



ICT FIREWALL RULES POLICY

1 July 2024

Table of Contents

1. PURPOSE OF THIS POLICY	2
2. GENERAL.....	2
3. FIREWALL ZONES.....	2
4. NETWORK ADDRESS TRANSLATION (NAT) POLICY.....	2
5. DEFAULT POLICIES	2
5.1 Global Default Policies	2
5.2 DMZ Default Policy.....	2
5.3 Internet Default Policy	3
6. FIREWALL RULES	3
6.1 Incoming Services to LAN Hosts.....	3
6.2 Outgoing Access	4
6.2 VPN Access	6
7. WEBSITE FILTERING POLICIES	7
7.1 Introduction.....	7
7.2 Logging	7
7.3 Globally allowed websites.....	7
7.4 Default Policy.....	7
7.5 Default Policy exceptions	9
7.6 Unrestricted Policy	10
8 SHORT TITLE	11

1. PURPOSE OF THIS POLICY

This document serves to define the standard configuration of the main firewall separating the Municipality from the Internet.

2. GENERAL

The firewall must be a multi-homed firewall, with at least one physical network adapter per zone, or virtual adaptor in the case of virtualisation. Public zones not belonging to the Municipality (Internet, external providers, etc) may not be hosted on the internal zones. It must be separated from the internal zones by placing the public zones on a different network adapter.

3. FIREWALL ZONES

At least the following zones must be configured:

- a) LAN: All subnets inside the Municipality.
- b) WAN: The Internet.
- c) DMZ: Isolated Zone hosting publicly accessible systems.
- d) VPN: Users accessing the network via VPN services.

4. NETWORK ADDRESS TRANSLATION (NAT) POLICY

All traffic originating from the LAN zone, leaving the organisation must be masqueraded by applying source NAT and hiding the traffic behind the public IP address(es) used to exit the organization.

All traffic originating from the LAN zone, accessing services on the public-facing IP addresses in the DMZ must be masqueraded by applying source NAT and hiding the traffic behind the firewall's public IP address used to access that part of the DMZ.

All DMZ hosts must have public IP addresses or must be hidden behind one of the firewall's public IP addresses using destination NAT.

5. DEFAULT POLICIES

5.1 Global Default Policies

By default, all network traffic between all zones must be dropped without rejection notifications.

5.2 DMZ Default Policy

By default, no traffic is allowed from any host outside the DMZ zone to any host inside the DMZ zone other than the exceptions documented in this document.

By default, no traffic is allowed from any host in the DMZ zone to any host outside the DMZ zone other than the exceptions documented in this document.

5.3 Internet Default Policy

No host outside the organization (in the Internet zone) may communicate with any host inside the organization (in the DMZ or LAN zones) in any manner other than the exceptions documented in this document.

6. FIREWALL RULES

6.1 Incoming Services to LAN Hosts

a) *Samras UAT Portal*

The Samras UAT Portal gives the public access to their Municipal accounts. The web services on the Samras UAT Portal public IP address must be forwarded to the internal Samras UAT web server.

Source	Destination	Protocol(s)	Port	Action
WAN	Firewall - Samras UAT IP Address	TCP	443	Forward to Samras server

b) *Reverse Web Proxy*

The reverse web proxy must be hosted in the DMZ and access to http and https ports must be allowed in all zones.

Source	Destination	Protocol(s)	Port	Action	Comment
All zones	Reverse Proxy	TCP	80	Accept	HTTP
All zones	Reverse Proxy	TCP	443	Accept	HTTPS

Where possible external access to web services for any internal web server should be routed via the reverse web proxy. This adds an additional layer of security.

Further to this, internal http services should, where possible, be encrypted by the reverse web proxy and delivered to the public as https using a valid SSL certificate.

The following is a list of these web services:

Public Hostname	Action	Comment
intranet.swellendam.gov.za	Proxied to Zimbra Server	Zimbra E-mail and collaboration server.
intranet.swellendam.gov.za/hel pdesk	Proxied to the ICT helpdesk server	ICT Helpdesk and asset management system.
intranet.swellendam.gov.za/mu nlogos	Proxied to the local webserver on which the reverse proxy is hosted	Logo images and related files are used in e-mail signatures.

c) *E-mail relay tunnel*

Incoming e-mails and outgoing mail are relayed through an external server hosted in the cloud. This is to protect the public addresses of the Municipality from being blacklisted in the event of a security breach that results in unsolicited e-mail being sent from the local mail server. The mail server must have access to the cloud-hosted mail relay server in order to establish the tunnel.

