F5 Security: Protecting Applications On-premises and in the Cloud

Application Access – Identity Federation

What is it?

Identity Federation (IdF): Allows user access to multiple applications across different organizations and domains without requiring multiple passwords.

Single Sign On (SSO): When a user can access multiple or different applications within a single organization or domain while only authenticating once;

Adaptive Authentication: Designed to identify potential authentication risks, applies authentication mechanisms of varying severity based on a number of factors, including the status of specific, variable user and client attributes, indicative of an increased risk of compromise.

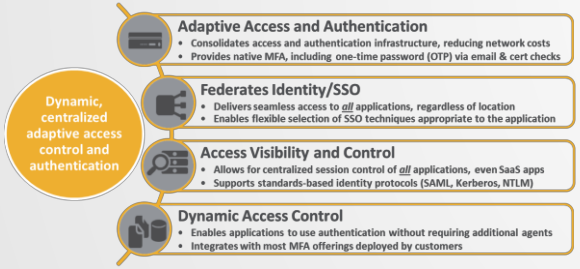
Why Customers Buy?

- **Protect Brand and Revenue:** With compromised or weak credentials leading to major security breaches, organizations are eager to halt potential breaches before they happen, and reduce the cost and damage of these attacks to their brand and business. (No one wants to be the next Anthem or U.S. Office of Personnel Management.)
- **Silos of Identity:** As mobility and cloud drive business today, they also create identity silos, many time requiring an organization to make their user credential databases available outside of their control, such as with cloud or SaaS providers, which is an uncomfortable and dangerous position.
- **Compliance Purposes:** Organizations that handle or transact sensitive data, often in the financial, health and government verticals, are required to implement federal policies intended to help mitigate cyber attacks (PCI, Sarbanes-Oxley, HIPAA) which mandate strong user passwords.

F5 Offerings

F5 BIG-IP Access Policy Manager (APM)

Provides dynamic, centralized and adaptive access control and identify federation for all applications



Questions to Ask Customers

- How is your organization handling multiple Identity Access Management applications?
- As SaaS adoption increases, do you have a single sign on strategy for on-premises and cloud based access?
- Are you currently sharing credentials with 3rd parties or placing it in the cloud?
  - Does that create some angst or concerns within the IT team from a security prospective?
- Are there multiple access methods for SaaS based applications?
- Do your users have different credentials for on-premises and cloud based applications?
- Are you aware that F5 has identity federation solution that simplifies and addresses access to both on-premises and cloud/SaaS applications?
- How are key internal and external customers accessing key applications?

SSL Everywhere

What is it?

SSL Offload – *inbound*: relieves web servers of the processing overhead of encrypting and/or decrypting traffic sent via SSL

SSL Intercept - *outbound*: Decrypts outbound SSL traffic to enable inspection by third-party security devices (e.g. NGFW, IPS, or DLP) for hidden threats

Why Customers Buy?

- **Compliance**: 64% say compliance is most important driver for SSL
- **Data Breaches:** Un-inspected SSL traffic poses a risk to hidden threats like malware. Gartner reports that by 2017, over 50% of all network attacks will use SSL.
- **Privacy:** 57% of Europeans are worried their data is not safe
- **Performance:** NGFW experience 80% performance loss with SSL enabled. SSL stresses the overall efficiency, security and performance of the infrastructure.
- **Operational Efficiency:** High profile SSL vulnerabilities require updates. Enforce consistent SSL policy without compromising on performance, key protection, or visibility

F5 Offerings

SSL Intercept:

Gain SSL visibility into user traffic with third-party devices (e.g. NGFW, IPS, DLP) to stop encrypted attacks

SSL EVERYWHERE

- Inspect SSL traffic for hidden threats like malware with third-party security for defense-in-depth protection
- Hardware SSL acceleration with leading scale and performance
- Firewall segmentation and key protection are an integral part of the design
- Bypass URL categories (e.g. banking) to protect user privacy
- iApp templates simply configuration for SSL Air Gap deployments

Questions to Ask Customers

- How much of your internal traffic is SSL vs unencrypted?
- Is your application architecture team requiring encrypted traffic moving forward? Are there external applications requirements?
- Are you familiar with AirGap and the business reasons behind implementing that architecture?
- Are your SSL cyphers up to date with leading standards?
- Are you aware that F5 has a SSL solution that can help address control over both in-bound and outbound SSL traffic?
- Have you run an SSL Labs test against your websites?

F5 Security: Protecting Applications On-premises and in the Cloud

Hybrid WAF

What is it?

Web Application Firewall (WAF): A firewall specifically designed to provide security for layer 7 application data.

WAF Managed Service: Often a subscription based, managed service offering , where WAF services are supported and managed by an external vendor.

Hybrid Deployment: A network architecture that utilizes on-prem. and cloud components.

Why Customers Buy?

