Firewall Strategies

June 2003

Executive Summary

Firewalls are one component of a strategy to combat malicious activities and assaults on computing resources and network-accessible information. Other components include anti-virus software and intrusion detection software. Most computers within Northwestern are protected by anti-virus software.

NUIT has prepared this document to orient both technical and management staff to the capabilities of firewall software, and to assist those persons to decide on an appropriate level of participation in this technology. While several approaches were considered for individual users, departments, and divisions, NUIT recommends that the University adopt a systematic approach to this security issue. Common equipment and common management approaches will leverage investments to increase overall security.

Brief survey of firewall concepts

What is the problem?

Due to ongoing occurrences of network security incidents and the increased requirements to protect institutional information, there is interest within University departments for a method of controlling the traffic that is allowed to access their computers. The ideal solution would be for each computer or networked device to be secured from intrusion and patched to eliminate vulnerabilities; however, this is not always a realistic scenario. The challenge lies in not only understanding the vulnerabilities of a system and in configuring a system to behave securely, but also in enforcing the security best practices for all the devices within one's domain. Products that have a default install of "unsecure" make this task all the more difficult. Many departments find it difficult to enforce security policies or to educate end users or themselves on how to do this. As a result of these concerns, many departments are looking for a way to control the traffic that is allowed to access their computer systems.

Although firewalls are not a complete solution to preventing security attacks against a host or the network itself, they can add another layer of security when properly deployed. A firewall is by no means a panacea; it's simply another tool to assist in controlling the types of traffic that a host must deal with. The only completely secure firewall is one that blocks all traffic; however, a computer with no network connectivity is not a very useful one these days.

What is a firewall?

A firewall is a device or software that can inspect traffic at a deeper level than most network elements. It can be software that resides on a host[1] and inspects traffic before it is allowed to interact with any other applications on that host. This type of firewall is known as a host-based firewall or personal firewall. A second type of firewall is a network firewall that does not reside on the computer system that it's protecting. It is a standalone device that must be inserted into the network so that it can inspect traffic that flows through it and make decisions on whether it will allow or deny a particular packet or flow of packets. Neither type of firewall has any "magic" that can decipher good traffic from bad traffic. The firewall makes a decision using the information that has been provided by the person responsible for the systems being protected. This information is expressed as a set of rules known as the "ruleset". The ruleset should follow a department's security policy, which is an essential component to establishing security. If one can't define what traffic should be allowed, then rules can't be developed to enforce it.

What skills are necessary to manage a firewall?

The management of a firewall requires a detailed understanding of data networking elements (routers and switches), as well as a detailed understanding of network protocols (the languages used when systems communicate over the network). Furthermore, it requires the ability to translate these concepts along with a security policy into an effective ruleset that can be applied to the firewall.

Beyond installation of the firewall into the network, firewalls must be configured with rulesets that accept or deny the types of traffic specific to the department's security policy. The collection of rules that make up the ruleset must be logically defined in the format dictated by the firewall's operating system and in the proper order.

Both routers and switches are network elements that require experience to effectively deploy and firewalls that perform these same functions have the same requirement. There are two general modes of operation for network firewalls. Network firewalls can act as routers (route mode) or switches (transparent mode). Route mode is the more traditional mode used by firewalls and requires modifications to the existing infrastructure in order to accommodate the new networks that are created for the protected hosts. NAT (network address translation) is a special form of route mode and will not be distinguished from route mode for the purposes of this discussion. Route mode also requires that the IP addresses of the protected hosts change. Transparent (switch) mode allows for a more seamless installation yet still requires an understanding of switching technology to safely deploy.

Do firewalls have a downside?

Putting every host behind a network firewall requires that all traffic go through the firewall in order to access resources on the other side. There is some benefit to putting up a barrier between a user and network resources but there are also negative effects.

