ITS Resource Center Home

Policies - Perimeter Firewall

Contact Information

Administrative Services
315-859-4169
its@hamilton.edu

Adopted November 2003

Information Technology Services at Hamilton College operates a Perimeter Firewall between the Internet and the College network to establish a secure environment for the College's computer and network resources. The Perimeter Firewall is a key component of the Hamilton network security architecture. 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 Hamilton network and information systems.

This policy is designed to protect college computers (student and employee computers) from hacking and virus attacks by restricting access to computers on the Hamilton campus from people who are off-campus. Every computer on the Hamilton network still must be secured and virus protected to be protected against other computers on the internal network.

Introduction

Among Hamilton's information technology priorities is the maintenance of a safe and secure computing environment. Historically, the risk of malicious packets making it into the College network has been relatively high. The assets at risk from targeted attacks against the network include data/information, software and hardware services, including access to the Internet and access to central servers are also at risk. Often, the data that is stored on such servers are the true targets of attackers.

The College's Perimeter Firewall must allow access to protected resources from authorized users located outside the firewall (users on the Internet). An increasing number of users work at home or while traveling. Research collaborators may also need to enter the Hamilton network from remote hosts. While this method does protect against many intrusions, it is not bullet proof. When a violation is suspected, the firewall architecture has logging capabilities to provide forensic information.

Information Technology Services (ITS) designed the Perimeter Firewall Policy to effectively enable the security control mechanisms found within the Perimeter Firewall. Consistent with all College information technology policies, the Perimeter Firewall Policy adheres to the College's General Policies on the Use of Information Technology.

A Perimeter Firewall is the first line of protection in the campus network. Similar to most modern hotels, one can enter and walk around many areas of the hotel such as the lobby unrestricted; however, to access a particular resource, such as a hotel room, one needs a key. In addition to the perimeter firewall which ITS will be maintaining, individuals and departmental system administrators are advised to make their desktop and server systems as secure as possible through a

"deny everything, permit on exception" firewall or system configuration approach. System administrators are encouraged to weigh the merit of placing firewall software on departmental servers and desktop machines. Host firewalls can block port scanners, protect against known exploits, log suspicious events and evaluate configurations.

Responsibilities

The Network and Telecommunications Team of ITS is responsible for implementing and maintaining the College network perimeter firewall. Therefore, ITS 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 ITS.

Policy for Perimeter Firewall

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

- Outbound - Allow ALL Internet traffic to hosts and services outside of the College with the exception of known security vulnerabilities (see below). This allows anyone connected to the Hamilton Network to utilize all services on the Internet with the exception of known vulnerabilities.
- Inbound - Only specific services which support the College mission will be allowed to be accessed from the Internet.

The chart below identifies the most common services used for Internet communications within the Hamilton 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 College.

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

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

Hamilton Network to the Internet: Services which are NOT allowed

- All Microsoft Networking Protocols
- Network Monitoring Protocols
- UNIX File System Protocols
- Virus Related Protocols
- Spyware Related Protocols
- (MarketScore Spyware)

Internet to Hamilton Network: Services which ARE allowed

- Hamilton E-mail Server
- Hamilton Web Server
- Blackboard
- SSS (FTP Only)
- Software (FTP Only)
- WebAdvisor
- Citrix Statistics Applications
- Library Catalog and Databases
- ListServ Mailing Lists

- Remote Desktop to Any OSX and Windows XP System
- Other Departmental Servers

Operational Procedures

Faculty, staff, and students may request access from the Internet for a service inside Hamilton for a new or existing server. These requests must be submitted in writing and need to include a rationale for the request. It is recommended that faculty, staff, and students submit the request through the ITS Help Desk.

The Network and Telecommunications Services Team and Vice President for Information Technology 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 Network and Telecommunications Services Team will, on a short-term basis, provide open access through the firewall. Subsequently, long-term, the Network and Telecommunications Services Team 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 Hamilton. This access needs to be approved by either a director or department chair and then coordinated through Network and Telecommunications Services Team.

If the original requestor considers the solution to be unsatisfactory, the request may be appealed to the Vice President for Information Technology.

Turn around time for a request of common services listed will be approximately 2 business days from the receipt of the Modification Form. Common Services include:

- FTP
- Telnet/SSH
- SMTP
- HTTP/HTTPS

Turn around time of a request for any other service will be no more than 5-10 business days. This additional time is needed to investigate any risk associated to the College.

Last Updated: January 10, 2012