# Civil-Engineering Firm Provides Secure Access to Support Major Collaboration Effort

BURGESS & NIPLE

## Overview

**Country or Region:** United States
**Industry:** Civil engineering

### Customer Profile

Founded in 1912 and headquartered in Columbus, Ohio, Burgess & Niple (B&N) provides civil-engineering services to government, military, educational, and private enterprises throughout Ohio and beyond.

### Business Situation

Leading the design phase of the largest transportation-infrastructure program in the state's history, B&N needed a way to provide subcontractor firms secure yet convenient access to its network.

### Solution

A solution based on Active Directory® client certificates, Microsoft® Internet Authentication Services, and a Cisco Catalyst 3550 Multilayer Switch provides 802.1x network access control for all network access points.

### Benefits

- Enhanced productivity and collaboration
- Effective protection against viruses
- A culture promoting partnership and collaboration

"With this solution, we can provide a convenient and cooperative working environment for our partners … while maintaining the integrity of our data and overall infrastructure."

Fred Mau, Chief Technology Officer, Burgess & Niple

Chosen to lead the design of the largest transportation-infrastructure project in Ohio's history, Burgess & Niple (B&N) faced a challenge that had nothing to do with roads, bridges, overpasses, or on-ramps: how to enable engineers from 13 subcontractor firms to use on-site network resources without compromising the security or integrity of the firm's data. To address the challenge, the Columbus-based firm deployed a solution based on Active Directory® client certificates and a Cisco Catalyst 3550 Multilayer Switch. Through 802.1x network access control for all network access points, the solution not only supports the open, collaborative policy of B&N toward its subcontractor engineers on the transportation program, but also helps to protect the firm from computer viruses.

Microsoft Windows Server System

"We had comprehensive 802.1x security measures in place for our wireless network, but these measures were not designed to protect against unauthorized access into our larger wired network."

Fred Mau , Chief Technology Officer, Burgess & Niple

## Situation

Founded in 1912 and headquartered in Columbus, Ohio, Burgess & Niple (B&N) provides civil-engineering services to government, military, educational, and private enterprises worldwide. With offices in 15 locations throughout the United States and a staff of more than 600, this award-winning firm has designed everything from roads, dams, and sewers to military housing, hydroelectric power plants, and wastewater treatment facilities.

Having pioneered breakthrough techniques for water treatment, bridge inspection, and other vital infrastructure services, B&N engineers have earned a reputation for innovation. Now, the firm is applying its innovation to the largest transportation-infrastructure program ever undertaken in the state: the redesign of the Cleveland Innerbelt Freeway System. That program, estimated to cost nearly a billion dollars and to require up to nine years of construction effort, will ultimately involve the participation of thousands of people. The design phase alone includes not only dozens of engineers from B&N, which is acting as the lead contractor, but also dozens of others from 13 partner firms that are subcontracting as part of the larger design team.

These engineers are spending a lot of time at the B&N Cleveland office, which is headquarters for the design phase of the program. At that office, the engineers are giving presentations, attending meetings, consulting, and reviewing what will ultimately total hundreds or thousands of essential design documents. They also are connecting their portable computers to the B&N network to gain remote access to their own companies' file servers and to gain local access to the B&N printers, plotters, and document-management system.

"Having access to such resources is essential for our partner engineers to do their work efficiently and for the whole team to work productively," says B&N Chief Technology Officer Fred Mau. "But in the beginning, providing such access forced us to confront a significant security challenge."

As Mau explains, when he and his colleagues initially considered the prospect of having dozens of "outside" computers connecting to the B&N network, they knew that further security would be required to protect against unauthorized access to confidential data and against inadvertent infection with viruses. "We had comprehensive 802.1x security measures in place for our wireless network, but these measures were not designed to protect against unauthorized access into our larger wired network," he says.

So Mau and his colleagues began thinking about how to address the challenge of secure access for the outside computers. "We initially considered configuring several wall outlets for Internet access only," he says. "But we risked having our own staff members plug into them and then consume technical support resources by asking why they couldn't access the server. Similarly, we felt that merely labeling the outlets was not sufficiently secure because we could not ensure that a partner engineer would never plug into the other, nonrestricted outlets."

In sum, B&N needed a system that would automatically enforce network access privileges from any wall outlet in the Cleveland office. Mau concludes, "That was the only way we could prevent outside computers from gaining access to our internal, confidential systems and yet remain a good host to our partner firms."

"We couldn't have done this so cleanly and quickly without the support of Microsoft and Cisco Systems."

Fred Mau , Chief Technology Officer, Burgess & Niple

## Solution

Because B&N relies exclusively on Microsoft for its server and client software (including the Active Directory® service for user authentication) and Cisco Systems for its networking hardware, Mau and his colleagues felt that the obvious solution was to integrate the most powerful security technologies from both vendors. For this reason, Mau's team were delighted to learn that the companies had recently launched a joint effort to provide a particularly high level of interoperability between two such technologies: Network Access Protection (NAP), a feature of Microsoft® Windows Server™ 2003 that provides end-point enforcement of security policies, and Cisco Network Admission Control (NAC), a specification for security-policy compliance.

In response, the team used those technologies to implement 802.1x network access control for all network access points in the Cleveland office. Specifically, they integrated Active Directory client certificates and a Cisco Catalyst 3550 Multilayer Switch. The certificates assign unique identification to each B&N computer, and the switch enforces a multiple virtual LAN (VLAN) policy. (Active Directory is a component of Windows Server, the operating system foundation of Microsoft Windows Server System™ integrated server software.)

Mau explains that the deployment uses Active Directory policies to distribute the client certificates and Microsoft® Internet Authentication Services to authenticate them. The team also installed a domain controller to authenticate users when they come online.

