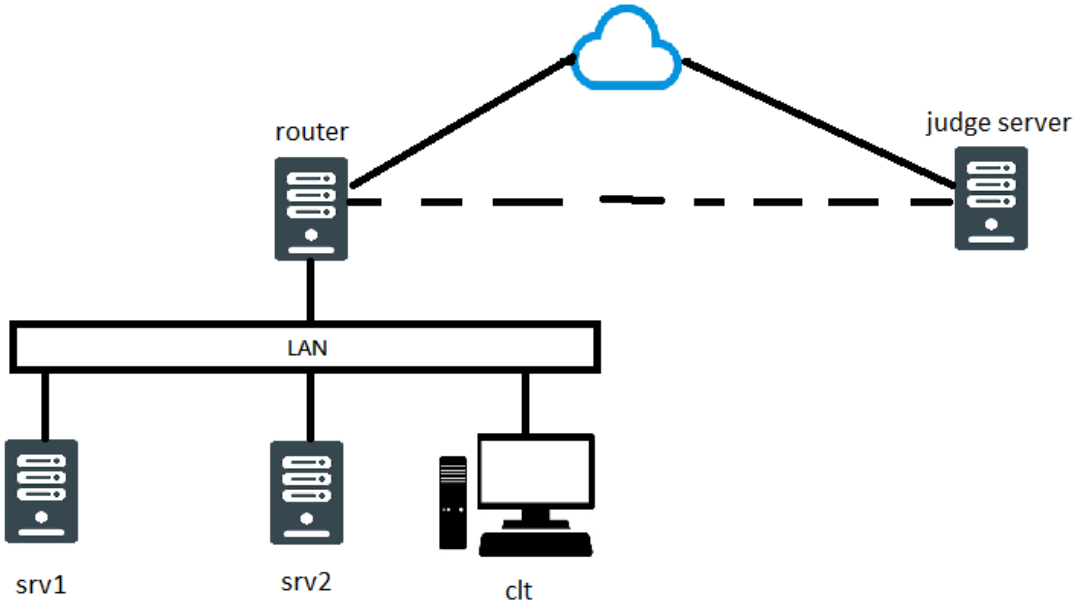
請將所有 VM 依規定安裝系統並連上發放之 VPN 開放所有網路搜尋 但禁止使用通訊軟體交換答案或想法 歡迎檢舉，完成時請使用我們提供的 judge server，輸入帳號密碼，並上傳 ROOTCA 憑證後進行 judge。
另外 judge server 將提供裝好系統的 VM ova 供下載。

整體架構



本環境中的所有密碼皆設為 finalexam
環境中的服務一律開啟 ICMP 協定。
請為環境中所有機器安裝 ssh server 並允許 root 登入作為評測用途。
除了必須以檢視設定值的方式進行評分的項目外,所有面向用戶的服務一律由用戶端系統進行功能測試,否則該項目不予計分。
router 連公網後請用我們配發的 wiregaurd vpn profile 與 judge server 連線。本環境將使用 wiregaurd vpn 的網路模擬外網環境，不會使用到公網。公網是會給你們做測試用途，測試外網環境，測試環境請自己架設。

router:

1. 安裝 linux 模擬內部 Gateway 及 Firewall，並依照附錄 A 設定 IP 位址。
2. 安裝 dns server 並管理<username>.finalexam.ncku 網域，該 dns 將提供外網與內網服務，請勿讓外網查到內網 IP，內網包含 ikev2 VPN client。
3. 安裝 DHCP 供 clt 上網。
4. 讓內網可以使用外網 IP 上網。
5. 讓外部使用者可由 http://www.<username>.finalexam.ncku 與 https://www.<username>.finalexam.ncku 瀏覽 srv2 的 web server。

另外，若是 srv2 的 VPN server 沒架起來，請為 ssh server 做 port forward:
srv1 -> 23
srv2 -> 24
clt -> 25

srv1:

