Guide

F5 Application Services for Federal Workloads on AWS

TABLE OF CONTENTS

Introduction

For several years now, the security of the public cloud has been at the center of much debate. These concerns have undoubtedly played a part in defining the cloud strategy of many businesses. Nevertheless, as time passes and these cloud platforms mature, adoption rates increase—and so, too, does user confidence. Heightened user confidence ultimately leads to more and more organizations accepting and embracing the cloud, including federal agencies.

For federal agencies making the transition to the cloud, ensuring the security of their apps and data is of paramount importance. Surprisingly, the rate of cloud adoption among this vertical hasn't been much slower than its commercial counterparts. In fact, Amazon Web Services (AWS)—the undisputed market leader in the cloud space—boasts that more than 2,000 governmental agencies[1] worldwide trust, and are currently utilizing, its cloud platform to run highly sensitive workloads, reinforcing the fact that confidence in the public cloud is rising.

But as the AWS Shared Responsibility Model states, security of the cloud is one thing while security in the cloud is an entirely different story. While AWS may guarantee the security and upkeep of the underlying infrastructure and networking components (layers 1-3 in the OSI model), the security of everything above this (layers 4-7) is the sole responsibility of the customer. It's also important to note here that although AWS is responsible for all L3 traffic outside of virtual private clouds (VPCs), customers are still responsible for the security of any L3 traffic within their VPCs. All of this means that any federal agencies looking to adopt AWS must implement the necessary security precautions to ensure that all applications and data are protected up to the varying standards which they require, whether that be FedRAMP, ITAR, HIPAA, FIPS, or the like.

This needn't be cause for concern, however, as F5's extensive portfolio of security solutions is built to safeguard mission-critical apps and their data in the AWS commercial cloud, GovCloud (US), and C2S region—relieving federal agencies of this burdensome responsibility. In this overview, we'll review some of the most common F5 security use cases on AWS specific to the federal vertical, how F5 enables the creation of environments that comply with DoD Secure Cloud Computing Architecture (SCCA) requirements, and a summary of deployment and licensing options for F5 solutions on AWS.

USE CASE

01 SSL Visibility and IPS Functionality

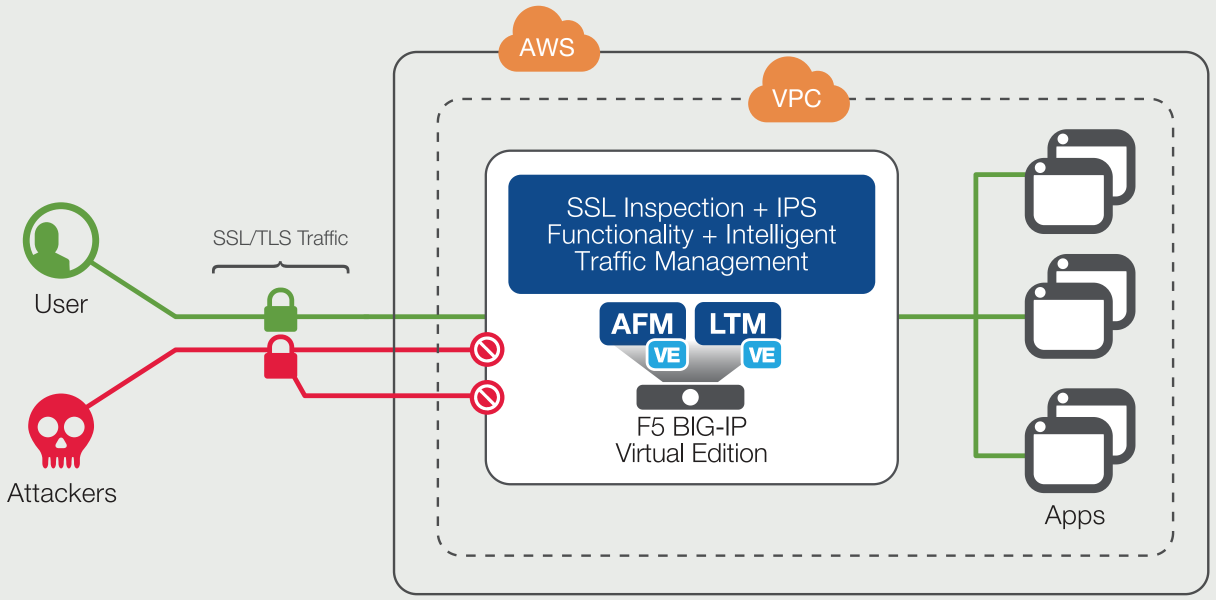
AWS
VPC
SSL/TLS Traffic
User
Attackers
SSL Inspection + IPS Functionality + Intelligent Traffic Management
AFM
VE
LTM
VE
F5 BIG-IP Virtual Edition
Apps

