Thomas S. Adeimy
Dr. Lunsford
DTEC6823
November 29th, 2005

Firewall Technologies and Securing a Network Classroom Lab

The transition from industry into academia meant not having total access to computer hardware and software resources. I was going to teach computer and networking courses, and could not wait to use my real life industry experiences as learning tools in a classroom/lab setting. It wasn't long until my newfound enthusiasm began to be tested. I was an instructor, not a member of the campus IT staff. All the campus labs were general purpose computer labs. Computer desktops were "locked down" by group policies, Internet access was restricted by "Cyber Patrol" controls, BIOS settings were password protected. Access to the "Server Room" was protected by a keypad, and of course I was not given the password. These were just some of the things that began to make my life miserable as a computer instructor. It became very clear that a dedicated networking lab was needed. What followed was a long and hard fought battle to convince those in charge of the purse strings that this was an endeavor worth pursuing.

A "sales pitch" was made to the planning committee along with our Division/Department chairs to secure funds for this project. The table below shows the proposed equipment budget:

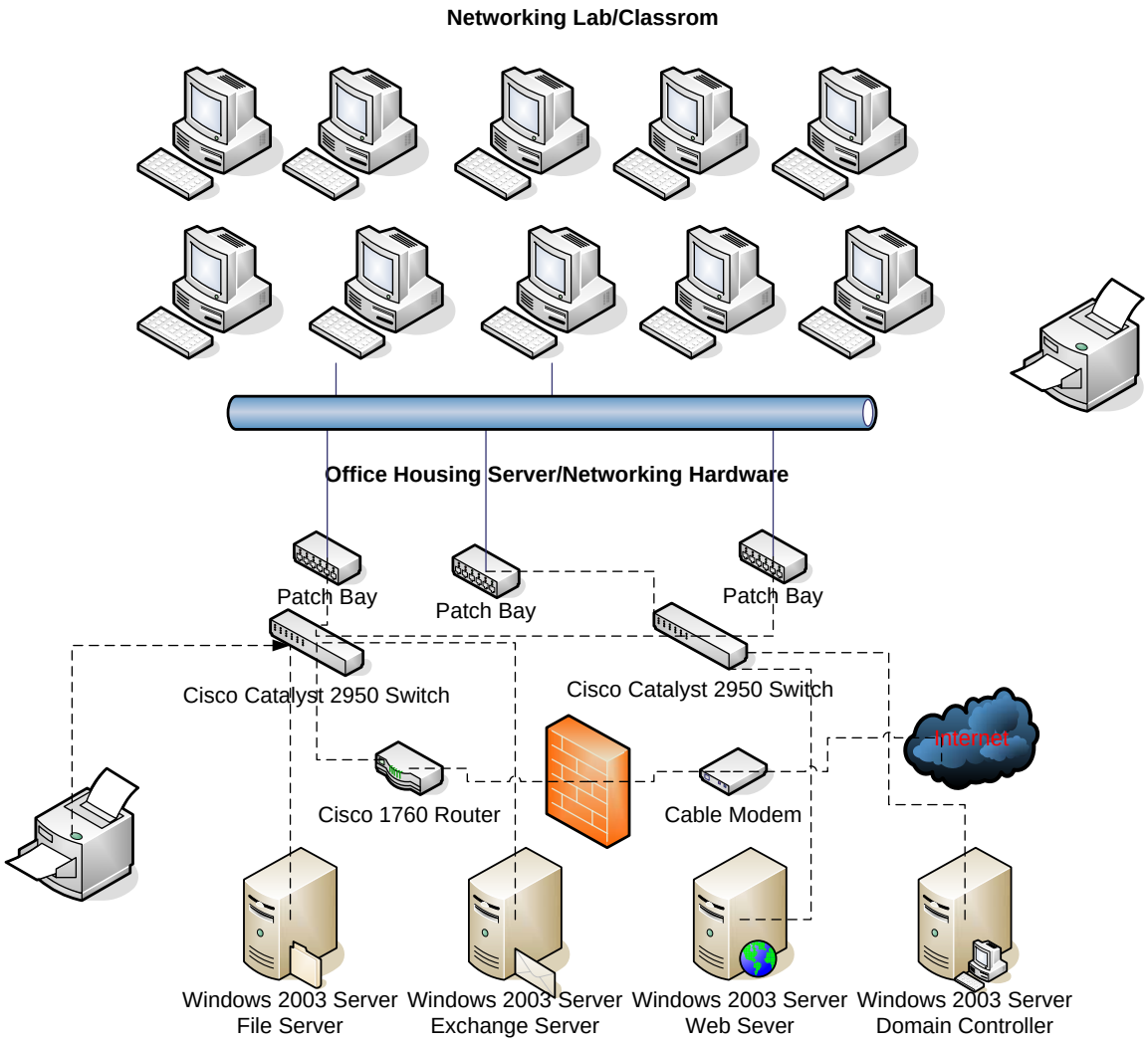
Equipment Proposal			
Qty	Item	Cost	Total
1	Cisco 1760 Access Router	$1,247	$ 1,247
2	Cisco 2950 24-Port Switch	$ 497	$ 994
4	Dell Poweredge 2650 Server	$3,740	$14,960
1	Dell 8-Port KVM Switch	$ 629	$ 629
1	Dell Server Rack & Hardware	$ 650	$650
1	APC Smart-UPS 3000VA Rack Mount 3U XL	$1,289	$ 1,289 Total: $19,769

