threat Protection

Many organizations rely on Amazon Web Services (AWS) to run sensitive and business critical applications—and for good reason. Your apps are arguably your most valuable assets. They're the digital front door to your business. AWS enables you to showcase what makes you different from competitors with acceleration, flexibility, and cost-effectiveness.

But while building apps in AWS helps you innovate with an efficiency-forward mindset, it's become more challenging and disruptive for organizations to protect against the escalating encrypted threat landscape without sacrificing agility and complicating cloud architecture.

This leaves organizations at an inflection point because of three challenges.

Visibility

Attackers launch threats like ransomware and other malware hidden in encrypted payloads and use encrypted channels to evade detection during data exfiltration and command-and-control communications. In response, organizations deploy an arsenal of security solutions, from a next-generation firewall (NGFW) to an intrusion prevention system (IPS). Unfortunately, these tools struggle to inspect the growing volume of SSL/TLS traffic efficiently at scale, allowing encrypted attacks to go undetected and expose assets to breaches. In addition, since most organizations lack the ability to centrally control and implement decryption policies across their security stack, organizations resort to tediously—and manually—configuring security point products in a daisy-chain setup, increasing latency and risk.

Complexity

Public-facing apps have traffic that flows from an external environment to internal systems, and internal systems may need to connect to both external services and other internal systems. All these traffic patterns have different security requirements that must be enforced. To accommodate every unique traffic and security policy combination, most organizations are left to develop a sprawl of topologies, encompassing virtual private clouds (VPCs), peering, gateways, and route tables. While operating in the cloud helps drive customization, implementing and monitoring all these permutations ends up burying organizations in complexity.

KEY FEATURES

Protect against encrypted threats entering at layer 3 through layer 7
Safeguard your apps and network from attacks entering through a wide range of vectors.

Leverage advanced traffic classification
Enjoy advanced and context-aware traffic classification and policy-based steering delivered on AWS.

Move beyond visibility to orchestration
Dynamically group security tools to create focused, appropriate security chains based on traffic and network conditions.

Provide higher availability
Ensure high availability and routing traffic flows with AWS GWLB health checks against virtual appliance instances.

Agility

The advantages of cloud technology are steeped in increasing agility and speed. But while resources are just a click away in AWS, having to build, monitor, and refresh complex topology designs really negates an organization's ability to cash in on the benefits of cloud computing. As a result, while many organizations rush to create the next innovation that could unlock a new competitive advantage, "good enough" security app services far too often get put in place. In a world where the global threat landscape's evolving and security risks are mounting, it's too risky and dangerous to allow security sacrifices for an agile deployment process.

BIG-IP SSL Orchestrator and AWS Gateway Load Balancer

F5® BIG-IP® SSL Orchestrator® helps you to discover and eliminate threats hidden in encrypted traffic before an attack can occur. It's designed and purpose-built to provide security solutions across your security stack with enhanced visibility into SSL/TLS traffic, enabling security inspection to expose threats with greater efficiency. With its high-performance encryption and decryption capabilities, BIG-IP SSL Orchestrator ensures encrypted traffic can be decrypted, inspected by your existing security solutions, then re-encrypted—delivering superior visibility to mitigate encrypted threats traversing your network and optimizing your security investments.

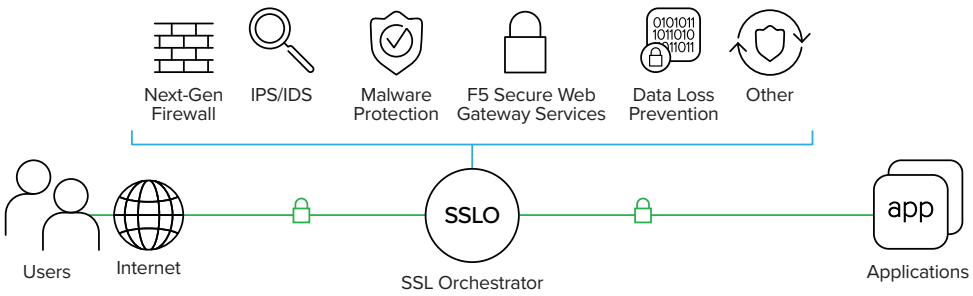

Figure 1: BIG-IP SSL Orchestrator maximizes efficiency and performance for a wide range of inspection devices while maintaining optimal security.

