WELCOME TO THE F5 DoD USER GROUP

The session will start shortly.

carahsoft

Enhanced Web Security & F5 BIG-IP ASM

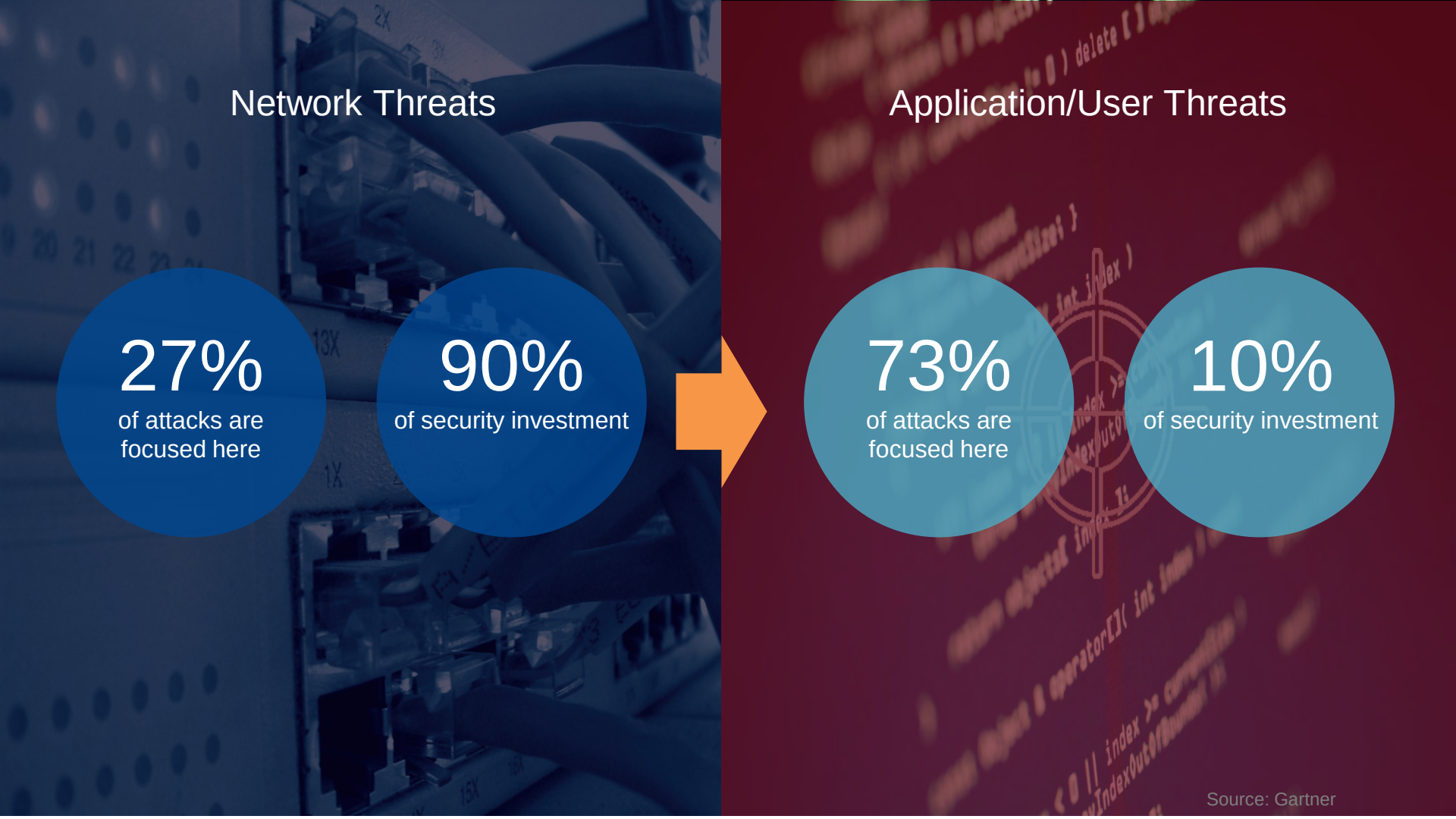
Presented By:

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

F5 Application Security Manager (ASM)

