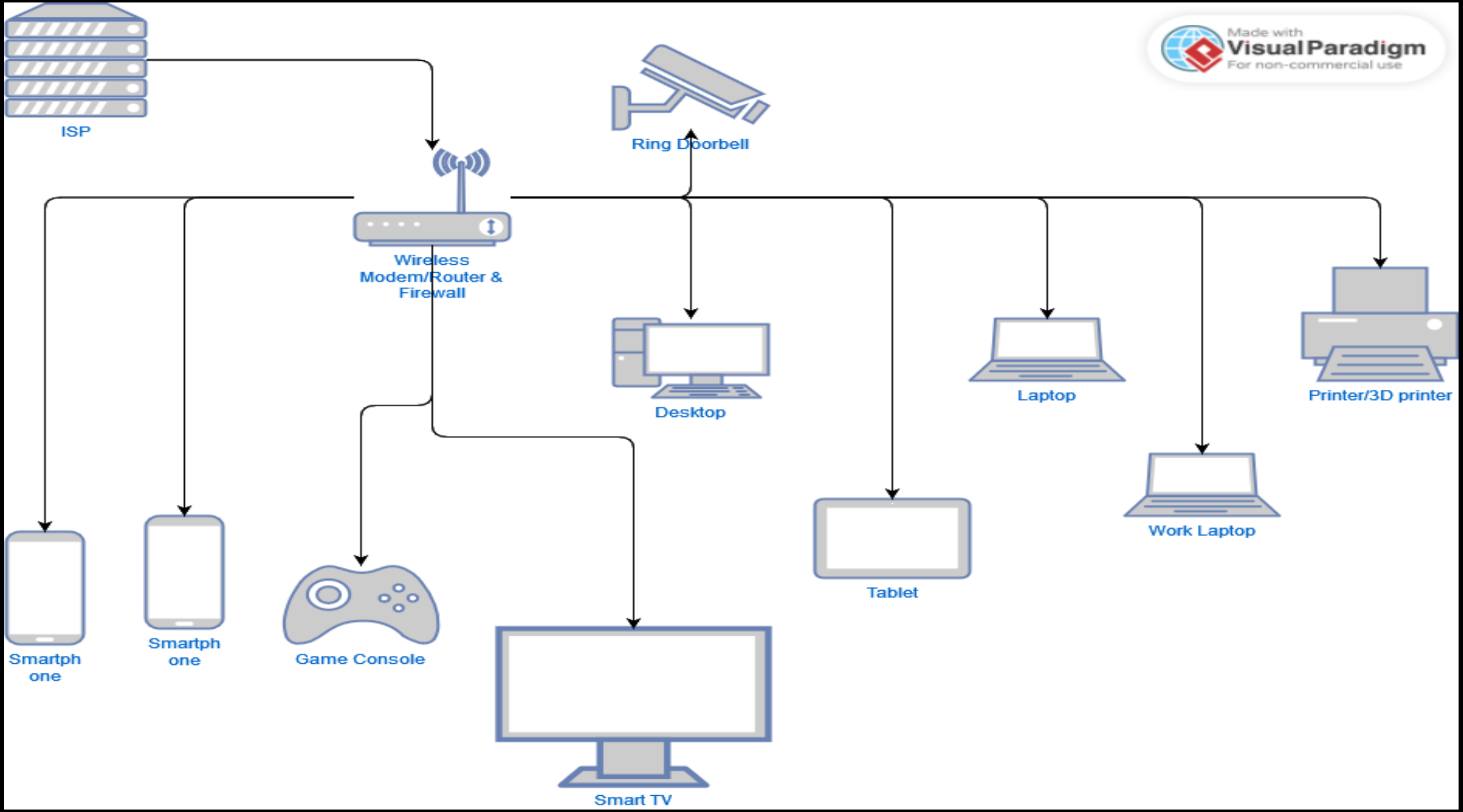
Home Security Series

Part 1: Home Networking

Traditional Home Network



Problems?

