WELCOME TO THE F5 DoD USER GROUP

The session will start shortly.
Enhanced Web Security & F5 BIG-IP ASM

Presented By:
Jimmy Jennings
&
Paul Simmons
USN and USMC Federal Sales Engineers
Network Threats

- 27% of attacks are focused here
- 90% of security investment

Application/User Threats

- 73% of attacks are focused here
- 10% of security investment

Source: Gartner
Web Application Firewall

- A WAF filters, monitors and/or blocks web traffic to and from a web application to protect against malicious attempts to compromise the system or exfiltrate data. By inspecting web traffic, a WAF can prevent web application attacks such as:
  - Cross-Site Scripting (XSS)
  - SQL Injection
  - Cookie poisoning
  - Invalid input
  - Layer 7 DoS
  - Brute force and credential stuffing
  - Web scraping
  - Bot Mitigation
## WAF Deployment Options

### Positive Model
- Whitelist known good
- Behavior analysis
- Complex deployment
- No application disruption *
- Higher chance of initial breach

### Negative Model
- Blacklist known bad
- Signature based
- Simple deployment
- Application disruption
- Lower chance of initial breach

### Hybrid Model
- Combines known bad with behavior analysis
- Simple Deployment
- Minimal application disruption
- Low chance of initial breach
Many organizations identify application security vulnerabilities using automated, dynamic application scanning tools (DAST) and services from providers like WhiteHat Security, HP, ImmuniWeb, Nessus, Qualys, Quotium, and Trustwave. Typically, security testing teams manually triage the output from these tools and assign high risk vulnerabilities to application development teams for resolution.

The BIG-IP ASM system provides support for automated, closed-loop remediation of many vulnerabilities identified by these tools. When you use this feature, the system automatically customizes your security policy to resolve the vulnerability, or if it cannot, the system reports the liability so the administrator can take further action of necessary.

Allows for a simple process of building policies to protect known vulnerabilities within web applications.
F5 ASM and Rapid Deployment

1861 vulnerabilities blocked by only specifying the Operating System, Web Server Application, Language and Database

<table>
<thead>
<tr>
<th>Assigned Systems:</th>
<th>Available Systems:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>Java Servlets/JSP</td>
</tr>
<tr>
<td></td>
<td>Lotus Domino</td>
</tr>
<tr>
<td></td>
<td>Macromedia ColdFusion</td>
</tr>
<tr>
<td></td>
<td>Macromedia JRun</td>
</tr>
<tr>
<td></td>
<td>Outlook Web Access</td>
</tr>
<tr>
<td></td>
<td>PHP</td>
</tr>
<tr>
<td></td>
<td>SSI (Server Side Includes)</td>
</tr>
<tr>
<td></td>
<td>WebDAV</td>
</tr>
<tr>
<td></td>
<td>XML</td>
</tr>
<tr>
<td></td>
<td>jQuery</td>
</tr>
<tr>
<td><strong>Operating Systems</strong></td>
<td>IBM DB2</td>
</tr>
<tr>
<td>Microsoft Windows</td>
<td>MySQL</td>
</tr>
<tr>
<td></td>
<td>Oracle</td>
</tr>
<tr>
<td></td>
<td>PostgreSQL</td>
</tr>
<tr>
<td></td>
<td>Sybase/ASE</td>
</tr>
<tr>
<td><strong>Web Servers</strong></td>
<td>Other</td>
</tr>
<tr>
<td>IIS</td>
<td>Cisco</td>
</tr>
<tr>
<td></td>
<td>Novell</td>
</tr>
<tr>
<td><strong>Languages, Frameworks and Applications</strong></td>
<td></td>
</tr>
<tr>
<td>ASP.NET</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Database Servers</strong></td>
<td></td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td></td>
</tr>
</tbody>
</table>

1861 signatures will be assigned to the Security Policy

Rapid Deployment Security Policies can be deployed in 2 minutes
F5 ASM & AWAF

- Traditional ASM (Standalone, Add-on and Best Bundle ASM have same feature set)
- Unlimited Behavioral DOS/BaDOS (ASM is limited to 2 virtual servers)
- Data Safe
- Guided Config
- Upstream signaling to Silverline (future)
- The ability to add Anti-Bot Mobile SDK and Threat Campaigns
A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) makes a resource unavailable to its intended users and obstructs the communication media between the intended users and the victimized site so that they can no longer communicate adequately. Perpetrators of DoS attacks typically target sites or services, such as banks, credit card payment gateways, and e-commerce web sites.

Application Security Manager™ (ASM) helps protect web applications from DoS attacks aimed at the resources that are used for serving the application: the web server, web framework, and the application logic. Advanced Firewall Manager™ (AFM) helps prevent network, SIP, and DNS DoS and DDoS attacks.

