

# STRATEGIC NETWORK SECURITY ARCHITECTURE

## 2005 COMPUTERWORLD HONORS CASE STUDY

### EDUCATION & ACADEMIA

A NETWORK-BASED FIREWALL SOLUTION IS DESIGNED AND STRATEGICALLY DEPLOYED TO PROTECT MISSION-CRITICAL APPLICATIONS AND SERVICES WHILE SUSTAINING THE OPEN NETWORK ENVIRONMENT ON WHICH TEACHING AND RESEARCH HEAVILY DEPEND. [20055368]



### SUMMARY

The University of Pittsburgh has implemented a network-based firewall solution that is designed and strategically deployed to protect mission-critical applications and services while sustaining the open network environment on which teaching and research heavily depend.

### APPLICATION

The University of Pittsburgh, one of the nation's top public universities and regarded as one of the world's leading research institutions, supports flourishing academic programs spanning an astonishingly diverse number of disciplines including groundbreaking research, community collaborations, and global educational initiatives. The University's students, faculty, and staff along with visiting scholars and researchers from over 100 countries depend upon the University's world-class network "PittNet" for their daily teaching and learning, research, and business activity.

At the heart of PittNet is a multi-switch gigabit network backbone that joins hundreds of local Ethernets into a large, geographically-distributed network supporting over 100,000 networked devices and more than 60,000 users. These devices include file servers and workstations, along with laboratory data acquisition tools, critical computer-based medical equipment, and facility control systems. PittNet also provides access to networked University resources through a variety of connections, including the Internet, wide area network links to collaborating institutions including the University of Pittsburgh Medical Center (UPMC) and the Pittsburgh Supercomputing Center (PSC), and research networks including the Internet2 Abilene network and National LambdaRail.

#### Threats and Risks Facing the University's Network

Because of the large number of connections to external networks — especially the Internet — and because of the numerous ways users can access PittNet, including direct network connections through PittNet or the Internet, as well as 802.x wireless and remote dial-up, the University found itself highly susceptible to a wide range of security threats from numerous points of origin. Malware in the form of viruses, Trojan horses and worms along with deliberate denial of service attacks disrupted University network services. Daily scans of University systems for system vulnerabilities via the open Internet gateways registered in the thousands. The number of University systems successfully compromised by hackers also raised concerns about the availability and integrity of sensitive information including student and employee records, patient information, and customer information as defined by federal regulations such as the Gramm-Leach-Bliley (GLB) Act and the Health Insurance Portability and Accountability Act (HIPAA).

While the introduction of traditional centralized security controls such as firewalls and network ingress filtering could alleviate most security risks, the University found itself unable to take full advantage of these types of solutions. Any controls limiting the ability of faculty and students to openly share information internally or with colleagues at other institutions would significantly impair activity that is the lifeblood of the University. For example, it was determined that controls used to protect research data on web servers would inevitably hinder shared access to this information via web browser. With literally hundreds of separate departments and administrative units, the potential task of balancing access controls and management requirements at an acceptable level for all of these groups would prove time-consuming, complex, costly, and inevitably unfeasible for the university.

Traditional centralized security based on current technology controls also posed the problem of technology performance limitations. With over 60,000 active users on PittNet and with the Internet gateways supporting streams of up to a terabyte of packets daily, most centralized security approaches such as a standard two-tier bastion host firewall architecture for the Internet Gateway would not have the capacity to deal with these massive amounts of data without having a significant adverse impact on network performance.

Robert Carrigan,  
Chairman of the Chairmen's Committee

Ron Milton,  
Vice-Chairman of the Chairmen's  
Committee

Dan Morrow,  
Chief Historian

## The University's Strategic Network Security Architecture

In 2004, Computing Services and Systems Development (CSSD), the University's central information technology unit, developed and presented to the University community a network security architecture strategy addressing security risks while protecting open collaboration and information sharing where appropriate.

At the heart of the strategy was the introduction of a "Zones of Trust" approach for PittNet. Because of the diversity of data types and applications used by various University groups, such as faculty, researchers, and administrators, it made sense to virtually divide the network into separate zones, from which we can then ascertain the appropriate amount of control and protection needed. For example, network segments supporting student residence halls, faculty research programs, and administrative services such as e-commerce transactions or access to online tuition bills and payments, all need various types and degrees of protection.

