White Paper

Securing Banks In Changing Times

The financial services industry is facing significant pressure from customers, competitors, and governments to secure and improve all types of networked applications while meeting customer demand for increased channel access and complying with new regulations. F5 ADCs can speed compliance and time to market while increasing security on public-facing websites.

by Don MacVittie
Technical Marketing Manager

Contents

Introduction

The pressures upon organizations in the financial services industry (FSI) today are perhaps the highest they've ever been. Customer loyalty is at an all-time low even as customers demand new methods of access. Regulatory burdens are growing following the global financial crisis (GFC) of 2008-2009. Application downtime and the risk of customer information leaks threaten brands. Each of these pressures has a significant impact on IT. Today, more than ever, FSI organizations need a solution that can speed implementation of new systems and improve the security of applications while maintaining or improving uptime and customer satisfaction.

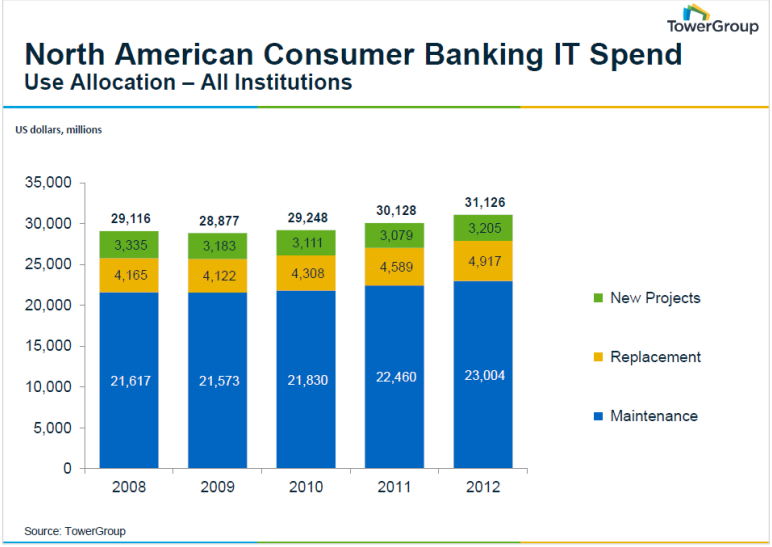

Figure 1: Banks are expending resources on core systems and security.

> "To enable the best deployments for fraud detection, data protection, and adoption of new platforms and standards (e.g. mobile and DNSSEC, respectively), many financial institutions are currently placing a heavy emphasis on modernizing their core systems. This updated infrastructure and modern analytics will help them be more nimble in effectively addressing emerging threats."
>
> —Jason Malo, Research Director, CEB TowerGroup, 2012

Changing regulations place overhead on financial services firms, and yet since the GFC those regulations are changing and growing faster than they have in a long time—possibly faster than ever. And with time, regulations stack up, meaning there is more to maintain while implementing new regulations and systems. IT management must implement current regulations in a timely manner, maintain compliance with existing regulations without significant overhead, and offer secure and stable systems that will maintain or improve customer satisfaction. At the same time, they must make available and secure the host of new technologies—from mobile access to remote deposit capture—that customers are demanding be available to them for banking use. These new technologies can pose a large burden for the average FSI organization's IT department, requiring IT to secure systems that

are designed to give customers easy access to their money, stocks, or annuities. Yet security and easy access can seem mutually exclusive.

The risks from downtime and hacker attacks are generally far greater in FSI than in other vertical industries. While most organizations strive for five nines of uptime, failure to meet those numbers in FSI can have lasting impact upon the organization's reputation, company performance metrics, and even the careers of the individuals in IT involved in security and availability.

Yet the existing solutions to security often do not adequately protect financial services from the wide array of contemporary attacks, and while any penetration and information theft is bad, in financial services it strikes right at the heart of the business, risking damage to company—and IT staff—reputations.

The reality is that these issues and many more must be managed in a comprehensive, yet flexible manner. Compliance is mandatory, and customer satisfaction and broader access to services are expected. What IT departments need is a holistic solution that helps with these specific issues while making the overall architecture more stable, secure, and adaptable. F5 Networks can provide that holistic solution.

