ICTS Policies

Policy UCT Perimeter Firewall policy

Document summary

Effective date	10 May 2008	**Last updated**	27 March 2012
Policy owner	Executive Director: Information and Communication Technology		
Approved by	Senate and Council		

Table of Contents

Purpose

Information and Communication Technology Services (ICTS) at the University of Cape Town (UCT) operates a Perimeter Firewall to establish a secure environment for the University's computer and network resources. The Perimeter Firewall is an essential component of UCT's Information and Communication Technology (ICT) security infrastructure. A firewall is a security system that controls and restricts both Internet connectivity and Internet services. The Perimeter Firewall separates the UCT network from the Internet.

The Perimeter Firewall:

- provides the first level of protection for the campus network and computer resources.
- protects UCT's limited, expensive, Internet bandwidth from abuse.

This Perimeter Firewall Policy governs how the Perimeter Firewall will filter Internet traffic to:

- mitigate the risks and losses associated with security threats to the UCT network and computer systems.
- enforce Internet bandwidth management mechanisms.

This policy is designed to help protect computers attached to the UCT network from hacking and virus attacks by restricting access from external networks. The Perimeter Firewall is the first line of protection for the campus network. Every computer on the UCT network must still be secured (i.e. install Operating System patches, and applications security patches) and virus protected to mitigate threats from other computers on the internal network.

Definitions

Term	Definition
UCT network	For the purposes of this document, the UCT network is defined as: *The data network that extends across UCT-owned or -leased premises excluding the Graduate School of Business. The network connects various classes of devices to each other and to third-party networks such as the Internet.* *The UCT network consists of data cables and network infrastructure devices.* Broadly, from the average end-user's perspective, this includes the network up to the plug in the wall.
Firewall	A security system that controls and restricts both Internet Protocol connectivity and Internet services. Firewalls establish a perimeter where access controls are enforced. Connectivity, as the word is used here, defines which computer systems can exchange information. A service, as the word is used here, is sometimes called an application, and it refers to a way for information to flow through a firewall. Examples of services include FTP (file transfer protocol) and HTTP (web browsing).
Perimeter Firewall	The firewall that separates the UCT network from the Internet.
Outbound connection	An outbound connection is one which is initiated from inside the UCT network.
Inbound connection	An inbound connection is one which is initiated from outside the UCT network.
ResNet	Residents in UCT accommodation managed by Student Housing and Residence Life are connected to ResNet.
Proxy	A proxy server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server services the requests of its clients by forwarding requests to other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server provides the resource by connecting to the specified server and requesting the service on behalf of the client.
SSH	Secure Shell (SSH), sometimes known as Secure Socket Shell, is a Unix-based command interface and protocol for securely getting access to a remote computer.

Telnet	Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers. Through Telnet, an administrator or another user can access someone else's computer remotely. Telnet is not secure.

Applicable to

All devices connected to the UCT network.

Exclusions

- This policy only applies to the Perimeter Firewall and not to other firewalls that may be used on the UCT network.
- ResNet will be subject to even stricter firewalling policies. The University Information and Communication Technology Committee (UICTC) has approved that ResNet should only be allowed Internet access via the UCT Proxy server and this has been implemented. UICTC has also approved that ResNet will only be allowed access to a limited set of services on the UCT network. This will be implemented along with the server registration process.

Policy summary

1. The UCT network is under threat from the Internet and must be protected.
2. Connections from the Internet to the UCT network (inbound connections): Only specific services which conform to the Appropriate Use of Computer Facilities policy will be accessible from the Internet.
3. Internet bandwidth is very expensive, and thus must be managed appropriately.
4. Connections from the UCT network to the Internet (outbound connections): Block known security vulnerabilities. Outgoing connections may be blocked to enforce bandwidth management mechanisms.

Policy details

1. Threats to the UCT Network

1.1. The University network is scanned every day from the Internet. Much of this scanning is done to determine the number and location of potentially vulnerable systems. UCT computer systems have been compromised, and have been used to attack other systems on the Internet and the local network. Denial of Service (DOS) attacks from the Internet have occurred in the past, and will be attempted again in the future against University systems.

1.2. Risks to our academic mission are most apparent. The loss or corruption of data or unauthorized disclosure of information on research and instructional computers, student records, and financial systems is unacceptable. The University also has a responsibility to secure its computers and networks from misuse. Use of this content is governed by the concept of “fair usage”.

2. Internet to UCT network

2.1. By default, deny access

Deny all Internet traffic initiated from outside the UCT network (inbound connection) unless explicitly permitted. Access may be permitted by IP address, port number or other mechanism. Access may be temporarily removed if a threat is detected.

This policy is designed to protect University network users from attacks launched from the Internet.

2.2. Register externally visible servers

Many servers need to offer their services to clients who are outside the University. This potentially renders them vulnerable to attack. Not only does this threaten the services they host, but it may also be used as a base to launch further attacks on other servers. Therefore precautions need to be taken to reduce this threat to an acceptable level.

2.2.1. Those responsible for externally visible servers need to be familiar with the appropriate measures they must take to safeguard their servers from attack.

2.2.2. Traffic from outside the University needs to be restricted and connections should be permitted only to those servers that are intended to be externally visible

2.2.3. All servers connected to the UCT network for which there is a requirement to offer services to client computers outside the University or to ResNet must be registered with the Information and Communication Technology Services by a UCT staff member.

2.2.4. ICTS shall not refuse any request for registration other than on the grounds of a significant threat to the integrity of the computing infrastructure or a violation of the Appropriate Use of Computer Facilities policy, nor shall they delay registration unreasonably.

3. Internet bandwidth management

UCT currently spends R 7,800,000 per annum on Internet bandwidth. By international standards, South African Internet bandwidth is very expensive. Management of this resource is thus a key priority.

3.1. ICTS is to allocate suitable amounts of bandwidth to infrastructural services (e.g. DNS), to email, to library services (Calico and electronic library resources) and to the residence network. The majority of the remaining bandwidth is allocated to general web browsing.

3.2. ICTS is to allocate some bandwidth to services that cannot be easily proxied (e.g. SSH).

3.3. Undergraduate and honours students are to be restricted to a monthly Campus Internet Quota, which is monitored via UCT's Internet Security and Acceleration (ISA) server.

3.4. UCT staff, third parties and post graduate students are not restricted to a monthly Campus Internet Quota. They do, however, need to log on via ISA, so their individual bandwidth usage can be tracked by volume.

3.5. CMD must be kept informed of the identity of all website and web content owners, and web content managers.

4. UCT network to the Internet

4.1. Block known security vulnerabilities

4.1.1. Block known security vulnerabilities, including Microsoft Networking protocols, virus-related and spyware-related protocols. This will reduce reputational risk, by protecting others on the Internet from attacks launched from the University's network.

4.2. Protect UCT's Internet bandwidth

4.2.1. Proxies allow the University to account for bandwidth usage. Firewall rules may be used to enforce the use of proxies.

4.2.2. For specific protocols that cannot be proxied and use significant bandwidth to the detriment of other applications, outgoing connections may be blocked entirely or restricted to those who can demonstrate an academic or administrative requirement, after due consultation with the University community.

Policy violations

1. Any device found to be in violation of this Policy, or found to be causing problems that may impair or disable the network in any way, is subject to immediate disconnection from the University's network. ICTS may require specific security improvements where potential security problems are identified.
2. Attempting to circumvent Internet bandwidth management, security or administrative access controls for information resources is a violation of this Policy. Assisting someone else or requesting someone else to circumvent Internet bandwidth management, security or administrative access controls is also a violation of this Policy.