



April 4, 2018

F5 Solutions in Microsoft Azure

Paul Simmons – F5 – Systems Engineer

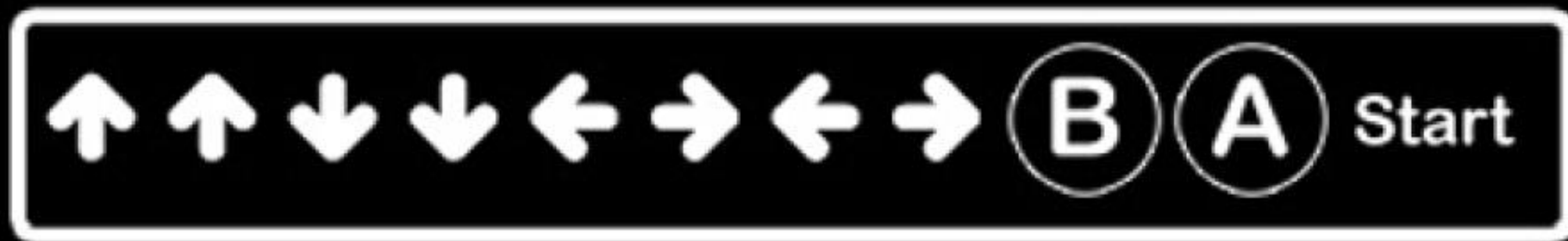
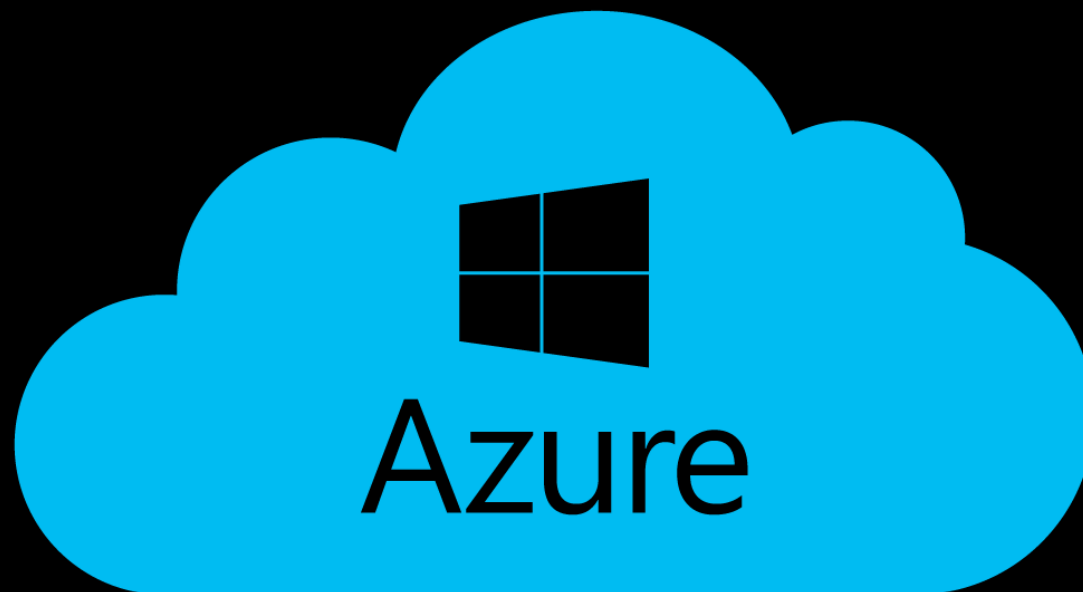
August Winterstein - F5 Systems Engineer

WHY ARE WE HERE?

- Secure connectivity to the cloud is the biggest hurdle to DoD's cloud adoption
- DoD needs a secure architecture that is easy to deploy and repeatable
- This architecture needs to comply with SCCA FRD
- Enable DoD's cloud adoption
 - Agility
 - Scalability
 - Power
 - Speed

F5 Partnership

- F5's platform covers almost every SCCA requirement
- Large presence in DoD today
- Understanding of DoD policy
- Passionate about the DoD's success



Let's start the demo!

State of DOD Cloud







Data Breach

Cyber Attack

Protection Failed

Data Leak Detected

System Safety Compromised

Lots of Barriers to Cloud Adoption



- Cloud Access Points
- VDSS/VDMS Requirements
- FIPS Compliance
- Contracts
- Accreditation
- Workforce Skill Sets

To CAP or not to CAP?



- DISA
- SPAWAR
- No CAP?
- Stand up your own?

But There Is Hope



- Some Early Adopters
- Office 365 is a Key Driver
- Cloud Service Providers are Ramping Up Fed Offerings
- Navy Will Be a Big Cloud Customer Over the Next 5 Years
 - Application Hosting (1700ish Apps)
 - Office 365 for 700,000+ Users

Terms

- **SCCA – Secure Cloud Computing Architecture**
 - 4 Components
- **CAP – Cloud Access Point**
 - ICAP – Internal Cloud Access Point
 - BCAP – Boundary Cloud Access Point
- **VDSS – Virtual Datacenter Security Stack**
- **VDMS – Virtual Datacenter Management Services**
 - Management of other Services
- **TCCM – Trusted Cloud Credential Manager**
 - A person

Requirements

The VDSS shall perform break and inspection of SSL/TLS communication traffic supporting single and dual authentication for traffic destined to systems hosted within the CSE12.

The VDSS shall provide a capability that monitors network and system activities to stop or block detected malicious activity.

The VDSS shall provide a capability to inspect and filter application layer conversations based on a predefined set of rules (including HTTP) to identify and block malicious content.

The VDSS shall maintain virtual separation of all management, user, and data traffic.

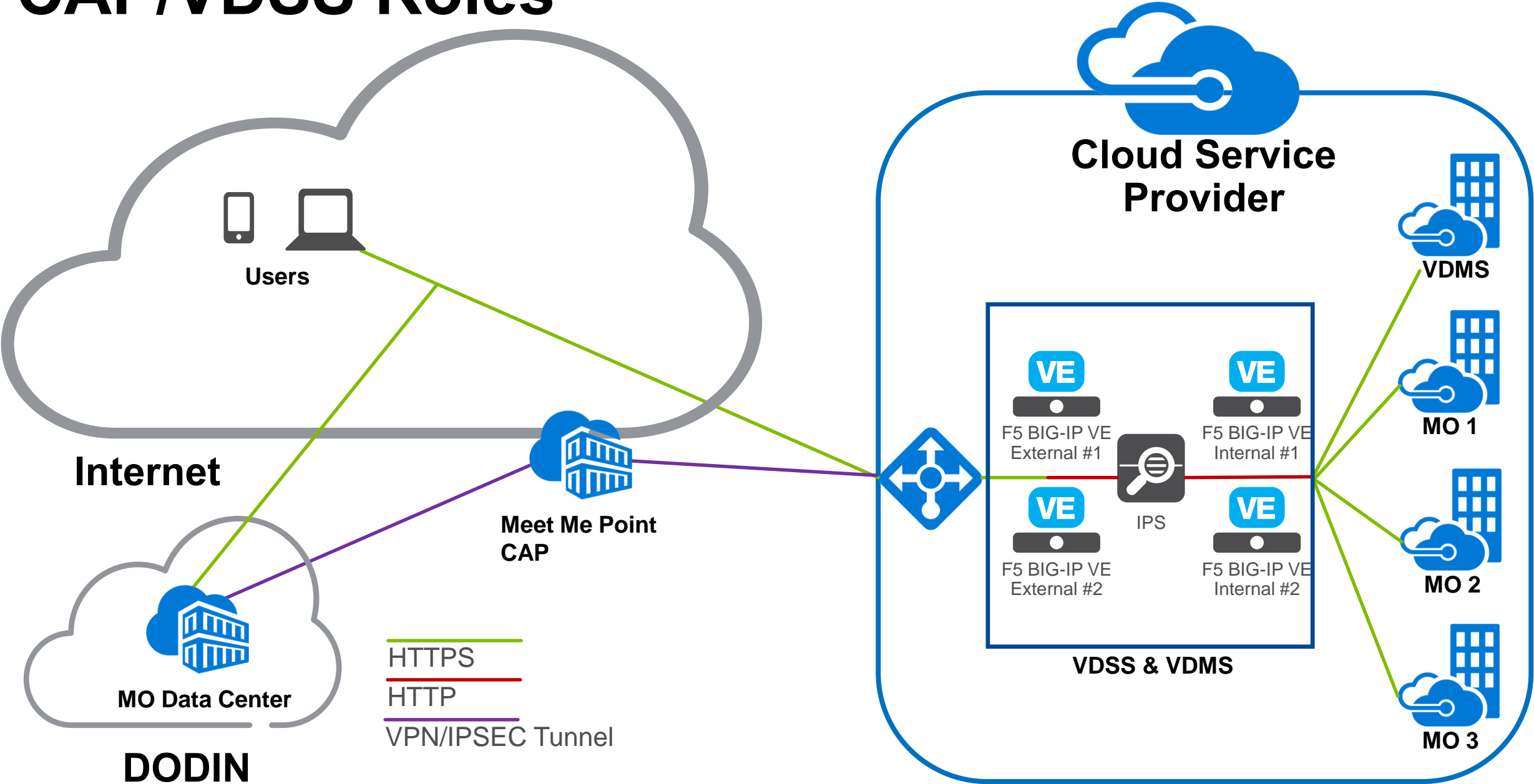
The VDSS shall provide a reverse proxy capability to handle access requests from client systems.

The VDSS shall inspect and filter traffic traversing between mission owner virtual private networks/enclaves.

The VDSS shall provide a capability that can distinguish and block unauthorized application layer traffic.

VDSS shall allow the use of encryption for segmentation of management traffic.

