1. Overview

Firewalls are used to prevent unauthorized access by Internet users to private network resources. Firewalls can be implemented using hardware, software, or a combination of both. The University Firewalls provide “perimeter” protection against outside attacks. All traffic entering or leaving the University of Arizona network passes through a firewall, which examines each message and blocks those that do not meet specified security criteria. Attacks from inside the campus network do not pass through the perimeter firewalls and may pose greater threats than outside attacks.

Host-based firewalls may be used to provide an additional level of security to individual computer systems. Host-based firewalls are typically software that is installed on a single computer that can provide customized protection for that computer.

2. Purpose

The following guidelines will assist university affiliates in installation and use of host-based firewalls and securing university networked devices. Departments and individuals are encouraged to contact local computer support before implementing. These guidelines should not be used to hamper the procedures that may already exist.

3. Scope

These firewall software guidelines apply to all devices connected to the university network for the transmission of electronic communications. This includes all devices that are connected to the university network directly or are using a VPN.

4. Guidelines

Proper firewall configuration and maintenance is necessary in order to protect your system. It is strongly recommended that you read and understand the documentation for the firewall.

4.1. Windows Operating System

4.1.1. Windows XP Firewall

Windows Firewall is available for Microsoft Windows XP and above. If you are running Windows XP Service Pack 2 (SP2), Windows Firewall is turned on by default. However, some computer manufacturers and network administrators might turn it off.


4.2. Other Operating Systems

Please refer to vendor documentation for specific firewall configuration.

Related Guidance
Information Security Policy (IS-100)
Information Security Terms Guideline (IS-G100)
Minimum Security for Networked Devices Standard (IS-S602)
Minimum Security for Networked Devices Implementation Guideline (IS-G602A)

All *italicized terms* used in this standard are defined in the Information Security Terms Guideline (IS-G100).

**Revision History**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Draft</td>
<td>5/25/06</td>
</tr>
<tr>
<td>Effective Date</td>
<td>5/27/08</td>
</tr>
<tr>
<td>Revision (only new numbering):</td>
<td>08/22/12</td>
</tr>
<tr>
<td>Effective Date:</td>
<td>9/17/12</td>
</tr>
</tbody>
</table>