
Calvin's Docs Documentation

Calvin Bui

Sep 13, 2018

Infrastructure:

1	ESXi	1
2	FreeNAS	5
3	Domain Controller	7
4	Networking	11
5	pfSense	13
6	Telstra Modem	19
7	Switch	21
8	UniFi	23
9	OpenVPN	25
10	Server	27
11	Printer	29
12	UPS	31
13	IPMI	33
14	Downloader	35
15	Surveillance	37

Networking	
Hostname	esxi
IP	10.0.0.3
Website	https://10.0.0.3
Software	
Version	6.5.0 U1 b5969303
Last Updated	Aug 3 2017
Hardware	
CPU	E3-1230v3
Memory	32GB DDR3

Currently installed on a 16GB Cruzer Blade (mpx.vmhba32:C0:T0:L0)

1.1 Update ESXi

Go [here](#) and click on the latest Imageprofile

1.2 Licenses

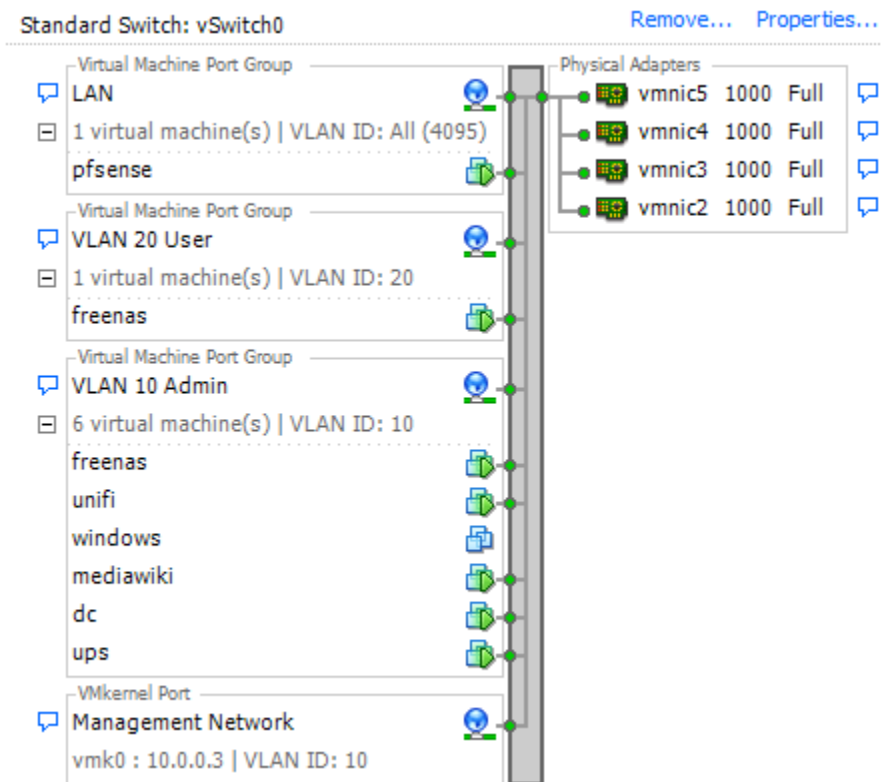
ESXi 6.0 FREE License from VMware, works with 6.5

(Decrypt with OpenSSL)

U2FsdGVkX1/7Sozs6M4f650PqfEPMSXY4ts26Cir8D4lA3rPMm9LiQXNetw9yqNX

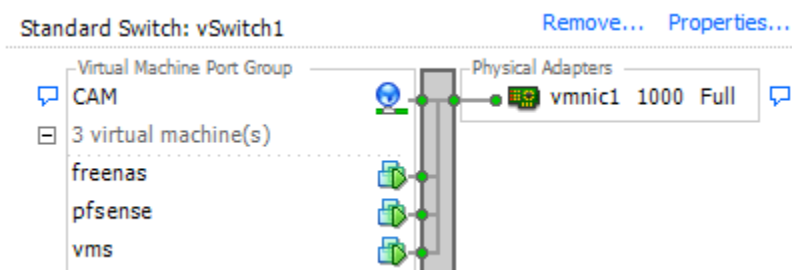
1.3 vSwitchs

1.3.1 vSwitch 0

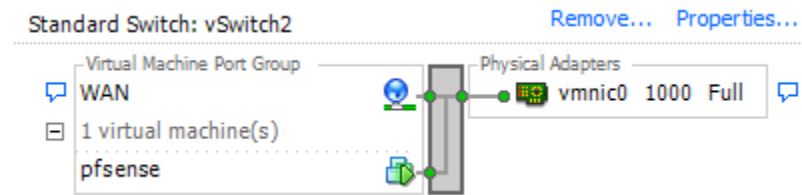


- All port groups are set to **Route Based on IP Hash**

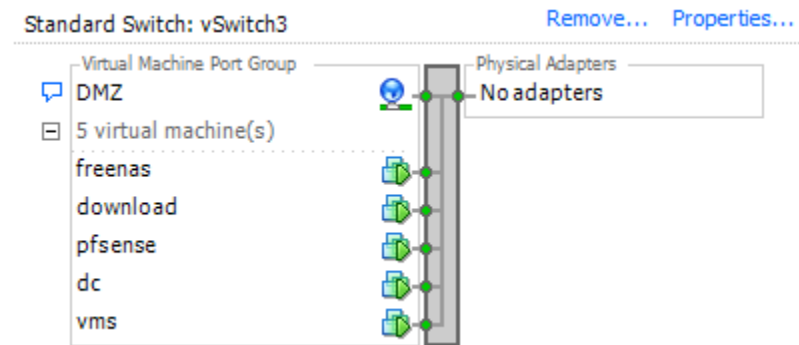
1.3.2 vSwitch 1



1.3.3 vSwitch 2



1.3.4 vSwitch 3



1.4 Storage

- HDD (10.0.0.5:/mnt/hdd)
- SSD (10.0.0.5:/mnt/ssd)
- RECORDING
- ZFS0 - dc, pfsense and freenas main drive
- ZFS1 - dc, pfsense and freenas mirrored

