



++++financial apps+++++

BY PETE BARTOLIK

Illustration by David Flaherty

In the money

With financial applications, performance and security are more important than ever.

Financial applications are the lifeblood of the modern enterprise. They extend the reach of data throughout an organization so that employees can obtain real-time information to make better business decisions. They can link business partners as real-time collaborators and provide customers with the ability to access up-to-date records or execute transactions. But enthusiasm over application availability is tempered by the critical needs to ensure security and uphold performance requirements.

In most organizations, these applications provide the financial underpinning for tracking and analyzing every part of an organization's capital resources, from general ledger to purchasing, billing, forecasting, and much more. They tap into a variety of back-end databases that store corporate information assets. They also provide tempting targets for nonauthorized outsiders.

Coast Capital Savings, Canada's second-largest credit union with \$6.7 billion in assets, relies on 24/7 network operations to handle the many applications and enormous data flows of modern banking. IT professionals require frequent remote access

during off-hours for network administration, support, and troubleshooting. A cadre of mobile sales brokers—both employees and contractors—also need to access email, a contact management system, and banking and brokering applications. “Any time you wedge an application into your IP stack,

you have potential for trouble,” says Andrew Banman, a systems engineer on the Coast Capital Savings IT infrastructure team, which devised a new architectural approach to remote access security built around a FirePass Controller from F5 Networks.

Application struggles

While many enterprises are developing browser-based access to enterprise and web applications, others are still struggling with the issues of effectively supporting client/server infrastructures. According to a Forrester Research survey conducted for F5, which polled 300 IT decision makers in North America, many companies are stymied by poor performance and security issues as they try to innovate and introduce new applications. Often they are supporting a wide portfolio of applications, including packaged products like SAP, PeopleSoft, and Oracle; home-grown software; and open-source offerings.

“With security, the challenge is even more complex,” said Ido Breger, F5 product manager for application security. “Who owns security in a web application? Is it the web server administrator, the firewall person, the database administrator, engineering? Often these groups don't even talk to each other.”

Forrester recommends creating a flexible architecture that bridges the gap between infrastructure and applications. What is referred to as an application delivery infrastructure addresses technology problems as well as people and process requirements by enabling increased collaboration between application developers, network operations, and enterprise architects. And,

says the market research organization, a unified, policy-driven platform will provide the flexibility to accommodate changes in business requirements without recoding applications or deploying additional back-end resources.

The Application Ready Network

That type of flexibility is at the core of F5's Application Ready Network approach, says Alan Murphy, F5 technical marketing manager for security. "Typically, an existing F5 customer will already have BIG-IP Local Traffic Manager at the edge of their network, so they're providing access to their web app and maybe FTP servers or mail servers, and they're already front-ending an application server in their network. They have this orchestrated network that is working really well, but they need to add web application security."

According to Murphy, adding BIG-IP Application Security Module (ASM) to the BIG-IP application traffic management platform provides application-layer protection from both targeted and generalized application attacks to ensure that applications are always available and performing optimally. That can be accomplished with a simple license activation, Murphy explains.

F5's announcement earlier this year of the F5 Application Ready Network for Microsoft and the F5 Application Ready Network for SAP heralded a holistic application network architecture and infrastructure. These were designed and optimized for Microsoft Office SharePoint Server 2007, Microsoft Exchange Server 2007, and Microsoft Live Communications Server 2005, as well as for solutions that use the SAP NetWeaver platform and an enterprise service-oriented architecture.

Policy out of the box

The latest release of ASM [see sidebar] enhances the Application Ready Network approach with ready-made policies out of the box, says Breger. As it monitors live traffic, ASM prompts administrators to add more rules into the policy based on actual activity. "While ASM is listening to traffic, it starts embedding more and more specific rules based on the traffic. It introduces additional rules until it has profiled all of the traffic that is passing through a web site," says Breger.

With developers crafting applications as fast as possible and business teams urging rapid "webification" of applications, "many times security is left to the last step before production," according to Breger. With ASM, developers can focus on the rapid deployment of new applications and functionality, knowing that their code is sitting behind an established security perimeter, rather than having to scour for security holes and then hard-code plugs to fill them.

Secure access to online services, whether for customers or internal clients, is critical to today's business operations. "It is no exaggeration to say that responsiveness and stability of services are our life," says Kunihiko Sato, general manager of systems planning for Matsui Securities Co. Ltd., the first securities broker in Japan to specialize in online transactions.

Customer service requirements

A BIG-IP Local Traffic Manager (LTM) customer since 2002, Matsui in 2006 upgraded to the BIG-IP v9 series with two BIG-IP 6400 LTMs and four BIG-IP 1500 LTMs. The company had seen online transactions increase from 20,000 in 2002 to almost 200,000 in 2005. A key consideration in the upgrade decision was the need to handle a rapid increase in the number

A HANDS-FREE APPROACH TO BUILDING POLICY

The latest release of BIG-IP Application Security Module (ASM) now features the real traffic policy builder, which automatically builds policy rules as it monitors live traffic. Once ASM is installed, says Alan Murphy, F5 technical marketing manager for security, "The first thing it is going to do is watch live traffic going across the network. Then it will start building a security policy based on that live traffic. Passive monitoring builds a live application policy. It requires very little interaction with the administrator."

In the case of financial services companies and others that develop custom applications, network administrators will be able to apply ASM to new applications as they are being developed and tested, says Murphy. As a result, they will be able to generate secure policies without having to know the nitty-gritty of the application.

In addition, ASM comes with ready-made policy templates that can have an organization up and running immediately for certain popular environments, including the Microsoft Office system and Lotus Domino. "Over time, as we continue to roll out more Application Ready Networks, we're going to add to those templates," says Murphy.

F5 will also encourage customers of other environments to post their own policies to the online customer community, F5 DevCentral. "This is perfect for open-source software," says Murphy. "Over time we will have great community open-source templates."

of transactions should the release of information prompt a spike in customer activity.

According to the Forrester Research survey, improving customer satisfaction is the top IT priority, ahead even of improving the company's top or bottom line. Yet almost one-fourth of those surveyed reported problems with application deployments in the previous year, and 53% said they've experienced performance issues during deployments.

Forrester argues that an application delivery infrastructure streamlines application deployments and delivery, enabling organizations to deliver results from legacy apps more rapidly, as well as ease application architecture transitions. This provides a policy-driven platform that creates an abstraction layer between basic network transport and application middleware.

Murphy recommends that enterprises approach the application delivery issue by first focusing on building a highly available infrastructure. "That's the critical component," he says. "Typically an administrator is going to put a BIG-IP product in a staged environment in front of some applications. Once they have that set up, then they can just activate ASM and let it run."

There's no question that application delivery is a business-critical requirement for financial services organizations. But overburdened IT organizations are faced with the challenges of building an infrastructure for financial applications that must scale to meet the needs of hundreds, thousands, or even millions of users, while delivering high availability without compromising security. Application Ready Networks provide a framework for financial services organizations to achieve those goals with a proactive, relatively hands-free solution. ✱

Pete Bartolik is a Hopkinton, Mass.-based freelance writer.

Read the Forrester study, "Improving Application Deployments," at www.f5world.com.