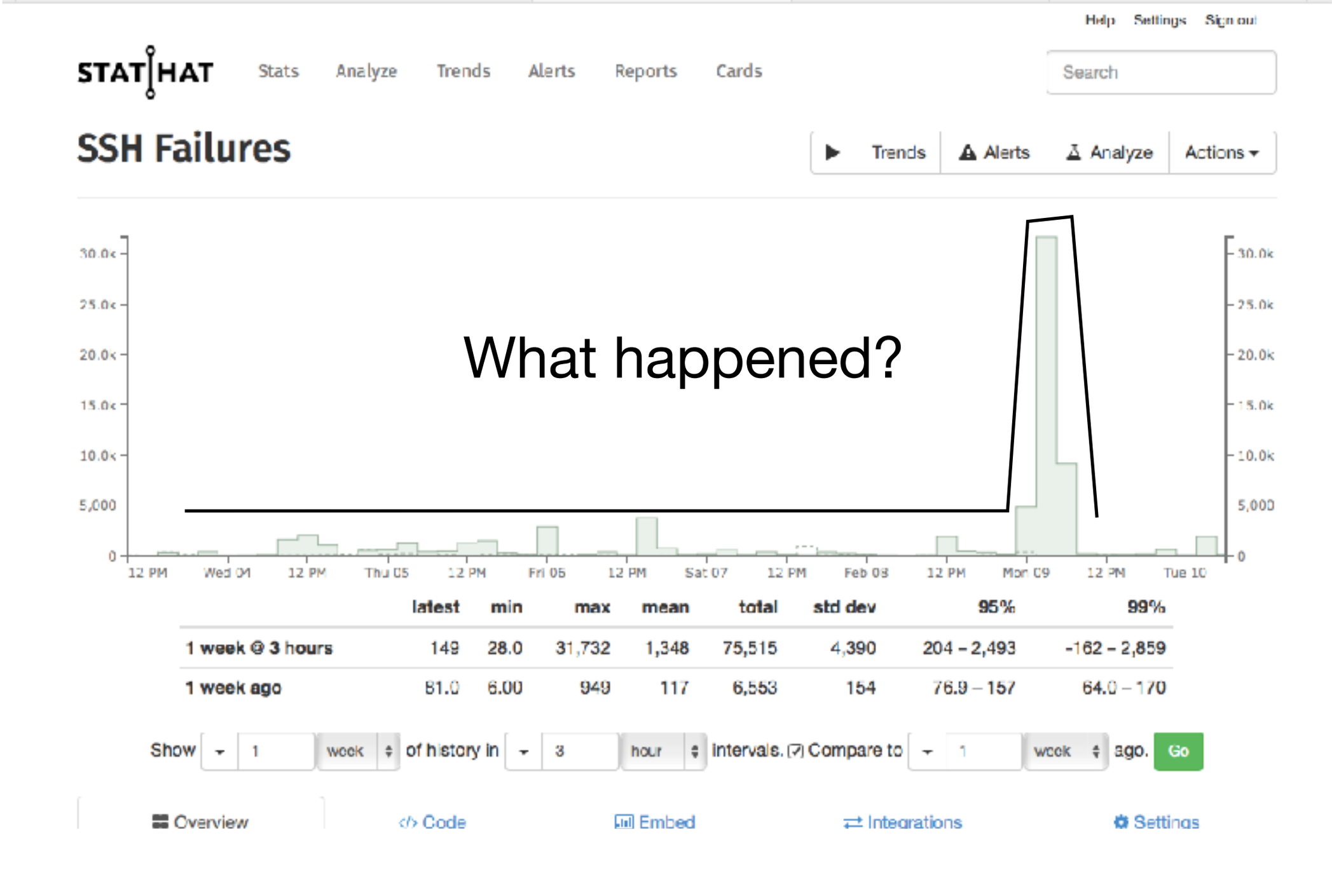
Network Security 8: Virtual Firewalling

i.g.batten@bham.ac.uk

Before we start…



```
Feb 10 03:55:36 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 4736 ssh2
Feb 10 03:55:41 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 4455 ssh2
Feb 10 03:55:41 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 4455 ssh2
Feb 10 03:55:41 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 4455 ssh2
Feb 10 03:55:44 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 4804 ssh2
Feb 10 03:55:44 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 4804 ssh2
Feb 10 03:55:44 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 4804 ssh2
Feb 10 03:56:04 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 3673 ssh2
Feb 10 03:56:05 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 3673 ssh2
Feb 10 03:56:05 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 3673 ssh2
Feb 10 03:56:07 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 1373 ssh2
Feb 10 03:56:07 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 1373 ssh2
Feb 10 03:56:07 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 1373 ssh2
Feb 10 03:56:10 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 1373 ssh2
Feb 10 03:56:10 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 1373 ssh2
Feb 10 03:56:10 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 1373 ssh2
Feb 10 03:56:12 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 1373 ssh2
Feb 10 03:56:12 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 1373 ssh2
Feb 10 03:56:12 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 1373 ssh2
Feb 10 03:56:14 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 1373 ssh2
Feb 10 03:56:15 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 1373 ssh2
