Network Firewall Standard

Version: 1.0
Publish: June 3, 2021
Published By: Information Security Office, Information Services
Approved By: Information Services Executive Team
Approval Date: April 6, 2021

1. Introduction

The purpose of this Information Services Standard is to provide guidance on the use of network firewalls and to protect the University's IT infrastructure and data against unauthorized access or potential malicious attack.

The IT Standard will assist in minimizing the risk of incorrectly configured network security devices, which could result in exploitable vulnerabilities.

Firewalls are a vital part of any information system's defense against attack. They are designed to detect and block unwanted traffic traversing the network and to minimize the adverse effects of intrusion should it occur.

2. Scope

The requirements in this standard apply to network firewalls positioned at the perimeter of the University of Regina campus network. These firewalls are known as edge firewalls, perimeter firewalls, or internet firewalls. This standard is scoped to non-data centre subnets and targets the protection of endpoint devices connected to the University of Regina internal network.

3. Standard

3.1. All in scope firewalls must be properly installed, configured and managed as per this standard. Failure of a network firewall to conform to this standard may create an exploitable vulnerability within the University's IT infrastructure. A successful exploit could compromise the University's networks, IT systems or data and consequently damage the University's reputation.

3.2. All University IT systems are required to be protected by at least one managed firewall.

3.3. Firewalls will block all incoming traffic that has not been explicitly permitted by the University's default firewall configuration. Access to University network and assets is set to deny all inbound traffic by default and any permitted inbound network traffic is only allowed based on approved business requirements.

3.4. Firewalls will only allow appropriate source and destination IP addresses and are required to block all traffic that is addressed to or appears to come from invalid or malformed IP addresses.

3.5. Only authorized protocols will be permitted through the in-scope firewalls.

3.6. Only authorized ports will be opened on the in-scope firewalls.

3.7. By default, in-scope firewalls must be set to fail-safe mode (deny passage of all inbound and outbound traffic if the firewall itself fails). For example, the external firewalls must not fail-open if they encounter a technical issue.

3.8. All network based firewalls are to be configured to record event logs, which must be transmitted and stored in the same way as other security-related logs. Traffic logs should be recorded where feasible.

3.9. All network firewalls must have routine configuration backup scheduled and stored offline in a secure location.

3.10. All network firewalls must operate in a fault tolerant configuration where an automated fail-over can occur if a failure occurs on a component.

3.11. Where possible and practical, externally exposed services should be provisioned from a data centre subnet.

3.12. When firewall rules are expected to be long term or permanent, static IP addresses should be utilized to prevent unintended exposure or interruption in external services should a dynamically assigned address change.

3.13. Whenever possible, existing mechanisms should be utilized to provide necessary access rather than requesting an exception to the standard. For example, rather than requesting that remote access be provided directly to a desktop, the standardized VPN configuration should be utilized.

3.14. Firewall rule exceptions are to be reviewed periodically to ensure that all opened ports are still valid.

3.15. This standard is subject to compliance audit, review and revision to ensure its effectiveness as firewall controls, threats, and risks change.

4. Responsibilities

4.1. The Information Security Office is responsible for:

4.1.1. Developing and maintaining this standard document.

4.1.2. Conducting annual reviews of firewall rules.

4.1.3. Reviewing and approving exception requests.

4.2. Firewall Administrators / Network Services is responsible for:

4.2.1. Ensuring firewalls in scope and under their management will comply with the firewall standard as defined in this document.

4.2.2. Ensuring that any exceptions are authorized by the Information Security Office in advance of implementation.

4.3. System/Service Owners are responsible for:

4.3.1. Acting in accordance with the Use of Computer and Network Systems policy. System/service owners must not attempt to modify, deactivate, or circumvent firewall rules.

4.3.2. Reporting any apparent misconfiguration or malfunction of the firewall rules.

4.3.3. Users seeking exceptions to this standard recognize and accept the risk exposing services/applications to the internet.

5. Exceptions

5.1. Exceptions to this standard require a documented request from the applications/service owner.

5.2. Exception requests must be requested by the application/service owner. Application/service owners must be staff or faculty.

5.3. Exception requests must include a documented business justification.

5.4. The Information Security Office will evaluate the request to ensure that:

5.4.1. The exception request is for minimal access in terms of ports and protocols.

5.4.2. The exception request is for minimal duration.

5.4.3. The exception request is not for vulnerable services such as those which could lead to data leakage, vulnerably exploitation, or reflected/amplified denial of service attacks. For example, database ports such as 1526, authentication services such as LDAP, file access such as SMB, or protocols susceptible to denial of service attacks like SSDP should not be exposed externally.

5.4.4. In determining whether an exception is warranted, consideration will be given to any comparable security measures in place or mitigating controls used to manage information security risks in a manner consistent with the intent of this standard.

Related Information

- Use of Computer and Network Systems Policy OPS-080-005
- Computing Services Technote #569

Revision History

Version	Version Date	Status	Summary of Change	Author
0.1	Feb. 4, 2020	Draft	Initial authoring	R. Jesse
0.2	Mar. 18, 2021	Draft	Revisions	R. Jesse
0.3	Mar. 31, 2021	Draft	M. Haidl contributions	R. Jesse
1.0	April 6, 2021	Final	ISET Approval	R. Jesse