In order to implement the Zones of Trust architecture, CSSD has deployed 36 Lucent VPN Firewall Brick® firewall appliances to provide security controls that include:

- Network firewall filtering and monitoring services
- Secure VPN network access for remote external users into a zone
- VPN IPSec tunneling between defined zones
- Monitoring and logging of each zone's inbound network activity

Each firewall appliance has been configured after an assessment of the particular zone's requirements for access as well as security, following a needs assessment process developed by CSSD. For example, one zone of trust has been established for network connections between the University's School of Medicine and UPMC. Medical researchers now have secure access from their workstations, protected behind a Lucent VPN Firewall Brick® 1100 appliance, to UPMC applications and medical databases via a dedicated VPN tunnel from the firewall. This configuration allows medical researchers unrestricted access to patient information resources critical to their research initiatives while protecting the integrity and confidentiality of the data and allows both institutions to be fully compliant with the privacy provisions of the Health Information Portability and Accountability Act (HIPAA) of 2000.

Supporting thirty-six individual firewall appliances and VPN tunnels into and among them could have proven cost- and time-consuming for CSSD to manage, especially as firewall rule sets need to be changed quickly to both accommodate new access privileges needed by the University community and to respond to new network-based security threats. The University needed a solution that proved to be scalable, cost-effective and able to facilitate administration of firewalls throughout PittNet's large, multi-site network environment.

The solution proposed to address the University's security management concerns was the Lucent Security Management Server (LSMS). It was implemented as part of the network security architecture strategy. Its features include:

- Security policies that can be established centrally and automatically downloaded to any firewall appliance on PittNet.
- Role-based administration, distributing management across local and remote administrators.
- Flexible, group-based management model: manage a collection of devices, security policies, VPN tunnels and user authentication components as a single entity; control policies at global, user, device, interface, VLAN and IP address range levels.
- Real-time monitoring, robust logging and customized reporting.
- High-speed content security that is interoperable with third-party products to provide URL blocking and virus scanning.

## **BENEFITS**

The University realized both anticipated and unanticipated benefits from the rollout of its network security architecture. This deployment proved beneficial for a number of reasons:

- Centrally managed security controls including management consistency reduced staff time and effort to support a large number of devices and the implementation of administrative controls such as logging administrator access and activities.
- The Lucent VPN Firewall Brick supports Layer-2 bridging. In cases where organizations deploy firewalls on PC's or routers, these security devices become part of network connections or act as gateways to NAT networks, becoming visible to network monitoring tools and easily identifiable to attackers looking for network vulnerabilities. Layer-2 bridging acts as a transparent bridge between protected networks and the outside world. This transparency dramatically decreases the possibility that a firewall will be compromised by attackers.
- The VLAN policy support enabled by the firewall appliances allows the necessary segmentation by class of user. This flexibility provides the mechanism for the University to administer and manage the diverse types of users from a number of different locations.

## IMPORTANCE

- As in most large organizations, the University must insure that only authorized users are granted access to protected resources. Additionally, not all users have similar access needs; therefore, it was essential that any VPN solution have the capability of managing role-based access for a large numbers of users. The Lucent solution provided the ability to grant roles-based access for up to 7000 VPN users per device. Additionally, the Brick 1100 can also handle a full Gigabit of IPSEC traffic. That further increased the type and number of applications that the University could make accessible to remote staff users and administrators.
- The solution provided the ability to customize rule-set and firewall zones to the individual department versus attempting to find a general configuration that would support the entire university community.
- One of the real differentiating factors between firewall platforms lies in the efficiency in which communication is coordinated between the management console and the individual device and the level of security provided by the management application. It is very important that network security devices do not themselves become security liabilities. Typically the weakest point in any network-based distributed security control rests with the management console because the management console needs to be accessed by administrators from various locations whereas the security devices themselves can have traffic limited only to the management console. The University's firewall architecture is managed by LSMS deployed on a hardened Solaris 9 Operating System. Remote management is provided by the LSMS remote Navigator that is secured using 3DES encryption and SHA1 authentication.
- By using utilizing a virtual architecture, the University was able to deploy firewall protection to departments and units as an "opt-in" service. This provides the added benefit of being able to customize rule-set and firewall zones to the individual department versus attempting to find a general configuration that would support the entire university community.
- Addresses regulatory compliance, most notably HIPAA.
- Provides the ability to logically group hosts and implement those groups locally or globally.
- Does not negatively impact bandwidth or latency.
- Improves reaction time to critical events. With LSMS, when systems administrators are notified of a critical issue, they can remotely access systems over a secure connection to correct errors or troubleshoot problems.