Feb 10 03:56:15 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 1373 ssh2
Feb 10 03:56:23 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 3367 ssh2
Feb 10 03:56:23 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 3367 ssh2
Feb 10 03:56:24 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 3367 ssh2
Feb 10 03:56:26 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 3968 ssh2
Feb 10 03:56:26 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 3968 ssh2
Feb 10 03:56:26 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 3968 ssh2
Feb 10 03:56:31 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 3109 ssh2
Feb 10 03:56:32 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 3109 ssh2
Feb 10 03:56:32 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 3109 ssh2
Feb 10 03:56:37 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 3577 ssh2
Feb 10 03:56:37 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 3577 ssh2
Feb 10 03:56:37 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 3577 ssh2
Feb 10 03:56:55 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 4316 ssh2
Feb 10 03:56:55 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 4316 ssh2
Feb 10 03:56:55 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 4316 ssh2
Feb 10 03:56:57 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 4576 ssh2
Feb 10 03:56:57 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 4576 ssh2
Feb 10 03:56:58 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 4576 ssh2
Feb 10 03:57:03 research-1.batten.eu.org sshd: [ID 800047 auth.notice] Failed password for root from 222.186.51.150 port 2217 ssh2
```

Geo IP Tool

View my IP information | More info about IPs | Language

Host/IP

Hostname: 222.186.51.150

IP Address: 222.186.51.150

Country: China

Country Code: CN (CHN)

