ARFNET2 deployment

After the disastrous ISP schism

Masterplan

Stage 1: very safe

- Close all ports
- Nuke (or stop) all old VMs (exclude OPNSense)
- Make DMZ
- Make new basic VMs (cloning deb12 template)
- Open basic ports

Stage 2: new services

- IONOS VPS for mail
- Some new very safe services
- HE IPv6 tunnel
- Own authoritative nameservers for domain zone

*Stage 3: finally

- Another VPS in unknown provider for
  - Tor
  - Reverse-proxying the media library
- PHP on main site with more web services from scratch, hopefully secure
- More new services

Stage 4: DN42

- Make DN42 router VM with bird and wg
- Peer with people
- Bring up BGP sessions
- Services

Stage 5: Telephony

- Asterisk
- IP phones and ATAs
- Trunks; SDF, Tandmx, uwutel, PSTN

*Stage 6: Site B (piso)

- Firewall and switch
- Site to Site wireguard
- Establish telephony

*Stage 7: CA, PKI, LDAP and SSO

- Unify all logins
- Single authentication and authorization LDAP store
- SSO on as many services as possible
- Private CA PKI server certs for private endpoint security
- User certificates for extra secure endpoints

***Stage 8: Internal DNS**

- Drop OPNsense unbound, use BIND
- Use .local.arf20.com zone or something
- PiHole

Domain

arf20.com

Registrar: namecheap

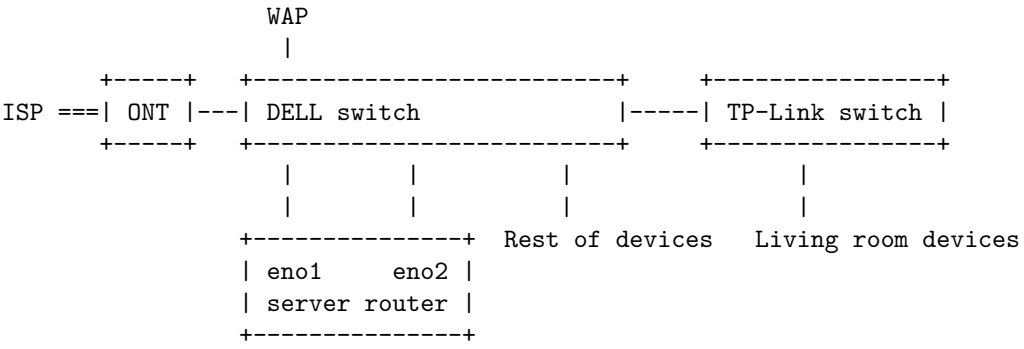
Name sever glue records at registrar

Nameserver	Name	IP
NS1	ns1.arf20.com	2.59.235.35 2600:70ff:f039:4::13
NS2	ns2.arf20.com	5.250.186.185 2001:ba0:210:d600::1

Networking

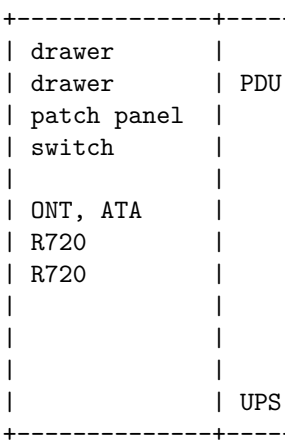
Hardware

Physical network



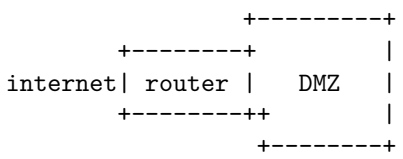

```
- 1000BASE-T
= GPON fiber
```

12U rack



- ONT: CPE Huawei GPON
- switch: DELL PowerConnect 5424
- server: DELL PowerEdge R720 @ 2x E5-2670 + 64GB + (240+120)GB SSD + (4+3x7RAID5)TB HDD
- ATA: Cisco/Linksys PAP2T

