F5 Networks Capability Use-Case Highlights

PRESENTED BY:

F5 Networks Army Account Team

CECOM – Picatinny Arsenal

WE MAKE APPS GO FASTER. SMARTER. SAFER.

U.S. Army Account Team

- Brig Lambert — Major Account Manager – Army West
- Todd Favakeh — Major Account Manager – Army East
- Michael Slavinsky — Sales Engineer – Army West
- Shaun Simmons — Sales Engineer –Army East

F5 Networks U.S. Army Footprint

Army Analytics Group
Army Benefits Center
National Guard Bureau
USMEPCOM
Joint IED Defeat Organization
AAFES
U.S. Army Pacific
Army Corps of Engineers
US Army NETCOM

US Army Human Resource Command
Army Knowledge Online
ALTESS
GCSS-Army
US Army ERP
PEO Missiles & Space
PEO Aviation
US Army WSMR
US Army Test & Evaluation Center

Joint Regional Sec Stacks
JRSS JMS
Redstone NEC
Belvoir NEC
US Army Ft. Eustis
US Army Europe
Army Reserves Command
US Army Aberdeen Test Center
US Army TRADOC – ATSC

Yuma Proving Grounds

Texas, Colorado, Oklahoma National Guard

F5 Networks List of Capabilities

Application Security

- **Advance Web Application Firewall (AWAF)**
- **AI / ML for increased security and improve the user experience (Nginx App Protection / Shape Security)**
- **Bot protection (ASM, IPI Subscription)**
- **Application acceleration**

Access

- **CAC authentication**
- **Invisible MFA**
- **VPN**
- **Remote access**
- **SSO**
- **VDI – authentication and reduction in infrastructure**
- **Privileged User Access – ephemeral password for PKI**
- **Webtop portal**
- **Identity and Access proxy**
-

Networking

- IDAM
- DMZ STIG
- DNS & DNSSEC
- Improve User Experience
- Assured resilient communication
- Full Proxy – Forward, Reverse
- IP Intelligence
- IDS / IPS
- IoT (does this belong here or in DevOps or both?)
- Fully extensible via iRulesLX using node.js libraries

F5 as a Service

- Advanced WAF
- API Security & Management
- Bot protection
- Stop DDoS attacks
- Global Server Load Balancing
- Shape Enterrise Defense – Advanced Fraud and Automation Protection

Data Center - Local and Remote (COOP / DR)

- Server load balancing
- Geographic site to site load balancing
- Ability to scale for 100K(s)+ users across 100s of sites
- Traffic Steering (SSL-O)
- Traffic shaping
- All capabilities available in both Hardware & Software platforms
- Remote Device Management (BIG-IQ)

Zero Trust

- F5 can be a PEP (policy enforcement point) and a PDP (policy decision point)
- Identity Aware Proxy
- Attribute based look-up and validation
- AD/LDAP lookups
- End Point checks – interrogation – IP, Antivirus,Firewall,Certificate...etc.
- Per-Request policy checks
- Third Party telemetry integration
- Trust Algorithm Scoring

Cloud

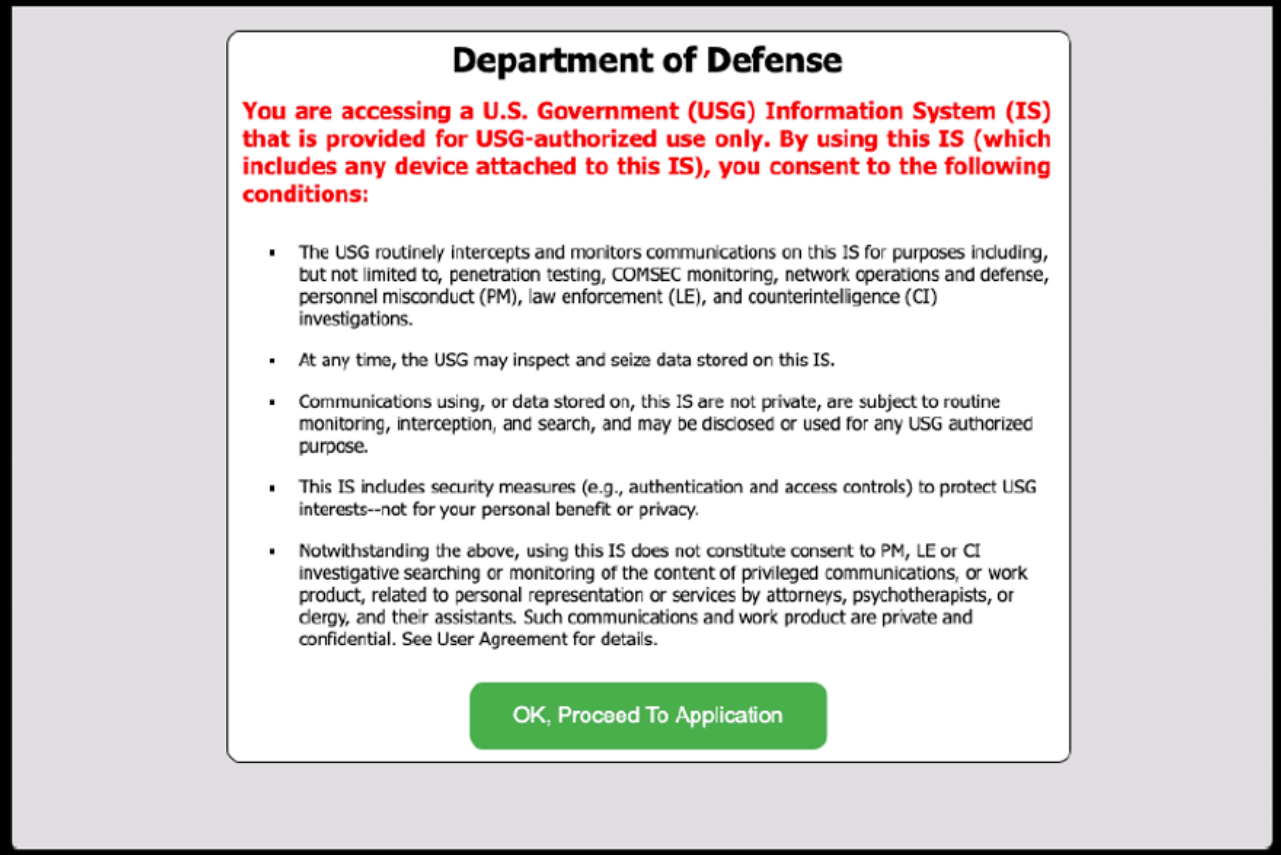
- SCCA (Secure Cloud Computing Architecture)
- Multi Cloud

