Information Security - Firewall Security Guidelines

Section 1 - Purpose / Objectives

(1) Safe and secure network services are essential for the University operational goals. Firewalls are the first line of defence against attacks and are part of the overall security of electronic equipment and the information they work with. They provide a point where security can be imposed and can provide the University with information about the traffic passing through them.

(2) The purpose of the Firewall Security Guidelines is to define security standards for all equipment owned and/or operated by Victoria University,. These standards are designed to minimise the potential exposure of Victoria University to the loss of sensitive confidential data, intellectual property, damage to public image etc., which may follow from unauthorised use of Victoria University resources.

(3) Modern attackers will use multi-pronged attack methodology to gain access to internal and external facing services. This requires the University ensure it operates all network services, regardless of perceived access levels with a stringent secure configuration and operation.

Section 2 - Scope / Application

(4) This Guideline applies to:

a. All equipment or devices deployed that are owned and/or operated by Victoria University (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by Victoria University.
b. Any host device outsourced or hosted at external/third-party service providers, if that equipment resides in a Victoria University domain or appears to be owned by Victoria University.

Section 3 - Definitions

(5) Firewall

Section 4 - Policy Statement

(6) Nil

Section 5 - Procedures

(7) Nil

Section 6 - Guidelines

Server Network Production Firewall Operation Rules

(8) All network firewalls will have a default deny mantra.

(9) All servers providing services to directly to the Internet must be located in Presentation (External) zone.

(10) Firewall rules must be in place and will govern the communication allowed into each tier and between the tiers.

(11) Firewall rules are to be minimum required to deliver business needs — following a least privileged model.

(12) All administrative and management access which is required to servers within the corporate and development silo will be provided by the Management VPN solution.

(13) All Backup and Monitoring will be provided through the management network. (in the future).

(14) IPs are to be issued by the Communications Team, according to the IP allocation process. Change of Tier/Silo will require an IP change.

(15) Standard firewall change process will be carried out twice weekly.

(16) Changes for BAU group assignment (e.g. Finance One access) will be performed on an ad hoc basis.

(17) Additional changes are possible and should be included as part of the normal change management processes sent for CAB review (include firewall rules with system/service deployment changes noting ITSSO agreement or disagreement).

(18) Where direct communication with other networks is not viable, a connection via proxy where viable is preferred over a NAT approach.

Server Network Development Operation Rules

(19) All network firewalls will have a default deny mantra.

(20) All hosts will be issued with private IP addresses.

(21) All servers providing services to directly to the Internet must be located in Presentation (External) zone.

a. Policy based NAT will be created to allow for external communication.
b. Preference will be for the NAT configuration to be enabled and disabled based on work being carried out. This is not mandatory.
c. additional scrutiny for requests where a NAT rule will need to be established will be carried out.

(22) Firewall rules must be in place and will govern the communication allowed into each tier and between the tiers.

(23) Communication directly with production systems is to be discouraged. However, exceptions can — and will — be made where it is not possible or appropriate to have a completely isolated development environment.

(24) All administrative and management access which is required to servers within the corporate and development silo will be provided by the Management VPN solution.

(25) All Backup and Monitoring will be provided through the management network. (in the future).

(26) All data transfers (e.g. production to development) must be perform through intermediary hosts within the management network (providing an "air gap" between prod and dev).

(27) IPs are to be issued by the Communications Team, according to the IP allocation process. Change of Tier/Silo will require an IP change.

(28) With the exception of communication to the wider internet and production silos, firewall changes can be performed ad-hoc and without in-depth scrutiny.

(29) Where direct communication with other networks is not viable, a connection via proxy where viable is preferred over a NAT approach.

Border Firewall Operation Rules

(30) Default deny ingress traffic.

(31) Allowing connections direct to client networks is expressly forbidden.

(32) Dangerous or historically abused ports and services will be blocked where practical.

(33) Where practical user traffic will be proxied provide further security to the user network.

(34) Legacy Servers cannot request firewall changes and must migrate to the Server Network.

(35) No new servers can be deployed into the legacy network.

Other Firewalls Including Host Based

(36) Default deny ingress and egress traffic.

(37) Rules allowing traffic must follow principle of least privilege.

(38) Rules should limit access to defined expected users or services (e.g. VU Internal or DNS servers).

(39) Rules allowing administrative access should be limited as much as possible.

Status and Details

Status	Historic
Effective Date	18th August 2015
Review Date	16th August 2019
Approval Authority	Vice-Chancellor
Approval Date	11th August 2015
Expiry Date	26th February 2020
Accountable Officer	Lisa Line Deputy Vice-Chancellor Enterprise and Digital Lisa.Line@vu.edu.au
Responsible Officer	Lisa Line Deputy Vice-Chancellor Enterprise and Digital Lisa.Line@vu.edu.au
Enquiries Contact	James Munro Associate Director, VU Cyber 0437216020 Information Technology Services

This policy document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to always refer to Victoria University's Policy Library for the latest version.