Figure 1: F5 offers SSL visibility and IPS capabilities that help mitigate hidden attacks.

MITIGATE ATTACKS AND ENFORCE PROTOCOL COMPLIANCE

Over the past decade, the number of websites leveraging SSL or TLS to encrypt and secure the transfer of data between clients and websites has increased dramatically, with more than 50 percent of global webpages now employing these security protocols.[2] While SSL/TLS enables organizations to more securely send data between cloud-hosted apps and end-users via the use of encrypted tunnels, there is a fundamental problem with this. These encrypted tunnels do such a great job of protecting the data from external attackers that they can also be exploited to conceal harmful malware such as viruses, trojan, and ransomware from security devices such as IPSs.

For many federal agencies, deploying an intrusion prevention system (IPS) is an essential security component used to protect cloud networks from common vulnerabilities and exposures. However, most devices are not designed to handle the vast quantities of encrypted traffic that traverses data streams nowadays, which results in them often being deployed in passive-only detection mode to cope with the extra workload. This is undesirable as passive-only mode provides reactive protection which ultimately allows attacks to reach their target before blocking and intercepting the attack; versus inline mode which provides proactive protection that prevents attacks from reaching their targets in the first case.

THE SOLUTION

Deploying an F5® BIG-IP™ virtual edition (VE) in your AWS VPC solves both problems thanks to its full-proxy architecture, IPS functionality, and SSL inspection capabilities. As encrypted L4 traffic reaches a VE, it can seamlessly decrypt traffic before inspecting it. Should any of these requests trip a malicious signature within the extensive library of BIG-IP Advanced Firewall Manager™ (AFM), those packets would be quickly blocked and the attack mitigated. This eliminates the need to implement a separate dedicated IPS device behind your VE, simplifying management and architectural complexity while also improving your overall security posture. In addition to providing IPS functionality, BIG-IP AFM delivers the scalability, performance, and control needed to mitigate the most aggressive, voluminous DDoS attacks across a wide variety of protocols before they reach your VPC—keeping your AWS workloads online. F5 BIG-IP VEs have also been verified by NIST as being FIPS 140-2 level 1 certified on AWS, ensuring secure encryption and storage of SSL certificates while meeting various other compliance requirements.

