Information Communication and Technology (ICT) Firewall Policy

Matjhabeng Local Municipality

(MLM)

Table of Contents

1. INTRODUCTION

Information and systems security have become increasingly important to the municipality. Driven by technological changes and current and new regulatory changes. Information security is one of the main issues in the current municipality ICT infrastructure and IT systems. The Firewall is one of the key parameters gatekeepers in the IT Security and infrastructure that maintains and up hold the integrity of IT systems.

2. SCOPE

This policy applies to all Firewalls within the MLM. This is managed either by third parties or by internal assigned IT professionals. Deviations from this policy will be done in accordance to Policy, in writing and authorised by the ICT Manager. All MLM systems playing the role of firewalls, whether they are formally called firewalls, must be managed according to the rules defined in this policy. In some instances, this will require that these systems be upgraded so that they support the minimum functionality defined in this policy.

3. REQUIREMENTS

Prior to deployment of any Firewall at and MLM offices there has to be a diagram reflecting the permissions' path. This will also consist of the jurisdiction on each on these pathways, a description of each pathway, and must be submitted to the ICT manager. This is also the training to the level of administrators of the PaloAlto to a competent level to manage the system within the confines of the MLM council.

4. TECHNICAL EDUCATION

Members that administer the firewall system must be a competent level of understanding and education in order to manage and run the administrative roles required in this position.

5. DEFAULT AND DENIAL

Every connectivity path and service that is not specifically permitted by this policy and supporting documents issued by the ICT department must be blocked by MLW firewalls.

The list of currently approved paths and services

- Must be documented and distributed to all system administrators with a need to know by the ICT department.
- The IT department must maintain an inventory of all access paths in and out of MLM internal networks.

6. CONNECTIONS BETWEEN MACHINES

Real-time shared connections between two or more MLM computer systems must not be established or enabled unless the ICT department has determined that such connections will not jeopardize information security and must be filtered through the Firewall. This requirement applies no matter what technology is used, including wireless connections, microwave links, cable modems, integrated services digital network lines, and digital subscriber line connections. Any connection between an in-house MLM production system and any external computer system, or any external computer network or service provider, must be approved in advance by the ICT department.

7. REGULAR TESTING

Because firewalls provide such an important control measure for MLM networks, their strength and proper configuration must be tested on a regular basis. Where vendor software supports it, this testing must include the use of software agents that automatically check to determine whether firewalls remain configured and running in a manner that is consistent with both MLM security policies and the MLM Information Architectural plan. The vendor has to also provide the training for the skills required to administer the system. This testing process must include consideration of defined configuration parameters, enabled services, permitted connectivity paths, current administrative practices, and adequacy of the deployed security measures, bypass processes. These tests must include the regular execution of vulnerability identification software and the regular performance of penetration tests. These tests must be performed by technically proficient persons, either in the ICT department or working for a third-party contractor. Those responsible for either the administration or management of the involved firewalls must not perform these tests.

8. LOGS

All changes to firewall configuration parameters, enabled services, and permitted connectivity paths must be logged. All suspicious activity that might be an indication of either unauthorized usage or an attempt to compromise security measures also must be logged. His integrity of these logs must be protected with checksums, digital signatures, encryption, or similar measures. These logs must be promptly removed from the recording systems and stored in a physically protected container for at least six months after the time they were recorded. These logs must be reviewed periodically to ensure that the firewalls are operating in a secure manner.

9. INTRUSION DETECTION

All MLM firewalls must include intrusion detection systems approved by the ICT department. Each of these intrusion detection systems must be configured according to the specifications defined by the ICT department. Among other potential problems, these intrusion detection systems must detect unauthorized modifications to firewall system files, and detect denial of service attacks in progress. Such intrusion detection systems must also immediately notify by pager the Technical staff that is in a position to take corrective action. All technical staff working on firewalls must be provided with remote access systems and privileges so that they can immediately respond to these incidents even when they are physically removed from the firewall.

