

Firewall Advanced Technology Project

Final Report

Background

The constant threat of hackers breaking into UC Davis networks and computer systems has caused many campus units to consider new security practices and tools. One information security tool that is widely used by many organizations is a network firewall. A network firewall is a device that inspects and controls traffic between different networks. Several campus units are considering the use of network firewalls as part of their information security program. The possibility of increased use of network firewalls raises important questions regarding the benefits and disadvantages of using network firewalls within a Doctoral/Research-Extensive University¹. These questions tend to focus on five areas: What are network firewalls? How are network firewalls used? What are the security benefits of network firewalls? Are network firewalls applicable to all or particular campus computing environments? What are the costs to develop, install and support network firewalls?

In late March 2001, the Vice Provost, Information and Educational Technology (IET), initiated a Firewall Advanced Technology Project. Under the broad review of the Vice Provost and Communication Resources, the project team was composed of representatives from Office of the Vice Provost, IET Communication Resources, IET Information Resources, the School of Medicine, College of Letters and Science and the Human Resources Department. The overall purpose of this advanced technology project was to inform the campus community regarding network security issues and the appropriateness of firewalls in mitigating these security issues. The charge of the Firewall Advanced Technology Project was to:

- Identify the role and functions of the components of enterprise network security architecture, including network firewalls.
- Review the application of network firewalls within departmental networks and within the broader campus VLAN architecture.
- Identify the factors that impact the deployment of firewalls, such as bandwidth performance, security, reliability, management, availability, administration and cost.
- Recommend policies for use, acquisition, support and maintenance of network firewalls within department networks and within the broader campus VLAN architecture.

This report represents a summary of the findings and recommendations of the Firewall Advanced Technology Project.

UC Davis Network Overview

¹ As classified by the Carnegie Foundation for the Advancement of Teaching, <http://www.carnegiefoundation.org/Classification/index.htm>

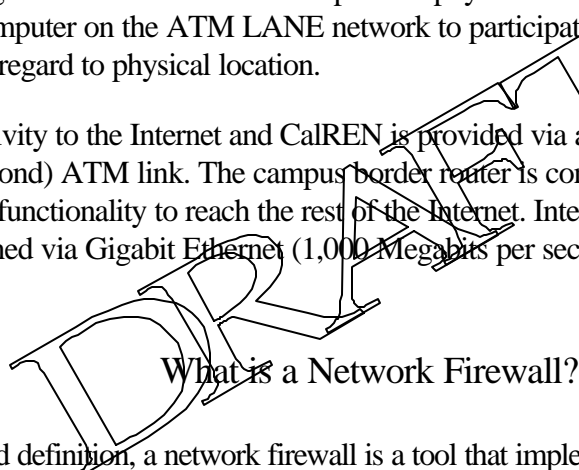
The majority of the UC Davis campus is currently connected via Asynchronous Transfer Mode (ATM) technology and local area network emulation (LANE). This implementation utilizes a high speed ATM switched network in the core, and switched Ethernet technology at the edge of the network. The network was designed to provide low latency connectivity across campus in support of the University's mission of teaching and research.

The campus is geographically divided into seven areas. Each area consists of an Area ATM switch, which connects to numerous Building ATM switches within the same area. The Building ATM switches in turn provide connectivity to multiple Edge ATM/Ethernet switches located in building floor distribution wiring closets. This design provides a tree structure, which starts from the Area ATM switch and fans out across the area to every building, floor closet, and eventually client computers. There are approximately 90 ATM core switches, and 800 ATM/Ethernet edge switches in the current network.

A radial mesh topology interconnects each of the seven areas. Area 3 serves as the hub, with connections to all other areas. The other six areas connect to Area 3 and two adjacent areas. IP routing for the network is provided by one ATM LANE connected router per area. These are commonly referred to as campus Area Routers or Area Distribution Frames.

The network was also designed to implement virtual local area network (VLAN) technology. This creates a logical network structure on top of the physical network infrastructure. VLANs allow a client computer on the ATM LANE network to participate in a departmental sub-network without regard to physical location.

External connectivity to the Internet and CalREN is provided via a high bandwidth (622 Megabits per second) ATM link. The campus border router is connected to this link and provides routing functionality to reach the rest of the Internet. Internal connectivity to the border router is maintained via Gigabit Ethernet (1,000 Megabits per second).



Using a simplified definition, a network firewall is a tool that implements security policy to control traffic between two or more networks. ² A firewall can be a special network appliance or a device that is configured using a desktop computer, operating system (e.g., Microsoft Windows 2000, Sun Solaris, OpenBSD, Linux) and a network firewall application.

