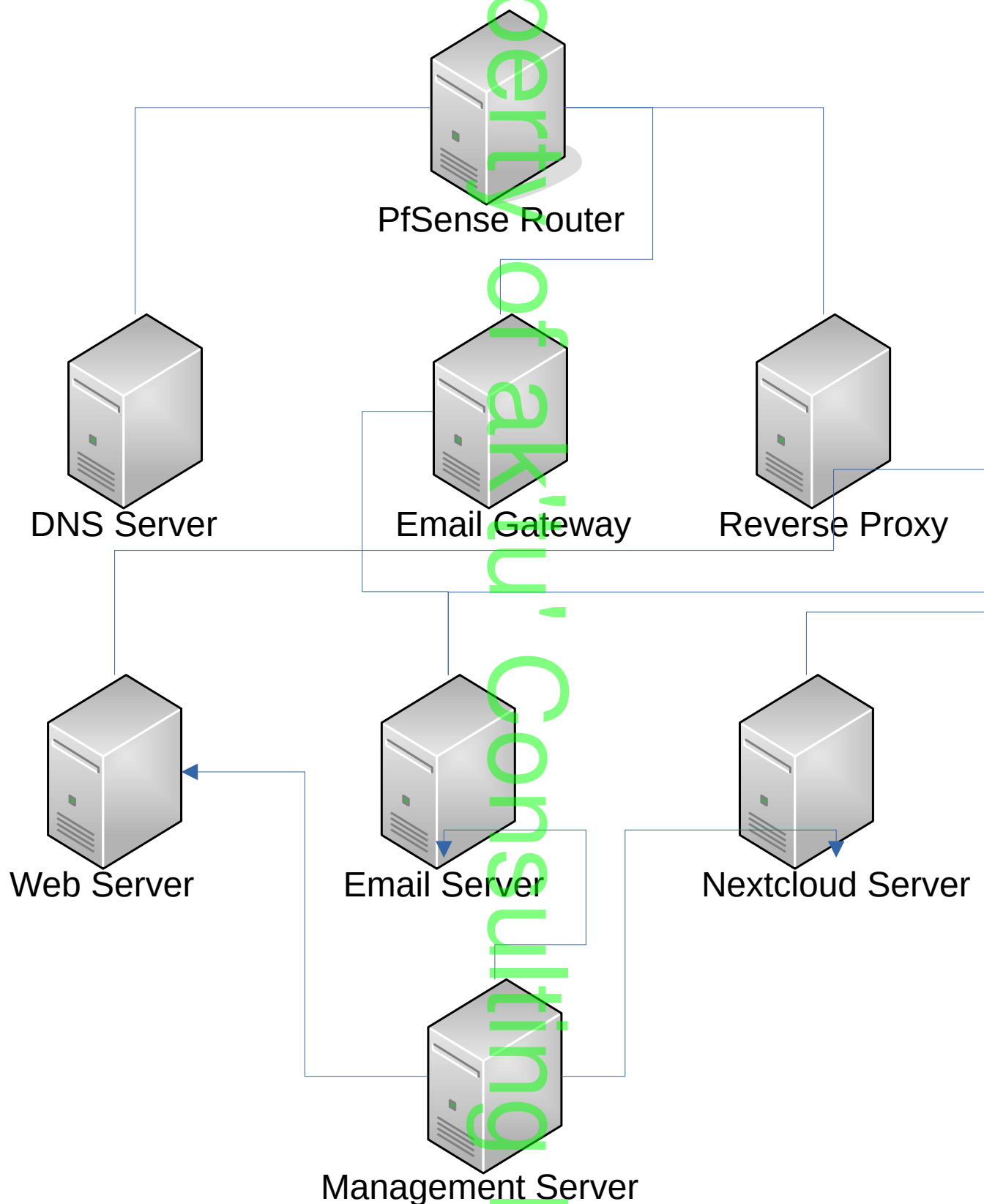


ak'tu' Consulting Network Architecture PoC
Self-Hosted
Architecture Overview



ak'tu' Consulting Network Architecture PoC
Self-Hosted
Software Components

Function	Software/Library	Supporting Infra
E-mail server	Mailcow	docker
E-Mail Gateway	Proxmox PMG	LXC (Proxmox)
DNS	BIND9	docker/Bare Metal
Reverse Proxy	NPM	docker
Cloud Storage	NextCloud	docker
Web Server	nginx	docker
orchestration/ standardization	ansible	ansible
Office Suite	OnlyOffice	docker/Nextcloud
Central Database	MariaDB	docker
Conference Software	Jitsi	docker