1.5 VM Startup and Shutdown

1. dc
2. pfsense
3. freenas (180 seconds)
4. ups
5. vms
6. the rest

Networking	
Hostname	freenas
IP	10.0.X.5
Virtual Machine	freenas
Software	
Version	FreeNAS 11.1
Last Updated	Feb 10 2018
Hardware	
CPU	4
Memory	16GB
Network	All
Storage	8GB (mirror ZFS0/1)
PCI Device	LSI2308

FreeNAS is the storage system holding everything together. It runs the **SSD** and **HDD** ZFS pools.

2.1 Pools

- Boot Drive: Mirrored (2x) on ZFS0 and ZFS1
- SSD: Mirrored (2x) 512GB Samsung 850 PRO
 - Mirror 0: da1p2 + da0p2
- HDD: Mirror (3x) in a stripe (RAID10)
 - Mirror 0: da5p2 + da4p2
 - Mirror 1: da7p2 + da6p2
 - Mirror 2: da3p2 + da2p2

2.2 Permissions

All files and folders should be owned by “nobody:HOME\Domain Users”

2.3 Access

2.3.1 CIFS/SMB

Available at /files and /ssd on all network interfaces.

Access available to domain users.

Permissions are handled through Windows Security via Active Directory (home.net) using the freenas service account.

Workgroup is set to HOME (Domain) so no Domain is required.

2.3.2 FTP

Access available to root on port 21

2.3.3 NFS

Serving NFSv4

Restricted IP access.

SSD: /mnt/ssd - Only 10.0.0.3 is allowed (ESXi) HDD: /mnt/hdd - 10.0.0.3 (ESXi) and 10.0.9.4 (Download)

2.4 Disks

(Decrypt with OpenSSL)

```
U2FsGvKX1/8pzLHffB0LyIiKO+H33t6KRGoSKe41DY2xA0yCFhPgFwH+lpuc9en
1hQBuvjiI1xby0cZJ9CNS6o1gL4rqA1QYPZkULNPsNUPUfg+4BP1539Q1c40rvc5
1t/BFiOI1iKzNn4xx3R6VNz84R1c6JTGnIMradReSFsbpzv8+RW5o1bcEUTNeFQI
DG1Hp/beSDY6vz+ZzTQKoOV3gfcfjVvdKr6jxCTYYWa+7e2JJA1sG5ONNRaE0eO
Y5R2pQ85Ror2EO94wuZZj2fOQOxAzWCBGiziRBG+VucaPVfz2HxMBN/94dmnfoWO
JY7ufj1NHK1tXUkKiTjk01foBGY6fUBZWGIHZhBmSBNj/uI7QG8uxmbpyBVeg9z0
vLzU9pGZDyhaFmPCemgzV5/Nw9qW5BaBuar/c3ZMjntJ9C6D2wZUH/sA7ZeRdVqJ
2Y0vrUAHNaf96GBN8eMW+Tr5RPNmyV04OW1zb0++FmI=
```

2.5 LSI 2308

Currently installed: PH20.00.08.00-IT

SAS Address 000000000

Latest versions: [ftp://ftp.supermicro.com/driver/sas/lsi/2308/Firmware/IT/](http://ftp.supermicro.com/driver/sas/lsi/2308/Firmware/IT/)

Boot into UEFI DOS Mode (built-in) and browse a connected USB to upgrade.

CHAPTER 3

Domain Controller

Networking	
Hostname	home.net
IP	10.0.0.16/10.0.9.10
Virtual Machine	dc
Software	
OS	Windows 2016
Last Updated	August 2017
Hardware	
CPU	4
Memory	2GB
Network	Admin + DMZ
Storage	80GB (mirror ZFS0/1)

Domain Controller, Active Directory, RADIUS server, Certificate Authority and DNS.

3.1 Domain

Runs the `home.net` domain

3.2 Active Directory (AD DS)

Users are broken into two categories: Real and Fake

`CN=Real, CN=Users, DC=home, DC=net`

Runs on port 389 and 636 (SSL)

- User naming attribute: `samAccountName`

- Group naming attribute: cn
- Group member attribute: memberOf

3.3 DNS

Currently forwards to 10.0.0.1 (ADDS Properties -> Forwarders)

3.4 RADIUS (Network Policy Server - NPS)

Current RADIUS clients: 10.0.0.7

Policies

- Network policy grants access to people in the 'HOMEPeople' group
- Connection Request policy is for 'Wireless - Other OR Wireless - IEEE 802.11'

Security

- Microsoft: Protected EAP (PEAP)