It should also be mentioned that the networking lab would also need its own Internet connection, and a broadband cable modem supplied by Time Warner Cable would cost approximately $99 per month.

The next problem was getting a classroom that would be dedicated as networking lab only. Cause and effect became obvious, as our dedicated lab would mean that other classes would no longer be able to utilize this classroom, and those that labored over the scheduling process were not enthusiastic supporters. Because one of the Information Systems offices was located beside Classroom 18 in the Lee Building, it was the proposed choice. Our Office would house the server hardware and networking equipment, and the classroom would house the lab. The proposal was approved, now we had to put it all together and make it operational and secure.

Housing the Server/Network hardware in our office meant having a dedicated electrical circuit/breaker installed by the campus physical plant. The cabling labor was assigned as a project to the Network Support class students.

Category 5 cables were run from the networking lab classroom through the ceiling to the adjoining office housing the network equipment. The lab is approximately 780 square feet, and already has 24 Dell E series PCs and one HPLaserJet 4000 printer with an HPJetDirect card provided by the College IT department. See the figure below.



Network Design

The twenty four lab workstations will have Windows XP Pro SP2 operating systems, and Microsoft Office XP application software. Each PC is a Dell E Series computer, with the following configuration:

Manufacturer	Gateway
Model	E Series
CPU	Intel 2.4GHz
RAM	256MB
Hard Drive Space	40GB

Each of the four servers has SCSI hard drives. The domain controller has 5 drives, the web server 2 drives, the exchange server 3 drives, and the file server also has 2 drives. Each has the following configuration:

Manufacturer	Dell
Model	PowerEdge 2650
CPU	(2) Intel 2.8GHz
RAM	1GB
Hard Drive Space	140GB

The servers will have Microsoft 2003 Server Standard edition operating systems. One server will act as Domain Controller, another will function as a web server, another as a file server, and another will have Microsoft Exchange installed, and will be used as an email server. How will we protect our new lab and server room?

Physical security protects your organization's physical computer facilities. It includes access to the building, to the computer room(s), to the computers (mainframe, mini, and micros), to the magnetic media, and to other media *(Handbook of Information Security Management).* The lab will be behind a locked

door. Only Instructors who will be teaching classes in the lab will have keys. The door shall be locked at all times, and students will never be left in the lab without instructor supervision.

The Network hardware in the adjacent instructor's office will also be behind locked doors. There will be only three instructors with access to this room, and they will be required to never leave the office unlocked, unless there is another instructor present. We hope that this will be a step toward insuring that the assets in both areas will be reasonably safe from theft or misuse.

The workstations should be kept updated with the latest security patches and service packs. There are two ways to accomplish this goal: Configure each computer to download and install its own updates, or configure a Software Update Services (SUS) server to download the updates, and then have the workstations download the updates from the SUS server. If our lab was larger or we were using multiple classrooms, then using a SUS server would make sense. The SUS server would be the only computer utilizing network bandwidth to download updates. However, since our lab is relatively small (24 computers), and we will have our own Internet connection, each computer will be configured to automatically download and install updates on a daily schedule during non-peak hours.

