Progressive Martial Arts And Fitness Center

System Administrator Documentation

- THIS DOCUMENT IS WHITEWASHED FOR SECURITY -
- PORTFOLIO USE ONLY - NETWORK DATA IS NOT ACCURATE -

1.0 - Index

1.1 - Introduction

This document is to layout and guide those unfamiliar with the security system network installed at:

Progressive Martial Arts and Fitness Center

Due to the nature of the contents, this document should only be given to those who are completely trusted to uphold and maintain the existing network integrity.

What you will find in this document:

All Hardware Deployed, and their Specs
Layout of the Network in both text and visual format
Security Specs
Administrator Passwords
SSL Certificate Information
Guides for adding new devices
Software Layout

2.0 - Network Layout

This network has been deployed with 4 Virtual LANs over 1 Main Router.

They are described below:

VLAN1 (br0) (10.78.10.0/24)	Main Server/NVR VLAN
VLAN2 (WAN)	WAN Port VLAN (To Modem)
VLAN3 (br1) (10.78.20.0/24)	Security Camera VLAN
VLAN4 (br2) (10.78.30.0/24)	General WiFi

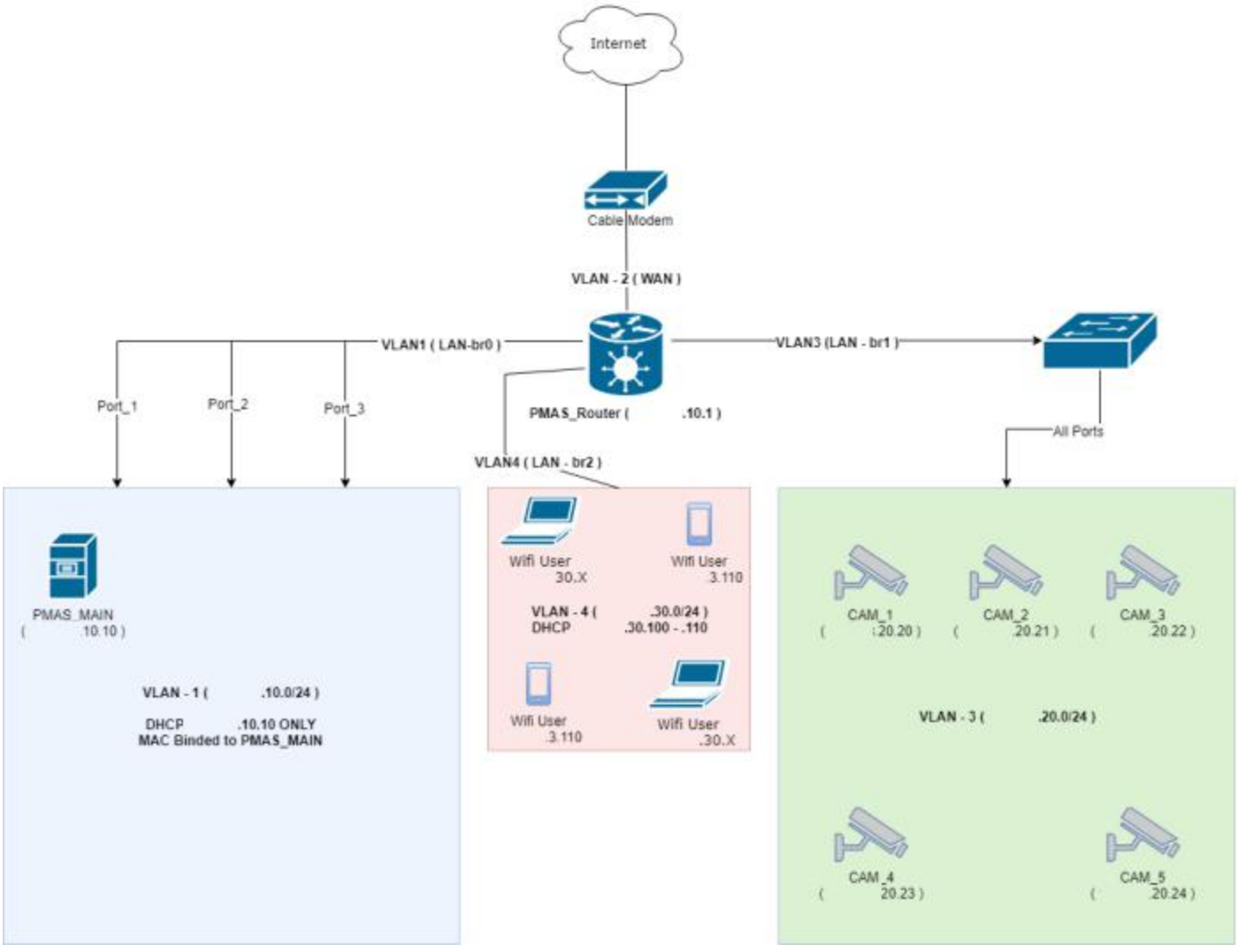
In short:

VLAN1 is where the main server resides. It is DHCP enabled for 10.78.10.10 - 10.78.10.10
The server is MAC bound to this address

VLAN3 handles all Security Camera Equipment outside of the NVR.

