On home labs

osku@sanoma.com

About me

- Used to be a sw dev for ~20 years in various roles
- M.Sc. (EE)
- Chief Security Architect / Sanoma Media Finland
- HelSec co-founder. TallinnSec/TurkuSec member, Disobey contributor, KyberVPK volunteer
- I play with and hack stuff. OSCP.
- When not hacking stuff inside my lab I’m building ebikes or paddling on the sea

Agenda

- I’ll describe my home lab setup
- You ask questions and I’ll elaborate the interesting or not so obvious parts

About home labs

in the context of this talk

- Home lab is a lab which is at your home
- Here, I define “home lab” as an environment with lots of networks and computers to play with
- I’ll talk a bit about these in general
- Then I’ll share how I built mine and what’s in it

What for?

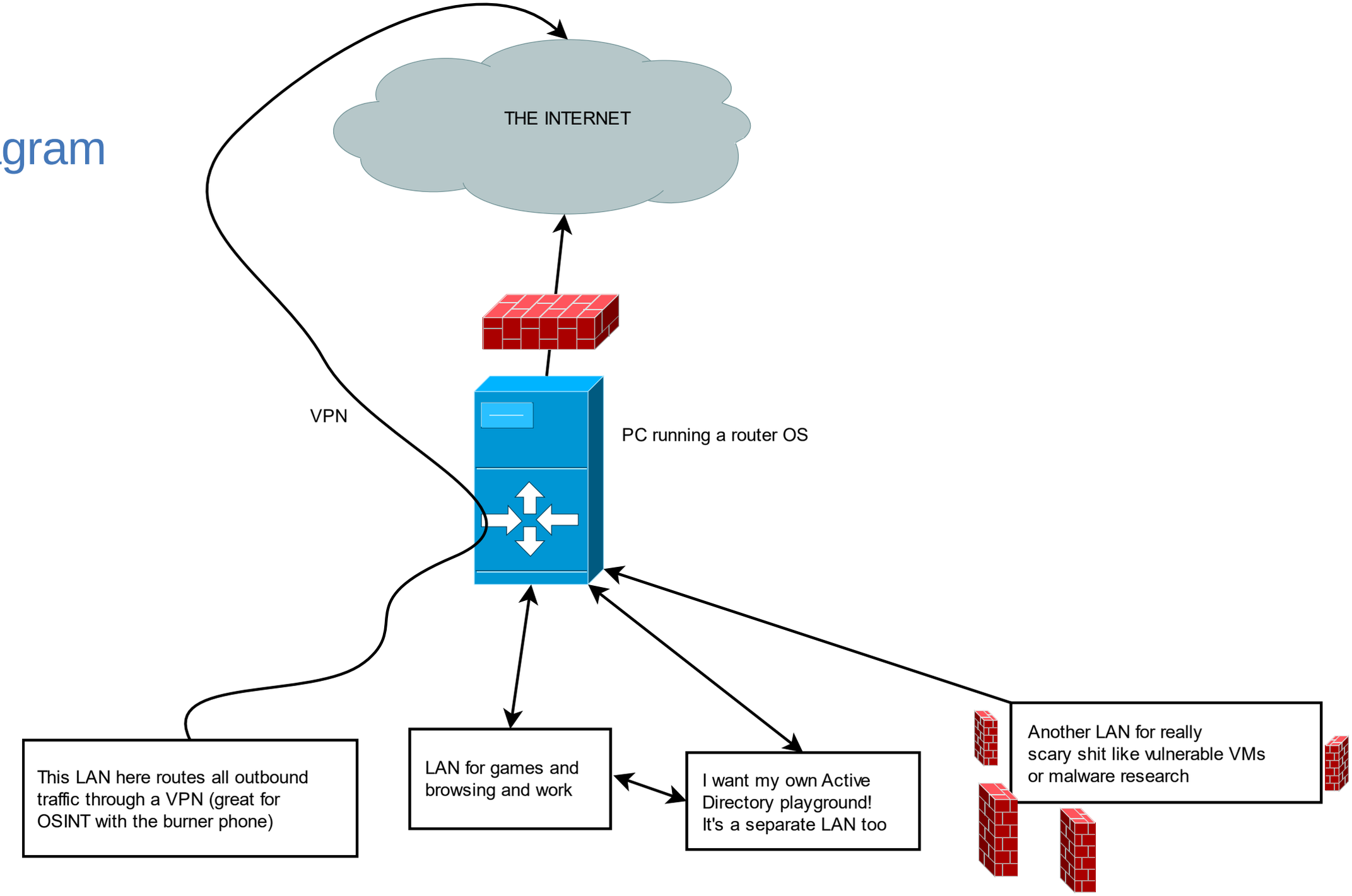
- Run one/some/lots of servers and services
- Try out different OSes
- Run vulnerable VMs
- Simulate complex network environments
- == Self-study