- 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

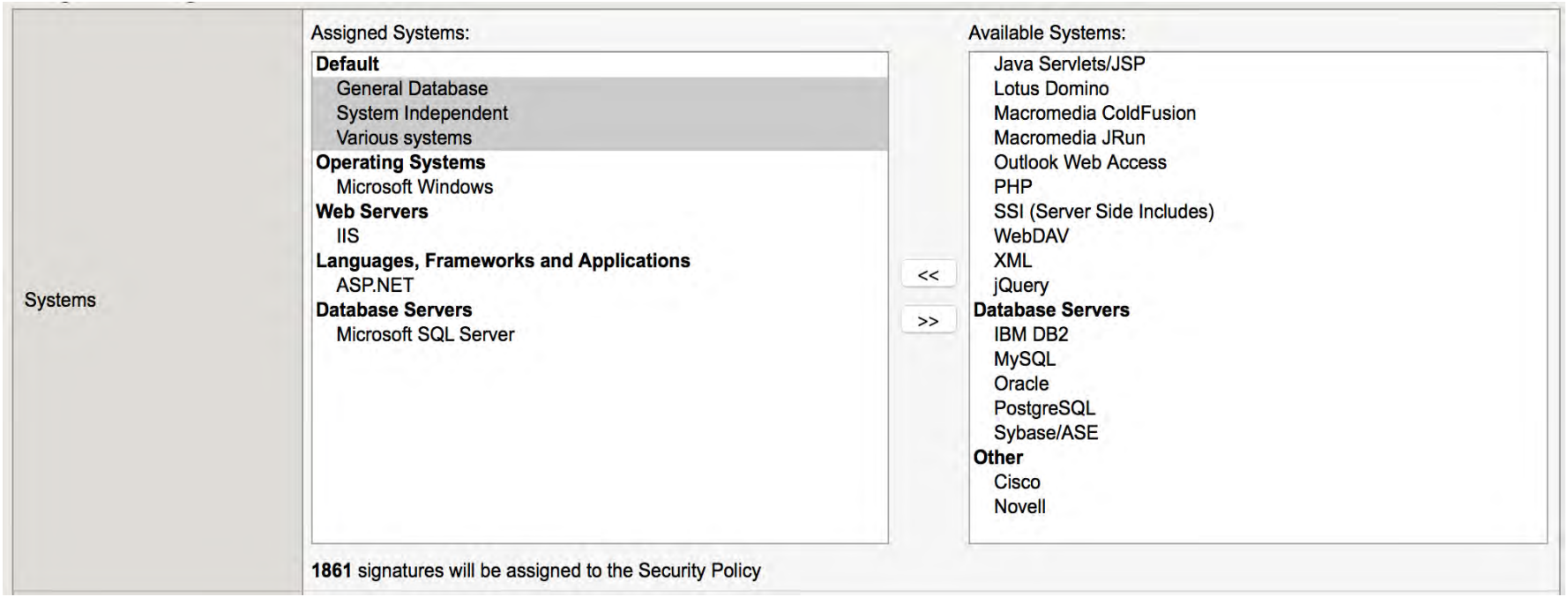
- Combines known bad with behavior analysis
- Simple Deployment
- Minimal application disruption
- Low chance of initial breach

F5 ASM and DAST

- 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



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

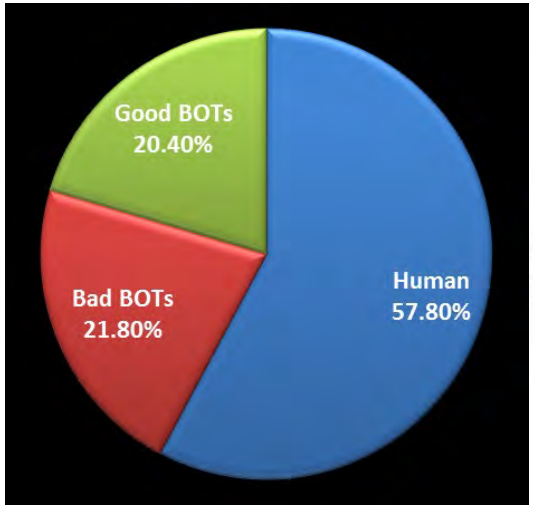
F5 ASM and Application Denial Of Service

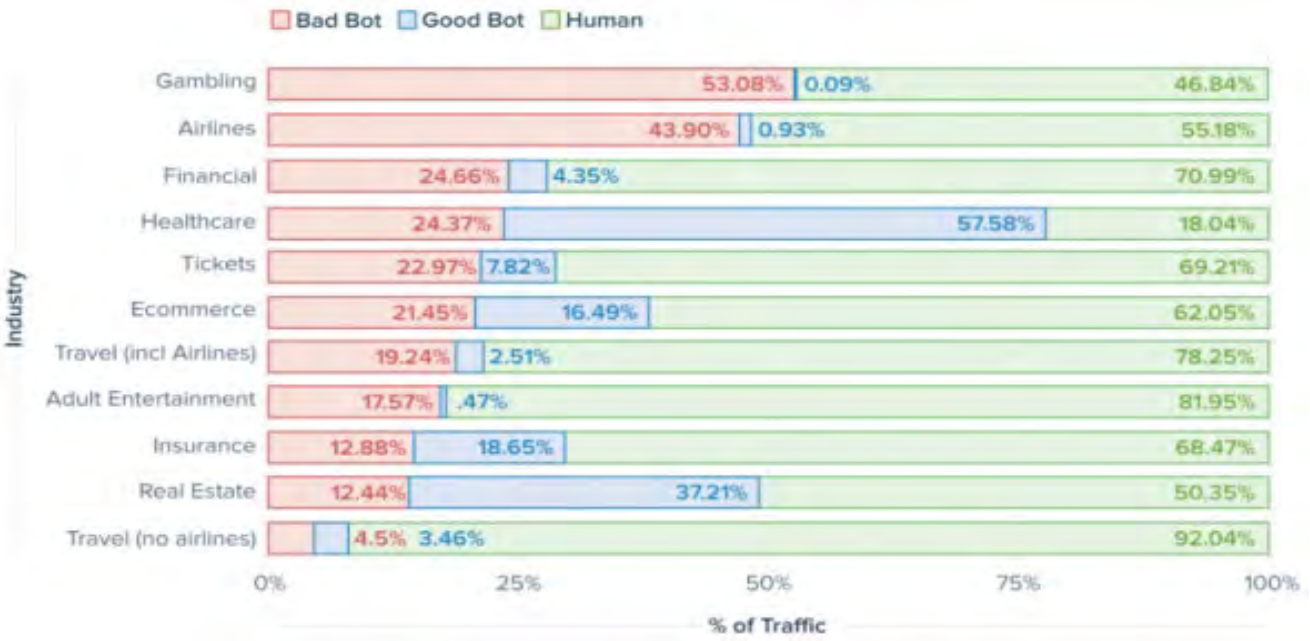
- A ***denial-of-service attack (DoS attack)*** or ***distributed denial-of-service attack (DDoS attack)*** makes a resource unavailable to its intended users and or obstructs the communication media between the intended users and the victimized site so that they can no longer communicate adequately. 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