VLAN4 is where all WiFi connections are handled.
WiFi supports a maximum of 10 Clients to reduce bandwidth consumption.

2.1 - Network Layout Visual



3.0 - Hardware Specs

This section contains all relative information to deployed hardware.

3.2 - Deployed Equipment

Custom Server (Specs Below)
Amcrest 8 Port PoE Switch
5x SV3C 1080p IP Cameras

3.2 - Main Server / NVR (Network Video Recorder)

The Main Server runs Linux Mint x64 OS

Main-board :	ASUS ROG B350-F
CPU :	AMD - Ryzen 5 1600X 6 Core 3.6Ghz
RAM :	16GB (2 x 8GB) - 2 Slots Free
SSD :	WD Blue 500GB

3.3 Cameras

In effort to reduce cost, the cameras used are SV3C 1080p IP Cameras.

Due to their low cost and production location these are considered to be non-trusted devices.

They have been isolated on VLAN3 with very restrictive firewall settings to prevent tampering or outside access.

Only 10.78.10.10 is allowed to communicate to them, and they are only allowed to communicate to 10.78.10.10

4.0 Security

This section covers all methods used to secure the network and its devices

4.1 Passwords

All actions below require passwords:

Router Admin Access
Server User Login / - Root Login Disabled
CA Server Login / - Root Login Disabled
CA Server Decryption
Direct Camera Admin Access
Webmin Access
PhPMyAdmin Access
ZoneMinder (NVR) User & Admin Access

All the above passwords can be found handwritten in the passwords section of this document

4.2 Firewall

The Main Router utilizes a firewall to protect against unauthorized use.

The below additional iptables rules are in included and in effect on deployment:

Source	*Destination*	*Action*
10.78.10.10 (Server)*	VLAN3 (Camera VLAN)	ACCEPT
VLAN3 (Camera VLAN)*	10.78.10.10 (SERVER)	ACCEPT
VLAN3 (Camera VLAN)	WAN (Outgoing)	DROPPED
WAN (Incoming)	VLAN3 (Camera Network)	DROPPED
VLAN4 (WiFi VLAN)	VLAN1 (Server VLAN)	DROPPED

All DROPS are logged at the router.

* These rules allow the Camera System and NVR to communicate, all other communications regarding VLAN3 are dropped

Static IP MAC Bound Administrative Devices inside VLAN4 are white listed in the router iptables

These devices are allowed to communicate to the server from VLAN4 (Wifi Access)

4.3 Ports

The Main Router only listens on the ports : *45000* & *47000*

45000 is used for external SSH connections. 22 Can still be used within the LAN.

47000 External is sent to 10.78.10.10:27500 on the internal network.

This port is used to access ZoneMinder for remote security camera viewing
ZoneMinder is left web-facing for end-user ease and requires further authentication

Applications Bound to Ports

The below table illustrates which software is available and where:

Keep in mind all web applications must be accessed via https / port 443

Application	On LAN	On WAN	Location	Int Port	Ext Port
Entrance Portal	X		10.78.10.10 (Server)	443	-
Webmin	X		10.78.10.10 (Server)	10000	-
PhpMyAdmin	X		10.78.10.10 (Server)	443	-
ZoneMinder	X	X	10.78.10.10 (Server)	27500	47000
XRDP	X		10.78.10.10 (Server)	3389	-
SSH	X	X	10.78.10.1 (Router)	22	45000

*Non external applications are accessible through SSH Remote Tunneling - Read more in section *5.0 Administration*

4.4 SSH

The Main Router is the point of contact for remote SSH connections

SSH from remote to the Main Router requires public key authentication by the router.

Only authorized devices have their keys stored in the router

Learn more about adding future devices in *5.0 - Administration*

-

The Main Server may only be connected via SSH remotely after tunneling to the router

4.5 In House Certificate Authority Server

In effort to reduce costs, an internal virtual CA server has been deployed on the Main Server.

This CA server handles all internal SSL certificates.

The CA Server should only be used to sign or generated new certificates for new applications that are to be installed on the network.

The Certificate Authority Server is encrypted for further isolation.

4.6 SSL CA Certificate Location & Adding to new device

Devices that wish to connect to any of the internal services must recognize the internal CA as an authorized source.

To do so, the internal CA certificate must be added to the devices authorities.

The CA certificate can be found on the Main Server's Entrance Portal when accessed on the LAN or through SSH Tunneling

Most devices will support adding the certificate on visiting the link from the main Web Portal

You may have to consult documentation for your device on adding a new *Certificate Authority.*

5.0 - Administration

All relevant common guides for administration are found in this section.

All administrative web applications can be accessed easily through the web portal by directing your browser, via LAN, to:

10.78.10.10

5.1 - Intro to Administration

This set-up has been provided with numerous tools to make administration of this network as simple as possible, they will be covered individually on a per section basis.