DevOps & DevSecOps

- Open Source (NGINX) – light weight
- NGINX Plus
- Light weight Application Firewall
- Service Mesh
- API Security & Management
- Per app side-car models
- Programmability/DevOps focus
- F5 Automation Tool Chain
- Integration with many A/O tools ….Ansible, Terraform

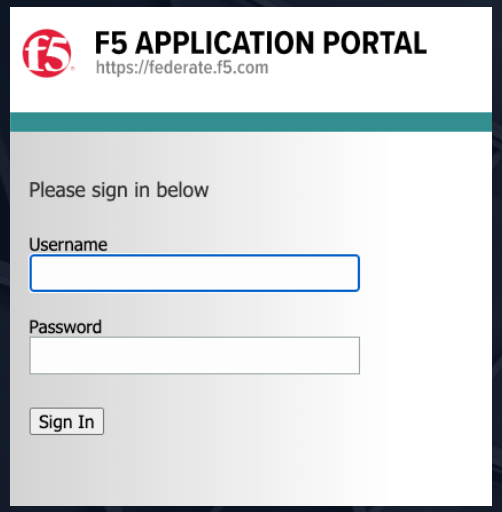
- CAC authentication
- VPN
- Remote access
- SSO (Single Sign On)
- VDI – authentication and reduction in infrastructure. Deployment Guide
- Webtop portal (Example Slide 8)
- Identity and Access proxy - “Zero-Trust”