10. CONTINGENCY PLANNING

The plans must be periodically tested to ensure that they will be effective in restoring a secure and reliable networking environment. Administrative staff members working on firewalls must prepare and obtain ICT Management approval for contingency plans that address the actions to be taken in the event of various problems including system compromise, system malfunction, system crash, system overload, and Internet service provider unavailability. These contingency plans must be kept current to reflect changes in the MLM information systems environment.

11. EXTERNAL CONNECTIONS

All in-bound real-time Internet connections to MLM internal networks or multi-user computer systems must pass through a firewall before users can reach a logon banner. The computer systems requiring firewall protection include web servers, electronic commerce servers, and mail servers. All personal computers with digital subscriber line or cable modem connectivity must employ a firewall approved by the ICT department. Wherever a firewall supports it, logon screens must have a notice indicating that the system may be accessed only by authorized users, users who log on represent that they are authorized to do so, unauthorized system usage or abuse is subject to disciplinary action including criminal prosecution, and system usage will be monitored and logged. No MLM computer system (This includes personal computers) may be attached to the Internet unless it is protected by a firewall

12. FIREWALL ACCESS PRIVILEGES

Privileges to modify the functionality, connectivity, and services supported by firewalls must be restricted to a few technically trained individuals with a business need for these same privileges. Unless permission from the ICT Manager has been obtained, these privileges must be granted only to individuals who are full-time permanent employees of MLM, and not to temporaries, contractors, consultants, or outsourcing personnel. All firewalls must have at least two staff members who are adequately trained to make changes, as circumstances require. Such training includes periodic refresher training course or conference attendance to permit these staff members to stay current with the latest developments in firewall technology and firewall operations. Care must be taken to schedule out-of-town ones so that at least one person capable of effectively administering the firewall is readily available at all times. In the event that a third party vendor/service provider is present then the said party will work/abide by the policy set out by MLM.

13. SECURED SUBNETS

Portions of the MLM internal network that contain sensitive or valuable information, such as the computers used by the Human Resources department, should employ a secured subnet. Access to this and other subnets should be restricted with firewalls and other access control measures. Based on periodic risk assessments, the ICT department will define the secured subnets required in the Information Architecture.

14. FIREWALL PHYSICAL SECURITY

All MLM firewalls must be located in locked rooms accessible only to those who perform authorised firewall management and maintenance tasks approved by the ICT Manager. The placement of firewalls in an open area within a general-purpose data processing center is prohibited, although placement within separately locked rooms or areas, which themselves are within a general data processing center is acceptable. These rooms must be equipped with alarms and an automated log of all persons who gain entry to the room.

15. DEMILITARIZED ZONES

All Internet commerce servers including payment servers, database servers, and web servers must be protected by firewalls, and be located within a demilitarized zone (DMZ), a subnet that is protected from the Internet by one or more firewalls. An internal network, such as an intranet, is also protected from the DMZ subnet by one or more firewalls.