CAP/VDSS Roles



BCAP - Requirements

| REQ ID. | BCAP Security Requirements | Module |
|-----------|---|---------|
| 2.1.1.1.1 | The BCAP shall provide the capability to detect and prevent malicious code injection into the DISN originating from the CSE | ASM |
| 2.1.1.1.2 | The BCAP shall provide the capability to detect and thwart single and multiple node DOS attacks | ASM/AFM |
| 2.1.1.1.3 | The BCAP shall provide the ability to perform detection and prevention of traffic flow having unauthorized source and destination IP addresses, protocols, and Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) ports | ASM |
| 2.1.1.1.4 | The BCAP shall provide the capability to detect and prevent IP Address Spoofing and IP Route Hijacking | ASM |
| 2.1.1.1.5 | The BCAP shall provide the capability to prevent device identity policy infringement (prevent rogue device access) | APM |
| 2.1.1.1.6 | The BCAP shall provide the capability to detect and prevent passive and active network enumeration scanning originating from within the CSE | AFM |
| 2.1.1.1.7 | The BCAP shall provide the capability to detect and prevent unauthorized data exfiltration from the DISN to an end-point inside CSE | Limited |
| 2.1.1.1.8 | The BCAP and/or BCAP Management System shall provide the capability to sense, correlate, and warn on advanced persistent threats | ASM |

BCAP – Requirements Cont.

| REQ ID. | | Module |
|------------|--|-----------|
| 2.1.1.1.9 | The BCAP shall provide the capability to detect custom traffic and activity signatures | ASM |
| 2.1.1.1.10 | The BCAP shall provide an interface to conduct ports, protocols, and service management (PPSM) activities in order to provide control for BCND providers | AFM/APM |
| 2.1.1.1.11 | The BCAP shall provide full packet capture (FPC) for traversing communications | TMOS/Core |
| 2.1.1.1.12 | The BCAP shall provide network packet flow metrics and statistics for all traversing communications | TMOS/Core |
| 2.1.1.1.13 | The BCAP shall provide the capability to detect and prevent application session hijacking | ASM |

VDSS - Requirements

| REQ ID. | BCAP Security Requirements | Module |
|---------|---|---------|
| 2.1.2.1 | The VDSS shall maintain virtual separation of all management, user, and data traffic. | LTM |
| 2.1.2.2 | The VDSS shall allow the use of encryption for segmentation of management traffic. | LTM |
| 2.1.2.3 | The VDSS shall provide a reverse proxy capability to handle access requests from client systems. | LTM |
| 2.1.2.4 | The VDSS shall provide a capability to inspect and filter application layer conversations based on a predefined set of rules (including HTTP) to identify and block malicious content. | ASM |
| 2.1.2.5 | The VDSS shall provide a capability that can distinguish and block unauthorized application layer traffic. | ASM |
| 2.1.2.6 | The VDSS shall provide a capability that monitors network and system activities to detect and report malicious activities for traffic entering and exiting Mission Owner virtual private networks/enclaves. | ASM |
| 2.1.2.7 | The VDSS shall provide a capability that monitors network and system activities to stop or block detected malicious activity. | ASM |
| 2.1.2.8 | The VDSS shall inspect and filter traffic traversing between mission owner virtual private networks/enclaves. | LTM/ASM |
| 2.1.2.9 | The VDSS shall perform break and inspection of SSL/TLS communication traffic supporting single and dual authentication for traffic destined to systems hosted within the CSE12. | LTM/APM |

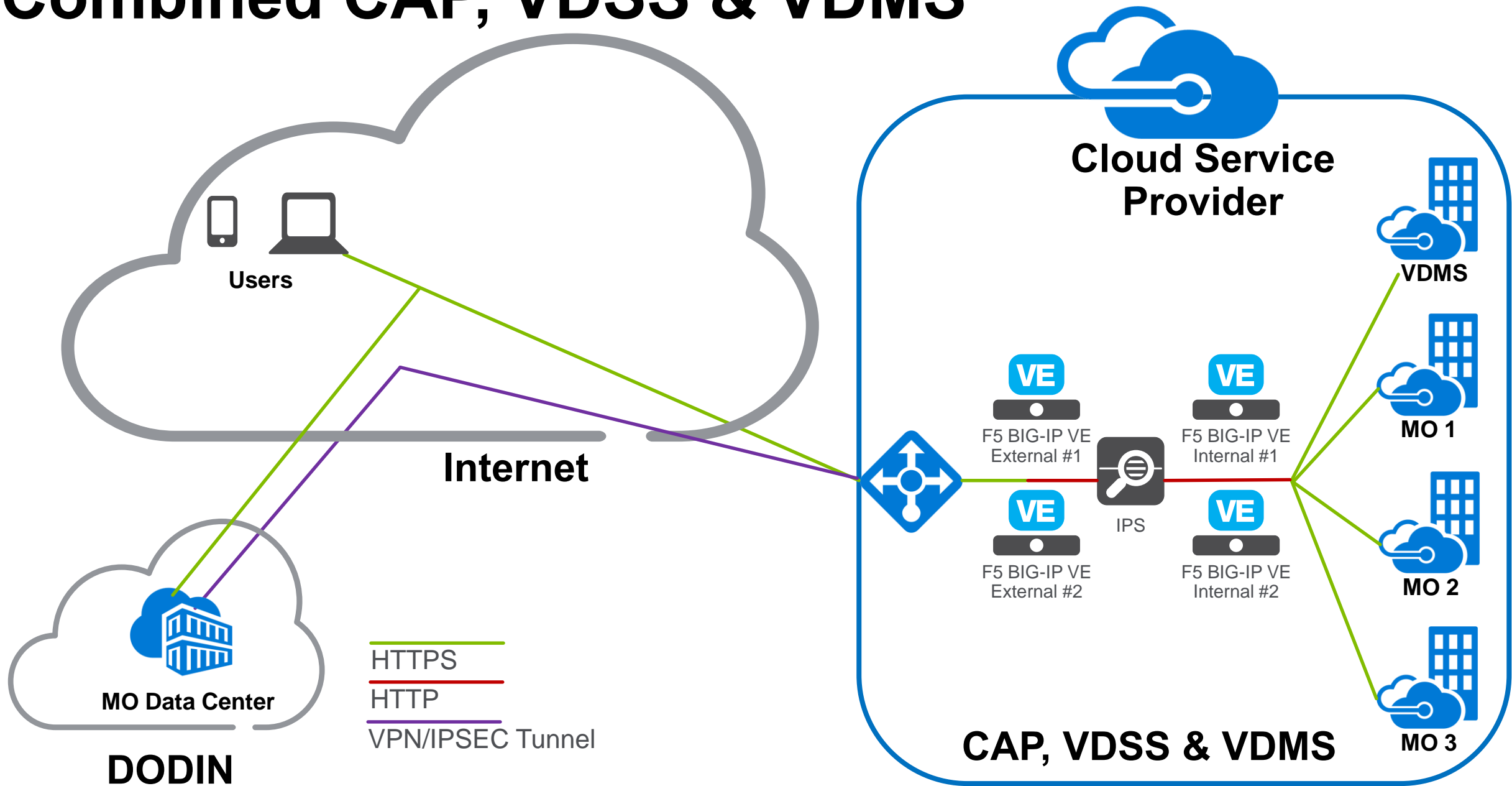
VDSS – Requirements Cont.

| REQ ID. | BCAP Security Requirements | Module |
|----------|--|-----------|
| 2.1.2.10 | The VDSS shall provide an interface to conduct ports, protocols, and service management (PPSM) activities in order to provide control for MCD operators. | APM/AFM |
| 2.1.2.11 | The VDSS shall provide a monitoring capability that captures log files and event data for cybersecurity analysis. | LTM |
| 2.1.2.12 | The VDSS shall provide or feed security information and event data to an allocated archiving system for common collection, storage, and access to event logs by privileged users performing Boundary and Mission CND activities. | TMOS/Core |
| 2.1.2.13 | The VDSS shall provide a <u>FIPS-140-2 compliant encryption key management</u> system for storage of DoD generated and assigned server private encryption key credentials for access and use by the Web Application Firewall (WAF) in the execution of SSL/TLS break and inspection of encrypted communication sessions. | LTM |
| 2.1.2.14 | The VDSS shall provide the capability to detect and identify application session hijacking. | ASM |
| 2.1.2.15 | The VDSS shall provide a DoD DMZ Extension to support to support Internet Facing Applications. | LTM |
| 2.1.2.16 | The VDSS shall provide full packet capture (FPC) or cloud service equivalent FPC capability for recording and interpreting traversing communications. | LTM |
| 2.1.2.17 | The VDSS shall provide network packet flow metrics and statistics for all traversing communications. | LTM |
| 2.1.2.18 | The VDSS shall provide for the inspection of traffic entering and exiting each mission owner virtual private network. | LTM |