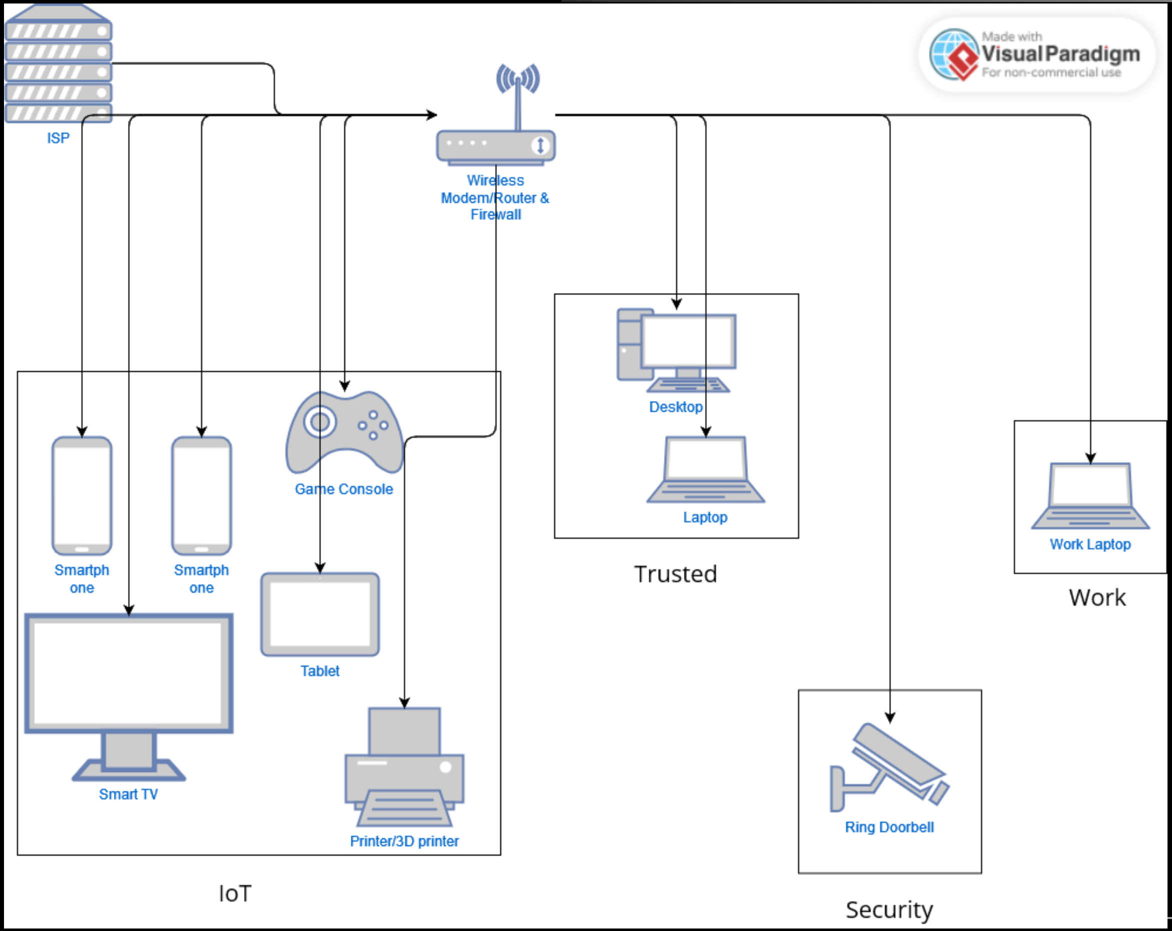
- No security
- No privacy
- At risk for being hacked*
- No segmentation

- Anyone can just “join”
- Single failure point
- *Lateral movement* is easy
- Potential for slower speeds

Mitigation

- Segmentation – create VLANs
- Isolation – cut off access
- Default Deny and No Default LAN
- Firewall rules

What would this look like?



Planning

- Group devices into categories or levels of trust.
- Think about the level of permissions each device should have.
  - Should they know about all devices on my network
  - Should they reach the internet
  - etc

Planning Cont.

- Examples:
  - IoT – least amount of trust
  - Security – high amount of trust, no internet access
  - Management – management interfaces of networking devices. Web UI’s
  - Trusted – Desktop or laptop computers that need to access to management interfaces

Things to Note

- Just putting devices into VLAN’s does not make them more secure
- Firewall rules will need to be setup

- You will probably need more hardware
- Take notes of your configurations
- There is no 1 correct way

Hardware & Software

Hardware Involved

- Modem
- Router*
- Switch (Managed)
- Wireless Access Points (WAP’s)

Software Involved

- Router:
  - Default
  - OPNSense
  - Pfsense
  - OpenWRT.
  - DD-WRT

Software Involved Cont.