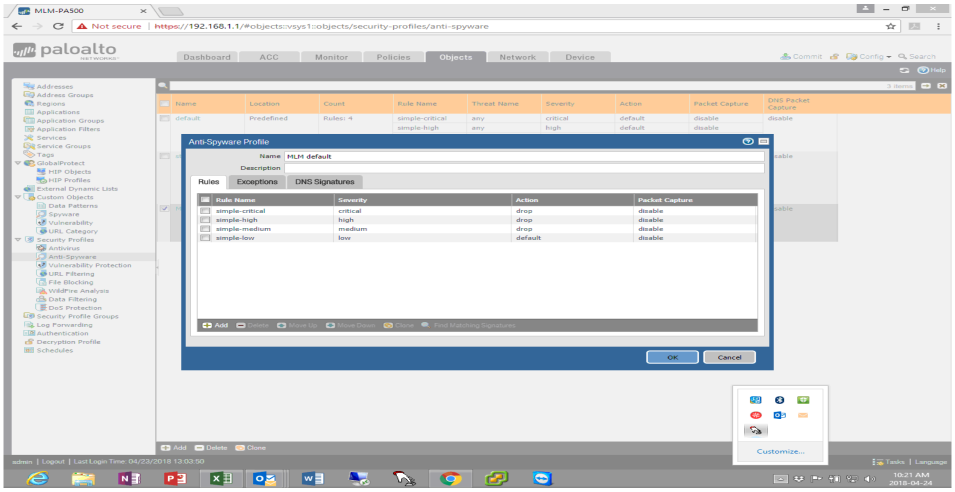
16. NETWORK MANAGEMENT SYSTEMS

Firewalls must be configured so that they are visible to internal network management systems. Firewalls also must be configured so that they permit the use of remote automatic auditing tools to be used by authorized MLM staff members. Unless deliberately intended as a test, such automatic auditing tools must not trigger a response sequence through firewall-connected intrusion detection systems.

17. DISCLOSURE OF INTERNAL NETWORK INFORMATION

The internal system addresses, configurations, products deployed, and related system design information for MLM networked computer systems must be restricted such that both systems and users outside the MLM internal network cannot access this information.

MLM Predefined Anti Spyware



Name	Location	Count	Rule Name	Threat Name	Severity	Action	Packet Capture	DNS Packet Capture
default	Predefined	Rules: 4	simple-critical	any	critical	default	disable	disable
			simple-high	any	high	default	disable	

Anti-Spyware Profile

Name: MLM default

Description:

Rules | Exceptions | DNS Signatures

Rule Name	Severity	Action	Packet Capture
simple-critical	critical	drop	disable
simple-high	high	drop	disable
simple-medium	medium	drop	disable
simple-low	low	default	disable

18. SECURE BACKUP

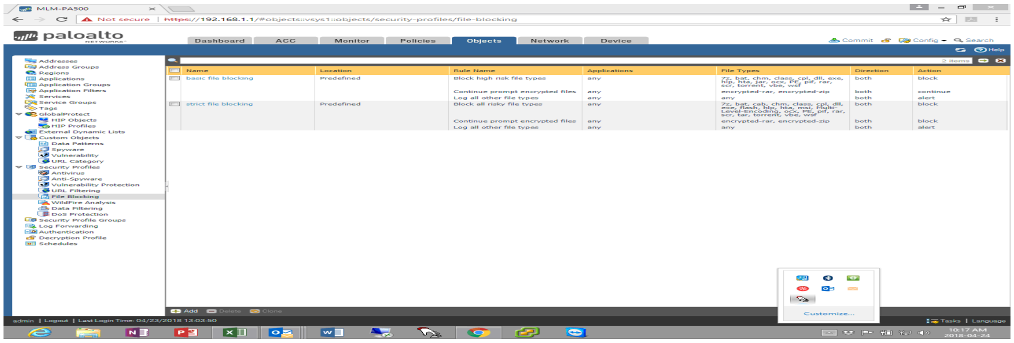
A permissible alternative to offline copies involves online encrypted versions of these same files. Where systems software permits it, the automatic establishment of approved copies of these systems files must proceed whenever an unauthorized modification to these files has been detected. Current offline back-up copies of firewall configuration files, connectivity permission files, firewall systems administration procedural documentation files, and related files must be kept close to the firewall at all times.

19. VIRUS SCREENING AND CONTENT SCREENING

Virus screening software approved by the ICT department must be installed and enabled on all MLM firewalls. Because the files passing through a firewall may be encrypted or compressed, firewall based virus detection systems may not detect all virus-infected files. For this reason, virus screening software is also required at all MLM mail servers, departmental servers, and desktop personal computers. Both content screening software and software that blocks users from accessing certain non-business web sites must also be enabled on all MLM firewalls.

MLM File blocking is currently set as:

Predefined basic and strict file blocking.



