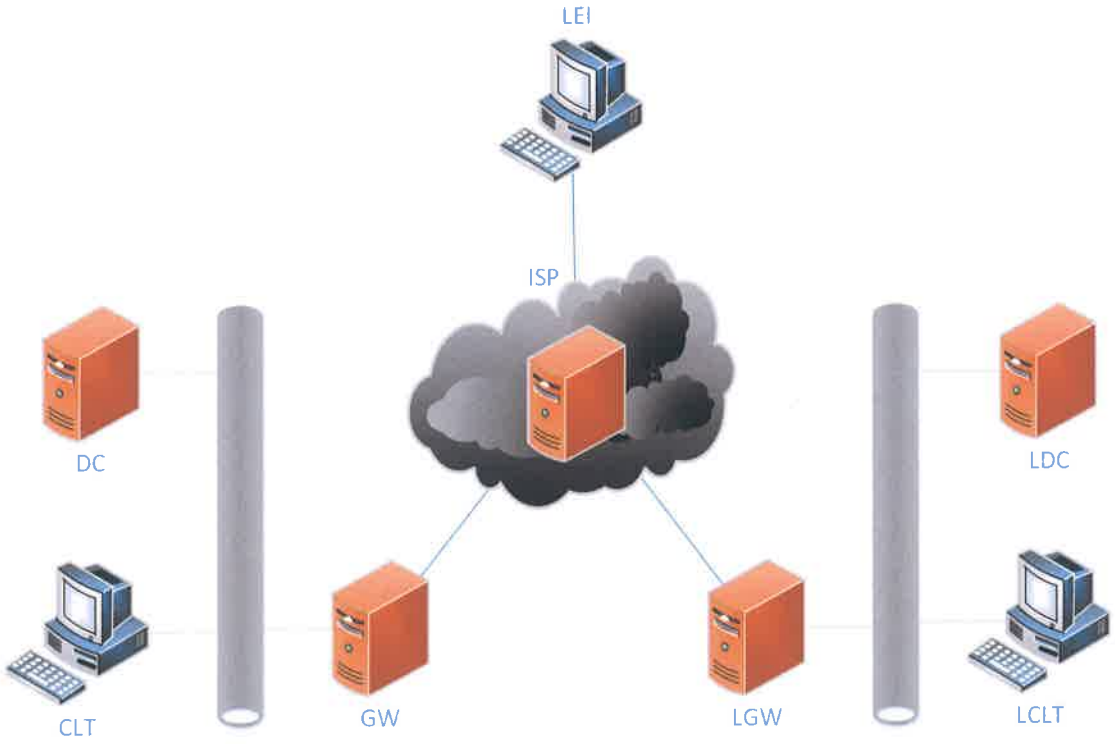
第四十七屆全國技能競賽 第二天

資訊與網路技術



。本競賽為固定式起訖時間，請選手自行掌握工作流程，並依據試題敘述完成要求。

。如在比賽過程中有任何疑問，或題意描述不清楚，請立即向裁判反應。

。評分前將對所有虛擬系統進行重新啟動的動作，建議選手於競賽結束前預留些許時間，自行關閉虛擬系統。

。評分時，將盡可能採用功能測試，項目之區隔以評分表所列為主，個別項目完全符合試題之敘述即得分，無部份給分。

。工作項目中須設定密碼之處，若試題未明確指定，則一律使用 **Skills39**。

。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**。

試題情境

經過幾天的會議與討論，雷氏企業決定將網路總部轉至雷哥航空，要求你架設雷哥航空的網路環境，並將網域與大部分服務遷移至雷哥航空。請延續昨日的試題，依據試題說明完成這樣任務。