When deployed in AWS, BIG-IP SSL Orchestrator can decrypt and re-encrypt traffic, orchestrate dynamic service chaining to third-party and F5 security services for content inspection and threat analysis, and process and route traffic through context-aware security policies that can adapt to changing network conditions—all in the cloud.

WHEN YOU COMBINE BIG-IP SSL ORCHESTRATOR WITH AWS GWLB, YOU ACCELERATE AND STREAMLINE THE DEPLOYMENT OF BIG-IP SSL ORCHESTRATOR IN AWS AND SEE VALUE—AND ENHANCED SECURITY—MORE QUICKLY.

BIG-IP SSL ORCHESTRATOR AND AWS GWLB CREATE A HIGH-PERFORMING, JOINT SOLUTION DEFENDING AGAINST TODAY'S—AND TOMORROW'S—ENCRYPTED ATTACKS.

BIG-IP SSL Orchestrator intelligently manages encrypted traffic flows—whether they be inbound, outbound, or east-west patterns—across your entire security stack. It unifies inspection and ensures the right security solutions are deployed against the right decrypted traffic, reducing administrative cost and preventing security blind spots. Instead of manually creating redundant, static service chains with security tools and complicating your cloud architecture and topologies in AWS, BIG-IP SSL Orchestrator dynamically and logically chains security devices, independently monitors and scales them, and leverages classification metrics to create custom, focused, appropriate security service chains based on traffic dimensions.

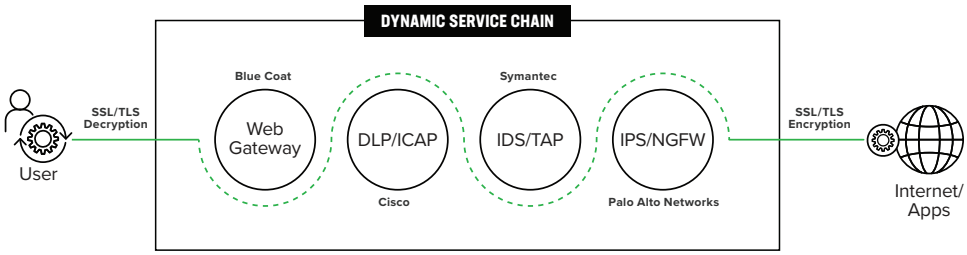

Figure 2: BIG-IP SSL Orchestrator enables the creation of dynamic service chains based on traffic classification.

When you combine BIG-IP SSL Orchestrator with AWS Gateway Load Balancer (GWLB), you accelerate and streamline the deployment of BIG-IP SSL Orchestrator in AWS and see value—and enhanced security—more quickly. You gain control of and visibility into SSL/TLS traffic flowing into, out of, and across your AWS estate while applying security solutions to your organization.