Common Banking Challenges

Operational Risk and Compliance

Operational risk is a fact of life for all enterprises, but the risks for banks and other FSI organizations are significantly higher than they are for the average organization. The information that banks contain is the exact information attackers and cyber criminals want. While fraudsters want the very Information that banks wish to keep away from them, governments are watching banks more closely since the GFC. Protecting the good name of the bank is an operational risk as well, with phishing scams targeting bank customers to get information by masquerading as the bank itself, so a single data leak can cost the organization years of reputation building.

The goal is to protect customer data and prevent fraud while protecting the organization's reputation and complying with all required regulations.

While policy and procedure are mandatory to institute and verify compliance, effective systems are also required. A platform certified for a variety of the compliance standards that impact FSI organizations can help streamline compliance implementation and maintenance.

PCI DSS compliance

Payment Card Industry Data Security Standard (PCI DSS) compliance focuses on protecting web applications from attacks designed to steal customer account information or any personally identifiable information. The solution, a web application firewall (WAF), should incorporate a comprehensive set of rules that block known vulnerabilities and common attack vectors. Add to this the ability to stop credit card information from leaking out through web applications and you have a powerful compliance tool that also protects organizational reputations.

FIPS compliance

The FIPS 140-2 mandate considers the security of encryption passing over a network and of the encrypting device. A network-based FIPS 140-2 Level 2 compliant solution should handle the encryption and offload it from the CPUs of data center servers onto high-performance, custom hardware such as a hardware security module (HSM). For instance, a physical server hosting 10 virtual servers should not be trying to serve the encryption needs for all of those virtual servers while also switching between them. Offloading the encryption to a specialized encryption product that also functions as an HSM can increase virtual machine (VM) density and improve application performance, all while making customer data more secure.

Phishing and DNS poisoning prevention

Phishing is a common online banking scam in which the attacker sets up a false banking site designed to obtain the authentic bank customers' private information. This form of attack targets and may corrupt Domain Name System (DNS) servers in what's known as DNS poisoning, which enables malicious use of domain addresses. When a customer requests a web address through a browser, a poisoned DNS cache sends customers to a invalid site without the customers realizing they've been misdirected to a site created for phishing. The solution involves providing encryption keys that validate authentic DNS server responses in real-time[1]. In essence, these DNS Security Extensions (DNSSEC) add a digital signature to ensure the authenticity of certain types of DNS transactions, helping prevent rogue servers from sending invalid DNS responses and thus protecting the organization's domain name and related web properties.

F5 Provides Security for Financial Web Services

"F5 solutions provide good assurance that our web services infrastructure is adequately secured."

—Security Manager, Small Business Banking Company

Source: TechValidate
TVID: CF6-B6B-D90

1 DNSSEC: The Antidote to DNS Cache Poisoning and Other DNS Attacks

Security

Because security in a financial services environment is multifaceted and often overlaps with compliance, FSI organizations need tools to seamlessly manage both. Using hardware to offload encryption reduces the number of servers required. Encryption on commodity servers is expensive in terms of CPU utilization and slow in terms of transactions per second. Those drawbacks are exaggerated in a virtualized environment where the CPU is serving not one OS, but many, each with its own encryption requests.

DoS attack defense

Banking web sites have been brought down by distributed denial-of-service (DDoS) attacks, in which attackers from a variety of locations start connections and then leave them, and diverse distributed denial of Service (3DoS) attacks, where geographically dispersed attackers use several different methods of attack simultaneously, making the attack harder to detect. These strategies make DDoS protection mandatory today. Protecting against DoS, DDoS, and 3DoS attacks not only protects the company's reputation, it also ensures that a DDoS attack cannot become the gateway to more attacks directed toward stealing data.

Figure 2: One F5 customer's 3DoS experience (click for video)

Tunneled encryption

When sending data over the public Internet between two data centers for active/active systems, backup, or replication, encryption is good and tunneled encryption is better. The ability to tell two devices that they talk to each other privately over the

public Internet provides one more layer of obfuscation for attackers to unravel. Since a device is required on both ends of a secure tunnel, tunnel sessions also provide good opportunities to perform symmetric deduplication, reducing the amount of bandwidth taken up by back-office functions by shrinking the amount of data sent between the two locations.

High-speed logging

Finally, with the number of attacks on the rise and the targeting and sophistication of these attacks improving with technology and hacker experience, high-speed logging and the ability to utilize industry-specific toolsets to analyze log data and detect malfeasance is necessary. Preferably, logging and log analysis should enable the automatic blocking of connections that are determined to be malicious. Logging that can handle a high enough volume of traffic to support the largest websites in the world without data loss while under a DDoS attack can protect systems while the attack is underway and improve security posture after the fact by enabling log aggregation and analysis tools to pore over the resulting data and help predict future attack vectors.