Logical network



DELL PowerConnect 5424 switch Port assignents

port	endpoint	options
g2	ONT	VLAN access 2
g4	server eno2 WAN	VLAN access 2
g6	test2	VLAN access 2
g3	WAP	VLAN access 5
g5	PC	VLAN access 4
g7	Living R.	VLAN access 5
g9	server eno1 DMZ+LAN	VLAN trunk 4, 5
g12	voip poe switch	VLAN access 9
g15	test4	VLAN access 4
g16	ATA	VLAN access 4
g17	test1	VLAN access 1
g19	test5	VLAN access 5
g21	iDRAC	VLAN access 4
g23	printer	VLAN access 4

Management

- interface vlan 4: 192.168.4.2/24 gw 192.168.4.1

Public IPs

- AVANZA_STATIC: 2.59.235.35
- AVANZA_CGNAT: dynamic 100.x.x.x
- HE prefixes
  - 2001:470:1f21:125::/64
  - 2600:70ff:f039::/48
- IONOS VPS: 5.250.186.185 2001:ba0:210:d600::1

Gateways

- AVANZA
  - WAN_STATIC: 2.59.235.1
  - WAN_CGNAT: dynamic
- HE v6 tunnel
  - server: 216.66.87.102, 2001:470:1f20:125::1/64
  - client: 2.59.235.35, 2001:470:1f20:125::2

Physical and Logical Networks

name	VLAN	net	desc
WAN	2		
DMZ	4	192.168.4.0/24 2600:70ff:f039:4::/64	Services
LAN	5	192.168.5.0/24 2600:70ff:f039:5::/64	Clients
VPN		192.168.6.0/24 2600:70ff:f039:6::/64	Wireguard clients
dark		192.168.7.0/24	dark IPsec remote subnet
B:PSN	un	192.168.18.0/24	Site-B:PisoNET
B:SBN		192.168.8.0/24	Site-B:SiteBNET
voip	9	192.168.9.0/24	VoIP
dn42	42	172.20.196.32/27 fdfd:acab:caca::/48	DN42 ARFNET-MNT

Firewall

Interface Rules

- WAN_CGNAT in
  - deny *
- WAN_STATIC in
  - allow v4 from * to {services} –> NAT rules
- DMZ in
  - deny v4 to LAN net
  - allow v4 to firewall
  - allow v4 to * gw WAN_STATIC
  - allow v6 to * gw HE_TUNNELV6
- LAN in
  - allow v4 ICMP to firewall
  - allow v4 IP DNS to firewall
  - allow v4 to DMZ net
  - allow v4 to * gw WAN_CGNAT
  - allow v6 to * gw HE_TUNNELV6
- Wireguard in
  - allow v4+6 to DMZ net
  - allow v4 to * gw WAN_CGNAT
  - allow v6 to * gw HE_TUNNELV6

IPv4 NAT Rules

Service	Customer	IPProto	Ext Port	Host	Re Port
WireGuard		UDP	51820	router	
DNS NS1		TCP/UDP	53	misc	
iperf3		TCP	5201	misc	
NNTP		TCP	119	misc	
Web		TCP	80,443	web	
Git		TCP	9418	web	
bittorrent		TCP/UDP	8999	nas	
rsync		TCP/UDP	873	nas	
IRC		TCP	6667	comm	

Service	Customer	IPProto	Ext Port	Host	Re Port
IRCS		TCP	6697	comm	
XMPP c2s		TCP	5222	comm	
XMPP s2s		TCP	5269	comm	
TURN STUN		TCP/UDP	3478	comm	
TURN		TCP/UDP	5349	comm	
TURN UDP relay		TCP/UDP	49152-50176	comm	
mc waterfall proxy		TCP	25565	game	25567
mc bedrock geyser		TCP	19132	game	19132
css-ds		TCP/UDP	27015	game	
hblink		TCP	54000	comm	
hbmon websocket		TCP	54000	comm	
exo ssh	exo	TCP	4041	exovps	22
exo extra	exo	TCP	4040	exovps	4040
yero ssh	yero	TCP	1511	yerovps	22
yero mc	yero	TCP	25569	yerovps	25565
yero panel	yero	TCP	24444	yerovps	24444

