THE ESSENTIAL SECURITY GUIDES SERIES

# JUST TELL ME WHAT I NEED TO KNOW...

## F5 BIG-IP® SECURITY

CLEAR ANSWERS. PRACTICAL INSIGHTS.
ESSENTIALS ONLY.


PROTECT YOUR APPLICATIONS

SECURE TRAFFIC. ENSURE AVAILABILITY.

CONTROL ACCESS. REDUCE RISK.

BEST PRACTICES. REAL-WORLD USE.

BELSHAW CONSULTING

# Just Tell Me What I Need To Know
# F5 BIG-IP Security

## A Security Architect's Practical Guide

Belshaw Consulting

**Copyright Notice**

This book is an independent educational work. F5, F5 BIG-IP, NGINX, and related product names are trademarks of their respective owners. Belshaw Consulting is not affiliated with or endorsed by F5, Inc.

Technology, product capabilities, licensing, and security guidance change over time. Readers should verify current vendor documentation and organizational requirements before implementing any design or configuration.

# Table of Contents

# PART I – Foundations

## CHAPTER 1 - Introduction to F5 BIG-IP Security

Modern organizations run on applications. Whether supporting online banking, healthcare systems, e-commerce platforms, government services, or internal business operations, applications have become the primary interface between organizations and the people they serve. As applications have grown more critical, they have also become one of the most attractive targets for cyberattacks.

For many years, cybersecurity strategies focused primarily on protecting networks. Firewalls, intrusion prevention systems, and perimeter defenses were designed to prevent attackers from reaching internal resources. While these controls remain important, modern attackers increasingly target the applications themselves. SQL injection, credential theft, API abuse, bot attacks, ransomware delivery, and distributed denial-of-service attacks all focus on the services organizations expose to users rather than the networks that support them.

This shift has fundamentally changed the role of application delivery technologies.

Organizations no longer need platforms that simply distribute traffic. They need platforms that can secure, optimize, monitor, and manage applications while maintaining availability under increasingly demanding conditions. This requirement has elevated the importance of F5 BIG-IP[1] from a load balancing solution to a strategic application delivery and security platform.

F5 BIG-IP occupies a unique position within enterprise architectures because it sits directly between users and applications. Every request entering an environment typically

[1] For the purposes of this book, the term F5 BIG-IP is used as a unified framework to represent all F5 BIG-IP technologies.

passes through F5 BIG-IP before reaching backend services. This placement provides visibility into application traffic and creates opportunities to enforce security policies, authenticate users, inspect requests, terminate encryption, and optimize application performance before traffic reaches protected systems.

The platform's strategic value comes from this position in the traffic path. Rather than relying solely on endpoint or network-based security controls, organizations can implement security decisions at the point where users, applications, APIs, and services interact. As applications become increasingly distributed across data centers, cloud environments, containers, and edge locations, this control point becomes even more valuable.

While many professionals associate F5 with load balancing, modern F5 BIG-IP deployments often support far broader objectives. Security teams use the platform to protect applications against sophisticated attacks. Identity teams leverage it to enforce authentication and access controls. Network teams depend on it for availability and traffic management. Cloud teams integrate it into hybrid and multi-cloud architectures. Security architects frequently view F5 BIG-IP as one of the most important policy enforcement points within the enterprise.

The platform itself consists of multiple integrated technologies.

- Local Traffic Manager provides traffic distribution, health monitoring, and availability services.
- Advanced WAF protects applications and APIs from application-layer attacks.
- Advanced Firewall Manager addresses network-layer threats and denial-of-service attacks.
- Access Policy Manager provides identity-aware access controls that support Zero Trust initiatives.

Additional services such as F5 BIG-IP DNS, SSL Orchestrator, F5 BIG-IQ, NGINX, and Distributed Cloud extend the platform into areas including global traffic management, encrypted traffic visibility,

centralized governance, cloud-native application delivery, and multi-cloud security.

Together, these technologies form a comprehensive application delivery and security ecosystem.

Understanding F5 BIG-IP, however, requires more than understanding individual products. Successful security architects focus on the problems these technologies solve. Organizations deploy F5 BIG-IP because they need to improve availability, reduce risk, support compliance requirements, protect applications, secure APIs, enable remote access, and modernize infrastructure. The technologies themselves are simply mechanisms for achieving those objectives.