3.5 Certificate Authority (AD CS)

Required for LDAPS

CA Certificate

```
-----BEGIN CERTIFICATE-----
MIIDXzCCAkegAwIBAgIQH0J+6HSqh7RHJJa5uKLJCjANBgkqhkiG9w0BAQUFADBC
MRMwEQYKCZImiZPyLQGDBGYDbmV0MRQwEgYKCZImiZPyLQGDBGYEA9tZTEVMBMG
A1UEAxMMaG9tZS1BRERTLUNBMB4XDTE0MTAwOTA3MzIOM1oXDTM5MTAwOTA3NDI0
M1owQjETMBEGCgmSjomT8ixkARKWA25ldEUMBIGCgmSjomT8ixkARKWBghvWUx
FTATBgNVBAMTDGhvbWUtQUREUy1DQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAAJ5HigUI49W7X402s5XH4vsC+UBkaxqKqL+OFbRktf3lmmTas6/ZEGE9
MuXYdsCOL3U/jjTZfXRe4KEHTbWEgFWiBIZ6hg25RbTKzRv6c4n/CdIToI09Ec8F
4cLHvV0C5Se0MiP/7X5KQtzXIdyy6KS1p87wEqYe3nFaigZRTgx+QVSGskHMIJeO
ttLSV3k7EDMj+HeQaGZkIMMBguzr56Gbyl2oxY+V3lggfAs1IYVk/X6U0JP1dMTC
5ffOqjKSFTtxbbb47S4qzPaY7/H/LCVxObZ4ab/yW4VgOd0C5I+T25udBpa8psXj
FQQ7Qm9WjvnnjKywLu9Yr6HfDNG3y6UCAwEAAANRME8wCwYDVR0PBAQDAgGMA8G
A1UdEwEB/wQFMAMBAf8wHQYDVR0OBByEFPrFTh+nx6zgECM/h00YyIT67ZKAMBAG
CSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEBBQUAA4IBAQAADHHR2PBNAfFnBD0Y9
xdIvRXIfC19RDGMgRgvaTE8q8Z270+Cp4hJvbdEB0wJzCy551SYTbm3CU/FoJFH
z92h45ULZkf76XjEFp3B4ialpYiVVLc0tQUW799afGeRSWGvdwqvkb3FyQq5gTKH
eWSnngKlWI4wOj+Rlyxje/+Cu9SZrWmlbiRZo228JZb9cTdkxt1b6evJjZoJcF49
l/UYFBwnmzkQzVBxNP7prc7jDxXbHs3NfGY+8wzCKqdTYGJG9BioNAdWFIv5JwL
8FVx2OgTujk0yRMku1sUVG3ASfJG7SvtOfORHxntHr3PxbZk6H/zMTDfIwKRMdqw
RC+d
-----END CERTIFICATE-----
```

CA Decrypted Private Key (Decrypt with OpenSSL)