IPv6 port rules

Service	Customer	IPProto	Dest Host	Dest Port
DNS NS1		TCP/UDP	misc	53
Web		TCP	web	80,443
NNTP		TCP	misc	119
iperf3		TCP	misc	5201
Git		TCP	9418	web
bittorrent		TCP/UDP	8999	nas
rsync		TCP/UDP	873	nas
IRC		TCP	6667	comm
IRCS		TCP	6697	comm
XMPP c2s		TCP	5222	comm
XMPP s2s		TCP	5269	comm
TURN STUN		TCP/UDP	3478	comm
TURN		TCP/UDP	5349	comm
TURN UDP relay		TCP/UDP	49152-50176	comm
mc-waterfall-proxy		TCP	25565	game
exo-ssh	exo	TCP	4041	exovps
exo-extra	exo	TCP	4040	exovps
yero-ssh	yero	TCP	1511	yerovps
yero-sql	yero	TCP	1512	yerovps
FiveM SuperioresRP	yero	TCP/UDP	30120,40120	yerovps

Hosts

- server - DELL PowerEdge R720 running Proxmox PVE - ...
- mail - IONOS VPS running Debian 12 - 5.250.186.185 2001:ba0:210:d600::1
- dark - HostMeNow VPS running Debian 12 - 92.60.77.4

Management

- OPNSense router DMZ.1
- DELL switch DMZ.2
- TP-Link WAP LAN.2
- Proxmox hypervisor DMZ.4
- DELL server iDRAC DMZ.5
- HP printer DMZ.7
- Linksys ATA DMZ.18

server VMs and services

server runs Proxmox PVE.

All VMs are Debian 12 (templated) with wazuh agent

proxmox DMZ.4 (hypervisor)

- SSH
- Proxmox management interface :8006
- smartmon + node exporter :9100
- sensor exporter*
- NUT - Network UPS TOols daemon (and proper UPS)*

router DMZ.1

- (routing/firewalling)
- SSH
- DHCP
- unbound DNS
- OpenVPN
- WireGuard
- IPsec
- ntopng :3000
- telegraf - note: editing config via webfig breaks (timeout and unbound config)

nas DMZ.6

RAID attached here (with the grey stuff) (local only)

- SSH
- NFS
- Samba SMB*
- MiniDLNA*
- FTP
- qBittorrent-nox
- jellyfin
- nginx
- mpd :8000

vhost	webroot/proxy	Comment
dark.arf20.com	/d/FTPServer/	Allow only VPS and private

web DMZ.9

- SSH

- cerbot
- nginx (status at :8080)
- fastcgi PHP
- mariadb SQL
- nginx-prometheus-exporter :9113
- prometheus :9090
- telegraf
- influxdb :8086
- grafana :3000
  - Proxmox
  - nginx
  - iDRAC
- zabbix*
- netbox*
- fcgiwrap
- git-http-backend - git smart http server CGI
- gitd - git daemon
- cgit - web frontend for git
- phpBB - forum software
- Jekyll - blog static site generator thing
- opentracker? - bittorrent tracker*
- gophernicus - gopher server*
- photoprism - photo shit
- squid - http proxy server :3128

vhost	webroot/proxy	Comment
default	<return 418 im a teapot>	
default:8080	<return nstub_status>	
arf20.com	/var/www/arf20.com/html/	
www.arf20.com	<301 redirect arf20.com>	
matrix.arf20.com	http://comm.lan:8008/_matrix	
webmail.arf20.com	/var/www/webmail.arf20.com/html/	SquirrelMail
nextcloud.arf20.com	/var/www/nextcloud.arf20.com/html/	
grafana.arf20.com	http://localhost:3000	
jellyfin.arf20.com	http://nas.lan:8096	
git.arf20.com	/srv/git/	
cgit.arf20.com	fastcgi:/usr/lib/cgit/cgit.cgi	
blog.arf20.com	/var/www/blog.arf20.com/_site/	
forum.arf20.com	/var/www/forum.arf20.com/html/	
deb.arf20.com	/d/FTPServer/software/debian/	
memes.arf20.com	/var/www/memes.arf20.com/, /d/FTPserver/{dcimg, dcmemes, explosionsandfire}	
news.arf20.com	Web-News NNTP newsgroups frontend	
dash.arf20.com	/var/www/dash.arf20.com/html/	CSTIMS
ftp.arf20.com	/d/FTPServer/public/	
photo.arf20.com	[::1]:2342	photoprism
radio.arf20.com	/ = /var/www/radio.arf20.com/html/; /stream = nas:8000	
os.arf20.com	/ = /d/FTPServer/OS/	
dark.arf20.com	/ = /var/www/dark.arf20.com/html/	
wiki.arf20.com	/usr/share/dokuwiki	
qbt.arf20.com	http://192.168.4.6:8085	

