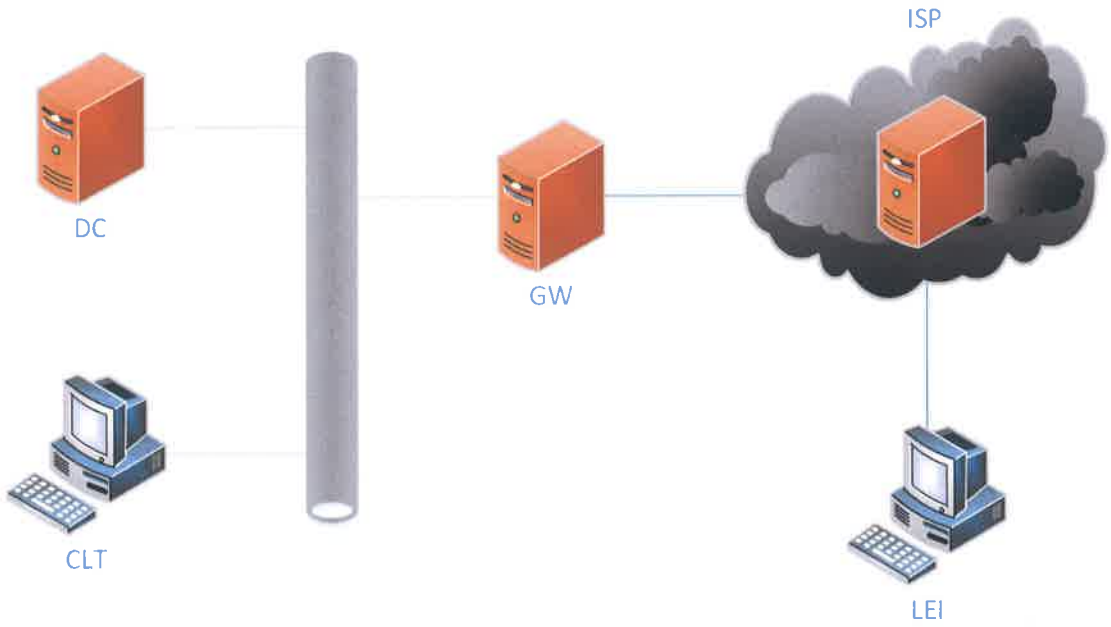
第四十七屆全國技能競賽 第一天

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

雷氏企業成立了雷哥航空公司，並決定重新部署總公司與雷哥航空的網路環境，因此聘了你來幫忙完成這項工作；第一天將會先設置總公司網路環境，其餘的工作將於第二天進行，請依據試題說明完成這項任務。

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
- 憑證請統一使用 CA 服務發放之憑證，評測時請勿出現憑證錯誤畫面

Routing

- 在 Internet 啟用 OSPF 路由
- 為模擬真實網路環境，請透過 OSPF 發出一筆往 ISP 的 Default Route

Active Directory

- 將 DC 設為網域控制站，管理 skills.com 網域
- 根據附錄 C 建立使用者與群組
- 家目錄（H:）：\\share.skills.com\home*%username%*
- 漫遊設定檔：\\share.skills.com\profile$*%username%*
- 重新導向 Document 目錄：\\share.skills.com\document*%username%*
- 群組資料夾（G:）：\\share.skills.com\groupshare*%groupname%*
- 用戶不可存取其他用戶之家目錄，設定檔與文件目錄
- 用戶不可存取其他群組之群組資料夾
- 使用者家目錄與 Document 目錄分別最多可使用的容量為 500MB，而各群組的群組資料夾可使用的最高容量為 2GB
- 每月 1 日與 15 日自動將群組資料夾內建立超過三個月的檔案移除
- 對 Visitor 群組內的使用者，以上四項均不需做設定，僅需指定強制設定檔，路徑為 \\share.skills.com\profile$\VisitorProfile，並在桌面放上 Putty.exe
- 允許 IT 群組使用者本機登入 DC