Firewalls are high-touch systems that need to look much deeper into a packet than a simple switch or routing device. As a packet flows through a firewall, many processes need to occur: 1) a connection must be accepted from the outside, 2) information about the connection must be stored, 3) a decision must be made about how to process the packets associated with that connection, and 4) new connections to the inside need to be established. This processing needs to happen separately for each connection or communication between two hosts and in both directions. Comparing this processing with that of a low-touch network element such as a switch or router, firewalls will cause delay that could affect the flow of information between hosts on a network. The amount of delay experienced through a firewall is dependent on how the firewall is implemented. Firewalls that process in hardware will be faster than firewalls that process in software.

The complexity and high-touch aspect of firewalls also limits the new applications that can be supported behind a firewall since the firewall must be updated to understand each new application. This is especially important in a university department that requires high bandwidth applications or advanced services such as jumbo packets, IP version 6 or encryption. The original design of the Internet stressed the end-to-end argument that put intelligence and complexity at the edges while keeping devices in the middle simple and efficient. This design is important to researchers because it does not put up a barrier to the development of new and innovative applications.

Recommendations

What are the options?

In determining the placement and method of attaching firewalls to the network, there are several alternatives to consider. Placement of the firewall determines what set of users can be protected from each other and how easily a solution can be managed both from NUIT's perspective and the University community. When deciding on how to incorporate a firewall into a security strategy, department administrators have three options from which to choose: consumer network appliances; managed network firewall service or a host-based firewall. The consumer network appliance and the managed firewall service are for deploying network firewalls. Host-based firewalls can be utilized where a network firewall is impractical or unfeasible (as discussed below), or as an additional layer of control in conjunction with a network firewall. NUIT investigated the options available and found that a managed firewall service would be the best solution for

deploying a network firewall. The features and concerns of all three options are outlined below beginning with the drawbacks of the consumer appliance.

Consumer appliances

When considering a network firewall, there are several things of which a system administrator should be aware. There are many network firewalls available to the average consumer, but they do not have the features, reliability or management options of an enterprise class device. Most are SOHO (small office home office) firewalls that are limited in features and robustness:

- Most are limited to 10Mbps of bandwidth:
- They do not support advanced features such as remote access VPN, multicast, H.323, VoIP or transparent mode
- Most are limited to NAT (Network Address Translation) mode.
- The level of robustness varies. Many are slow performers or run an operating system that is not capable of withstanding DoS (denial of service) attacks itself.
- Logging from such devices is not as detailed as required for an enterprise and management is lacking.
- The level of "statefulness" [2] is lacking in some applications.

Beyond these limitations, there are also other issues that an administrator needs to be aware of when considering the implementation and management of a consumer appliance firewall:

- NUIT cannot offer assistance in trouble-shooting problems with the firewall or the hosts hidden behind the firewall.
- Extending the network with department-owned equipment makes it more difficult for NUIT to manage network capacity.
- The department would be responsible for backing up and monitoring the firewall.
- A consumer appliance firewall cannot accommodate protected machines in multiple locations within a building.
- NUIT can not provide usage reports to departments when computers are hidden behind a consumer appliance firewall.
- All machines behind the firewall could lose connectivity if a port is shut off.
- Should the departmental IT staff with knowledge of a consumer appliance firewall leave, there will be no central support.
- Failure or incorrect configuration leading to loss of connectivity would be the responsibility of the department.
- There will be no access to future NUIT services such as correlation of logs that will enhance the overall security of the University.
- Technology creep wherein the hardware becomes obsolete is the department's responsibility.

Network Firewall Service

The recommended solution is the firewall service option where the network firewall is installed, managed and maintained by NUIT. Choosing to purchase a firewall service from NUIT has several benefits. The department will be alleviated of the everyday management of the device, which will be backed up and monitored by NUIT. Should the device fail, NUIT will replace it on the spot and put the configurations back to get the department up and running quickly. The appliance would a best-of-breed solution that NUIT certifies for installation into the University network. Such a device will have the features necessary to run applications supported by the University.

The firewall features of this enterprise class equipment are outlined below:

- Bandwidth capacity from 70Mbps to 12 Gbps
- Support for advanced features such as remote access VPN, multicast, H.323, VoIP, transparent mode
- Support for multiple deployment options (route mode, NAT mode and transparent mode)
- Robustness features such as hardware processing and several mechanisms to prevent DoS attacks.
- Enhanced logging and management.