- **Layer 7 App Security**: Provide layer 7 application security that traditional network firewalls do not provide
- **Constantly Changing Threats:** New attacks focused on taking down a companies enterprise and customer facing apps. (**2.3M Bots** actively attacking (Symantec Internet Security Report 2014)
- **Protect Brand:** With major security breaches making monthly headline news, customers are eager to mitigate the cost of such attacks to their brand and business.
- **Compliance/Policy:** Customers need layer 7 app security to meet compliance and different industry standards (FSI= PCI compliance)

F5 Offerings

Customer Managed Hybrid WAF: F5 BIG-IP Application Security Manager™ (ASM) is an on-premises, enterprise web application firewall (WAF)

Comprehensive security against sophisticated layer 7 attacks and enable compliance with key regulatory mandates.

Deploy as an appliance, in virtual or cloud environments, and support multi-tenant services while incorporating external intelligence that secures against known IP threats

Industries best BOT detection measures and secures against the OWASP top 10

Internally Managed Hybrid WAF

F5 Managed Cloud Based WAF: F5 Silverline™ Web Application Firewall is a fully managed enterprise-grade service built on BIG-IP ASM

Protect web applications and data from layer 7 attacks with F5 cloud-based WAF

Outsource app security expertise and Leverage 24x7x365 F5 SOC support from highly specialized security experts

Deploy across hybrid environments and work with existing BIG-IP implementations.

Enable compliance with industry security standards, such as PCI DSS,

Externally Managed F5 Silverline

Questions to Ask Customers

- Does your current architecture give you visibility into SSL application level attacks beyond your IDS/IPS architecture?
- What type of application protection is necessary from a regulatory environment? Are PCI and HIPAA regulations critical to your business?
- Are you able to quickly show PCI-DSS compliance if asked?
- What's your strategy around SSL in your organization? Is all of the traffic required to be encrypted? Does your organization have requirements around decryption and re-encryption of SSL traffic?
- What is the business impact of having key applications unavailable for internal/external use?
- Are you aware that F5 has a managed WAF offering?

Hybrid DDoS Protection

What is it?

Distributed Denial of Service (DDoS): DDoS is a type of cyber attack that leverages multiple compromised systems, often infected with a Trojan, and used to target a single system causing a Denial of Service (DoS) attack.

DDoS Protection Solutions: Technologies designed to detect, prevent and contain DDoS attacks. Most common include: cloud scrubbing, ISP services, end-point security, firewalls, and network/traffic intelligence solutions. Demand for hybrid solutions that leverage both physical devices and cloud-based services is increasing.

Why Customers Buy?

- **Protect Brand:** With major outages making monthly headline news, customers are eager to reduce the cost and damage of these attacks to their brand and business.
- **Financial Impact:** According to a 2015 Ponemon report, the average total cost per year to deal with DoS is approximately $1.5 million. This includes lost productivity, disruption to operations, damage to infrastructure, and loss of revenue.
- **Compliance Purposes:** Organizations that handle or transact sensitive data, often in the financial, health and government verticals, are required to implement federal policies intended to help mitigate cyber attacks (PCI, Sarbanes-Oxley, HIPAA)
- **Future Proofing:** Customers are looking to strengthen their IT security now rather than pay the much higher costs associated with cleaning up and recovering from a successful DDoS attack.

F5 Offerings

Cloud-based DDoS Protection:

F5 Silverline™ DDoS Protection is a fully managed service that augments resources for DDoS mitigation

F5 Silverline DDoS Protection

Cloud-based, Enterprise Grade, L3-L7 DDoS Protection

- **Managed Service:** the industry's most responsive 24/7 SOC
- **Expert Resources:** access to the world's foremost DDoS experts
- **Transparent Operations:** immediate visibility into all SOC actions and threats
- **Extensible Solution:** Integrates with F5 on-premises AFM & ASM
- **Protects Datacenter:** defends against the largest DDoS attacks without regard for ISP, Origin
- **Drive efficiencies with a hybrid DDoS solution:** F5 offers comprehensive DDoS protection on-premises and as a cloud-based service.

Questions to Ask Customers

- Has your company or companies in your market segment suffered a DDoS attack? Are you ready if your company is attacked via DDoS?
- Have you received a ransom letter threatening a DDoS attack for money and/or bitcoin?
  - If you're covered with DDoS with your ISP, is it through multiple ISP's or through BGP manipulation?
  - Does your DDoS service provide the ability to view on-premises and cloud based attacks?
- How are DDoS attacks currently being mitigated? What's the size of your Internet connection?
- Do regulations in your industry or organization require a DDoS mitigation strategy?
- Are you aware F5 has an emergency hotline number if you're under a DDoS attack?
- What security framework has your organization based it's architecture on? (NIST, ISO 27000 - likely only a question that will apply to larger organizations)