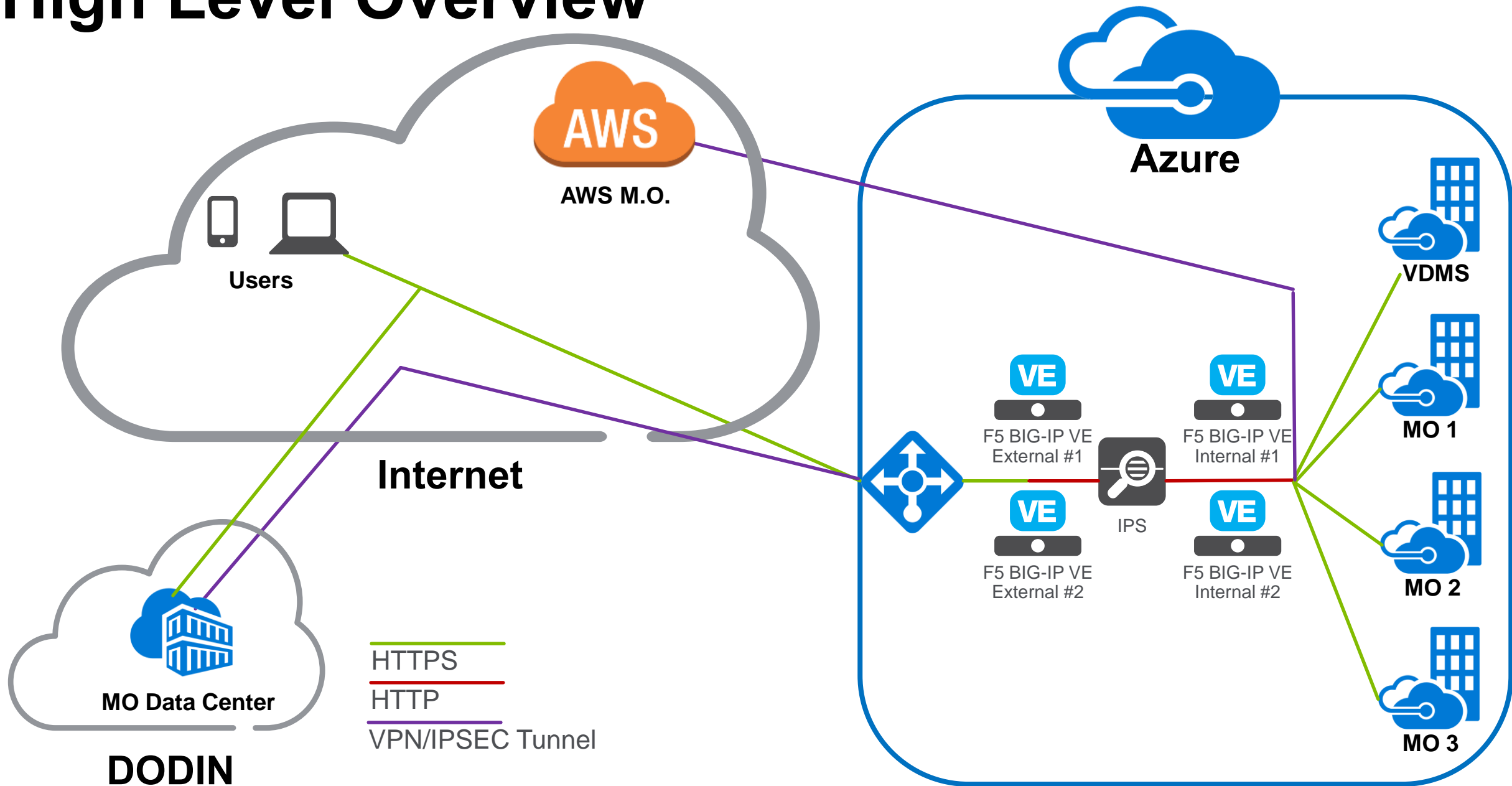
VDMS – Requirements

| REQ ID. | BCAP Security Requirements | F5 |
|---------|---|-------------------|
| 2.1.3.1 | The VDMS shall provide Assured Compliance Assessment Solution (ACAS), or approved equivalent, to conduct continuous monitoring for all enclaves within the CSE. | N/A |
| 2.1.3.2 | The VDMS shall provide Host Based Security System (HBSS). | N/A |
| 2.1.3.3 | The VDMS shall provide identity services to include an OCSP responder for remote system DoD CAC two-factor authentication of DoD privileged users to systems instantiated within the CSE. | APM |
| 2.1.3.4 | The VDMS shall provide a configuration and update management system to serve systems and applications for all enclaves within the CSE. | BIG-IQ |
| 2.1.3.5 | The VDMS shall provide logical domain services to include directory access, directory federation, DHCP, and DNS for all enclaves within the CSE. | APM/BIG-IP DNS |
| 2.1.3.6 | The VDMS shall provide a network for managing systems and applications within the CSE that is logically separate from the user and data networks. | LTM/APM |
| 2.1.3.7 | The VDMS shall provide a system, security, application, and user activity event logging and archiving system for common collection, storage, and access to event logs by privileged users performing BCP and MCP activities. | TMOS/Core |
| 2.1.3.8 | The VDMS shall provide for the exchange of DoD privileged user authentication and authorization attributes with the CSP's Identity and access management system to enable cloud system provisioning, deployment, and configuration. | APM |
| 2.1.3.9 | The VDMS shall implement the technical capabilities necessary to execute the mission and objectives of the TCCM role. | APM |

Combined CAP, VDSS & VDMS



High Level Overview



Extensibility

Meet Me
Point



Express
Routes



IPSEC
Tunnels



Physical TLS
Termination
FIPS140-2 L3



IDS/IPS
NGFW
DLP
& More



Voltron is a Verb



F5

—

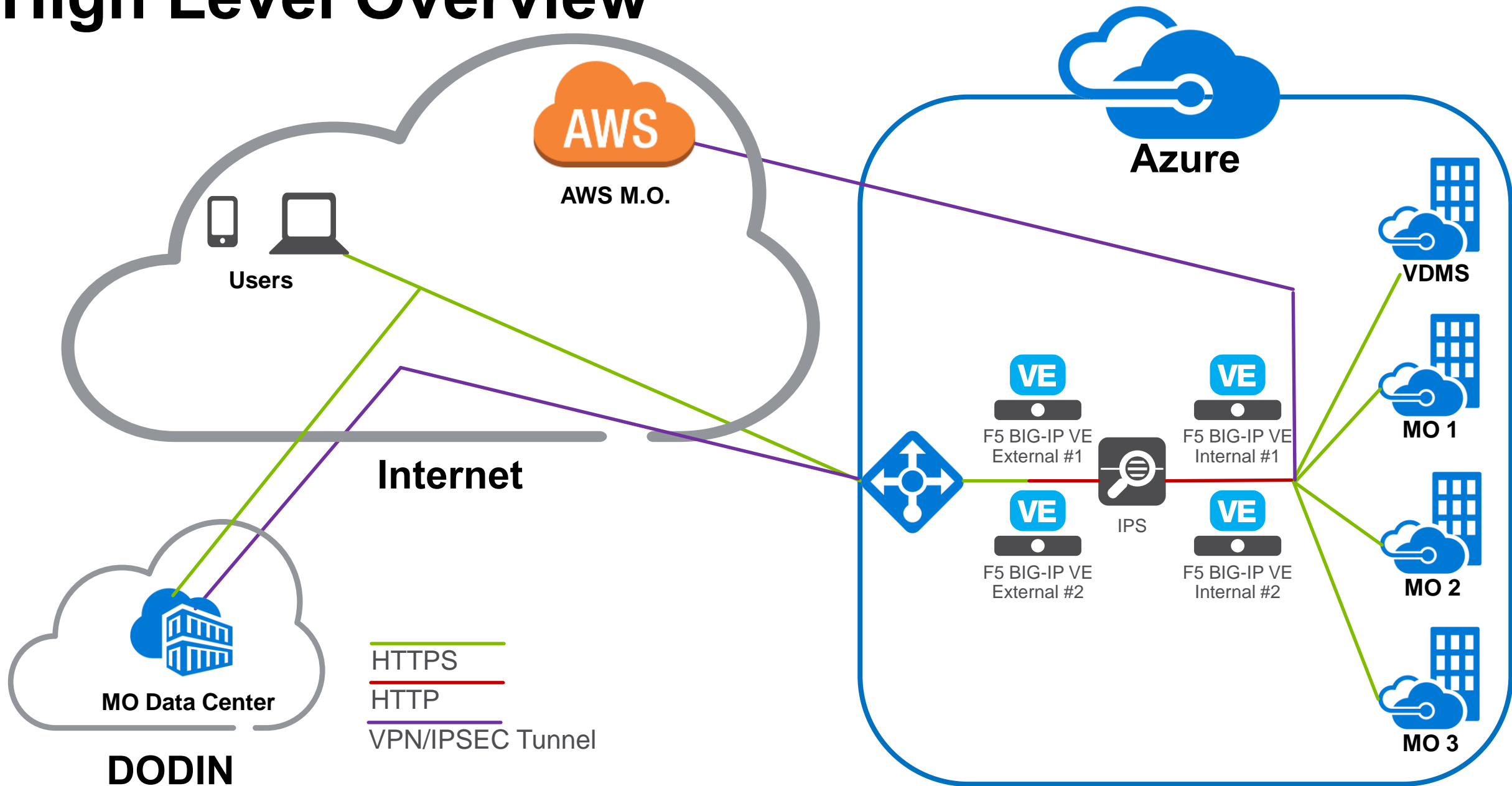
What are our application services?



- **App Security** – SSL inspection, DDoS protection, Network Firewall, DNS Firewall, L7 Web Application Firewall, bot detection, anti-fraud, anti-phishing, compliance reporting.
- **App Access & Identity** – Endpoint inspection, anti-malware, SAML federation, Cloud federation, Single Sign-On, SSL VPN, per app VPN, MDM integration.
- **App Availability** – Data center & server load balancing, DNS caching and DNS resolution, cloud bursting, disaster recovery.



High Level Overview



Protect Your Public Cloud Apps with F5 WAF



Ensure continuous business operation by protecting applications and their data

The Problem

Protecting your applications & data from attacks or loss?

- Cloud vendor's basic firewall capabilities do not protect applications layer attacks
- Constantly evolving array of attack surfaces and frameworks
- Most attacks are hidden in encrypted traffic
- Web application attacks accounted for 40% of data breaches in 2016¹

The Solution

BIG-IP ASM VE

- Complete protection against OWASP top 10 and mitigation of L7 DDoS attacks
- Automated-learning adapts security policies to protect against newly emerging attack types
- SSL Decryption to provide visibility and mitigate encrypted attacks
- Supports both positive and negative security models
- Automated patches mitigate zero-day attacks

Benefits

Reduce Business Risk

- Prevent attackers taking down applications and data theft, thus increasing user satisfaction and business revenue
- Prevent data leakage that could damage company reputation
- Highly customizable security policies to suit individual business requirements
- Adherence with major regulatory standards (PCI-DSS, HIPAA etc.)

¹Verizon DBIR 2016 Report

Secure Access to Public Cloud Apps with F5



Secure, simplified user access to all public cloud applications

The Problem

Providing access to apps without compromising security

- Many application users required to memorize large number of ID & Password combinations
- Admins managing multitude of policies & applications per user
- Concerns with putting company user information in the cloud
- Internet facing applications are ripe for hacks/attacks

The Solution

BIG-IP APM VE

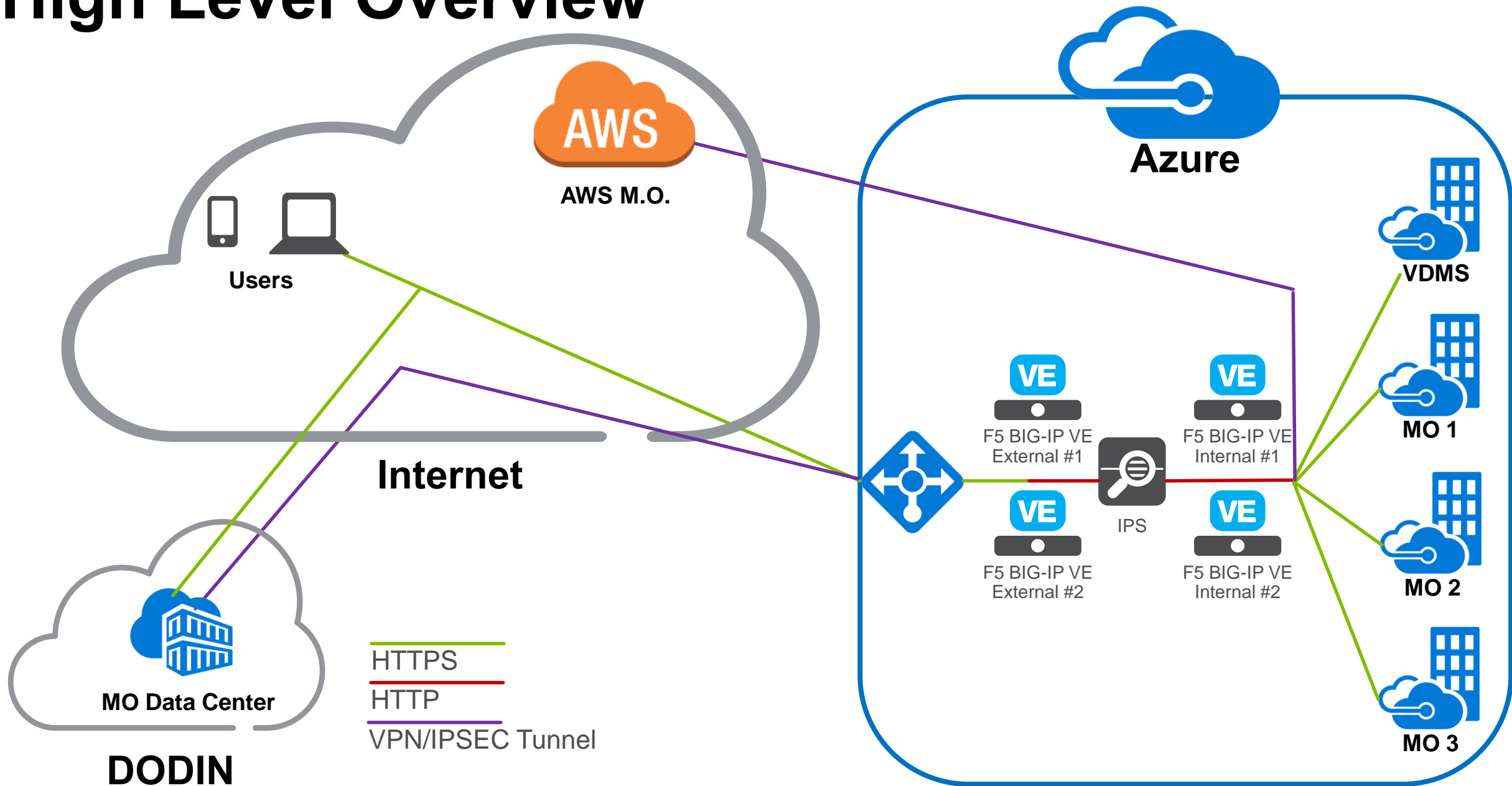
- Federated user identity and single sign on (SSO) across hybrid cloud deployments
- Vast array of authentication methods including Multi-factor Authentication & OAuth
- Integrates with on-premise active directory to maintain security of credentials
- Visual Policy editor enables fast, error-free policy creation & modification