In addition to the powerful feature set, the network firewall service provides additional benefits to technical administrators:

- Support contracts are handled by NUIT while customer pays a easily budgeted annual fee.
- Ability for the customer to manage their own rulesets; while NUIT manages the rest of the firewall.
- Upgrades would be handled as part of the service.
- Customers can take advantage of future NUIT services such as correlation of logs that will enhance the overall security of the University.
- Positions the customer for new firewall services that will provide immediate protection against new attacks that may arise.

Personal or host-based firewalls

Host-based firewalls can be very effective in defining a security policy because they are only responsible for a single host. For the majority of hosts that are client [3] PC's, a single rule such as "don't allow any communication to this host unless this host initiated the conversation" will suffice. This type of rule can be easily applied with most firewalls, but may be too restrictive for hosts that need to accept outside connections. An example of such a host would be one

participating in a video conference. In general, if the hosts within a domain are homogenous with respect to their security policy, firewalls (host-based and network) will be very effective. Management issues occur when the host security policies are unique for each host. In this case management of each individual host-based firewall will be time consuming without a centralized management console.

Depending on the licensing and central management features, host-based firewalls can also be expensive. For those departments that are able to upgrade to Windows XP or Windows 2000 a host-based firewall is included with the price of Windows. The Linux operating system also has a built-in firewall. Separate firewall products often come with subscription support that can be valuable when no other layers of protection are deployed. See Appendix B for a brief discussion of this software.

Host-based firewalls can be used alone or in conjunction with a network firewall for an added layer of security. The benefits of host-based firewalls are summarized below:

- A host is protected even if it is moved from network to network (as with mobile devices)
- Certain operating systems provide host-based firewalls free of charge (Windows XP, Mac OS X, Linux)
- Host-based firewalls can have very effective rulesets since they enforce the security policy for a single host.

Host-based firewalls have the following issues that may decrease their effectiveness when used for servers or clients with diverse security requirements:

- A host-based firewall on a heavily loaded computer may delay processing needed for other tasks the host is required to do. Therefore, host-based firewall software may not be a good solution for a server.
- Host-based firewalls are only as secure as the underlying operating system and may be more susceptible to DoS attacks.
- Managing several host-based firewalls with unique rulesets will be difficult without additional management software.

Special constructs for researchers:

The operational requirements for research computer systems are very different from the operational requirements of administrative computer systems. Administrative systems look very much like the business world and firewalls that exist today meet their needs nicely; however, research systems cannot be accommodated with firewalls that exist in the industry today.

On the same network as administrative systems, may reside computer systems that need unfettered access to the network because they are used for fundamental network research. For example, there may be systems that have high-bandwidth applications or applications that are using advanced mechanisms such as jumbo packets, IP version 6 or encryption. Such mechanisms are either unsupported, as is the case with jumbo packets and IP version 6, or prevent the firewall from appropriately identifying traffic. For these systems, the best choice may be to follow security best practices for the particular operating system and to run a host-based firewall since a network firewall may hinder or prevent proper functioning of the system.

Which computer systems should be protected?

There are certain types of data or computer systems that are more important or that hold more sensitive data than others. These systems that need additional protection are good candidates for enhanced security measures and such systems should be governed by a security policy that details the level and type of access to these resources. Using a firewall to enforce security policies for such systems will provide additional security and auditing for such data stores.

The computer systems that require enhanced security are those that hold data not accessible to everyone or that if destroyed will cause significant loss of productivity while the system is unavailable. Each department will need to reflect on the security requirements of their systems (hosts, servers, printers, PDA's) and decide what level of security will work in their environment. Such a classification of information is necessary in determining an effective security policy. The inconvenience associated with increased security must be weighed against the risk of not securing it.