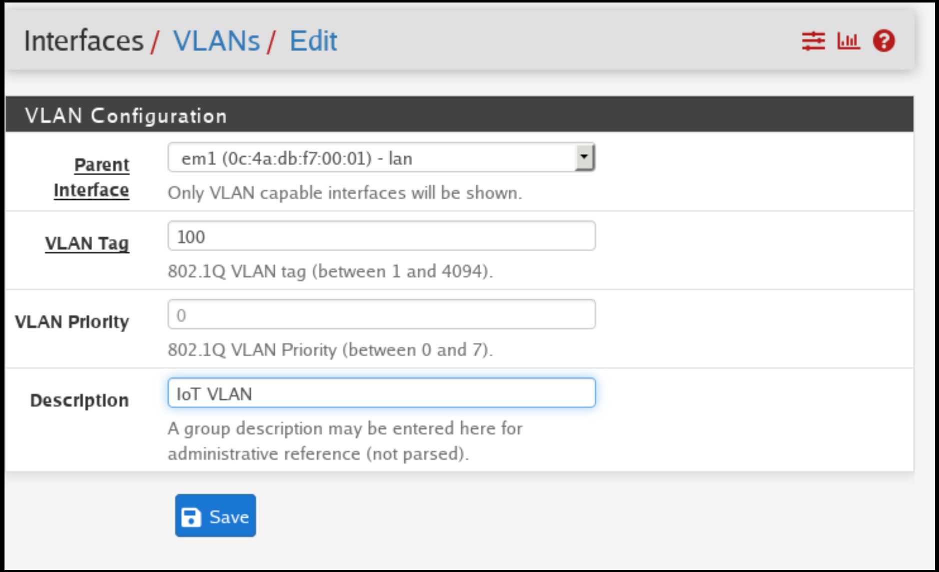
- Switch:
  - Default
- Wireless Access Point:
  - Default
  - OpenWRT

Configuration: Firewall

Configuration: Firewall

- Create a new VLAN
  - You will need a name: Ex - IoT
  - VLAN tag: Ex - 100
  - Description: Ex – Internet of Things Network
  - Interface to assign this to: Ex – eth0, igb0, wlan0, etc
- Repeat for each VLAN

VLAN Config

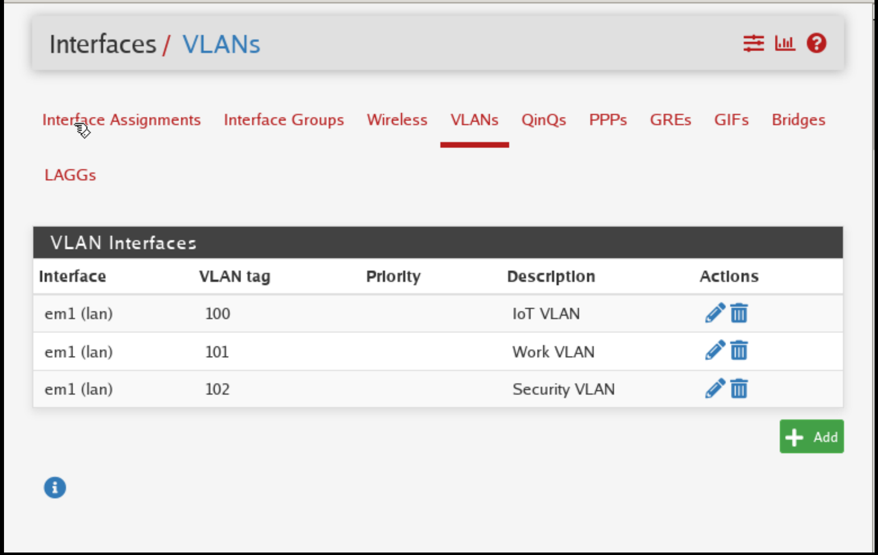


Interfaces / VLANs / Edit

VLAN Configuration

Parent Interface	em1 (0c:4a:db:f7:00:01) - lan Only VLAN capable interfaces will be shown.
VLAN Tag	100 802.1Q VLAN tag (between 1 and 4094).
VLAN Priority	0 802.1Q VLAN Priority (between 0 and 7).
Description	IoT VLAN A group description may be entered here for administrative reference (not parsed).

Setup your VLAN



Interfaces / VLANs

VLAN Interfaces

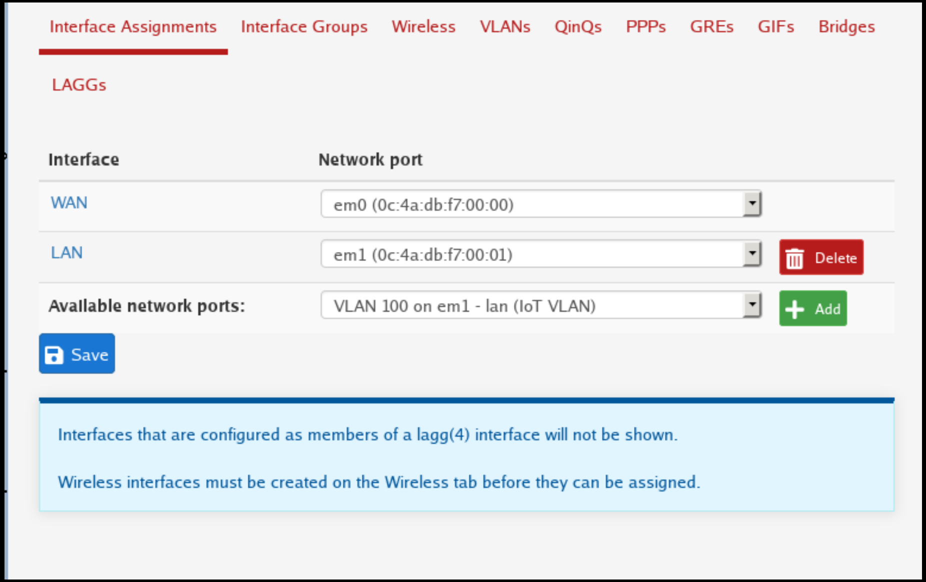
Interface	VLAN tag	Priority	Description	Actions
em1 (lan)	100		IoT VLAN	
em1 (lan)	101		Work VLAN	
em1 (lan)	102		Security VLAN	