Benefits

Simple & Secure Access

- Eliminate 'password fatigue' for users
- Fast, simple access policy development & deployment
- Single access solution for public cloud, SaaS and on premise applications
- No need to pass user credentials to applications, instead a trusted token is used to gain user access, enhancing security

High Level Overview



F5 Provides Intelligent Traffic Management



Deliver an optimized application experience for your customers

The Problem

Ensuring application availability

- Lost Revenue resulting from high-latency or unavailability of applications
- Lack of visibility and programmatic control over encrypted network traffic
- Complex configuration and management of application services

The Solution

BIG-IP LTM VE

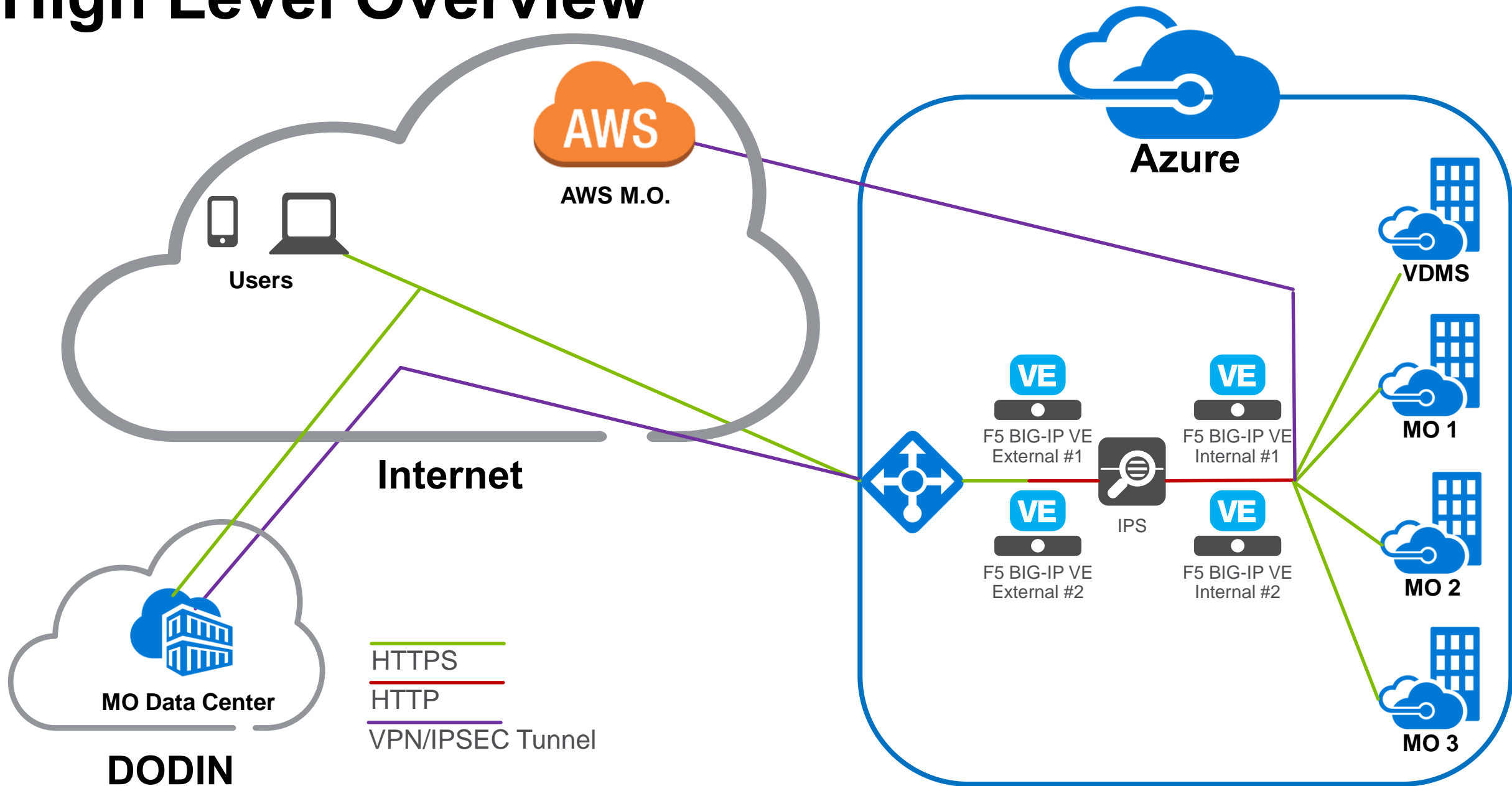
- Advanced traffic management capabilities with 27 supported protocols and 7 load balancing algorithms
- Industry best SSL offloading
- Programmability and manipulation of traffic flows through F5 iRules
- Simplified deployment and management of applications with F5 iApps templates

Benefits

Increased app performance & availability

- Minimized application latency for assured user experience and customer satisfaction
- SSL offloading combined with F5 iRules provides visibility and control over traffic, tightening network security.
- Automated deployments reduce management complexity

High Level Overview



F5 Delivers Global Server Load Balancing



Hyper scale your DNS infrastructure and ensure app availability across hybrid-cloud environments

The Problem

Improving Global Application Performance

- High-latency applications or inability to connect to apps impacts user experience
- Large volumetric DNS DDoS attacks, cache poisoning and other security threats impact business operations
- Inability to load balance across hybrid-cloud environments

The Solution

BIG-IP DNS VE

- Re\Direct users to globally distributed servers across multi-cloud environments based on their real-time operating performance
- Provide DNS firewall services and DNSSEC signing to ensure security of DNS infrastructure
- VE's provide up to 900,000 DNS query RPS

Benefits

Enhanced user experience & business revenue

- Provide optimized user experience by reducing latency from 300ms to as little as 15ms
- Prevent DNS DDoS attacks & cache poisoning, leading to increased app availability and revenue
- Increase availability by utilizing multiple public clouds to host identical applications

Secure Azure Computing Architecture (SACA)