ak'tu' Consulting Network Architecture PoC
Self-Hosted

Pfsense Router Config

Function	Module/Action	Details
SSH	Turn on SSH	Turn on SSH for crowdsec setup
Security	Crowdsec	Install to block scans from the internet crowdsec Reference Doc
Backup	Auto Configuration Backup	Backup pfSense Changes
HTTPs	HTTPS	Enable UI HTTPS
Outbound NAT	Hybrid NAT	Enable Hybrid NAT future configs
DNS	System DNS	Add System DNS Servers for WAN Cloudflare: 1.1.1.1 1.0.0.1 OpenDNS 208.67.222.222 208.67.220.220

ak'tu' Consulting Network Architecture PoC
Self-Hosted
BIND9 DNS Bare-Metal

Install Bind9 with package manager (Debian/Ubuntu)

```
apt-get update
```

```
sudo apt install -y bind9 bind9utils bind9-doc dnsutils
```

Setup named.conf.options file

```
sudo vi /etc/bind/named.conf.options
```

Paste the following content

```
#ACL for users on any network that want to query the DNS zone of your choosing
acl internet {
    0.0.0.0/0;
};

#Split Zone for any internal resolutions you may choose to do later on
acl internal-network {
    192.168.1.0/24;
};

#Options for the DNS server
options {
#Cache Directory
    directory "/var/cache/bind";
#What networks/servers are allowed to submit queries for name resolution to this DNS server
    allow-query { localhost; internet; };
#what DNS servers will we send queries if we don't have the address
#DNS servers chosen (Cloudflare, OpenDNS, GoogleDNS)
    forwarders { 1.1.1.1; 1.0.0.1; 208.67.222.222; 208.67.220.220; 8.8.8.8; 8.8.4.4; };
#recursion disabled for internet facing resolution
    recursion no;
#Automatic Validation: This setting tells the DNS server to automatically validate DNSSEC signatures
for DNS queries where the domains are signed with DNSSEC.
    dnssec-validation auto;
    listen-on-v6 { any; };
};
#/etc/bind/named.conf.local", in this file we will define the zone files for our domain
vi /etc/bind/named.conf.local

#This is the zone that we will be hosting on the internet (set your zone)
zone "ytube.aktu.onl" IN {
# Indicates this DNS server is the master for the domain indicated in zone
    type master;
#config file for the zone in question
    file "/etc/bind/ytube.aktu.onlne.conf";
#What systems can query for this domain
    allow-query { internet; };
#you can also set allow-query to any
    #allow-query { any
};
```

ak'tu' Consulting Network Architecture PoC
Self-Hosted
BIND9 DNS Bare-Metal

Setup the zone file for the domain you just created

vi /etc/bind/ytube.aktu.online.conf

Paste the following content

;TTL is the duration (in seconds) that a DNS record is cached by a resolver or intermediary server before the resolver queries the authoritative server for updated information

\$TTL 1d

;Optional but will auto complete the domain

;\$ORIGIN aktu.onl.

;SOA record indicates this is the primary domain server in the event you have more than 1, this makes it authoritative

@ IN SOA ytubenas notifications.aktumedia.com. (

;Serial number for changes, defaulted to date but you can choose your own

18090716 ; Serial Number Using Date of setup

12h ; refresh Time

15m ; retry time

3w ; expire time

2h ; minimum ttl

)

;Nameservers for this domain

IN NS ytubenas.aktumedia.com.

; IN NS ns1.aktumedia.com.

; IN NS ns3.aktumedia.com.

@ IN A 54.39.78.22;

;Records Below

test IN A 1.1.1.1;

;CNAME Entries

;MX Records

;TXT Records

Startup Service

systemctl enable bind9

Systemctl start bind9

ak'tu' Consulting Network Architecture PoC
Self-Hosted
BIND9 DNS Bare-Metal

Update PFSense

Firewall > IP > Add IP

Add DNS Server IP > Apply Changes

Add NAT

Firewall > NAT > Add

Protocol: UDP

Destination: WAN

Destination Port Range: DNS

Redirect Target IP: DNS_Server

Redirect Target Port: DNS

Save > Apply

ak'tu' Consulting Network Architecture PoC
Self-Hosted
Proxmox PMG

Update PFSense

Firewall > Aliases > Add

Add Proxmox PMG Server Details

- Name: PMG_Server
- Description: ProxMox Mail Gateway
- Type: Host(s)
- IP or FQDN: IP of your PMG Server
- Save