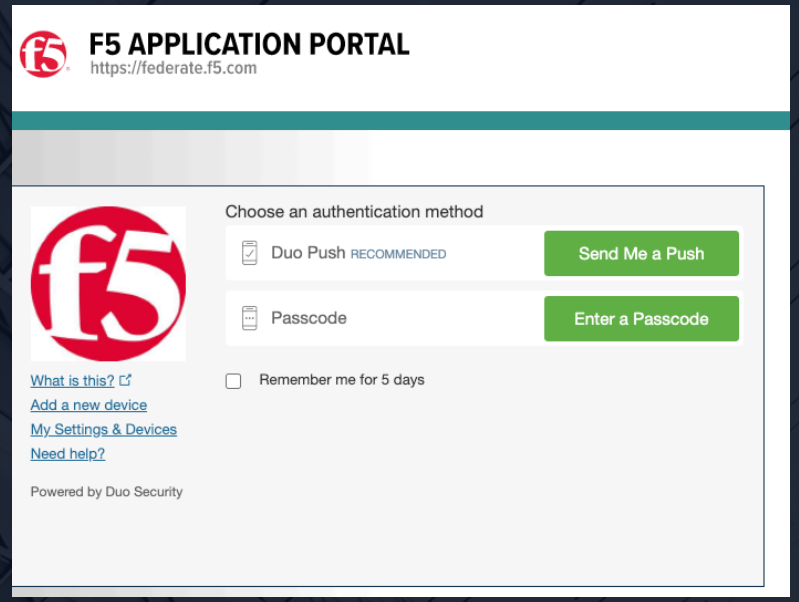
CAC Auth - MFA

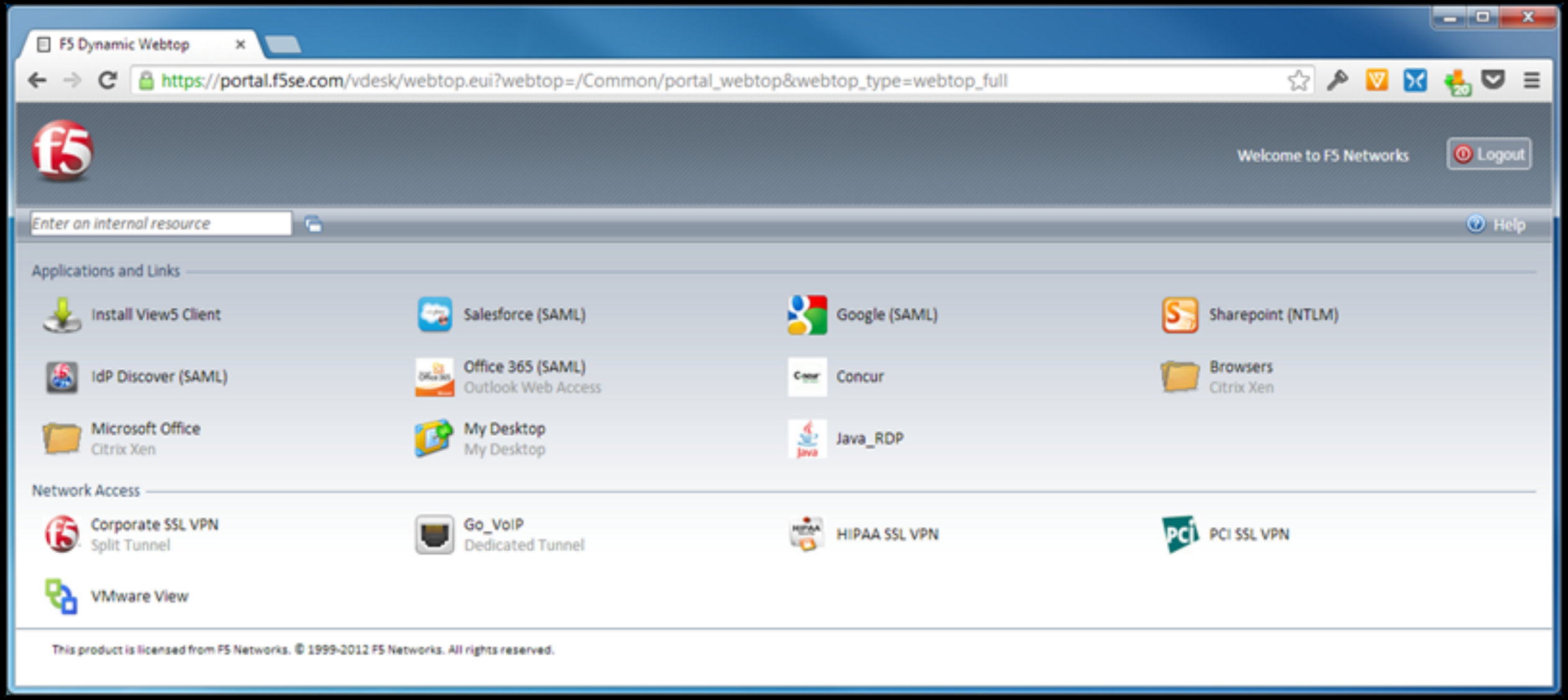


NIST Definition: MFA, sometimes referred to as two-factor authentication or 2FA, is a security enhancement that allows you to present two pieces of evidence – your credentials – when logging in to an account

MFA Enablement






F5 Dynamic Webtop
https://portal.f5se.com/vdesk/webtop.eui?webtop=/Common/portal_webtop&webtop_type=webtop_full
Welcome to F5 Networks
Logout
Enter an internal resource
Help
Applications and Links
Install View5 Client
Salesforce (SAML)
Google (SAML)
Sharepoint (NTLM)
IdP Discover (SAML)
Office 365 (SAML)
Outlook Web Access
Concur
Browsers
Citrix Xen
Microsoft Office
Citrix Xen
My Desktop
My Desktop
Java_RDP
Network Access
Corporate SSL VPN
Split Tunnel
Go_VoIP
Dedicated Tunnel
HIPAA SSL VPN
PCI SSL VPN
VMware View
This product is licensed from F5 Networks. © 1999-2012 F5 Networks. All rights reserved.

...and i should care, why?

Why

Zero Trust is an ***architectural concept*** that has caught on in online media and become a buzzword, spawning analyst frameworks and intense customer interest.

WHAT?

Pioneered by Google "Beyond Corp" to enable protected access to their own internal applications by their employees, the focus of the movement is **away** ***from protecting networks*** and ***toward authenticating and authorizing devices and users***.

- **F5 can be a PEP (policy enforcement point) and a PDP (policy decision point)** 🔗
- **Identity Aware Proxy** 🔗
- **Attribute based look-up and validation**
- **AD/LDAP lookups**
- **End Point checks – interrogation – IP, Antivirus,Firewall,Certificate...etc.**
  - Are HBSS Virus definitions up to date? - Yes or No - *If No, the user will be Denied access !
  - **“Comply To Connect”**

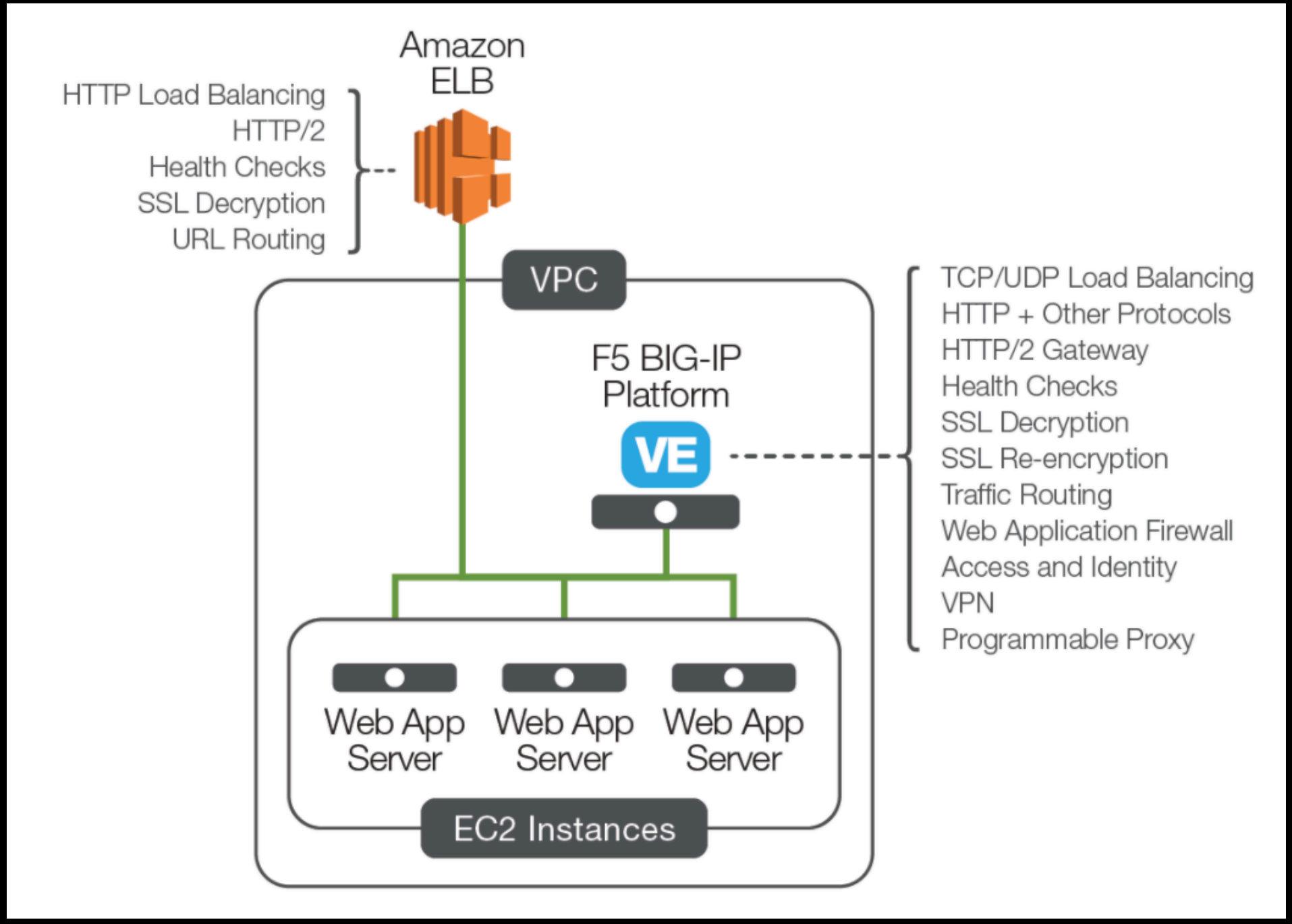
Per-Request policy checks – “Never trust, always Verify!”