Source	Destination	Protocol(s)	Port	Action	Comment
Local Mail server	Cloud relay server 0 relay03.wirelessweb.co.za	TCP	6595	Accept	Secure tunnelling port

6.2 Outgoing Access

Access to services hosted outside the organization must be filtered and controlled. This section defines the types of services that internal hosts are allowed to access on the Internet and additional controls that should be applied for each category of service.

a) *Globally Allowed Outgoing Access*

The following services are allowed between all computers in the organization and the Internet:

- (i) SSH (TCP Port 22)
- (ii) Ping (ICMP Port 8)
- (iii) Traceroute (UDP Port 33434 to 33524 and ICMP Port 8)

b) Access to Internet websites

Internet websites should be categorized as best possible. Filtering policies must be defined which define the categories of websites that may be used and users must be connected to these policies.

Source	Destination	Protocol(s)	Port	Action	Comment
LAN	WAN	TCP	80	Allow, but apply filter policies	HTTP
LAN	WAN	TCP	443	Allow, but apply filter policies	HTTPS

c) Access to public NTP (Time) Servers

All local domain controllers should be able to update their time from any time server on the Internet.

Source	Destination	Protocol(s)	Port	Action	Comment
Domain Controllers	WAN	TCP/UDP	123	Allow	Time Services

d) Access to public DNS Servers

All local DNS servers should be able to query public DNS servers in order to serve name resolution queries to the local networks and to update their local DNS caches.

Source	Destination	Protocol(s)	Port	Action	Comment
Local DNS Servers	WAN	UDP	53	Allow	DNS

e) Sending and Receiving E-mail via External E-mail servers

The SAMRAS system sends accounts via an external SMTP server.

Source	Destination	Protocol(s)	Port	Action	Comment
SAMRAS	External E-mail Server Address	TCP	25	Allow	SMTP
SAMRAS	External E-mail Server Address	TCP	587	Allow	SMTP

f) Patch Management

The WSUS system requires internet access to download the latest patches.

Source	Destination	Protocol(s)	Port	Action	Comment
Security Server	Internet	TCP	80/443	Allow	HTTP and HTTPS

6.2 VPN Access

The following rules apply to VPN users dialled in via VPN:

a) Staff

Staff in the employ of the Municipality to whom VPN access has been granted must have full access to all resources in the LAN.

Source	Destination	Protocol(s)	Port	Action	Comment
VPN - Internal Users	LAN	All	All	Allow	
LAN	VPN - Internal Users	All	All	Allow	

b) ESRI Consultants

ESRI Consultants provide support on the GIS systems and may only have access to the internal GIS Servers.

Source	Destination	Protocol(s)	Port	Action	Comment
VPN - ESRI Consultants	GIS Servers	All	All	Allow	

c) Samras Consultants

Samras Consultants may only have access to the Samras servers.

Source	Destination	Protocol(s)	Port	Action	Comment
VPN - Samras Consultants	Samras Servers	All	All	Allow	

d) *Collaborator Consultants*

Collaborator Consultants may only have access to the Collaborator Servers.

Source	Destination	Protocol(s)	Port	Action	Comment
VPN - Collaborator Consultants	Collaborator Servers	All	All	Allow	

7. WEBSITE FILTERING POLICIES

7.1 Introduction

The default workspace policy will apply to all users by default. An approval process must be in place to allow users to request access to sites that are not allowed in the default policy.

7.2 Logging

All websites visited by all users must be logged.

7.3 Globally allowed websites

The following is a list of websites and website categories that everyone should have access to:

Site/Category	Description
Intranet Sites	All services provided by the organization to its employees.
Video Conferencing	Microsoft Teams and Zoom Video Conferencing.
Webmail	private email e.g. gmail.