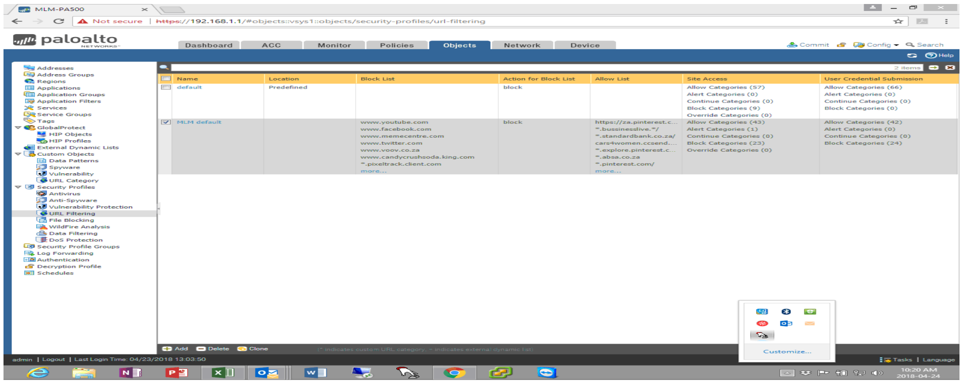
Name	Location	Rule Name	Applications	File Types	Direction	Action
basic file blocking	Predefined	Block high risk file types Continue prompt encrypted files Log all other file types	any any any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf encrypted-rar, encrypted-zip any	both both both	block continue alert
strict file blocking	Predefined	Block all risky file types Continue prompt encrypted files Log all other file types	any any any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf encrypted-rar, encrypted-zip any	both both both	block block alert

Objects and sites blocking, include

- Video Streaming (You tube note that the SSL is not blocked)
- Social Media(Twitter, Facebook, Memecenter, Voov)

Objects and sites Allowed, include

- Banking sites (Standard Bank, Nedbank, First National Bank, ABSA)
- Business informative and News
- Pinterest (Needs to be assessed for current usage)



Name	Location	Block List	Action for Block List	Allow List	Site Access	User Credential Submission
default	Predefined		block		Allow Categories (57) Alert Categories (0) Continue Categories (0) Block Categories (9) Override Categories (0)	Allow Categories (66) Alert Categories (0) Continue Categories (0) Block Categories (0)
☑ MLM default		www.youtube.com www.facebook.com www.memecentre.com www.twitter.com www.voov.co.za www.candycrushsoda.king.com *.pixeltrack.client.com more...	block	https://za.pinterest.c... *.bussinesslive.*/ *.standardbank.co.za/ cars4women.ccsend.... *.explore.pinterest.c... *.absa.co.za *.pinterest.com/ more...	Allow Categories (43) Alert Categories (1) Continue Categories (0) Block Categories (23) Override Categories (0)	Allow Categories (42) Alert Categories (0) Continue Categories (0) Block Categories (24)

20. VIRTUAL PRIVATE NETWORKS

To prevent unauthorized disclosure of sensitive and valuable information, all inbound traffic, with the exception of Internet mail, approved news services, and push broadcasts, that accesses MLM networks must be encrypted with the products approved by the ICT department. These connections are often called virtual private networks (VPNs). The VPNs permissible on MLM networks combine extended user authentication functionality with communications encryption functionality.