- **Third Party telemetry integration**
- **Trust Algorithm Scoring**

Why is Secure Cloud Architecture Important?

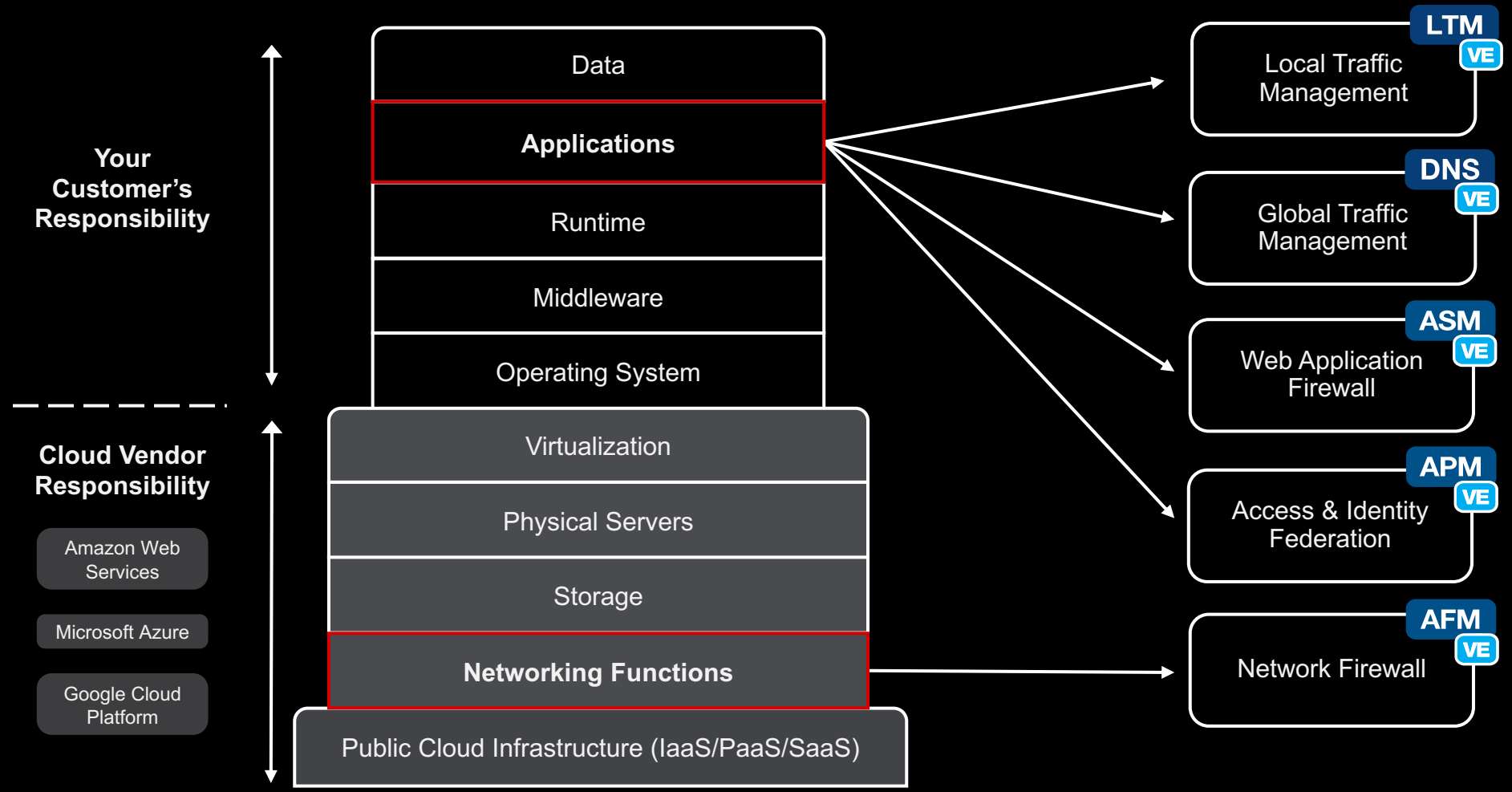
- Secure connectivity to the cloud is the biggest hurdle for the federal government's cloud adoption.
- Agencies need a secure architecture that is easy to deploy, use, and sustain.
- The architecture needs to comply with DISA's Secure Cloud Computing Architecture functional and security requirements regulations.