The network firewall performs several security functions. Primarily, a firewall monitors, inspects and controls inbound/outbound network traffic. The firewall implements user-defined security policies to determine whether to permit or deny particular network traffic. The security policies define the characteristics of acceptable and unacceptable network traffic based on packet criteria at the IP level and above. Typically, network traffic that represents hostile intrusion attempts, denial of service attacks and/or unauthorized attempts to read, modify or delete

² Additional references discussing firewall techniques are provided in Appendix 3.

information is proactively denied by the firewall. A network firewall's capability to inspect and control network traffic also permits the firewall to logically separate a network into public and private segments as well as a semi-private segment (often referred to as a demilitarized zone –DMZ) between the public and private network areas. Secondly, a network firewall provides detailed logs describing permitted and denied network traffic. Finally, many firewalls can hide selected internal network segments from external networks by the providing network address translation services (NAT).

While the capabilities of a network firewall seem quite powerful, it should be noted that a network firewall does have functional limitations. A network firewall can't protect against hostile traffic it cannot observe or is not configured to block. For example, internal network traffic behind an external border firewall will not be inspected and controlled by the perimeter firewall. A network firewall doesn't identify and control malicious code, such as viruses. Finally, a firewall may be unable to defend against a severe distributed denial of service attack and could, under such an attack, itself become a failure point. The limitations of a network firewall need to be considered when developing an effective information security program.

Use of Network Firewalls

Network firewalls are typically used either to isolate an organization's internal network from the external Internet or to logically isolate a portion of the internal network from the organization's network at large. This former firewall type often referred to as a network perimeter or border firewall. The latter firewall use is often referred to as an internal firewall. A conservative network security architecture could employ a broad system of network firewalls, of varying design capabilities, at the external network border to the Internet and internal network locations.

Border Firewall

A border firewall separates a private network from the general Internet. The border firewall will inspect and allow only Internet traffic that has been pre-defined by security policy as permissible. In addition, the border firewall must be able to perform this inspection and logging function reliably and at a performance level equal to the network bandwidth capabilities for the Internet connection.

In a corporate environment, use of a border firewall is a generally a de facto security standard. In a higher-education setting the presence of a border firewall is not as common. UC Davis, like most other higher-education institutions, uses a computing network that serves both academic and administrative needs. In this network environment, overly restrictive security-related traffic policies can negatively impact collaborative research projects that involve participants from network locations other than UC Davis. In addition, the high-bandwidth connection between the campus and the Internet and CalREN (622 Mbps ATM and 1,000 Mbps Ethernet) pose a significant challenge to current network firewall technology. Moreover, the provision of higher-speed connectivity between research institutions is expected to exceed current firewall

technology. It is anticipated that there will be a continual leap-frog effect between external connection speed and high-speed firewall capability.

The UC Davis Medical Center (UCDMC) recently evaluated the use of a border firewall. UCDMC identified security benefits from a border firewall, but also learned that a restrictive border firewall policy can have negative effects on its research, teaching and public service mission. In addition, UCDMC identified the need for a more expensive network firewall device in order to reduce network latency.

It is reported that UC Irvine is evaluating the use of a border firewall.³ The UC Irvine border firewall security definitions currently emulate the access control list contained within their border routers. Accordingly, the UCI border firewall is not providing additional security control over the capability of the border routers. Depending on the extensiveness of the router access control lists, a properly-sized border firewall may provide network performance benefits through reduced latency over a router. However, extensive border firewall security policies will ultimately introduce network latency problems.

Internal Firewall

An internal firewall can be used to inspect and control traffic to and from internal network locations through VLANs. However, the primary purpose of VLANs is not for a security function, but rather to manage broadcast domains and to permit placement of a departmental system at nearly any physical location on campus and still be associated with a specific logical network segment.

A departmental VLAN can be used for security purposes; however, there are tradeoffs, generally in the area of additional network configuration and management costs. Having unique solutions for each department also introduces additional network management complexity. Network complexity is often correlated to information security risks. Finally, the co-location of academic and administrative traffic on a single department may limit the ability to implement aggressive security policies to restrict VLAN traffic. Similar to a border firewall, a network firewall placed on a VLAN may provide limited security benefits but impose additional acquisition, maintenance and support costs.