A successful data classification policy empowers system administrators to properly identify the locations of data stores that are to be protected and made available to the user community. This system can also provide useful guidance in the controls required to protect data, while reducing effort and costs associated with those controls by isolating their implementation to only those systems that are deemed critical or sensitive.

Any system storing University business information or information that falls under legal protections such as HIPPA or FERBA should be placed behind a firewall. It is advisable to look at research data as well when classifying data stores according to their security requirements. How will the loss or availability of such data affect the project? What are the consequences of a compromise to the integrity of the data?Mobile clients are a special concern because they travel from one network to another.

Mobile clients may plug in to a network at home or away or even a wireless network inside a coffee house. If such a client is not secured properly when

placed on an untrusted network, it will compromise the integrity of the secure network as it moves back to its "trusted" domain.

NUIT's approach to firewall deployment

The most successful implementation of a firewall can be found when the systems it protects are a collection of hosts with similar security requirements. How large or small the collection of hosts will be will vary for each department or administrative unit. In short, fewer exceptions yield better security. As a result NUIT expects firewall deployment close to the protected hosts to be the norm.

Balancing effectiveness and costs

The effectiveness of a ruleset for implementing a security policy is directly related to the placement of the firewall within the network:

- A firewall at the Internet border would be relatively ineffective in implementing a security policy for the entire university because of the diversity of operational requirements for all hosts on campus. Such a firewall would also need to be able to deal with the high bandwidths needed for all connections across the University border routers.
- Placing the firewall at a network "regional" level gives slightly more granularity in providing an effective ruleset, but still requires a basic coordinated policy for the entire network. A network "region" might be based upon user type (such as a "dormitory" region) but would more likely be based upon application and protocol affinities ("business" region). The region may contain multiple departments as well as a heterogeneous mix of users within a single department (e.g., a school). The greater this diversity, the more difficult ruleset maintenance becomes.
- Placing the firewall at a department level can effectively protect a number of hosts with the same security policy. In addition it can free the support staff from maintaining multiple host-based firewalls.
- Host-based firewalls (personal firewalls) on each end-user computer represent a full personalization of the firewall preferences – and the greatest maintenance cost for upkeep.

Mixing and matching firewall solutions

NUIT advocates a strategy that combines regional, departmental, and host-based firewalls. Under overall central management, this will maximize the effectiveness of the firewall component of the University's security plans.

As one approaches a particular host computer, each layer of this firewall strategy can be more specific about protection than applies:

- At the Internet border, NUIT can filter out protocols that are simply not accepted from outside the University. This might include certain database binding or file-sharing protocols.
- At the network regional level, a firewall can specifically reject attempts to connect with certain protocols from other network regions. This might block financial systems from intrusions from dormitory or external networks.
- At the department level, rulesets could protect local servers from being visible elsewhere to printer sharing or database queries.
- On the individual client desktop, a host-based firewall could protect a mobile device from times when it is connected to another network while traveling.

Only when the firewall security design takes into account all of these interlocking layers will the best protection strategy be found for the lowest cost.

NUIT planned service offering

NUIT will offer a firewall service based upon the principles outlined above. This service will focus on network firewalls with various forms of central ruleset management, measurement and maintenance. The object of the service is to provide the highest level of security with flexibility and minimum customer manpower investment.

NUIT is committed to offering a service that is reliable, secure and robust. The vendors NUIT chooses are industry leaders and best-of-breed solutions. An enterprise class solution is needed for service that is on a par with existing voice and data networks demands.

NUIT's approach to supporting multiple firewalls is to make their management similar to what is in place now for the other network elements. NUIT managed firewalls will have their rulesets and configurations backed up to allow rapid recovery in the event that their software configurations are lost or hardware should fail. Choosing a firewall that has true appliance characteristics makes this rapid deployment possible.

