

Firewall Policy

Version 2.0 / 2014



Waterberg
District Municipality

on the Go for Growth

Table of Contents

Firewall Policy Scope and Compliance Requirements.....	3
Firewall Policy Enforcement.....	3
Perimeter Security Maintenance.....	3
Firewall Logon Access.....	3
Firewall Operational Maintenance and Responsibility.....	4
Firewall Log Configuration and Maintenance.....	4
Firewall(s) Security Services.....	4
Firewall Rule Set Management and Change Control Process.....	5
Firewall Application Traffic Ruleset Matrix.....	6
Network Connection Policy	8
Trusted Networks Policy	8
Non-trusted Networks Policy.....	9
Periodic Review of Firewall Security Policies	9

Firewall Policy For Waterberg District Municipality

Firewall Policy Scope and Compliance Requirements

These guidelines are intended to supplement, not replace all existing laws, regulations, agreements, and contracts that currently apply to institutional computing and networking services. Persons given access to the department's technology and information assets must sign a statement that they have read, understood, and agree to abide by this policy.

Firewall Policy Enforcement

Security policy enforcement will emphasize the use of security technology mechanisms to mitigate security risks wherever possible. When actual prevention is not enforceable with security tools, sanctions will be used.

Perimeter Security Maintenance

Perimeter security for this department will be maintained by a firewall. The firewall will inspect packets and sessions to determine if they should be transmitted or dropped. In effect, the firewall will act a single point of network access where traffic can be analyzed and controlled. Access to the department's internal network will be based on parameters such as (but not limited to):

- Application use.
- User authentication, authorization, and accounting, for both incoming traffic from remote users and outgoing traffic to the Internet.
- IP Address and port

Firewall Logon Access

Enable or privileged logon access to the firewall will be restricted to the Network Administrator. Enable password construction will be consistent with the strong password creation practices utilized in the department.

Firewall Operational Maintenance and Responsibility

Day-to-Day operation and maintenance will be the responsibility of the department's Network and Security Engineer (or assigned position). Firewall support duties for the Network and Security Engineer include:

- Act as the departmental technical lead for departmental security policy and procedure implementation, has the primary responsibility for ensuring operational continuity for the department's security policy.
- Perform firewall rule set changes, adds and deletions as approved by the departmental security committee.
- Perform firewall software maintenance and hardware upgrades to the firewall.
- Monitor firewall logs.
- Initiate the department's response to any possible security incident.
- Perform security risk management by initiating a cycle of securing, monitoring, and testing security mechanisms and procedures. Review findings will be used to update security policy, procedures, and security mechanisms on a continual basis.
- Launch annual review of the departmental firewall policy to ensure the firewall policy is current with actual firewall rule set practices.

Firewall Log Configuration and Maintenance

The firewall will be configured to use system logging. At a minimum, the firewall log will be configured to detect:

- Emergencies, such as system unusable messages
- Alerts, critical conditions, and Error message
- VPN sessions,
- Failed/unsuccessful login attempts
- Logon Access and configuration attempts made to the firewall

The firewall logs will be backed up daily and archived on a weekly basis, in accordance with current data backup practices.

Firewall(s) Security Services

At a minimum, the departmental firewall(s) will perform the following security services:

- Access control between the internal network and un-trusted networks.

- Block unwanted traffic, as determined by firewall rule sets designed to implement the department's Security Policy while providing security that does not place an undue burden on authorized users.
- Hide system names, network topology, network device types, and internal user ID's from the Internet.
- Provide more robust authentication (RADIUS/TACACS+) than standard applications.
- IPSEC VPN Connectivity.
- Log interesting traffic to and from the department's internal network.