Some administrative departments, such as Human Resources, are planning to develop and implement department firewalls for a single administrative location. The network firewalls will be based on an OpenBSD as the border firewall and a Linux platform for the internal NAT firewall and public domain tools. In order to maintain the network security and availability for workstation and servers behind the network firewalls, Human Resources must:

- Develop department security, acceptable use and incident handling policies,
- Develop department disaster recovery plans
- Develop and maintain firewall design and configuration documentation,

³ Mike Iglesias, Network and Academic Computer Services, University of California, Irvine, April 18, 2001

- Develop and maintain firewall configuration,
- Maintain and review firewall audit logs,
- Troubleshoot firewall design, configuration and performance issues,
- Maintain firewall operating systems and related applications, and
- Ensure adequate training for the firewall administrators,
- Ensure the availability of department personnel to support production network firewalls.

In most cases the existing VLAN configuration for campus units is not designed along strict administrative functions. During a discussion with system administrators from several academic departments, the system administrators indicated their departments had insufficient resources to support network firewalls to the degree dictated by the above responsibilities. The project team understood that the available resources within academic units for designing, implementing and maintaining network firewalls will vary and, in fact, some academic departments have experienced security benefits from network firewalls to some degree.

Alternatively, the use of an internal firewall for a purely administrative unit or data center function could be implemented using VLANs and provide substantial security gains. Several representatives of Banner, DaFIS and Advancement applications indicated an interest in the application of a network firewall as an additional security measure for application and database servers resident in the campus Data Center. This interest was tempered by a concern about the resulting firewall acquisition and support costs.

Internal Firewall at the IET Data Center

In order to explore the use of network firewalls at the IET Data Center, the project team discussed firewall usage with a technical specialist from the IET Data Center. Due to the broad use of UC Davis computing resources housed within the IET Data Center and the existing Data Center VLAN configuration, it was determined unlikely that a restrictive firewall security policy, such as “deny all network traffic unless expressly permitted,” could be implemented at the Data Center. It was considered more likely that a network firewall within the IET Data Center could be more valuable as a reactive defensive tool, blocking hostile network traffic as identified by support staff. It should also be noted that the IET Data Center implements a variety of information security practices to minimize the Data Center’s vulnerabilities to common security exposures. Some of these security practices eliminate specific security vulnerabilities that are typically addressed by a network firewall.

New applications that may be housed at the IET Data Center, however, may require the Data Center to use a network firewall in the more traditional manner. For example, the campus is presently considering the establishment and support of a central credit card authorization and transaction system for Internet credit card transactions. The major credit card companies, such as Visa, require merchant organizations to employ extensive information security measures, including network firewalls to proactively restrict hostile network traffic from being directed towards servers holding sensitive cardholder authentication and transaction information. Failure

to comply with the credit card security requirements could jeopardize low academic discount rates on credit card transactions and/or result in other financial penalties.

For the purpose of this report, the project team was interested in documenting the components and general architecture of a network firewall. Accordingly, the project team requested Communication Resource's Systems Engineering and Design group to develop a firewall design that could be implemented at the IET Data Center to enhance the security for Tier-1 applications and/or a future E-credit card authorization system. This exercise was conducted to provide a sample network firewall design and estimate the costs to acquire and support the network firewall design. The firewall design was based on fulfilling four objectives:

- Consistency with a high availability architecture
- Absence of a single point of failure
- Support of moderate to high traffic levels (at least 300Mbps)
- Capability to secure security logs to secondary sources

The network diagram (See Figure 1) represents the sample network design that meets the above four firewall design objectives for a low to moderate amount of network traffic, defined to range from 120Mbps to 370 Mbps and approximately 125,000 to 250,000 simultaneous connections. In order to implement this firewall design, we estimate the acquisition costs to be about \$55,000 and annual maintenance and support costs to be about \$38,000 per year. These costs do not include any estimates for VLAN configuration changes that could be required to implement the design. It should also be noted that the sample design does raise support issues. For example, if the Data Center maintains the network firewall security policies, consideration is required to permit network infrastructure support staff to configure and maintain the internal switches that are "protected" by the firewall.