HTTP-GET attacks and page flood attacks are typical examples of application DoS attacks. These attacks are initiated either from a single user (single IP address) or from thousands of computers (distributed DoS attack), which overwhelms the target system. In page flood attacks, the attacker downloads all the resources on the page (images, scripts, and so on) while an HTTP-GET flood repeatedly requests specific URLs regardless of their place in the application.
Nearly Half of all Internet traffic is now BOTS
A BOT is an application that performs an automated task

• Bots are everywhere in technology. There are good bots like:
  – Trusted Vulnerability Scanners
  – Disability Assistance Tools
  – Trusted Content Web Crawlers
  – Best Deal Locators, etc

• There are also malicious bots
  – Crawlers/Spiders
  – Automated Vulnerability Scanners
  – Web Content ScAPPers
  – DDoS tools
F5 ASM Proactive BOT Defense Protections

- Out-of-Box 950+ BOT Signatures
- Built-in BOT Classification + IP Reputation
- Custom BOT Signature Creation
- Posture client connection
- Identify sophisticated BOT by checking for human interaction on client
- Built-in Image CAPTCHA challenge for suspected client
- Rate Limiting
- Anti-BOT SDK for mobile apps
- Programmability to fingerprint specific pattern and block it
Behavioral DoS (BADoS) provides automatic protection against DDoS attacks by analyzing traffic behavior using machine learning and data analysis. Working together with other BIG-IP DoS protections, Behavioral DoS examines traffic flowing between clients and application servers and automatically establishes the baseline traffic and flow profiles for Layer 7 and Layers 3 and 4.

For example, in the case of a DDoS attack from a botnet, each request may be completely legal but many requests all at once can slow down or crash the server. Behavioral DoS can mitigate the attack by slowing down the traffic no more than necessary to keep the server in good health.

Behavioral DoS continuously monitors server health and loading, by means of a custom feedback loop, to ensure the real-time correlations, and validate server conditions, attacks, and mitigations. Any subsequent anomalies are put on watch, and the system applies mitigations (slowdowns or blocks) as needed.
Behavioral DoS works by:

• Learning typical behavior of normal traffic

• Detecting an attack based on current conditions (server health)
  – An attack can be classified by malicious intent, or accidental overloading of a system by running large reports or unattended behavior

• Uses Machine Learning and AI to detect behavior anomaly (what changed to cause congestion?)

• Mitigates by slowing down suspicious clients

• Improves over time by having a larger dataset for the algorithms to understand the traffic patterns
• **Purpose**
  – Achieve a high level of security for DOD public-facing websites in keeping with cybersecurity best practices.

• **End state**
  – Interdict threat actors’ attempts to exploit DOD public-facing websites.
  – Increase the level of security for their DOD public-facing websites and the DODIN defensive posture is heightened.
  – DODIN Cyberspace Forces within all areas of operation (AO) perform the key tasks associated with the directed security actions.

  – DHS BOD 18-01 – “Enhance Email and Web Security”
    
    https://cyber.dhs.gov/bod/18-01/
    
    DHS BOD 18-01 has complementary security directives.
Enhanced Security Key Tasks Overview

• Eliminate weakly encrypted protocols, ciphers, and certificates (30 days)
• Implement redirection to HTTPS (30 days)
• Remove and upgrade outdated web servers and related software products (90 days)
• Utilize commercial publicly trusted certificates (120 days)
• Implement HTTP Strict Transport Security (HSTS) (120 days)
• Enable Web Application Firewall (WAF) Active Protections (120 days)
• Introduction to HTTPS
  – https://https.cio.gov/faq/

