

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

Domain

arf20.com

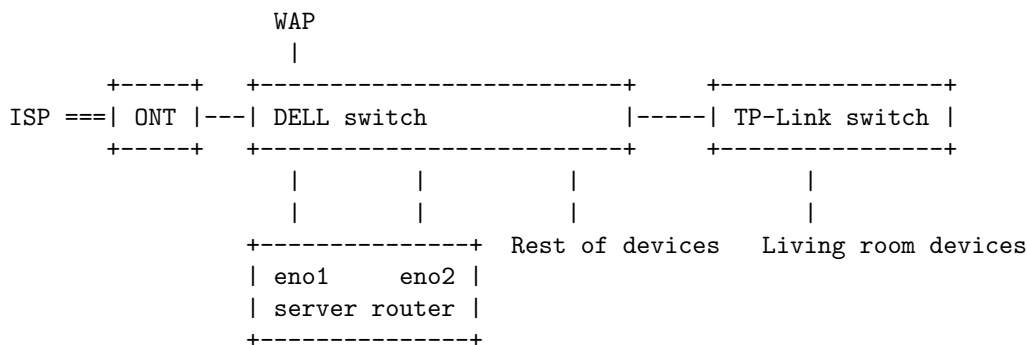
Registrar: namecheap

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 |

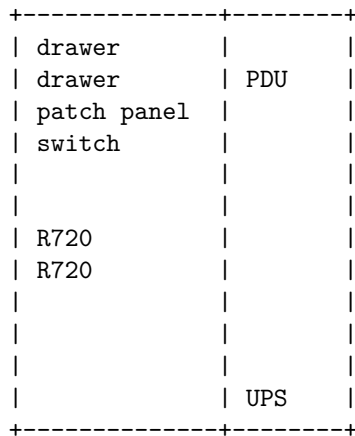
Networking

Hardware



- 1000BASE-T
- = GPON fiber

12U rack



DELL PowerConnect 5424 switch Port assignments

| 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 |
| g15 | test4 | 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
- 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 |

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 | |
| IRCS | | TCP | 6697 | comm | |
| XMPP c2s | | TCP | 5222 | comm | |

| Service | Customer | IPProto | Ext Port | Host | Re Port |
|--------------------|----------|---------|-------------|---------|---------|
| 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 |
| css-ds | | TCP/UDP | 27015 | game | |
| exo-ssh | exo | TCP | 4041 | exovps | 22 |
| exo-extra | exo | TCP | 4040 | exovps | 4040 |
| yero-ssh | yero | TCP | 1511 | yerovps | 22 |
| yero-sql | yero | TCP | 1512 | yerovps | 3306 |
| FiveM SuperioresRP | yero | TCP/UDP | 30120,40120 | yerovps | |

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

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

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

| 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*

| 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/{dcing, 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/ | |
| status.yero.dev | http://yerovps.lan:3001 | |
| panaland.arf20.com | /var/www/panaland.arf20.com/html/ | |

wazuh DMZ.10 -> secure*

- SSH
- wazuh
- password manager server*

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*

misc (Deb12 LXC) DMZ.13

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

pubnix?*

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

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

- SSH*
 - IPsec tunnel*
 - IP forward to nas*
-

yerovps DMZ.192 (yero)

- SSH
- mariadb
- FiveM SuperioresRP

exovps DMZ.195 (exo)

- SSH
- netbox

*TODO

Internal Name and Number Assignment Table

DMZ IPv4s and IPv6 ends in the same way

| Addr | Name |
|---------|-------------|
| DMZ.1 | router.lan |
| DMZ.2 | switch.lan |
| DMZ.3 | wap.lan |
| DMZ.4 | proxmox.lan |
| DMZ.5 | idrac.lan |
| DMZ.6 | nas.lan |
| DMZ.7 | printer.lan |
| DMZ.8 | desktop.lan |
| DMZ.9 | web.lan |
| DMZ.10 | wazuh.lan |
| DMZ.11 | game.lan |
| DMZ.12 | comm.lan |
| DMZ.13 | misc.lan |
| DMZ.192 | yerovps |
| DMZ.195 | exovps |

DNS

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 | |

| Name | Type | Content | Comment |
|--------------------------|-------|----------------------|------------------------------|
| web.arf20.com | AAAA | | |
| game.arf20.com | A | 2.59.235.35 | |
| 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 | |
| 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 | |
| panaland.arf20.com | CNAME | web.arf20.com | |
| _acme-challenge.jellyfin | CNAME | (challenge) | |
| _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 | arfnet.nexo.moe. | |

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
- status page (TODO)