Fetakgomo Local Municipality

Council Resolution No. C43/2014

ICT FIREWALL POLICY

27 February 2014

Table of Contents

1. Introduction

Firewall is an essential component of any organization's information systems security infrastructure. The firewall is an appliance (a combination of hardware and software) or an application (software) designed to control the flow of Internet Protocol (IP) traffic to or from a network or electronic equipment. It is used to examine network traffic and enforce policies based on instructions contained within the Firewall's ruleset. Firewalls represent one component of a strategy to combat malicious activities and assaults on computing resources and network-accessible information. Other components include, but are not limited to, antivirus software, intrusion detection software, patch management, strong passwords/passphrases, and spyware detection utilities. Firewalls are typically categorized as either "Network" or "Host": a Network Firewall is most often an appliance attached to a network for the purpose of controlling access to single or multiple hosts, or subnets; a Host Firewall is most often an application that addresses an individual host (e.g., personal computer) separately. Both types of firewalls (Network and Host) can be and often are used jointly. Firewalls are defined as security systems that control and restrict the local area network, Internet connectivity and Internet usage services. Firewalls establish a parameter where access controls are enforced.

2. Audience

This policy is applicable to all user(s), departments, and divisional units that cause Electronic Equipment to be connected to the Fetakgomo Local Municipality network.

3. Terms and Definitions

Electronic Equipment: All Municipality-owned or issued and any personally-owned computer or related equipment (e.g., servers, workstations, laptops, PDAs, printers, fax and other such devices) that attaches to the Fetakgomo Municipality's network, or is used to capture, process or store Municipality data, or is used in the conduct of Municipality business.

Enterprise System: Applicable to any infrastructure as a means of describing its importance to the Mucipality's mission and how it should be administered, protected and funded. From a functional viewpoint, an Enterprise System will be either
(a) the only delivery platform for an essential service, or
(b) A platform for a service to a very broad constituency spanning organizational boundaries. An Enterprise System is most frequently administered and protected by an institutional unit with expertise in both the technology and the business functions delivered.

Firewall: Any hardware and/or software designed to examine network traffic using policy statements (ruleset) to block unauthorized access while permitting authorized communications to or from a network or electronic equipment.

Firewall Administrator: The Municipality function charged with the responsibility of Firewall Configuration and/or ruleset administration. Administrative duties typically include implementation and documentation of approved changes, analysis of activity logs, and execution and documentation of reviews of system settings and/or rulesets.

Firewall Configuration: The system settings affecting the operation of a firewall appliance.

Firewall Ruleset: A set of policy statements or instructions used by a firewall to filter network traffic.

Host: Any computer connected to a network.

Host Firewall: A firewall application that addresses a separate and distinct host. Examples include, but are not limited to: Symantec's Norton Personal Firewall, Zone Labs' ZoneAlarm, native firewall functionality supplied under operating systems, e.g., Mac OS XI, Linux, Windows 7 SP2 (and higher).

Internal Information: Information that is intended for use by and made available to users of the Fetakgomo Local Municipality who have a business needs to know. This information is not restricted by local, state, national, or international statute regarding disclosure or use. Internal information is not intended for public dissemination but may be released to external parties to the extent there is a legitimate business need. The Municipality reserves the right to control the content and format of Internal information when it is published to external parties. Examples include employment data, financial expenditure detail, Job Evaluations, and Directory Information (not subject to a FERPA hold).

Legally/Contractually Restricted Information: Information that is required to be protected by applicable law or statute (e.g., HIPAA, FERPA, or the Illinois Personal Information Protection Act), or which, if disclosed to the public could expose the Municipality to legal or financial obligations. Examples include, but are not limited to, occurrences of personally-identifiable information, e.g., employee salary information, personnel records, medical records. Specific Municipality policies may apply to particular data in this classification, e.g., Secure Handling of employee Salary information, Security of Electronic Protected Health Information, etc.

Network Device: Any physical equipment attached to the Municipality network designed to view, cause or facilitate the flow of traffic within a network. Examples include, but are not limited to: routers, switches, hubs, wireless access points.

Network Extension: Any physical equipment attached to the Municipality network designed to increase the port capacity (number of available ports) at the point of attachment. Examples include, but are not limited to: routers (wired and wireless), switches, hubs, gateways.

