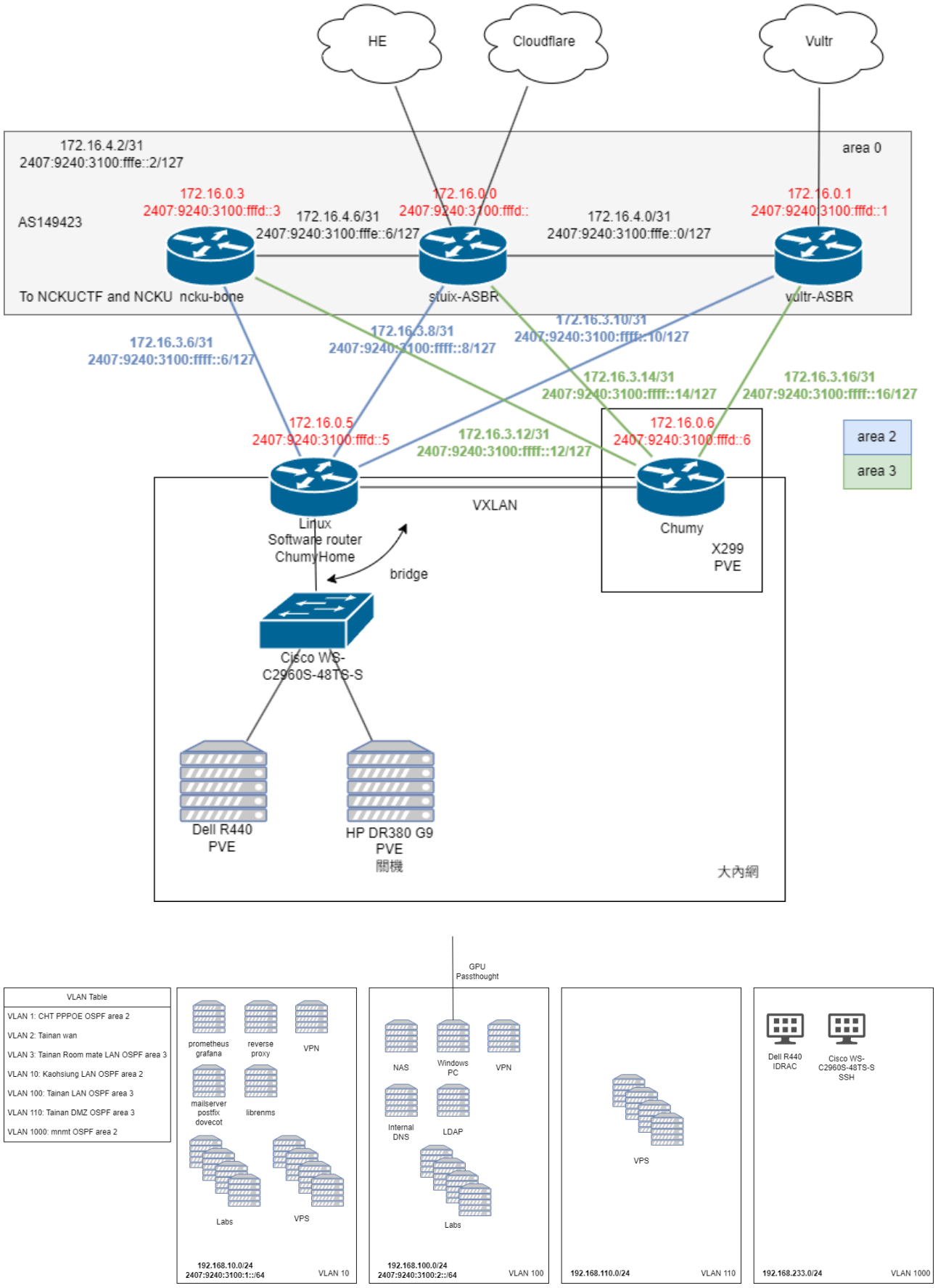
系統與網路管理實務經驗

Home Lab



本身持有 ASN 149423 與一段 IPv6 接入 STUIX 與內部成員做 BGP Peering，主要由 HE 與 Vultr 進行 IP Transit，有趣的是由於成大 IPv6 Outbound 沒有對 Source IP 做檢查且 TANet 與 HINET 有直接 Peering，因此我可以利用這點針對中華電信的路由 Outbound 走成大出去，回來再走 Vultr，延遲可以降到 50ms 左右。