Repeat for each VLAN

Configuration: Firewall

- After creating the VLAN’s you may need to assign them to an interface. If you have multiple network interfaces you can assign multiple VLAN’s to each one.
- Ex:
  - Eth0 – IoT, Lab VLANs
  - Eth1 – Security
  - Eth2 – Guest, Work
  - etc

Interface Assignment

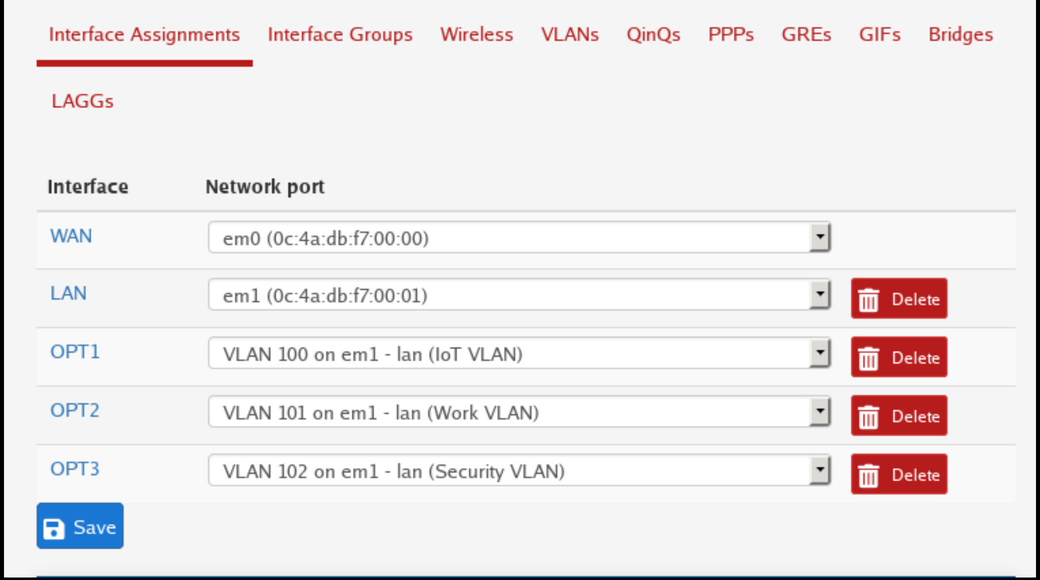


Interface	Network port
WAN	em0 (0c:4a:db:f7:00:00)
LAN	em1 (0c:4a:db:f7:00:01)
Available network ports:	VLAN 100 on em1 - lan (IoT VLAN)

Interfaces that are configured as members of a lagg(4) interface will not be shown.

Wireless interfaces must be created on the Wireless tab before they can be assigned.

Assign Iot interface



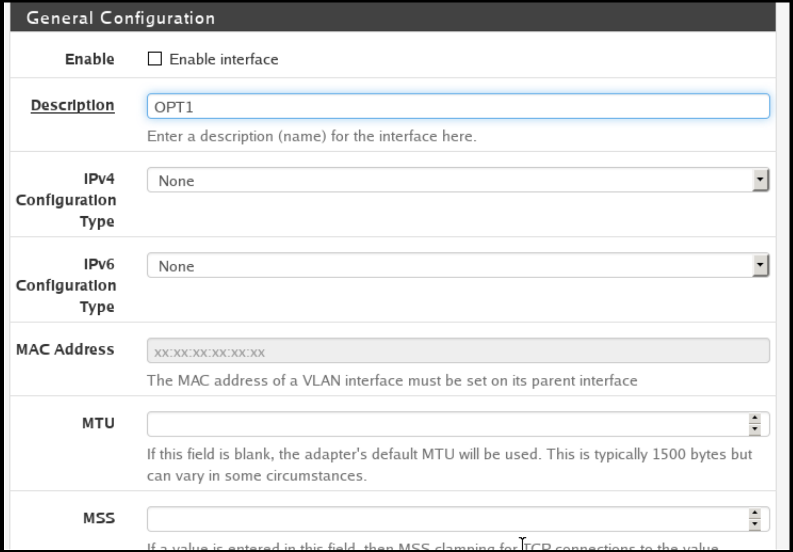
Interface	Network port
WAN	em0 (0c:4a:db:f7:00:00)
LAN	em1 (0c:4a:db:f7:00:01)
OPT1	VLAN 100 on em1 - lan (IoT VLAN)
OPT2	VLAN 101 on em1 - lan (Work VLAN)
OPT3	VLAN 102 on em1 - lan (Security VLAN)