Network Firewall: A firewall appliance attached to a network for the purpose of controlling traffic flows to and from single or multiple hosts or subnet(s).

Public Information: Information that is available to all users of the Fetakgomo local Municipality, and may be released to the general public. The Municipality reserves the right to control the content and format of Public Information. This information is not restricted by local, provincial, national, or international statute regarding disclosure or use. Examples include the Municipality's auditable financials, schedule of IDP, and Managerial Strategic planning meetings.

Sensitive Data: See "Legally/Contractually Restricted Information" above.

Municipality Network: The network infrastructure and associated devices provided or served by the Municipality.

FTP (File Transfer Protocol): a standard Internet protocol that allows users to transfer files from one computer to another over a network.

HTTP (Hypertext Transfer Protocol): set of rules for transferring files (text, graphic images, sound, video and other multimedia files) on the World Wide Web.

Security device: Hardware or software that provides security services.

Inbound Traffic: Traffic coming into Local Area Network

Outbound Traffic: Traffic going out of Local Area Network

Exploitation: The process of obtaining intelligence information from any source and taking advantage of it.

Perimeter Firewall: a Firewall installed between a private network and public networks, such as the Internet.

Network security: refers to any activities designed to protect network, especially the usability, reliability, integrity and safety of the network and data.

Network Security Architecture: a subset of network architecture specifically addressing network security.

Security Functionality: are the security-related features or functions employed within an information system or the infrastructure supporting the system.

IT Security Requirements: describe functional and non-functional requirements that need to be satisfied in order to achieve the security attributes of an IT system.

Remote Access Points (RAPs): provide secure always-on network access to corporate enterprise resources from remote locations.

Data: a minimal piece of information that need to be translated into a form that is more convenient to move or process.

VPN (Virtual Private Network: A virtual private network (VPN) is a network that uses a public telecommunication infrastructure and their technology such as the Internet, to provide remote offices or individual users with secure access to their organization's network

Proxy server: is a computer that acts as a gateway between a local network and a large –scale network such as the Internet. Proxy servers provide increased performance and security.

Database: is a collection of information that is organized so that it can easily be accessed, managed and updated.

TCP/IP: a set of protocols (including TCP) developed for the internet in the 1970s to get data from one network device to another

Authentication: a systematic method of confirming the identity of an individual or system

Service: is a long-running executable that performs specific functions and which is designed not to require user intervention.

Traffic: is data in a network. In computer networks, the data is encapsulated in packets

Threat: is a possible danger that might exploit a vulnerability to breach security and thus cause possible harm.

Vulnerability: is a weakness which allows an attacker to reduce a system's information assurance

SITA: is a state information technology agency which mandated among others not limited to the IT business for the largest employer and consumer of IT products and services in South Africa – the Government.

4. Purpose

The purpose of this ICT Firewall Policy is to allow or block unauthorized network or Internet devices and services sending traffic or receiving traffic over a network. To define standards for provisioning security devices owned and/or operated by FETAKGOMO To prevent exploitation of insecure services, restrict inbound/outbound traffic from unregistered devices, control inbound/outbound access to/from specific services or devices and monitor traffic volumes.
To provide guidance on when firewalls are required or recommended. A Network Firewall is required in all instances where Sensitive Data is stored or processed; a Host Firewall is required in all instances where Sensitive Data is stored or processed and the operating environment supports the implementation. Both the Network and Host Firewalls afford protection to the same operating environment, and the redundancy of controls (two separate and distinct firewalls) provides additional security in the event of a compromise or failure.
Raise awareness on the importance of a properly configured (installed and maintained) firewall.

5. Scope

This policy defines the essential rules regarding the management and maintenance of Firewall at Fetakgomo local Municipality and it applies to all users that use computers and the network of Fetakgomo Municipality.

6. Policy statement

The Municipality of Co-Operative Governance, Human Settlement and Traditional Affairs operate perimeter firewalls between the Internet and the municipality network in order to establish a security environment for the municipality's Information Technology resources. Fetakgomo Municipality perimeter firewalls are a key component of the overall municipality's Network Security Architecture. This ICT Firewall policy governs how the perimeter Firewalls will filter Internet traffic to mitigate risks and possible losses associated with security threats to the networks and information systems. Where Electronic Equipment is used to capture, process or store data identified as Municipality "Legally/Contractually Restricted" and the Electronic Equipment is accessible via a direct or indirect Internet connection, a Network Firewall appropriately installed, configured and maintained is **required**.