DNS

- DC 管理 skills.com 的內網 DNS 紀錄，將其他查詢轉送給 ISP
- GW 管理 skills.com 服務外部之 DNS 紀錄
- ISP 管理 Internet（internet.org.tw）之 DNS 紀錄，並將 skills.com 網域之查詢轉送給 GW
- 請依環境需求設定適當 DNS 紀錄

DHCP

- DC 負責發放 skills.com 的內網 IP，DNS 指向 DC
- ISP 負責發放 Internet 的 IP，DNS 指向 ISP

Certificate Authority

- 在 DC 上安裝憑證服務，負責憑證簽發與管理
- 將根憑證 CN 命名為 SKILLS-ROOT
- 在網域內，對所有使用者（除了 Visitor 群組）與所有電腦自動發放憑證，憑證範本名稱為 Skills-User 和 Skills-Computer
- 設定 CRL 為 http://cert.skills.com/CertEnroll/SKILLS-ROOT.crl
- 設定 AIA 為 http://cert.skills.com/CertEnroll/SKILLS-ROOT.crt
- 設定 OCSP 為 http://cert.skills.com/ocsp
- 以上三項將會在內網與外網做測試

Web

- 在 GW 上做 Reverse Web Proxy，在外部可透過 https://www.skills.com 連至位於 DC 的公司首頁，首頁內容顯示<h1>SK Home Page</h1>
- 在外部可透過 https://internal.skills.com 連至公司內部網站，時需輸入驗證資訊，僅允許 IT 群組登入，並在頁面顯示<h1>SK Internal Page</h1>

Remote Login

- ISP 與 GW 僅允許從內網使用 DC 遠端登入 SSH，並使用 Port 22222
- 上述之 SSH 服務，若連續三次登入失敗，鎖定該來源 IP 五分鐘
- 網域內 Windows 系統均允許 IT 群組遠端桌面登入

VPN

- 在 DC 上設定 SSTP VPN，允許由 Internet 撥入並存取內部資源
- 僅允許 IT 群組登入 VPN
- 連入 VPN 後僅能存取 DC

Firewall

- **ISP 將會拒絕轉送任何 RFC1918 內規範的私有網段！！**
- 在面對 Internet 的介面中，GW 與 ISP 每秒最多接受並回應一個 ICMP 請求；對內部網段則無相關限制

試題情境

雷氏企業成立了雷哥航空公司，並決定重新部署總公司與雷哥航空的網路環境，因此聘了你來幫忙完成這項工作；第一天將會先設置總公司網路環境，其餘的工作將於第二天進行，請依據試題說明完成這項任務。

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
- 憑證請統一使用 CA 服務發放之憑證，評測時請勿出現憑證錯誤畫面

Routing

- 在 Internet 啟用 OSPF 路由
- 為模擬真實網路環境，請透過 OSPF 發出一筆往 ISP 的 Default Route

Active Directory

- 將 DC 設為網域控制站，管理 skills.com 網域
- 根據附錄 C 建立使用者與群組
- 家目錄（H:）：\\share.skills.com\home*%username%*
- 漫遊設定檔：\\share.skills.com\profile$*%username%*
- 重新導向 Document 目錄：\\share.skills.com\document*%username%*
- 群組資料夾（G:）：\\share.skills.com\groupshare*%groupname%*
- 用戶不可存取其他用戶之家目錄，設定檔與文件目錄
- 用戶不可存取其他群組之群組資料夾
- 使用者家目錄與 Document 目錄分別最多可使用的容量為 500MB，而各群組的群組資料夾可使用的最高容量為 2GB
- 每月 1 日與 15 日自動將群組資料夾內建立超過三個月的檔案移除
- 對 Visitor 群組內的使用者，以上四項均不需做設定，僅需指定強制設定檔，路徑為 \\share.skills.com\profile$\VisitorProfile，並在桌面放上 Putty.exe
- 允許 IT 群組使用者本機登入 DC

