Brock University

STANDARDS FOR FIREWALL DEPLOYMENT AND MANAGEMENT

PURPOSE

A standard includes specific low level mandatory controls that help enforce and support a policy.

The purpose of this document is to support and outline in detail the requirements of the IT Firewall Policy. These requirements are mandatory and must be adhered to by all network and system administrators.

Firewall deployment

Protection of the University's IT systems must follow a layered approach of defense.

- At a minimum, the following firewalls must be deployed:
  - A stateful network perimeter firewall must be deployed at the network edge to protect the University's network from the Internet;
  - A stateful network perimeter firewall must be deployed in the campus core to protect the University's administrative private internal network zones;
  - A stateful network perimeter firewall must be deployed to protect identified high risk services;
  - A web application firewall must be deployed to protect identified high risk web services;
  - Intrusion Prevention Systems must be deployed to detect the source of, and protect the University's network, from threats;
  - URL Filtering technology must be deployed to protect the University's network from known malicious sites;
  - A host-based firewall must be deployed on every University system acting as a server if supported by the operating system.

Responsibility for firewall administration

- All installations and implementations of host-based firewalls and their administration, including configuration of rulesets, are the responsibility of the designated system administrators;
- All installations and implementations of designated network perimeter firewalls and their administration, including configuration of rulesets, are the responsibility of the designated network administrators;
- All installations and implementations of designated web application firewalls and their administration, including configuration of rulesets, are the responsibility of the designated system administrators in conjunction with network administrators for physical and logical network connectivity.

Firewall user access: administrative access

- Administrative access to firewalls is restricted to authorized network and system administrators;
- A documented request (security access request form) for administrative access to network perimeter or application firewalls must be submitted to the Director, Infrastructure for approval;
- All authentication for administrative access must use Active Directory credentials;
- One local emergency administrative account is permitted.

Firewall user access: non-administrative access to network perimeter firewalls

- Read only access to firewalls may be granted to non-ITS employees based on their job responsibilities;
- Non-administrative access to network firewalls must be approved by the Director, Infrastructure;
- All authentication for non-administrative access must use Active Directory credentials.

Firewall ruleset configuration and maintenance

- Each individual rule must be documented with a brief description (purpose);
- Prior to deployment, all default ruleset settings (sometimes referred to as policy settings) must be reviewed and re-configured as appropriate to maximize security, e.g., an

"any-any allow" default rule must be changed to deny all, etc.;

- The default ruleset settings on any firewall for inbound traffic, i.e., traffic destined for protected system(s), must specifically deny all traffic. This rule must be the last rule in the inbound direction;
- All other changes to the ruleset configurations which allow access to protected systems must be configured using explicit permit statements;
- Permit statements must be specific and grant access to specific services or ports;
- Ruleset expiry dates, where known and supported by the firewall operating system, must be utilized. Each individual rule must utilize date of expiry if an identified date of expiry is known.

Firewall ruleset change management and approval process for network perimeter firewalls

- All changes to firewall rulesets must be submitted as a change request;
- After the changes have been implemented, all ruleset changes must be verified by the requestor as operational (i.e., working as intended). This confirmation must be documented by the requestor in the change request;
- At a minimum, the following detailed information must be submitted in the change request regarding ruleset or entry changes:

Title	**Firewall Change**
Requester:	Name and contact (phone, email)
Service owner:	Name and contact
Change type:	Addition, modification or deletion
Change category:	Regular or emergency
Date of proposed change	
Source IP address (subnet) or fully qualified DNS hostname	
Destination IP address (subnet) or fully qualified DNS hostname	
Destination TCP/UDP port / service (e.g., tcp/80 or web browsing)	
Date of expiry:	If the requested change has a defined time, provide effective date of expiry
Brief description of what you are trying to accomplish and reason behind requested change	

- When a service or a server is being discontinued, the system administrator responsible must issue a change request for the removal of the associated firewall / ruleset entries;
- All changes to firewall rulesets must comply with the IT Change Management Policy and associated Standards;
- The following approval process is in effect for all firewall ruleset changes:

Risk*	**Approval process**	**CAB required?**
Low	No approval required	No
High	Requires documented approval by at least two (2) senior ITS Infrastructure personnel consisting of subject matter experts (SMEs)	Yes

* Examples of corresponding risk levels are provided below:

- Low risk **(ticket required):
  - A device is bought / replaced and has to be added to a firewall group with other similar devices; includes devices such as UPS, camera, alarm panel, building automation systems ("BAS"), etc.
  - Backup for an employee or new employee to be added to the same group with the same access as the primary
  - Administrative department moving a service from one client to another requires the firewall rule to be expanded to include the new client
  - Changes to rulesets that do not modify security parameters (e.g., renaming, merging of rules, enabling/disabling logging, etc.)
  - Ruleset changes for troubleshooting to be enabled within a clearly defined timeframe.

** These examples are reflective only. The risk level of a specific change may not necessarily correspond to the risk level in the example above given the context of the specific change. All risk levels in individual change requests may be subject to challenge

- High risk (ticket required):
    - Addition or deletion of rules
    - Addition or deletion of ports or services in an existing rule
    - Addition or deletion of servers in an existing rule
    - Enabling or disabling of rules.

Firewall ruleset change management and approval process for web application firewalls

- The cross functional team must propose and track application firewall changes via change requests;
- All approved changes will be implemented by the designated system administrators.

Firewall review

- Firewall configurations and rulesets require documented periodic review to ensure accuracy and provide the required levels of protection. The ruleset must be reviewed during initial implementation and annually thereafter by designated network and system administrators;
- Rules which have been identified during the review process as no longer required will be removed following the change control process;
- The results of the review must be submitted to the Associate Director, Infrastructure for signoff;
- Documentation supporting firewall reviews must be retained in a secure location for a period of 18 months;
- All administrative and non-administrative user access must be reviewed semi-annually by the IT Security Specialist. The review including the outcome must be documented and signed off by the Director, Infrastructure.

Firewall backups

- Firewall configuration and associated rulesets must be backed up on a daily basis and stored on a secure remote system which complies with IT Backup Policy and associated Standards.

Firewall performance monitoring for non host-based firewalls

- Firewall performance must be monitored to identify potential resource issues to be addressed;
- Long-term utilization graphs must be available to monitor:
  - CPU and memory utilization;
  - Throughput (bandwidth) utilization;
  - Concurrent session utilization.

Firewall patching

- The operating system/firmware and patching level must be kept current for the given release;
- Network and system administrators must stay current with new vulnerabilities and patches;
- Vendor patches identified as critical must be deployed within 30 days of notification.

Any exception to the requirements in this Standard must be documented and approved by the Director, Infrastructure.

Definitions

Application: A computer program designed for a specific task or use.

Firewall: A network security system that controls the incoming and outgoing network traffic based on an applied rule set. A firewall establishes a barrier between a trusted, secure internal network or host containing sensitive data and another network or host that is assumed not to be secure and trusted. Firewalls exist both as software solutions and 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.

Intrusion Prevention System (IPS): Network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.

Network Administrator: An IT expert who manages an organization's network infrastructure.

Network Perimeter Firewalls: Firewalls located at the boundary between the internal network and external networks such as the Internet.

URL Filtering: Limits access by comparing web traffic against a database to prevent access to harmful sites such as phishing pages.

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 would be 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 and/or applications, or network devices.

System Administrator: The person responsible for the upkeep, configuration and reliable operation of computer systems such as servers and network infrastructure.