This book was written for professionals responsible for designing, implementing, assessing, or operating secure application environments. Security architects, security engineers, cloud architects, DevSecOps practitioners, network engineers, and cybersecurity professionals will all encounter situations where understanding F5 BIG-IP technologies becomes important. While the platform includes a substantial number of features and capabilities, the goal of this book is not to create administrators. The goal is to help readers understand how F5 technologies fit into modern security architectures and how they can be used to solve real business problems.

Throughout the chapters that follow, we will examine the core components of the F5 ecosystem, explore modern application security challenges, discuss cloud-native and Kubernetes environments, examine API and AI security considerations, and study the architectural patterns that security professionals use to build resilient, secure systems. Along the way, the focus will remain on practical application rather than product memorization.

Technology changes rapidly. Architectural principles change much more slowly. Security architects who understand risk, trust boundaries, identity, availability, visibility, and governance will

continue to make effective decisions regardless of how the technology landscape evolves. F5 BIG-IP provides an excellent lens through which to examine these principles because it operates at the intersection of nearly every major discipline in modern cybersecurity.

By the end of this book, readers should understand not only what F5 products do, but why they matter and how they contribute to secure, resilient, and scalable application architectures.

## CHAPTER 2 - Application Delivery and Security Fundamentals

Before exploring specific F5 BIG-IP technologies, it is important to understand the problem they were designed to solve. Application delivery is often described as the process of making applications available to users, but this definition understates its importance. In modern environments, application delivery encompasses availability, performance, scalability, security, identity, visibility, and resilience. It represents the collection of services that ensure users can reliably and securely interact with applications regardless of where those applications are hosted.

At first glance, the process appears simple. A user sends a request and an application responds. In reality, numerous systems operate between those two events. Traffic traverses networks, passes through security controls, encounters authentication systems, and interacts with multiple application components before reaching its final destination. Every step introduces opportunities for failure, performance degradation, or compromise.

Historically, organizations often relied on individual servers to host applications. As traffic increased, these systems became bottlenecks. A single hardware failure could cause a critical service outage. Load balancing emerged as a solution to this challenge by distributing traffic across multiple servers rather than relying on a

# STOP DROWNING IN DOCUMENTATION.
# START UNDERSTANDING WHAT MATTERS.

F5 BIG-IP is one of the world's leading application delivery and security platforms, trusted by governments, financial institutions, healthcare providers, and Fortune 500 companies to protect their most critical applications. Yet many professionals only understand a small part of what it can do.

**This book changes that.**

Whether you're preparing for an interview, designing secure application architectures, implementing Zero Trust, securing APIs, supporting cloud-native applications, or simply trying to understand how F5 technologies fit into a modern cybersecurity program, this book gives you the knowledge you actually need—without hundreds of pages of product manuals.

## INSIDE YOU'LL LEARN:

- Application Delivery Controllers (ADCs) and modern application delivery
- Local Traffic Manager (LTM), Advanced WAF, AFM, APM, BIG-IP DNS, and SSL Orchestrator
- Web application, API, and network security
- Load balancing, reverse proxies, SSL/TLS, and traffic management
- Zero Trust architectures and identity-aware access
- Kubernetes, containers, DevSecOps, and cloud-native security
- Automation, Infrastructure as Code, and policy-driven operations
- AI security, modern application architectures, and the future of F5 platforms
- Security architecture patterns, design trade-offs, and operational best practices

## MORE THAN A PRODUCT GUIDE

this book explains why these technologies exist, how they work together, and when to use them to solve real business problems.

## WHO THIS BOOK IS FOR

Whether you're a Security Architect, Cloud Engineer, Network Engineer, DevSecOps professional, consultant, student, or IT leader, you'll gain the confidence to discuss, design, and implement F5 BIG-IP security solutions in today's hybrid and multi-cloud environments.

**PROTECT APPLICATIONS**
Secure web, API, and network traffic.

**DELIVER PERFORMANCE**
Ensure availability and scalability.

**ENABLE ZERO TRUST**
Verify identity. Control access.

**SUPPORT MODERN ENVIRONMENTS**
Cloud, containers, and DevSecOps.

**AUTOMATE & OPERATE**
Simplify with automation, IaC, and policies.

## YOU DON'T NEED TO KNOW EVERYTHING. YOU JUST NEED TO KNOW WHAT MATTERS.

BELSHAW CONSULTING