Repeat for each interface

Interface Configuration

- Next you will have to configure the newly assigned interface

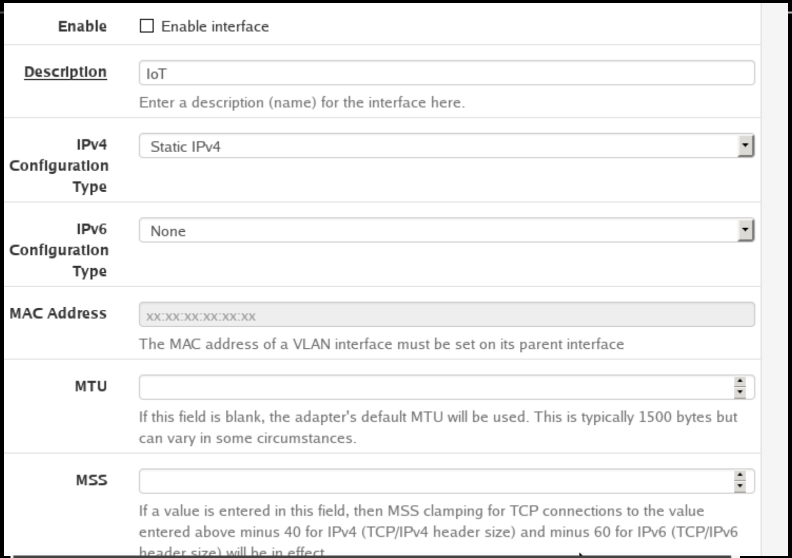
Interface Config Cont.



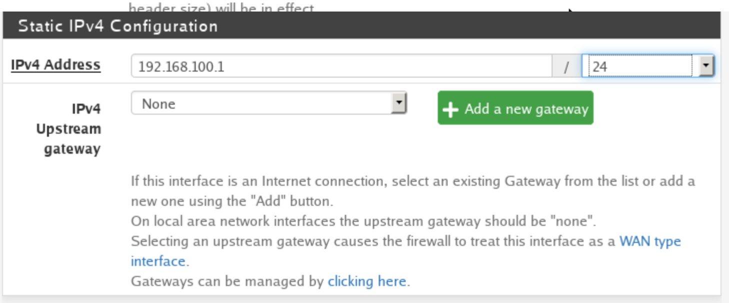
General Configuration

Enable	☐ Enable interface
Description	OPT1 Enter a description (name) for the interface here.
IPv4 Configuration Type	None
IPv6 Configuration Type	None
MAC Address	xx:xx:xx:xx:xx:xx The MAC address of a VLAN interface must be set on its parent interface
MTU	If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	If a value is entered in this field, then MSS clamping for TCP connections to the value

Sample Config



Enable	☐ Enable interface
Description	IoT Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	xx:xx:xx:xx:xx:xx The MAC address of a VLAN interface must be set on its parent interface
MTU	If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.



Static IPv4 Configuration

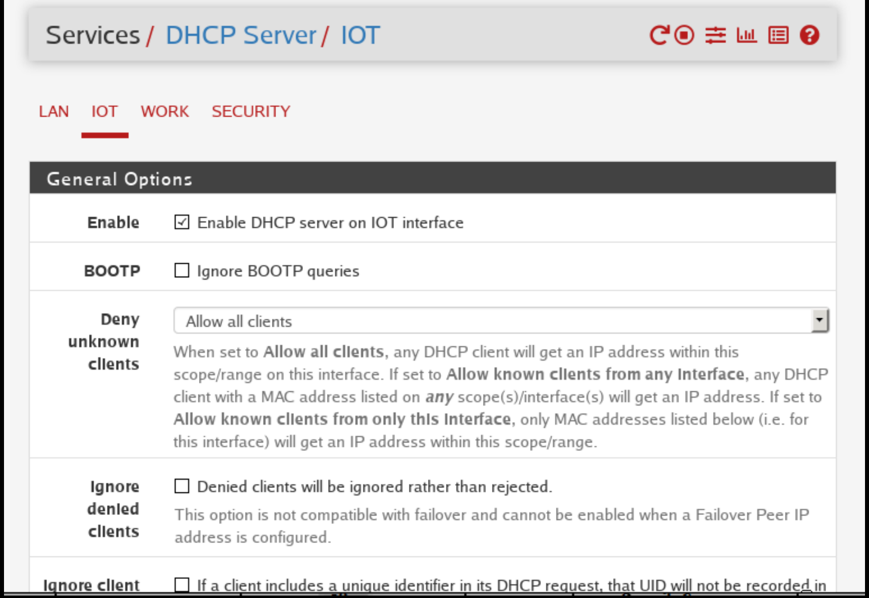
IPv4 Address	192.168.100.1 / 24
IPv4 Upstream gateway	None If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface. Gateways can be managed by clicking here.

