Bank Uses F5 Firewall Solution to Protect Multiplatform Applications, Meet Regulations

Banco Supervielle was using Cisco ACE XML Gateway as its web application firewall, but the solution had reached the end of its service life. By replacing it with an F5 solution, the bank gained richer functionality, stronger protection for a wider range of critical multiplatform applications, labor savings, regulatory compliance, and better support.

Business Challenges

Since its founding in 1887, Banco Supervielle has grown into a nationwide private bank that serves nearly 1.5 million customers in Argentina. To preserve its reputation, the bank’s security department must maintain highly reliable and secure IT systems.

Recently, the company needed to upgrade the Cisco ACE XML Gateway that functioned as its web application firewall (WAF). The solution was reaching end of life and did not protect key applications, meet the bank’s requirements for a high availability (HA) environment, or provide accurate security monitoring. Finally, within the bank’s IT infrastructure, the Cisco solution did not permit disabling of a key security protocol—SSLv3—without service interruption. (SSLv3 had security vulnerabilities.)

“Not all of our key applications were protected by the WAF," says Marcelo Lorenzo, Senior Information Security Analyst at Banco Supervielle. “We weren’t able to create a sufficiently secure separate quality assurance [QA] environment to change and test all applications before moving them into production.” Given the magnitude of these issues, the Central Bank of Argentina informed Banco Supervielle that the company was out of compliance.

Any new solution that Banco Supervielle might choose would not only have to resolve these issues, but also seamlessly integrate with existing IT systems and support multiple internal and third-party applications.

“With our F5 solution, every time we deploy or upgrade an application, we can be confident that it belongs in production and is well protected. That is a critical benefit for us.”

—Marcelo Lorenzo, Senior Information Security Analyst

Solution

To address these challenges, Banco Supervielle engaged an F5 partner that deployed F5® BIG-IP® Application Security Manager™ (ASM).
“We evaluated third-party products but did not request bids,” says Lorenzo. “We quickly decided that F5 made the most sense.”

He explains that the networking side of IT had already decided to deploy BIG-IP® Local Traffic Manager™ (LTM) for its superior secure application delivery and load balancing capabilities. He further notes that the bank wanted a standalone security management solution and a standalone traffic management solution—separate tools to avoid sharing files between the network and other systems for security reasons.

Daniel Debarbieri, Senior Infrastructure Security Analyst, emphasizes the point: “We liked the option to license and deploy a WAF-only box from one company and completely isolate it from the networking side of IT.” He continues, “It was logical to choose F5 for our WAF because, whether it’s separate or not, we can support multiple solutions with the same technology and the same expert people.”

Says Lorenzo, “The other major reason for selecting F5 was its partner’s expertise. We observed this during implementation and now support. Whenever we need support, F5 and its partner are always responsive.” He notes that this expertise was especially helpful as applications were tested with BIG-IP ASM in parallel across four sites. “Once we were all set up, we were able to simulate a production environment for the most thorough possible testing.”

“It was logical to choose F5 for our WAF because…we can support multiple solutions with the same technology.”

—Daniel Debarbieri, Senior Infrastructure Security Analyst

Benefits

By choosing BIG-IP Application Security Manager as its comprehensive web application firewall, Banco Supervielle extended coverage to additional critical applications and regained compliance with Central Bank of Argentina regulations. It also saved on IT labor and could create a high availability environment.

Strengthens security

The bank reinforces security in several ways by using BIG-IP ASM as its WAF. First, by separating its QA and test environment from its production environment, the bank ensures that all applications (including those not supported by its prior WAF) are fully tested with a working WAF in place. “With our F5 solution, every time we deploy or upgrade an application, we can be confident that it belongs in production and is well protected,” says Lorenzo. “That is a critical benefit for us, and it fully addresses the biggest problem that concerned the Central Bank of Argentina.”

In regard to SSL security, a third-party security rating agency previously gave Banco Supervielle a low rating for the configuration of its SSL web servers. “Now we are ranked among the top-secured sites in Argentina,” says Lorenzo. “This is critical because some customers were saying, ‘Why are you ranked so poorly in this area?’ That is no longer a problem.”

Supports multiple platforms
The new Banco Supervielle WAF from F5 protects applications ranging from home banking and corporate websites to credit cards and electronic billing. Also, in a clever but unconventional use case, the bank employs the WAF to protect a mobile device management solution from Citrix. The applications run on a variety of platforms, including Microsoft Internet Information Services, IBM WebSphere, Java 6.0, and ASP.NET.

“Most of these applications are third-party products,” explains Lorenzo. “They’re developed in different languages and operating systems. We choose the best products from among the various brands because we don’t want to be a one-vendor shop.”

With BIG-IP ASM, Banco Supervielle has the capacity to create policies for these different platforms and applications. “The versatility we now have to deploy any application we want and define rules for it will enable us to improve and develop new services more quickly and with more confidence,” Lorenzo says.

**Provides system insight; saves labor**

The previous system generated many false-positive errors, blocking system functionality and web pages that were not actually compromised. “We rarely have to respond to false positives anymore,” says Lorenzo. Each trouble ticket—positive or false-positive—takes about 15 minutes, and the number of tickets has dropped from several dozen to fewer than 10 per month. “Consequently, we don’t have IT technicians chasing down errors that may or may not exist, which saves on labor and gives us the opportunity to work on other value-added projects.”

He adds that the monitoring capabilities of BIG-IP ASM provide better visibility into application security, giving his team the ability to respond to possible threats before they affect system operation. As an example, he cites January 2014 versus January 2015: “Before the new WAF, we proactively identified and resolved only about 20 events; now it’s more than 55.”
“IT departments tend to receive punches when things go wrong, but no applause when systems run smoothly,” Lorenzo concludes. “Users don’t see how we monitor system health—all they see are the help-desk tickets they file in their day-to-day work. Today we are seeing better system health and fewer tickets, and that tells us we’re doing things right.”