The cost model for this service has three components and is detailed in Appendix C. The first component is a one-time fee for initial consultation, installation and provisioning of the network firewall. The second component is an annual fee based on the level of firewall service that is chosen. This fee pays for the firewall hardware and ongoing maintenance of the firewall. This annual fee is based on the level of firewall service necessary to accommodate the specific application. The level is based on bandwidth capacity of the firewall as well as the number of connections [4] that are required to go through the firewall. The addition of more hosts or hosts that are bandwidth intensive will increase the level of firewall service that is needed. The last component of the firewall service is an annual

fee for ruleset management. This fee pays for ongoing maintenance of the ruleset and would mean that all changes to rules must come through NUIT. If the technical administrator for the department chooses to manage their own ruleset they may do so and would not have to pay the ruleset management fee.

NUIT feels strongly that a secure network is a collaborative effort with the University departments. NUIT's envisions utilizing tools to detect anomalous behavior before it results in a compromise. This aggregation and analysis of traffic information will only be possible with a carefully constructed firewall environment.

Conclusion

Security is a difficult job that involves constant care. Computer systems or other networked devices are vulnerable by virtue of their ability to connect and communicate with other systems. A firewall reduces some of the risk by reducing the number of devices that can communicate with a protected host.

Purchasing and installing a firewall device or software is only part of the job. After installation, rulesets must be defined and adjusted for new applications; emergency steps must be taken when new compromising techniques are made known; hardware must be maintained and replaced. The skills required are significant.

A single firewall device may seem to be the best approach for a given application. In other situations, personal or host-based firewalls may be the wisest deployment. However, most situations involve a hybrid of these solutions since business applications themselves are complex network-based programs.

NUIT will offer an enterprise-scale firewall service to meet the needs of the University.

Appendix A – Firewall Vendor Recommendation

Introduction

NUIT Telecommunications and Network services has reviewed three vendors' firewall products; Checkpoint, Cisco and Netscreen. The recommendation takes into consideration that the product will be provisioned by NUIT as part of an overall managed firewall service as well as allowing departments the ability to manage their own rulesets. The underlying goal of the review was to find a single vendor solution that would provide state of the art firewall services, easy and flexible integration into the infrastructure and effective management in a centralized deployment.

The Netscreen products provided the best fit for Northwestern. Their ease of management, product line diversity and integration options gave them a clear advantage among the competitors.

The deployment of network firewalls throughout the infrastructure should be viewed as a solution to the problem of protecting distributed information resources, which typically reside on a server. The network firewall can provide an effective means of restricting access to distributed servers and the services on those servers. A network based firewall solution across campus should happen in conjunction with a host based firewall service that provides more granular control. As most end-user hosts are not providing services or acting as servers, they can be configured to not allow any inbound traffic without prior outbound traffic being generated. Such a simple rule can easily be implemented with host-based firewalls. Host-based or personal firewalls also reduce the bottlenecking problem that firewalls create within the infrastructure. Since firewalls need to do deep packet inspection they introduce delay that becomes more significant as the number of connections that traverse the firewall increase. Host-based firewalls only handle the connections associated with the host the software resides on whereas a network firewall must do deep packet inspection on traffic associated with multiple hosts. As Northwestern's intent is to continue to grow high bandwidth applications, a overall firewall plan that minimizes the impact on application growth while providing a high level of security is required.

Criteria/Requirements

In making the determination, several key factors were considered. The primary concerns that were relevant to a managed firewall were:

- Ease of integration into existing infrastructure
- Ease of management and administration of the platform

Additional considerations in the decision making process were:

- Support available to allow shared management of the firewall. This allows NUIT to provide system support while allowing departments to mange their own rule sets.
- Support for virtual firewalls, which allow multiple administrative units to share a firewall but still have their own view and access to only their rulesets.
- Support for advanced features (VPN, Multicast, VOIP/SIP, H.323)
- Company's References (industry and customer references)
- Cost of implementation

An additional consideration for the managed firewall is whether to implement a larger scale shared firewall at each routing location or to provision a smaller box at the customer edge. Investigation of the how the firewall services technology may be used revealed a need for a small appliances at the edge that could protect a few select servers within a department. The additional complexity and much higher upfront costs for a shared model cannot be justified for the initial expected deployment. In NUIT's experience when discussing firewalls with departments – they are most interested in protecting a small number of hosts at a single location.