Iot Config

DHCP Server

- Each VLAN should have a DHCP server to give out IP addresses to devices that are connected to it.

DHCP Server



Services / DHCP Server / IOT

LAN IOT WORK SECURITY

General Options

Enable ☑ Enable DHCP server on IOT interface

BOOTP □ Ignore BOOTP queries

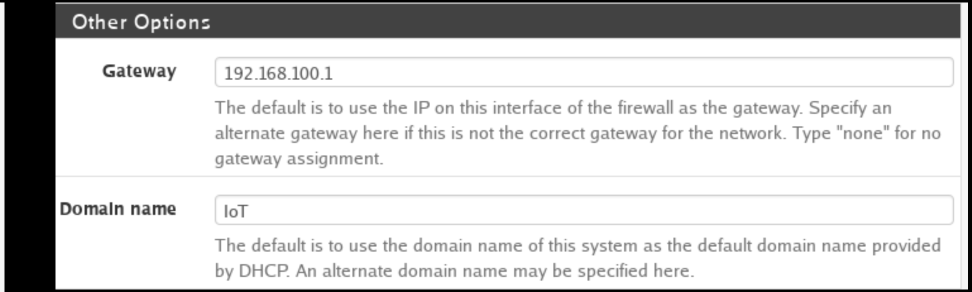
Deny unknown clients Allow all clients

When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed on ***any*** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.

Ignore denied clients □ Denied clients will be ignored rather than rejected.

This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client □ If a client includes a unique identifier in its DHCP request, that UID will not be recorded in



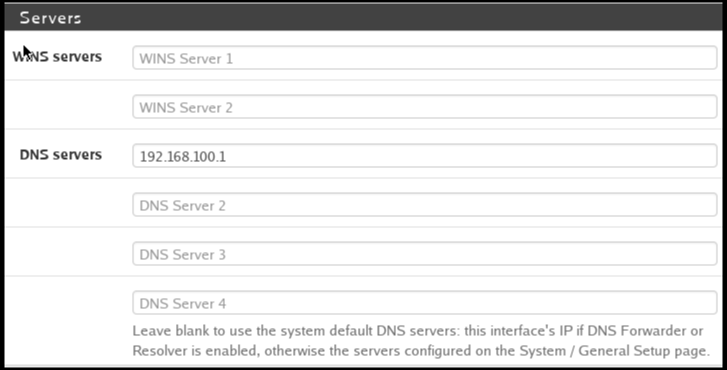
Other Options

Gateway 192.168.100.1

The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.

Domain name IoT

The default is to use the domain name of this system as the default domain name provided by DHCP. An alternate domain name may be specified here.



Servers

WINS servers WINS Server 1

WINS Server 2

DNS servers 192.168.100.1

DNS Server 2

DNS Server 3

DNS Server 4

Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.

Configuration: Firewall

- Once each VLAN is assigned to an interface you will now need to setup firewall rules.
- Firewall rules work in a top down approach.