Region: Jiangsu

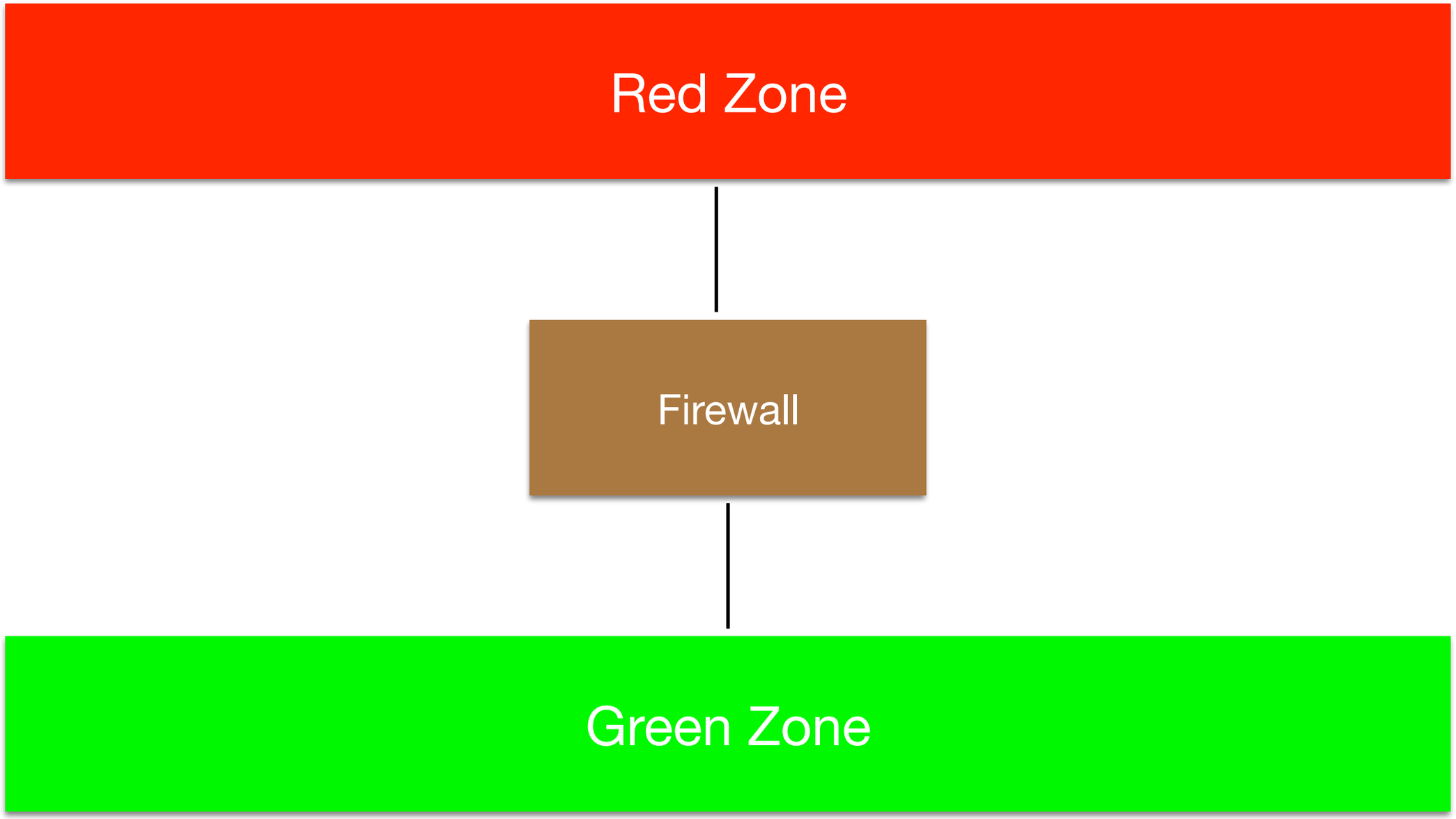
City: Nanjing

Local time: 10 Feb 22:47 (CST+0800)