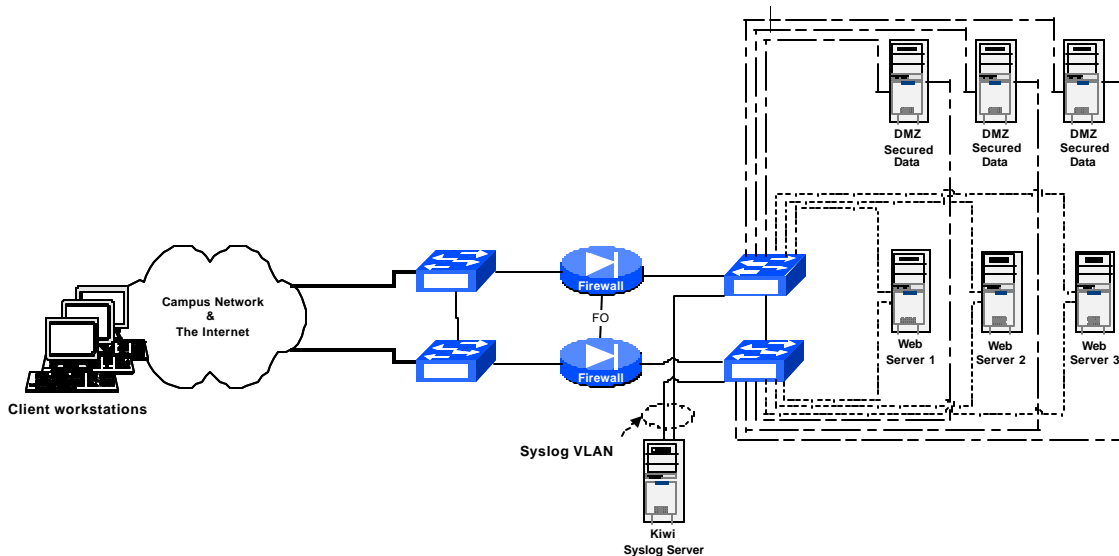


Figure 1: Sample Firewall Design for Low to Moderate Traffic Levels

DRAFT

Other Information Security Alternatives

One of the fundamental principles of information security is to use multiple and, to some degree, redundant mechanisms to provide a more secure computing environment. This approach reduces the likelihood that failure of a single information security program component does not cause a broad security failure. The workgroup members and system administrator participants (see Appendix 1) acknowledged the limited value in sole dependence on network firewalls as an information security measure. Many of the participants expressed greater interest in the development and implementation of a more diverse information security strategic plan. This strategic plan would emphasize the four major information security program components: avoidance, assurance, detection and investigation and recovery. The possible security practices and tools within such a plan is described in the following figure:

Program Components	Practices and/or Tools
<p>Avoidance: Proactive and reactive information security policies, standards, procedures, and guidelines and security awareness programs</p>	<p>Proactive Security Measures</p> <ul style="list-style-type: none"> • Network Firewall Solutions • Network Address Translation • Physical Security Standards • Strong Authentication • Role-Based/Least Privilege Authorization • Operating System and Application Maintenance • Publication of Alerts and Recommended Practices • Secured OS Distribution • Malicious Code Detection/Prevention • Security Awareness Training Program <p>Reactive Security Measures</p> <ul style="list-style-type: none"> • Host Intrusion Detection • Network Intrusion Detection and Analysis at Campus Border • Site Licenses for Security Software, SSL Server Certificates • Log Analysis Assistance
<p>Assurance: Tools and strategies to evaluate and maintain an effective information security program, such as security vulnerability assessment</p>	<ul style="list-style-type: none"> • Security Assessment Vulnerability Services • Post-Assessment Security Enhancement Assistance
<p>Detection and Investigation: The timely detection, investigation, tracking and management reporting of information security breaches.</p>	<ul style="list-style-type: none"> • Incident Response Team Function
<p>Recovery: Tools and practices to develop and implement timely recovery from information security breaches.</p>	<ul style="list-style-type: none"> • Backup Methodology • Off-site Backup Storage • Disaster Recovery Plan Development

Figure 2: Information Security Architecture Components

Findings and Recommendations

Finding 1: The campus units most likely to benefit from the use of a network firewall are those units that support administrative functions or can easily segregate administrative networks from research networks. The administrative functions are more compatible with restrictive firewall security policies. Campus units supporting both broad research goals and administrative functions generally find restrictive network firewall security policies disrupt required network communication.

Although the use of network firewalls may be more compatible with administrative applications, the decision to employ network firewalls should be left to unit directors and managers. The acquisition, development and support requirements of a production network firewall design that meets a high available and secure architecture is not trivial effort or expense. The absence of personnel with the requisite knowledge and experience and a continuing strong network firewall maintenance and support program will diminish any security benefits provided by the firewall over time.

If the campus establishes a central e-commerce credit card authorization and transaction support system, the major credit card companies require the campus to use a firewall to control and monitor network traffic to protected e-commerce systems. The Office of Administration is presently developing a credit card policy that will outline the UC Davis requirements for the acceptance of Internet-based credit card transactions.