STUIX 那邊我設定做為 IBGP 的 route reflector，內部的 IGP 使用 OSPF 做路由交換，首先我將高雄的 router 與 台南的 router 與 backbone 打 wireguard tunnel，每個都打是因為當有一台掛掉的時候會有備援，接著高雄是 area 2 台南是 area 3。

台南與高雄 router 另外用 VXLAN 將兩邊 LAN bridge 起來並且使用 VLAN 來切個網路，可以參考上面 VLAN Table，主要 VLAN 10 會走高雄出去 VLAN 100、110 會走台南出去。

將中華電信與台南的外網接入內網並且用 VLAN 做區隔，這樣進行一些測試的時候可以在 PVE 內直接切 VLAN 就能使用對應的 PPPoE 或社區網路。

IPv4 的部分使用 iptables 做 NAT，有趣的點是有幾個朋友希望跟我要三級域的 NS 於是我用 iptables 的 string module 對對應域名的 query 做 DNAT 的分流到對應的機器上。

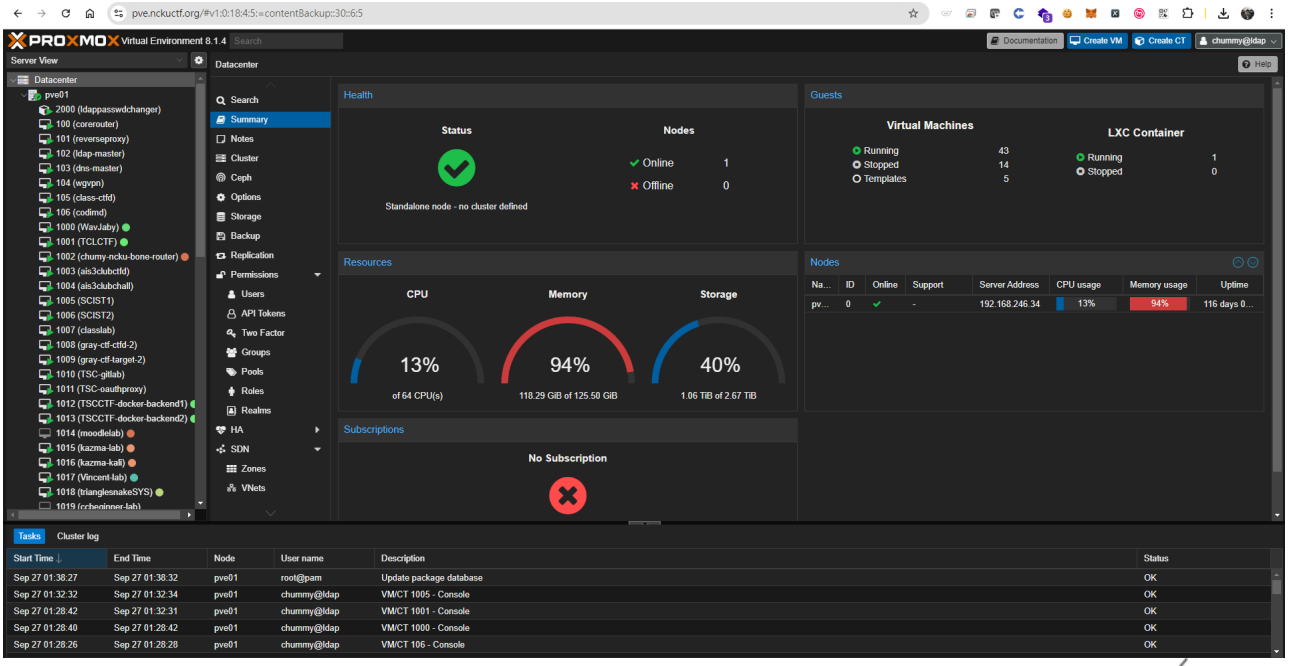
PVE 的部分高雄使用 Dell R440，台南則用直接架在個人實體主機，並且使用台南的 NAS 做 storage，目前是使用 VM 架設 NAT，之後考慮額外找一台主機將其分離出來。