## ORIGINALITY

The need to balance network security with open access to information among faculty with colleagues scattered across the globe calls for a "soft on the outside, hard on the inside" approach to perimeter security. The University of Pittsburgh has met the challenge of ensuring open network access for research and teaching while securing critical applications by effectively implementing an original "zones of trust" approach within its network, made possible through the distributed use of 36 firewall appliances and centralized management and monitoring using LSMS. In addition to preserving the open nature of the academic computing environment, the University's zones of trust provides needed security for critical financial records, student data, and research as well as medical information. This model also provides adequate security support for nontraditional network devices including medical equipment and data acquisition devices.

The strategy employed by the University is also original in that enterprise firewall management has been implemented as a central service to those units that either are required by law to have or desire firewall protection. The University was able to effectively leverage the firewall and firewall administrative server technologies provided by Lucent to enable the zones of trust architecture while not becoming mired in the process of separately configuring and managing 36 individual firewall appliances.

## SUCCESS

The number of security incidents involving compromised computers has dramatically decreased in those University units where firewalls have been implemented. For example, 288 compromises were reported within a single major graduate school during the second half of 2003. By comparison, in 2004 following the implementation of a firewall serving this school specifically, the number of incidents dropped to 55, a decrease of 81 percent. The incidents that were reported in 2004 were all attributed to the opening of e-mail virus attachments and connecting already-infected computers to the network behind the firewall.

The overall success of the strategy within the University is similar to that experienced within the example above. Where firewalls have been implemented, the number of security incidents has decreased substantially. In combination with user awareness strategies, anti-virus software distribution

initiatives, and the implementation of effective security policies and procedures within the University's units, it is clear that the zones-of-trust firewall implementation model represents a highly-effective solution.

The firewall strategy has also led to CSSD's ability to negotiate agreements with the University's affiliated hospital system to allow continuing access to protected health information. University medical school faculty serve as physician providers within the health system. Physician and non-physician faculty members and certain staff employees interact to a high degree with the health system's medical information databases. HIPAA regulations required the hospital system to maintain a highly secure environment that might severely limit the ability of research faculty or physicians served by the University's network to access critically-needed hospital system resources. The University's firewall strategy has made possible the implementation of LAN-to-LAN VPN and other secure VPN solutions that protected access to these critical resources.

## **DIFFICULTY**

The deployment of centrally-managed firewall appliances and the implementation of the zones-of-trust model for firewall security have been relatively easy. The primary difficulty facing the University, as with any other large educational institution, involves user provisioning and awareness. The volume of electronic collaboration among research faculty and graduate students presents unique challenges for the design of firewall rule sets to serve the needs of these units.

While deploying the Lucent VPN Firewall Brick appliances and the LSMS management console are relatively easy, the main challenge surrounding this project is related to user provisioning and awareness.

Most of the University's researchers and academic units share information with the University and with partners globally. Because of this, each University unit has its own unique configuration challenges and internal provisioning procedures that had to be incorporated into each firewall deployment. Although the LSMS management console eases this challenge, the number of disparate systems and units has made initial provisioning and change control a rather large undertaking.

The "Zones of Trust" approach, facilitated by the use of the sophisticated filtering and management capabilities of Lucent VPN Firewall Bricks, also allows the University to take advantage of new communication tools without the firewalls hindering their use. This includes:

- Instant messaging
- Peer to peer (P2P) software
- Network applications that utilize non-standard ports

The flexibility of supporting these types of tools while still providing network security controls allows the University community to take advantage of these tools to communicate over the Internet with students, researchers and academics worldwide.