U2FsdGVkX19/EGAhI2rKlv4oDw0K1dOyLbRRC9hGDrV1LQiRobvbK4C2L6yL14Rh
JUDNS6/mGvL9sVvrKuQatd6nmfNkNDNWsc0ecKOV0VQrD2UiIN9WU1RwkqeASIBN
tlvl1lrhrwYpI8PuxiCpAZghUe8clK94Y0RqarqQ8DwWd4jgohYhv3xAwYoJh6ct
AFilhBACuZkbN4MVH3TfRA6k15jMvLssWE/RNHpk+XtV8fGWf1Rjm7K7ohjV8jog
RbW32UFAh1zab6cL1b1Kn6NF2/b5J0L97yEHgqVdXtk40ZzOAAzKJwZYU/bHU/GM
LU2GjvVxRgqzSa4xqF1qG1bqcYyQjKZPjUvBkkQMp5+wF8PNfHTLVpxtFB2ApZoS
MHVlWgBhp0U+nlx48eFxJIvGShqHUG9+7juJ9G06Afpv4sZaoAk99SzeSNjRRCsU
Ulht21/y7lyilrFW11oFDT9xNVq5tnuQxzg6MVz8Szo2gUC9sIYJP5mKoK+iOakX
K/1jEPX6542WkJ11v5qEEJ6BSj15Q1qSkjLTi72nRQUupjEjmwdu9eNdUbZOW8sN
nEUIH5g9D6qmRkU4rqYIXfRO4VNg7C6P1SIij/jM9QECGwG79L1q7M6JEbxjBsmS
pyYI7211YFIItVzhPtOQCcWFiJIAxMwvZRu+ZL6gtZuqIYLIId+3+9lKMkTyBWukP6
67Mox7UG2P0y0XRTTX/oZs+E6w6xH0xNINLXbr7AnnGbAOIqJhTXWQhPzglD5qGW
oSQ0xPva4jnLBXJeGvXNFPPlAtSxwTizpYYFpBRfs6q5zwLiToquWKzTXGevR+70
mXaR4E9GTNlyShZ8L8sC1kd1NpDuiA9ybQeVh7euWrdTQvS1QoWixSq+7ANp6KQw
mz/OT5snooV3Ph1/C+pUKgiOhuhYmhQdjZfgL0ReJ8e0IB/i/9yn4Tws+3QYrE9I
/vtVJG1T96qYtUePMzImT5FJsLnRNw1BELFKugPn9z8+GWCM/5jyqLJXGfcPobMI
+ri3Um5UblrItkM0RB+OMwjnjHU3qwyXJod1+Mq6MD8BuKQ7VSevojsloJoEEEx/C
hvcv3951T915R+UhtHstlj2nKn9NyCZm2jYhcnPcnkMiIfObtv2P0QYrP1JLMF3O
bUb88oTMEUNaiFhIngCvZXarR2LljLJg34gpUdxEW+BOSJ1QUXLtv007CEvp4yZb
zox+Rbud2MmZUDJY3wNhZS1jhQCg1gHZUFpFaOjTEw13ky+Uow22QSpnXSRLJ1c9
hOcyKQrI60KLnNYeQ36SIQjG/E7v8tALJSkSw2Ab0+c8k0XQD0GsoQdjviXmt8L
K96nMwXcoHW7cMjVnRbQTWy80gHCqIgUkOKn8G9UIjvdH3Qma/wJUGrVnnLZnpeo
cPGqUHe8FYRpyF5hr5zIIZQRD7TIhazlr4ITKcK8x12V76xZE4ybNPzGdt6M+sAu
BLfVtY3lFRS15hyZG7wfuK6VW7sqcxQ7iJXU5wUEpPGXh3OkO+U6C5PSIJ8I5VoE
pmIoXmi6mc5wLfmvZbFBVC5kyU1mG3qkAtdCYL5aGoIK9kAbUvblheG/oTPG3d5
8lgDQ81pj5hyNsNtntvsdzHUNWXFyF7LGcmFzUj19h+O/WmokBVlpQyQP6bVpWA
oZQ2g2UES4xQbs8Y7VG/mvzv2Xn7YxtD/eFjiVq1Tv22kLCv3IhVz2FXyaD6Ft2p
PJplN3kuEvUBx3pa+iNOK0rXcLQOsde5JJbBvOmk+5KUCRV3GmaZFS16uBd3haNF
hMS1463GrYeo4aTzo25oF3Q+ClVsWrAYfTCKwKR/nP+M94pHr3hIDSs0PM84PfIY
j9pIXEKYpMSXBp9faNaYV0AHQ/+tcKjsPMzCGz7tDP8wb5xE8FQko0+SGDNuo6uL
rULJ+NFxyUpCy0gNVnT6RSARBWJiDwzT3UGqNabxM8c8UL9fpGu7k/pYIvYrmWbq
X/1muEEQCpZUrcEOSDFpPhPA5tJfCD64cIZv/JDoqAKfYsetBtHACzw3uPruNzUR
elBBfDUotWs+253nBhuRFZPJ+4MmdmZCx+ZIo5rJJN+KUmaOFellSnWONFoUaERv
ku4h+v+1+uDGRASDFKwKIJ1w3HmzTApkKV1fZxKlr9wHkhQ7TTmNTRuwlwWxt5/W
vaqKk+7xW0NBz/+n7JtYK/aTW0fLAdncrQx2sLRYst5TkbzYXnocktSlPhI+0ixg
fyCmYpduVFUs8WJ47bn2swLj1VsrCVcq4S04apJM0XehQOkQOYEuppn2sC04g0NX

4.1 Ubuntu

/etc/network/interfaces

```
iface eth0 inet static
address 10.0.9.6
network 10.0.9.0
netmask 255.255.255.0
broadcast 10.0.9.255
gateway 10.0.9.1
dns-nameservers 10.0.9.1

iface eth0 inet static
address 10.0.0.6
network 10.0.0.0
netmask 255.255.254.0
broadcast 10.0.1.255
gateway 10.0.0.1
dns-nameservers 10.0.0.1
```