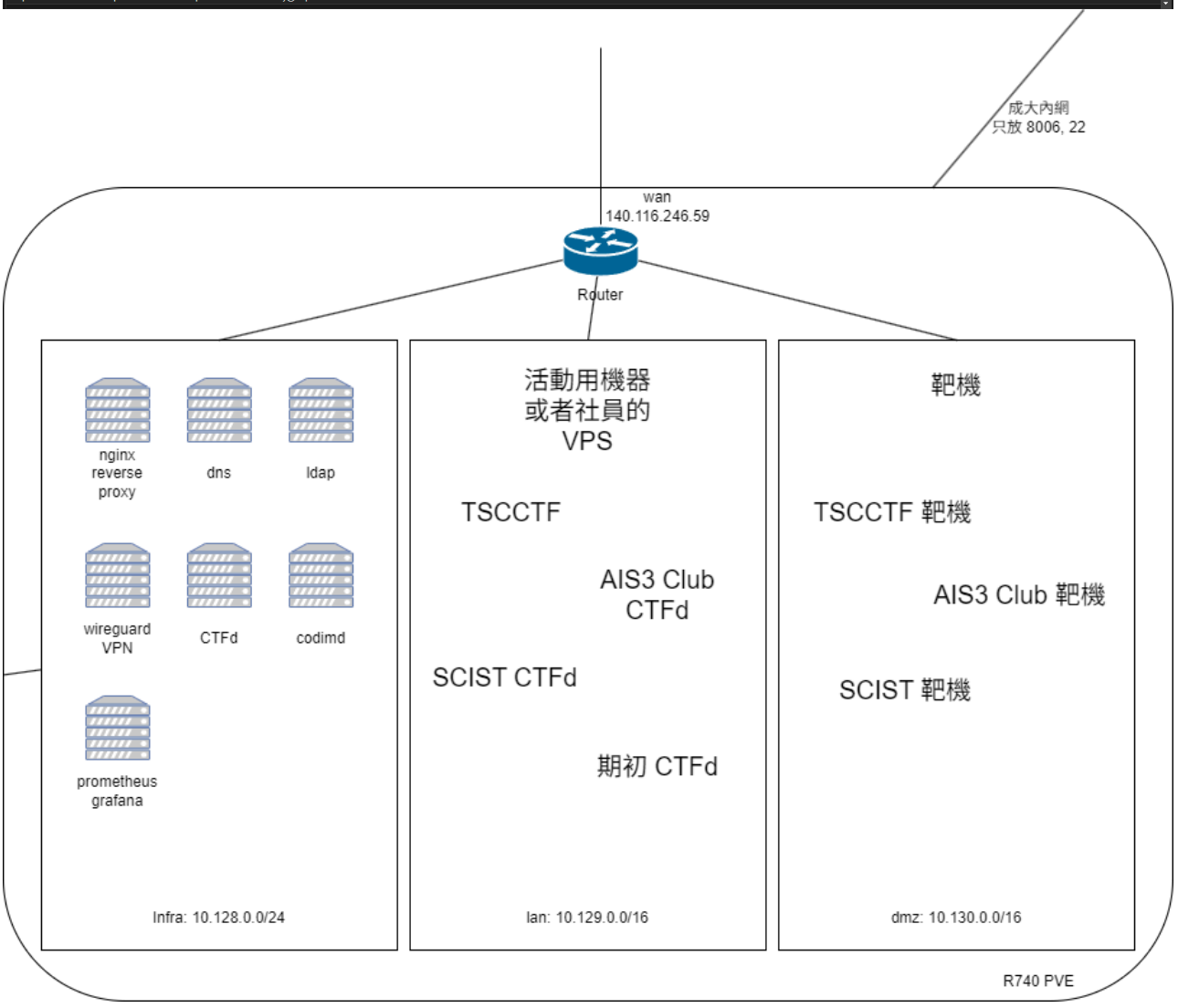
個人平時用的電腦的部分這邊直接使用 VM 裝在 PVE 內，並且 GPU Passthrough 出來，如此就可以不用額外買電腦，且做備份還原等也會很方便。