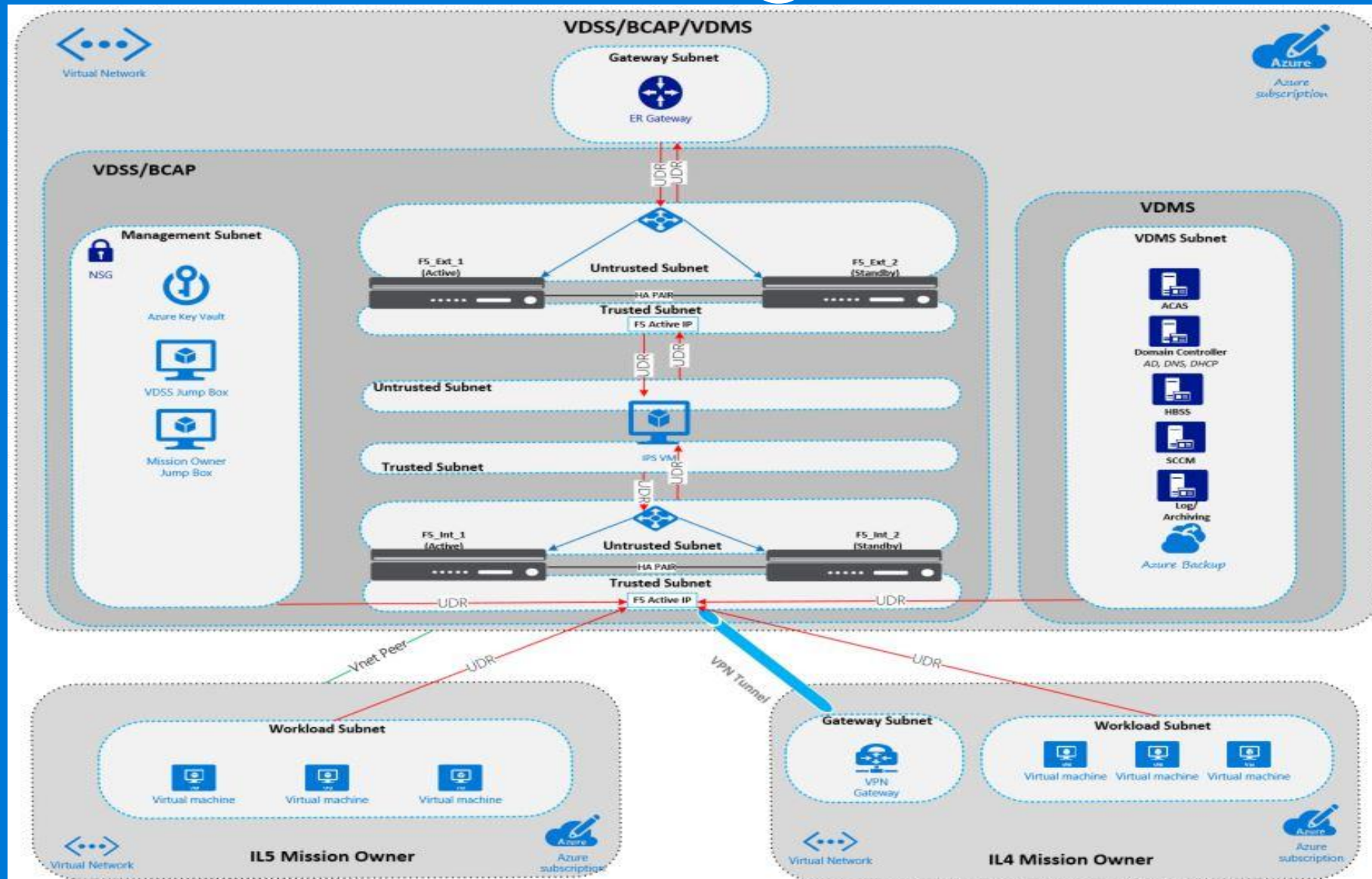


F5 / Microsoft SACA

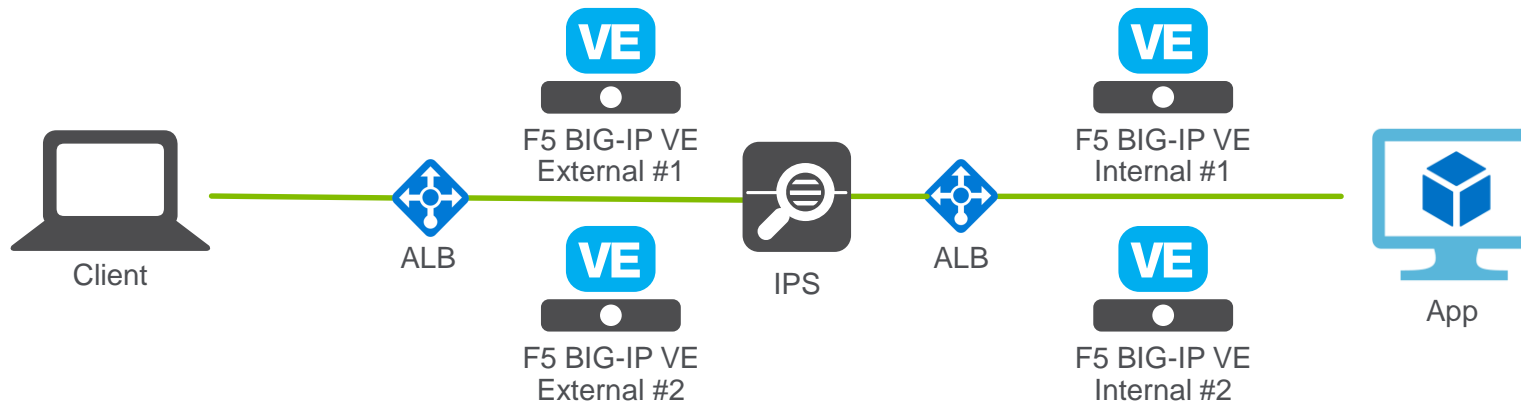
- **High Availability**
- Ingress / Egress Traffic
- **Visibility**
- L3/L4 Logging
- L7 Request Logging
- SSL Inspection
- **Security**
- L3/L4, L7 DDoS
- Network Firewall
- Web Application Firewall
- **Azure Integrated**



SACA Diagram

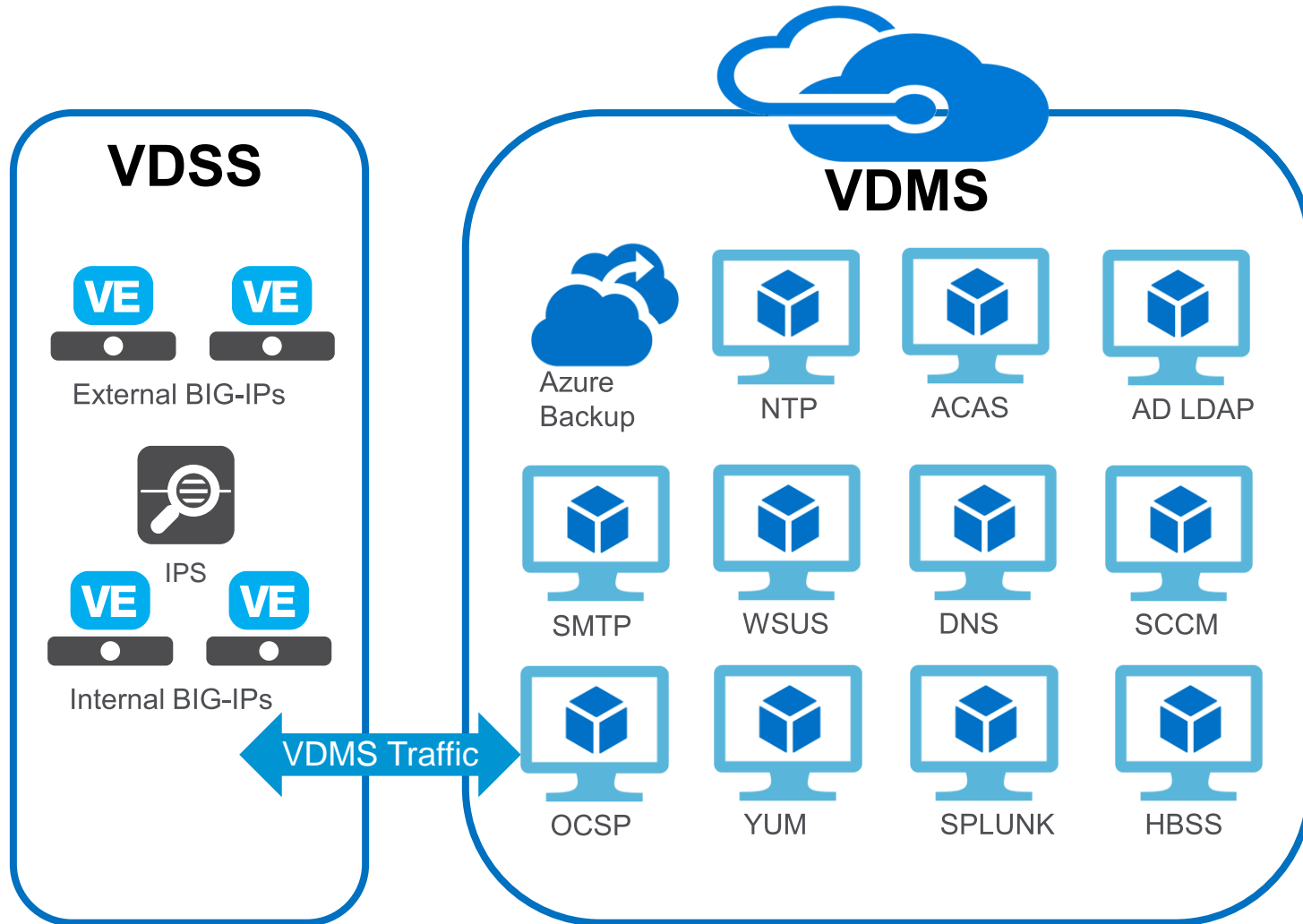


SACA - VDSS Overview



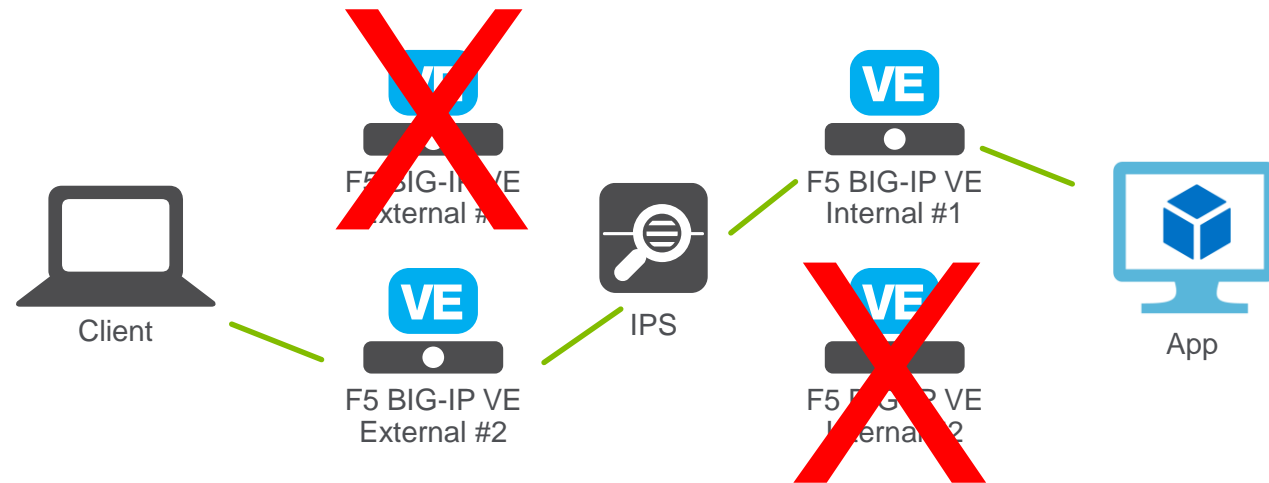
- **High Availability**
 - External / Internal pair of F5 devices
- **Visibility**
 - Traffic Logging
 - SSL inspection zone
- **Authentication**
 - CAC/ALT/PIV Authentication
- **Security**
 - Network Firewall
 - Web Application Firewall
- **Prescribed Solutions**
 - IPS Firepower/McAfee NSP

SACA - VDMS Overview

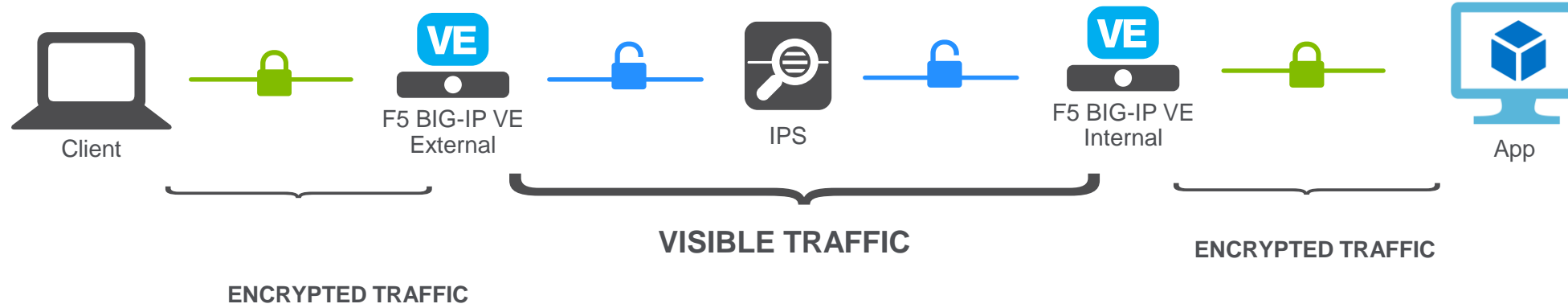


- **Visibility**
 - Traffic Logging
- **Authentication**
 - Azure AD
- **Continuous Monitoring**
 - Log Archiving
 - Azure Backup
 - SCCM
- **Prescribed Solutions**
 - ACAS
 - SPLUNK
 - HBSS