21. FIREWALL DEDICATED FUNCTIONALITY

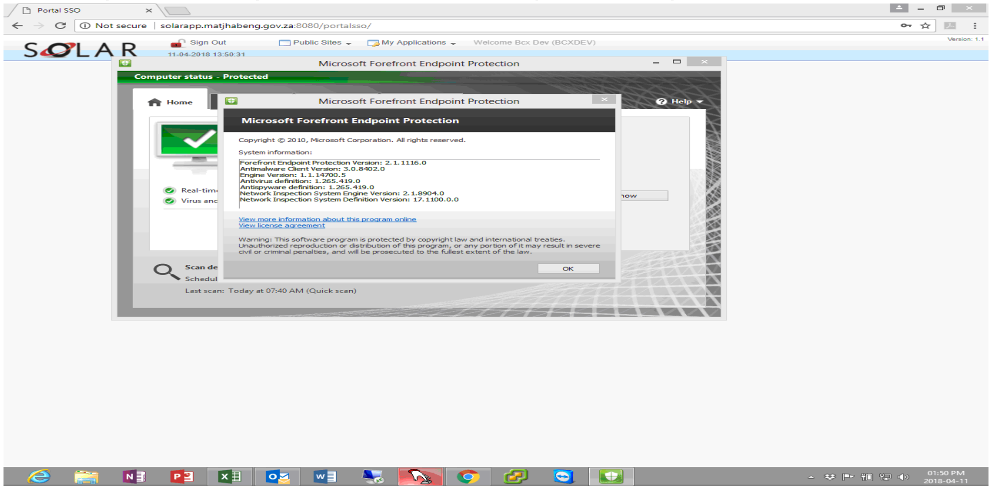
Firewalls must run on dedicated machines that perform no other services, such as acting as a mail server. Sensitive or critical MLM information must never be stored on a firewall. Such information may be held in buffers as it passes through a firewall. Firewalls must have only the bare minimum of operating systems software resident and enabled on them. Where the supporting operating system permits it, all unnecessary and unused systems software must be removed from firewalls. MLM does not permit its internal information to be resident on or processed by any firewall, server, or other computer that is shared with another organization at an outsourcing facility. Outsourcing organization provided shared routers, hubs, modems, and other network components are permissible.

22. FIREWALL CHANGE CONTROL

Because they support critical MLM information systems activities, firewalls are considered all production systems. All changes to the firewall software provided by vendors, excluding vendor-provided upgrades and patches and fixes must go through the Change Management Process. A firewall policy, defining permitted and denied services and connections, should be documented and reviewed at least twice a year by the Security Engineer. Major changes to the MLM internal networking environment, any changes to the production business applications supported, and any major information security incident must trigger an additional and immediate review of the firewall policy. The same documentation that is required for changes on production systems must also be prepared for firewall changes.

23. POSTING UPDATES

MLM firewalls must be running the latest release of software to repel these attacks. Where available from the involved vendor, all MLM firewalls must subscribe to software maintenance and software update services. Unless approved in advance by the ICT Manager, staff members responsible for managing firewalls must install and run these updates within two business days of receipt. As per image below all firewalls within the MLM must be update on a regular basis as per the service provider requirements that is the products specifications.



Microsoft Forefront Endpoint Protection

Copyright © 2010, Microsoft Corporation. All rights reserved.

System information:

```
Forefront Endpoint Protection Version: 2.1.1116.0
Antimalware Client Version: 3.0.8402.0
Engine Version: 1.1.14700.5
Antivirus definition: 1.265.419.0
Antispyware definition: 1.265.419.0
Network Inspection System Engine Version: 2.1.8904.0
Network Inspection System Definition Version: 17.1100.0.0
```

View more information about this program online
View license agreement

Warning: This software program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it may result in severe civil or criminal penalties, and will be prosecuted to the fullest extent of the law.

OK

Last scan: Today at 07:40 AM (Quick scan)

