University of Cincinnati Perimeter Firewall Policy

January, 2002

UC Firewall Task Force:

Carol Caperelli, College of Pharmacy
Jim Downing, UCit
Perry Morgan, Chair, UCit
Bryan Newswanger, UCit
Frank Pinski, College of Arts & Sciences, Physics
Mark Rance, College of Medicine
Jim Robinson, UCit
Ken Thompson, College of Engineering
Pearl Tsang, College of Arts & Sciences, Chemistry
David Will, College of Arts & Sciences, Physics

About the Firewall Task Force:
In developing the institution’s firewall strategy, the University of Cincinnati (UC) sought an appropriate and effective balance between network security and ample network access for the university community. The Firewall Task Force was assembled to examine the technical requirements for the University’s Perimeter Firewalls. The following Perimeter Firewall Policy attempts to reconcile the trade-off between performance of network security and support of an open academic and research-oriented environment. The Perimeter Firewall Policy includes configuration recommendations that apply to all University Perimeter Firewalls.
University of Cincinnati Perimeter Firewall Policy

Purpose

The University of Cincinnati operates Perimeter Firewalls or gateways between the Internet and the university network to establish a security environment for the university’s computer and network resources. The University’s Perimeter Firewalls are key components of the University’s Network Security Architecture. The University Perimeter Firewall Policy governs how the Perimeter firewalls will filter Internet traffic to mitigate the risks and losses associated with security threats to the University’s network and information systems.

Introduction

Among a university’s information technology priorities is the maintenance of a safe and secure computing environment. Historically, the risk of malicious packets making it into the university 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 university manages roughly 5,550 accounts on its MS Exchange servers. Each user is allocated 15MB. The University’s BearCat Online Platform supports approximately 39,818 accounts. Each user is allocated 5MB. The combined central servers have approximately 283 GB of data at risk.

The University’s Perimeter Firewalls must allow access to protected resources from authorized users located outside the firewall. An increasing number of users work at home or while traveling. Research collaborators may also need to enter the UC 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.

The University of Cincinnati Firewall Task Force designed the Perimeter Firewall Policy to effectively enable the security control mechanisms found within the Perimeter Firewalls. Consistent with all University of Cincinnati information technology policies, the Perimeter Firewall Policy adheres to the University’s General Policy on the Use of Information Technology, and the Policy on Information Technology Management.

The University’s Network Security Architecture provides a multi-layer-approach (Appendix B) for network security. This traditional approach is to have a Perimeter Firewall as the first line of protection. 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 fact, each switch-level router subnet (hotel room) can protect its own perimeter with much more regulated filtering. The University’s tiered solution allows the institution to segregate internal networks to reduce the risk from inside attacks. This provides an additional measure for an individual College and department to secure its business. Under this model, Colleges and Departments define this policy level at Tier 2. UCit is available to assist departments in defining a Tier 2 policy and subsequently implementing the policy at the switch-level router subnet.

Individuals and departmental system administrators are advised to make their systems as secure as possible through a “deny everything, permit on exception” firewall or system configuration approach. System administrators are encouraged to weigh the merits of placing firewall software on departmental servers and desktop machines for Tier 3 protection. Host firewalls can block port scanners, protect against known exploits, log suspicious events and evaluate configurations. Tier 3 solutions are the responsibility of the end user and College or department IT administrator.

Responsibilities

The Office of the Vice President For Information Technologies (UCit) is responsible for implementing and maintaining the University network’s perimeter firewalls. Therefore, UCit is also responsible for activities relating to this policy. While 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 UCit. Accordingly, UCit’s Network and Systems Security Team will manage the configuration of the University’s Perimeter Firewalls.
Policy for Perimeter Firewalls

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

- **Outbound** - Allow ALL Internet traffic to hosts and services outside of the University.
- **Inbound** – Allow Internet traffic from outside the University that supports the mission of the Institution as defined by the unit IT coordinator. The unit IT coordinator is defined by the College or department and can be an individual or group making these decisions.

The chart below identifies the most common services used for Internet communications within the 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 University file servers to support the mission and business of the University.
- **Secure UC VPN Internet to UC**- VPN stands for Virtual Private Network and uses a secure client application for the remote system (a system external to UC’s network). This method is only needed if an individual is accessing a non-public server or system. IT administrators will be the primary users of this type of access. Email systems and public university web pages do not require the use of the VPN client.
- **UC to Internet**- All traffic originating from a university computer to an external host has no firewall policies applied.
- **Internet to UC Open Zone**- Any university department has the capability to locate a server in UC’s open zone. The open zone is physically located in the UCit Data Center in the Medical Sciences Building. The benefit of doing this provides additional security to the department and university because the open zone is a separate network from UC’s main network. This is currently an evolving concept and with no UC systems currently located in the open zone.
- **Internet to UC**- This column uses the phrase “permission needed”. This means that departmental IT coordinators need to identify its servers and services that support its business. This process is taking place during the CISCO network conversion.