• Why HTTPS for Everything?
  – https://https.cio.gov/everything/

• Certificates
  – https://https.cio.gov/certificates/

• HTTP Strict Transport Security
  – https://https.cio.gov/hsts/

• PULSE Compliance Check
  – https://pulse.cio.gov/https/domains/
Requirements

• An F5!!
• LTM + ASM or AWAF
• F5 must be in line between client and server
• TLS offload
• F5 DoD Military Unique Deployment Guide
Off to the Demo!
<table>
<thead>
<tr>
<th>Service</th>
<th>Position / Region</th>
<th>Name</th>
<th>Email</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Air Force</td>
<td>AE / East</td>
<td>Eddie Augustine</td>
<td><a href="mailto:e.augustine@f5.com">e.augustine@f5.com</a></td>
<td>301-717-4131</td>
</tr>
<tr>
<td></td>
<td>AE / West</td>
<td>Dustin Purkey</td>
<td><a href="mailto:D.Purkey@F5.com">D.Purkey@F5.com</a></td>
<td>714-501-4815</td>
</tr>
<tr>
<td></td>
<td>SE / East</td>
<td>Arnulfo Hernandez</td>
<td><a href="mailto:A.Hernandez@f5.com">A.Hernandez@f5.com</a></td>
<td>202-360-1984</td>
</tr>
<tr>
<td></td>
<td>SE / West</td>
<td>Paul Deakin</td>
<td><a href="mailto:p.deakin@f5.com">p.deakin@f5.com</a></td>
<td>949-395-0051</td>
</tr>
<tr>
<td></td>
<td>AE</td>
<td>David Thomas</td>
<td><a href="mailto:d.thomas@f5.com">d.thomas@f5.com</a></td>
<td>703-930-9623</td>
</tr>
<tr>
<td></td>
<td>AE</td>
<td>Thomas Ries</td>
<td><a href="mailto:T.Ries@f5.com">T.Ries@f5.com</a></td>
<td>703-850-4654</td>
</tr>
<tr>
<td></td>
<td>SE</td>
<td>Anthony Graber</td>
<td><a href="mailto:anthony.graber@f5.com">anthony.graber@f5.com</a></td>
<td>443-987-6487</td>
</tr>
<tr>
<td>DISA</td>
<td>AE</td>
<td>John Manning</td>
<td><a href="mailto:j.manning@f5.com">j.manning@f5.com</a></td>
<td>703-898-4135</td>
</tr>
<tr>
<td></td>
<td>AE / West</td>
<td>Archie Newell</td>
<td><a href="mailto:a.newell@f5.com">a.newell@f5.com</a></td>
<td>858-922-2654</td>
</tr>
<tr>
<td></td>
<td>SE / East</td>
<td>Paul Simmons</td>
<td><a href="mailto:p.simmons@f5.com">p.simmons@f5.com</a></td>
<td>843-300-7392</td>
</tr>
<tr>
<td></td>
<td>SE / West</td>
<td>Jimmy Jennings</td>
<td><a href="mailto:j.jennings@f5.com">j.jennings@f5.com</a></td>
<td>951-334-8558</td>
</tr>
<tr>
<td>Navy Marine Corps</td>
<td>AE / East</td>
<td>Mark Oldknow</td>
<td><a href="mailto:m.oldknow@f5.com">m.oldknow@f5.com</a></td>
<td>512-410-9462</td>
</tr>
<tr>
<td></td>
<td>SE</td>
<td>August Weinerstein</td>
<td><a href="mailto:a.winterstein@f5.com">a.winterstein@f5.com</a></td>
<td>301-660-9644</td>
</tr>
<tr>
<td>Pentagon Defense Agencies</td>
<td>AE</td>
<td>Mark Oldknow</td>
<td><a href="mailto:m.oldknow@f5.com">m.oldknow@f5.com</a></td>
<td>512-410-9462</td>
</tr>
<tr>
<td></td>
<td>SE</td>
<td>August Weinerstein</td>
<td><a href="mailto:a.winterstein@f5.com">a.winterstein@f5.com</a></td>
<td>301-660-9644</td>
</tr>
<tr>
<td>Army</td>
<td>MAM / West</td>
<td>Brig Lambert</td>
<td><a href="mailto:B.Lambert@f5.com">B.Lambert@f5.com</a></td>
<td>801-319-1221</td>
</tr>
<tr>
<td></td>
<td>MAM / East</td>
<td>Todd Favakeh</td>
<td><a href="mailto:t.favakeh@f5.com">t.favakeh@f5.com</a></td>
<td>847-334-5610</td>
</tr>
<tr>
<td></td>
<td>SE / East</td>
<td>Shaun Simmons</td>
<td><a href="mailto:S.simmons@f5.com">S.simmons@f5.com</a></td>
<td>412-329-8366</td>
</tr>
<tr>
<td></td>
<td>SE / West</td>
<td>Michael Slavinsky</td>
<td><a href="mailto:M.Slavinsky@f5.com">M.Slavinsky@f5.com</a></td>
<td>206-637-2056</td>
</tr>
<tr>
<td>Date</td>
<td>Title</td>
<td>F5 DoDVUG Topic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Apr 9th</strong></td>
<td>F5 DoD Virtual User Group #1</td>
<td>F5 Access Policy Manager with remote access, network tunneling, and CAC/PIV Authentication.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thursday@ 1500</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>April 23rd</strong></td>
<td>F5 DoD Virtual User Group #2</td>
<td>Get Your SaaS in Gear Enterprise Application Strategy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thursday@ 1500</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>May 7th</strong></td>
<td>F5 DoD Virtual User Group #3</td>
<td>Enhanced Web Security using F5 ASM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thursday@ 1500</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>May 21st</strong></td>
<td>F5 DoD Virtual User Group #4</td>
<td>Automation/Orchestration - F5 A/O Toolchain</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thursday@ 1500</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>June 4th</strong></td>
<td>F5 DoD Virtual User Group #5</td>
<td>SCCA / SACA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thursday@ 1500</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>June 18th</strong></td>
<td>F5 DoD Virtual User Group #6</td>
<td>SSLO Orchestrator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thursday@ 1500</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Additional Information
Key Task 1 - Eliminate weakly encrypted protocols, ciphers, and certificates.

