



THE COMPUTERWORLD HONORS PROGRAM

CASE STUDY

LOCATION:
*Pittsburgh, Pennsylvania,
United States*

YEAR:
2006

STATUS:
Laureate

CATEGORY:
Education and Academia

NOMINATING COMPANY:
Novell Incorporated

ORGANIZATION:

University of Pittsburgh

PROJECT NAME:

Secure Network Access

Summary

Providing secure remote access to network-based resources is a critical consideration for the University of Pittsburgh. Providers of subscription-based resources such as online library journals still depend on legacy IP address-based licensing schemes that make access to these resources difficult for students and faculty working from home or traveling. In addition, network firewalls have been implemented at key points in the University's network infrastructure to protect critical systems. VPN client solutions are effective in providing access to resources behind firewalls, but the software is difficult to configure and causes user frustration. The University required a solution that provides the needed level of security while avoiding user frustration. The University's Secure Network Access solution, with an enterprise VPN gateway solution at its core, achieves the balance needed in providing the level of worldwide access to systems and services critical to a world-class institution without risk to IT security requirements.

Introductory Overview

Higher education has evolved over the past ten years from being a series of scheduled lectures in classrooms and lecture halls to a dynamic series of interactions between faculty and students. Increasingly, classes are conducted entirely online serving students spread over wide geographic areas. Library research has increasingly changed from poring over stacks of dusty books to electronically searching thousands of digital books, journals, and other materials. Students and faculty use personal computers in homes, offices, residence halls, and locations across the globe. Remote connections are becoming the rule rather than the exception as people increasingly connect to academic and business systems from home and while traveling.

It was once possible to restrict access to resources based on a geographically assigned IP address with the connection being made from an on-campus network port or dialup modem pool. However, faculty, students, and even University staff are now connecting from third party Internet service providers who assign addresses from entirely different ranges. Ironically, third party providers of online journals and other electronic resources have been slow to move to other means of controlling authorized access to these resources other than using a defined range of allowable IP addresses.



THE COMPUTERWORLD HONORS PROGRAM

CASE STUDY

ORGANIZATION:
University of Pittsburgh

PROJECT NAME:
Secure Network Access

LOCATION:
*Pittsburgh, Pennsylvania,
United States*

YEAR:
2006

STATUS:
Laureate

CATEGORY:
Education and Academia

NOMINATING COMPANY:
Novell Incorporated

The University of Pittsburgh has implemented a variety of technological solutions to address these challenges. First and foremost, the central information technology unit, Computing Services and Systems Development (CSSD), eliminated IP range-based restrictions to enterprise applications and services in favor of using LDAP authentication. Users authenticate to these resources from any network with no more than the username and password assigned to them by CSSD. Efforts to encourage third party providers to make use of CSSD's LDAP authentication resources have largely been unsuccessful and other means of resolving the problem were needed.

In 1999, CSSD contracted with a third party ISP to provide subscription-based dialup and DSL services to its users. The critical component of this service is that University subscribers were provided with access to a virtual private network (VPN). When authenticated over the VPN, the user was assigned a University IP address and was able to access the needed resources. The problem with this approach is that the service was useful only within certain geographic limits and was difficult to use.

In 2004, CSSD implemented a Web-based Secure Sockets Layer VPN (SSL VPN) service. This service is based on the Juniper Networks SSL VPN appliance. Rather than require a VPN client program, users authenticate to the SSL VPN service with their University username and password. Once authenticated, they are assigned a University IP address and have unrestricted access to online library resources. The solution proved to be an immediate success because it can be used at any time, from any location, without installing or configuring any software. An additional advantage of the solution is that it is highly flexible and can be used to provide secure access to resources protected by firewalls.

The Secure Network Access solution is integrated with the University's Central Directory Service (CDS) authentication architecture. This system allows for centralized identity management and integration with other applications and services. The CDS architecture, which leverages Novell's directory technology extensively, uses LDAP and allows for tight integration with the SSL VPN service.

A key element of the project is the implementation of host checking features.

The service creates the need for authentication of users with valid access to the network and screens for proper anti-virus protection. This prevents machines that are compromised or infected with a virus from accessing University network services and therefore minimizes the potential impact on other machines on the University network. Host checking also prompts users to keep their machines updated with the latest security patches and virus definitions each time they connect to the system. A considerable benefit of the system is that it can be used by students, faculty, and staff with Windows, Macintosh, and Linux operating systems.