1. 安裝 linux 並依照附錄 A 設定 IP 位址。
2. 請安裝 ldap server 並按照附錄 B 新增使用者，host 設為 ldap.<username>.finalexam.ncku，dc 設為<username>.finalexam.ncku。
3. 建立 CA 憑證，配發憑證供對內及對外服務使用。

srv2:

1. 安裝 linux 並依照附錄 A 設定 IP 位址。
2. 架設 ikev2 vpn 使外網可以存取內網服務 fqdn 設為 vpn.<username>.finalexam.ncku，新增帳號 vpn 做登入，客戶端連線後將客戶端 nameserver 改為 192.168.140.254。
   (如果 ikev2 架不起來請用 wiregaurd ，public、private、psk 從直接用我們給的 vpn profile 裡的 clientip 請 allow 192.168.87.87)
3. 安裝 web 服務（用甚麼不限），並依下述需求設定。
   a. 提供 http://www.<username>.finalexam.ncku 與 https://www.<username>.finalexam.ncku，頁面內容不限。
   b. 若 Client 使用 http 協定瀏覽時自動轉到 https。
   c. 瀏覽/auth 目錄時需進行帳密驗證，請使用 ldap 的 WEB 群組中的帳號做登入，頁面內容不限。
4. 新增三個磁碟，做 Raid5，並以 4GB 左右(+-0.5G)的空間掛載於/share
5. 安裝 nfs 並將分享目錄設為/share 與內網做檔案分享。

clt:

1. 安裝 linux 並依照附錄 A 設定 IP 位址。
2. 安裝 ldap client，允許使用 ldap 的 USER 群組帳號並禁止 WEB 群組帳號登入 ssh。
3. 將 nfs srv2.<username>.finalexam.ncku:/share mount 到/srv2nfs 目錄

附錄 A：

Hostname	Interface	IP Address	Gateway	Nameserver
router	wan(vpn)	In vpn profile	In vpn profile	127.0.0.1
	lan	192.168.140.254/24		
srv1	eth0	192.168.140.1/24	192.168.140.254	192.168.140.254
srv2	eth0	192.168.140.2/24	192.168.140.254	192.168.140.254
clt	eth0	Via DHCP		

附錄 B：

Username	Group	Password	login shell
WEB01 WEB02 …… WEB50	WEB	finalexam	disable login shell
USER01 USER02 …… USER50	USER		enable login shell

Test at external or internal	Host	Target	Test command	Score
External	router	讓外部使用者可由 http://www.<username>.finalexam.ncku 與 https://www.<username>.finalexam.ncku 瀏覽 srv2 的 web server	curl -L -k http://www.<username>.finalexam.ncku curl -L -k https://www.<username>.finalexam.ncku	
		安裝 dns server 並管理 <username>.finalexam.ncku 網域	dig @<client wan ip> www.<username>.finalexam.ncku	
		該 dns 將提供外網服務，請勿讓外網查到內網 IP。(www & vpn)	dig @<client wan ip> www.<username>.finalexam.ncku dig @<client wan ip> vpn.<username>.finalexam.ncku	
	srv2	若 Client 使用 http 協定瀏覽時自動轉到 https。	curl --HEAD http://www.<username>.finalexam.ncku | grep "Location: https:"	
		瀏覽/auth 目錄時需進行帳密驗證，請使用 ldap 的 WEB 群組中的帳號做 登入，頁面內容不限。	curl --HEAD -L https://www.<username>.finalexam.ncku/auth -k | grep -P "HTTP/\d.\d 401" curl --HEAD -L https://www.<username>.finalexam.ncku/auth -k --user WEB<random number>:finalexam | grep -P "HTTP/\d.\d 200"	
		https 的 certificate 是否使用 srv1 的 CA 做配發	curl -L https://www.<username>.finalexam.ncku --cacert ca.crt	
		架設 ikev2 vpn 使外網可以存取內網服務 fqdn 設為 vpn.<username>.finalexam.ncku，新增帳號 vpn 做登入。	將提供 client 端所使用的 config 檔	
Internal	router	安裝 dns server 並管理 <username>.finalexam.ncku 網域	dig @192.168.140.254 www.<username>.finalexam.ncku	
		該 dns 將提供內網服務	dig @192.168.140.254 www.<username>.finalexam.ncku +time=1 +tries=1 | grep A | grep "192.168"	
		安裝 DHCP 供 clt 上網。	sshpass -p finalexam ssh root@<clt ip> "grep dhcp-server-identifier /var/lib/dhcp/dhclient.*.leases" | grep 192.168.140.254 sshpass -p finalexam ssh root@<clt ip>	