The lab computers need to be protected from misuse, whether accidental or intentional. Since this will be a networking lab, there will be experimentation and configuration changes to both software and hardware. We need the ability to

restore the computers to their original operational state with a minimum of downtime and inconvenience (to both students and instructors/network administrators). To be able to make these kinds of changes, there are times when students will need administrative privileges to the local computers and the Domain. To allow them local administrator privileges, but to provide fault tolerance/disaster recovery in the case of accidents or mischief, the first lab computer will be setup and configured for lab use. An image will be made from this properly configured computer, and the other lab computers will be installed from this image. In the event of a problem, we will be able to easily restore the affected computer from this image.

To address the problem of giving administrative privileges to students on the domain, we will install and use removable hard drives. A student taking a course needing a server operating system will be able to install his own version, create his own domain, and have administrative privileges.

Each lab computer has anti-virus protection. The above mentioned steps should give us protection against internal risks and threats. Next we must consider fault tolerance and disaster recovery on the server/network side.

Since we have a total of twelve SCSII hard drives, it was decided to implement some sort of RAID for fault tolerance/redundancy. The benefits of RAID are:

Reliability

- Provides real-time data recovery with uninterrupted access when a hard drive fails
- Increases system uptime and network availability
- Protects against data loss

Performance

- Multiple drives working in parallel increase system performance *(Adaptec: "Let's Talk About RAID").*

RAID Level 10 was chosen, which is a combination of RAID Level 0 (disk striping) and RAID Level 1 (disk mirroring). There will be no mission critical file storage on any of these servers, so we decided not to implement a back-up strategy. In the event of a hard drive failure, spare disk drives will be purchased to replace the faulty drive.

The lab will have its own connection to the Internet, separate from the school network. Students will need access to the Internet for many reasons; experimenting with Web hosting, Remote Access, VPNs, FTP, Internet Printing, Support and Knowledge Base articles for trouble shooting, and downloading device drivers, among other things. Networking lab users will need access to external information and Internet services as well as the network's own private information (website, file storage, etc.). How will we allow our lab to connect to

the Internet, while maintaining the safety and security of information and network resources?

A firewall provides a single point of defense between two networks-it protects one network from the other (*Evolution of the Firewall Industry*). A relatively new technology, firewalls have evolved over the past twenty years into four generations of architectures.

Packet filter firewalls are first-generation firewall technology, appearing around 1985, and have been around almost as long as routers. Network traffic is analyzed at the transport protocol layer. Each IP network packet is examined to see whether it matches one of a set of defined rules. The rules identify whether the transfer of data is prohibited or allowed using controls such as:
The physical network interface on which the packet arrives, the source IP address, the destination IP address, the transport layer type (TCP, UDP, and ICMP), the transport layer source port, and the transport layer destination port.

If a network packet is “allowed”, it can be routed to its proper destination. If it is “denied”, then it will not. Packet filters usually apply command sets to check whether there is a rule to permit or deny specific port and protocol combinations. Implemented in the network layer, packet filters are not able to process state information in high-level protocols, such as FTP. However, using a

packet filter that includes higher-level protocol port filtering capabilities, you can permit certain types of connections to be made to specific computers, prevent other types of connections to those computers, and also permit or prevent similar connections to other computers.

Packet filtering firewalls are the least secure of the firewall technologies, because they do not inspect the network's application layer data or track the state of connections. Access is allowed through the firewall with minimal inspection. If a network packet passes this inspection, it is allowed to be routed through the firewall based on the rules defined in its routing table. However, this minimal inspection of network data makes it the fastest firewall technology available and is often found in hardware solutions, such as IP routers.

Circuit level firewalls are the second-generation of firewall technology. They are used to confirm that a packet is either a connection request, a data packet belonging to a connection, or a virtual circuit between two peer transport layers. Checking the information in each network packet, it is determined whether the transmitting computer has permission to send data to the receiving computer and whether the receiving computer has permission to receive the data. They can only detect one transport layer protocol, TCP. Like packet filters, they have a limited understanding of the protocols used in network packets. Only network packets that are associated with an existing connection are allowed through the firewall.

Established rules are checked to determine whether that connection should be allowed, and if it is, all packets associated with that connection are routed through the firewall as determined by the firewall's routing table. There are no other security checks. Thus, circuit level firewalls are very fast and provide limited amounts of state checking. In addition, this type of firewall can be used to detect IP spoofing and limited forms of packet data modification.