DNS

- DC 管理 skills.com 的內網 DNS 紀錄，將其他查詢轉送給 ISP
- GW 管理 skills.com 服務外部之 DNS 紀錄
- ISP 管理 Internet（internet.org.tw）之 DNS 紀錄，並將 skills.com 網域之查詢轉送給 GW
- 請依環境需求設定適當 DNS 紀錄

DHCP

- DC 負責發放 skills.com 的內網 IP，DNS 指向 DC
- ISP 負責發放 Internet 的 IP，DNS 指向 ISP

Certificate Authority

- 在 DC 上安裝憑證服務，負責憑證簽發與管理
- 將根憑證 CN 命名為 SKILLS-ROOT
- 在網域內，對所有使用者（除了 Visitor 群組）與所有電腦自動發放憑證，憑證範本名稱為 Skills-User 和 Skills-Computer
- 設定 CRL 為 http://cert.skills.com/CertEnroll/SKILLS-ROOT.crl
- 設定 AIA 為 http://cert.skills.com/CertEnroll/SKILLS-ROOT.crt
- 設定 OCSP 為 http://cert.skills.com/ocsp
- 以上三項將會在內網與外網做測試

Web

- 在 GW 上做 Reverse Web Proxy，在外部可透過 https://www.skills.com 連至位於 DC 的公司首頁，首頁內容顯示<h1>SK Home Page</h1>
- 在外部可透過 https://internal.skills.com 連至公司內部網站，時需輸入驗證資訊，僅允許 IT 群組登入，並在頁面顯示<h1>SK Internal Page</h1>

Remote Login

- ISP 與 GW 僅允許從內網使用 DC 遠端登入 SSH，並使用 Port 22222
- 上述之 SSH 服務，若連續三次登入失敗，鎖定該來源 IP 五分鐘
- 網域內 Windows 系統均允許 IT 群組遠端桌面登入