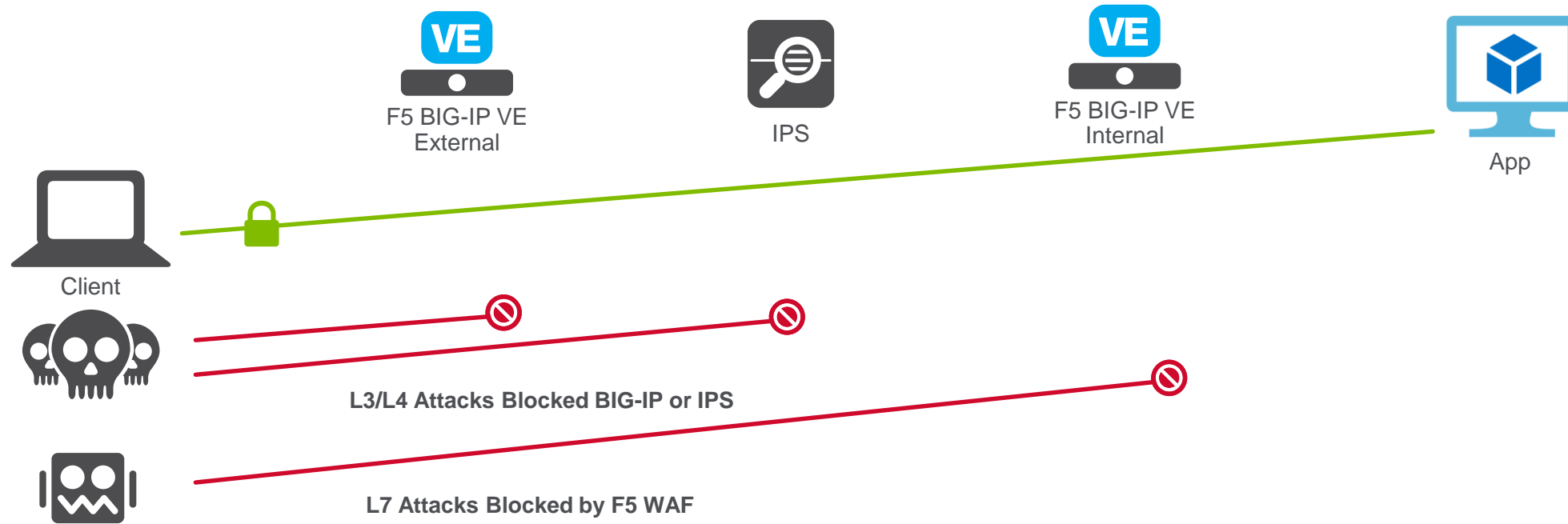
High Availability



SSL Visibility



Layered Security





Demo



After Deployment Completes

n_F5_External
e group

| | | | |
|--------------------------|---|-----------------|-------------------|
| <input type="checkbox"/> |  | f5-alb-ext-pip0 | Public IP address |
| <input type="checkbox"/> |  | f5-alb-ext-pip1 | Public IP address |

Resource group ([change](#))

[chen_F5_External](#)

IP address

52.247.168.220

DNS name

-

Associated to

[f5-ext-alb](#)

Click to copy



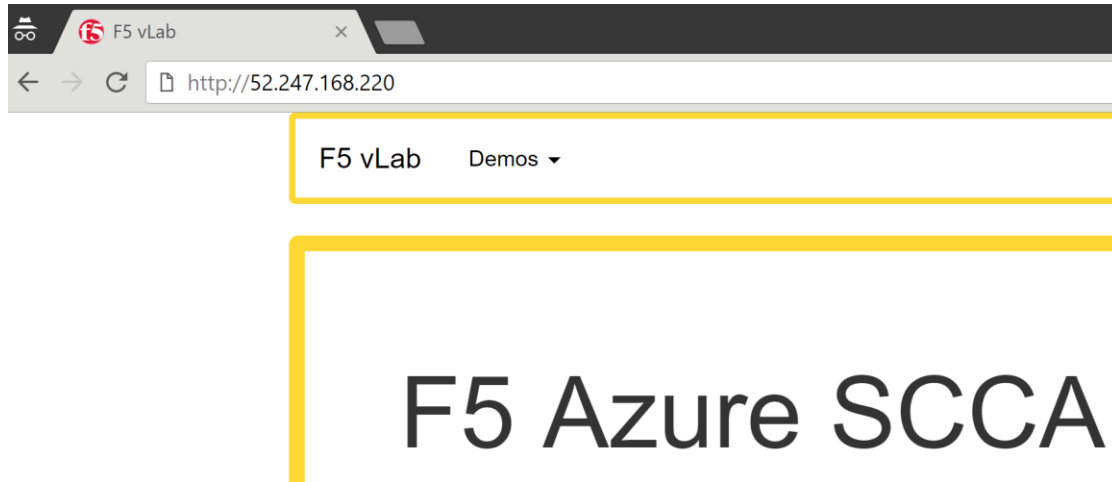
[Azure F5 SCC](#)

Subscription ID

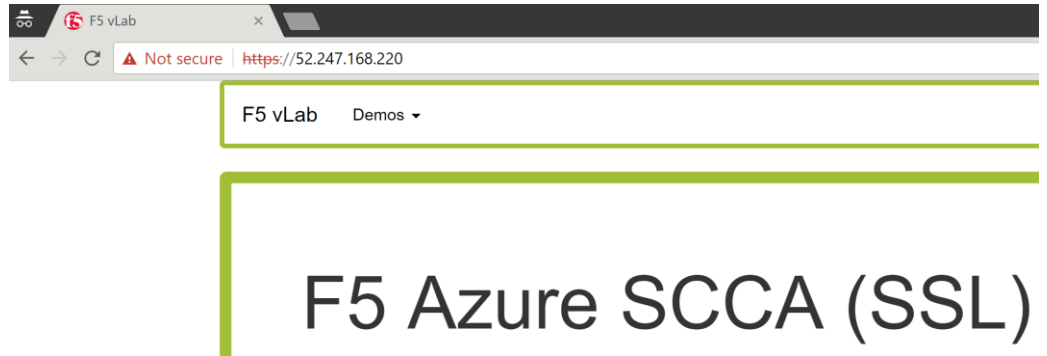
8e9cb3c0-22c

Demo Sites

HTTP



HTTPS (SSL)



Text Version

HTTP

```
← → ↻ http://52.247.168.220/txt

=====
F5 Deno-Apex
=====

Node Name: F5 Azure SCCA
Short Name: VDSSJumpBoxLinux

Server IP: 172.16.0.5
Server Port: 80

Client IP: 100.45.96.143
Client Port: 52079

Client Protocol: HTTP
Request Method: GET
Request URI: /txt

host_header: 52.247.168.220
user-agent: Mozilla/5.0 (Windows NT 10.0; Win
```

HTTPS (SSL)

```
← → ↻ ⚠ Not secure https://52.247.168.220/txt

=====
F5 Deno-Apex
=====

Node Name: F5 Azure SCCA (SSL)
Short Name: VDSSJumpBoxLinux

Server IP: 172.16.0.5
Server Port: 443

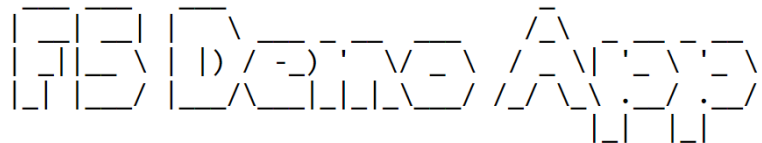
Client IP: 192.168.5.4
Client Port: 53150

Client Protocol: HTTPS
Request Method: GET
Request URI: /txt

host_header: 52.247.168.220
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64
x-forwarded-for: 100.45.96.143
```

Packet Capture: IPS

No SSL Visibility



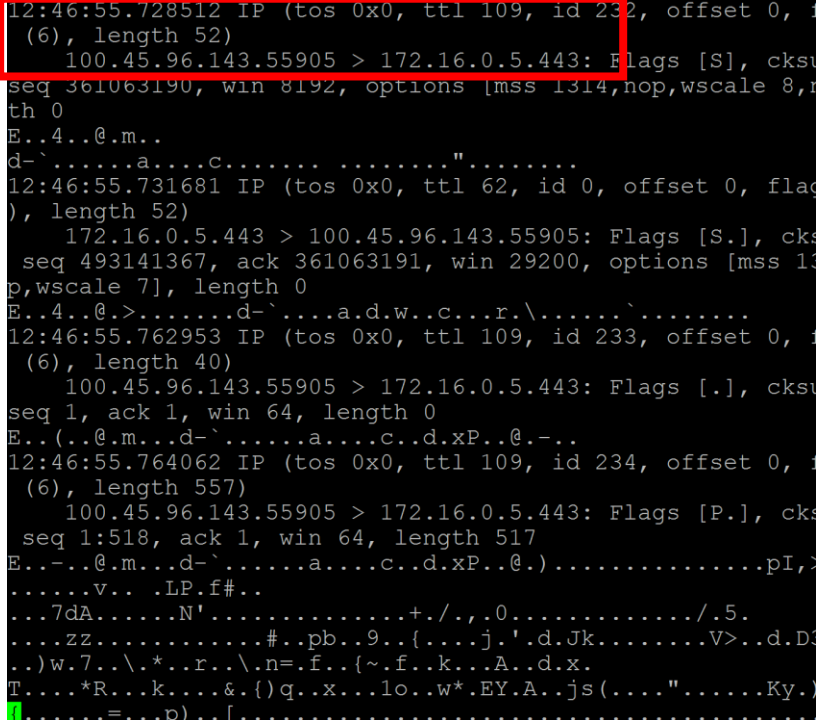
Node Name: F5 Azure SCCA (SSL)
Short Name: VDSSJumpBoxLinux

