F5-TRG-BIG-SEC-2
Securing Apps with F5 Solutions

Overview

This Security Workshop provides participants with an opportunity to experiment with many of the different components of F5's security solutions in a hands-on lab environment using a real-world application delivery deployment scenario. The goal of the course is to put to practical use the extensive capabilities of the BIG-IP system to safeguard application delivery in today's growing threat landscape, and to help the audience think differently about application security. The labs in this workshop are designed to demonstrate how you might deploy some of F5's security solutions to protect applications at different layers of the OSI reference model. The course focuses on some of the features and functionality available in several BIG-IP modules, including:

- BIG-IP Local Traffic Manager (LTM)
- BIG-IP Advanced Firewall Manager (AFM)
- BIG-IP Application Security Manager (ASM)
- BIG-IP Access Policy Manager (APM)
- BIG-IP Fraud Protection Service (FPS), also known as F5 Web Safe

Course Length

2 days

Topics covered in this course Include

- Using L7 local traffic policies to direct expected traffic from a public-facing virtual server to private virtual servers for additional processing
- Configuring and using security event logging to monitor legitimate traffic patterns and detect aberrations
- Using network firewall rules to protect perimeter resources at L3/4
- Using a web application firewall to detect and protect perimeter resources from known attack signatures
- Using a web application firewall on internal resources to apply a positive security model and protect from data leakage
- Using iRules to help maintain identity information for clients connecting from CDN and other proxy networks

- Allowing DNS resolution through the BIG-IP system and implementing protection against unauthorized query types and recursive resolution requests
- Mitigating DoS attacks using device DoS protection and eviction policies
- Mitigating known L3/4 attack vectors at the perimeter
- Using the Secure Web Gateway feature to categorize and filter webpages for use in access controls
- Implementing access controls to prevent unauthorized access to sensitive applications
- Consolidating logon functionality for all domains on a single domain
- Implementing Single Sign-On (SSO) access to multiple applications
- Using Fraud Protection Services (Web Safe) to protect the integrity of data shared between clients and the applications they connect to
- Using the FPS Login Page feature to provide alerts upon successful or unsuccessful log into an application
- Using the FPS Automatic Transactions feature to help differentiate "human" traffic from bot traffic
- Using the FPS Malware Detection feature to recognize malware on clients and safeguard against its introduction into applications the clients connect to
- Using the FPS Application Layer Encryption feature to automatically encrypt form data on the client as it is entered in a form field

Audience

This workshop is intended for security and network administrators who are responsible for protecting applications delivered through a BIG-IP system, and who would like a more holistic view of applying F5 solutions to achieve greater application security.

Prerequisites

The following F5 Certifications are required:

- F5 Certified BIG-IP Administrator

Working knowledge of and practical experience deploying configurations using one or more of the following BIG-IP modules is required:

- BIG-IP Local Traffic Manager (LTM)
- BIG-IP Application Security Manager (ASM)
- BIG-IP Advanced Firewall Manager (AFM)
- BIG-IP Access Policy Manager (APM)
- Fraud Protection Service (FPS) – also known as Web Safe

This is an advanced workshop and is not designed to teach students how to configure these products in isolation. For practical experience learning how to configure each of these products, we recommend taking any of our Configuring courses first.

Course Outline

Day 1:

- Lab 1: Adding Traffic Management Directional Controls
- Lab 2: Adding L3/4 Firewall Protections and Traffic Inspection
- Lab 3: Implementing L7 Protections for a Vulnerable Web Application
- Lab 4: Protecting DNS Services
- Lab 5: Defending Against L4 DoS Attacks at the Global Context
- Lab 6: Defending Against L4 DoS Attacks at the Virtual Server Context
- Lab 7: Defending Against L7 DoS Attacks

Day 2:

- Lab 8: Detecting Client-Side Malware
- Lab 9: Deploying Client-Side Application Layer Encryption
- Lab 10: Detecting Client-Side Automatic Transaction
- Lab 11: Implementing Access Controls
- Lab 12: Implementing Multi-Domain Sign-On
- Lab 13: Implementing Single Sign-On to Applications
- Lab 14: Defending on Your Own Terms