注意！

評分時將會先評 Web 功能，在評完網頁服務後將會直接將 DC 關機，DC 將不會參與後續的任何評分項

基本設置

基本設置不會一項一項作評分，但在評分過程中若發現有基本設置未做設定或是設定錯誤，將會於另外的評分項扣分

- Host 主機不參與整個網路環境，請將其所有網卡 IPv4 與 IPv6 功能關閉
- 試題中 Linux 主機皆不會使用到圖形化介面，不建議安裝圖形化介面；並請自行分配 CPU 與記憶體使用量，避免記憶體不足
- 試題中將不會指定 VM 所在的 Host 主機，請自行判斷最佳的分配方式
- 在所有 VM 中安裝 VMware Tools
- 將所有 VM 名稱設定與主機名稱相同
- 根據附錄 A 設定主機名稱與 IP 位址
- 在所有 Windows Client 關閉登入初始動畫與睡眠
- 請讓裁判人員評分時找的到 Putty 用，可以放在桌面，分享資料夾或是網頁上

Routing

- 在 Internet 啟用 OSPF 路由，並在鄰居間啟用 MD5 密碼驗證

VPN Tunnel

- 在 GW 與 LGW 間用 OpenVPN 建立 Site-to-Site Tunnel，並使用網域簽發之憑證作驗證
- 請透過 OpenVPN 發送對方網段的路由

Active Directory

- 將 LDC 設為網域控制站，管理 skills.com 網域，並將 DC 降級為一般網域電腦
- 網域使用者將保留所有家目錄，設定檔，重新導向目錄與群組資料夾的設定；將原本在 DC 上的分享資料夾轉移至 LDC 上，並保留相關權限設定
- 將網域客戶端 SMB 流量限制為 10M/s

DNS

- 將原本 DC 上的 DNS 服務轉至 LDC 上

DHCP

- 將原本 DC 上的 DHCP 服務轉至 LDC 上，負責發放 skills.com 的內網 IP

Certificate Authority

- 將原本 DC 上的 CA 憑證服務轉至 LDC 上，並保留原本根憑證與憑證發放紀錄
- 保留原本自動發放憑證功能，CRL，AIA 與 OCSP 功能
- 以上三項仍將會在內網與外網做測試

Web

- 保留 GW 上的 Reverse Web Proxy 功能，設定網頁備援功能，在 DC 網頁服務關閉時由 LDC 作為備援首頁，並將 DC 首頁內容改為<h1>SK Home Page DC</h1>，將 LDC 首頁內容設定為<h1>SK Home Page LDC</h1>
- 將 Internal 站台移至 LGW，保留驗證功能與頁面內容

Remote Access VPN

- 取消原本在 DC 上的 SSTP VPN，改在 LGW 上用 OpenVPN 取代，允許由 Internet 撥入並存取內部資源
- 利用 AD 做登入驗證，並僅允許 IT 群組登入 VPN
- 連入 VPN 後僅能存取 LDC