Server IP: 172.16.0.5
Server Port: 8443

Client IP: 100.45.96.143
Client Port: 55906

Client Protocol: HTTPS
Request Method: GET
Request URI: /txt

Packet Capture



`sudo tcpdump -i eth0 -vvv -n -s 0 -A "(port 80 or port 443) and (host 192.168.4.7 or host 100.45.96.143)"`

Text Version

HTTP

```
← → ↻ http://52.247.168.220/txt

=====
F5 Deno-Apex
=====

Node Name: F5 Azure SCCA
Short Name: VDSSJumpBoxLinux

Server IP: 172.16.0.5
Server Port: 80

Client IP: 100.45.96.143
Client Port: 52079

Client Protocol: HTTP
Request Method: GET
Request URI: /txt

host_header: 52.247.168.220
user-agent: Mozilla/5.0 (Windows NT 10.0; Win
```

HTTPS (SSL)

```
← → ↻ ⚠ Not secure https://52.247.168.220/txt

=====
F5 Deno-Apex
=====

Node Name: F5 Azure SCCA (SSL)
Short Name: VDSSJumpBoxLinux

Server IP: 172.16.0.5
Server Port: 443

Client IP: 192.168.5.4
Client Port: 53150

Client Protocol: HTTPS
Request Method: GET
Request URI: /txt

host_header: 52.247.168.220
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64
x-forwarded-for: 100.45.96.143
```

Packet Capture: External

HTTP

```
11:57:51.883610 IP (tos 0x0, ttl 255, id 50855, offset 0, flags 0x0000, length 669) 52.247.168.220.http > 100.45.96.143.64499: Flags [P], cksum 583, win 4050, length 669 out slot1/tmm3 lis=/Common/ssl_visibl...E.....@.....4...d-`..P..[... ..P..*.G..HTTP/1.1
Date: Fri, 19 Jan 2018 11:57:51 GMT
Server: Apache/2.4.29 (Unix) LibreSSL/2.5.5
Accept-Ranges: bytes
X-COLOR: ffd734
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/plain

158
=====
IS Demo App
=====

Node Name:
d
F5 Azure SCCA
```

HTTPS (SSL)

```
12:02:58.623093 IP (tos 0x0, ttl 110, id 23718, offset 0, flags 0x0000, length 615) 100.45.96.143.65218 > 52.247.168.220.https: Flags [P.], cksum 326, ack 1857716426, win 16616, length 615 in slot1/tmm1 lis=/Common/ssl_visibl...E...\.@.n..3d-`.4.....`...n...P.@.....b.....X2...
...06p{...|+...61V@...:|...3V.....<gq...<.....Sk.T...
...+.A.+..U.....y.H
...m...H.....n.<.L....(.....zp.O...!.R...4..[4..0!..."...qy
3..&.f.....eg.....'.=^L+kM.g. ....3=...j.pG.w.....R.N.....
...Common/ssl_visibl...
12:02:58.623102 IP (tos 0x0, ttl 255, id 59319, offset 0, flags 0x0000, length 515) 52.247.168.220.https > 100.45.96.143.65218: Flags [.], cksum 515, win 5503, length 0 out slot1/tmm1 lis=/Common/ssl_visibl...E...(.@.....4...d-`.....n...`...P...../Common/ss
12:02:58.624154 IP (tos 0x0, ttl 255, id 59321, offset 0, flags 0x0000, length 586) 100.45.96.143.12461 > 192.168.4.7.http: Flags [P.], cksum 1307191016, ack 2516132629, win 6428, length 586 out slot1/tmm1 lis=/Common/ssl_visibl...E...r...@.....`d-`.....0..PM.$...#.P.....GET /txt HTTP/1.1
Host: 52.247.168.220
```

Client to External F5: HTTPS (SSL)
External F5 to IPS: HTTP

tcpdump -i 0.0 -vvv -n -s 0 -A "(port 80 or port 443) and (host 192.168.2.7 or host 100.45.96.143)"

Packet Capture: IPS

HTTP

```
12:07:39.886603 IP (tos 0x0, ttl 62, id 22419, offset 0, flags [P.], cksum 172.16.0.5.80 > 100.45.96.143.49686: length 668)
length 668: HTTP, length: 668
  HTTP/1.1 200 OK
  Date: Fri, 19 Jan 2018 12:07:39 GMT
  Server: Apache/2.4.29 (Unix) LibreSSL/2.5.5
  Accept-Ranges: bytes
  X-COLOR: ffd734
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Transfer-Encoding: chunked
  Content-Type: text/plain

158
=====
F5 DENO APP
=====

Node Name:
d
F5 Azure SCCA
```

HTTPS (SSL)

```
12:09:55.263551 IP (tos 0x0, ttl 254, id 11082, offset 0, flags [P.], cksum 192.168.4.7.80 > 100.45.96.143.2480: length 934)
length 934: HTTP, length: 934
  HTTP/1.1 200 OK
  Accept-Ranges: bytes
  X-COLOR: ffd734
  Content-Type: text/plain
  Connection: Keep-Alive
  Date: Fri, 19 Jan 2018 12:09:55 GMT
  Age: 462
  Content-Length: 767

=====
F5 DENO APP
=====

Node Name: F5 Azure SCCA (SSL)
Short Name: VDSSJumpBoxLinux
```

`sudo tcpdump -i eth0 -vvv -n -s 0 -A "(port 80 or port 443) and (host 192.168.2.7 or host 100.45.96.143)"`

Packet Capture: Internal

HTTP

```
12:13:19.965630 IP (tos 0x0, ttl 63, id 58759, of
  172.16.0.5.http > 100.45.96.143.50618: Flags
583, win 30264, length 669 out slot1/tmm2 lis=/Co
....E.....@.?......d-`..P....vD....P.v8s...HTTP/
Date: Fri, 19 Jan 2018 12:13:19 GMT
Server: Apache/2.4.29 (Unix) LibreSSL/2.5.5
Accept-Ranges: bytes
X-COLOR: ffd734
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/plain

158
=====
F5 DevNet App
=====
Node Name:
d
F5 Azure SCCA
```

HTTPS (SSL)

```
12:41:42.444921 IP (tos 0x0, ttl 255, id 16722, of
  192.168.4.7.http > 100.45.96.143.48118: Flags
win 54883, length 0 out slot1/tmm2 lis=/Common/ht
....E..(AR@.....d-`..P..#....X..P..c.....7....
12:41:42.444940 IP (tos 0x0, ttl 255, id 16724, of
  192.168.4.7.http > 100.45.96.143.48118: Flags
586, win 54883, length 954 out slot1/tmm2 lis=/Co
....E...AT@....U....d-`..P..#....X..P..c.@..HTTP/1
Accept-Ranges: bytes
X-COLOR: ffd734
Content-Type: text/plain
Connection: Keep-Alive
Date: Fri, 19 Jan 2018 12:41:42 GMT
Age: 2369
Content-Length: 767
=====
F5 DevNet App
=====
Node Name: F5 Azure SCCA (SSL)
```

`sudo tcpdump -i eth0 -vvv -n -s 0 -A "(port 80 or port 443) and (host 192.168.4.7 or host 100.45.96.143)"`

Logging: Firewall

| Security » Event Logs : Network : Firewall | | | | | | | | | | | | | | | | | |
|--|---------------------|----------------|--------------------------|-----------------------------|---------------------|--------------|------------------|------------------|-----------|---------|-----------------|-------|------------------|-------------|---------|----------------|------|
| ⚙️ | | Protocol | Network | Network Address Translation | | DoS | Logging Profiles | | | | | | | | | | |
| | | | Last Hour | | Search | Reset Search | Custom Search... | | | | | | | | | | |
| | | | | | | | Source | | | | | | | Destination | | | |
| ✓ | Time | Context | Name | Policy Type | Policy Name | Rule | Subscriber ID | Subscriber Group | Region | FQDN | Address | Port | VLAN / Tunnel | Region | FQDN | Address | Port |
| <input type="checkbox"/> | 2018-01-15 19:37:30 | Virtual Server | /Common/mgmt_outbound_vs | Enforced | /Common/log_all_afm | allow_all | unknown | unknown | No-lookup | unknown | 172.16.0.7 | 34122 | /Common/internal | No-lookup | unknown | 13.72.43.40 | 443 |
| <input type="checkbox"/> | 2018-01-15 19:37:30 | Virtual Server | /Common/mgmt_outbound_vs | Enforced | /Common/log_all_afm | allow_all | unknown | unknown | No-lookup | unknown | 172.16.0.5 | 57290 | /Common/internal | No-lookup | unknown | 91.189.91.157 | 123 |
| <input type="checkbox"/> | 2018-01-15 19:37:30 | Virtual Server | /Common/mgmt_outbound_vs | Enforced | /Common/log_all_afm | allow_all | unknown | unknown | No-lookup | unknown | 172.16.0.7 | 34120 | /Common/internal | No-lookup | unknown | 13.72.43.40 | 443 |
| <input type="checkbox"/> | 2018-01-15 19:37:30 | Virtual Server | /Common/is_alive_vs | Enforced | /Common/log_all_afm | allow_all | unknown | unknown | No-lookup | unknown | 168.63.129.16 | 60812 | /Common/external | No-lookup | unknown | 192.168.0.5 | 80 |
| <input type="checkbox"/> | 2018-01-15 19:37:30 | Virtual Server | /Common/jumpbox_ssh_vs | Enforced | /Common/log_all_afm | allow_all | unknown | unknown | No-lookup | unknown | 221.194.44.211 | 48812 | /Common/external | No-lookup | unknown | 52.247.161.156 | 22 |
| <input type="checkbox"/> | 2018-01-15 19:37:30 | Virtual Server | /Common/mgmt_outbound_vs | Enforced | /Common/log_all_afm | allow_all | unknown | unknown | No-lookup | unknown | 172.16.0.7 | 37541 | /Common/internal | No-lookup | unknown | 91.189.89.198 | 123 |
| <input type="checkbox"/> | 2018-01-15 19:37:29 | Virtual Server | /Common/is_alive_vs | Enforced | /Common/log_all_afm | allow_all | unknown | unknown | No-lookup | unknown | 168.63.129.16 | 60805 | /Common/external | No-lookup | unknown | 192.168.0.5 | 80 |
| <input type="checkbox"/> | 2018-01-15 19:37:29 | Virtual Server | /Common/jumpbox_ssh_vs | Enforced | /Common/log_all_afm | allow_all | unknown | unknown | No-lookup | unknown | 221.194.47.239 | 53106 | /Common/external | No-lookup | unknown | 52.247.161.156 | 22 |
| <input type="checkbox"/> | 2018-01-15 19:37:28 | Virtual Server | /Common/mgmt_outbound_vs | Enforced | /Common/log_all_afm | allow_all | unknown | unknown | No-lookup | unknown | 172.16.0.5 | 41766 | /Common/internal | No-lookup | unknown | 13.72.43.40 | 443 |
| <input type="checkbox"/> | 2018-01-15 19:37:28 | Virtual Server | /Common/mgmt_outbound_vs | Enforced | /Common/log_all_afm | allow_all | unknown | unknown | No-lookup | unknown | 172.16.0.5 | 41764 | /Common/internal | No-lookup | unknown | 13.72.43.40 | 443 |
| <input type="checkbox"/> | 2018-01-15 19:37:28 | Virtual Server | /Common/jumpbox_rdp_vs | Enforced | /Common/log_all_afm | allow_all | unknown | unknown | No-lookup | unknown | 107.211.207.225 | 63474 | /Common/external | No-lookup | unknown | 52.247.161.156 | 3389 |
| <input type="checkbox"/> | 2018-01-15 19:37:28 | Virtual Server | /Common/mgmt_outbound_vs | Enforced | /Common/log_all_afm | allow_all | unknown | unknown | No-lookup | unknown | 172.16.0.5 | 49288 | /Common/internal | No-lookup | unknown | 23.97.32.78 | 443 |
| <input type="checkbox"/> | 2018-01-15 19:37:27 | Virtual Server | /Common/mgmt_outbound_vs | Enforced | /Common/log_all_afm | allow_all | unknown | unknown | No-lookup | unknown | 172.16.0.7 | 34114 | /Common/internal | No-lookup | unknown | 13.72.43.40 | 443 |
| <input type="checkbox"/> | 2018-01-15 19:37:27 | Virtual Server | /Common/mgmt_outbound_vs | Enforced | /Common/log_all_afm | allow_all | unknown | unknown | No-lookup | unknown | 172.16.0.7 | 34116 | /Common/internal | No-lookup | unknown | 13.72.43.40 | 443 |
| <input type="checkbox"/> | 2018-01-15 19:37:26 | Virtual Server | /Common/jumpbox_rdp_vs | Enforced | /Common/log_all_afm | allow_all | unknown | unknown | No-lookup | unknown | 107.211.207.225 | 62453 | /Common/external | No-lookup | unknown | 52.247.161.156 | 3389 |
| <input type="checkbox"/> | 2018-01-15 19:37:25 | Virtual Server | /Common/mgmt_outbound_vs | Enforced | /Common/log_all_afm | allow_all | unknown | unknown | No-lookup | unknown | 172.16.0.5 | 47459 | /Common/internal | No-lookup | unknown | 91.189.91.157 | 123 |
| <input type="checkbox"/> | 2018-01-15 19:37:25 | Virtual Server | /Common/mgmt_outbound_vs | Enforced | /Common/log_all_afm | allow_all | unknown | unknown | No-lookup | unknown | 172.16.0.7 | 49909 | /Common/internal | No-lookup | unknown | 91.189.89.198 | 123 |
| <input type="checkbox"/> | 2018-01-15 19:37:24 | Virtual Server | /Common/mgmt_outbound_vs | Enforced | /Common/log_all_afm | allow_all | unknown | unknown | No-lookup | unknown | 172.16.0.7 | 34110 | /Common/internal | No-lookup | unknown | 13.72.43.40 | 443 |