F5 ASM and Proactive BOT Defense

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 Scrappers
  - DDoS tools

F5 ASM Proactive BOT Defense Protections

- Out-off-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

F5 ASM & Behavioral DoS

- ***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.

F5 ASM & Behavioral DoS

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

Enhanced Security Background Overview

- 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)

Additional Information

- 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!

F5 DoD Account Team

Air Force		AE / East	Eddie Augustine	e.augustine@f5.com	301-717-4131
		AE / West	Dustin Purkey	D.Purkey@F5.com	714-501-4815
		SE / East	Arnulfo Hernandez	A.Hernandez@f5.com	202-360-1984
		SE / West	Paul Deakin	p.deakin@f5.com	949-395-0051
DISA		AE	David Thomas	d.thomas@f5.com	703-930-9623
		AE	Thomas Ries	T.Ries@f5.om	703-850-4654
		SE	Anthony Graber	anthony.graber@f5.com	443-987-6487
Navy Marine Corps		AE / East	John Manning	j.manning@f5.com	703-898-4135
		AE / West	Archie Newell	a.newell@f5.com	858-922-2654
		SE /East	Paul Simmons	p.simmons@f5.com	843-300-7392
		SE / West	Jimmy Jennings	j.jennings@f5.com	951-334-8558
Pentagon Defense Agencies		AE	Mark Oldknow	m.oldknow@f5.com	512-410-9462
		SE	August Weinerstein	a.winterstein@f5.com	301-660-9644
Army		MAM / West	Brig Lambert	B.Lambert@f5.com	801-319-1221
		MAM / East	Todd Favakeh	t.favakeh@f5.com	847-334-5610
		SE /East	Shaun Simmons	s.simmons@f5.com	412-329-8366
		SE / West	Michael Slavinsky	M.Slavinsky@f5.com	206-637-2056

F5 DoD Virtual User Group (DoDVUG) Schedule

Date	Title	F5 DoDVUG Topic
Apr 9th Thursday@ 1500	F5 DoD Virtual User Group #1	F5 Access Policy Manager with remote access, network tunneling, and CAC/PIV Authentication.
April 23rd Thursday@ 1500	F5 DoD Virtual User Group #2	Get Your SaaS in Gear Enterprise Application Strategy
May 7th Thursday@ 1500	F5 DoD Virtual User Group #3	Enhanced Web Security using F5 ASM
May 21st Thursday@ 1500	F5 DoD Virtual User Group #4	Automation/Orchestration - F5 A/O Toolchain
June 4th Thursday@ 1500	F5 DoD Virtual User Group #5	SCCA / SACA
June 18th Thursday@ 1500	F5 DoD Virtual User Group #6	SSLO Orchestrator

Additional Information

Achieving Compliance

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
  - F5 BIG-IQ Certificate Monitoring - https://support.f5.com/kb/en-us/products/big-iq-centralized-mgmt/manuals/product/big-iq-centralized-management-device-6-0-0/6.html
- Disable TLS 1.0
  - Add !TLS1v1 to F5 ClientSSL profile - https://support.f5.com/csp/article/K17370

Achieving Compliance

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

Achieving Compliance

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

Achieving Compliance

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
  - https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-profiles-reference-13-1-0/2.html
- 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

Achieving Compliance

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
  - https://f5.com/pdf/products/big-ip-application-security-manager-ds.pdf
  - https://disa.deps.mil/ext/cop/iase/stigs/Documents/FOUO_DoD_Internet-NIPRNet_DMZ_Technology_V3R5_STIG.zip
  - https://iase.disa.mil/cloud_security/documents/u-cloud_computing_srg_v1r1_final.pdf
- 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

Application Monitoring

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