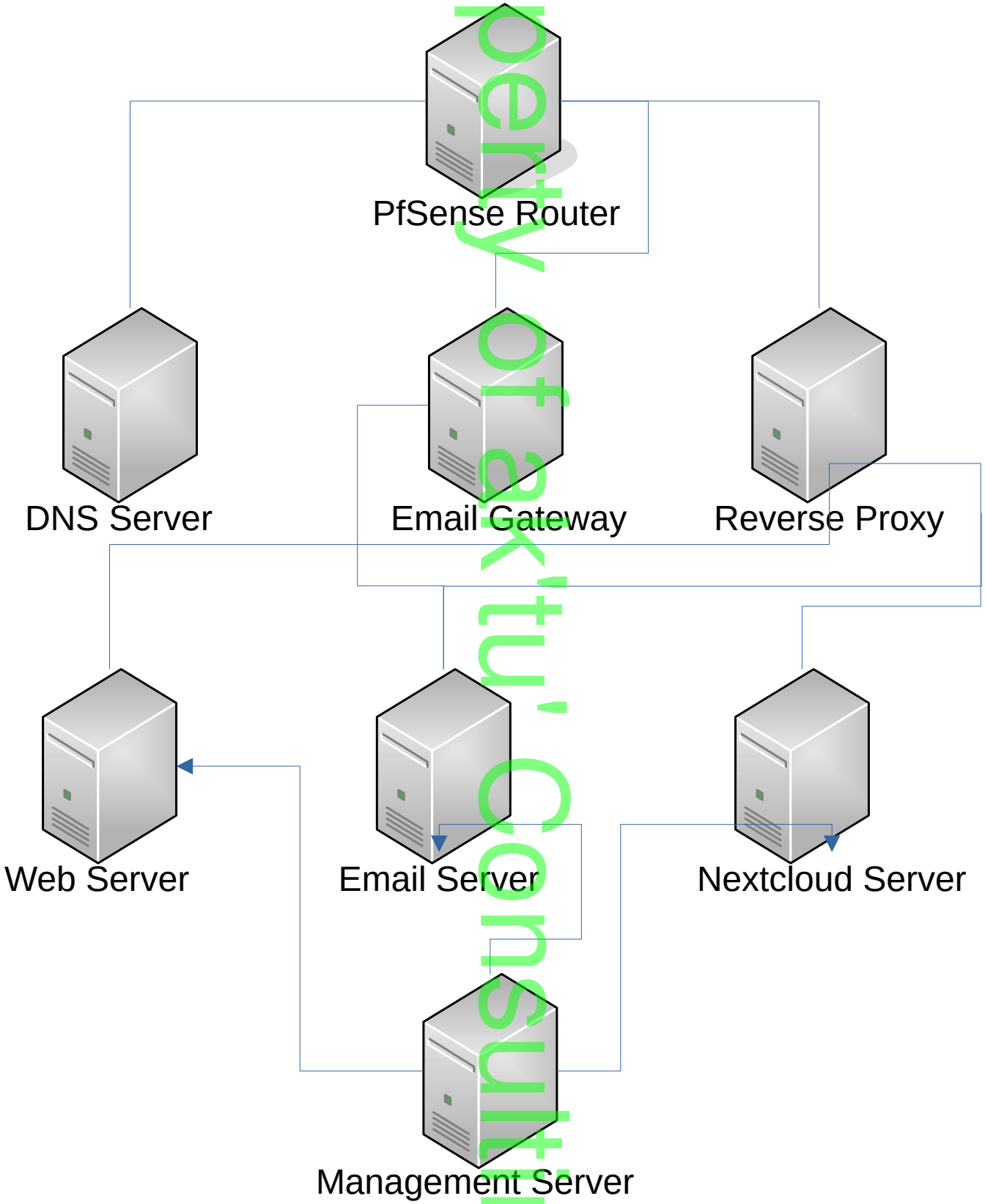
ak'tu' Consulting Network Architecture PoC
Self-Hosted
Architecture Overview



Property of ak'tu' Consulting

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

Property of ak'tu' Consulting

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

Property of ak'tu' Consulting

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
};
```

Property of ak'tu' Consulting

Property of ak'tu' Consulting

Setup the zone file for the domain you just created

vi /etc/bind/ytube.aktu.onlne.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.aktu.onl           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

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

Property of ak'tu' Consulting