USE CASE

02 Web Application Firewall (WAF)

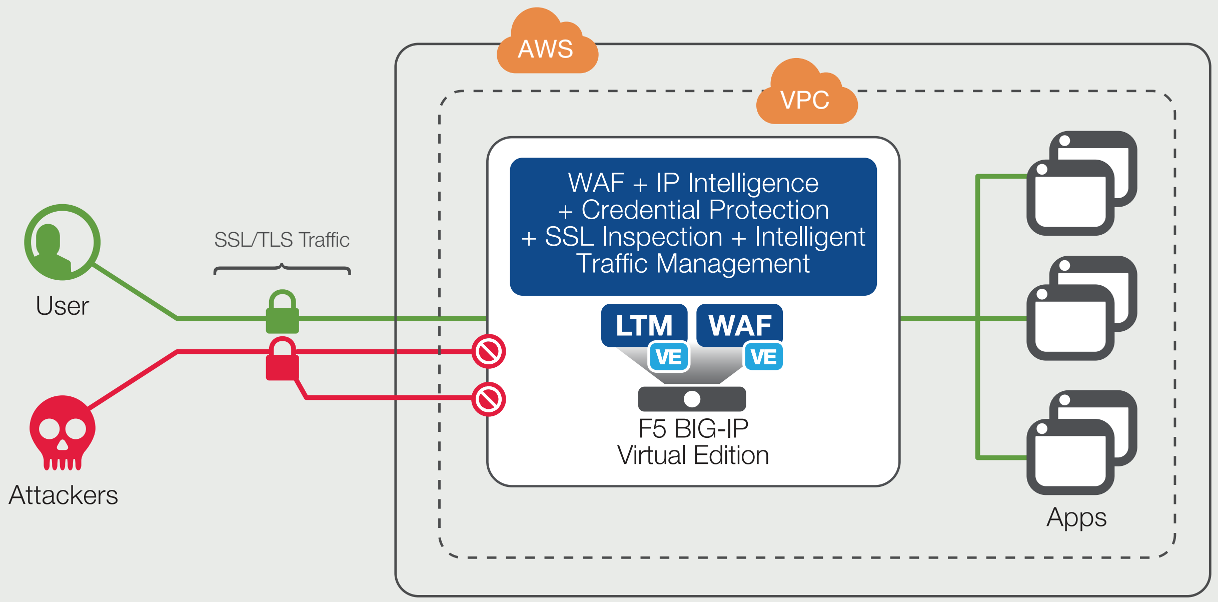

Figure 2: F5 WAF provides comprehensive application layer security.

PROTECT WORKLOADS WITH ROBUST, FEDERAL-GRADE SECURITY

It should come as no surprise to learn that government agencies are among the top five industries most targeted by cybercriminals. In fact, between 2006 and 2015 the number of cybersecurity incidents reported by federal agencies swelled from 5,500 to just over 77,000—an increase of more than 1,300 percent.[3] And in a day and age when almost all significant government cyber breaches are broadcast and amplified by the media, it's even more vital to impose the most stringent security precautions available to protect highly sensitive information, as well as the reputations of the agencies entrusted with that information.

THE SOLUTION

F5's advanced Web Application Firewall (WAF) provides robust protection at the application layer (L7), identifying and securing against a plethora of threats aimed at disrupting services, stealing data and credentials, or taking advantage of compromised accounts. These threats include, but are not limited to:

- Stealthy L7 denial-of-service (DoS) attacks that may go undetected by traditional signature- and reputation-based solutions like Next-Gen Firewalls and Cloud Native DoS protection tools.
- OWASP Top 10 threats as well as thousands of other attack vectors.
- Bots that target browser-based and mobile clients.
- Common application vulnerabilities that can be exploited by attackers.

Shielding highly sensitive cloud workloads with F5 WAF is also a quick and easy way to ensure that all applications meet the necessary regulatory compliance mandates specific to the government industry, including FedRAMP, HIPAA, ITAR, and PCI DSS. And to ease ongoing policy maintenance, F5 WAF also integrates with various commercial vulnerability scanners. Furthermore, F5 solutions include pre-built security policies that mitigate thousands of out-of-the-box signatures as well as a provide a streamlined approach to policy management. The result? You don't have to be a security professional to implement professional security with F5 on AWS.

If you already operate F5 WAF in other environments—whether in additional clouds or on-premises—you can quickly and easily replicate security policies across environments to ensure consistent security across your architecture, preventing loopholes which may arise through the use of multiple security products.