Recommendation 1: The deployment of network firewalls should continue to be a campus unit decision and it is recommended that UC Davis adopt no formal policy requiring the use of network firewalls at the department level or centralized data center. However, this recommendation must not preclude IET continuing to work with Office of Administration on the development and centralized support of Internet credit card authorization and transaction systems. The campus must comply with network firewalls requirements, as prescribed by the security provisions of the credit card companies and financial institutions. The sample network firewall design (Figure 1) should be used as an initial starting point for the e-commerce network firewall. In addition, this sample network firewall design could be used to support campus middleware components that are developed to support an enterprise portal model.

Finding 2: Greater overall campus information security improvements are more likely to be gained from the development and implementation of other security measures. While IET has researched and is moving forward on some of these security measures, such as incident response to both network and/or computer abuse and security vulnerability assessment services; a broader campus strategy is needed that encompasses the security programs components, as described by Figure 2. Such a strategy should identify program priorities, including proactive and reactive measures, with an implementation period extended over multiple years.

During project discussions, the merits of several information security tools and practices were identified that do not require the use of network firewalls. For example, several host-based firewall software products (e.g., Tiny Firewall, Network Ice, Zone Alarm) are available that will block system external threats directed at a specific host rather than the campus network or a single VLAN. In a multiple-use computing environment where a network firewall cannot be effectively used, a host-based firewall product may provide significant security benefits to specific servers. In addition, a campus-wide software licensing program could promote enhanced ability to withstand security threats by providing attractive licensing alternatives to faculty, staff and students.

Many commercial organizations use network address translation (NAT) to “hide” the actual originating Internet Protocol (IP) address of protected internal servers/computing hosts. This technique, if promoted at UC Davis, could reduce the ability of hostile network traffic from being targeted to specific hosts and/or servers. However, the use of NAT does require the installation of an internal network device to perform this function.

Recommendation 2: IET engage campus units to participate in the development of a broad information security strategic plan. The information security strategic plan would be developed with the guidance of the recently appointed Electronic Security Advisory Committee. The resulting information security strategy would be reviewed and discussed within the campus-wide IT policy and planning framework of the Administrative Computing Coordinating Council (AdC3), Academic Coordinating Computing Council (AC4), Technology Infrastructure Forum (TIF) and Information Technology Policy Board (ITPB). The implementation of specific components of the information security strategy must be incorporated into the campus budget review process.

DRAFT

Appendix 1: Project Participants

Project Sponsors

John Bruno, Vice Provost, Information and Educational Technology

Kent Kuo, Associate Director, Communication Resources, IET

Project Team

John Brittnacher, School of Medicine

Adam Getchell, Human Resources

Kevin Mayeshiro, Communications Resources, IET, Co-Chair

Minh Nguyen, College of Letters and Science

Robert Ono, IT Security Coordinator, IET, Co-Chair

Michael Timineri, IET Information Resources

Campus Resources Consulted During Project

Loren Bennett, Transportation and Parking Services

Bill Broadly, Mathematics Department

Todd Chapman, Communication Resources, IET

Rodger Hess, Communication Resources, IET

Tom Hill, Financial Aid Office

N. Dale Hurt, University Relations

William Grabert, Accounting and Financial Services

David Johnston, Office of the Registrar

Jonathon Keller, Accounting and Financial Services

Susan Morin, Graduate Studies

Jeremy Smith, Language Learning Center

Sherie Sprague, Chancellor's Office

Katie Stevens, Accounting and Financial Services

Davis Zavatson, Information Resources, IET

Appendix 2: Terms and Definitions

- ATM Asynchronous Transfer Mode - a network technology based on transferring data in *cells* or *packets* of a fixed size. The cell used with ATM is relatively small compared to units used with older technologies. The small, constant cell size allows ATM equipment to transmit video, audio, and computer data over the same network, and assure that no single type of data hogs the line.
- CalREN California Research and Educational Network - the California Research and Education Network (CalREN) is a statewide network that links California's higher education institutions to each other and to the nation, building an infrastructure capable of supporting advanced research and educational applications.
- LANE Local Area Network Emulation - technology that allows an ATM network to function as a local area network backbone.
- NAT Network Address Translation - an Internet standard that enables a local area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. The internal IP addresses are hidden from the external IP addresses. NAT services may be provided by a network firewall or router.
- VLAN Virtual Local Area Networks - a network of computers that appear as if they are connected to the same subnet even though they may actually be physically located on different segments of a local area network.

DRAFT

Appendix 3: Suggested References

Building Internet Firewalls by D.Brent Chapman and Elizabeth D. Zwicky, O'Reilly & Associates, 1995.

Firewalls and Internet Security: Repelling the Wily Hacker by William R. Cheswick and Steven M. Bellovin, Addison-Wesley, 1994.

Linux Firewalls by Robert L. Zeigler, New Riders Publishing, 1999.

DRAFT