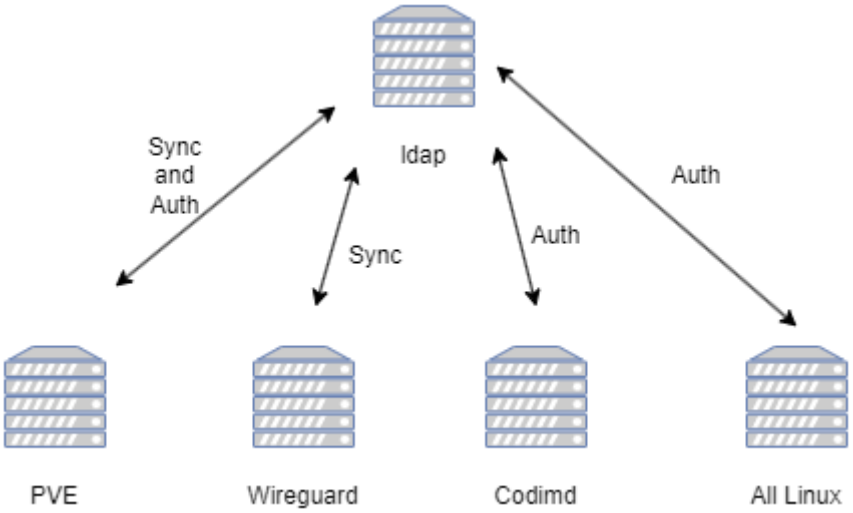
使用 prometheus 與 grafana 還有 librenms 做監控。

使用 postfix 與 dovecot 直接自架 mail server 並且使用 NAT 做 storage 用 NFS mount 到 mail server 上，所以可以使用 chummy@chummydns.com 寄信。

