SOLUTION OVERVIEW

BIG-IP Advanced WAF as a BIG-IP SSL Orchestrator Service

Expose and mitigate threats with greater efficiency by combining two F5 solutions to enable dynamic service chaining and policy-based traffic steering capabilities with market-leading WAF.

KEY BENEFITS

Gain comprehensive protection
Seamlessly apply robust WAF protection to your security stack with no service downtime using an 'easy button' and guided configuration.

Optimize security performance and efficiency
Empower market-leading F5 WAF to focus on what it does best by employing dynamic service chaining and policy-based traffic steering capabilities.

Lower total cost of ownership
Simplify configuration, reduce footprint, and shave administrative overhead by deploying BIG-IP Advanced WAF with BIG-IP SSL Orchestrator.

The Need for Efficient, Comprehensive WAF Coverage in Today's App-Driven, Digital Economy

The dramatic surge in the deployment of applications and services, which has more than doubled since the COVID-19 pandemic,[1] marks a notable shift in how enterprises operate in today's digital age. Applications and APIs have evolved into the lifeblood and core of a company's operations.

This evolution, however, presents a double-edged sword. While apps and APIs offer numerous benefits, they also expose organizations to a wide array of security threats, including SQL injection attacks, distributed denial of service (DDoS) attacks, and exploitation of unknown vulnerabilities (zero-day exploits).

As threats continue to advance and grow in complexity, web application firewalls (WAFs) have become indispensable. They play a pivotal role in safeguarding apps and ensuring overall enterprise security. Yet, securing apps and APIs has become more challenging than ever.

To achieve business velocity and long-term growth, organizations must go beyond simply deploying a WAF. Organizations need to *optimize* their WAF and other security investments. With the soaring volume of encrypted traffic now comprising nearly 90% of all Internet traffic, this presents a significant challenge to doing so.

The ever-increasing volume of SSL/TLS traffic hampers security solutions' ability to decrypt encrypted traffic at scale while performing their assigned security functions at full potential. This can create a blind spot for security, which cybercriminals use to their advantage to launch encrypted threats, bypassing overburdened security solutions, delivering malware and ransomware inside the network, and stealing data.

ACHIEVING BUSINESS VELOCITY AND LONG-TERM GROWTH GOES BEYOND SIMPLY DEPLOYING A WAF. ORGANIZATIONS MUST OPTIMIZE THEIR WAF AND OTHER SECURITY INVESTMENTS.

To thrive in this app-driven economy, organizations must bolster their security measures with comprehensive WAF capabilities *and* effectively protect against the evolving encrypted threat landscape.

Simplify Traffic Orchestration and Configuration to Market-Leading WAF by Integrating Powerful F5 Solutions

F5 offers a powerful security solution that transforms the way enterprises combat encrypted threats to their apps and APIs. The integration of F5® BIG-IP® Advanced WAF® with F5® BIG-IP® SSL Orchestrator® creates a dynamic and potent joint solution. It combines

KEY FEATURES

Secures apps against common, known, and unknown (zero-day) attacks
Defends against common attack vectors, including known vulnerabilities (CVEs), OWASP Top 10, SQL/PHP injection, and more.

Protects credentials from theft
Prevents man-in-the-browser credential theft tied to app-level credential encryption.

Safeguards APIs
Secures GraphQL, REST/JSON, XML, and GWT APIs, while also simplifying API protection profile configurations.

Orchestrates the security stack
Shortens time-consuming security change management processes, simplifying changes to the security stack and mitigating detrimental impacts.

Routes traffic based on context and policy
Increases administrative efficacy by utilizing security resources more efficiently through a contextual classification engine.

Dynamically chains security services
Creates dynamic, logical service chains based on the type of incoming traffic leveraging new and existing security solutions, including BIG-IP Advanced WAF.

BY LEVERAGING BIG-IP ADVANCED WAF WITH BIG-IP SSL ORCHESTRATOR, ORGANIZATIONS CAN EFFICIENTLY IDENTIFY AND BLOCK ATTACKS OTHER WAFs MISS.

rich policy-based traffic steering, dynamic orchestration, and high-performance SSL/TLS decryption capabilities with market-leading WAF capabilities, enabling security teams to safeguard their apps, APIs, and business with comprehensive WAF coverage—all with ease.

Unlike other WAFs, BIG-IP Advanced WAF delivers robust security features that mitigate automated app attacks, shield against known and emerging vulnerabilities, and enhance security through F5's intelligent threat services. BIG-IP Advanced WAF also safeguards sensitive web form data, such as login credentials, provides app-layer DoS protection, defends against targeted threat campaigns (with an add-on subscription), and offers proactive bot defense.