Technical Background

There are two basic architectures for firewall implementations. The first is a true appliance platform that consists of specialized hardware and firmware. The second is a software solution that runs on a general purpose PC platform with a general-purpose operating system that has been hardened to resist attack. After careful consideration of the two architectures, this appliance was found to be a superior platform in terms of manageability and support. The software solution is unattractive because it would require NUIT to support multiple software components and hardware that is provided by a 3rd party.

There are two general modes of operation for firewalls. Firewalls can act as routers (route mode) or switches (transparent mode). Route mode requires changes to the existing infrastructure in order to accommodate the new networks that are created for the protected hosts. Route mode also requires the IP addresses of protected hosts to change. Transparent mode allows for a more seamless installation. Servers are not required to readdress and changes are not required to the routing structure.

Product Descriptions

Cisco – PIX and FWSM

The PIX is Cisco's standalone appliance offered in 5 models. The models accommodate the SOHO business users up to a high-end firewall. Overall high-end capacity on the PIX tops out at 1.7Gbps.

The PIX does not run the same software as the Firewall Services Module (FSM), but has a similar command line interface. Features in the FWSM are slightly behind the PIX feature set.

The FWSM is a blade that installs into the equipment at a routing location and would be used for a large-scale deployment that fits the shared firewall model.

Even though the shared firewall model was eliminated as an effective solution today, the FWSM was tested as it is Cisco's latest offering. The issues remaining with the FWSM are the following:

- Since the FWSM is integrated into the existing Cisco 6500 platform there is an issue with software revisions on the switching and routing components that will need to support the new FWSM. In addition, upgrades become more complicated as there are now 3 different images running on these routing nodes
- No ability at this time to handle sharing of the firewall between multiple administrators – this functionality will be in a future release
- There is no VPN capability on FWSM (A separate VPN blade would need to be purchased). This is an issue since NUIT believes most departments would have the need for VPN access to their servers located behind a firewall. (Allowing connections from the campus VPN server would be too broad of a user base for most departments security policies)

Netscreen

Netscreen is an appliance-based firewall that offers several models to accommodate the very low end user to the very high end user. Overall high-end capacity on Netscreen tops out at 12Gbps.

In addition Netscreen offers a virtual firewall concept that allows a single firewall device to be shared by multiple departments with the proper access controls and separate the administration of rule sets by department. This capability is very attractive if large numbers of firewalls are deployed at each routing node.

Checkpoint

The Checkpoint firewall is a software-only solution that runs under several operating systems and hardware platforms. Third party vendors offer appliance-like products that package a general purpose PC into an appliance form factor

yet still run the Checkpoint software on a general purpose operating system such as Linux. Overall high-end capacity varies considerably, based upon the hardware that it is run on. Configurations that provide speeds between those of the Cisco and Netscreen models are common.

Vendor comparison

Ease of management and administration of the platform

- Netscreen has excellent documentation, which simplifies setup and configuration.
- Netscreen offers transparent mode, which eliminates routing changes to the network infrastructure.
- Checkpoint has a nice graphical interface, but initial setup can be time-consuming when the hardware and operating system are not purchased as part of the product.
- Cisco PIX configuration was not straightforward.
- The Netscreen platform can be managed both locally as well as through a central management console where as the Cisco PIX platform requires management in one fashion or the other, but not both.
- Checkpoint added additional administration, as it requires support of the operating system and the firewall application running over it.
- Out of band management via a console port is also missing from the Checkpoint solutions that run on PC hardware.

Installation into the infrastructure

- Netscreen firewalls can be configured in transparent mode, which eliminates the creation of many small networks and allows NUIT to deploy firewalls without having the customer change the IP addresses of the protected hosts.
- Pix can only run in routing mode, which requires changes to the network infrastructure and IP addressing changes.
- Checkpoint can only run in routing mode, thus requiring the same changes as the Cisco PIX.

Shared management

- Netscreen has the virtual firewall feature, allowing shared management of the firewalls, integrated into their product today.
- Cisco has this concept on their roadmap, but it is not yet available and it is not clear when it will be implemented.

