



SECURE YOUR APPS WITH F5 SECURE APPLICATION SERVICES: WAF ADMINISTRATION

Securing applications is one of your organization's top priorities. Although there are different ways to secure your apps, the most common is via a web application firewall (WAF).



KEY FEATURES

Maintain control. Maintain administrative control over your F5 assets.

Hybrid WAF administration. Maintain multiple security policies for different types of applications in both multi-cloud and on-premises environments.

Minimized restrictions. Full interaction with F5 Security experts who can tune your application's security posture regardless of software version.

Reduce false positives. Optimize your WAF by reducing the number of false positives generated by untuned policies.

Increase your team's business focus. By adding the WAF Administration service, you extend your staff's ability to focus on other business objectives while leaving policy administration to F5.

Translate security requirements. Application security experts will translate DevOps requirements into SecOps/NetOps requirements.

F5 offers a variety of products to secure your applications—F5® BIG-IP® Application Security Manager™ (ASM), F5® Advanced Web Application Firewall™, and F5® Silverline® Web Application Firewall. To help you maintain application security while retaining administrative control of your devices—whether in the public cloud, private cloud, enterprise data center, or a hybrid multi-cloud environment—we've created the WAF Administration service.

The WAF Administration service provides you with expertise to maintain the security policies on your F5 devices that protect your applications wherever they're deployed and regardless of the F5 product version. As long as you have BIG-IP ASM or Advanced WAF.

HOW THE WAF ADMINISTRATION SERVICE WORKS

WAF Administration is one of the services in the Secure Application Services family. It provides proactive administration of WAF policies for BIG-IP ASM or Advanced WAF in a service you can renew annually.

WAF Administration also helps supplement your internal staff's technical knowledge while also making sure you're using the features and functions that'll give you maximum app protection and increase your security posture.

SERVICE DETAILS

F5 Professional Services security experts take on the responsibility of reviewing, updating, and maintaining your F5 WAF policies. Our experts will collaborate with your DevOps, SecOps, or NetOps teams at a defined interval (up to twice per month) for a duration of 12 months to:

- Establish optimum process and procedures for maintaining WAF security policies.
- Optimize and implement security functionality.
- Review security performance of the WAF.
- Strategically plan for upcoming changes in applications and security requirements.
- Provide guidance for implementation of new software functions and features.
- Mentor your staff in the recommended practices of supporting an F5 WAF.
- Provide ad-hoc knowledge while working with your staff during the defined intervals.

In addition to the advice of experts, this service uses eight key components to help you secure your apps. These components are defined in three areas, the onboarding workshop, WAF administration, and guidance services.

ONBOARDING WORKSHOP

As a partner in the maintenance of your WAF policies, the first step is helping us understand your security practices and your company's security requirements so we can help you meet your business and technical goals. The onboarding workshop covers the following:

- Review security practices
- Review application development processes
- Review/implement security processes
- High-level application delivery infrastructure architecture review
- Review WAF base configurations and redundancies
- Review WAF security logs (historical and current)
- Review existing security policies
- Recommendations to enhance application security posture
- Establish service security plan

ADMINISTRATIVE COMPONENTS

Four key components make up the WAF Administration service: security configuration optimization, security enablement, performance, and strategic planning. These four components are vital to provide the optimum security posture for your applications both today and in the future. The following bullets provides specific details of the administrative components.

Security Configuration Optimization

- WAF policy updates
- Review/recommendations for security posture improvements
- Optimized deployment processes

Security Enablement

- Enforcement using F5's security capabilities (e.g. migrating from transparent to blocking mode)
- SecOps collaboration for organization security policy compliances
- Signature software updates
- Subscription updates (if applicable)

Performance

- Thorough review of WAF reports, logs and events
- Review of capacity, utilization and performance

Strategic Planning

- Periodic current state review with customer
- Review of application development plans
- Understanding of customer's desired end state security goals
- Joint planning to achieve customer business and security goals

GUIDANCE SERVICES

F5 provides guidance in three areas—knowledge transfer, software version consultation, and periodic out-of-cycle assistance—to help you learn about the features and functionality available to you with your WAF’s current software version, as well as learning what new features can help optimize your application security posture.

We also know that, sometimes, you need to talk to an engineer to figure out the impacts of changes you want to make or to help you deploy a policy. To make sure you’re successful, F5 gives you a way to ask for periodic assistance from our security experts. See below for details of our guidance services.

Knowledge Transfer

- Provide guidance to enable customer success
- Provide an overview of the configuration or activities performed during the policy enhancements
- Review operational and troubleshooting methodologies for the WAF solution
- Provide operational/functional overview of WAF features
- Share recommended practices for protecting applications

Software Version Consultation

- Discuss potential upgrades to new software versions or hotfixes
- Review new and updated security features to increase the customer’s security posture
- Discuss and recommend new WAF (basic or advanced) features the customer is interested in

Periodic Out-of-Cycle Assistance

- Aid with the configuration of WAF features
- Discuss CVE’s notified by F5
- Assist with scheduled change windows
- Provide guidance to aid in securing the customer’s application
- Review changes that may impact an application’s security posture

CONCLUSION

The intent of the F5 WAF Administration service is to mitigate risk to your applications and give your staff the chance to learn about the service from F5 security experts. Overall, this service helps you move forward with an improved application security posture, making it easier to achieve your business goals.

WHY F5 PROFESSIONAL SERVICES?

The world's largest businesses, service providers, government entities, and consumer brands rely on F5's intelligent services framework to secure and deliver their applications and services. The mission of F5 Professional Services is to simplify the deployment of F5 solutions and maximize the value of your F5 product investment *throughout* its lifecycle.

For more information about F5 Secure Application Services or to inquire about purchasing a service, contact your F5 Professional Services sales team at consulting.sales@f5.com.

