LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
ECONOMIC DEVELOPMENT, ENVIRONMENT & TOURISM

ICT FIREWALL POLICY 2021 v3

I. Introduction

This document describes the standard firewall rules that will be applied to all firewalls connected to the Department's networks. The Department's standard firewall is the Sophos XG Firewall.

II. Firewall Overview

The Department has implemented a "Security Zone" approach to firewall configuration and deployment. These "Security Zones" are implemented as rule-sets on Department firewalls. Each firewall will provide multiple "Security Zones" to implement specific security controls for each zone. Default sets of "Security Zones" are created during the implementation of each Department firewall as follows:

- Workstation Zone
- Server Zone
- "Demilitarized" Zone (DMZ)

Security Zones to be implemented for each firewall as follows:

- **Workstation Zone** – The Workstation zone is designed to protect a department Unit's workstations, network printers, and other local network devices (inside the firewall) from all other zones. Access to this zone from all other zones is restricted and controlled.

- **Server Zone** – The Server zone is designed to protect a Department Unit's critical infrastructure such as domain controllers, file, print, intranet (internal web applications), application, and database servers. Access to this zone is limited to the Unit's Workstation Zone.

- **DMZ Zone** – The DMZ zone is designed to protect any server that is accessed by a broad audience. An example of this is a web server that is accessed by users from around the world. This zone acts as a protective layer between a Department Unit's workstations and servers. Only necessary ports are allowed inbound to this zone. Additionally, the Unit's Workstation and Server zones are allowed to access the DMZ zone.

III. Firewall Configuration

1) All physical network interfaces or VLAN interfaces will be configured with static IP addresses.

2) Each physical firewall will be configured to support multiple virtual firewalls. Each virtual firewall has its own routing information, its own set of IP addresses, its own firewall policies, etc. through the use of partitions.

3) Serial port access will be enabled on each physical firewall to allow local console management. A unique secure password will be assigned to each physical firewall for local console management.

4) All rule-sets, rules, host groups and service groups will have a complete description (ex. the "VNC" service group description should be "VNC remote control application", and describe the port and protocol "tcp5900").

5) Host groups will be defined as local to each firewall. Host groups that are used across multiple firewalls will be defined as global. Local firewall host group names will be identified using mixed case characters. Global firewall host group names will be identified using all upper case characters. When a Host groups that are converted from local to Global Group they will be modified to upper case.

6) Service groups will be defined as global to all firewalls. Service groups that will be utilized for only one firewall will be defined as local to that firewall. Local firewall service group names will be identified using mixed case characters. Global firewall service group names will be identified using all upper case characters.

7) All firewalls will be assigned a local console rule-set ("firewall") and an administrative zone rule-set ("administrative zone").

IV. Firewall Rule-Sets

1) Rule-sets will be defined for each "Security Zone" (Workstation Zone, Server Zone, DMZ Zone) as needed. Multiple rule-sets may be defined for each "Security Zone".

2) The system generated "firewall" rule-set will be assigned to the "local" interface for each firewall. The system generated "administrative zone" will be assigned to one of the network "etherX" interfaces for each firewall.

V. Passwords, Authentication, Responsibilities and Operations

A firewall user must provide a username and password for authentication when initiating a connection to the firewall. Passwords must meet the standards set out in the ICT Policy.

Access to Firewall hosts shall be blocked by default and access will only be permitted to Firewall system administrators. Firewall system administrators will each have their personal login credentials to access the firewall hosts. No group logins will be permitted. Only IP addresses reserved for system administrators will be given access to the Firewall.

Only personnel with the appropriate authorization shall make changes to the Firewall software, hardware, configuration and access rules. All change requests shall be guided by the LEDET Change Request Form.

Logging and Audit facilities provided by the firewall shall be enabled to detect breaches of the firewall's security and attempted network intrusions. Firewall administrators shall regularly examine logs and set mechanisms to respond to alarms.

Logs shall be kept for a minimum period of one month, before archiving and overriding the previous logs.

GITO will be the sole responsible entity for putting in place firewalls and the management of them in the LEDET environment. Monitoring, configurations and changes will be done by GITO only.

VI. Firewall Change management process

1) A user raises a request for a particular change.
2) The request is approved by the IT Director, and all the details on who approves the request are recorded for future reference.
3) After approval, the configuration is tested to confirm whether changes in the firewall will have the desired effect without causing any threat to the existing setup.
4) Once the changes are tested, the new rule is deployed into production.
5) A validation process is performed to ensure that the new firewall settings are operating as intended.
6) All changes, reasons for changes, time stamps, and personnel involved are recorded

VII. Redundancy or failover

1) System backup-The system, logs and configuration is configured to automatically back up on a daily.
2) Hardware Health- The DRP tests will be conducted quarterly to monitor the health and status of the appliance's components.
3) Software Updates- Software update will be done in accordance with change management procedure

VIII. Audit and Compliance

1) Regular reviews to the firewall rules shall be conducted to make sure that the firewall system meets the business requirements
2) Regular testing of the firewall shall be carried out to check for configurations errors.
3) The firewall systems shall have an alert capability and supporting procedures in order to report violations and intrusions to the system administrator.
4) There shall be an active auditing/logging regime to permit analysis of firewall activities both during and after a security event so that an audit trail can be documented if there was an attempt to illegally access the firewall.

IX. Policy Review

The Firewall policy shall be reviewed every thirty-six (36) months

X. Effective Date

The Policy comes into effect from the date of approval.

XI. APPROVAL

Approved by:

HEAD OF DEPARTMENT

23/02/2022.