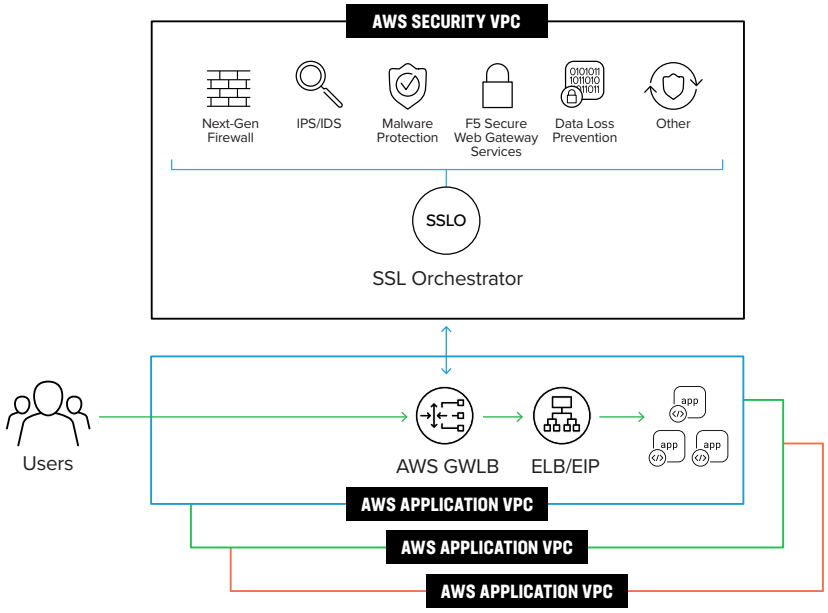

Figure 3: BIG-IP SSL Orchestrator is defined as a service presented by AWS GWLB and deployed into a security VPC. This service contains your full suite of malware inspection tools and can support multiple disparate application environments. Deploying this architecture requires a simple set of Terraform templates.

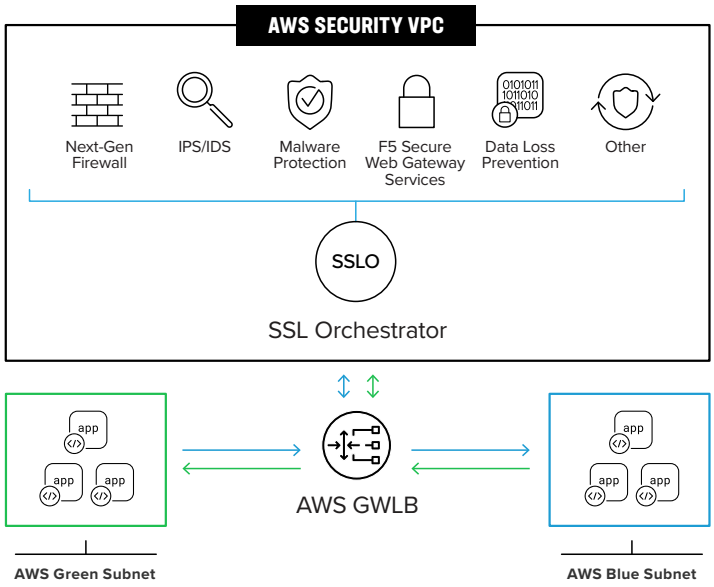

Figure 4: By combining BIG-IP SSL Orchestrator and AWS GWLB, you can insert critical security services between subnets for inter and intra VPC topologies. These security services present capabilities above and beyond the network access control list or security group constructs. Now you can transparently insert dynamic security services based on asset value.

With AWS GWLB, BIG-IP SSL Orchestrator integrates with your AWS architecture more easily and enables you to offload encrypted traffic management with greater efficiency. Your VPC and route table sprawl is reduced by the insertion of endpoints and intelligent F5 traffic matching. You gain the performance of cloud-native load balancing with excellent infrastructure acceleration, elasticity, and flexibility. AWS GWLB also helps BIG-IP SSL Orchestrator fit more easily and naturally within your existing AWS operational processes and systems, allowing you to deliver superior encrypted threat protection—uncomplicating the complicated, with speed.

Conclusion

Implementing enhanced encrypted threat protection in AWS with BIG-IP SSL Orchestrator has never been easier and faster. BIG-IP SSL Orchestrator and AWS GWLB create a high-performing, joint solution defending against today's—and tomorrow's—encrypted attacks while adapting to fast-changing network conditions and organizational needs. With BIG-IP SSL Orchestrator and AWS GWLB, you'll achieve stronger, enhanced security and performance in the cloud that meets—and surpasses—the agility, flexibility, and scalability demands of today's modern security landscape.

To learn more, contact your F5 representative or an F5 security expert.