24. MONITORING VULNERABILITIES

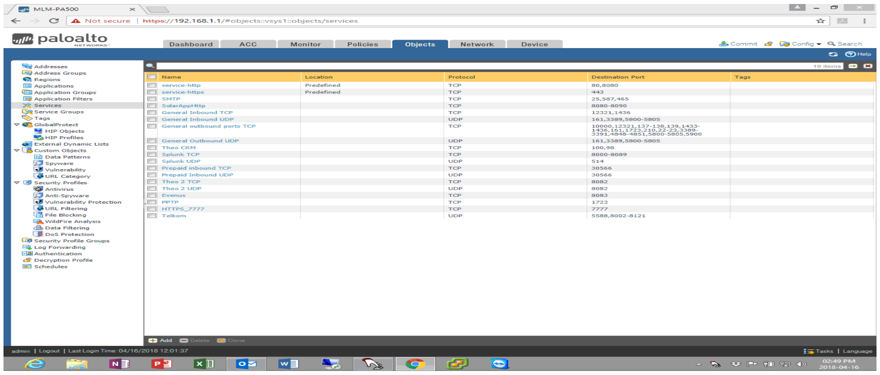
MLM staff members responsible for managing firewalls should stay current with information about firewall vulnerabilities. Any vulnerability that appears to affect MLM networks and systems must promptly be brought to the attention of the ICT Manager.

Part of the vulnerabilities is the ports currently in use. Ports for example 443, 8080. Common ports, such as TCP port 80 (HTTP), may be locked down but other ports may get overlooked and be vulnerable to hackers. In your security tests, be sure to check these commonly hacked TCP and UDP ports: Note that there is software available for PORT vulnerability testing.

- TCP port 21 — FTP (File Transfer Protocol)
- TCP port 22 — SSH (Secure Shell)
- TCP port 23 — Telnet
- TCP port 25 — SMTP (Simple Mail Transfer Protocol)
- TCP and UDP port 53 — DNS (Domain Name System)
- TCP port 443 — HTTP (Hypertext Transport Protocol) and HTTPS (HTTP over SSL)
- TCP port 110 — POP3 (Post Office Protocol version 3)
- TCP and UDP port 135 — Windows RPC
- TCP and UDP ports 137–139 — Windows NetBIOS over TCP/IP

- TCP port 1433 and UDP port 1434 — Microsoft SQL Server

25. FIREWALL ACCESS MECHANISMS



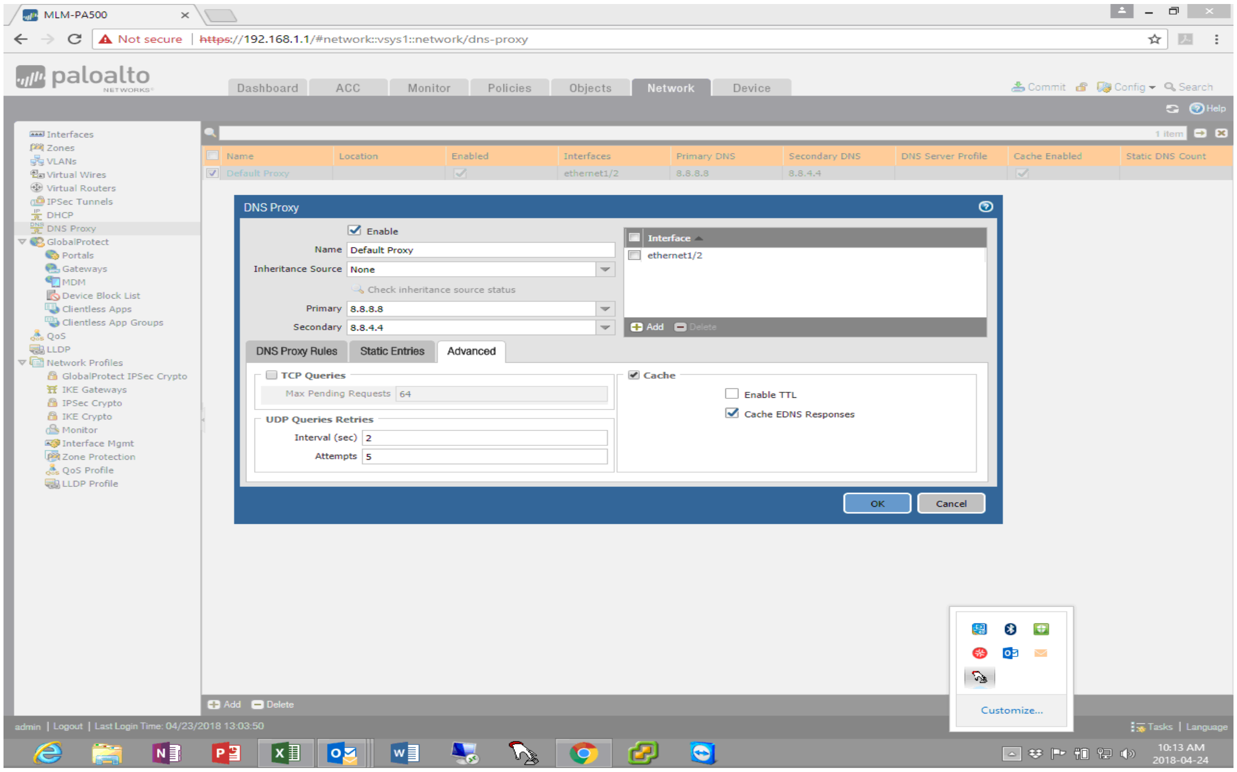
Name	Location	Protocol	Destination Port	Tags
service-http	Predefined	TCP	80,8080	
service-https	Predefined	TCP	443	
SMTP		TCP	25,587,465	
SolarAppHttp		TCP	8080-8090	
General Inbound TCP		TCP	12321,1436	
General Inbound UDP		UDP	161,3389,5800-5805	
General outbound ports TCP		TCP	10000,12321,137-138,139,1433-1436,161,1723,210,22-23,3389-3391,4848-4851,5800-5805,5900	
General Outbound UDP		UDP	161,3389,5800-5805	
Theo CRM		TCP	100,98	
Splunk TCP		TCP	8000-8089	
Splunk UDP		UDP	514	
Prepaid inbound TCP		TCP	30566	
Prepaid Inbound UDP		UDP	30566	
Theo 2 TCP		TCP	8082	
Theo 2 UDP		UDP	8082	
Evenus		TCP	8083	
PPTP		TCP	1723	
HTTPS_7777		TCP	7777	
Telkom		UDP	5588,8002-8121	