Firewall Rule Set Management and Change Control Process

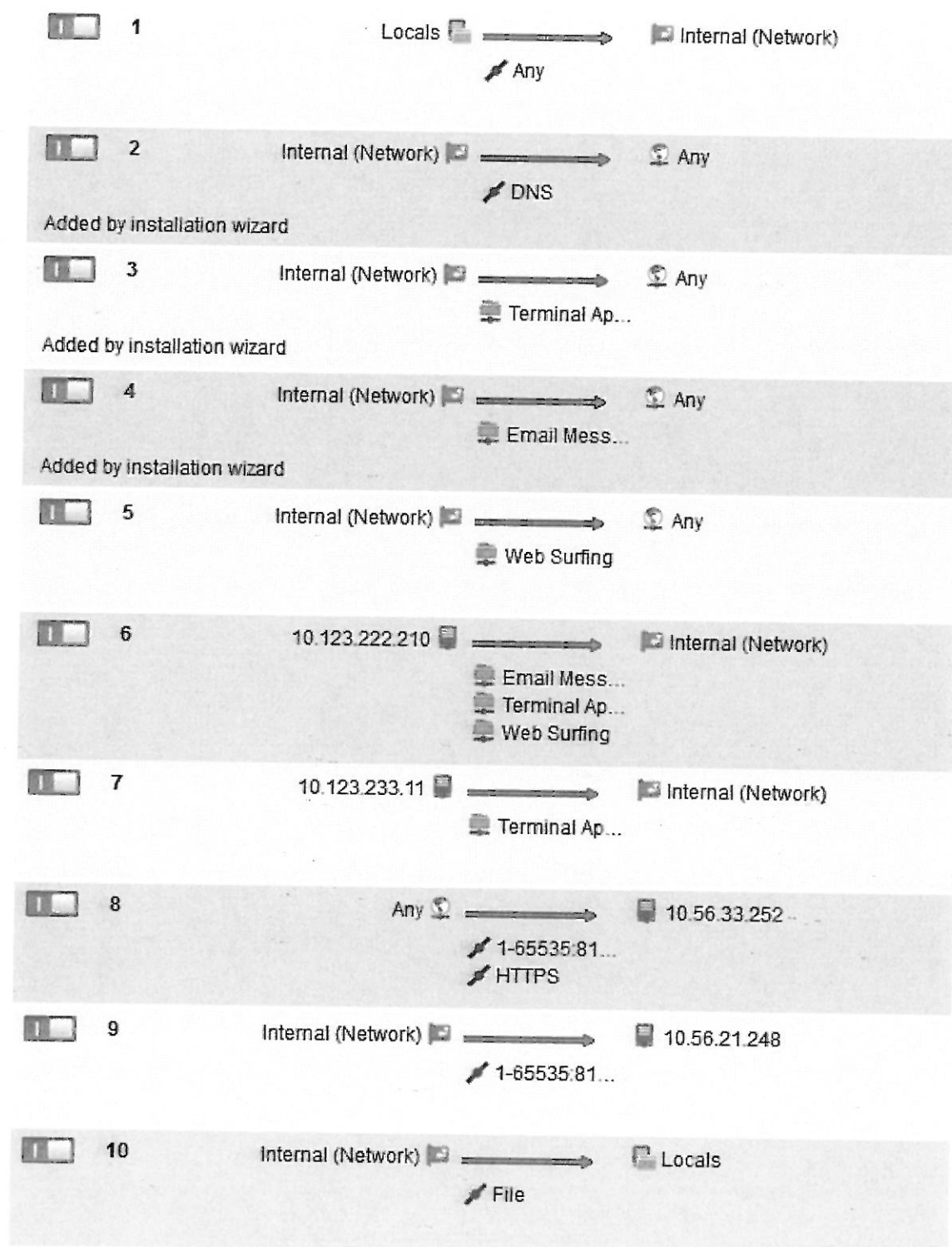
The departmental security committee must approve all rule set (ACL's) changes. The departmental security committee must approve all changes and upgrades. At a minimum, the following information will be included in any firewall change request.