4.2 CentOS

/etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE="eth0"
ONBOOT=yes
TYPE=Ethernet
BOOTPROTO=static
NAME="System eth0"
IPADDR=10.0.0.9
NETMASK=255.255.254.0
```


Networking	
Hostname	pfsense
IP	10.0.100.0 / 10.0.X.1
Virtual Machine	pfsense
Website	https://10.0.0.1/
Software	
Version	2.4.2-RELEASE-p1
Last Updated	Feb 10 2018
Hardware	
CPU	1
Memory	512MB
Network	All
Storage	8GB (mirror ZFS0/1)

pfSense is an open source firewall/router computer software distribution based on FreeBSD. It is installed on a computer to make a dedicated firewall/router for a network and is noted for its reliability and offering features often only found in expensive commercial firewalls. It can be configured and upgraded through a web-based interface, and requires no knowledge of the underlying FreeBSD system to manage. pfSense is commonly deployed as a perimeter firewall, router, wireless access point, DHCP server, DNS server, and as a VPN endpoint.

5.1 Packages

- Avahi
- mailreport
- Open-VM-Tools
- openvpn-client-export
- snort

5.2 Firewall Rules

Floating

WAN

LAN

DMZ

VLAN10ADMIN

VLAN20USER

CAM

OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	0 / 0 B	IPv4 TCP/UDP	*	*	gateways	443 (HTTPS)	*	none			

Floating

WAN

LAN

DMZ

VLAN10ADMIN

VLAN20USER

CAM

OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	0 / 0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
	0 / 72 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
	0 / 11.21 MiB	IPv4 TCP	*	*	10.0.9.4	webserver	*	none		NAT	
	0 / 0 B	IPv4 UDP	*	*	WAN address	8080	*	none		OpenVPN wizard	
	0 / 0 B	IPv4 UDP	*	*	WAN address	8080	*	none		OpenVPN wizard	

Floating

WAN

LAN

DMZ

VLAN10ADMIN

VLAN20USER

CAM

OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	0 / 0 B	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	
	0 / 0 B	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
	0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Floating

WAN

LAN

DMZ

VLAN10ADMIN

VLAN20USER

CAM

OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	0 / 20.68 MiB	IPv4 *	DMZ net	*	DMZ address	*	*	none			
	0 / 1.19 MiB	IPv4 *	DMZ net	*	privatenetworks	*	*	none			
	1.713 K / 119.24 GiB	IPv4 *	DMZ net	*	*	*	*	none			

Floating

WAN

LAN

DMZ

VLAN10ADMIN

VLAN20USER

CAM

OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	34 / 18.15 GiB	IPv4 *	*	*	*	*	*	none			

Floating

WAN

LAN

DMZ

VLAN10ADMIN

VLAN20USER

CAM

OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	0 / 0 B	IPv4 *	10.0.2.6	*	NintendoUpdateServers	*	*	none		wii u block	
	0 / 3.76 MiB	IPv4 *	VLAN20USER net	*	VLAN20USER net	*	*	none			
	0 / 0 B	IPv4 *	VLAN20USER net	*	VLAN20USER address	*	*	none			
	0 / 0 B	IPv4 *	VLAN20USER net	*	infrastructure	*	*	none			
	0 / 0 B	IPv4 TCP	VLAN20USER net	*	10.0.9.4	80 - 8082	*	none		NVR	
	0 / 7 KiB	IPv4 *	VLAN20USER net	*	privatenetworks	*	*	none			
	0 / 0 B	IPv4 *	VLAN20USER net	*	*	*	*	none			

Floating

WAN

LAN

DMZ

VLAN10ADMIN

VLAN20USER

CAM

OpenVPN

Rules (Drag to Change Order)

5.2. Firewall Rules 15

5.3 DNS Entries

Host Overrides				
Host	Domain	IP	Description	Actions
3ds		10.0.2.7		 
cam-backyard		10.0.3.7		 
cam-driveway		10.0.3.8		 
cam-frontyard		10.0.3.6		 
cam-leftside		10.0.3.9		 
download		10.0.9.4		 
esxi		10.0.0.3		 
freenas		10.0.0.5		 
freenas-cam		10.0.3.5		 
freenas-dmz		10.0.9.5		 
freenas-user		10.0.2.5		 
ipmi		10.0.0.4		 
lifx		10.0.0.13		 
pfsense		10.0.0.1		 
pfsense-cam		10.0.3.1		 
pfsense-dmz		10.0.9.1		 
pfsense-user		10.0.2.1		 
printer		10.0.1.131		 
ps4-lan		10.0.2.3		 
ps4-wifi		10.0.2.4		 
switch		10.0.0.2		 
switch-cam		10.0.3.2		 
unifi		10.0.0.6		 
unifi-ap-1		10.0.0.7		 
ups		10.0.0.8		 
vms-cam		10.0.3.3		 
vms-dmz		10.0.9.3		 
wiiu		10.0.2.6		 
Domain Overrides				
Domain	IP	Description	Actions	
home.net	10.0.0.16		 	
home.net	10.0.9.10		 	

5.4 Dynamic DNS

Dynamic DNS Clients RFC 2136 Clients Check IP Services

Dynamic DNS Clients					
Interface	Service	Hostname	Cached IP	Description	Actions
WAN	CloudFlare	@.ac		use API key instead of password	  
WAN	Custom	vpn.me		vpn.me	  
WAN	Namecheap	@.io			  

 Add

5.5 Snort Suppress

```
#(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
suppress gen_id 120, sig_id 3

#(http_inspect) BARE BYTE UNICODE ENCODING
suppress gen_id 119, sig_id 4

#(spp_ssl) Invalid Client HELLO after Server HELLO Detected
suppress gen_id 137, sig_id 1

#(http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE
suppress gen_id 120, sig_id 8

#(http_inspect) DOUBLE DECODING ATTACK
suppress gen_id 119, sig_id 2

#(http_inspect) UNESCAPED SPACE IN HTTP URI
suppress gen_id 119, sig_id 33

#(ftp_telnet) FTP command parameters were too long
suppress gen_id 125, sig_id 3

#(http_inspect) JAVASCRIPT OBFUSCATION LEVELS EXCEEDS 1
suppress gen_id 120, sig_id 9

#(http_inspect) UNKNOWN METHOD
suppress gen_id 119, sig_id 31

#(http_inspect) IIS UNICODE CODEPOINT ENCODING
suppress gen_id 119, sig_id 7

#(ftp_telnet) Invalid FTP Command
suppress gen_id 125, sig_id 2

#(http_inspect) JAVASCRIPT WHITESPACES EXCEEDS MAX ALLOWED
suppress gen_id 120, sig_id 10
#(spp_sip) URI is too long
suppress gen_id 140, sig_id 3
```

(continues on next page)

(continued from previous page)

```
#!/usr/bin/perl -w
#(http_inspect) SIMPLE REQUEST
suppress gen_id 119, sig_id 32``
```

CHAPTER 6

Telstra Modem

Netgear CG3100D-2 provided by Telstra.

<http://192.168.100.1/>

6.1 Configuration

NAT Mode = Bridged Wireless disabled

Password in KeePass

Switch

Networking	
Hostname	switch
IP	10.0.0.2
Website	https://10.0.0.2/
Software	
Version	1.10.016
Last Updated	July 2015

D-Link DGS-1100-16 EasySmart Switch

7.1 Warranty

Limited Lifetime Warranty. This means the warranty will only end five years after D-Link (or its successor) discontinues sales of the product in Europe. You must register your product to get the Limited Lifetime Warranty (see below).

(Decrypt with OpenSSL)