Logging: Web Application Firewall

Security » Event Logs : Application : Requests

Application Protocol Network Network Address Translation DoS Bot Defe

Q Date Newest

| | | |
|-------------------------------------|-----------------------------|-----|
| <input checked="" type="checkbox"/> | [HTTP] /headers/ | 200 |
| <input checked="" type="checkbox"/> | [HTTP] /viprion.ssvg | 200 |
| <input checked="" type="checkbox"/> | [HTTP] /appliance.ssvg | 200 |
| <input checked="" type="checkbox"/> | [HTTP] /virtualedition.ssvg | 200 |
| <input checked="" type="checkbox"/> | [HTTP] /mobile.ssvg | 200 |
| <input checked="" type="checkbox"/> | [HTTP] /css/f5footer.scss | 200 |
| <input checked="" type="checkbox"/> | [HTTP] /css/f5header.scss | 200 |
| <input checked="" type="checkbox"/> | [HTTP] /css/f5demo.css | 200 |

Delete Request Export Request

[HTTP] /headers/

| | |
|-------------------|----------------------|
| Geolocation | United States |
| Source IP Address | 205.153.92.178:58472 |
| Session ID | 59739fdff16de541 |

Request

Request actual size: 630 bytes.

```
GET /headers/ HTTP/1.0
Host: 52.247.160.49
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) App
fari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q
Referer: https://52.247.160.49/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: BIGipServerhttps_pool=83890348.47873.0000; TS0126
0b5fc8e520faf1e5d98ac4efbc1189e13e4f263fc503bb319acb
X-Forwarded-For: 205.153.92.178
```

Logging: Web Application Firewall

Security » Event Logs : Application : Requests

Application

Protocol

Network

Network Address Translation

DoS

Bot Defense

Logging Profiles

Q

↑ Date ↓

Newest ↓

☒ [HTTP] /etc/passwd

205.153.92.178

20:47:07 2018-01-16

5

N/A

☐ [HTTP] /headers/

205.153.92.178

20:43:22 2018-01-16

✓

200

☐ [HTTP] /viprion.ssvg

205.153.92.178

20:43:16 2018-01-16

✓

200

☐ [HTTP] /appliance.ssvg

205.153.92.178

20:43:16 2018-01-16

✓

200

☐ [HTTP] /virtualedition.ssvg

205.153.92.178

20:43:16 2018-01-16

✓

200

☐ [HTTP] /mobile.ssvg

205.153.92.178

20:43:16 2018-01-16

✓

200

☐ [HTTP] /css/f5footer.scss

205.153.92.178

20:43:16 2018-01-16

✓

200

☐ [HTTP] /css/f5header.scss

205.153.92.178

20:43:16 2018-01-16

✓

200

Delete Request

Export Request

Attack signature detected [2]

HTTP protocol compliance failed [2]

Illegal method [1]

[HTTP] /etc/passwd

| | | | |
|-------------------|---------------------|------------------|--|
| Geolocation | United States | Time | 2018-01-16 20:47:07 |
| Source IP Address | 205.153.92.178:8152 | Violation Rating | 5 <div></div> |
| Session ID | 58c8f55a0e90b58f | Attack Types | <div>Non-browser Client</div> <div>Information Leakage</div> <div>HTTP Parser Attack</div> |

Request

Response N/A

Request actual size: 121 bytes.

cat /etc/passwd / HTTP/1.1

User-Agent: Bad Hacker

Host: 52.247.160.49

Accept: */*

X-Forwarded-For: 205.153.92.178

Logging: Web Application Firewall

Delete RequestExport Request

Attack signature detected [2]

Detected Keyword

/etc/passwd

Attack Signature

Signature ID

200003056

Signature Name

"/etc" execution attempt (URI)

Context

URL

Applied Blocking Settings

Staged

Detected Keyword

/etc/passwd

Attack Signature

Signature ID

200003316

Signature Name

"passwd" execution attempt (URI)

Context

URL

Learn more

➔ Architecture Documentation:
<http://f5-azure-saca.readthedocs.io/en/latest/>

GitHub Repository:
<https://github.com/f5devcentral/f5-azure-saca>



Contact Info

F5

- John Manning – J.Manning@f5.com
- Archie Newell – A.Newell@f5.com
- Jimmy Jennings – J.Jennings@f5.com
- Paul Simmons – P.Simmons@f5.com

Microsoft

- Jason Henderson - Jason.Henderson@microsoft.com
- Kyle Hoyer - khoyer@microsoft.com



Upcoming Sessions

Privileged User Access - 11-12pm

- Jimmy Jennings, *Systems Engineer, F5*

Lunch - 12-12:30pm

Multi-Cloud TechTalk— 12:30-1:30pm

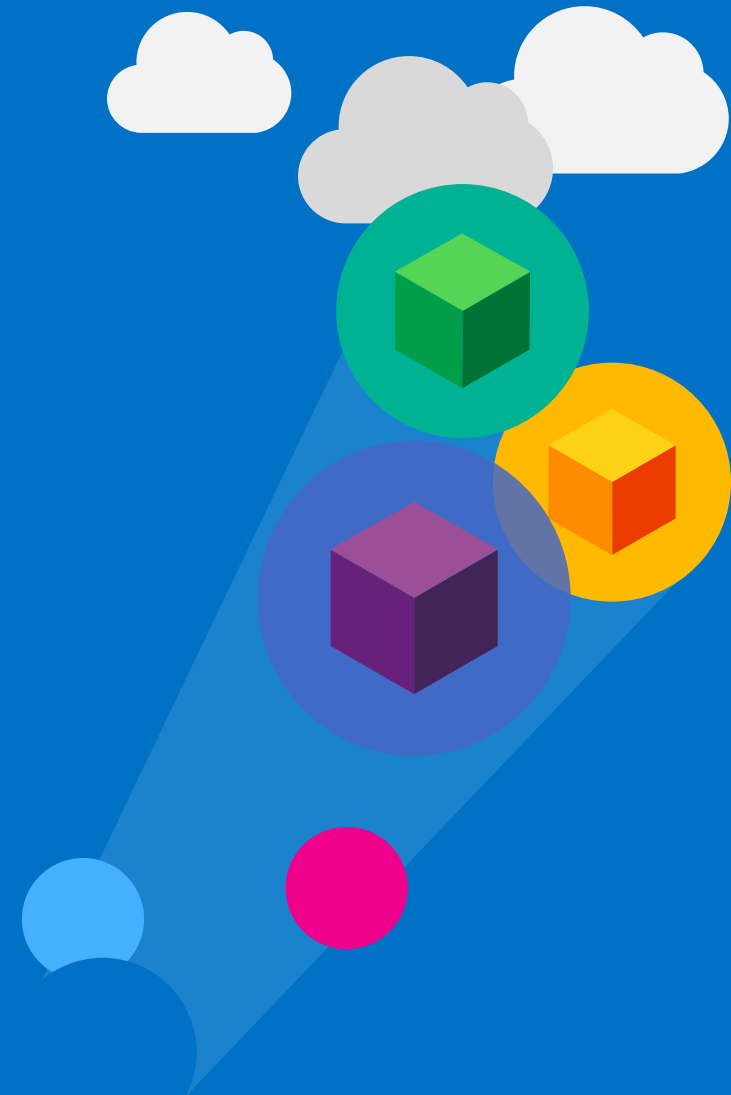
- Paul Simmons, *Systems Engineer, F5*

Capture the Flag Contest — 1:45 4:45pm

-Peter Scheffler, *Solution Architect, F5*

AFCEA USNI West 2018 Reception - 6-8pm

@ Marriott Marquis San Diego Marina Bayside Pavilion



Questions



WE MAKE APPS



FASTER. SMARTER. SAFER.