vhost	webroot/proxy	Comment
radarr.arf20.com	http://192.168.4.6:7878	
sonarr.arf20.com	http://192.168.4.6:8989	
kanboard.arf20.com	/ = /var/www/kanboard.arf20.com/html/	
vw.arf20.com	http://192.168.4.10:8000	
raip.arf20.com	/ = /var/www/raip.arf20.com/html/status = http://comm.lan:8080	
pki.arf20.com	/ = /var/www/pki.arf20.com/html/download/ = http://ca.lan:80	
testcert.arf20.com	/ = /var/www/testcert.arf20.com/html/	
status.yero.dev	http://yerovps.lan:3001	
panaland.arf20.com	/var/www/panaland.arf20.com/html/	

secure DMZ.10

- SSH
- nginx
- php-fpm8.4
- wazuh*
- vaultwarden :8000
- OpenLDAP slapd :389
- ldap-account-manager :8389

vhost	webroot/proxy	Comment
:8389	/ = /usr/share/ldap-account-manager	

game DMZ.11

- SSH
- waterfall (minecraft reverse proxy) :25565
  - mclobby (auth)
  - minepau*
- panaland mc modded :25566
- css dedicated server :27015

comm DMZ.12

- SSH
- cerbot
- unrealircd - IRC
- synapse - matrix
- postgresql - DB for synapse
- pantalaimon - encrypt matterbridge traffic to matrix
- matterbridge - bridge channels with different protocols
  - discord
  - matrix
  - irc
  - xmpp
- prosody - XMPP
- coturn - TURN server for matrix and xmpp
- asterisk - VoIP SIP PBX

- hblink :54000
- hbmon :8080 :9000 wesocket

Dialplan

- 1xxx -> users
- 2xxx -> services
- 8xxxxxxx -> tandmx
- 733xxxx -> SDF
- 0119xxxxxxx -> uwutel
- xxxxxx -> regional PSTN
- xxxxxxxxx -> national PSTN
- 00x! -> international PSTN

number	description
2000	IVR
2001	conference
2002	time
2003	voicemail
2100	test hello world
2101	test digits 10
2102	test echo
1000	alias for operator
1001	Site A ATA p1
1002	Site A ATA p2
1011	Site B ATA p1
1012	Site B ATA p2
1021	soft phone 1
1022	soft phone 2
1031	remote phone 1
1032	remote phone 2
1051	cisco 3911 1
1101	cisco 7941

misc (Deb12 LXC) DMZ.13

- SSH
- iperf3
- bind9 - master authoritative nameserver for arf20.com zone NS1
  - public recursive*
- INN2 - NNTP USENET server with SDF peering
- Discord servers
  - gDebrid (gookie)
- squid - HTTP proxy
- microsocks - SOCKS5 proxy

t2 (T/2 SDE build box) DMZ.15

pubnix (OpenBSD 7.5) DMZ.16

- SSH

cucm (Cisco Unified Communications Manager) DMZ.19

callbox DMZ.20

- Amarisoft Callbox

dn42 DMZ.21

- (ip forward)
- wireguard
- bird eBGP daemon
- bind9 master arfnet.dn42

peer	asn	bgp
prefixlabs	4242421240	fe80::1240
routedbits	4242420207	fe80::207
lezi	4242423377	fe80::3377
carlos	4242420034	172.23.34.1
exo	4242421112	fe80::dead

dn42-services DMZ.23

- bind9 slave
- nginx reverse proxy

vhost	webroot/proxy	comment
arfnet.dn42	http://192.168.4.9	ARFNET in DN42

open5gs DMZ.22

Remote gNodeB

- Open5GC
- Kamailio
- OAI?

