



## Coast Capital Savings Banks Rely On The FirePass Controller For Easy and Secure Remote Access

### Customer Profile

**Company Name:**

Coast Capital Savings

**Location:**

Vancouver, B.C.

**Industry:**

Financial Services

**Web site:**

<http://www.coastcapitalsavings.com/>

**Company information:**

– Canada's second largest credit union with \$6.7 billion in assets, 44 branches and 2,000 employees.

– Named one of Canada's 50 Best Managed Companies in 2004, a designation it has received each year since 1999.

**About Coast Capital Savings**

Coast Capital Savings is Canada's second largest credit union, with 300,000 members and 44 branches across the Fraser Valley, Lower Mainland and Vancouver Island. Their long-term vision is to serve communities across Canada and to be the first choice for financial services, products and financial planning advice.

### Executive Summary

Behind the data network so vital to the 24x7 operations of Coast Capital Savings is a team of IT professionals who need frequent remote access during off-hours for network administration, support and troubleshooting. What's more, a cadre of mobile brokers who sell the credit union's financial products need remote network access to its applications and data. To keep these associates productive no matter where they are and to keep unwanted intruders out of its network, Coast Capital Savings deployed F5's FirePass 1000 Controller as a mainstay of its perimeter security and to replace a complex, hard-to-manage IPSec VPN scheme.

### Challenge

Like all financial institutions today, Coast Capital Savings relies on its network to handle the many applications and enormous data flows that have come to represent modern banking. Keeping that vital network operating 24x7 as well as securing it from hackers and all kinds of malicious attacks is the job of the credit union's information technology staff.

To meet these critical and ongoing demands, IT staff members often must log into the network from home - not matter whether they're teleworking during the day, working off-hours on nights and weekends, or traveling. This way, they can do the network administration, maintenance and occasional troubleshooting needed without the time and bother of coming into the office.

But they aren't the only ones with remote access needs. A group of mobile sales brokers - both credit union employees and contractors - operate far enough away from the institution's regional offices that they too need to connect to the network several times a day. In addition to email, their requirements include access to a contact management system, to banking and brokering applications, and to transactional capabilities while conducting business on a customer's premises.

For Andrew Banman, a systems engineer on the Coast Capital Savings' IT infrastructure team, providing remote access to both his colleagues and the brokers was a constant concern. Although the credit union had an IPSec-based VPN solution in place, the overhead associated with administering it was considerable. Issues with IP addressing, network address translations, limited remote device support, and the installation and maintenance on every client PC required IT's time and constant attention. "Plus, anytime you wedge an application into your IP stack, you have potential for trouble," he said.

Even with the IPSec VPN solution in place and despite a considerable cost of ownership, Banman still wasn't satisfied that the credit union's network perimeter was secure. "VPN solutions are easy to find, but one that could meet our needs isn't," he explained. "That's because most VPNs tie the remote desktop or laptop physically into the network so they become network nodes." And that, he added, is where the trouble comes in.

"The reality is that few people manage their (remote client) PCs correctly and so many of those PCs are virus-ridden without their users even knowing it. So when they dial into the network, their problems become our problems."



Banman has good reasons to worry. With more than 100,000 known viruses, plus some 250 more spreading across the Internet each month, isolated user problems can become big problems<sup>1</sup>. In fact, more than 90 percent of the businesses responding to the 2004 ICSA Labs Virus Prevalence Study said they had installed virus protection on 100 percent of their networks. However, 51 percent of these respondents said they had experienced at least one virus disaster in the past year.<sup>2</sup> The average attack, according to the ICSA report, led to 17 hours of server downtime and the loss of 24 person-days. The average cost of a security disaster, meanwhile, was estimated at \$100,000<sup>2</sup>.

"So far, we've been lucky to evade the worst of what's out there," said Banman, "but we have had instances of users' PCs broadcasting viruses into the network, causing us considerable time and effort to clear them out."