In all, Mau's two-person team spent about two weeks in development. Much of that time was devoted to identifying attachments to the switch ports and testing the connected computers. "Because it was our first time developing this kind of solution, we did a lot of experimenting," Mau explains. "But now that we have, I feel confident we could implement a similar solution in a matter of hours." Since the deployment has been complete, Mau reports no significant problems, which he attributes largely to the expert telephone assistance that his team received from Microsoft Services Essential Support and Cisco SMARTnet Onsite Solutions. "It was vital that we have easy access to professionals who understood the subtleties of technical features and could provide advice on how to distribute the certificates and integrate them with the switch," he says. "We couldn't have done this so cleanly and quickly without the support of Microsoft and Cisco Systems."

## Benefits

Today, there are about 600 B&N client computers that regularly access the corporate network and, at any given time, about a dozen computers from partner engineers. These engineers simply plug into any wall outlet and access the Internet, their own office file servers, B&N printers and plotters, and the document-management system without compromising the security of the B&N network.

### *Innovative, Effective Approach to Access and Security*

As Mau explains, when a partner computer is plugged into a B&N wall outlet, it is put on a very restricted VLAN that isolates it from the larger network. "This security goes way beyond prohibiting logon to B&N servers. A partner's computer cannot even 'see' the B&N servers, or B&N client computers, for that matter," he points out. "On the other hand, when a B&N employee plugs into the outlet, the system recognizes the computer as one of our own and gives the user IP access to the network through the regular logon procedure."

"With this solution we can provide a convenient and cooperative working environment for our partners ... while maintaining the integrity of our data and overall infrastructure."

Fred Mau , Chief Technology Officer, Burgess & Niple

Mau points out that the solution he and his colleagues implemented is not all that common. "Consider that we are basing a security system on revocable client certificates with standard Active Directory and Internet Authentication Services features for access by wired, rather than wireless, computers," he says. "When we consulted the Microsoft and Cisco support personnel during development, even they found it a bit unusual. That said, it certainly has been effective."

### *Strong Protection Against Viruses*

Mau says the solution does more than support the efficient and secure partner access that is essential for the success of the Innerbelt Freeway System program. It also helps to protect B&N against a potentially far more serious threat than, for example, a partner's inadvertent access to confidential data: viruses and other malicious incursions. "We don't dictate the security practices of our partner firms, so we can't ensure that their computers meet the same antivirus standards as our own," he says. "That's another reason why this security solution is so vital."

In addition to being vital to B&N's participation in the Innerbelt Freeway System program, the security solution has proven to be highly effective, Mau says. "We have had no virus attacks, not one, since deployment."

Even after the current program is complete and the partner engineers are no longer accessing the B&N network, there will be sales representatives, consultants, or repairpersons who may need on-site Internet access, Mau points out. "As well, there are always our own engineers traveling on assignment and checking e-mail from remote locations. We may be diligent about issuing security updates to users here, but if remote users don't log on for a few days, they might miss the update and inadvertently pass a virus to the network."

To address such potential security challenges, B&N will implement a solution to verify that any computer accessing the network is authenticated and that it complies with the most up-to-date security requirements. For this, the firm will use Microsoft Network Access Control solutions to provide a security audit before any computer can connect to the network.

### *Maintaining Openness and Innovation*

As Mau points out, security audits are especially important in the civil-engineering environment. "Civil engineering is a traditionally open culture, where work is for the public and a free flow of information nourishes innovation," he says. "At B&N, we aren't particularly proprietary about our work, we don't wear badges, and literally anyone could walk into one of our offices and plug into a wall outlet."

Mau believes that the security solution his team implemented with Active Directory helps to demonstrate that the firm can maintain its open, collaborative approach. "With this solution," he says, "we can provide a convenient and cooperative working environment for our partners on the Innerbelt Freeway System program and on other projects in the future, while maintaining the integrity of our data and overall infrastructure."

He says that the solution also helps to demonstrate the value of client certificates in Active Directory and the ability of Active Directory to integrate with mainline network vendors, in particular Cisco Systems. "And that makes the technologies of both Microsoft and Cisco Systems central to the well-being of our firm."

## For More Information

For more information about Microsoft products and services, call the Microsoft Sales Information Center at (800) 426-9400. In Canada, call the Microsoft Canada Information Centre at (877) 568-2495. Customers who are deaf or hard-of-hearing can reach Microsoft text telephone (TTY/TDD) services at (800) 892-5234 in the United States or (905) 568-9641 in Canada. Outside the 50 United States and Canada, please contact your local Microsoft subsidiary. To access information using the World Wide Web, go to: www.microsoft.com

For more information about  products and services, call  or visit the Web site at:

For more information about Burgess & Niple products and services, call (614) 459-2050 or visit the Web site at: www.burgessniple.com

## Microsoft Windows Server System

Microsoft Windows Server System integrated server infrastructure software is designed to support end-to-end solutions built on the Windows Server operating system. Windows Server System creates an infrastructure based on integrated innovation, Microsoft's holistic approach to building products and solutions that are intrinsically designed to work together and interact seamlessly with other data and applications across your IT environment. This helps you reduce the costs of ongoing operations, deliver a more secure and reliable IT infrastructure, and drive valuable new capabilities for the future growth of your business.

For more information about Windows Server System, go to: www.microsoft.com/windowsserversystem

## Software and Services

- Microsoft Windows Server System
  - Microsoft Windows Server 2003 Standard Edition
- Services
  - Microsoft Services Essential Support
- Technologies
  - Active Directory

## Hardware

- Cisco Systems Catalyst 3550 Multilayer Switch



Document published June 2005