USE CASE

03 Identity and Access Management

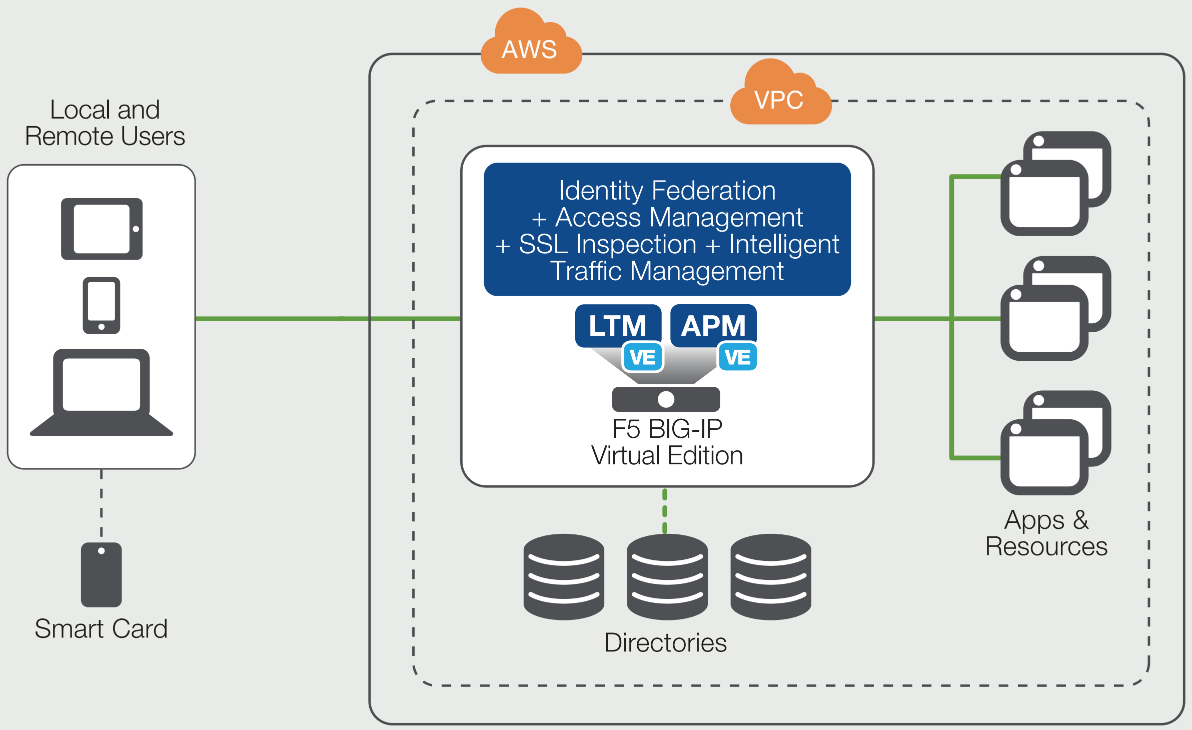
AWS
VPC
Local and Remote Users
Identity Federation + Access Management + SSL Inspection + Intelligent Traffic Management
LTM
APM
VE
VE
F5 BIG-IP Virtual Edition
Apps & Resources
Smart Card
Directories

Figure 3: F5 BIG-IP helps prevent fraudulent application access.

PREVENT FRAUDULENT ACCESS

Government agencies should have real-time visibility into who has access to what resources, when, and for how long—and they should be in control of these insights at all times. And while it is important that users are able to securely access resources appropriate to them, granting surplus access is likely to expose agencies to unnecessary risk. Thus, the ability to segregate and define users' access based on their roles and responsibilities is critically important – especially when dealing with varying degrees of classified information.

THE SOLUTION

F5 BIG-IP Access Policy Manager™ (APM) provides a centralized identity and access control point, ensuring that user access to cloud-based and on-premises applications is both secure and simple—thereby preventing fraudulent access to sensitive data. By leveraging SAML 2.0, BIG-IP APM supports connections initiated by both SAML IdPs and service providers, which in turn allows identity federation and single sign-on (SSO) to any cloud-based application, from any device. In addition to supporting standard authentication methods such as SAML and OAuth for federating user identity, BIG-IP APM supports SSO and Kerberos ticketing across multiple domains—enabling other authentication techniques including the use of Common Access Cards (CACs) and Personal Identity Verification (PIV) cards. Utilizing these cards, users can be automatically signed on to back-end applications that are a part of a Kerberos realm, delivering a seamless authentication flow after a user has been authenticated via a user-authentication mechanism.

BIG-IP APM also employs user authentication through pre-defined access control lists (ACLs). These ACLs describe which individuals or groups have access to specific applications and networks—restricting user access to only the necessary applications, permitted devices, and permitted locations, thus preventing accidental over-exposure. These ACLs and various other BIG-IP APM configurations can be quickly and easily implemented, updated, and managed with Visual Policy Editor, a feature of BIG-IP APM.