https://dl.dod.cyber.mil/wp-content/uploads/cloud/pdf/SCCA_FRD_v2-9.pdf

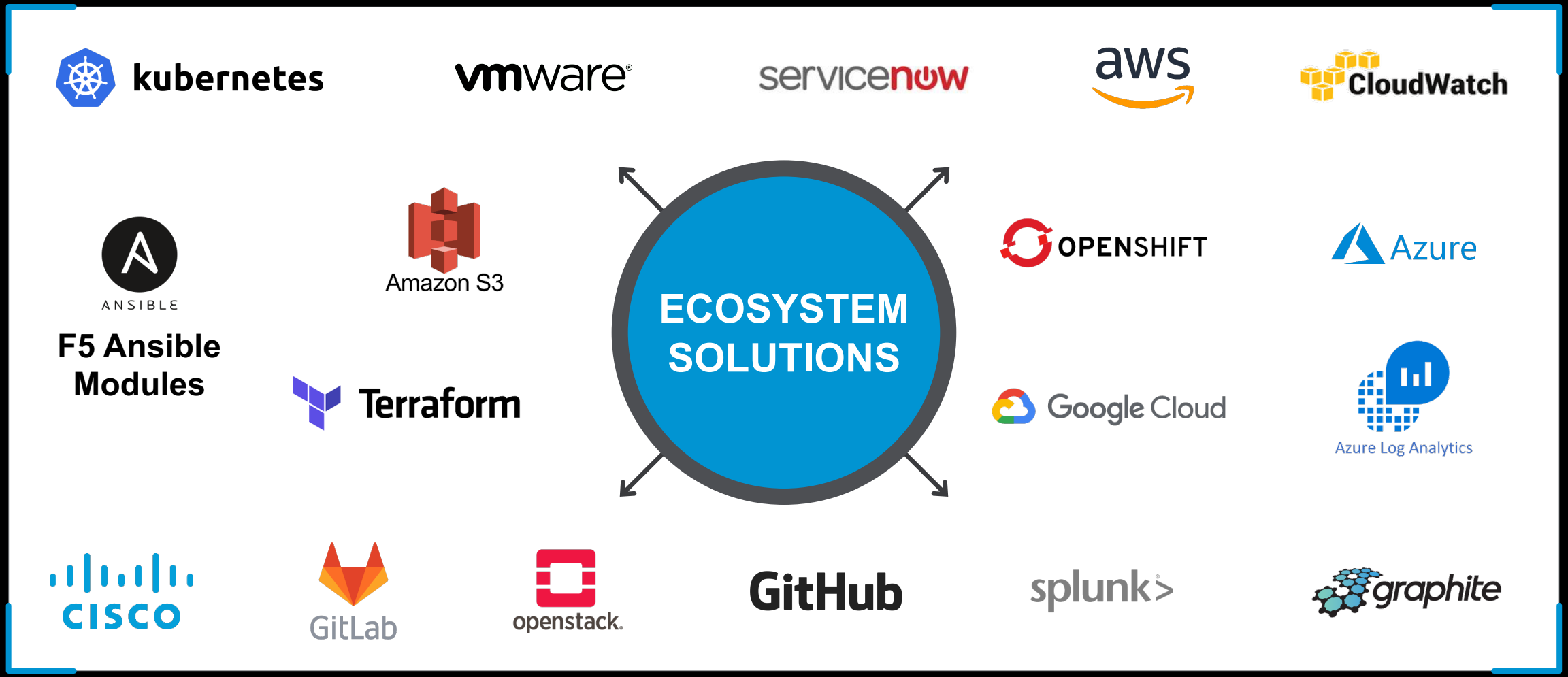

Amazon
ELB
HTTP Load Balancing
HTTP/2
Health Checks
SSL Decryption
URL Routing
VPC
F5 BIG-IP
Platform
VE
TCP/UDP Load Balancing
HTTP + Other Protocols
HTTP/2 Gateway
Health Checks
SSL Decryption
SSL Re-encryption
Traffic Routing
Web Application Firewall
Access and Identity
VPN
Programmable Proxy
Web App
Server
Web App
Server
Web App
Server
EC2 Instances

Shared Responsibility Model

Cloud vendors leave layer 4-7 services to the cloud customer



Ecosystem Integrations



BIG-IP is an Application Delivery Controller (ADC)

Reverse (Web) Proxy

- Load Balancing
- Local Traffic Management
- Global Traffic Management
- Web Content Acceleration Caching
- Session Management
- Context Management
- Geo-Intelligence
- Layer 2 & 3 Aware
- PKI Enablement
- TCP Optimization
- HTTP Compression
- HTTP Protocol Optimization
- Rate Shaping
- IPv6
- NAT64
- SSL Acceleration
- SSL Bridging
- SSL Off Loading
- SSL Translation (SH
- Intelligent DNS
- DNSSec
- Web App Firewall
- OPSWAT Protections
- PII Security
- Web Forms Protection
- L2 - L4 Firewall IP Intelligence
- End Point Inspection
- API Extensibility
- Authentication
- DDOS Protection
- HTTP 2.0
- Websocket Support
- Programmability
- Management & Orchestration
- VDI Integration
- BYoD Integration
- Cloud Ready
- Xero Trust

The F5 BIG-IP is *NOT* just a Load Balancer

Forward (Web) Proxy

- SSL Visibility & Break & Inspect
- SSL Air Gap
- URL Categorization
- Malware Inspection
- Authentication
- Transparent Proxy
- Explicit Proxy
- Web Content Filtering
- Per Request Policy
- Outbound Bandwidth Control
- End Point Inspection

Advanced Web Application Firewall

Advanced WAF is the evolution of F5's Web Application Firewall

- F5's standalone WAF Application Security Manager (ASM) AWAF is included in the Best Bundle

