FIREWALL POLICY

November 2006 TNS –POL - 008

Introduction

Network Security Services (NSS), a department of Technology and Network Services, operates a firewall to enhance security between the Internet and the Southern University network to establish a reliable network for the Universities computer and network resources. The Firewall is a key component of the Southern University network security architecture.

This Firewall Policy governs how the firewall will filter Internet traffic to mitigate the risks and losses associated with security threats to the Southern University network and information systems. This policy will attempt to balance risks incurred against the need for access.

Purpose

A firewall is one element of security for the campus network. It reduces the threat of outsiders either damaging Southern University systems or using the systems as a jumping off point for illegal entry into other systems. A firewall does not prevent malicious or illegal activities from inside the firewall.

This policy is designed to protect the Universities computers (student, faculty and staff) from hacking and virus attacks by restricting access to computers on the Southern University campus from users who are off-campus.

Scope

The policy applies to all Southern University network users: faculty, staff, administrators, contractors, students, systems, applications and networks.

Definitions

Firewall

A Firewall is a hardware and software device that controls access between two networks. There are several different mechanisms for performing this access control but the essential point is that a firewall implements a network security policy.

Firewall System

A firewall system includes both the Firewall Product and additional controls, that may or may not be available as part of the base firewall product. Typically these can comprise solutions to block or filter content; e.g. anti-virus email gateways, intrusion detection systems, audit and logging tools, mobile code (ActiveX, Java) monitors, integrity checkers, email content scanners and URL blockers.

Responsibilities

Network Security Services is responsible for implementing and maintaining the University's network perimeter firewall. Therefore, NSS is also responsible for activities

relating to this policy. Responsibility for information systems security on a day-to-day basis is every employee's responsibility. Specific guidance and direction for information systems security is the responsibility of NSS.

Policy and Procedures
The Firewall permits the following for outbound and inbound Internet traffic:

• **Outbound**- Allow ALL Internet traffic to hosts and services outside of Southern University with the exception of known security vulnerabilities (see below). This allows anyone connected to the Southern University Network to utilize all services on the Internet with the exception of known vulnerabilities.

• **Inbound**- Only specific services which support Southern University mission will be allowed to be accessed from the Internet. The chart below identifies the most common services used for Internet communications within the Southern University environment.

The following is a limited explanation for each column:
Server Functions and Services - This a listing of the most common Internet services used on the College file servers to support the mission and business of the University.

Southern University Network to Internet - All traffic originating from a University computer to an external host has no firewall policies applied except for known security vulnerabilities which are described in the chart below.

Internet to Southern University Network - All traffic originating from a computer on the Internet (some where off-campus) to a computer on the Southern University network is only allowed into the following systems.

Southern University Network to the Internet: Services which are NOT allowed	**Internet to Southern University Network:** Services which ARE allowed
• All Microsoft Networking Protocols • Network Monitoring Protocols • UNIX File System Protocols • Virus Related Protocols • Spyware Related Protocols (MarketScore Spyware)	• E-mail Server • Web Server • Blackboard • SSS (FTP Only) • Software (FTP Only) • Web Advisor • Library Catalog and Databases • Remote Desktop to Any OSX and Windows XP System • Web Helpdesk • Terminal Services • Library Catalog Search • Remote Desktop (as needed) • Other Departmental Servers

Operational Procedures

Only firewall system administrators are permitted to logon to the firewall.

- Access to firewall hosts must be tightly controlled. Only firewall system administrators are allowed to have user accounts on firewall hosts.
- Firewall system administrators must have personal accounts; i.e. no group logins are allowed.
- Direct remote root access is not allowed. All root access must be via a personalized logon.

Only personnel with the appropriate authorization can make changes to the firewall access rules, software, hardware or configuration.

- All changes should be as a result of a request recorded using the Firewall Change Request Form although emergency modifications can be requested by phone, with a follow up email and change request.
- Only authorized personnel must be able to implement the changes and an audit log must be retained.

ONLY AUTHORIZED departmental technical contacts may request any changes to the Southern University firewall. These requests must be submitted in writing or electronic including a rationale for the request by submitting the ***Firewall Change Request Form***. It is recommended that submit the request by visiting the Network Security Services website.

The Security Coordinator of IT Security will evaluate the risk of opening the firewall to accommodate requests. Where the risk is acceptable, granting of requests will be dependent on network infrastructure limitations and the availability of required resources to implement the request. If the risk associated with a given request is deemed objectionable, then an explanation of the associated risks will be provided to the original requestor and alternative solutions will be explored.

If during the implementation it is determined that the original request does not provide the functionality to meet the unit's business need, then the Security Manager of NSS has the authority to deny the request.

NSS will, on a short-term basis; provide open access through the firewall. Subsequently, long-term, the NSS will work with the requestor to determine exactly what ports are needed to meet the unit's business needs. Certain mission-critical functions require outside vendors and other entities to have secured and limited access to departmental network resources from the Internet to Southern University. This access needs to be approved by the department technical contact and then coordinated through NSS by submission of the Firewall Change Request Form.

If the original requestor considers the solution to be unsatisfactory, the request may be appealed to the Director of Technology and Network Services.

Turnaround time for a request for a normal change request will be handled in approximately 5 business days from the receipt of the Firewall Change Request Form.
Common Services include:
• FTP
• Telnet/SSH
• Mail
• Remote Access
• SMTP
• HTTP/HTTPS

Turn around time of a request for any emergency request will be handled as quickly as possible. To be an emergency the change must correct a major security risk. This additional time is needed to investigate that risk associated to the University.

Configuration
The firewall will be configured to deny any service unless it is expressly permitted.
- If there are no rules defined for a University network address, then traffic to or from that address must be denied.
- Access to the University network must be blocked during the start-up procedure of the firewall.