USE CASE

04 DNSSEC

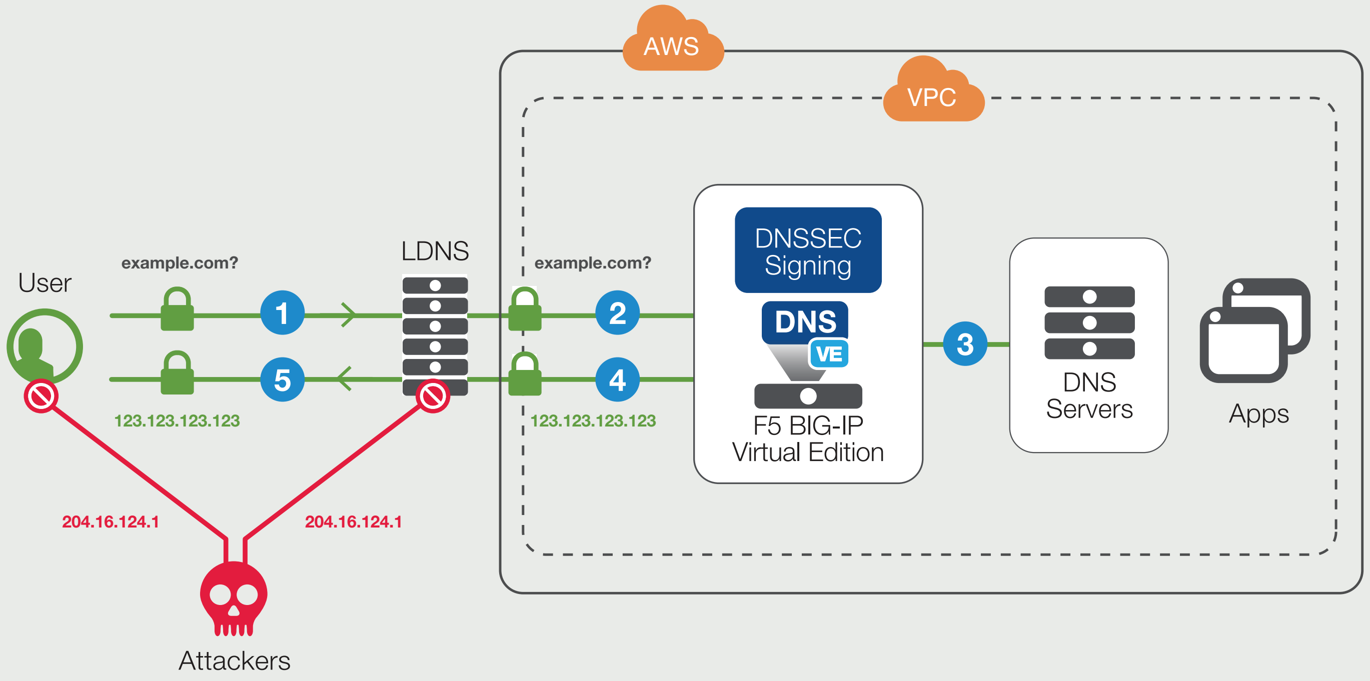

Figure 4: F5 BIG-IP ensures secure DNS resolution.

PREVENT DNS HIJACKING

By today's standards, DNS hijacking is a relatively straightforward cyberattack. It involves a simple rewrite of an internet device's configuration such that instead of routing DNS queries to authentic DNS servers, it re-directs them to malicious DNS servers. This can be highly problematic as legitimate web users can be directed to illegitimate websites that may have an identical look and feel. Unaware that they're attempting to sign in to a fake web page, these users may unknowingly provide compromising credentials directly to cyber criminals. In the federal world, these forms of phishing and pharming are of great concern—especially among agencies that have not implemented multi-factor authentication—as it allows attackers to quickly and easily obtain user and password combinations, and subsequently gain access to sensitive information.