```
U2FsdsGVkX19kOjKpDShVuMhrHUj5X9fJUpaL4ovP/gxQQ2oR48AazozkfaLU9JCQ
eYn0d/YzUJDx901isGXo2Q1VpwJpCoKFj8PnAQEzqdZMzf2wsebzHif9G7HpXMPB
Lw6cpcgXgzWngGkFSmkzREEHb/qo7gB5Ww/TDiLhEkK8nxIb/6WOVZ6REZpTAgB
lNLRO+ROAMgxxfcfcNl7+cuQjmlNnOOqDim0Ejhif4Ev1Jbkeg+ecgyVa5nIWo5eM
vX9t/aEGFuyTBFaerTiZAJ/yEc0dIkbb6Ct+40ZNvhTlY2Q2Y0/bNODUi0dDpPde
Nmi95w8A+Rl/htsm8tND51ulI997We1Cx1va+wetlx812fat7s669l/6bYgMiBOg
3BAO9WoSWk91nSIRpVq+9Qs1TreggR/YB3YOamAmnUYb/v4QLfXY6r+dDVtFcd5r
bwNlBMHLBbyYrsPFG49YV13QR0VP0Ua7ERlioETha55FQPeL6kfU5vX3lWwMBDPY
LCDVTKOj7vKMDCESM6Fr94qa3TODEQq2xQZau30S3IunYL+MfrM/AXZCYXXrvET9
cK87vDkvtYOgTsMho8UbUO7WLqyWRXL4mPN0qhce+jFBcyXeILAR5+8x1hIsyQAgr
/ojOHZ0unWSoInIPG2vyqtE57bemKAC3SGyIo+AT9hCGQpjpFbk9o3vQt+Vp0nk
tbA3o1JyPvOlprSX4vi9vSuWfcHmFZV+GTDi9Nsch8M=
```

7.2 Port Trunking

Port 1,2,3,4 are in a trunk group

7.3 IEEE 802.1Q VLAN

10 is Management VLAN (Admin)

999 is LAN

VID	Untagged	Tagged
1	None	None
10	1 to 12	13-16
20	None	12-16
999	None	None

7.4 Configuration and Firmware Backups

<https://github.com/calvinbui/documentation/tree/master/docs/network/switch>

Networking	
Hostname	unifi
IP	10.0.0.6
Virtual Machine	unifi
Website	https://10.0.0.6:8443
Software	
Version	5.5.20
Last Updated	Aug 3 2017
OS	Ubuntu 16.04.3 LTS
Hardware	
CPU	1
Memory	512MB
Network	Admin
Storage	8GB (SSD)

8.1 Installation

Deployed using <https://github.com/calvinbui/ansible-unifi>

8.2 Access Point

Model: UniFi AP-AC v2

IP Address: 10.0.0.7

Version: 3.7.58.6385

8.3 Wireless Networks

Wireless Networks

WLAN Group

Default







NAME ↑	SECURITY	GUEST NETWORK	VLAN	ACTIONS	
Calvin Admin	wpaesap			 EDIT	 DELETE
Calvin Hidden	wpapsk			 EDIT	 DELETE
Calvin User	wpapsk		20	 EDIT	 DELETE

8.4 RADIUS

Add to RADIUS server first.

10.0.0.16:1812

8.5 User Groups

The *Calvin User* group is limited to 8000/500.

CHAPTER 9

OpenVPN

OpenVPN is configured via pfSense to use the home.net backend for authentication.

Users will be tunneled through to 10.0.7.0/24

Find the installers here: <https://github.com/calvinbui/documentation/tree/master/docs/network/openvpn>

CHAPTER 10

Server

Take a look at <https://github.com/calvinbui/documentation/raw/master/docs/hardware/server/server.xlsx>

CHAPTER 11

Printer

Networking	
Hostname	printer
IP	10.0.1.131
Website	https://10.0.1.131
Software	
Version	05/25/2017 X/1.09/N
Last Updated	July 2017

Details: <https://www.brother.com.au/colour-laser-led-mfc/mfc-9340cdw-detail>

Model Name: Brother MFC-9340CDW

Serial: (Decrypt with OpenSSL) U2FsdGVkX18NmWQdTvTXtmjxhyCndpc6zeVd/6007nIze99CUsJe4aV/b03HMaD7

Main Firmware Version: X

Sub1 Firmware Version: 1.09

Sub2 Firmware Version: N1607192100

Memory Size: 256MB

Purchased 30/06/2017 from Mediaform Computer Supplies Pty Ltd on eBay

Networking	
Hostname	ups
IP	10.0.0.8
Virtual Machine	ups
Software	
Version	Agent 3.2.3
Last Updated	May 2017
Hardware	
CPU	1
Memory	1GB
Network	Admin
Storage	16GB (SSD)
USB Device	Cyber Power System

CyberPower PFC Sinewave Series 1300Va 780W UPS.

Must use the Virtual Appliance (PowerPanel Business Edition Agent) as it has the ability to shutdown ESXi. The Linux and Windows version does not.

12.1 Warranty

Comes with 2 years advance replacement including international batteries

Warranty is from 17/06/2014 to 17/06/2016

12.2 PowerPanel Business Edition Agent

The software which allows remote management of the UPS

- Alerts via email
- Shutdown, startup and reboot of UPS
- Shutdown of ESXi when power loss detected

Download Virtual Appliance from here: <https://www.cyberpowersystems.com/product/software/powerpanel-business-edition-for-virtual-machines/>

Login is admin:admin

12.3 Commands