Latitude: 32.0617

Longitude: 118.7778

Physical Firewalls, Physical Networks



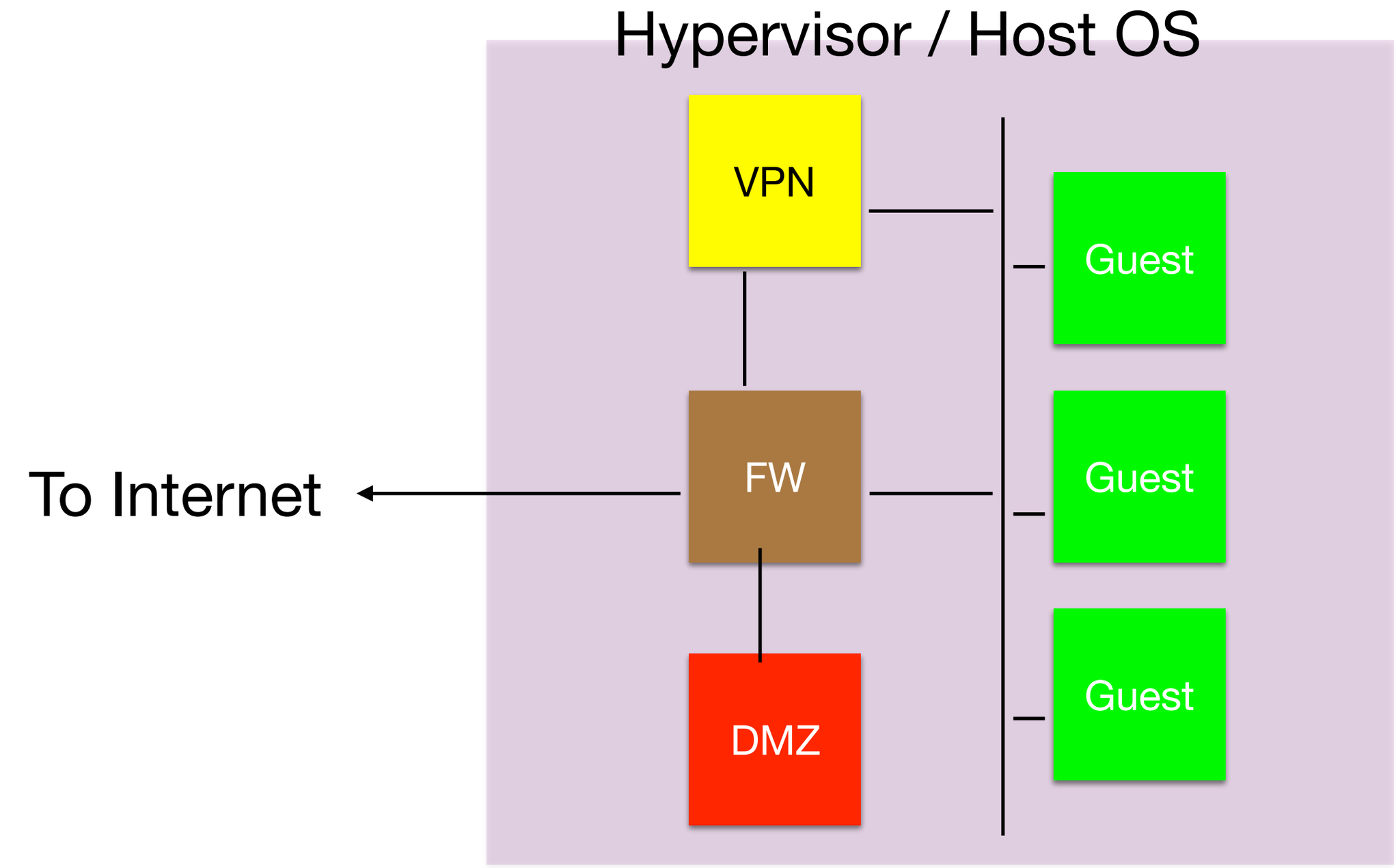
Reality is Virtual

- Virtual **Networks**
- Virtual Firewalls
- Virtual Hosts
- All of the above can exist within one computer

Purpose of Today

- Two different meanings of, and approaches to, virtualisation

Virtualisation



Definitions

- Problem with word “Virtual” is that it means many different things.
- In networking, a Virtual Network is a set of tags on a physical network
- In virtualisation, a Virtual Network is a purely software construct

VLANS

- An extra “tag” inserted into the Ethernet packet format, saying which network the packet belongs to.
  - 4 extra bytes ahead of type/size fields, first 16 bits 0x8100 to unambiguously mark “this is a tag” (no real untagged packet will have 0x8100 there), 3 bits of priority, 1 bit to specify if frame is droppable, 12 bits for tag.
  - Tag 0 is equivalent to untagged, tag 1 is often used internally by switches, tag 0xFFF (4095) is reserved.
- In principle, MAC addresses only need to be unique on a per-tag basis, but relying on this will break lots of switches.