THE SOLUTION

To combat this, BIG-IP provides a complete, real-time DNSSEC solution that allows digital signing and encryption of DNS query responses. This enables the DNS resolver to determine and verify the authenticity of any responses it receives, and to ensure that the user is directed to the desired website, and not a malicious replica. Furthermore, in most networks DNS resolvers offload DNSSEC record requests and crypto calculations due to the high CPU loads this would otherwise place on DNS resolver servers. With BIG-IP DNS, however, administrators can easily offload, validate, and resolve DNSSEC on the client side, resulting in enhanced DNS performance and a dramatic improvement in the end users' experience.

ENABLING THE CREATION OF DISA SECURE CLOUD COMPUTING ARCHITECTURES

In addition to the use cases previously discussed, F5 also empowers DoD customers to create secure cloud computing architectures in AWS that meet the strict security requirements stipulated by the Defense Information Systems Agency (DISA). SCCA (Secure Cloud Computing Architecture) describes the functional requirements for securing the Defense Information Systems Network (DISN) and commercial cloud provider connection points, as well as how mission owners secure cloud applications at the connection boundary. The four major components of the SCCA that are required to gain compliance are:

- Boundary Cloud Access Point (BCAP)
- Virtual Datacenter Security Stack (VDSS)
- Virtual Datacenter Services (VDMS)
- Trusted Cloud Credential Manager (TCCM)

F5 provides the solutions required to meet or optimize most, if not all, of the sub-requirements across each of these four categories. These solutions deliver key capabilities such as the separation of user and management traffic, and reverse proxy capabilities to handle access requests from client systems. Implementing the necessary F5 solutions in accordance with these SCCA requirements ensures the high availability of cloud resources, unparalleled visibility into all traffic, as well as robust security of the cloud network, applications, and data.

DEPLOYMENT AND LICENSING ON AWS

As the most widely integrated public cloud ADC vendor on the market, F5 provides unparalleled flexibility when it comes to deploying and licensing F5 services on AWS. Not only is BIG-IP virtual edition integrated with the AWS commercial marketplace for use in the AWS commercial cloud, but it is also directly available from both the AWS GovCloud (US) Marketplace, and AWS Marketplace for the U.S. Intelligence Community (IC)—allowing for fast deployment of VEs into the AWS GovCloud (US) and Commercial Cloud Services (C2S) regions respectively. When deploying in either the commercial or GovCloud (US) regions of AWS, F5 has also created an extensive portfolio of AWS CloudFormation templates to simplify and automate the deployment of various BIG-IP topologies. These templates can be found within the F5 CloudFormation Template repository on GitHub.

F5 offers various licensing methods from each of the supported marketplaces to deliver a range of both CapEx- and OpEx-based purchasing models—from cloud-native Pay-As-You-Go (PAYG) to more traditional Bring-Your-Own-License (BYOL) offerings which include perpetual, subscription, and enterprise licensing agreement (ELA) options.

Conclusion

F5 SOLUTIONS PROTECTS SENSITIVE FEDERAL APPLICATIONS AND DATA IN AWS

Federal workloads are among those most targeted by cybercriminals annually. While ensuring the security of these resources when deployed in the public cloud is the sole responsibility of application owners themselves, F5 provides a diverse portfolio of advanced security solutions to meet various security and compliance requirements, including but not limited to:

- SSL traffic visibility, inspection, and blocking: BIG-IP Local Traffic Manager™ and BIG-IP Advanced Firewall Manager
- Advanced application layer protection – BIG-IP Application Security Manager™ or F5 Advanced WAF
- Secure access and identity management – BIG-IP Access Policy Manager
- DNS hijacking prevention with DNSSEC – BIG-IP DNS

These solutions are all available via F5 BIG-IP virtual edition. BIG-IP VE provides consistent features and functionality with other BIG-IP devices that may already be deployed on-premises or in other environments, allowing for fast, simple policy and service replication across multi-cloud environments.

REFERENCES

1 https://n2ws.com/blog/aws-cloud/5-facts-amazon-cloud-essentials

2 https://www.wired.com/2017/01/half-web-now-encrypted-makes-everyone-safer/

3 http://www.infoguardsecurity.com/5-industries-top-hit-list-cyber-criminals-2017/

WE MAKE APPS

GO

FASTER. SMARTER. SAFER.