5.2 - Intro to Webmin

Webmin is a Web based gui for easy administration of linux devices.

Almost all basic tasks can be performed through Webmin.

If further information on Webmin is needed please visit:

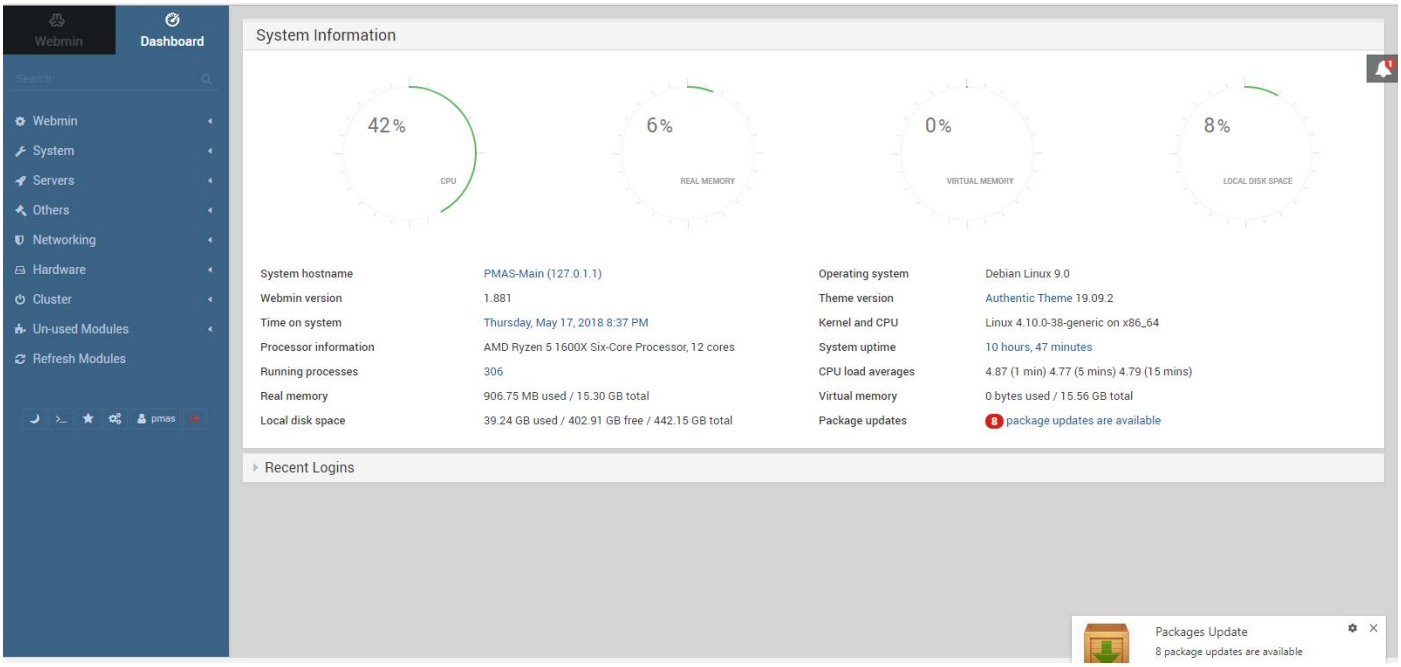
https://doxfer.webmin.com/Webmin/Main_Page

Remember Webmin, is a non-web facing application. In must be accessed through the LAN or tunneled to via the router.

Your Webmin interface can be found via the Web Portal or at https://10.78.10.10:10000

The login will use the webmin credentials found in the Administrative Passwords section.

The screen shot below shows you the basic web GUI after logging in:



5.3 - Intro to RDP (Remote Desktop Protocol)

RPD is a method for viewing the server remotely as if you were sitting at it.

To RDP to the Main Server you must be in the LAN n VLAN4 Wifi and on an authorized white listed device

OR

You must be SSH Tunneled to the router.

In windows you can use the included Remote Desktop Connection to connect to the Main Server

Just point the RDP client to 10.78.10.10

The standard port is used, so there is no need to add any additional information.

5.4 - Administrative Passwords

Application	Username	Password
WiFi Password		
Main Server User Login		
CA Server Login		
CA Server Decryption Password		
CA Private Key Password		
Router Administrator Login		
MySQL / PhpMyAdmin Root		
IP Camera Logins (All The Same)		
ZoneMinder Admin Login		
Main Server SSH Key Password		

5.5 - Adding Administration Devices (Issuing new SSL Certs)

New devices can be added by using the virtual CA inside the main server to issue new SSL Certificates.

Documents are included within the encrypted CA on how to do this.

5.6 - Adding authorized users to Router SSH

New authorized SSH users for the router must be added in the admin panel of the Tomato firmware.

Log into your router at the specified address above and add the client keys to the authorized keys section in the ‘admin’ panel.