成大資安社社內基礎建設

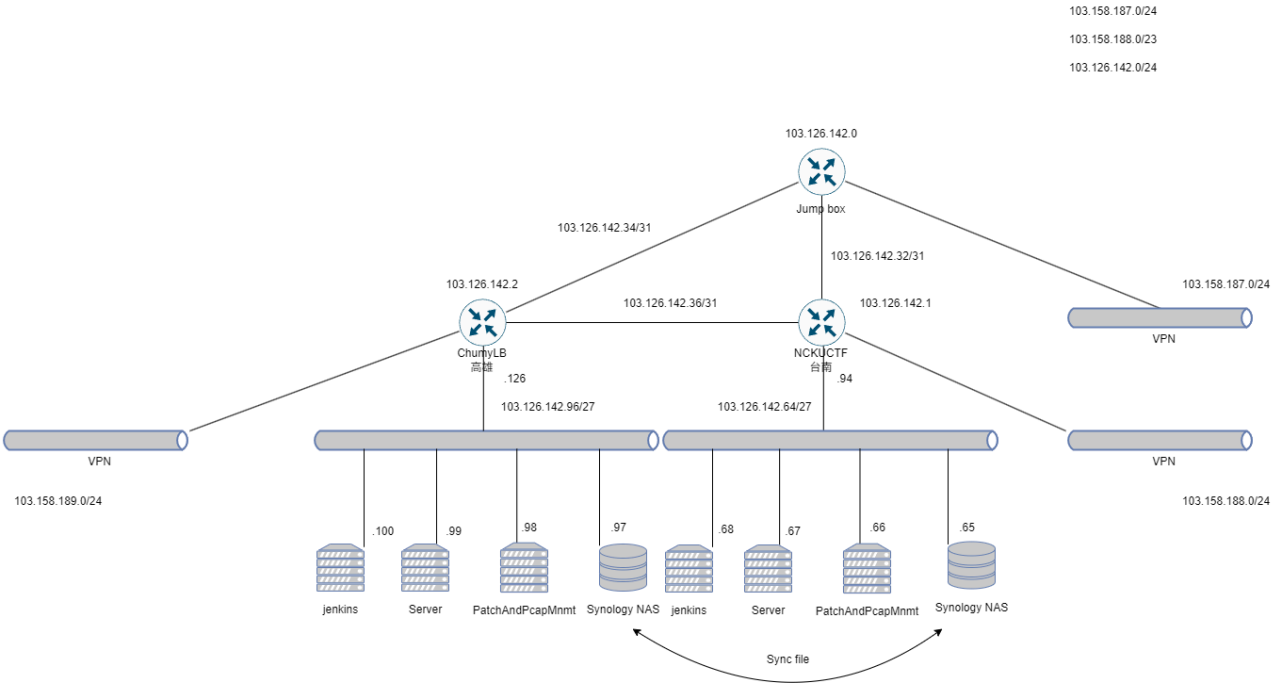






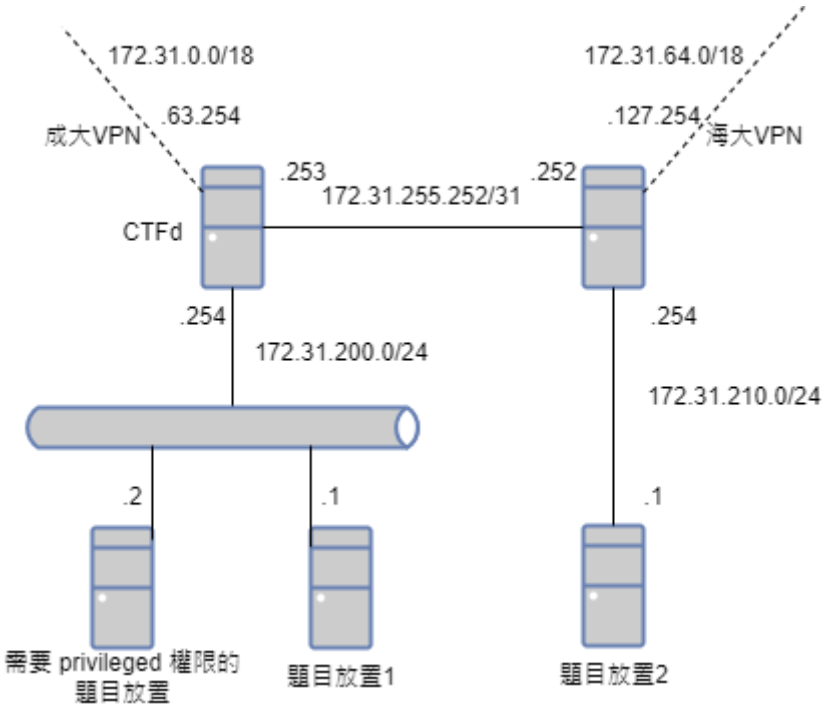
社團管理一台由資訊系贊助的 Dell R740 內部使用 PVE 做虛擬化環境，雖然由於社團是新社團因此目前還沒購入實體 router ，但為了與資訊系內網做隔離因此使用 Debian 做虛擬路由器方便管理網路，對內使用 iptables 做 NAT，內部 DNS 使用 Bind9 架設，外部採用 cloudflare，身分驗證使用 LDAP，monitor 的部分使用 prometheus 與 libNMS，IPAM 用 phpIPAM。

