IT FIREWALL POLICY

PURPOSE

The purpose of this Policy is to outline the requirements for deployment, management and operation of key firewalls at Brock University. The University subscribes to a layered defense or defense-in-depth approach to network security and firewalls are an essential layer of the University's IT security infrastructure.

SCOPE

This Policy applies to all firewalls and virtual firewall segments protecting the University's IT systems.

If any provision of this Policy is found to be inconsistent with the provisions of a collective agreement, the collective agreement will prevail, unless the Policy provision is required by law, in which case the Policy provision will prevail.

POLICY STATEMENT

This Policy outlines key requirements for firewalls in scope as detailed in the Standards for Firewall Deployment and Management. These Standards must be adhered to at all times.

- The University's servers must be protected with network perimeter and host-based firewalls. Responsibility for the deployment and administration of the network perimeter firewalls rests with the Information Technology Services ("ITS") Infrastructure Group. Responsibility for the deployment and administration of the host-based firewalls rests with assigned server system administrators.

- Web application firewalls must be deployed to protect the core applications as necessary. Responsibility for the deployment and administration of the web application firewalls rests with the ITS Infrastructure Group.

- Firewalls must be deployed to protect the University's IT systems from intrusion, suspicious anomalies, threats and block harmful traffic.

- All firewall ruleset changes must be documented, approved and verified.
- Firewall rulesets must be reviewed periodically as specified in the Standards for Firewall Deployment and Management.
- All administrative access to firewalls must be logged and the logs monitored.
- Access to both firewall and ruleset configuration must be reviewed periodically as specified in the Standards for Firewall Deployment and Management.

DEFINITIONS

Firewall: A network security system that controls incoming and outgoing network traffic based on an applied ruleset. A firewall establishes a barrier between a trusted, secure internal network or host and a network or host that is assumed not to be secure and trusted. Firewalls exist both as software solutions and / or as hardware appliances.

Host Based Firewalls: Firewalls designed to protect an individual system regardless of the network that the system is connected to. Host-based firewalls are typically provided as an integral component of the host's Operating System (OS) or as a third-party software add-on.

Network Perimeter Firewalls: Firewalls located at the boundary between the internal network and external networks such as the Internet. Network perimeter firewalls are purpose built enterprise grade devices (appliances).

Web Application Firewall: Controls incoming and outgoing network traffic at layer 7 of the OSI model. Unlike a regular firewall which looks only at network source, destination, port or an application signature, a web application firewall examines data content and allows or blocks traffic based on the content of the network connection. For example, a web application firewall that monitors SQL traffic is able to examine SQL queries and the data returned. It is able to block SQL queries and/or data that contain credit card numbers.

Server: A computing device capable of accepting requests from a client and giving responses accordingly.

Systems: Servers, services, applications or network devices.

COMPLIANCE AND REPORTING

The firewall and system administrators are responsible for adherence to this Policy and accompanying Standards.

ITS enforces this Policy and the related Standards at all times. Anyone who has reason to suspect a deliberate and / or significant violation of this Policy is encouraged to promptly report it to the ITS Help Desk. Policy violations that come to the attention of the ITS Help Desk will be escalated to the IT Security Specialist.

Policy violations will be assessed and action taken to remediate the violation subject to collective agreements and / or other contractual conditions.

Where Policy violations are considered severe and / or cannot be easily remediated, the incident will be escalated to the AVP, ITS for further action. Periodically, the AVP, ITS will provide to SAC a summary of all policy violations.

Policy owner:	Associate Vice-President, Information Technology Services
Authorized by:	Current version: Executive Team Prior versions: Board of Trustees, Capital Infrastructure Committee
Accepted by:	SAC
Effective date:	December 2021
Next review:	December 2022
Revision history:	2020 2019 2017 2016
Related documents:	Standards for Firewall Deployment and Management