*After the Cisco network conversion, if a department needs to add a new server or modify the policy for an existing server, then read Operational Procedures section.*

<table>
<thead>
<tr>
<th>Server Functions and Services</th>
<th>Secure UC VPN Internet to UC</th>
<th>UC to Internet</th>
<th>Internet to UC Open Zone</th>
<th>Internet to UC</th>
<th>Examples/Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Mail</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>Permission Needed</td>
<td>Pop/imap/SMTP</td>
</tr>
<tr>
<td>Hosting Web Pages</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>Permission Needed</td>
<td>Http/www - Including SSL</td>
</tr>
<tr>
<td>Streaming Media/Video</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>Permission Needed</td>
<td>Audio/Video/H323/IP Video</td>
</tr>
<tr>
<td>Certificate Servers</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>Permission Needed</td>
<td>Entrust/VeriSign</td>
</tr>
<tr>
<td>File Transfer</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>Permission Needed</td>
<td>Authentication required for FTP access from the Internet to UC.</td>
</tr>
<tr>
<td>Other File Access</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>Permission Needed</td>
<td>Apple- Macintosh/Novel/NFS/NetBios - Required through VPN Concentrator.</td>
</tr>
<tr>
<td>Secure Shell</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>Permission Needed</td>
<td>SSH - Required use.</td>
</tr>
<tr>
<td>Telnet</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>Permission Needed</td>
<td>Telnet/Rlogin from the Internet to UC requires use of Secure Shell.</td>
</tr>
<tr>
<td>Remote Management</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>Permission Needed</td>
<td>Timbuktu/PcAnywhere/Vnc – Required through VPN Concentrator.</td>
</tr>
<tr>
<td>Databases</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>Permission Needed</td>
<td>SQL/Oracle/MSQL - Connections from Internet hosts to UC databases need to have appropriate approvals.</td>
</tr>
<tr>
<td>Other</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>Permission Needed</td>
<td>Access from the Internet to any other service as a default is denied.</td>
</tr>
</tbody>
</table>
Operational Procedures

- Faculty, staff, and students may request access from the Internet for service inside UC for a new or existing server. These requests can be submitted in writing and need to include a rationale for the request by submitting the Firewall Service Security Policy Modification Form (Appendix A). It is recommended that faculty and staff submit the request through their unit IT coordinator.

- The Network Operations Center (NOC) and the Network and Systems Security Team (NSST) 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 NOC & NSST will on a short-term basis provide open access through the firewall. Subsequently long-term, the NOC & NSST 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 UC. This access needs to be approved by the unit IT coordinator and then coordinated through the NOC and the NSST by submission of the form found in Appendix A.

- The UC OPEN ZONE is reserved to be used by university faculty, researchers, departments and sanctioned university groups or affiliates, with prior written approval from their respective unit IT coordinator and then coordinated through the NOC and the NSST by submission of the form found in Appendix A.

- If the original requestor considers the solution to be unsatisfactory, the request may be appealed to the Office of the Vice President for Information Technologies.

- Turn around time of a request for the common services listed on the chart (page 3) will be approximately 2 business days from the receipt of the Modification Form.

- 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 university.
Appendix A

UCit Firewall Service - Security Policy Modification Form

Please fax this form to Network Operations Center (NOC) at (513) 556-2010 when completed and signed. The NOC and the Network Systems and Security Team (NSST) will review the request and inform the requesting party of its determination. If the requested change is approved, the NOC will fax a copy of the modified security policy to the requesting party for their records.

<table>
<thead>
<tr>
<th>Name/Phone</th>
<th>Dept./Fax</th>
</tr>
</thead>
</table>

**Nature of Change** (check one):
- [ ] Addition
- [ ] Modification
- [ ] Deletion

<table>
<thead>
<tr>
<th>Source IP</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Destination IP</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Service(s)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Action</th>
<th>Check One:</th>
</tr>
</thead>
</table>
- [ ] Accept
- [ ] Drop

Be sure to sign and date this sheet before sending.

Signature: X________________________ Date: ________________

**Form Description**

**Nature of Change:** Indicate whether you are adding a new rule, modifying an existing rule, or deleting a rule.

**Source IP:** The source of the traffic to be affected by the security policy. This can be an IP address, a range of addresses, a network, or "Any" for any object.

**Destination IP:** The destination of the traffic to be affected by the security policy. This can also be an IP address, a range of addresses, a network, or "Any" for any object.

**Service(s):** The port numbers to be affected by the policy.
Appendix B

The University of Cincinnati
Multi-Layer-Approach to Network Security

Tier 1 - Internet perimeter connection for the University of Cincinnati

- This tier consists of a Perimeter Firewall, Intrusion Detection and VPN concentrator:
  - For detecting and stopping significant number of security breaches/intrusions.
  - Configured IDS to scan for incoming threats (scans/probes) to the UC Network.
  - Encryption between clients located anywhere in the world and to the university.

Tier 2 - Subnet/router layer

- Firewall software and IDS at the subnet level;
  - For internal colleges, units and university infrastructure servers.
  - Intrusion Detection helps identify and stop harm to internal university machines or external computers, in real time.

Tier 3 - Desktop machine, File Servers or UCit customer

- The responsibility of the end user and departmental system administrator:
  - Personal firewall and virus scanning software to protect the individual machine.
  - Responsibilities include:
    - Installing all updates and patches on a regular basis.
    - Perform regular backups to prevent data loss.