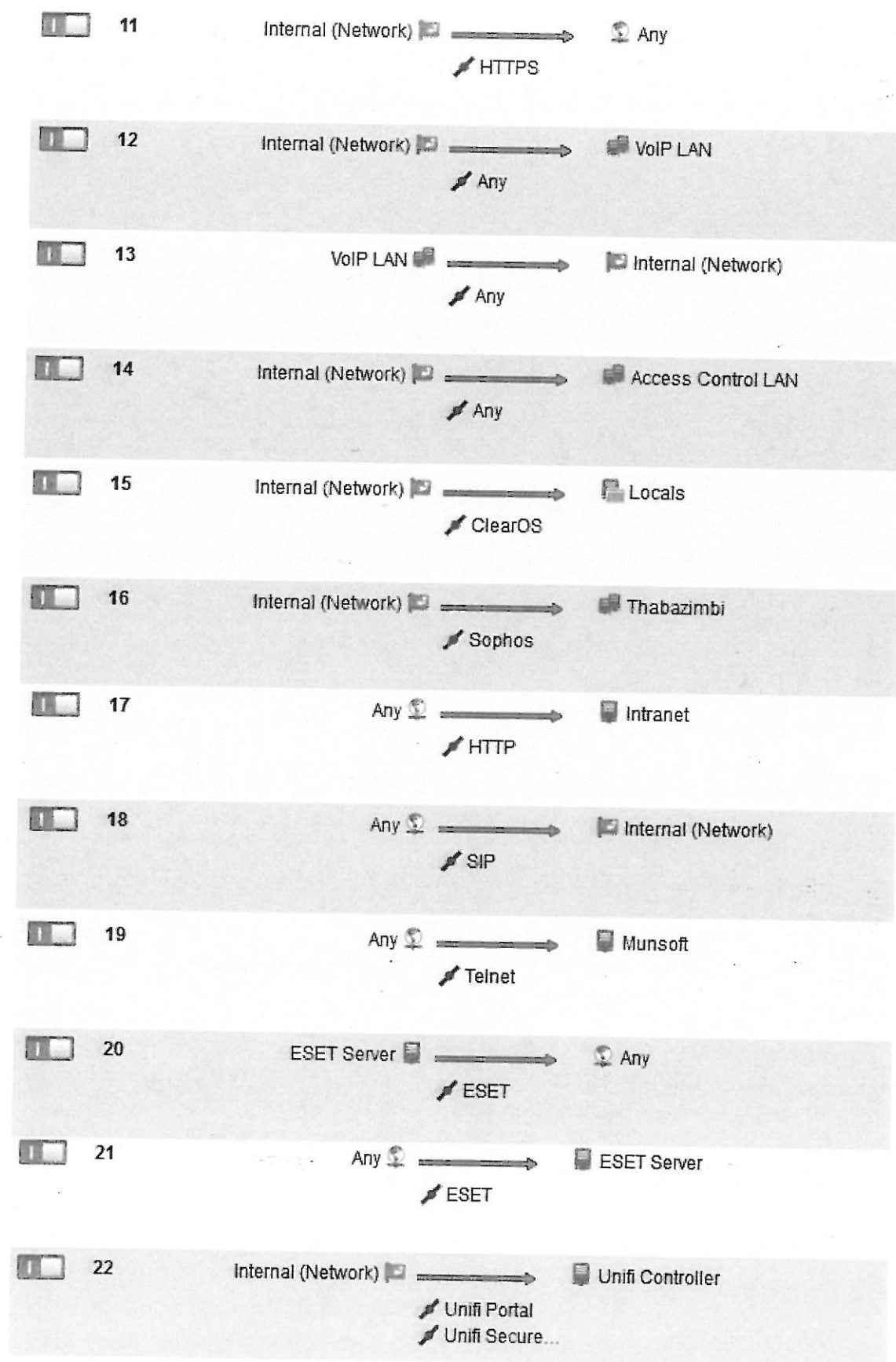
- Requesters Name
- Requested Due Date (when change will be applied)
- Change impact statement. Include any supporting documentation necessary to determine why the change is necessary. The change request will be delayed until change requirement has been established and approved.
- Rule Change Notification requirements (who need to be alerted about the change because of potential operational impact).
- Change Priority Level
 - 1 -emergency change needs to go in ASAP because of possible security breach
 - 2- Change will be applied as scheduled, upon security committee approval