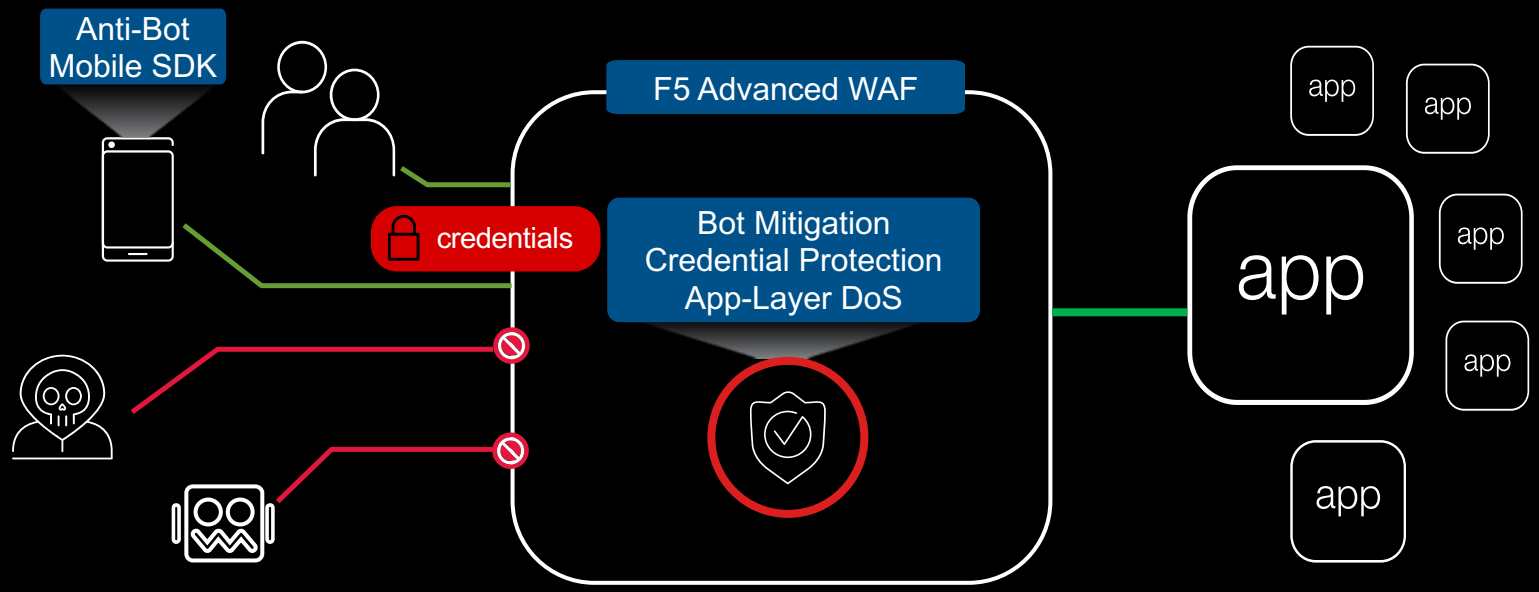
Advanced WAF introduces unique capabilities to the WAF market

- Bot detection beyond signatures and reputation to block evolving automated attacks
- Credential protection including application layer encryption to protect against credential theft
- Application layer (L7) DDoS detection using machine learning and behavioral analytics for high accuracy

****WAF Definition - A '"web application firewall (WAF)"' is an application firewall for HTTP applications. It applies a set of rules to an HTTP conversation****

Advanced WAF Overview

PROTECT AGAINST BOTS, CREDENTIAL ATTACKS, AND APP LAYER DOS



Defend against bots
- Proactive bot defense
- Anti-bot mobile SDK
- Client and server monitoring

Prevent account takeover
- App-level encryption
- Mobile app tampering
- Brute force protection

Protect apps from DoS
- Auto-tuning
- Behavioral analytics
- Dynamic signatures

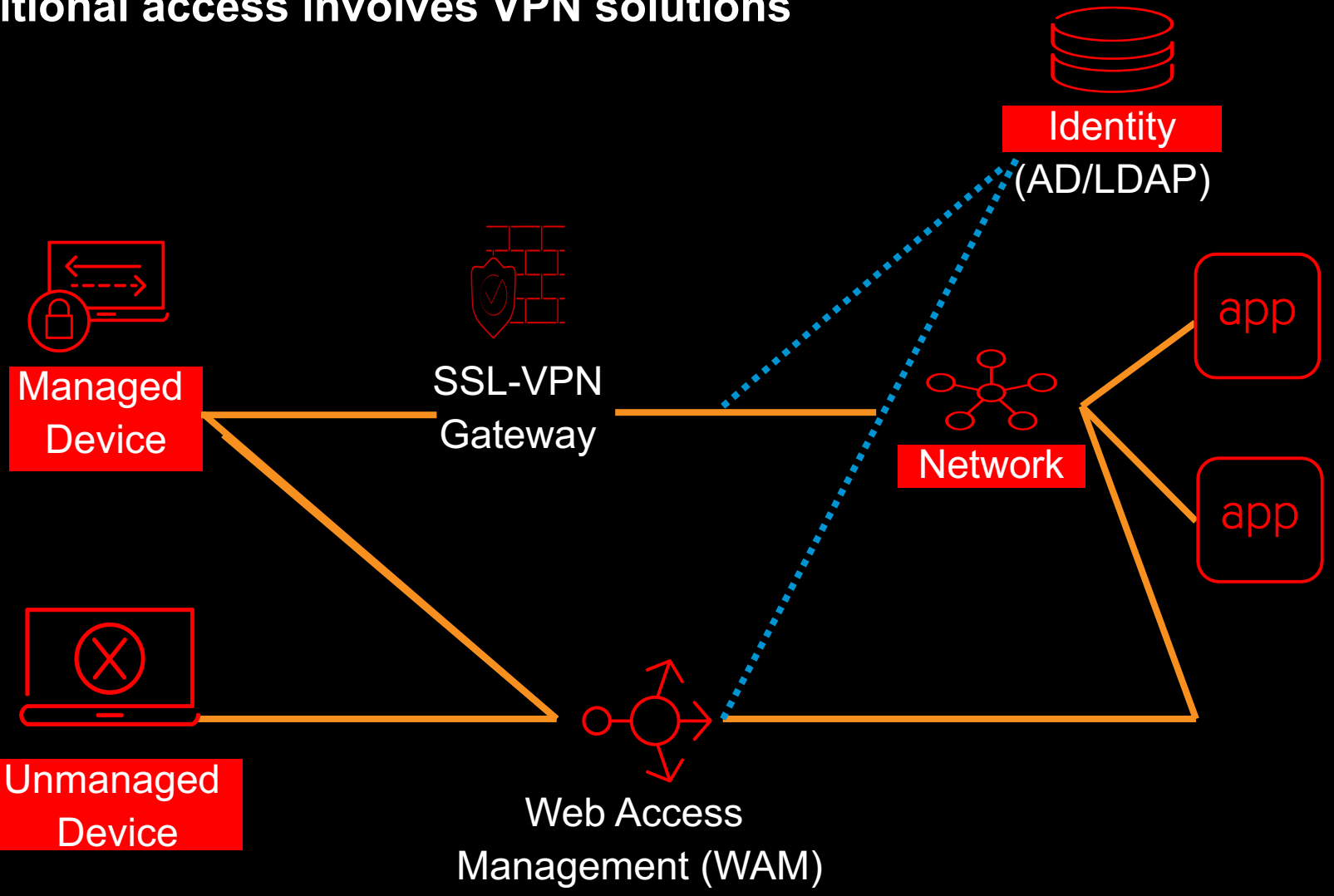
Key Benefits:
- Protects web and mobile apps from exploits, bots, theft, app-layer DoS
- Prevent malware from stealing data and credentials
- Prevent brute force attacks that use stolen credentials
- Eliminate time-consuming manual tuning for app-layer DoS protection

