# Stack : 3-Tier NPM/Tailscale Gateway

# Summary

This book details how to create a cheap and secure utility server including

- [ ] Cheapest OVH VPS Server in country of your choice
- [ ] OVH Domain Name for your services
- [ ] Squid Proxy Server
- [ ] PiHole AdBlocking DNS
- [ ] Homer Homepage

sdfsd

`docker-compose.yml`

```
services:
  tailscale_full:
    image: tailscale/tailscale:latest
    env_file: .env
    privileged: true
    environment:
      - TS_AUTHKEY=${TS_AUTHKEY}
      - TS_STATE_DIR=/var/lib/tailscale
      - TS_USERSPACE=false
      - TS_DEST_IP=${DMZ_NETWORK_ROUTE}
    volumes:
      - ./config/tailscale/state:/var/lib/tailscale
      - /dev/net/tun:/dev/net/tun
    cap_add:
      - net_admin
      - sys_module
    networks:
      - ${DMZ_NETWORK}
```

```
    restart: unless-stopped

  nginx_proxy_manager:
    image: 'docker.io/jc21/nginx-proxy-manager:latest'
    restart: unless-stopped
    env_file: .env
    ports:
      - ${HOST_IP}:80:80
      - ${HOST_IP}:443:443
      - ${DMZ_NETWORK_ROUTE}:81:81
      - ${DMZ_NETWORK_ROUTE}:80:80
      - ${DMZ_NETWORK_ROUTE}:443:443
    privileged: true
    volumes:
      - ./config/nginx_proxy_manager/data:/data
      - ./config/nginx_proxy_manager/letsencrypt:/etc/letsencrypt
    networks:
      - ${DMZ_NETWORK}
    environment:
      - VIRTUAL_HOST=proxymanager.admin.${TLD}
      - VIRTUAL_PORT=81
    healthcheck:
      test: ["CMD", "/usr/bin/check-health"]
      interval: 60s
      timeout: 30s


  internal_proxy:
    image: nginxproxy/nginx-proxy:latest
    container_name: internal_proxy
    volumes:
      - /var/run/docker.sock:/tmp/docker.sock
      - /var/run/fcgiwrap.socket:/var/run/fcgiwrap.socket
      - /var/run/php-fpm.sock:/var/run/php-fpm.sock
    networks:
      dmz:
      public:
      secure:
      admin:
```

```
  environment:
    - TRUST_DOWNSTREAM_PROXY=true
sso:
  env_file: .env
  image: drkno/plexsso:latest
  networks:
    public:
  volumes:
    - /etc/docker/config/sso:/config
  environment:
    - VIRTUAL_HOST=sso.${TLD}
    - VIRTUAL_PORT=4200
  deploy:
    resources:
      limits:
        cpus: "1"
        memory: 200M

portainer:
  env_file: .env
  image: portainer/portainer-ce:latest
  privileged: true
  networks:
    - admin
  volumes:
    - ./config/portainer:/data
    - /var/run/docker.sock:/var/run/docker.sock
  environment:
    - VIRTUAL_HOST=portainer.admin.${TLD}
    - VIRTUAL_PORT=9000
```

# Setup

The included configuration

- [ ] configure tailscale API key and update `env`
- [ ] configure drkno/plexsso `config.json`

```
config.json
```

- [ ] `docker-conmpose up -d`
- [ ] obtain the Tailscale IP address from the logs

```
docker logs tailscale | grep full
```

- [ ] launch your browser to http://tailscale-ip:81
  - [ ] login to Nginx Proxy Manager with the default credentials
  - [ ] update the admin credentials
  - [ ] create a new proxy host for `tld.com, *.tld.com`
    - [ ] request a new SSL certificate using DNS Validation

| | | | |
|---|---|---|---|
|  Screenshot 2024-12-21 at 02.49.50.png |  Screenshot 2024-12-21 at 02.49.50.png |  Screenshot 2024-12-21 at 02.49.50.png |  Screenshot 2024-12-21 at 02.49.50.png |

  - [ ] create a new proxy host for secure.tld.com, *.secure.tld.com
    - [ ] request a new SSL certificate using DNS Validation
    - [ ] update the Advanced config

| | | | |
|---|---|---|---|
| | | | |

```
# the advanced rule for the secure domain checks for the drkno/plexsso cookie
# if the cookie is present, the request is forwarded normally
# if the cookie is missing, the user is redirected to the SSO url

location ~* ^/$ {

set $subdomain "";
  if ($host ~* ^([^.]+)\.)
    { set $subdomain $1; }
```

```
  if ($http_cookie !~* "AdminDomain")
    { return 302 https://sso.tld.com/$subdomain.secure;}
}

# the $subdomain.secure URI ensues that once authentication is complete, the user
# is redirected to the requested host
```

- [ ] create a new proxy host for admin.tld.com, *.admin.tld.com
  - [ ] request a new SSL certificate using DNS Validation
  - [ ] update the Advanced config

| | | | |
|---|---|---|---|

```
# for the admin wildcard subdomain, any requests are checked for the
# source network - so any request via the Tailscale connection will be
# allowed, but any valid connection will pass through to the internal proxy

location ~* ^/$ {
  allow 172.250.250.0/24;
  deny all;
}
```

- [ ] update your DNS

```
# only configure wildcard domains in DNS, to reduce visbility of
# services that you are running behind your proxy

tld.com - A - 999.999.999.999
*.tld.com - CNAME tld.com

secure.tld.com - CNAME - tld.com
*.secure.tld.com - CNAME - tld.com

admin.tld.com - A - 000.000.000.000
*.admin.tld.com - CNAME - admin.tld.com
```