```
sudo service ppbed stop
sudo service ppbed start
```

12.4 Shutdown Settings

No.	Event	Notify		Command		Shutdown	
		Initiated	Repeat	Initiated	Duration	File	As
1	⚡ Local communication lost in a power event	<u>5 sec.</u>	<u>Inactive</u>	<u>Inactive</u>	<u>< 1 sec.</u>		<u>30 sec.</u>
2	⚡ Remaining runtime will be exhausted	<u>Instant</u>	<u>Inactive</u>	<u>Inactive</u>	<u>< 1 sec.</u>		<u>Instant</u>
3	⚠ Utility power failure	<u>5 sec.</u>	<u>Inactive</u>	<u>Inactive</u>	<u>< 1 sec.</u>		<u>30 sec.</u>
4	⚠ Batteries are not present	<u>5 sec.</u>	<u>Inactive</u>	<u>Inactive</u>	<u>< 1 sec.</u>		<u>30 sec.</u>
5	⚠ Local communication lost	<u>5 sec.</u>	<u>Inactive</u>	<u>Inactive</u>	<u>< 1 sec.</u>		<u>30 sec.</u>
6	⚠ Available runtime is insufficient	<u>Instant</u>	<u>Inactive</u>	<u>Inactive</u>	<u>< 1 sec.</u>		<u>Inactive</u>
7	⚠ UPS is fatal abnormal	<u>Instant</u>	<u>Inactive</u>	<u>Inactive</u>	<u>< 1 sec.</u>		<u>Inactive</u>
8	ℹ Battery replacement recommended	<u>Instant</u>		<u>Inactive</u>	<u>< 1 sec.</u>		
9	ℹ Shutdown initiated	<u>Instant</u>		<u>Inactive</u>	<u>< 1 sec.</u>		
10	ℹ Battery is fully charged	<u>Instant</u>		<u>Inactive</u>	<u>< 1 sec.</u>		

Networking	
Hostname	ipmi
IP	10.0.0.4
Website	http://10.0.0.4
Software	
Version	03.45
Last Updated	May 2017

The Intelligent Platform Management Interface (IPMI) is a set of computer interface specifications for an autonomous computer subsystem that provides management and monitoring capabilities independently of the host system's CPU, firmware (BIOS or UEFI) and operating system. IPMI defines a set of interfaces used by system administrators for out-of-band management of computer systems and monitoring of their operation. For example, IPMI provides a way to manage a computer that may be powered off or otherwise unresponsive by using a network connection to the hardware rather than to an operating system or login shell.

13.1 Download

<https://www.supermicro.com/products/motherboard/Xeon/C220/X10SL7-F.cfm>

<ftp://ftp.supermicro.com/utility/IPMIView/Windows/>

CHAPTER 14

Downloader

Networking	
Hostname	download
IP	10.0.9.4
Virtual Machine	download
Website	http://10.0.9.4
Software	
OS	Ubuntu 16.04.2 LTS
Last Updated	May 2017
Hardware	
CPU	4
Memory	2GB
Network	DMZ
Storage	100GB (SSD, thin)

A machine which uses Docker agents containing several different programs for downloading files.

14.1 Deploy

This machine was set up using <https://github.com/calvinbui/ansible-usenet-docker>

14.2 Docker Containers

- NZBGet
- Sonarr
- Transmission
- NZB Hydra

- Sonarr
- CouchPotato

14.3 Certificates

Certificates are generated using Let's Encrypt on the host machine.

14.4 Folders

Everything is based under `/usenet`.

14.5 NFS Shares

The NFS share to HDD is under `/usenet/hdd`.

This is configred in `/etc/fstab`.

FreeNAS has allowed this by white-listing the IP (10.0.9.4).

Networking	
Hostname	vms
IP	10.0.3.3, 10.0.9.3
Virtual Machine	vms
Website	http://10.0.9.3
Software	
OS	Windows 10
Version	Milestone 2017 R3
Last Updated	December 2017
Hardware	
CPU	1
Memory	4GB
Network	CAM, DMZ
Storage	80GB (SSD, thin)

15.1 Cameras

There are currently four Hikvision DS-2CD2335-I cameras. Two are 2.8mm (wide) and two are 4.0mm (narrow).

- cam-backyard 10.0.3.7 (wide - 2.8mm)
- cam-driveway 10.0.3.8
- cam-frontyard 10.0.3.6 (wide - 2.8mm)
- cam-leftside 10.0.3.9

Use Hikvision SADPTool to configure from factory

Video

ROI

Display Info. on Stream

Stream Type

Main Stream(Normal)

Video Type

Video Stream

Resolution

2048*1536

Bitrate Type

Variable

Video Quality

Highest

Frame Rate

15

fps

Max. Bitrate

7680

Kbps

Video Encoding

H.264

H.264+

OFF

Profile

Main Profile

I Frame Interval

50

SVC

OFF

Smoothing

50

[Clear<=>Smooth]

Save

There is one **Xiaomi Xiaofang Camera** in my room. It is on the Admin network as it connects over Wi-Fi. The Xiaofang camera has hacks applied to it from <https://github.com/samtap/fang-hacks> which allows it to provide an RTSP feed to Milestone, via VLC. The default credentials are root:ismart12.

- cam-xiaofang 10.0.1.129

Special firewall rules are also in place to allow a connection from the Milestone server to the camera.

Floating

WAN

LAN

DMZ

VLAN10ADMIN

VLAN20USER

CAM

OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	0/0 B	IPv4 *	camera server	*	10.0.1.129	*	*	none			
	0/0 B	IPv4 *	*	*	natelwave	443 (HTTPS)	*	none			

15.2 Milestone XProtect Essential

Milestone XProtect Essential is the free VMS being used.

Limitations include:

- 8 cameras max
- No built-in motion detection/alerts
- Popups
- Logo on video exports

15.2.1 Settings

XProtect Essential 2016 R3 25 day retention (3 for Xiaofang) 15FPS 7680 Bitrate (Variable) H264 Resolution 2048 * 1536

15.2.2 Storage

SSD (C:\) provides the OS and Milestone software.

A Seagate Skyhawk 8TB (D:\) drive holds the recording files and archive storage.

15.3 Motion Detection

Motion detection is handled by the cameras internally. They are then FTP'd to the server which is running FileZilla under the hikvision username. The path shared is D:\OneDrive\Surveillance.

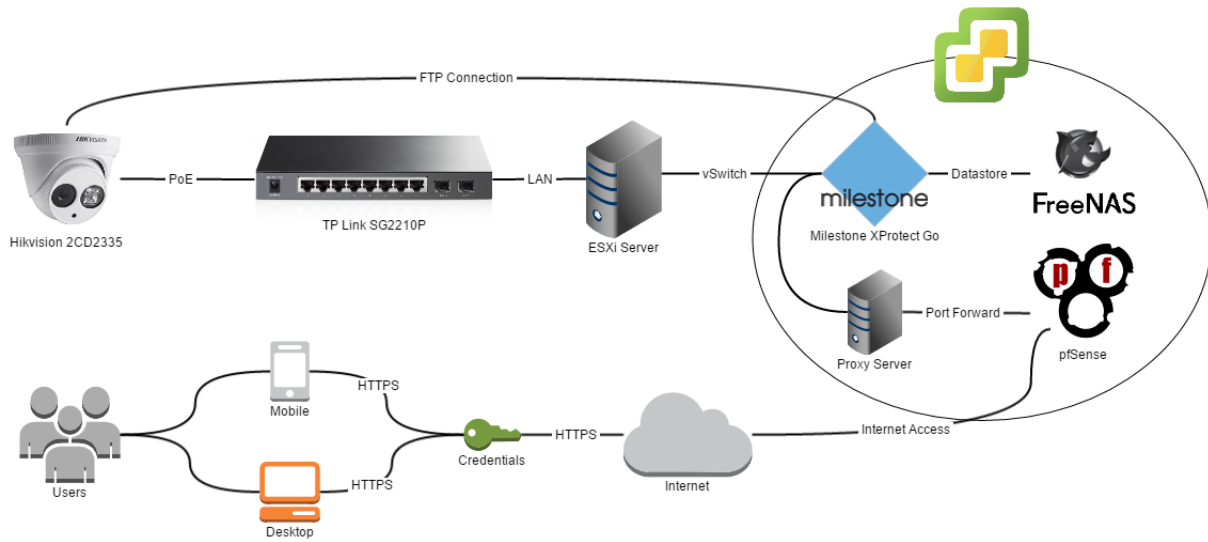
This is then uploaded to OneDrive.

This script (D:\remove_old_pictures.bat) is run daily by Windows Task Scheduler to delete pictures older than 14 days old.