admin | Logout | Last Login Time: 04/16/2018 12:01:37

All MLM firewalls must have unique passwords or other access control mechanisms. The same password or access control code must not be used on more than one firewall. Whenever supported by the involved firewall vendor, those who administer MLM firewalls must have their identity validated through extended user authentication mechanisms. In certain high security environments designated by the ICT Manager, such as the MLM Internet commerce site, remote access for firewall administrators is prohibited. All firewall administration activities must take place in person and on site.

Current Default Proxy listed below.

8.8.8.8 and 8.8.4.4



Name	Location	Enabled	Interfaces	Primary DNS	Secondary DNS	DNS Server Profile	Cache Enabled	Static DNS Count
Default Proxy		✓	ethernet1/2	8.8.8.8	8.8.4.4		✓	

DNS Proxy

☑ Enable
Name: Default Proxy
Inheritance Source: None
Check inheritance source status
Primary: 8.8.8.8
Secondary: 8.8.4.4

Interface: ☐ ethernet1/2

DNS Proxy Rules | Static Entries | Advanced

☐ TCP Queries
Max Pending Requests: 64

UDP Queries Retries
Interval (sec): 2
Attempts: 5

☑ Cache
☐ Enable TTL
☑ Cache EDNS Responses

OK | Cancel

admin | Logout | Last Login Time: 04/23/2018 13:03:50

Main Ethernet Lines Layer 3 Interphase, IPV4 Static.

Ping: 41.162.162.162/29

Ping: 41.162.162.164

Allow MGT: 192.168.1.254/24

26. STANDARD PRODUCTS

Unless advance written approval is obtained from the IT Management team, only those firewalls appearing on the list of approved vendors and products may be deployed with MLM networks. All firewall interfaces and features deployed, such as virus screening, must be consistent with the Information Architecture issued by the ICT department.

27. APPROVALS