Firewall rule sets (ACL's) will work to achieve a "best practices" approach in an effort to balance security risk and operational access requirements. Recommended practices include:

- Anything from inside the network is allowed out.
- All access to the firewall itself is blocked from the Internet.
- Restricted internal access to the firewall. Firewall administrators must be validated by two-factor authentication, such as SECURID.
- Allow SMTP e-mail support.
- ICMP services turned off
- Block FTP and Telnet access to all internal servers from the Internet.
- Remote access services for authorized users via VPN and/or approved secure authentication system.

Firewall Application Traffic Ruleset Matrix





Network Connection Policy

The Security Committee must approve all connections from the department network to any external networks. Only network connections that have been found to have acceptable security controls and procedures will be allowed to connect to the departmental network. Every attempt will be made to ensure that all external connections will pass through firewalls that meet the guidelines established by this policy. All connections and accounts related to external network connections shall be validated on an annual basis. When a network connection is no longer needed all accounts and system processes related to the connection should be deleted within one workweek.

Trusted Networks Policy

Network Trust Relationships Overview Approved and authorized network connections are considered trusted networks. Trusted networks share the similar security policy or implement security controls and procedures.

Un-trusted networks do not implement common security controls, or where the level of security is unknown or unpredictable. Network segments external to the department are under the control of different organizational entities, and will be considered as unknown and possibly compromised

The following networks are considered trusted networks and permitted **controlled access** by the department firewall(s). These networks are provided data services by the department's network:

The NGN (Next Generation Network) Backbone Network

This network contains the Parent firewall that separates the NGN from the Internet and also interconnects all of the Institute networks together through switches and routers.

Waterberg District Municipality LAN (10.56.33.0)

This network hosts the 10.56.33.0 range. The LAN interconnects WDM Head Office, Modimolle Abattoir and Modimolle Disaster Management Centre.

Waterberg District Municipality VoIP (172.1.1.0)

This network hosts the 10.56.33.0 range. It is utilized by the IP PBX and IP telephones.

Waterberg District Municipality CCTV (192.168.0.0)

This network hosts the 192.168.0.0 range. It is utilized by the IP CCTV system.

Non-trusted Networks Policy

All networks not specifically listed as a trusted network are non-trusted networks. Access to the department's network will be denied by the firewall(s). If complete access control cannot be managed by the firewall(s), other security technologies will be used in tandem to the department's firewalls to mitigate the security threat. Modem connections with business partners and/or remote sites are also considered un-trusted networks connections. The Network and Security Engineer may terminate unauthorized connections to departmental network without notice. An active network port or connection does not imply authorization for connectivity. To support this policy, unused and/or unknown network connections (switch ports, analog lines, etc.) will be disabled until they are properly identified, documented, and placed in or out of service.

Periodic Review of Firewall Security Policies

Firewall security policies will be reviewed yearly. When there are major changes to the network requirements this may warrant changes to the firewall security policy.

Changes include events such as the implementation of major enterprise computing environment modifications and any occurrence of a major information security incident.

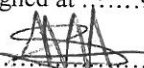
When new applications are being considered, a security review committee will evaluate new services before the firewall administrators are formally notified to implement the service. Alternatively, when an application is phased out or up-graded, the firewall ruleset should be formally changed where appropriate.

(This approach helps to minimize the presence of old and potentially insecure rules that are no longer needed.)

Firewall installations will be audited on a regular, periodic basis. These periodic reviews can be conducted on paper by reviewing hard-copy configurations provided by appropriate systems administration staff. In other cases, periodic reviews should involve actual audits and vulnerability assessments of the firewall.

Adopted by Council at its meeting held on 17 June 2015 per Council Resolution Number A250/2015

Signed at Modimolle on 22 June 2015


.....
Municipal Manager