Advanced features

- IPX and multicast traffic are supported in transparent mode on the Netscreens
- Cisco does not support IPX and supports multicast only by configuring a bypass tunnel.
- The Windows native client will not work in transparent mode on the Netscreens; however, it will work in route mode using L2TP over IPSEC. Running the Netscreen in transparent mode will require the use of a separate VPN client from Netscreen.
- The Cisco PIX allows both the Windows client and the Cisco client for VPN connections, which are the same clients used for the campus VPN concentrator.

Company focus

- Netscreen and Checkpoint are “best of breed” companies that concentrate on security products as their core business
- Cisco is more focused on being the integrator for all types of technologies.

References

- Netscreen had very positive recommendations
- Cisco references had chosen the product because they were a Cisco shop. General comments were apathetic.
- Checkpoint references were also good but much of their value seemed to come from managing very large installs (100’s –1000’s of Firewalls)

Appendix B – Personal Firewall Software

For this document, NUIT Technology Support Services examined personal or host-based firewall software as a possible stand-alone protection tactic. This investigation included testing of two popular software products, Norton Personal Firewall and Zone Alarm Pro. Both of the products tested were judged to be effective when configured by an IT professional. In addition, NUIT looked at what peer institutions are recommending and at reviews from industry publications.

Based upon this study, NUIT believes that personal firewall software can be valuable, especially for mobile computers that will be connected to "foreign" networks. However, widespread use of personal firewall software is not feasible because:

- The software is costly. Licensing costs for personal firewall software could exceed that currently paid by the University for anti-virus software.
- Installation and maintenance of the software requires an IT professional. Given that the software's intent is to limit communications between the host and the network, any special situations must be configured with care. Such exceptions are often relevant for an entire administrative unit, requiring either frequent visits to the workstation or additional control console software to automate distribution of rulesets.

The results of the NUIT study are available upon request.

Appendix C – Firewall Service Pricing

Service Description	Rate	Frequency of Charge
1. Initial consulting and firewall implementation recommendations	$1,600	One-time
plus		
2. Firewall hardware and ongoing maintenance (*Choose one based on size of firewall as specified by NUIT)* See note 1 below		Annual
a. Level 1 (1 or 2 servers / 70 Mbps)	$600	
b. Level 1+HA (provides for auto-failover to redundant hardware)	$1,900	
c. Level 2 (small server farm / 100 Mbps)	$1,680	
d. Level 3 (medium department / 170 Mbps)	$2,835	
e. Level 4 (large department / 400 Mbps)	$4,760	
f. Level 4 (large department / 550 Mbps)	$7,035	
3. Ruleset Management (***optional)*** See note 2 below	$1,300	

Notes

(1) The above descriptions of firewall levels are intended only as guidelines. The required level will be determined by NUIT during the consultation phase and is based on bandwidth capacity needs and the number of communication sessions that must traverse the firewall at any one moment. Once an initial firewall has been implemented, if a department later adds more hosts, especially hosts that are bandwidth intensive, the required level of firewall service may increase.

(2) The charge for ruleset management pays for ongoing maintenance of the ruleset by NUIT. This means that all changes to rules must come through NUIT. This is an optional service. The technical administrator for a department may choose to manage the department's own ruleset to avoid the ruleset management charge.

[1] The terms host and computer system are used interchangeably in this document. Any computer system that is communicating on the network is a host. Such a system could be a server (providing a service) or a client (accessing a service).
[2] Statefulness refers to the ability of a firewall to keep track of the information associated with a traffic flow and to use that information to react to a future event.
[3] Client refers to a computer system or host that does not provide any services. Services would be things like file serving that file servers provide or web services that web servers provide. Hosts that provide services are generally called "servers".
[4] The term 'connections" is used to mean the number of communication sessions that a firewall can keep track of at any one moment. Since a single computer can have multiple communication sessions open this is not equivalent to the number of computers that can be placed behind a firewall.

[TW1] How are they different?