```
forfiles /P "D:\\OneDrive\\Surveillance" /D -14 /C "cmd /c del @path"
```

Each image is prefixed with its name.

15.4 Networking



15.4.1 Switch

The cameras are connected to a TL-SG2210P switch.

There are no special configurations.

<http://10.0.3.2/>

<http://www.tp-link.com.au/download/TL-SG2210P.html#Firmware>

Firmware: 160912 (12/09/16)

Configuration backup available on GitHub <https://github.com/calvinbui/documentation/blob/master/docs/other/surveillance/switch.cfg>

15.4.2 Remote Access and Network Ports

To allow remote access, the gateway of the server is on DMZ (10.0.9.1).

It still has a CAM network adapter but without a gateway which shouldn't have a problem.

Speed is extremely slow when routed through CloudFlare

pfSense is currently port forwarding to 10.0.9.4.

NGINX from is proxying the Milestone web interface.

- HTTP enabled on 80 and 8081
- HTTPS enabled on 443 and 8082

15.5 NGINX Proxy Configuration

```
location / {
    proxy_pass http://vms-dmz:8081;
    proxy_buffering off;
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection "upgrade";
    proxy_set_header Host $host;
    proxy_set_header X-Forwarded-Proto $scheme;
    proxy_set_header X-Forwarded-For $remote_addr;
    proxy_set_header X-Forwarded-Port $server_port;
    proxy_set_header X-Request-Start $msec;
    proxy_set_header X-Real-IP $remote_addr;
}
```