Monitor

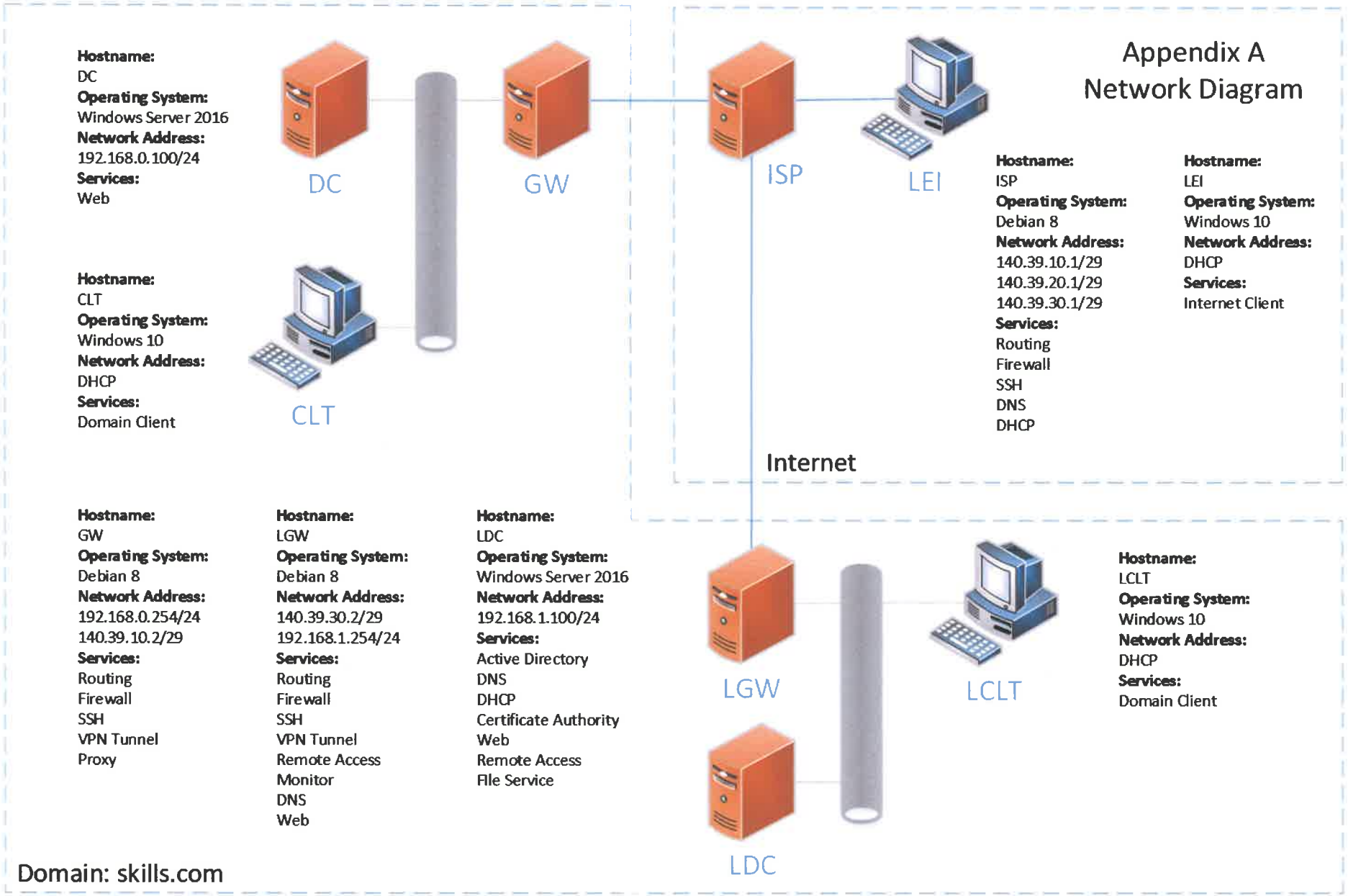
- 在 LGW 上安裝 Cacti，監控所有 Internet 介面之網路流量（GW、ISP、LGW 上擁有 Public IP 之網卡）
- 在 LGW 上安裝 Nagios，監控 LDC 上的服務是否正常運作（DHCP、DNS、HTTP、LDAP、NTP 選其中三項即可）
- 利用 AD 做登入驗證，並僅允許 IT 群組由內部網段登入 Cacti 與 Nagios 頁面，分別為 http://cacti.skills.com 與 http://nagios.skills.com

Firewall

- **ISP 將會拒絕轉送任何 RFC1918 內規範的私有網段！！**
- 在 GW 與 LGW 上以最嚴謹的方式設定防火牆規則，僅允許必要的流量，並將預設行為設定為 DROP（評分時會檢查 INPUT 與 FORWARD Table）
- 將 GW 與 LGW 防火牆規則的 Packet Count 記錄顯示在 http://firewall.skills.com，每 5 分鐘更新頁面，格式如下圖

```
August 03 2017 10:00:00

LGW

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   10   600 ACCEPT     icmp --  *      *       192.168.0.0/24       0.0.0.0/0
    0     0 ACCEPT     icmp --  *      *       192.168.1.0/24       0.0.0.0/0
    0     0 DROP       icmp --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 15 packets, 1000 bytes)
 pkts bytes target     prot opt in     out     source               destination

GW

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   10   600 ACCEPT     icmp --  *      *       192.168.0.0/24       0.0.0.0/0
    0     0 ACCEPT     icmp --  *      *       192.168.1.0/24       0.0.0.0/0
    0     0 DROP       icmp --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 15 packets, 1000 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Appendix A
Network Diagram



Appendix B - Logical Topology