Policy Title: Perimeter Firewall Policy	**Effective Date: 01/21/2011**
Policy ID: IT-5216	**Date of Last Review: 06/26/2026**
Oversight Department: Information Technology Services	**Next Review Date: 06/26/2027**

1. Purpose

Radford University (RU) utilizes available technologies on perimeter networking equipment to establish a firewall between its Internet connections and the RU network to establish a secure environment for the campus' network and computing resources. The perimeter firewall filters Internet traffic to mitigate the risks and potential losses associated with IT security threats to the campus network and information systems.

2. Policy

Given the academic nature of the university community, RU strives to maintain a firewall configuration that provides a secure and reliable environment while being cognizant of the special needs of faculty and students for a more open environment. Incoming TCP connections are denied by default and exceptions are made on an as needed basis.

In order for a system to be accessible by parties outside of the campus network, a request to allow the necessary traffic must be submitted via the IT ticketing system. This should include the ports, protocols, source, and destination IP addresses, permanent or temporary exception, expiration date and be approved by the system owner.

RU Information Security reserves the right to remove any firewall exception if the system is found to no longer be compliant with the Minimum System Configuration policy or if a related vulnerability is found that threatens the university's IT environment.

Firewall changes will be completed by Network Services staff during the normal maintenance window and must follow IT-5201 Change Control policy and procedures.

Backups of the firewall rulesets and configuration should be completed in accordance with the backup and restoration policy.

Firewall rulesets and configurations require periodic review to ensure that they afford the required levels of protection. This review should occur annually.

3. Procedures

The following generalized guidelines are utilized to configure the firewall.

Management of Incoming Traffic

1. Permit established connections to return to campus
2. Block IP's from known threats, compromised systems or high risk Internet subnets
3. Open only required ports to RU servers or systems that need to be accessible from the world
4. Deny all remaining IP Traffic

Management of Outgoing Traffic

1. Block private network address ranges as described in RFC's 1918 and 4193
2. General: port blocks for high risk Internet threats
3. Block all outgoing SNMP traffic
4. Only allow authorized RU mail servers to send outgoing SMTP traffic
5. Only allow authorized RU DNS servers to send and receive DNS requests
6. Allow all other outgoing traffic

4. Definitions

System Owner: The Radford University business manager responsible for having an IT system operated and maintained.

Sensitive system: The system is sensitive based on confidentiality, integrity or availability.

Maintenance window: A defined time when system changes, including minimal downtime, are acceptable

5. Related Information

Minimum System Configuration Standard – IT-5214s

Change Control Policy – IT-PO-5201

6. Policy Background

Radford University | Information Technology Services

7. Approvals and Revisions

Reviewed for comments: November 16, 2010 by ITAC committee
Approved: January 21, 2011 by Vice President for Information Technology & CIO

Reviewed: July 1, 2012
No changes.
Approved: July 1, 2012 by Vice President for Information Technology & CIO, Danny Kemp

Revised: February 3, 2016
Updated to reflect modifications to the Change Control policy and removed outdated references.
Approved: February 3, 2016 by Vice President for Information Technology & CIO, Danny Kemp

Reviewed: 6/13/2022
Policy reviewed during security standard review with minor wording changes for clarification. Revised with updated template.
Approved: June 15, 2022 by Associate Vice President for Information Technology & CIO, Ed Oakes

Reviewed: 8/2/2024
Revised procedures to reflect current technology.
Approved: August 2, 2024 by CISO, Bob Burton

Reviewed: 1/23/2025
Minor revisions for clarity.
Approved: January 23, 2025 by CISO, Bob Burton

Reviewed: 06/26/2026
Minor Wording changes
Approved: June 26, 2026 by CISO Bob Burton