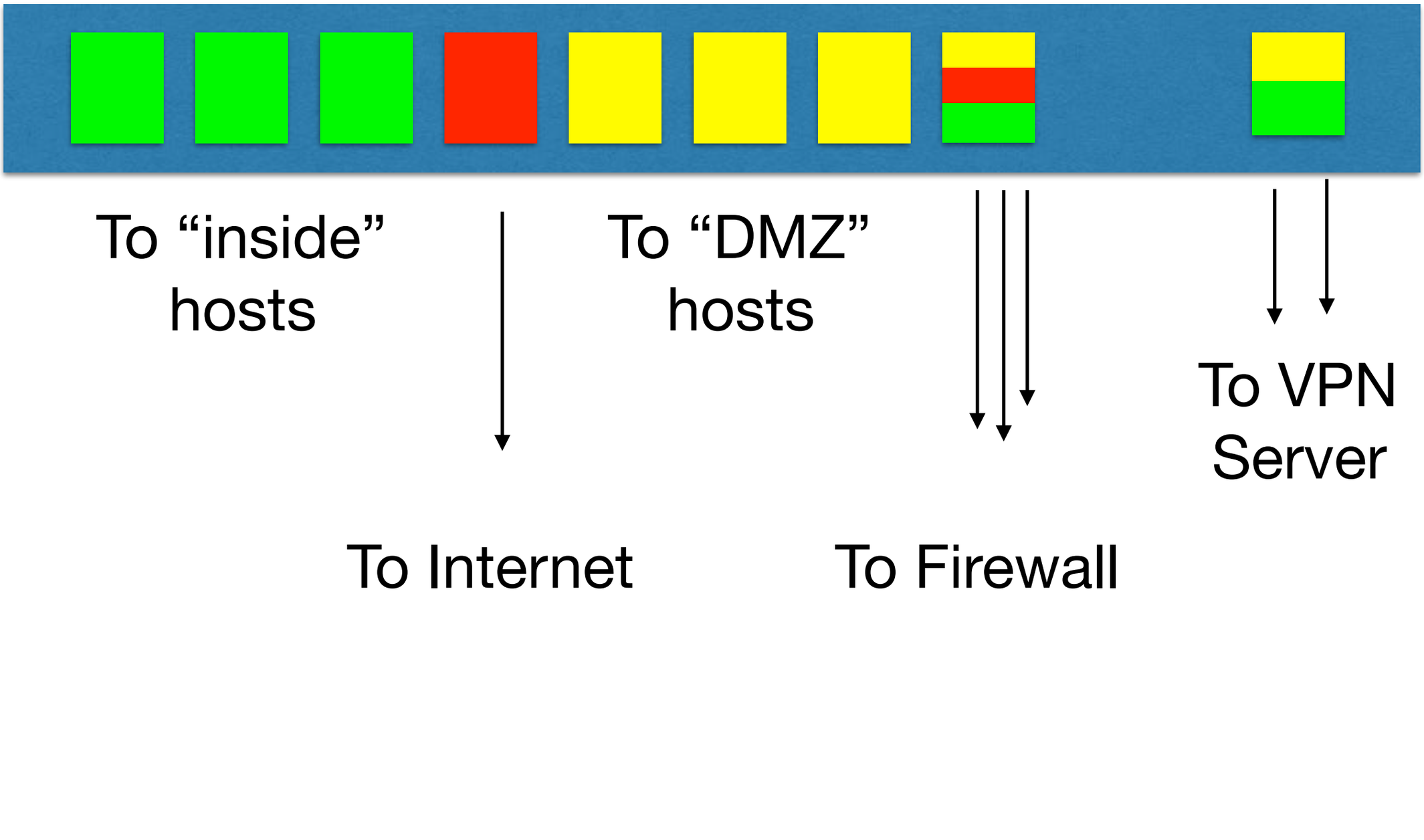
VLANS allow…

- Trunking of multiple networks along one cable
- Trunking of multiple networks through one interface
- Segregation of traffic by type, security label, etc

Common scenario

- Some ports of a switch “trunked” and carrying multiple VLANs with tagged packets, either to other switches, or VLAN-aware routers, firewalls, hosts.
- Some ports of a switch only carrying the default VLAN
- Some ports of a switch carrying a single non-default VLAN, untagged

Switch Config



Exercise Request

- I forgot to deal with the issue of interface names.
- If you can, it would be helpful if when you refer to interfaces in your script, you use variables, which you initialise at the top of your script with:
  - $inside_or_whatever=${SERVERNET-eth0}
  - $outside_or_whatever=${CLIENTNET-eth1}
- Where eth0 and eth1 are whatever your interfaces are called on your machine. That way, we can set the $SERVERNET and $CLIENTNET environment variables to make people's scripts work correctly, while your script continues to work normally.

Exercise Request

```
#!/bin/bash

inside=${CLIENTNET-eth0}
outside=${SERVERNET-eth1}

iptables -A FORWARD -i $inside …
iptables -A FORWARD -o $outside …
iptables -A FORWARD -i !$inside …

# and so on
```

Shell fun

- More generally, the things you can do (bash and ksh) with variables by writing ${variable□thing} where □ is punctuation are ~~horrifying~~ useful.

```
$ foo=XYZZY
$ echo $foo ${foo%Z*} ${foo%%Z*} ${foo:2:2} ${foo/X/A}
XYZZY XYZ XY ZZ AYZZY
$
```

Port Types

- “Tagged” or “Trunk” ports: each packet is marked with its tag (in sane networks, the global tag for its network: you can change the tags on a per-port basis, but you should not do this).
- “Untagged” or “Access” ports: packets are untagged, even if they originate from a non-default network.