All installations and implementations of and modifications to a Network Firewall and its Configuration and Ruleset are the responsibility of the authorized State Information Technology Agency(SITA) Firewall Administrator, with this exception: maintenance of a Network Firewall Ruleset may be performed by other than Fetakgomo IT personnel where permitted by a documented agreement between SITA and Fetakgomo IT Unit /Department/Divisional Unit assuming the Firewall Administrator's responsibilities.

Where Electronic Equipment is used to capture, process or store data identified as Municipality "Legally/Contractually Restricted" and the Electronic Equipment is accessible via an Internet connection, a Host Firewall appropriately installed, configured and maintained is **required** where the operating environment supports that installation. The maintenance of the Host Firewall's Configuration and Ruleset is the responsibility of that SITA.

Where Electronic Equipment is used to capture, process or store data identified as Municipality "Internal" or "Public" and the Electronic Equipment is accessible via an Internet connection, a Host and/or Network Firewall is **recommended**.

Use of a Host Firewall is **recommended** for any individual Host with access to the Fetakgomo's Internet; its maintenance is the responsibility of the IT personnel or designated support personnel.

7. Requirements

7.1 The Firewall system shall control all traffic entering and leaving the Fetakgomo Municipality Internal network.

7.2 Fetakgomo Municipality Firewall shall block all incoming and outgoing traffic by default.

7.3 Only authorized incoming and outgoing traffic shall be allowed to pass through Fetakgomo Municipality Firewall.

7.4 Traffic with invalid source or destination addresses shall always be blocked.

7.5 Traffic with an invalid source address for incoming traffic or destination address for outgoing traffic (an invalid "external" address) shall be blocked at the network perimeter.

7.6 Traffic with a private destination address for incoming traffic or source address for outgoing traffic (an "internal" address) shall be blocked at the network perimeter.

7.7 Outbound traffic with invalid source addresses shall be blocked.

7.8 Incoming traffic with a destination address of the firewall itself shall be blocked unless the firewall is offering services for incoming traffic that require direct connections.

7.9 Traffic from outside the network containing broadcast addresses that are directed to inside the network shall be blocked.

8. Operations

8.1 Only Firewall system administrators shall be permitted to logon to Firewall hosts. Access to Firewall hosts shall be tightly controlled. Only Firewall system administrators are allowed to have user accounts on Firewall hosts. Firewall system administrators shall have personal accounts; i.e. no group logins are allowed.

8.2 All changes to Firewall access rules shall be made through a single approved interface. The Firewall shall have a trusted path for its management e.g. a physically secure dedicated management process with a password-based identification and authentication system.

8.3 Only personnel with the appropriate authorization shall make changes to the Firewall access rules, software, hardware or configuration. All changes shall be as a result of a request recorded in a Change Management System although emergency modifications can be requested by phone, with a follow up email and change request. Only authorized personnel must be able to implement the changes and an audit log must be retained.

8.4 Logging and audit facilities provided by the Firewall system shall be fully utilized. All significant traffic through the Firewall shall be logged. The Firewall shall provide sufficient audit capacity to detect breaches of the Firewall's security and attempted network intrusions. Firewall System Administrators shall examine logs on a regular basis and also set up mechanisms to respond to alarms.

8.5 Fetakgomo employees may request changes to the firewall's configuration in order to allow previously disallowed traffic. A **firewall change request form**, with full justification, must be submitted to the IT Unit for approval. All requests will be assessed to determine if they fall within the parameters of acceptable risk. Approval is not guaranteed as associated risks may be deemed too high. If this is the case, an explanation will be provided to the original requestor and alternative solutions will be explored.

8.6 Fetakgomo employees may request access from the Internet for services located on the internal network. Typically, this remote access is handled via a secure, encrypted virtual private network (VPN) connection. VPN sessions will have an absolute timeout length of 1 day. An inactivity timeout will be set for 1 day. At the end of these timeout periods, users must re-authenticate to continue or re-establish their VPN connection. VPN connectivity request form, with full justification, must be submitted to the IT Unit for approval. Approval is not guaranteed. From time to time, outside vendors, contractors, or other entities may require secure, short-term, remote access to Fetakgomo local Municipality's network. If such a need arises, a third-party access request form, with full justification, must be submitted to the IT Unit for approval. Approval is not guaranteed.