For all these reasons affecting cost, productivity and security, Banman and the IT infrastructure team members devised a whole new architectural approach to Coast Capital Savings' remote access security. And to enable it, they chose a FirePass® 1000 Controller from F5 Networks.

<sup>1</sup> PC World, June 2004.

<sup>2</sup> ICSA Labs 9th Annual Computer Virus Prevalence Survey, ICSA Labs, a Division of TruSecure Corporation, 2004.

### Solution

With the F5 FirePass 1000 Controller, Banman and his IT colleagues have set up an SSL VPN that uses standard Web browser technology to provide secure access to remote users as if they were directly connected to the network.

In effect, this model lets remote users connect via a Web-based interface to the FirePass 1000 Controller, which can handle up to 100 concurrent sessions. Then the FirePass controller connects them to the credit union's network for the duration of their session.

"This gives us the ability to sever the remote users' direct tie into the network, putting their PCs in a quarantine of sorts but without denying them the use and productivity of the applications and data on the network," said Banman. "It's simple for users, but a highly effective approach to keeping the potential for security breaches at bay."

The FirePass model of separating remote users from the Coast Capital network was a key reason he chose the F5 solution. He pointed out that prior to installing the FirePass Controller, the few virus attacks that did manage to breach their already strict VPN and anti-virus measures cost the credit union several days worth of time for three to four IT staffers to uncover the virus source and then eradicate every instance they could find. The staff time involved approached \$4,000. "Even then," he said, "the virus might re-emerge months later. With FirePass, we haven't had a single incident."

To gain even greater security beyond the standard user-name and password protections, FirePass enabled Banman to institute two-factor authentication. For that capability he employed RSA SecurID® token-based key fobs. The FirePass benefits aren't all in terms of security though. Unlike traditional IPSec VPNs, the FirePass gives users remote access without their laptops or home PCs needing client software installed and configured. Of course, this saves time and hassle for both the IT staff and users from the start, but it also saves help desk tickets and ongoing support costs.

In addition, users gain tremendous flexibility in how they can connect to the network. That's because FirePass is the first SSL VPN solution with complete cross-platform support, so users can use whatever device is available to them regardless of operating system - Macintosh, PocketPC or Linux-based devices, as well as Windows, for accessing applications and data securely. All they need is a Web browser to get access to Coast Capital Savings' network.



## SUCCESS STORY

---

Additionally, the FirePass Controller allows them to connect to a broad set of applications, such as legacy host systems, terminal servers, client-server applications, or Windows desktops.

Banman cited another FirePass unique benefit of being able to ensure that remote users are in precise compliance with the credit union's licensing terms with Microsoft for its applications.

"Because we're using terminal services, we can guarantee a one-to-one relationship between users and their use of Microsoft's applications. We looked at a lot of products and only FirePass gave us this capability." Deploying the FirePass went smoothly, Banman reported, "due in great part to having no footprint on remote devices and the fact that FirePass requires zero client-side support."

"We started using the FirePass remote access model first with a pilot group within IT then to the broader IT group and then to the brokers. And even though we had a dramatic increase in users in the course of deployment, there was no noticeable increase in support calls."

Overall, Banman is extremely pleased with the FirePass controller. "We're really happy with the product," he said, "and we're looking to implement more of them into our network."

### About F5

F5 enables organizations to successfully deliver business-critical applications and gives them the greatest level of agility to stay ahead of growing business demands. As the pioneer and global leader in Application Traffic Management, F5 continues to lead the industry by driving more intelligence into the network to deliver advanced application agility. F5 products ensure the secure and optimized delivery of applications to any user - anywhere. Through its flexible and cohesive architecture, F5 delivers unmatched value by dramatically improving the way organizations serve their employees, customers and constituents, while lowering operational costs. Over 6,000 organizations and service providers worldwide trust F5 to keep their businesses running. The company is headquartered in Seattle, Washington with offices worldwide. For more information go to [www.f5.com](http://www.f5.com).