Benefits

The replacement of client-based systems with SSL VPN provides simple, yet secure access to applications behind firewalls. The ability to perform "client-side" integrity checks creates a more secure environment because it enforces compliance with the University's patch management and anti-virus initiatives.

The original system supported up to 2,500 concurrent users. The new system currently supports 5,000 concurrent users and plans are in place to increase the capacity to 10,000. The Secure Network Access architecture was developed using a scalable approach that will allow the Uni-



THE COMPUTERWORLD HONORS PROGRAM

CASE STUDY

ORGANIZATION:
University of Pittsburgh

PROJECT NAME:
Secure Network Access

LOCATION:
*Pittsburgh, Pennsylvania,
United States*

YEAR:
2006

STATUS:
Laureate

CATEGORY:
Education and Academia

NOMINATING COMPANY:
Novell Incorporated

versity to add capacity in incremental upgrades without re-engineering the system. This service will also support new tools such as conferencing and the ability to check the user's computer for specific software and operating system versions before granting access to the network.

The Secure Network Access service has fundamentally changed the way the University community remotely accesses information resources. The system provides flexibility for access to University systems at any time from any location and eliminates the frustration involved with installing and configuring client VPN software.

The Importance of Technology

The primary considerations in implementing SSL VPN gateway technology were ease of use and security. Client applications were completely eliminated in favor of permitting users to connect to the service using any current Web browser. The system makes it possible to provide this functionality with no compromise to overall network security. The state of the technology allows CSSD to provide access to specific applications and services to specific groups of users at a very granular level rather than simply creating a wide open door to the network.

The system in place would have been impossible to develop without the Central Directory Service. Developed by the University in 2000, CDS is the central authoritative source for information on the identity and roles of every user affiliated with the University. This directory permitted the implementation of a central LDAP directory for user authentication. The Secure Network Service relies on LDAP for user authentication and authorization to access specific services.

The system was designed to be highly available through the implementation of redundancy and integration with the monitoring, troubleshooting, and fault resolution capabilities of the University's 24-hour Network Operations Center.

Originality

Most institutions have resolved the problem of granting off-campus users access to IP-restricted library resources through the use of proxy servers. Users connect remotely to the proxy server and are then connected to the desired resources. Most proxy servers do not require user authentication and actually defeat the access restrictions that the third party content providers have put in place. In addition, these proxy servers could be used to launch anonymous attacks on other computer systems, both at the host institution and elsewhere.

Success

The project has exceeded its original goals of providing "web-enabled" access to University Library System resources and has become the preferred method of remote access. The system currently provides access to hundreds of concurrent users who require access from remote locations. Users have embraced the ease of use and simple interface, and demand from users continues to grow. CSSD continues to invest in the development of the service and has engaged in upgrades to improve reliability and availability by implementing redundant gateways and network connections. Users benefit by having customized menus and options that allow for the highest level of control and access. The service will be extended over time to replace traditional dial-up and



THE COMPUTERWORLD HONORS PROGRAM

CASE STUDY

ORGANIZATION:
University of Pittsburgh

PROJECT NAME:
Secure Network Access

LOCATION:
*Pittsburgh, Pennsylvania,
United States*

YEAR:
2006

STATUS:
Laureate

CATEGORY:
Education and Academia

NOMINATING COMPANY:
Novell Incorporated

vendor access methodologies.

The initial service had the capacity for 2,500 concurrent users. Over the past year, utilization has approached this limit and a capacity increase to 5,000 concurrent users was needed. Future plans call for a further capacity increase to 10,000 users. Concurrent usage is a significant indicator of adoption rate within the University community: if users do not like a system they will find an alternative solution. Additional evidence from focus groups, advisory committees, and other sources of feedback indicate that service has been very well received.

Difficulty

The most important obstacles to overcome were the development of host integrity and security compliance checking for remote user computers. A standard policy had to be developed and adopted by the CSSD Information Security team. The SSL VPN technology needed to be customized to check for University standard virus checking. By implementing host-integrity checking, users are required to have the latest updates to the software and can not gain full access rights until they pass the check. Communications and user guides had to be developed to inform users and ensure they knew how to get the latest software updates to pass the integrity check.