7.4 Default Policy

By default access to all websites is granted except as defined below.

a) *Default Policy - Blocked content*

By default, the following categories of websites should be blocked:

Category	Description	Reason
Anonymizers	Sites offering Online translation of URLs. These sites access the URL to be translated in a way that bypasses the proxy server, potentially allowing unauthorized access	Security Risk and potentially allow users to circumvent company policies.
Criminal Activity	Advocating, instructing, or giving advice on performing illegal acts such as phone, service theft, evading law enforcement, lock-picking, burglary techniques and suicide	Illegal content.
Hacking	Sites that provide information about or promote illegal or questionable access to or use of computer or communication equipment, software, or databases.	Security Risk. Legal Risk.
Games	Sites providing information about or promoting electronic games, video games, computer games, role-playing games, or online games	Unproductive.
Nudity	Sites depicting nude or seminude human forms, singly or in groups, not overtly sexual in intent or effect. It includes Nude images of film stars, models, nude art and photography	Inappropriate workplace conduct.
Peer-to-peer & torrents	Peer-to-Peer Activity	Primarily used for illegal downloads. Allow remote access to internal resources. Imposes legal and security risks. Negative impact on network bandwidth.

Category	Description	Reason
Personal Network Storage	Websites that permit users to utilize Internet servers to store personal files or for sharing, such as with photos.	Against policy.
Phishing and Fraud	Sites gathering personal information (such as name, address, credit card number, school, or personal schedules) that may be used for malicious intent	Security Threat.
Sexually Explicit	Adult sites not falling in "Porn, Nudity, Swimwear & Lingerie, Sex Education, and Sexual Health & Medicines" will be included in "Adult Content" and which may contain material not suitable to be viewed by audiences under 18	Inappropriate workplace conduct.
Social Networking	Dedicated Web sites to communicate informally with other members of the site, by posting messages, photographs, etc.	Unproductive.
Video Hosting	This category includes URLs that provide video searches.	Unproductive.
Video Streaming	Subscription Video Streaming	Unproductive.

7.5 Default Policy exceptions

The following policies are exceptions to the default policies. All the rules defined in the default policy will apply to users to whom these policies are applied, except for the exceptions defined below:

a) *Media Access*

This policy is designed for people in the organisation that require social media access to perform their duties.

Default Policy Exceptions

Social Networking

b) *Social Media and Streaming Access*

This policy is designed for people in the organisation that require social media access and access to media streaming to perform their duties.

Default Policy Exceptions
Social Networking
Video Hosting

c) *Social Media and Cloud Storage*

This policy is designed for people in the organisation that require social media access and access to cloud storage services to perform their duties.

Default Policy Exceptions
Social Networking
Personal Network Storage

d) *Cloud Storage Access*

This policy is designed for people in the organisation that require access to cloud storage services to perform their duties.

Default Policy Exceptions
Personal Network Storage

e) *Streaming Access*

This policy is designed for people in the organisation that require access to video streaming services to perform their duties.

Default Policy Exceptions
Video Hosting

7.6 Unrestricted Policy

This policy is designed for people in the organisation for whom no default policy applies. For this policy, everything is allowed, except for the following:

Blocked Categories
Criminal Activity

Nudity
Sexually Explicit

8 FIREWALL MANAGEMENT

The IT Department is responsible for implementing and maintaining Swellendam Municipality firewalls.

Swellendam Municipality has contracted with an IT service provider to manage the external firewalls. This service provider will be responsible for:

- a) Configuration of firewalls
- b) Firewall rule management
- c) Retention of the firewall rules
- d) Patch Management
- e) Review the firewall logs for system errors
- f) Blocked web sites
- g) Attacks
- h) Sending alerts to the IT Manager and CFO in the event of attacks or system errors
- i) Backing up the firewalls

Firewall rule management is the process of periodically reviewing and optimizing firewall rules. This process involves the following:

- a) Analyzing rule anomalies that affect the performance of the firewall.
- b) Reordering existing rules to improve rule performance.
- c) Identifying and removing unused rules.
- d) Analyzing the impact of a new rule on the existing rule set before making it live in the firewall.
- e) Recording the date the rule was added/change in a register.
- f) Recording the name of the person who added/change the rule set.

Emergency Firewall Rule management changes must be submitted to the CFO for approval. Other Firewall Rule changes will be sent to the IT steering committee for consideration and update of the firewall rule policy.

9 SHORT TITLE

This policy is called the ICT Firewall Rules Policy of the Swellendam Municipality and will be reviewed annually.