HITCON CTF 2024 Final 星爆牛炒竹狐 隊內基礎建設



使用說明書

TSCCTF



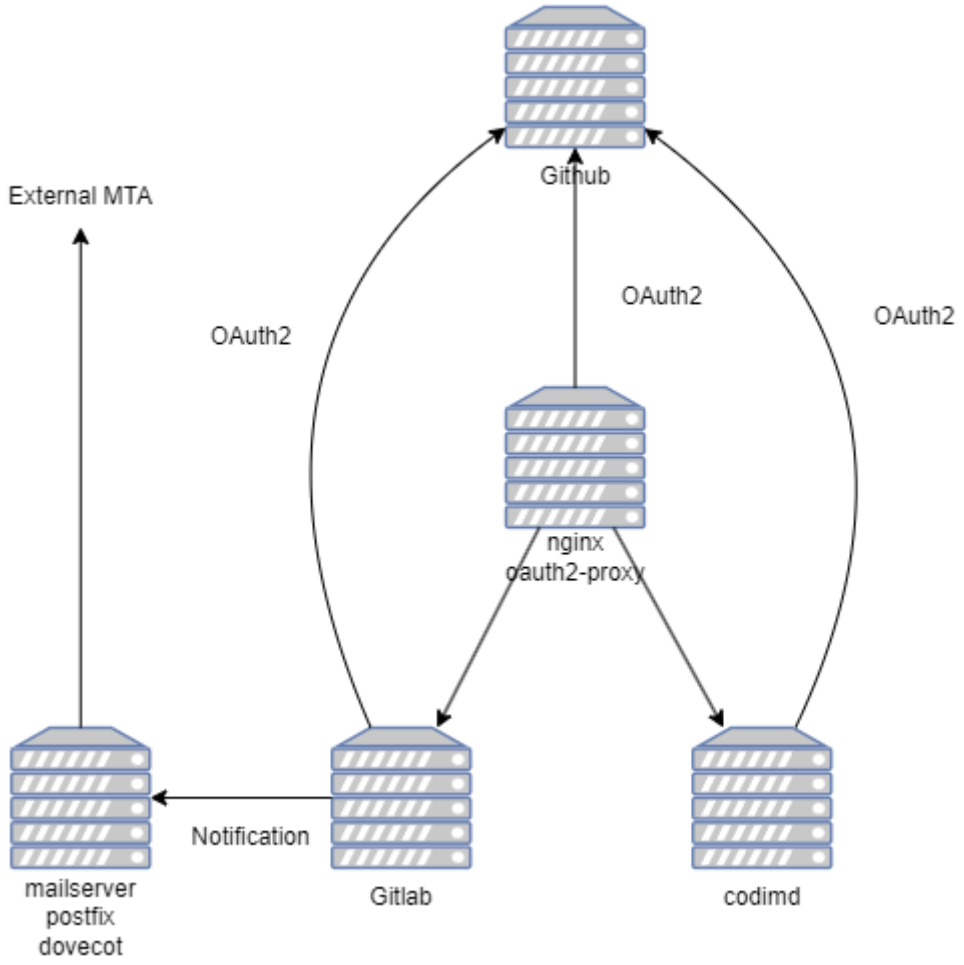
網管組第一次會議紀錄

網管組第二次會議紀錄

github org

提供了成大與海大節點做存取，兩邊用 wireguard 打 tunnel 並設定 static route 以後，CTFd 放置在成大這端，並在兩邊都架設 wireguard vpn 做 load balance，下面題目架設的部分為了方便維護因此使用 docker 並且請出題組自己填寫架設的位置。

TSC 內部 infra



由於有需要放一些不太能公開的資料，且可能需要使用一些線上版需要付費的功能，因此我們需要自架 codimd 與 gitlab，Access Control 與 Authentication 使用 OAuth2 串 github 檢查是否屬於我們的 github org。首先用 oauth2-proxy 做第一層驗證之後 reverse proxy 轉到對應的服務，之後也是用 OAuth2 串 github 做 Authentication，這樣就不用自架 IdP，由於 gitlab 需要用 email 做 Notification 而且 gmail 有 limit，因此這邊使用 postfix 與 dovecot 直接自架 mail server，但是由於手上的 public IP 不太方便設定 PTR 因此還是有進垃圾信的可能。