Lots of ways to “see” VLANS

- You can get at them directly, as on (some) Linuxes:

Note MAC addresses

```
igb@pi-one:~$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr b8:27:eb:e1:96:51
          inet addr:10.92.213.231  Bcast:10.92.213.255  Mask:255.255.255.0
          inet6 addr: 2001:8b0:129f:a90f:ba27:ebff:fe00:efe7/64 Scope:Global
          inet6 addr: fe80::ba27:ebff:fee1:9651/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:88366 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69956 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8540091 (8.1 MiB)  TX bytes:12480470 (11.9 MiB)

eth0.5    Link encap:Ethernet  HWaddr b8:27:eb:e1:96:51
          inet addr:81.187.150.211  Bcast:81.187.150.223  Mask:255.255.255.240
          inet6 addr: 2001:8b0:129f:a90e:ba27:ebff:fe00:efe7/64 Scope:Global
          inet6 addr: fe80::ba27:ebff:fee1:9651/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:29632 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27889 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3565578 (3.4 MiB)  TX bytes:5562868 (5.3 MiB)
```

“eth0” is untagged traffic

“eth0.5” is traffic using VLAN tag 5

Virtual Interface per tag

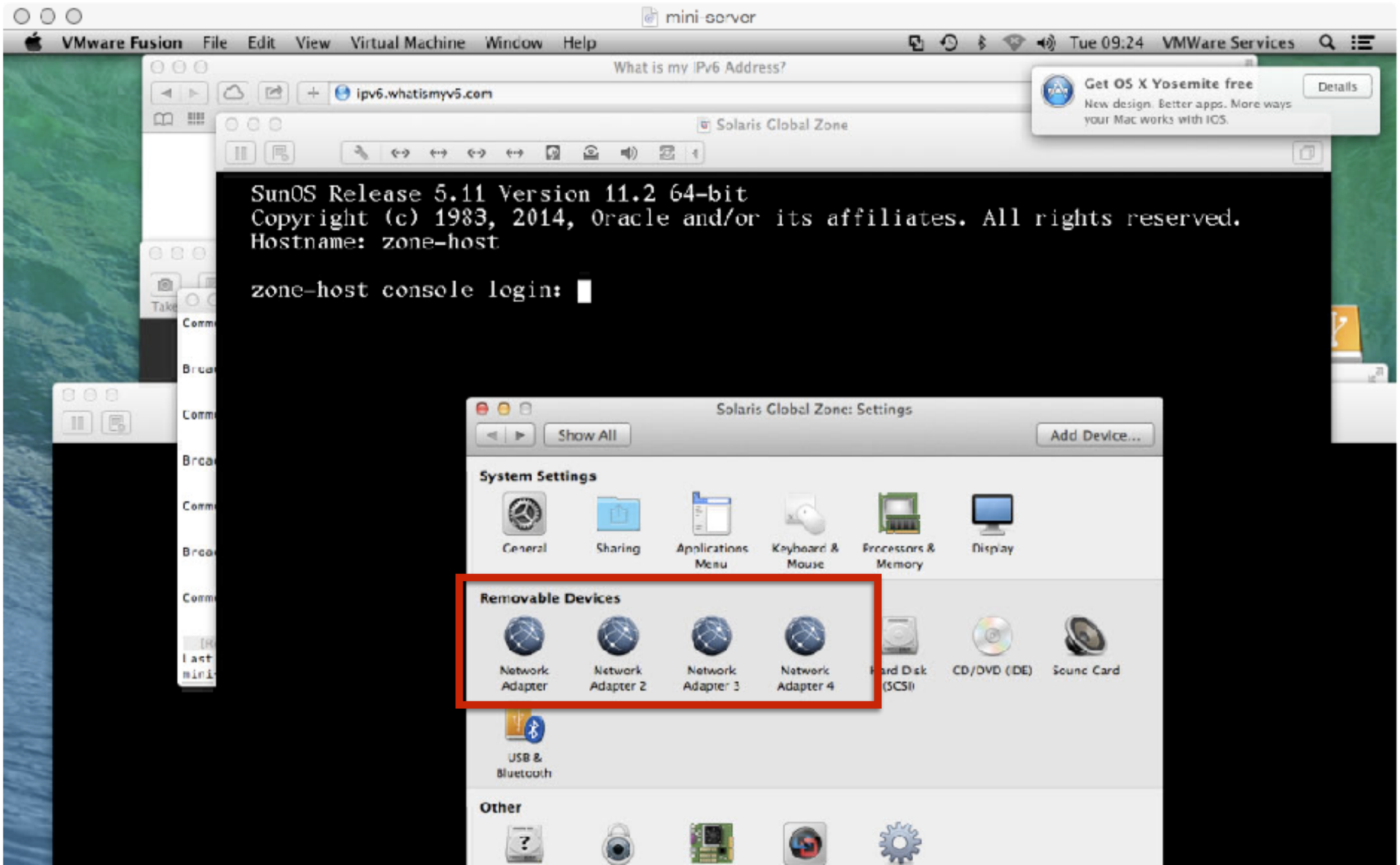
- You can see them as virtual interfaces, as on (modern) Solaris
- The physical link is the interface, then there are multiple virtual interfaces, one per tag

```
igb@research-1:~$ dladm
LINK                CLASS     MTU    STATE    OVER
net0                phys      1500   up       --
vnic6               vnic      1500   up       net0

igb@research-1:~$ dladm show-vnic vnic6
LINK                OVER              SPEED  MACADDRESS        MACADDRTYPE VIDS
vnic6               net0              1000   2:8:20:89:b5:a0   random      4008


igb@research-1:~$ ifconfig -a
net0: flags=100001000943<UP,BROADCAST,RUNNING,PROMISC,MULTICAST,IPv4,PHYSRUNNING> mtu 1500 index 2
        inet 147.188.192.246 netmask ffffff00 broadcast 147.188.192.255
vnic6: flags=120202000841<UP,RUNNING,MULTICAST,IPv6,CoS,PHYSRUNNING> mtu 1500 index 3
        inet6 fe80::8:20ff:fe89:b5a0/10
```