9. Configuration

9.1 The perimeter Firewall system shall be configured to deny any service unless it is expressly permitted. If there are no rules defined for the municipality network address, then traffic to or from that address shall be denied. Access to the municipality network shall be blocked during the start-up procedure of the Firewall.

9.2 The Firewall operating system shall be configured for maximum security. The underlying operating system of Firewall hosts shall be configured for maximum security, including the disabling of any unused services.

9.3 The Firewall product suite shall reside on dedicated hardware. Applications that could interfere with, and thus compromise, the security and effectiveness of the Firewall products, shall not be allowed to run on the host machine.

9.4 The initial build and configuration of the Firewall shall be fully documented. This provides a baseline description of the Firewall system to which all subsequent changes can be applied. This permits tracking of all changes to ensure a consistent and known state is maintained.

9.5 Security shall not be compromised by the failure of any Firewall component. If any component of the Firewall fails, the default response will be to immediately prevent any further access, both outbound as well as inbound. A Firewall component is any piece of hardware or software that is an integral part of the Firewall system. A hardware failure occurs when equipment malfunctions or is switched off. A software failure can occur for many reasons e.g. bad maintenance of the rules database on the Firewall or software which is incorrectly installed or upgraded.

9.6 There shall be regular reviews to validate the Firewall system meets the needs of the business regarding information security. The configuration of the Firewalls shall be regularly checked to ensure they still match the business requirements regarding the security. It may be necessary to implement separate Firewall modules to protect against the vulnerabilities of certain services. An example would be a package to scan email for viruses or other malicious software. The Firewall must also be regularly tested for vulnerabilities. Applications on internal hosts that handle incoming services will need to be checked for known vulnerabilities.

10. Audit and compliance

10.1 Regular testing of the Firewall shall be carried out. The Firewall shall be regularly tested for;

- Configuration errors that may represent a weakness that can be exploited by those with hostile intent.
- Consistency of the Firewall rule set.
- Secure base system implementation

10.2 The Firewall system shall have an alarm capability and supporting procedures. When an agreed specified event occurs, an alarm shall be sent to the security team. Documented procedures shall exist to permit an efficient response to such Firewall security alarms and incidents. In the event that the Firewall itself is the subject of malicious attempts to penetrate it and the Firewall has the capability, delivery of services should be terminated rather than permit uncontrolled access to the municipality network.

10.3 There shall be an active auditing/logging regime to permit analysis of Firewall activity both during and after a security event. An audit trail is vital in determining if there are attempts to circumvent the Firewall security. Audit trails must be protected against loss or unauthorized modification. The Firewall system must be able to provide logging of specific (or all) traffic when suspicious activity is detected.

11. Responsibilities

IT Unit will be the sole responsible entity for putting in place firewalls and the management thereof. The monitoring will be done by IT Unit and reported to Risk and Security management if any breach attempts are detected.

12. Change control

With any Firewall it is very important to have change control. When rules are introduced there should be a well-defined method for documenting these and in the case of temporary rules, the removal date for the rule should be added in a comment field. The only way of checking if the Firewall is actually enforcing the agreed policy is to either verify it with an Intrusion Detection System, or to do a manual verification using a penetration test or a Firewall review by third party.

13. Monitor stability

A Firewall is like any other infrastructure component and should be managed as such. It should be monitored for availability to ensure maximum uptime. If a Firewall isn't stable, people will find ways of avoiding the Firewall that leads to a low level of security.

14. Enforcement

IT Unit is responsible for enforcing this policy and continuously ensuring monitoring and compliance. Wherever possible, technological tools will be used to enforce this policy and mitigate security risks.

15. Consequences for Non-Compliance

Any employee who may found to have violated this policy may be subject to disciplinary action.

16. Policy Review

This policy shall be reviewed annually.

17. Implementation

This policy comes into effect from the date of approval.

C 43/2014

Council Resolution No.

31st March 2014

Date

Mamphekgo K.K

The Speaker

31.03.2014

Date