Add NAT

Firewall > NAT > Add

Protocol: TCP

Destination: WAN

Destination Port Range: SMTP

Redirect Target IP: PMG_Server

Redirect Target Port: SMTP

Save > Apply

Login to Proxmox Mail PMG

https://internal_PMG_IP:8006

Default Username: root

Passowrd: Setup on install

Configuration > Relay Domains > enter relay Domain
(ytube.aktu.onl)

DKIM > Create > Enter Domain (ytube.aktu.onl)

Selector > domain > update

Enable dkim signing > check enable DKIM signing on outgoing
mails

TLS > TLS Inboud Domains > Create >

Enable TLS > Check Enable

Enable TLS Logging > Yes

Relaying > default relay > internal mail server

ak'tu' Consulting Network Architecture PoC
Self-Hosted
Proxmox PMG

Update the zone file for the domain you created

vi /etc/bind/ytube.aktu.online.conf

Add **A** record for mail

ytubemail IN A SMTP Public IP;

Add **CNAME** Record for friendly mail lookup (optional)

;CNAME Entries

;MX Records

ytube.aktu.onl.	IN	MX	10	ytubemail.ytube.aktu.onl.
ytube.aktu.onl.	IN	MX	20	mail.ytube.aktu.onl.

;TXT Records

ytube.aktu.onl._domainkey IN TXT ("v=DKIM1; h=sha256; k=rsa; "

"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAplUcMZOI5G/6BT4W5HvW3q9g+O7
QzuG+IgDnymSKhv6g1F8acQOxy5B+pzMZJnmnYNHrpesrDwkgBTYKOlt7bbt9c3BSegM08yPXz/
RNmYu38CswQoesE9vG2aHYcNQ4buJQ66slSCOKwILhZKY3cwouMD7bkxsnRNzieUV94pFLVqE61
q1QUotaJgTfLG97wyV4aBagqHEQc"

"Shz57XZ9Xp3oA6n3Pzn/uxoG7KYpZd0kdKCUMjBjdLEgqldkyqTW8oDA3XLxgFhmoCSHC1Tw8vKJ
OqJKx+PeNcaxl4K8+EQ/FsTkLk0W0PQUY2Xh7SO8L5dDtN5mSkU4gb/VH1WQIDAQAB") ; -----
DKIM key ytube.aktu.onl

ytube.aktu.onl. IN TXT "v=spf1 a:ytubemail.ytube.aktu.onl
a:mail.ytube.aktu.onl -all"

_dmarc IN TXT "v=DMARC1; p=quarantine;
rua=mailto:admin@aktu.onl; ruf=mailto:admin@aktu.onl; fo=1"

Restart **Bind9**

#systemctl restart bind9

NOTE: DNS Propagation may take up to 48 hours please be patient while this propagates all over the world

ak'tu' Consulting Network Architecture PoC
Self-Hosted
Proxmox PMG

Test Mail Service

Validate MX Records (dig)

```
# dig ytube.aktu.onl MX +short  
20 mail.ytube.aktu.onl.  
10 ytubemail.ytube.aktu.onl.
```

```
# dig ytube.aktu.onl TXT +short  
"v=spf1 a:ytubemail.ytube.aktu.onl a:mail.ytube.aktu.onl -all"
```

```
# dig _dmarc.ytube.aktu.onl TXT +short  
"v=DMARC1; p=quarantine; rua=mailto:admin@aktu.onl;  
ruf=mailto:admin@aktu.onl; fo=1"
```

ak'tu' Consulting Network Architecture PoC
Self-Hosted
Proxmox PMG

Test Mail Service - Continued

Setup postfix

```
apt-get install -y postfix mailutils
```

Update the following Lines in main.cf

```
vi /etc/postfix/main.cf
```

```
myhostname = ubuntu.ytube.aktu.onl
```

```
mydestination = ytube.aktu.onl, $myhostname, localhost.localdomain, localhost
```

```
relayhost = 10.10.110.198:26
```

Restart postfix

```
systemctl restart postfix
```

```
systemctl enable postfix
```

```
mail -s "Test Send" -r test@ytube.aktu.onl info@aktuconsulting.ca ; tail -f /var/log/mail.log
```