Network firewall standards

Type of Policy: Administrative
Effective Date: March 2017
Last Revised: March 2017

Policy Owner: Georgia Tech Cyber Security
Policy Contact: Information Security Policy and Compliance Manager

1. Reason for Policy
These standards exist to provide security standards for all network firewalls.

2. Policy Statement
Network firewalls shall be configured as to deny all network traffic to and from the Internet by default.

Only ports/protocols that are enumerated in the white list contained in these standards are exceptions to this; these ports/protocols are allowed to and from the Internet.

An exception approved by Cyber Security is required to allow the configuration of network firewalls to allow network traffic from any ports/protocols to or from the Internet that are not in the white list.

3. Scope
These standards apply to all network firewalls on Georgia Tech networks.

4. White list
Network firewall configurations may allow network traffic from the following ports/protocols to and from the Internet.

<table>
<thead>
<tr>
<th>Port/protocol name</th>
<th>HTTP (TCP/80)</th>
<th>HTTPS (TCP/443)</th>
</tr>
</thead>
</table>

© Georgia Institute of Technology
Page 1 of 2
5. **Related Information**
List related Georgia Tech policy documents, USG-BOR policies, and/or external documents that provide helpful, relevant information to the policy. Use of links is recommended, but appendices and other related documents can also be uploaded directly to the policy page, if necessary.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Link</th>
</tr>
</thead>
</table>

6. **Policy History**

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Author</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>03-29-2017</td>
<td>Cyber Security</td>
<td>Initial Release</td>
</tr>
</tbody>
</table>