競賽

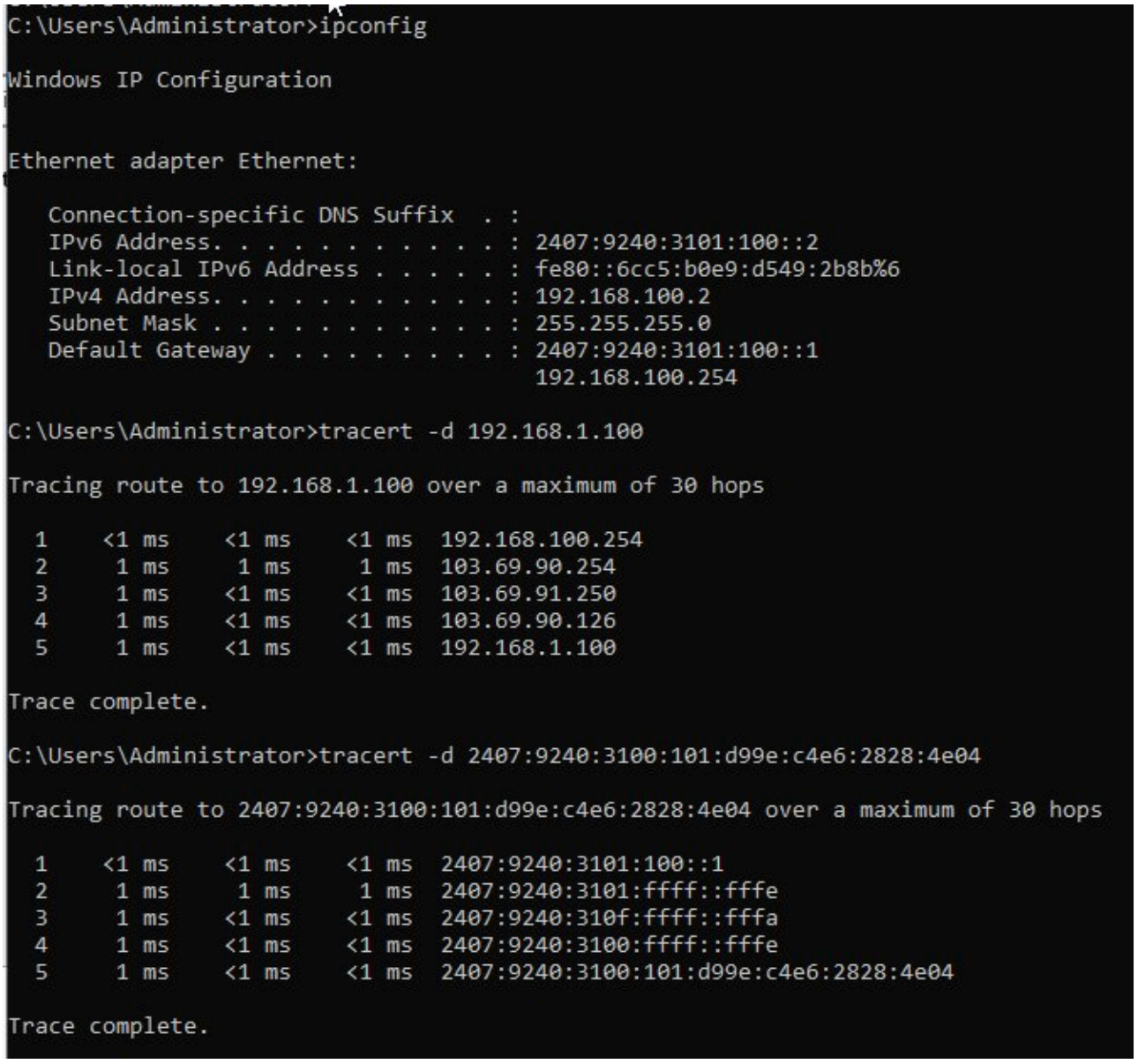
曾於全國技能競賽的資訊與網路技術拿到銀牌，並且成功打到備取國手，這個比賽的特色是全程斷網且禁止帶任何筆記，因此所有架設的方式及 config 都要記腦袋。

第 52 屆全國賽題目

國手賽

當時國手賽的時候很有趣是一開始他們叫我們自己出題，所以我剛好就想說結合一些自己的研究出了一個題目。

比如 SRv6 L3VPN 等等。



題目連結

雖說最後因為 windows 網卡設定 VLAN 有問題，還有切 VLAN 的時候出現一些問題導致比賽失常，但是依然拿到備取國手的成績。