BIG-IP SSL Orchestrator is purpose-built to enhance SSL/TLS infrastructure, provide security solutions—like BIG-IP Advanced WAF—with visibility into SSL/TLS encrypted traffic, and optimize and maximize existing security investments.

By integrating BIG-IP Advanced WAF into the BIG-IP SSL Orchestrator service catalog, it's never been easier for companies to improve their security posture by enabling intelligent traffic orchestration and security solution optimization with comprehensive WAF protection as a combined security solution in a custom dynamic service chain.

Starting with a simple click, organizations can centralize SSL/TLS inspection through BIG-IP SSL Orchestrator. This offloads the computationally intensive decrypting/re-encrypting tasks from new and existing solutions in the security stack. After, BIG-IP SSL Orchestrator provides a step-by-step guided configuration to set up intelligent, policy-based traffic steering and dynamic service chaining with existing security solutions. This enables better utilization of BIG-IP Advanced WAF, empowering it to focus on applying sophisticated controls to decrypted traffic tailored specifically for it—and quickly discover and prevent hidden attacks.

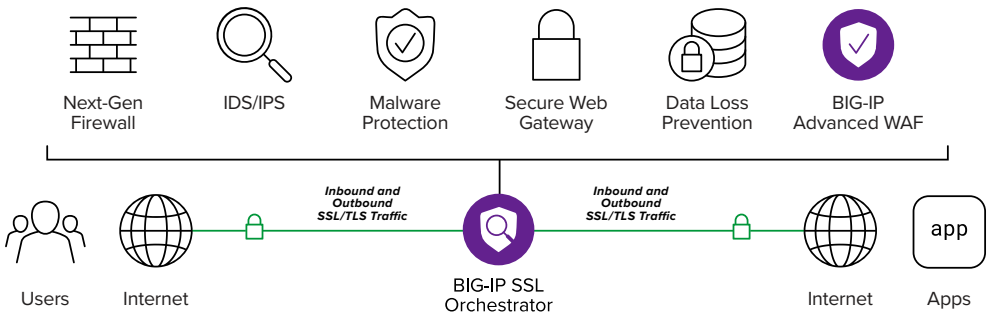

Figure 1: Implement BIG-IP Advanced WAF in your BIG-IP SSL Orchestrator deployment to enable comprehensive WAF coverage in your dynamic service chain.

BIG-IP ADVANCED WAF INTEGRATED WITH BIG-IP SSL ORCHESTRATOR IS A DYNAMIC AND POTENT JOINT SOLUTION, ENABLING SECURITY TEAMS TO EFFICIENTLY SAFEGUARD THE LIFEBLOOD OF THEIR BUSINESS THROUGH COMPREHENSIVE APPLICATION AND API SECURITY.

Deployed together, BIG-IP Advanced WAF and BIG-IP SSL Orchestrator boost defense in depth. This combination enables organizations to optimize and maximize their security investments while providing a robust suite of app and API protections. And it ensures traffic attempting to access a business' apps and APIs is free from malicious intent.

In addition, the joint solution allows organizations to simplify security change management and make changes to the security stack at minimal risk of unintentional traffic bypass. It eliminates downtime and ensures consistent security and inspection of all encrypted and unencrypted traffic. Furthermore, it lowers total cost of ownership through a combined security footprint, as well as reduces deployment complexity and administrative overhead.

Conclusion

In today's app-drive, digital economy, investing in WAF capabilities is no longer optional. It's a necessity. However, simply having WAF coverage in place isn't enough to withstand the evolving encrypted threat landscape. Organizations must go a step further and optimize their WAF and other security investments to defend against critical threats.

F5 offers a comprehensive solution that enhances encrypted threat prevention. By leveraging BIG-IP Advanced WAF with BIG-IP SSL Orchestrator, organizations can efficiently identify and block attacks other WAFs miss. This seamless integration enables businesses to easily provide robust WAF protection with no service downtime and maximize their security investments through dynamic orchestration capabilities while reducing operational costs. Reaping the benefits of this adaptable F5 solution has never been easier.

To deploy BIG-IP Advanced WAF as a service in BIG-IP SSL Orchestrator through its service catalog, download the latest version of BIG-IP SSL Orchestrator at my.f5.com.

To learn more, contact your F5 representative or visit the BIG-IP SSL Orchestrator and BIG-IP Advanced WAF product pages.

[1] F5, "2023 State of Application Strategy Report," 2023, found at https://www.f5.com/resources/reports/state-of-application-strategy-report