



## Case Study:

### Contra Costa Community College District Upgrades to SSL VPN

One of the largest community college districts in California, the Contra Costa Community College District serves Contra Costa County (east of San Francisco) with five campuses. The district office in Martinez, California houses administrative offices and central data processing for the district.

As the district's Network Technology Manager, Katherine Ogden's job is to keep the district's central computing facilities available to administrators as well as hardware and software vendors who need access to the network for periodic maintenance and updates. In addition, the district has an extensive ERP system and a staff to maintain it as well as the data center servers.

#### IPSec VPN: A Management Nightmare

The district office initially deployed a Cisco IPSec VPN and Cisco PIX 515E firewall to provide remote access for vendors and administrators back in 2001, but the system had always been plagued with problems. "It was a really frustrating system to use," says Ogden. "We had problems with installation and problems with connectivity that required constant support calls and a lot of unhappy users."

To provide a remote user with a VPN connection, the user had to take home a client installation CD from the district office. In more than one case, incompatibility between the Cisco client and other existing software on users' computers actually wiped out the operating system. "We had to rebuild those computers from scratch," says Ogden, "and even installing the client was a difficult process. We had written up a set of instructions and troubleshooting steps, but we still got calls for support."

Another problem was that the Cisco VPN had issues with connections dropping because it had a built-in timeout. Users would start a process that was supposed to run for two or more hours and the VPN appliance would drop the connection in the middle of the process.

As for functionality, the Cisco VPN was a "keys to the kingdom" access system. Once a user gained access to the network, they could access any part of the network. "We had one situation where a vendor had software on systems at the district office as well as on systems at specific campuses, and they logged in to our network remotely and then traversed our WAN to do maintenance on campus systems. We got into a lot of trouble because the campuses hadn't been notified that their systems would be down for maintenance," says Ogden. "We really wanted to be able to limit a vendor's access to specific servers."

Finally, the Cisco VPN had no endpoint security checking. "We wanted to check for virus protection and patch updates on remote user systems, but we couldn't," says Ogden. "Doing so would have required the purchase of third-party software to do so".

#### The NeoAccel Solution

With a very tight budget, Ogden and her staff muddled along with the IPSec VPN for several years. She had looked at a few alternative VPN appliances but wasn't convinced they would be worth the investment. But in 2006, she was approached by NeoAccel to be an early test site for the company's new SSL VPN-Plus product. "I was skeptical before they put it in, but the product sold itself," she says. "I hadn't planned to spend any money on VPN that year, but I once I was it working I was sold."



NeoAccel's SSL VPN-Plus offered a better experience for both the IT staff and end-users from installation to functionality and administration. SSL VPN-Plus offers a choice of clientless, thin-client, and full-client operation, depending on whether the remote user needs access to only Web-based applications, legacy applications or full applications. The Contra Costa District uses the full client, which the user downloads and installs. While the full client provides broader application access – essentially allowing the user's PC to work as if it was connected to the district's internal LAN, it has presented very few challenges. "Mostly, it's been a 'fire and forget' solution," says Ogden. "Most people do a self-install without any special directions from us, and we never hear from them again."

While there has been one installation problem out of dozens of installations – it occurred with a brand new, high-performance system – NeoAccel's support staff was already aware of the problem when it received a call from the district, and it had a fix on the way shortly. In all, the simplicity of SSL VPN-Plus installation has enabled Ogden and her staff to roll out VPN services to more of the district's administrators – a goal that had been prevented by the high administration overhead of the previous solution.

SSL VPN-Plus also provides full endpoint security checks prior to allowing network access. "I knew I had one individual who wasn't consistently running anti-virus on his machine, so I really liked having a product that would make sure the machine was safe before it allowed a connection to the network," says Ogden. The new solution also allows Ogden and her staff to limit users' access to specific servers.

From the user perspective, most feel that SSL VPN-Plus is faster. Users also appreciate the new solution's reliability, since it doesn't drop their connections in the middle of a session.

From a management perspective, SSL VPN-Plus integrates with user information from Microsoft Active Directory, so Ogden's staff doesn't have to issue new passwords for VPN access.

### **Ease of Use Expands Remote Access**

Having a fast, easy-to-deploy solution that provides full access control granularity has expanded Ogden's vision of remote access. "When we got SSL VPN-Plus, we realized it was so much easier to administer and it gave us so much finer control over what people could access, that we started rolling it out to some of the key administrators and vice chancellors of the district so they could log in from home as well," she says. "Eventually, I see us rolling this out to all of the managers and administrators at the district office as well as the remote administrators at the campuses."

Ogden is also excited about NeoAccel's new network access control product, NAM-Plus, because it offers the industry's only true application-level access control. "We don't allow access to our ERP system except for wired PCs at specific locations, so application-level control would be very nice," she says. "Some of our managers have laptops as their main system at work, and when they take the laptop home and VPN in, we don't want them to be able to launch the ERP system because they're not at a pre-secured location. We also have several conference rooms and empty cubicles at our offices, and it would be great to use a NAC to secure ports in those locations so a vendor or consultant couldn't just walk up and get on the network. We'd like to prevent that right now, but we don't have the staff to monitor switch ports."

With security solutions that are simple to deploy and provide unprecedented performance, access control granularity, and ease of use, NeoAccel is transforming access security for the Contra Costa Community College District.