



“At the time of deployment, we can secure critical applications proactively and rapidly, directly through the F5 unit. This gives us the advantage of not having to go through development and multiple rounds of testing, which saves us a lot in terms of rollout time and resources.”

Philippe Bossut
Network System Manager
Crédit Coopératif



Crédit Coopératif Secures Its Online Banking Services With F5 BIG-IP Application Security Manager

Industry

- Banking

Challenges

- Stay ahead of application security threats
- Ensure optimal quality of service

Solutions

- BIG-IP® Local Traffic Manager™ (LTM) with iRules™ scripting language,
- BIG-IP Application Security Manager™ (ASM), and SSL Acceleration Module

Benefits

- Ease of deployment and centralized administration for multiple functions
- User application performance improvement
- Customizable security configuration to address evolving needs
- Reduced total cost of ownership

Overview

Crédit Coopératif is a bank serving co-operative or grouped enterprises: small and medium enterprises and industries (SME-SMI); associations; public interest organizations and services; and private individuals. Crédit Coopératif covers all regions of France with a network of 75 branches and 1,750 employees.

With an Internet-focused service strategy running on a BEA Weblogic application platform, this leading cooperative bank keeps a step ahead of emerging security threats using a centralized solution for Application Delivery Networking from F5. This solution guarantees security, high availability, reliability, and future-proofing for its web applications.

Challenges

Crédit Coopératif has been delivering remote banking services to its clients since the early days of Minitel, France's highly successful, terminal-based Internet precursor that launched in the 1980s. Crédit Coopératif developed Internet applications in 2002 and is once again at the cutting edge of online banking services.

With a wide range of clients using its online services, Crédit Coopératif offers a number of custom applications that were developed entirely in-house on a J2EE platform. The majority of

Crédit Coopératif's customers now use its online banking services.

As the bank continued to develop its online service offerings, it required a security solution that would match the critical nature of these services, especially with regard to transaction applications.

Crédit Coopératif has a proactive policy of keeping ahead of security threats before they arise, while at same time providing optimal quality of service for its clients. The bank needed a security solution that could be integrated at the infrastructure level and that could be rolled out easily and adapt to meet future needs.

Solution

Crédit Coopératif turned to Adines, a Paris-based IT company specializing in the integration of LAN/WAN networks with global security systems, to help identify the best solution to meet its needs as well as the expectations of its online users.

After evaluating three vendors, Adines recommended that Crédit Coopératif implement an Application Delivery Networking infrastructure from F5 for all of its remote banking services. F5's track record and innovative technologies convinced Crédit Coopératif that F5 would provide the best strategic, long-term solution to meet the bank's security needs.



The bank chose F5 BIG-IP Local Traffic Manager (LTM) with the BIG-IP Application Security Manager (ASM) software module for the application firewall and SSL acceleration, termination, and re-encryption to the J2EE servers.

A single platform

“The ability to perform all of these different functions on one platform—from load balancing and application security to performance optimization through SSL acceleration—was a key differentiating factor, backed by the ease of both the implementation and the administration GUI,” says Sassi Mazroui, General Manager at Adines.

Beyond the centralized and simplified management of its web applications, Crédit Coopératif also saw benefits with F5’s iRules scripting language, which makes it possible to adapt the solutions to custom applications. iRules has been especially useful when applied to Java session persistence, resulting in a critical performance improvement for the online banking services.

Business-critical, strategic security

“Our security budget is a strategic IT investment,” says Philippe Bossut, Network System Manager at Crédit Coopératif. “This investment not only enables us to stop possible attacks, but is first and foremost an asset ensuring optimal responsiveness to meet the needs of our clients. They can use our services with complete peace of mind. It’s not about curing, but preventing.”

“The teams responsible for the infrastructure and the applications assess the potential risk associated

with each specific application, and we draw up an action plan accordingly,” explains Bossut. “At the time of deployment, we can then secure critical applications proactively and rapidly, directly through the F5 unit. This gives us the advantage of not having to go through development and multiple rounds of testing, which saves us a lot in terms of rollout time and resources.”

Handling data streams with an average size of 85 KB/page, the F5 solution processes an average of one million requests a day, with 1,200 HTTP/HTTPS connections per second at peak periods.

Easy, centralized administration

BIG-IP ASM is well-suited for remote banking applications, specifically for securing branch-to-branch, web-based banking applications. BIG-IP ASM proxies and logs all communications between the remote applications, allowing it to inspect all application traffic and guard against brute force attacks and validate all dynamic form parameters.

BIG-IP ASM continually inspects the application site structure, monitoring for changes to the application and the data patterns coming into the application. Via a dashboard interface, the security administrator can monitor when ASM detects these changes and view the suggested changes to the security policy, choosing either to accept those new blocking changes to the security policy or to reject them.

“The BIG-IP ASM [Real Traffic Policy Builder] architecture allows it to be compatible with applications based on application delivery

analysis,” explains Bossut. “From that analysis, the security teams determine the optimal application security policy, based on the application security risk and cost-based factors. Since the application is protected by BIG-IP ASM, it can then either be fixed or re-developed as needed for compliance, or be fixed and re-developed.”

Before deployment, each new application is therefore made compliant with Crédit Coopératif’s global protection policy, provided through the F5 solution. In this way, BIG-IP ASM makes it possible to implement the required configuration, application by application, through collaboration between the development teams.

By integrating the security, optimization, and load-balancing functions on one platform, Crédit Coopératif benefits from standardizing the security and maintenance of the applications. This one-stop solution for rolling out applications to users reduces the total cost of ownership by using the resources needed to manage these functions more efficiently.

Beyond the ease of configuration and implementation, the BIG-IP platform optimizes IT resources by performing load balancing and SSL acceleration without any negative impact on performance. In light of this success, Crédit Coopératif is considering ways to further integrate F5 technology into the business.

“Integrating these functions onto a single, centralized platform gives us a significant advantage in terms of application management and administration,” adds Bossut. “Now we can look forward to future developments with confidence.”

F5 Networks, Inc.
Corporate Headquarters
 401 Elliott Avenue West
 Seattle, WA 98119
 (206) 272-5555 Phone
 (888) 88BIGIP Toll-Free
 (206) 272-5556 Fax
www.f5.com
info@f5.com

F5 Networks
Asia-Pacific
 +65-6533-6103 Phone
 +65-6533-6103 Fax
info.asia@f5.com

F5 Networks, Ltd
Europe/Middle-East/Africa
 +44 (0)1932 582 000 Phone
 +44 (0)1932 582 001 Fax
emeainfo@f5.com

F5 Networks
Japan K.K.
 +81-3-5114-3200 Phone
 +81-3-5114-3201 Fax
info@f5networks.co.jp