Requirements

I want my home lab to offer:

- “normal” internet connectivity for gaming, browsing, and work
- One or more LANs for special purposes, eg: Active Directory, IoT, vulnerable VMs, studying malware, one that routes everything through VPN
- Wifi APs for any or all of the LANs
- Easily create, run, and destroy lots of (virtual) servers
- Take some of my lab with me when I leave my cave

Network diagram



OK how do I create arbitrarily many LANs while I only have one switch and a finite number of cables?

VLAN

Virtual Local Area Network

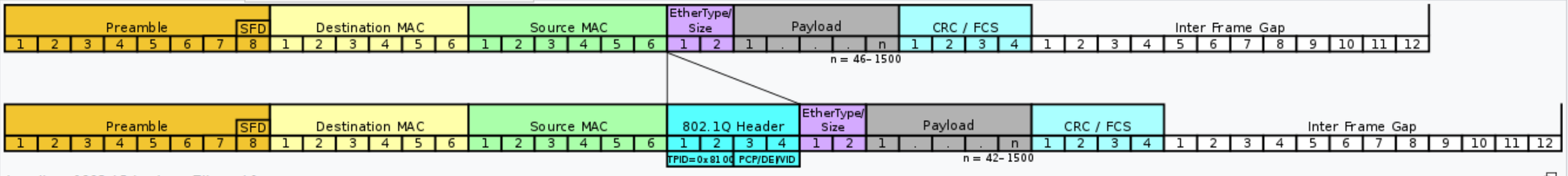
Remember what's in the TCP/IP stack:

4. Application (ssh)
3. Transport (TCP port 22)
2. Internet (192.168.0.100)
1. **Link (48:65:fc:32:13:37)** ***VLAN happens here***
0. Physical (electrical / light / radiation / carrier pigeons – see RFC 1149)

VLAN is an extension to the Ethernet standard

Frame format [edit]

Insertion of 802.1Q tag in an Ethernet frame



Insertion of 802.1Q tag in an Ethernet frame

ZYXEL GS1900-24E

Refresh Save Status Logout Help

Menu

- Getting Started
- Monitor
- Configuration
- Maintenance

- System
- Port
- VLAN
  - VLAN
  - Guest VLAN
  - Voice VLAN
- MAC Table
- Link Aggregation
- Loop Guard
- Mirror
- Multicast
- Spanning Tree
- LLDP
- QoS
- Security
- AAA
- Management

VLAN

VLAN Port VLAN Port

VLAN ID	VLAN Name	VLAN Type	Action
1	default	Default	
2	hax0002	Static	
3	domaintest0003	Static	
4	pialan0004	Static	

Add

ZYXEL GS1900-24E

Refresh Save Status Logout Help

Menu

- Getting Started
- Monitor
- Configuration
- Maintenance

- System
- Port
- VLAN
  - VLAN
  - Guest VLAN
  - Voice VLAN
- MAC Table
- Link Aggregation
- Loop Guard
- Mirror
- Multicast
- Spanning Tree
- LLDP
- QoS
- Security
- AAA
- Management