Advanced Firewall Manager
Protocol Inspection

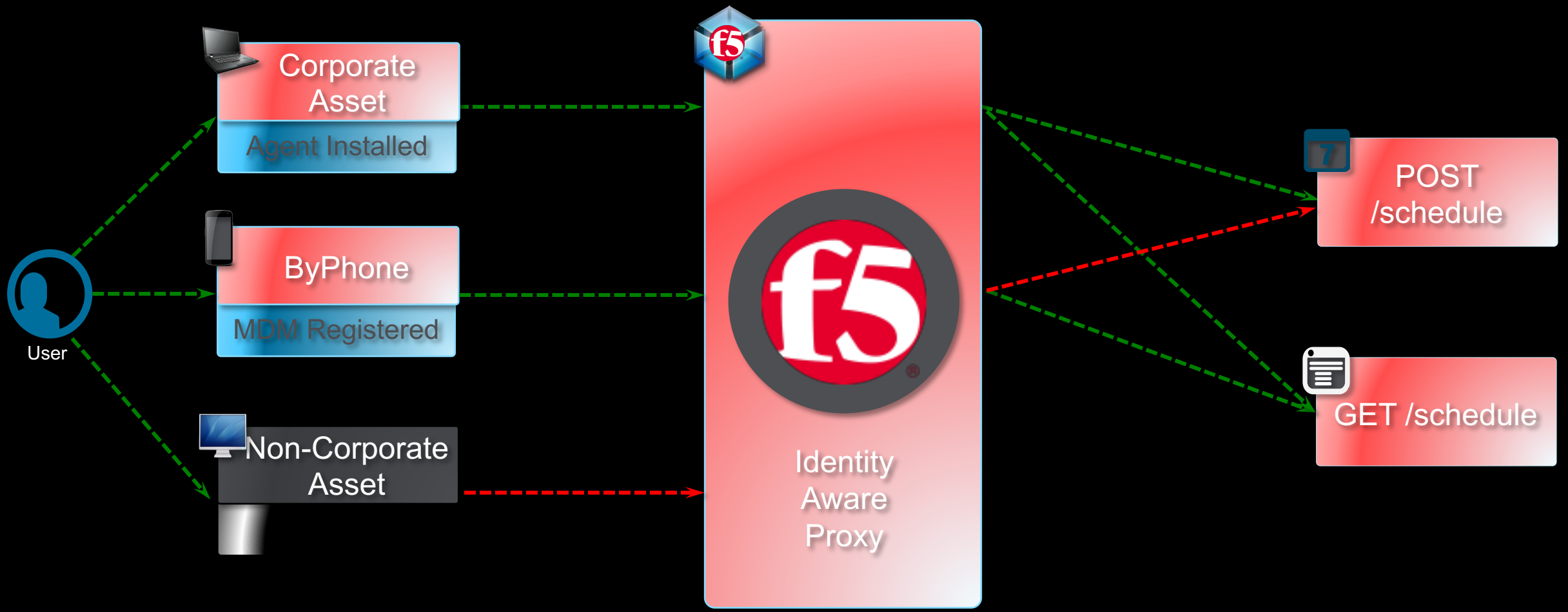
- Protocol Inspection Profiles as an Advanced Firewall Manager (AFM) Rule Action
- Supports Conformance & Signature Matching
- 20+ Protocols: HTTP, DNS, GTP, SIP, Diameter, RADIUS, DHCP, MQTT
- Protocol Security leverages Telus signatures, but SNORT signatures can be imported
- **https://telussecuritylabs.com/**
- IP Intelligence offers reputation based access control
- GeoIP offers location based access control
- SSH Proxy feature secures management connectivity

Traditional Remote Access

Traditional access involves VPN solutions



Identity Aware Proxy (IAP)



