<< [Organisation] Logo>>

<< Firewall and Router Policy >>

Version: 1.0
Date

Revision History

Date	Version	Author	Summary of Changes

Approvals

Name	Signature	Title	Issue Date	Version

Contents

Contents

INTRODUCTION

DOCUMENT PURPOSE

This document synthesizes documentation on firewall and router and related infrastructure to provide polices for the [organisation] throughout the full life cycle process of procuring, implementing and operating firewall and router solutions and other perimeter protection.

This policy applies to all firewalls and routers on the [organisation] network.

SCOPE

All firewalls and routers within, or connected, to the [organisation]'s network.

POLICY

Below are statements must be complied with.

Policy Statements

No:	Statements
	Boundary routers and perimeter firewalls are to be used as part of the [organisation] perimeter protection. Boundary routers will function as the network perimeter termination and accept traffic from the Internet Service Provider and third party connections. The boundary routers will be used to filter unapproved protocols and pass traffic to the firewall for additional packet screening and filtering a. All boundary routers will also implement ingress to protect against IP address spoofing and directed IP broadcasts. In addition, boundary routers will provide the first level of network access control using router access control lists (ACL) according to Router policy
	Perimeter firewalls will be used protect [organisation] from exploitation of inherent vulnerabilities. These firewalls must be in place to prevent unauthorized from the Internet from accessing [organisation]'s private networks connected to the Internet. These Perimeter firewalls will use Statefull inspection technology for packet filtering.
	Services. Only ports from required services for continued business operations shall be activated on the firewalls. Any service that is not needed shall be turned off or deactivated. Services and applications not for general access must be restricted by access control lists. Any services that are permitted to pass through a firewall whether inbound

	or outbound shall be documented as to: i. Service allowed (including TCP or UDP port number) ii. Description of the service iii. Business case necessitating the service.
	Ingress Filtering. As defined in this policy, ingress filtering will be performed to exclude/reject all data packets that have an internal host address (i.e. source address is in the local domain). Non-routable IP addresses specified in RFC 1918 (Private Network Addresses) shall be dropped.
	Egress Filtering. Egress filtering on the firewalls will be performed to prohibit packets from leaving the [organisation] network that have non-[organisation] addresses as their source address.
	Audit Logs. All firewall systems will have an audit capability to monitor firewall operation and substantiate investigations of real or perceived violations of local security policies. At a minimum, the audit logs will track information on client transactions: - 1. (i.e. IP address of source and destination, date and time, port, Uniform Resource Locator, etc), 2. attempted access to network services, 3. rejected source routed addresses, 4. Internet Control Message Protocol (ICMP) messages, 5. and any system information the local enterprise /network security officer deems relevant. Archived audit logs will be maintained for a minimum of one year and kept as a separate backup for easy retrieval when needed.
	High Availability. All firewalls should be implemented in redundant mode and provide failover functionality against hardware and software failures.
	Firewall Protocols. Insecure services or protocols (as determined by ICT Team) must be replaced with more secure equivalents whenever such exist.
	Change control Requests for firewall and router changes will be evaluated and approved by appropriate teams.
	All user accounts must be implemented in a secure manner.
	Remote administration must be performed over secure channels e.g., encrypted network connections using SSH or IPSEC
	Personal firewall software:- Mobile and/or employee-owned computers with direct connectivity to the Internet, and which are used to access the [organisation]'s network most have personal firewall software installed which is active and is configured by the [organisation] to specific polices.