VLAN Port

VLAN Port | Port | VLAN

VLAN ID: 3

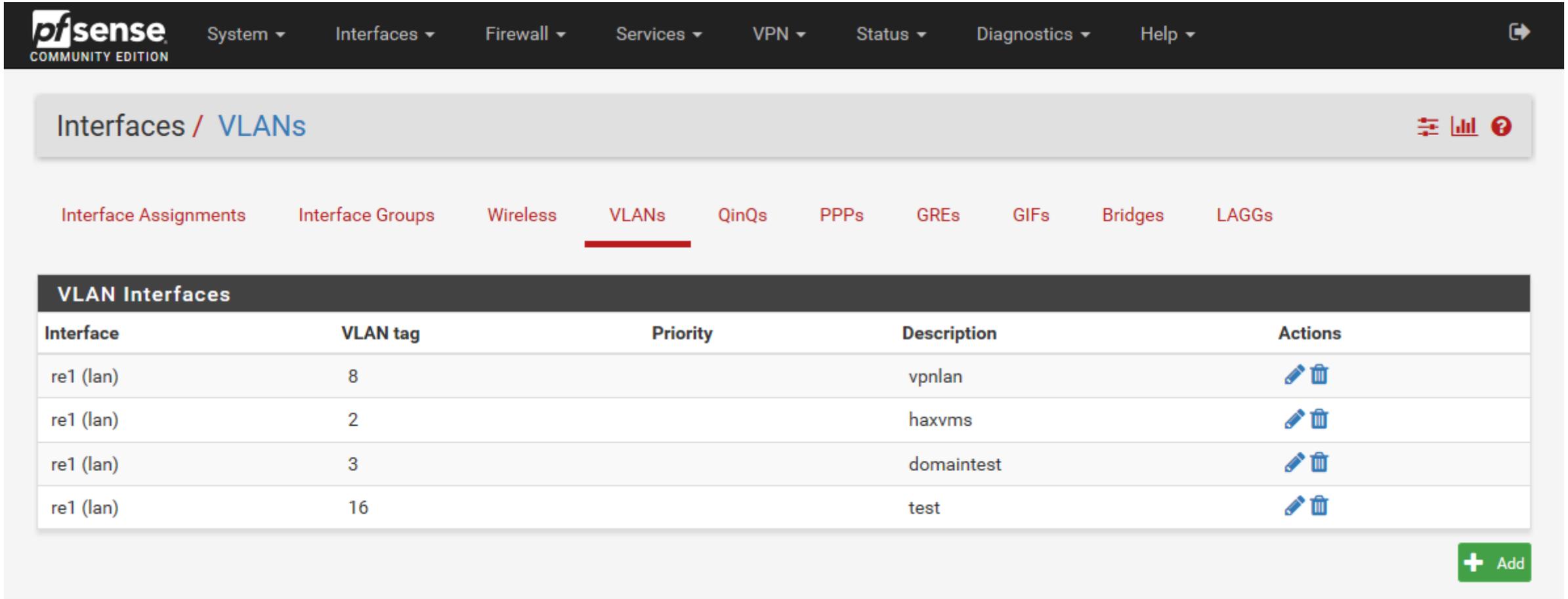
Port	Membership
*	Excluded
1	Forbidden Excluded Tagged Untagged
2	Forbidden Excluded Tagged Untagged
3	Forbidden Excluded Tagged Untagged
4	Forbidden Excluded Tagged Untagged
5	Forbidden Excluded Tagged Untagged
6	Forbidden Excluded Tagged Untagged
7	Forbidden Excluded Tagged Untagged
8	Forbidden Excluded Tagged Untagged
9	Forbidden Excluded Tagged Untagged
10	Forbidden Excluded Tagged Untagged
11	Forbidden Excluded Tagged Untagged
12	Forbidden Excluded Tagged Untagged
13	Forbidden Excluded Tagged Untagged
14	Forbidden Excluded Tagged Untagged
15	Forbidden Excluded Tagged Untagged
16	Forbidden Excluded Tagged Untagged
17	Forbidden Excluded Tagged Untagged
18	Forbidden Excluded Tagged Untagged
19	Forbidden Excluded Tagged Untagged
20	Forbidden Excluded Tagged Untagged
21	Forbidden Excluded Tagged Untagged
22	Forbidden Excluded Tagged Untagged
23	Forbidden Excluded Tagged Untagged
24	Forbidden Excluded Tagged Untagged
LAG1	Forbidden Excluded Tagged Untagged
LAG2	Forbidden Excluded Tagged Untagged
LAG3	Forbidden Excluded Tagged Untagged
LAG4	Forbidden Excluded Tagged Untagged
LAG5	Forbidden Excluded Tagged Untagged
LAG6	Forbidden Excluded Tagged Untagged
LAG7	Forbidden Excluded Tagged Untagged
LAG8	Forbidden Excluded Tagged Untagged

Apply Cancel

Routing

I’m using pfSense, it’s a router OS, based on FreeBSD. I’m liking it

This is how the VLANs look on the pfSense



Interfaces / domaintest (re1.3)

General Configuration

Enable	☑ Enable interface
Description	domaintest 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 (TCP/IP header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

