Firewalls: Residential Student Network Firewall Policy

Background

A firewall is a key component of network security architecture. It contains control mechanisms that are activated when a security violation on a network is suspected, and protects assets from a potential attack. Protected assets include data/information and hardware and software, including central servers and access to the Internet.

Network and Telecommunications Services (NETS) in the *Office Information Services* operates firewalls between the Internet and various University networks to establish a secure environment for computer and network resources.

Purpose

NETS designed the Residential Student Network Firewall Policy to effectively enable security control mechanisms within the residential student network firewall.

The policy governs how the firewall filters Internet traffic on the student network to mitigate the risks and losses associated with security threats.

The Residential Student Network Firewall Policy adheres to the University's general policies on information technology usage.

Definitions

Firewall A system designed to prevent unauthorized access to or from a network. The hardware/software examines network traffic and makes a determination based on rules to allow or deny access to network resources.

SSH Secure Shell is a command line interface used to securely access a remote computer.

SMTP Simple Mail Transfer Protocol is a protocol for sending electronic mail messages between computers.

DNS Domain Name Server (or System) is an Internet service that translates domain names into IP addresses.

TFTP Trivial File Transfer Protocol is a simpler but less secure network application than File Transfer Protocol.

SNMP Simple Network Management Protocol is a means of monitoring and controlling network devices, and managing performance, security, configurations, and the collection of statistics.

Scope

This policy applies to the wired residential student network on the Kingston campus. (Wireless networks use different security mechanisms but provide the same protection.)

General Provisions

Deny traffic from any computer on the Internet (off-campus or on another URI network segment) to a computer on the residential student network if the traffic is unsolicited or not established.

That is:
A student's machine connected to the Internet cannot be probed for service ports or running programs unless the student initiated contact by requesting Web pages, games, music, or other applications from the Internet.

Specific Provisions

Residential student network traffic on the following ports cannot access any other URI network segments or the Internet:

Port	*Protocol*	*Common Service*
22	TCP	SSH
* 25	TCP	SMTP
* 53	UDP	DNS
69	UDP	TFTP
135	TCP/UDP	Microsoft DCOM
137	TCP/UDP	NETBIOS Name Service
138	TCP/UDP	NETBIOS Session Service
139	TCP/UDP	Microsoft Session Service
161	UDP	SNMP
445	TCP/UDP	Microsoft Directory Service
1434	TCP/UDP	Microsoft SQL Monitor
* 1521	TCP	Oracle Port
* 3306	TCP	MySQL
* 6106	TCP	Veritas Backup

** Closed only to outside URI Internet addresses.*

Policy Violations

Any attempt to intentionally or unintentionally circumvent policy may result in suspension to network access. In addition, the University may take administrative action or legal action based on applicable State and/or Federal laws.

Impact on Other Policies

None known to date.

Effective Date

September 1, 2005.

Supersedes

None.

Next Review Date

One year from effective date.

Policy Contact

URI Information Security Architect
Network and Telecommunications Services, OIS
401-874-4787

Policy Exception Requests

OIS Help Desk
helpdesk@uri.edu or 401-874-HELP

Policy Authorization

M. Beverly Swan
Provost and Vice President for Academic Affairs

References and Attachments

None.