- Disable Secure Socket Layer (SSL2 and SSL3)
  - F5 DoD MUDG

- Disable DES, 3DES, RC4, NULL, and Export cipher suites
  - F5 DoD MUDG

- Disable MD5 hashing mechanisms
  - F5 DoD MUDG

- Disable all ciphers with key sizes less than 128 bits
  - F5 Default - https://support.f5.com/csp/article/K13156

- Disable insecure negotiation
  - F5 Default - https://support.f5.com/csp/article/K14783
Achieving Compliance

Key Task 1, Eliminate weakly encrypted protocols, ciphers, and certificates.

• Replace certificates with key sizes less than 2048 bits
  – F5 Support for >2048 key length
  – F5 Support for RSA, DSA, and ECDSA key types
  – https://support.f5.com/csp/article/K14620
  – F5 Support for up to FIPS 140-2 Level 3 HSM (internal or external)

• Replace certificates signed with MD5 or SHA1
  – https://support.f5.com/csp/article/K14620

• Replace expired certificates

• Disable TLS 1.0
  – Add !TLS1v1 to F5 ClientSSL profile - https://support.f5.com/csp/article/K17370
Key Task 2 - Implement Redirection to HTTPS. Redirect all unencrypted HTTP protocol requests to Internet facing web servers, web services, and RWPs to use the encrypted HTTPS protocol.

F5: Create a virtual server listening on 0.0.0.0:80 to capture all incoming HTTP requests and redirect to HTTPS using an http profile and redirect iRule.

when HTTP_REQUEST {
    HTTP::redirect https://[HTTP::host][HTTP::uri]
}

Achieving Compliance
Key Task 3 - Remove and upgrade outdated web servers and related software. Remove products and components of Internet facing web servers, web services, web application firewalls (WAF), and reverse web proxies (RWP) that are no longer supported by the vendor and upgrade to a supported version or alternate supported product.

F5: Ensure F5 platforms and BIG-IP software are supported and current.

K4309: F5 platform lifecycle support policy
https://support.f5.com/csp/article/K4309

K5903: BIG-IP software support policy
https://support.f5.com/csp/article/K5903

K9476: The F5 hardware/software compatibility matrix
https://support.f5.com/csp/article/K9476
Key Task 4 - Utilize commercial publicly trusted certificates. Obtain and use publicly trusted server authentication certificates that are trusted by default on common web browsers for Internet facing web servers, web services, and reverse web proxies (RWP) which regularly connect to non-DoD personnel and organizations.

F5: BIG-IP supports RSA, DSA, and ECDSA signed public certificates. BIG-IP also supports OCSP Stapling for faster browser processing and trust establishment. Large cipher support extends to mobile performance.

K14620: Managing SSL certificates for BIG-IP systems using the Configuration utility
https://support.f5.com/csp/article/K14620
K75106155: Configuring OCSP stapling (13.x)
https://support.f5.com/csp/article/K75106155
K13163: SSL ciphers supported on BIG-IP platforms (11.x - 13.x)
https://support.f5.com/csp/article/K13163
Key Task 5 - Implement HTTP Strict Transport Security (HSTS).

- **3.B.1.E.1.** – Add an HTTP Strict Transport Security (HSTS) header to HTTPS responses on Internet facing web servers, web services, and RWPs with a maximum age of at least one year in order to direct web clients to use HTTPS for future access.
  - F5 Option to enable and configure HSTS in HTTP profile

- **3.B.1.E.2.** – Ensure commercial publicly trusted certificates (if used) are in place before enabling HSTS on web servers, web services, and RWPs that use these publicly trusted certificates for non-DoD connections.
  - F5: K14620: Managing SSL certificates for BIG-IP systems using the Configuration utility
  - [https://support.f5.com/csp/article/K14620](https://support.f5.com/csp/article/K14620)
Task 6, Enable Web Application Firewall (WAF) Active Protections.

- Verify all Internet facing web servers and web services are in a Demilitarized Zone (DMZ) or an approved cloud computing environment with a WAF in accordance with REF C.
  - F5: Ensure your internet facing web servers and web services are protected by a WAF such as BIG-IP ASM and are in a DMZ or an approved cloud computing environment

- Review WAF security policies and implement WAF blocking policy for active protection to block malicious activity.
  - F5 BIG-IP Web Application Firewall can be deployed in a blocking mode
  - https://support.f5.com/csp/article/K07359270
Scan results of DOD public-facing websites will be available via the DISA Information Assurance Support Environment portal located at https://disa.deps.mil/org/rmed/card so that each AO can ascertain their compliance status.