Mobile Devices and Access Control

Today, customers are demanding access from anywhere, via any device. The banking focus is on customer-centric systems, with single sign on capability, application federation, customer identification and personalization, and context-aware user management all playing an important role in providing an enjoyable customer experience. Application development teams are rushing to get to the market mobile applications that meet these customer demands. Creating a mobile-specific site, supporting varying form factors and input methods, securing access from a variety of mobile devices, and even supporting multi-media to and from devices have become mandatory for the business. IT departments must find a way to implement the necessary systems with the least possible overhead.

When an attacker attempts to penetrate a public-facing system, the attacker has many vectors of attack from the operating system to a web application, and every new access device adds to the list. Security is best served by limiting the vectors of attack down to the smallest list possible, and making those more manageable.

To achieve a secure architecture, a good first step is implementing a system that can check if there is anti-virus control installed on a connecting device and that the device meets corporate standards for customer access or a minimum security

F5 Optimizes Traffic Management and Security for Financial Services

"F5 BIG-IP has the flexibility to manage transactional traffic especially in contingencies, and provides us a relatively easy way to comply with PCI DSS for web application services."

—IT Manager, Medium Enterprise Financial Services Company

Source: TechValidate
TVID: 4B6-33F-D38

posture, all before a connection completes with the server. This protects customer data, data center servers, and IT staff's sanity by removing the web application and operating system from the attack vectors available to an attacker without credentials. The result is a significantly improved security posture.

Second, implement a system that can redirect users based on items such as the user agent string, time of day, and geographic location. This type of system sends mobile devices to a separate web server for a mobile interface while sending desktop connections to full-function applications that are expecting users with full screens and high-speed access. This automated redirection saves on manual redirects and other coding methods to direct users, and it can be updated centrally when necessary.

When access control is implemented in the network instead of on application servers, it allows IT staff to set rules for how incoming connections are directed. Utilizing centralized authentication, authorization, and accounting (AAA) servers, an access control point can look at device type, time of day, and user attributes such as rights and group membership to determine how to handle an incoming connection.

The performance of mobile devices is also a factor to consider. Granting access to qualified mobile devices in the hands of users with valid credentials is not useful if the performance of the site when delivered through a phone is sub-par. This requires a solution that can optimize traffic based upon the type of client. While such a system offers benefits to all web-based applications through methods like caching and expiration controls on information being sent, the level of optimization can be enhanced to improve the user experience for devices on a wireless carrier network. For online banking, this optimization can make or break the customer experience in the eyes of highly mobile customers.

F5 Minimizes Web Application Downtime

"With F5 we were able to protect and maintain our web applications with minimum downtime. Their products are essential to our business, focusing on high availability, load balancing and security, with a high level of quality."

—IT Manager, Medium Enterprise Financial Services Company

Source: TechValidate
TVID: 5ED-C2C-1C9

The ADC as a Solution Platform

Application Delivery Controllers (ADCs) such as the F5® BIG-IP® product family provide a platform that enables granular control of the availability, performance, and security of an organization's application infrastructure. By residing at the strategic point of control between applications and the network, an ADC can use a layered approach to improving the areas of application delivery and networking that an organization needs the most. If performance of the server is an issue, load balancing and encryption offloading can be used. If high availability is an issue, the ADC can manage load balancing and clustering. If security is an issue, an ADC can deliver edge

security, application firewalls, and payload inspection. The ADC functions that can be enabled at this strategic point of control are limited only by the vendor's platform.

Some benefits that an F5 BIG-IP ADC can offer an FSI IT organization include:

- Institute load balancing to improve high availability and performance by spreading the work over multiple servers.
- Enable encryption offloading to specialty, network-hosted FIPS 140-2 compliant hardware, which improves performance of individual servers that require encryption services.
- Improve security by centralizing access control for all users, regardless of device or location, and applying policies to limit access based on the characteristics of the connection and user.
- Secure connections between data centers with secure remote tunneling, and improve throughput with advanced deduplication algorithms.
- Achieve comprehensive protection from the latest web security threats, including DDoS and SQL injection attacks, JSON payload vulnerabilities, web scraping, and more, to shield the corporate brand and customers' sensitive data.
- Speed content delivery to end users with optimizations that make web applications faster no matter what platform the client is running on.
- Implement DDoS protection and correct geographical routing of traffic.
- Deploy an ICSA-certified network firewall that can absorb much more DDoS traffic than a typical conventional firewall.
- Implement high-speed logging with a programmable interface to allow existing FSI attack-detection systems to shut down connections or block user addresses.
- Access a peer-to-peer and staff-to-peer support site with a thriving community at the F5 DevCentral™ community. This online community offers a broad selection of useful tools to benefit all parts of an IT infrastructure, as well as ready assistance to get new users acclimated to the more advanced tools and capabilities of BIG-IP features including F5 iRules®, F5 iControl®, and F5 iApps™.

Together, these benefits and capabilities help make an organization's data centers faster, more secure, and more available while resolving some of the problems that are unique to the financial services industry.

F5 Provides Web Security at Financial Services Company

"Using F5 BIG-IP, we consolidated SSL offload certificates and protected web servers at the application layer."

—IT Manager, Medium Enterprise Financial Services Company

Source: TechValidate
TVID: 874-E7D-038

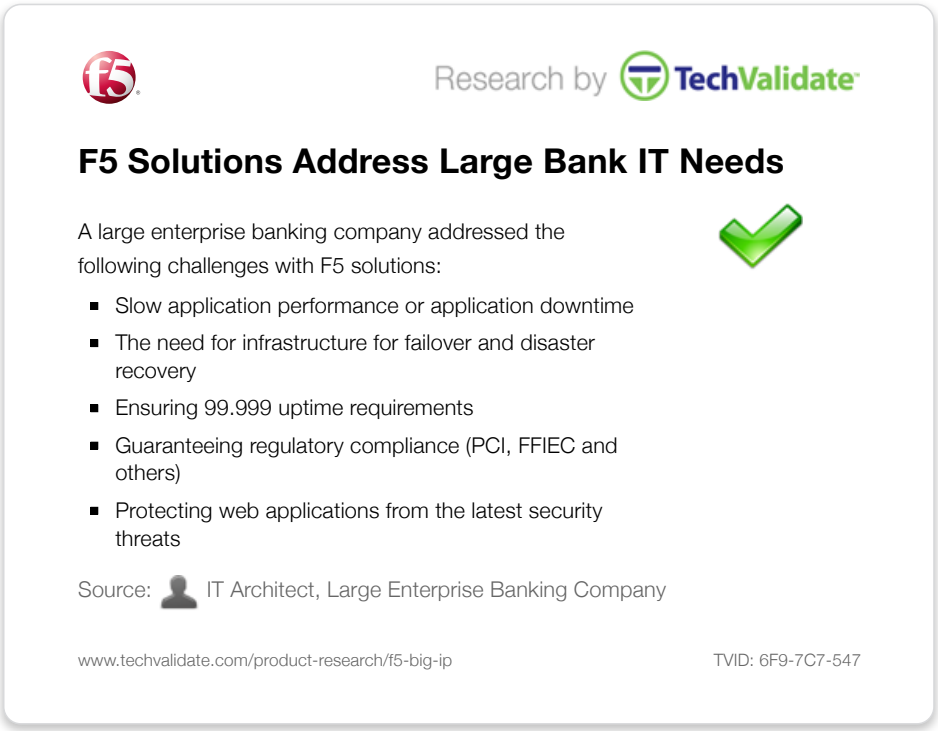

Figure 3: F5 solutions help create secure, fast, and available FSI IT architectures.

Conclusion

Financial Services IT departments are up against a tough collection of challenges that all insist on urgent attention. While customers are demanding secure access from a greater range of devices and expecting high availability, the government is regulating every type of interaction, and attackers are constantly finding new ways to disrupt business or steal customers' data. The BIG-IP product family helps with a cross-section of IT infrastructure issues, including the most difficult issues facing financial services organizations.

Whether an FSI organization's current priorities include remote access for employees, controlled access for customers, web application protection, DDoS protection, availability, compliance, or a combination of related concerns, the BIG-IP product family can help solve the largest problems in financial services while offering assistance to a wide variety of other issues, all from a single platform.

Resources

Case Study: Central American Bank Improves Network Availability and Resilience with F5 Solutions

Application Delivery Hardware: A Critical Component

Data Center Firewall Solutions

Web Application Security Solutions

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com