			ip a | grep dynamic	
		讓內網可以使用外網 IP 上網。	sshpass -p finalexam ssh root@<clt ip> ping 8.8.8.8 -c 1 -W 1 | grep "bytes from 8.8.8.8: icmp_seq=1"	
	srv1	請安裝 ldap server 並按照附錄 B 新增使用者，host 設為 ldap.<username>.finalexam.ncku，dc 設為<username>.finalexam.ncku。	ldapsearch -h ldap.<username>.finalexam.ncku -D "cn=admin,dc=<username>,dc=finalexam,dc=ncku" -w finalexam -b "dc=<username>,dc=finalexam,dc=ncku" "(uid=WEB<random number>)"	
	srv2	提供 http://www.<username>.finalexam.ncku 與 https://www.<username>.finalexam.ncku，頁面內容不限。	curl -L –k http://www.<username>.finalexam.ncku curl -L –k https://www.<username>.finalexam.ncku	
		若 Client 使用 http 協定瀏覽時自動轉到 https。	curl --HEAD http://www.<username>.finalexam.ncku | grep "Location: https:"	
		瀏覽/auth 目錄時需進行帳密驗證，請使用 ldap 的 WEB 群組中的帳號做登入，頁面內容不限。	curl --HEAD -L https://www.<username>.finalexam.ncku/auth -k | grep -P "HTTP/\d.\d 401" curl --HEAD -L https://www.<username>.finalexam.ncku/auth -k --user WEB<random number>:finalexam | grep -P "HTTP/\d.\d 200"	
		新增三個磁碟，做 Raid5，並以 4GB 左右(+-0.5G)的空間掛載於/share	sshpass -p finalexam ssh root@192.168.140.2 "mdadm -D \$(df | grep /share | awk '{print \$1}')" | grep "Array Size" | awk '{print $5}' | sed s/\(//g	
		安裝 nfs 並將分享目錄設為/share 與內網做檔案分享。	sshpass -p finalexam ssh root@192.168.140.2 showmount -e | grep /share	
	clt	安裝 ldap client。	sshpass -p finalexam ssh root@<clt ip> cat /etc/passwd | grep -P "(USER|WEB)" sshpass -p finalexam ssh root@<clt ip> getent passwd | grep -P "(USER|WEB)"	
		允許使用 ldap 的 USER 群組帳號登入 ssh。	sshpass -p finalexam ssh USER<random number>@<clt ip> whoami	
		禁止使用 ldap 的 WEB 群組帳號登入	sshpass -p finalexam ssh WEB<random	

		ssh。	number>@<clt ip> whoami	
		將 nfs srv2.<username>.finalexam.ncku:/share mount 到/srv2nfs 目錄	sshpass -p finalexam ssh root@<clt ip> df -H | grep "finalexam.ncku:/share"	

Ikev2 client config:

```
config setup
        strictcrlpolicy=yes

conn ikevpn
        auto=start
        keyexchange=ikev2

        leftsourceip=%config
        leftauth=eap-mschapv2

        right=vpn.<username>.finalexam.ncku
        rightsubnet=192.168.140.0/24
        rightid=%any
        rightauth=pubkey
        eap_identity=vpn
```