VLANs in Virtualisation



Tags have all been stripped

```
igb@zone-host:~$ dladm
LINK                CLASS     MTU    STATE    OVER
net1                phys      1500   unknown  --
net0                phys      1500   up       --
net2                phys      1500   up       --
ossec/net2          phys      1500   up       --
net3                phys      1500   up       --
ossec/net3          phys      1500   up       --
ossec/net0          vnic      1500   up       net0
igb@zone-host:~$
```

Good uses for VLANs

- Reducing the number of physical cables and interfaces used between a switch and a firewall
- Reducing the number of physical switches (you can use different tags with only access ports to split a single switch between disjoint networks, getting economies of scale)
- Bringing multiple networks into machines with insufficient physical interfaces (general case of firewall).

VLANs for segregation of management

- Telecoms practice divides hardware into three “planes”. It’s not common as a distinction in IT, but it’s a useful abstraction.
  - Management
  - Control
  - Data

Data Plane

- The actual switching of data, at speed and scale. Equivalent to the ethernet ports on an ethernet switch.

Control Plane

- Setting up calls, determining routes, and other less frequent, potentially higher impact, but usually automatic tasks
- Doesn’t always have a direct IT equivalent, but routing protocols like OSPF and BGP would fall into this category.
  - Not TCP SYN SYN/ACK ACK

Management Plane

- Reconfiguration of devices by manual action or by action of higher-level management systems
- Has ability to reroute traffic, shut down or reconfigure interfaces, etc, etc.
- Real telecoms equipment does not allow “in-band management” — you cannot cross to the management plane from the data plane.

Building a Management Plane

- Some very high-end, specialised equipment does have a separate management port, through which the equipment can be managed.
- It's rare for that port to be the **only** way to manage the device, and running separate cabling is a pain
- With care, you can use VLANs to get much of the benefit

Management VLAN

- Only listen for management traffic on one particular VLAN: packets for management must have that tag
- Why doesn’t this work without more care?

VLANs are insecure

- Anyone can put any tag on any packet
- VITAL that you police tags where they enter “trusted” (roughly, physically secure) parts of your network, by stripping tags that are not expected from edge ports

802.1x might have a role

- There are various dynamic solutions which allow you to configure switch ports based on MAC addresses, authentication material and so on.
- They are messy and tricky to get right (see previous discussion on 802.1x) but the alternatives can be messy as well.
- Planning a VLAN infrastructure requires a lot of thought.
- If I had my time again, I would not use default VLAN, and would tag **everything** except on access ports.
  - Usually you aren’t starting from a green field, and no-one uses VLAN tagging on their first switch.