arfnet2-ca DMZ.24 Debian 12 CT

Certificate Authority PKI

- clca
- OpenXPKI
  - serverd
  - clientd
- apache2 :80

---

mail (ARFNET-IONOS VPS) 5.250.186.185 2001:ba0:210:d600::1

- SSH
- certbot
- postfix - MTA smtpd, submission, submissions config
- dovecot - imapd
- opendkim
- opendmarc

- bind9 - slave authoritative nameserver NS2
- mlmmj - mailing list manager
  - installed to /usr/local/bin/mlmmj-webarchiver.sh and /etc/mlmmj-webarchiver
- mlmmj-webarchiver - mailing list archiver

vhost	webroot/proxy	Comment
default	<return 418 im a teapot>	
lists.arf20.com	/ = /var/www/lists.arf20.com/html/ /archive = /srv/www/htdocs/archive/	Mailing lists

proxy (ARFNET-HOSTMENOW VPS) 92.60.77.4

- SSH
- IPsec tunnel
- nginx reverse proxy to nas

vhost	webroot/proxy	Comment
default	<return 418 im a teapot>	
jokesondmca.mooo.com	http://nas/	Stuff

---

yero-debian VPS DMZ.192 (yero)

- SSH
- mariadb
- FiveM SuperioresRP

exo-debian VPS DMZ.195 (exo)

- SSH
- netbox

loofa-debian VPS DMZ.196 (loofa)

- SSH
- ?

*TODO

Internal Name and Number Assignation Table

DMZ IPv4s and IPv6 ends in the same way

Addr	Name	Description
DMZ.1	router.lan	OPNSense managent
DMZ.2	switch.lan	DELL PowerConnect 5424 management
DMZ.3	wap.lan	TP-Link Omada AP255
DMZ.4	proxmox.lan	Proxmox VE management
DMZ.5	idrac.lan	DELL R720 iDRAC7 management
DMZ.6	nas.lan	
DMZ.7	printer.lan	HP Officejet 8020
DMZ.8	desktop.lan	reserved for desktop on DMZ

Addr	Name	Description
DMZ.9	web.lan	
DMZ.10	secure.lan	
DMZ.11	game.lan	
DMZ.12	comm.lan	
DMZ.13	misc.lan	
DMZ.15	(t2)	T/2 SDE build box
DMZ.16	pubnix	
DMZ.17	[reserved]	for future raspi
DMZ.18	ata.lan	Linksys ATA
DMZ.19	cucmelan	Cisco CallManager
DMZ.20	callbox.lan	5G gNodeB
DMZ.21	dn42.lan	DN42 edge router
DMZ.22	open5gs.lan	Open5GS 5G core
DMZ.23	dn42-services.lan	DN42 service machine
DMZ.24	ca.lan	Certificate Authority
DMZ.192	yero-debian	yero.lan
DMZ.195	exo-debian	exo.lan
DMZ.196	loofa-debian	loofa.lan

Site-B:PiSoNet

Addr	Name	Description
PSN.1		Huawei CPE Combo Box
PSN.2		DELL switch on untagged
PSN.3		Mikrotik firewall downstream
PSN.4		Grandstream ATA
PSN.8		desktop (when applies)

DNS

Public domain zone

Name	Type	Content	Comment
@	NS	ns1.arf20.com	
@	NS	ns2.arf20.com	
ns1	A	2.59.235.35	
ns1	AAAA	2600:70ff:f039:4::13	
ns2	A	5.250.186.185	
ns2	AAAA	2001:ba0:210:d600::1	
arf20.com	A	2.59.235.35	
arf20.com	AAAA	2600:70ff:f039:4::9	
mail.arf20.com	A	5.250.186.185	ARFNET-IONOS
mail.arf20.com	AAAA	2001:ba0:210:d600::1	ARFNET-IONOS
web.arf20.com	A	2.59.235.35	
web.arf20.com	AAAA		
game.arf20.com	A	2.59.235.35	

