Multi-Layer Security for Multi-Layer Attacks

Preston Hogue
Dir, Cloud and Security Marketing Architectures
F5 Agility 2014

Network

Virtual Edition
Appliance
Chassis

[Physical • Overlay • SDN]
F5 Security Strategy
Evolving Security Threat Landscape

- Spear Phishing
- Redirected Traffic
- DNS Malformed Packet
- Smurf Attack
- Slowloris
- Web Scraping
- Malware
- Cookie Tampering
- Identity Extraction
- Malicious Code
- SSL Renegotiation
- CSRF
- Trojan
- SQL Injection
- Parameter Tampering
- Hash Dos
- ICMP Flood
- Smurf Attack
- Cookie Tampering
- UDP Flood
- DNS Malformed Packet
- HTTP Fragmentation
- Key Loggers
- Social Engineering
- URL Tampering
- XSS
- HTTP
- Phishing
- Ping of Death
- Phishing
- DNS Amplification
- Recursive GET
- Identity Extraction
- Excessive GET/POST
What does F5 know about security?
Control through context

Client Information  +  Traffic Content  +  Application Health
1. Client context in security

- Device
- Operating system
- Browser
- Geolocation
- IP intelligence
2. Traffic context in security

- Unauthorized access
- SYN flood
- XSS
- SQL injection
- Fraud
3. Application context in security
You can’t secure what you don’t know.
Full-proxy architecture

- iRule
- TCP
- SSL
- HTTP
- WAF
- LB1
- Data leakage
- Network Firewall
- Slowloris attack
- SSL renegotiation
- SYN flood
- ICMP flood
- XSS
- Slowloris attack
- SSL renegotiation
- SYN flood
- ICMP flood
- Network Firewall
- Slowloris attack
- SSL renegotiation
- SYN flood
- ICMP flood
- Network Firewall
Per Preston, make instances of iRule smaller. Add “Security context” above iRule.

Lorraine Barnes; 24.10.2013
F5 provides comprehensive application security

- Enterprise Mobility Management
- IP Intelligence
- Inspecting SSL
- DDoS Protection
- Secure DNS
- High-Performance IPS
- Web Application Firewall
- Web Fraud Protection
- Application Access Management
- Network Firewall

Securing access to applications from anywhere

Protecting your applications regardless of where they live

F5 Agility 2014
### Users
- Concurrent user sessions: 200K
- Concurrent logins: 3,000/sec.

### Resources
- Throughput: 640 Gbps
- Concurrent connections: 288 M
- Connections per second: 12.2 M
- SSL TPS (2K keys): 240K/sec
- DNS query response: 12 M/sec

Built for intelligence, speed and scale
Full proxy security
F5 Provides Complete Visibility and Control Across Applications and Users

Securing access to applications from anywhere

Protecting your applications regardless of where they live
Identity and Access Management (IAM) Solution

Securing access to applications from anywhere
Authentication, Authorization, and SSO to All Apps
Application Delivery Firewall (ADF) Solution

Protecting your applications regardless of where they live
Bringing deep application fluency and price performance to firewall security
F5 provides comprehensive application security

- Mobile App Management
- Network Access
- Application Access
- Network DDoS Protection
- SSL DDoS Protection
- DNS DDoS Protection
- Application DDoS Protection
- Web Application Firewall
- Fraud Protection
F5 security reference architectures

- Mobile App Management
- Secure Mobility
- Secure Web Gateway
- Secure VDI
- Application Access
- Network Firewall
- Remote Access
- Network DDoS Protection
- Web Access Management
- SSL DDoS Protection
- Application DDoS Protection
- Web App Firewall
- Inspecting SSL
- Secure DNS
- Versafe
- Network DDoS Protection
- DNS DDoS Protection
- Fraud Protection
- Secure Exchange DDoS
- Versafe
- Application Access
- Network Firewall
Reference Architectures
F5 Reference Architectures
Real solutions for real problems

Benefits

• Minimize deployment times
• Reduce security design costs
• Strengthen security posture
DDoS Protection Reference Architecture

Network attacks:
- ICMP flood
- UDP flood
- SYN flood

DNS attacks:
- DNS amplification
- Dictionary attack
- DNS poisoning

SSL attacks:
- SSL renegotiation
- SSL flood

HTTP attacks:
- Slowloris
- Slow POST
- Recursive POST/GET

Corporate Users

Next-Generation Firewall

Tier 1

Network and DNS

Tier 2

Application

IPS

Multiple ISP strategy

Cloud Scrubbing Service

Threat Feed Intelligence

Scanner
Anonymous Proxies
Anonymous Requests
Botnet
Attacker

Strategic Point of Control

Multiple ISP strategy

Network and DNS

DDoS Protection Reference Architecture

DDoS Attacker

Corporate Users

Financial Services

E-Commerce

Subscriber

Corporate Users
Identity Federation Architecture

- **On-Premises Infrastructure**
- **Corporate Users**
- **Corporate Applications**
- **Directory Services**
- **Access Management**
  - Identity federation
  - SAML
  - Identity management
  - Multi-factor authentication
  - Real-time access control
  - Access policy enforcement

- **Users**
- **Attackers**

- **SaaS Providers**
  - Office 365
  - Google Apps
  - Salesforce
  - Other SaaS providers
Secure Web Gateway Reference Architecture
Microsoft Threat Management Gateway Deployment

Diagram showing the flow of traffic management and control with the use of Intelligent Traffic Management (ITM) and BIG-IP Platform. The diagram includes:

- Corporate Users
  - TMG Client Users
  - SecureNAT Users
  - Web Proxy Users
  - Restricted Users

- Intelligent Traffic Management (ITM)
  - BIG-IP Platform
  - Threat Management Gateway Array

- LTM (Local Traffic Manager)
  - External Firewall
  - Internet
  - Malware and Restricted/Malicious Sites
  - Acceptable Websites

A: Forward web proxy controls outbound access with malware prevention, URL filtering, and content filtering.
B: Blocks inbound restricted content and malware.
F5’s Alternative to Microsoft Threat Management Gateway
Web Fraud Protection architecture diagram

Online Customers

Man-in-the-Browser Attacks

Copied Pages and Phishing

Network Firewall

Application

Security Operations Center

Customer Scenarios
- Malware Detection and Protection
- Anti-Phishing
- Transaction Analysis

Strategic Point of Control
High Performance IPS Reference Architecture
VMware Horizon View Architecture

- **External Users**
  - HTTPS
  - PCoIP

- **Internal Users**
  - HTTPS
  - PCoIP

- **On-Premises Infrastructure**
  - SSL Decryption
  - Authentication
  - High Availability
  - PCoIP Proxy

- **VDI Infrastructure**
  - HTTP/S
  - PCoIP

- **Strategic Point of Control**

F5 Agility 2014
Solutions for an application world.