The firewall Operating System will be configured for maximum security.
- The underlying operating systems of firewall hosts must be configured for maximum security, including the disabling of any unused services.

The firewall product suite must reside on dedicated hardware.
- Applications that could interfere with, and thus compromise, the security and effectiveness of the firewall products, must not be allowed to run on the host machine.

The initial build and configuration of the firewall must be fully documented.
- This provides a baseline description of the firewall system to which all subsequent changes can be applied. This permits tracking of all changes to ensure a consistent and known state is maintained.

Security must not be compromised by the failure of any firewall component.
- If any component of the firewall fails, the default response will be to immediately prevent any further access, both "outbound" as well as "inbound".
- A firewall component is any piece of hardware or software that is an integral part of the firewall system. A hardware failure occurs when equipment malfunctions or is switched off. A software failure can occur for many reasons e.g. bad maintenance of the rules database on the firewall or software which is incorrectly installed or upgraded.
- IP forwarding at the operating system level must be disabled until the firewall software is operational and IP filtering policies active.

Audit and Compliance
Regular testing of the firewall will be carried out
- The firewall must be regularly tested for:
    - configuration errors that may represent a weakness that can be exploited by those with hostile intent.
    - consistency of the firewall rule set; i.e. to confirm the current status matches that expected (and documented).

- secure base system implementation; i.e. the integrity of the firewall hosts and applications must be verified using an integrity-checking tool

The firewall system must have an alarm capability and supporting procedures

- When an agreed specified event occurs, an alarm must be sent to the security personnel. Documented procedures must exist to permit an efficient response to such firewall security alarms and incidents.
- There may be specific circumstances when it would be advantageous for the firewall system to react in an automated manner to defined security events.
- In the event that the firewall itself is the subject of malicious attempts to penetrate it, and the firewall has the capability, delivery of services should be terminated rather than permit uncontrolled access to the University network.

There must be an active auditing/logging regime to permit analysis of firewall activity either during or after a security event

- An audit trail is vital in determining if there are attempts to circumvent the firewall security.
- Audit trails must be protected against loss or unauthorized modification.
- The firewall system must be able to provide logging of specific (or all) traffic when suspicious activity is detected.

Compliance Requirements

These guidelines are intended to supplement, not replacing all existing policies, regulations, agreements and contracts that currently apply to institutional computing and networking services. Persons given access to the department's technology and information assets must sign a statement that they have read and agree to abide by this policy.

Periodic Review of Firewall Security Policies

Firewall security policies will be reviewed at least yearly. When there are major changes to the network requirements this may warrant changes to the firewall security policy.

Instructions for SU Firewall Change Request Form

Only authorized contacts can request firewall changes.

The Southern University Firewall Change Request Form should be completed by authorized firewall change request authority. Sections 1-10 at the top of the page should be completed by the department requesting modifications to the SU firewall.

1. Requester's Name (Printed):	Enter the name of the person making the firewall change request.
2. Requester's Phone #:	Enter the phone number of the contact person for the request.
3. Requester's Email:	Enter the email address of the contact person for the request. (Must be a subr.edu email address)
4. Department:	Enter the department name of the person making the request.
5. School/College:	Enter the school or college name of the person making the request.
6. Change Category:	Mark the change category. A normal change request will be handled within five (5) working days. An emergency change request will be handled as quickly as possible. To be an emergency the change must correct a major security risk.
7. Proposed Change Date:	Enter the date changes to the firewall should be applied. If changes do not need to be applied on a specific day leave this field blank.
8. Description of what you are trying to accomplish:	Enter a brief description of what is to be accomplished with the firewall rule change. If necessary attach additional pages.
9. Authorized Requester's Signature, Title:	Enter the signature and job title of the authorized department contact. If the form is submitted by email a signature is not required, but the email must originate from an authorized contact's email address. (Must be a subr.edu email address)

10: Date: Enter the date of signature.

The bottom portion of the form will be completed by the Network Security staff. The form should be submitted or emailed to NetworkSecurity@subr.edu. Conformation of the completion of the requested change will be made to the requester by phone or email.

Southern University
Firewall Change Request Form

Only authorized contacts can request firewall changes.

The default rule is to deny all traffic, and only enable those services that are needed.

1. Requester's Name (Printed)	2. Requester's Phone#	3. Requester's Email	4. Department	5. School/College	6. Change Category	7. Proposed Change Date
					☐ Normal ☐ Emergency	

8. Description of what you are trying to accomplish (use additional pages if needed):

9. Authorized Requester's Signature, Title	10. Date

The following section is to be completed by TNS staff:

1. Requested Changes:

	Source Address	Source Port	Destination Address	Destination Port	Action Deny/Accept	Add/Remove Rule	Reason for Change(s)
Ex.	Any	Any	192.222.222.2	80 TCP	☐ Deny ☐ Accept	☐ Add ☐ Remove	Adding web access to web server in DMZ from any outside source
a					☐ Deny ☐ Accept	☐ Add ☐ Remove	
b					☐ Deny ☐ Accept	☐ Add ☐ Remove	
c					☐ Deny ☐ Accept	☐ Add ☐ Remove	
d					☐ Deny ☐ Accept	☐ Add ☐ Remove	

2. Request/remove static address assignment for:

Private IP Address	Translated to Public Address	Private IP Address	Translated to Public Address
a	a	c	c
b	b	d	d

3. Change Request Security Review Results			
4. Change Request Results: Approved/Denied, and Comments			
5. Scheduled by	**6. Date**	**7. Time**	**8. Back-out File Name**
9. Request Closed by	**10. Date**	**11. Time**	