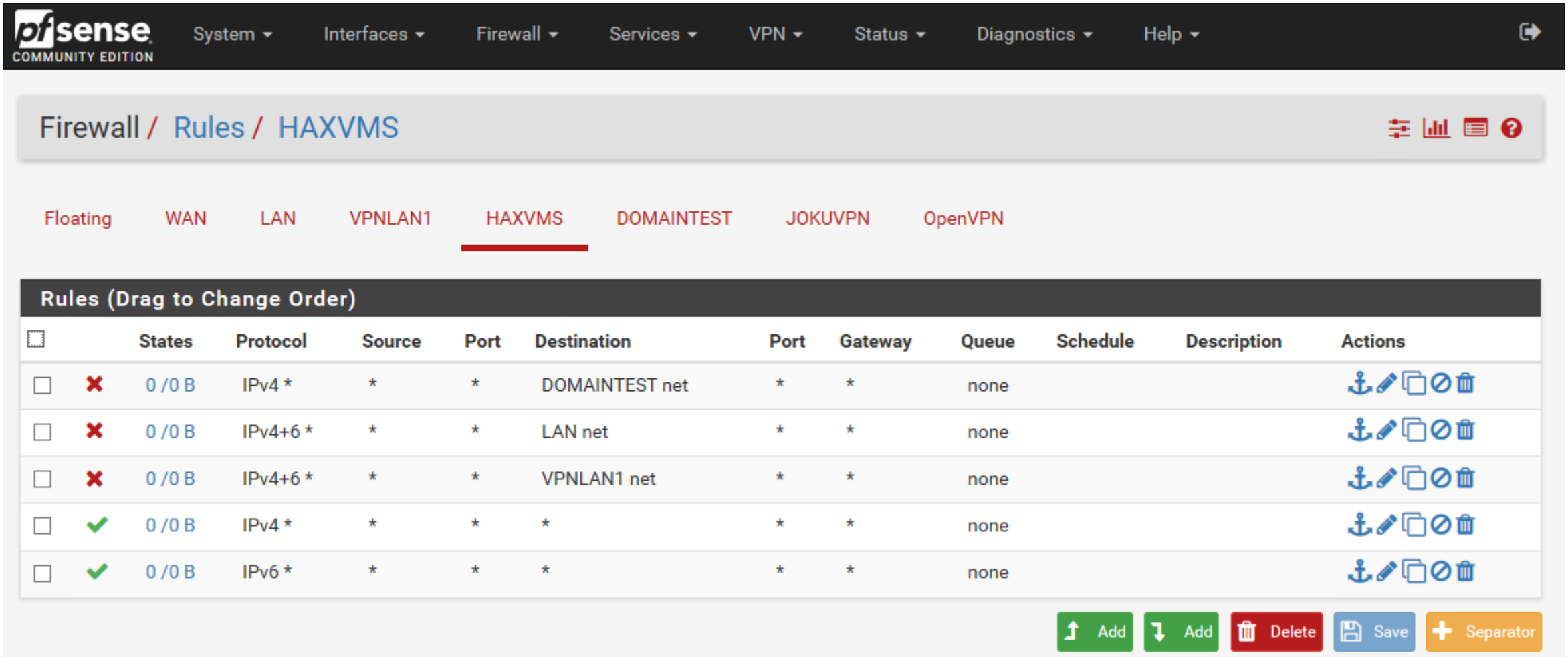
IPv4 Address	192.168.60.1 / 24
IPv4 Upstream gateway	None + Add a new gateway If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Gateways can be managed by clicking here.

Reserved Networks

Block private networks and loopback addresses	☐ Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Routing

… firewall



The servers

Proxmox

It’s a virtualization platform

Pros:

- Open source
- Can create clusters
- Seems stable

Cons:

- Idk?
- Not super easy to implement more complex scenarios

What to use Proxmox for

- Manually create VMs using GUI (like virtualbox, vmware)
- Create and use templates to quickly deploy new servers
- Cluster: maybe easier to manage than many independent Proxmox hosts

Proxmox

My cluster setup (or, one of them)

- 2x Lenovo S30 (circa 2013, cheap these days) (8-core Xeon e2650, 64G, a few TB total)
- A bunch of cheap dumpster finds (i3, 8/16G, SSD)
- Intel NUC (8gen i7, 32g, 1tb)

I’m taking the NUC with me when I go places

Proxmox is cool, show some demos

cloudinit

Post installation config for guest VMs

- Technically, a disk image containing config, and software to apply it

How to use:

1. Manually install an OS once on a VM
2. Install the cloud-init package on VM
3. Convert VM to a VM template
4. Then, each clone of the template can be configured separately (eg. hostname, ssh keys, ip address)

I have templates for kali, Debian, ubuntu

For windows, there’s cloudbase-init (but I haven’t tested it yet)

Now ask me things

sanoma

thank