Name	Type	Content	Comment
game.arf20.com	AAAA	2600:70ff:f039:4::11	
comm.arf20.com	A	2.59.235.35	
comm.arf20.com	AAAA	2600:70ff:f039:4::12	
misc.arf20.com	A	2.59.235.35	
misc.arf20.com	AAAA	2600:70ff:f039:4::13	
pubnix.arf20.com	A	2.59.235.35	
pubnix.arf20.com	AAAA	2600:70ff:f039:4::16	
irc.arf20.com	CNAME	comm.arf20.com	
jellyfin.arf20.com	CNAME	web.arf20.com	
matrix.arf20.com	CNAME	web.arf20.com	
nextcloud.arf20.com	CNAME	web.arf20.com	
turn.arf20.com	CNAME	comm.arf20.com	
webmail.arf20.com	CNAME	web.arf20.com	
www.arf20.com	CNAME	web.arf20.com	
xmpp.arf20.com	CNAME	comm.arf20.com	
xmppconf.arf20.com	CNAME	comm.arf20.com	
grafana.arf20.com	CNAME	web.arf20.com	
git.arf20.com	CNAME	web.arf20.com	
cgit.arf20.com	CNAME	web.arf20.com	
blog.arf20.com	CNAME	web.arf20.com	
forum.arf20.com	CNAME	web.arf20.com	
deb.arf20.com	CNAME	web.arf20.com	
zabbix.arf20.com	CNAME	web.arf20.com	
memes.arf20.com	CNAME	web.arf20.com	
news.arf20.com	CNAME	misc.arf20.com	
dash.arf20.com	CNAME	web.arf20.com	
ftp.arf20.com	CNAME	web.arf20.com	
photo.arf20.com	CNAME	web.arf20.com	
radio.arf20.com	CNAME	web.arf20.com	
os.arf20.com	CNAME	web.arf20.com	
tel.arf20.com	CNAME	comm.arf20.com	
netbox.arf20.com	CNAME	web.arf20.com	
dark.arf20.com	CNAME	web.arf20.com	
wiki.arf20.com	CNAME	web.arf20.com	
qbt.arf20.com	CNAME	web.arf20.com	
radarr.arf20.com	CNAME	web.arf20.com	
sonarr.arf20.com	CNAME	web.arf20.com	
kanboard.arf20.com	CNAME	web.arf20.com	
vw.arf20.com	CNAME	web.arf20.com	
raip.arf20.com	CNAME	web.arf20.com	
dmr.arf20.com	CNAME	comm.arf20.com	
pki.arf20.com	CNAME	web.arf20.com	
status.arf20.com	CNAME	mail.arf20.com	
lists.arf20.com	CNAME	mail.arf20.com	
mlmmj.arf20.com	CNAME	mail.arf20.com	
lahomosexualidadde.arf20.com	CNAME	weonpollo.xyz	
panaland.arf20.com	CNAME	web.arf20.com	
_acme-challenge.jellyfin	CNAME	(challenge)	

Name	Type	Content	Comment
_acme-challenge.irc	CNAME	(challenge)	
_acme-challenge.matrix	CNAME	(challenge)	
_acme-challenge.mail	CNAME	(challenge)	
_acme-challenge.xmpp	CNAME	(challenge)	
arf20.com	MX	mail.arf20.com	
selector._domainkey	TXT	(DKIM)	DKIM for selector ‘selector’
_dmarc	TXT	(DMARC)	
arf20.com	TXT	(SPF)	

HE v6 rDNS zone

Name	Type	Content	Comment
2600:70ff:f039:4::13	PTR	ns1.arf20.com	
2600:70ff:f039:4::9	PTR	arf20.com	
2600:70ff:f039:4::195	PTR	global.dns.navy	

IONOS rDNS zone

Name	Type	Content	Comment
5.250.186.185	PTR	mail.arf20.com	

Custom ARFNET software

- cstims: client, service, ticket and invoice management system
- lists: mailing list browser
- status: status monitor