Configuration: Firewall

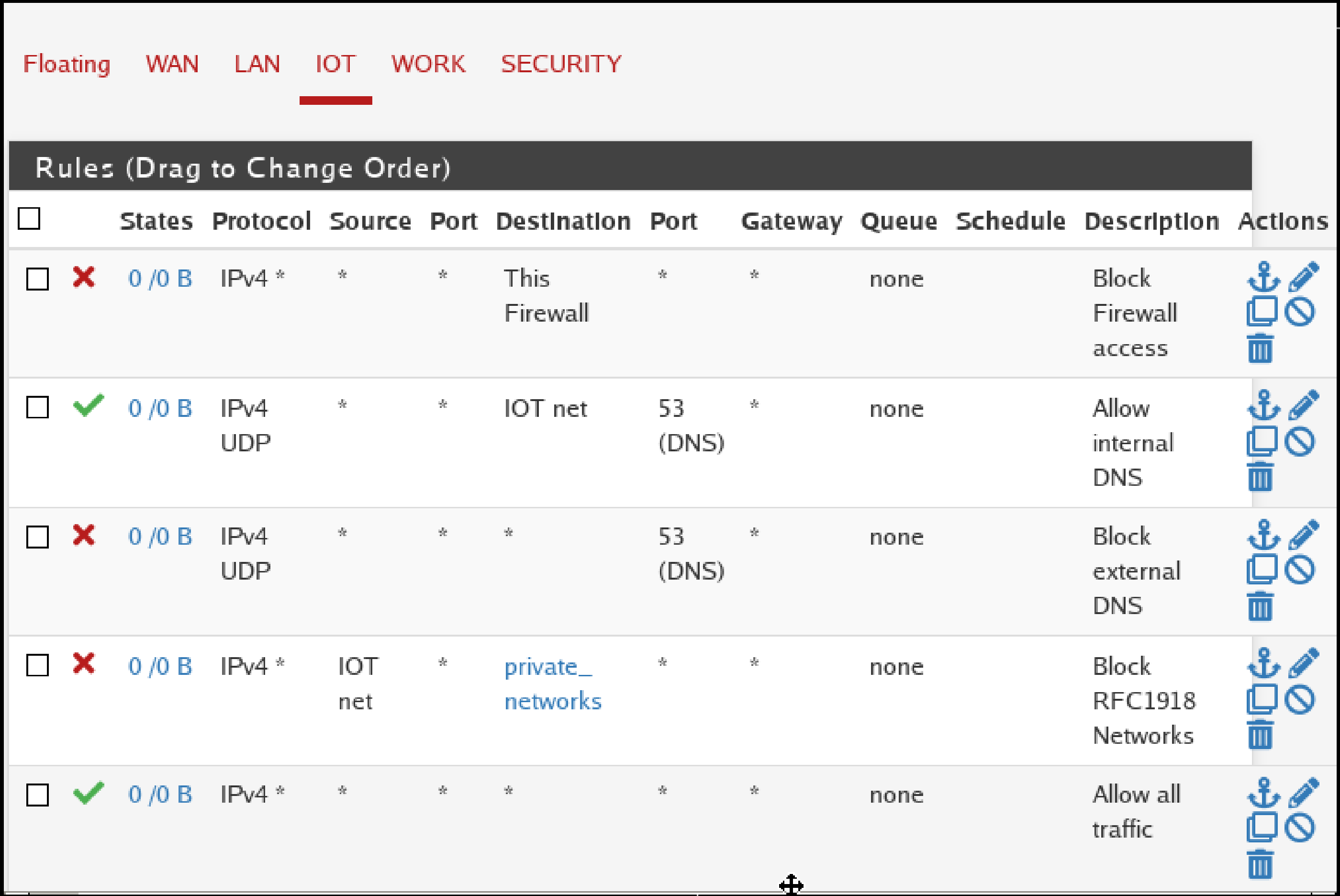
- Rules:
  - Block RFC1918 Networks
  - Block External DNS
  - Allow Internal DNS
  - Allow All

1) Blocks access to all private network addresses

2) Blocks external DNS. Ex: 8.8.8.8 (Google)

3) Allow all other traffic not specified

VLAN Firewall



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✗	0 /0 B	IPv4 *	*	*	This Firewall	*	*	none		Block Firewall access	
□	✓	0 /0 B	IPv4 UDP	*	*	IOT net	53 (DNS)	*	none		Allow internal DNS	
□	✗	0 /0 B	IPv4 UDP	*	*	*	53 (DNS)	*	none		Block external DNS	
□	✗	0 /0 B	IPv4 *	IOT net	*	private_ networks	*	*	none		Block RFC1918 Networks	
□	✓	0 /0 B	IPv4 *	*	*	*	*	*	none		Allow all traffic	

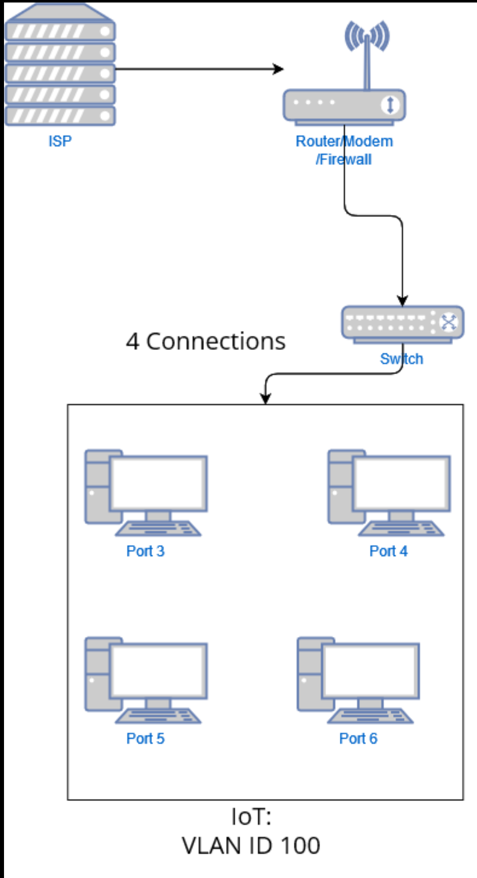
Configuration: Switch

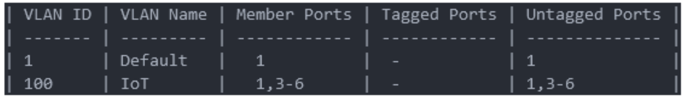
Switch Setup

- 802.1Q VLAN
- VLAN Tagging
- Tagged vs Untagged
- PVID

- Tagged ports: usually “trunked” connection. Connect 2 switches together.*
- Untagged: no VLAN identifier is attached to the packet.*