F5 BIG-IP DNS

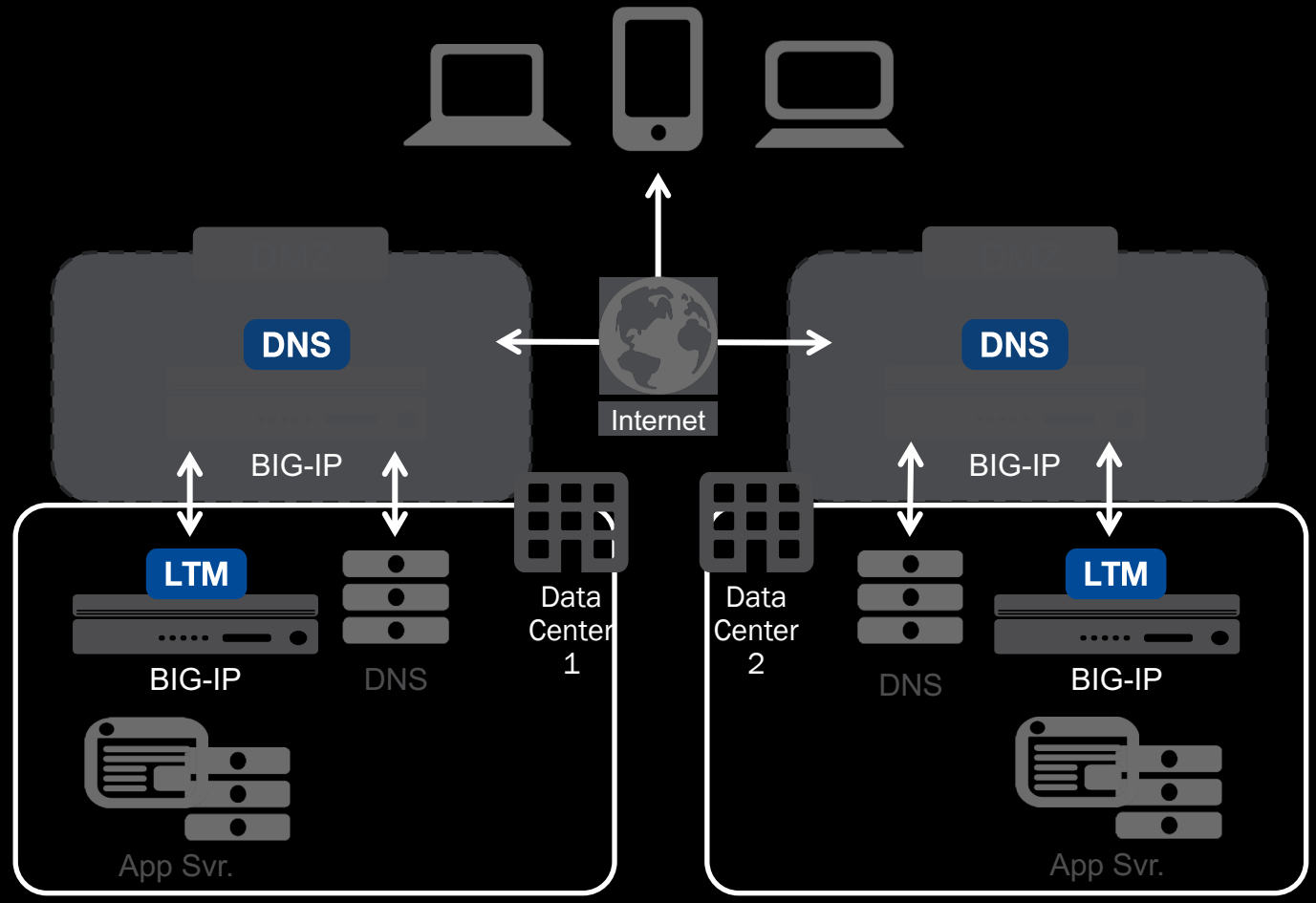
Scale and Security for Intelligent DNS and Global App Management

OPTIMIZED APPLICATIONS & DATA

- Auth. DNS Scalability up to 200x
- DNS Caching and Resolving
- Intelligent Global Load Balancing
- Geolocation routing
- Automatic site-to-site failover
- IPv6/IPv4 Translation
- DNS and App Health Monitoring

SECURE APPLICATIONS & DATA

- DNS DDoS Mitigation
- DNS Firewall Services
- Domain Filtering of malicious IPs
- Real-time DNSSEC signing
- DNSSEC Validation
- Transaction Assurance
- DNS iRules for programmability



F5 and NGINX

- Trusted open source leader in web and application server technology
- Mindshare with AppDevs and DevOps
- Provide cloud-native support for container-based microservices environments, including API management and reverse proxy services
- Fuels 375M+ web sites, 60% of the busiest 100K sites
- Provide application developers lightweight load balancing

- Software company that branched into hardware, and now cloud software
- Mindshare with NetOps and SecOps
- Broadest portfolio of best-in-class app services: WAF, DNS, DDoS protection, SSLO, Bot protection
- Enterprise footprint of 25,000 customers, with a professional services organization whose customer satisfaction is 9.6/10
- Cloud product portfolio that helps our customers “shift left” from app deployment, to continuous integration, continuous delivery in a multi-cloud environment

F5 Federal Certifications & Compliance

https://f5.com/about-us/compliance-and-certifications

- DODIN APL (TN#1312201): Cyber Tool
- DODIN APL (TN#1630801): Cyber Tool
- NIST FIPS 140-2 CMVP: Virtual Edition, iSeries Platform
- NIST SP 800-53r4
- USGv6 (IPV6)
- NIAP CC EAL2+ & EAL4+
- ICSA Certifications:
- WAF, Network Firewall, IPSEC, SSL-TLS VPN
- Legacy: JTIC PKE Certification
- Legacy: US Army's IA- APL

- C&A (RMF) Current ATO
- F5 Device STIG/SRG
- DISA
- NMCI
- JWICS
- SOCOM & CENTCOM
- ARMY
- USMC
- NAVY
- AF

WE MAKE APPS

FASTER. SMARTER. SAFER.