Application layer firewalls are the third-generation of firewall technology. Network packets are evaluated at the application layer for validity before a connection is allowed. All packets are examined at this layer and connection state and sequencing information are maintained. This type of firewall can also validate other security items that appear within application layer data, such as user passwords and service requests. Application layer firewalls can also provide proxy services, which are programs that manage traffic through a firewall for specific services, such as HTTP or FTP. Users communicate with the proxy server instead of the actual service, and the proxy either accepts or denies the connection based on the set of rules defined for that particular network service. The network is protected by the proxy by never allowing direct connections, and all network packets are inspected and filtered for accuracy. To the user this service is transparent. The user perceives that they are dealing with the real service, and the real service perceives it is dealing directly with a user on the proxy server. Proxy

services shield internal IP addresses from external networks. Since proxy services are placed on top of the firewall host's network stack and operate in the application layer only, each packet must pass through lower level protocols before being passed to the application layer. Once inspected, the packets must travel back down the stack for distribution. This means that proxy services are slow.

Dynamic packet filter firewalls are the fourth generation of firewall technology. The security rules are allowed to be modified on the fly. To do its job, all UDP packets that cross the security perimeter are related with a virtual connection. If a response packet is generated and sent back to its originator, then a virtual connection is established allowing the packet to pass through the firewall. Information associated with a virtual connection is remembered for a short period of time, and then invalidated if no response packet is received during this time period. One of its big advantages over first-generation packet filter firewalls is not allowing unwanted UDP packets onto an internal network. Response packets from external networks must contain a matching destination address, matching transport layer destination port, and the same transport layer protocol type as the request originated from the internal host. As a result, application layer protocols, such as Domain Naming System (DNS) can be allowed to operate across the security perimeter. An internal DNS server can make requests to other DNS

servers on the Internet to retrieve address information for unknown hosts using a TCP connection or UDP virtual connection.

Packet filter firewalls can be used to readdress network packets so that outgoing traffic appears to have originated from a different host rather than an internal host. Network Address Translation allows a single device, such as a router, to act as an agent between the Internet and a private network. This means that only a single, unique IP address is required to represent an entire group of computers. The topology and addressing schemes of trusted networks are hidden from untrusted networks. Circuit level firewalls are often configured to readdress network packets to cause outgoing traffic to appear to have originated from the firewall instead of the internal host. Since they maintain information about each session, they can route external responses back to the appropriate internal host. Application layer firewalls can also perform network address translation.

When evaluating firewall technology alternatives, it is usually a comparison between performance and security. Generally, packet filter firewalls provide the highest performance, followed by circuit level firewalls, dynamic packet filter firewalls, and application layer firewalls. The security aspect usually follows the reverse order because as packets pass through more protocol layers, they are inspected more thoroughly. Thus application layer firewalls are considered more secure than dynamic packet filter firewalls, followed by circuit

level firewalls, then packet filter firewalls. Application layer firewalls are generally considered to be the most protective firewall technology.

The firewall chosen to protect our networking lab is the Cisco IOS Firewall, implemented on the Cisco 1760 Modular Router. It will allow us to use a single device as the security and routing solution for our network, providing secure, per-application access control across network perimeters. It is a stateful inspection firewall option for Cisco routers. Each time a TCP connection is established from an inside host accessing the Internet through the firewall, the information about the connection is logged in a stateful session flow table. The table contains the source and destination addresses, port numbers, TCP sequencing information, and additional flags for each TCP connection associated with that particular host. This information creates a connection object in the PIX Firewall. Inbound packets are compared against session flows in the connection table and are permitted through the firewall only if an appropriate connection exists to authenticate their passage. This connection object is temporarily set up until the connection has been terminated. The Cisco IOS Firewall adds inspection intelligence to ACL capabilities. The Cisco IOS Security Firewall integrates firewall functions and intrusion detection and prevention. As an add-on feature to the existing Cisco IOS Software, the existing router has security-specific features such as: application-based filtering, dynamic per-user authentication and

authorization, URL filtering, and more. When combined with other technologies, the firewall can provide an integrated VPN solution. This choice allows the ability to configure the Cisco router as a firewall. The network benefits from advanced security features without the additional cost of purchasing another network appliance. Some of the many features available are; dynamic packet filtering, advanced application inspection and control, authentication proxy, DoS detection and prevention, dynamic port mapping, and network address translation.