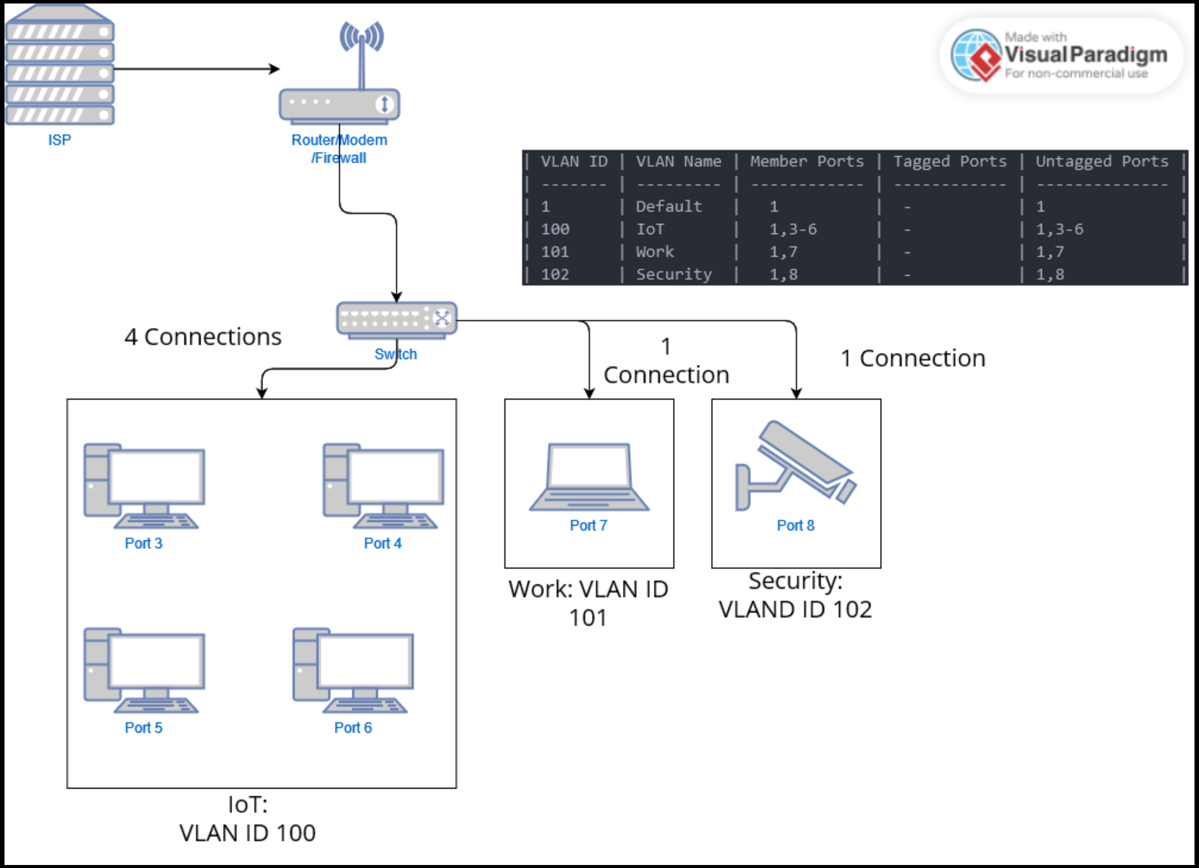
IoT Switch VLAN Example





VLAN ID	VLAN Name	Member Ports	Tagged Ports	Untagged Ports
1	Default	1	-	1
100	IoT	1,3-6	-	1,3-6

Repeat



```
| VLAN ID | VLAN Name | Member Ports | Tagged Ports | Untagged Ports |
| ------- | --------- | ------------ | ------------ | -------------- |
| 1       | Default   |  1           |  -           | 1              |
| 100     | IoT       |  1,3-6       |  -           | 1,3-6          |
| 101     | Work      |  1,7         |  -           | 1,7            |
| 102     | Security  |  1,8         |  -           | 1,8            |
```

Considerations

- Remove ports from the default VLAN
- Setup a “Dead VLAN”
  - Ex: 999 → All unused ports should be a member of this VLAN