The 1760 router has SDM (Security Device Manager) imbedded Web-based management tool. The graphical user interface allows the novice to use smart wizards to deploy and manage the router with limited knowledge of the Cisco IOS software. Cisco SDM offers smart wizards and advanced configuration support for LAN and WAN interfaces, NAT, stateful firewall, and IPSec VPN features *(Cisco, Inc. NAT White Paper)*. Wizards are divided into basic and advanced. The basic firewall wizards implement pre-built configuration templates on user selected interfaces, requiring minimal user input. The advanced firewall wizard allows users to customize firewall inspection rules and create DMZs. In the advanced mode, users can also tweak the Cisco IOS Firewall configurations through the ACL and inspection rule editors.

This firewall selection seems to be the right choice for our particular situation. The existing router was upgraded at a minimal cost, the features allow

us to begin with a basic configuration, but allow for expanded services and growth with minimal cost. The router and firewall is being used by the Cisco Academy instructors and classrooms, so technical support is never far away.

Our newfound freedom has come with new challenges and responsibilities. As the old saying goes, “be careful what you wish for”. The instructor has become a DST, Network Technician, System Administrator, and Information Security Manager. But it is worth the extra burden to insure that students receive the benefits of hands-on, real-world experiences. Hopefully this endeavor will provide a learning environment that can be resilient towards the risks and threats it will face.

References

Adaptec: Let's Talk About RAID. **Adaptec, Inc.** Retrieved November 2, 2005, from http://www.adaptec.com/worldwide/product/markeditorial.html?cat=%2fTechnology%2fRAID+Controllers&prodkey=talk_about_raid&sess=no&language=English+US

Adaptec RAID 10 and its Alternatives. **Adaptec, Inc. 2002.** http://graphics.adaptec.com/pdfs/raid_10_and_alternatives.pdf#search='RAID%2010%20AND%20adaptec'

Ainsworth, Jerry K., and Kristine A. Kriegel. *System Administration, "Preparing for Network+ Certification"*. St. Paul: Paradigm Publishing, 2004.

Caudle, Kelly, and Kelly Cannon. *CCNA Guide to Cisco Networking, Third Edition*. Canada: Course Technology, 2004.

Cert Coordination Center. *Deploying Firewalls.* **Carnegie Mellon University, 2001.** http://www.cert.org/security-improvement/modules/m08.html

Cisco IOS Firewall. **Cisco Systems, Inc.** Retrieved November 2, 2005, from http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_white_paper0900aecd8029d0a6.shtml

Cisco's PIX Firewall and Stateful Firewall Security. White Paper. **Cisco Systems, Inc. 2000.** http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/tech/nat_wp.htm

Evolution of the Firewall Industry. **Cisco Systems, Inc. 2002.** http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm

Forouzan, Behrouz A. *Local Area Networks*. Boston: McGraw-Hill, 2003.

Frederick Avolio. *Firewalls and Internet Security.* **The Internet Protocol Journal. Cisco System, Inc.** Retrieved November 2, 2005 from http://www.cisco.com/en/US/about/ac123/ac147/ac174/ac200/about_cisco_ipj_archive_article09186a00800c85ae.html

Kurose, James F., and Keith W. Ross. *Computer Networking "A Top-Down Approach Featuring the Internet"*. Boston: Addison-Wesley, 2001.

Lief Akesson. *Security Beyond Firewalls.* **Intranet Journal, 2002.** http://www.intranetjournal.com/articles/200003/se_03_29_00a.html

Microsoft Small Business Security Center. "Small Business Security Computer Check List". **Microsoft Corporation, 2005.** http://www.microsoft.com/smallbusiness/support/checklist/default.mspx

Subramanian, Mani. *Network Management, Principles and Practice"*. Boston: Addison-Wesley, 2000.

Whitman, Michael E., and Herbert J. Mattord, *Management of Information Security*. Canada: Course Technology, 2004.

Zacker, Craig. Managing and Maintaining a Microsoft Windows Server 2003 Environment. Redmond: Microsoft Press, 2004.