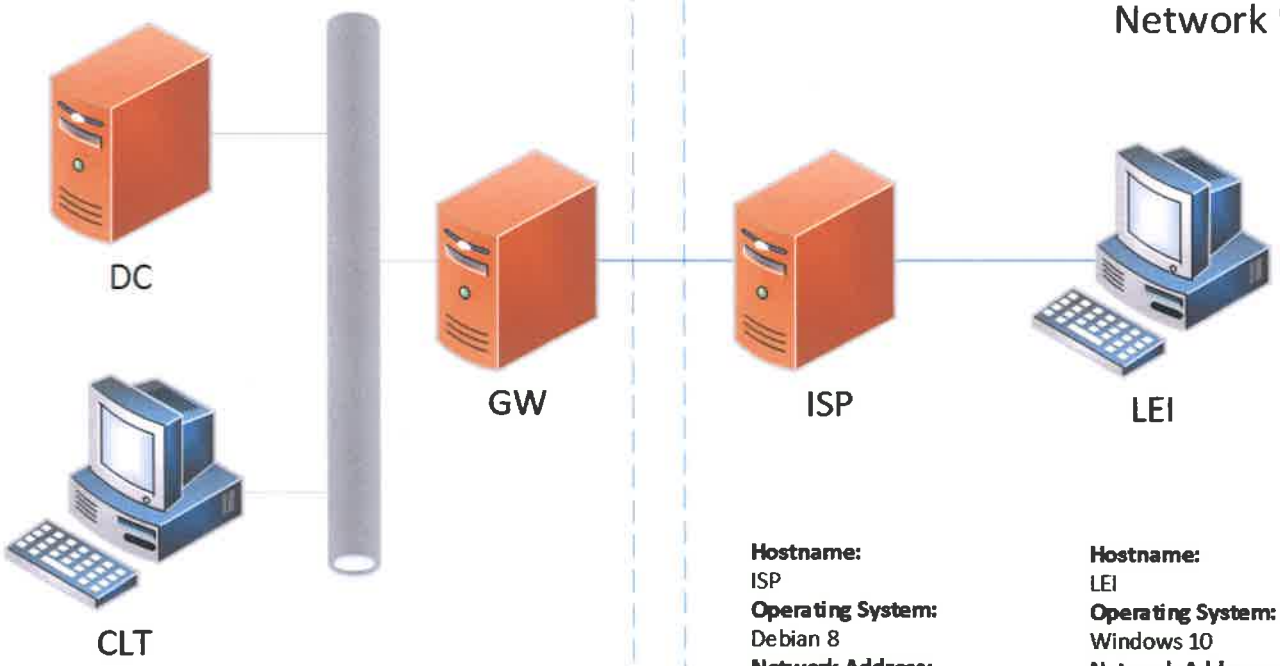
VPN

- 在 DC 上設定 SSTP VPN，允許由 Internet 撥入並存取內部資源
- 僅允許 IT 群組登入 VPN
- 連入 VPN 後僅能存取 DC

Firewall

- **ISP 將會拒絕轉送任何 RFC1918 內規範的私有網段！！**
- 在面對 Internet 的介面中，GW 與 ISP 每秒最多接受並回應一個 ICMP 請求；對內部網段則無相關限制

Appendix A
Network Diagram



Hostname:
DC
Operating System:
Windows Server 2016
Network Address:
192.168.0.100/24
Services:
Active Directory
DNS
DHCP
Certificate Authority
Web
Remote Access
File Service

Hostname:
CLT
Operating System:
Windows 10
Network Address:
DHCP
Services:
Domain Client

Hostname:
GW
Operating System:
Debian 8
Network Address:
192.168.0.254/24
140.39.10.2/29
Services:
Routing
Firewall
SSH
Proxy
DNS

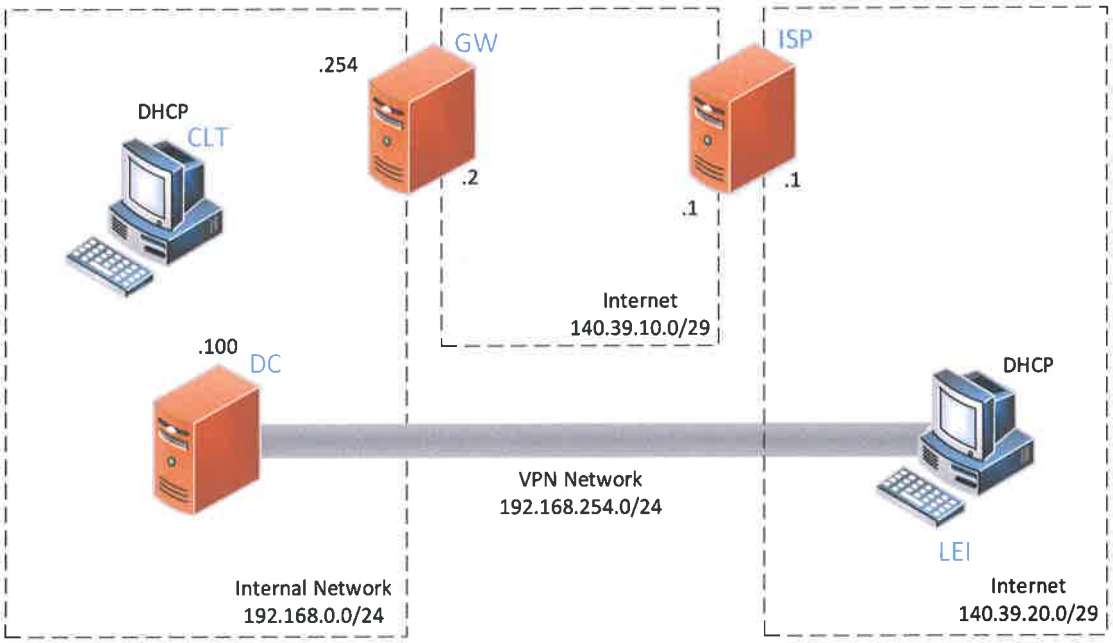
Domain: skills.com

Hostname:
ISP
Operating System:
Debian 8
Network Address:
140.39.10.1/29
140.39.20.1/29
Services:
Routing
Firewall
SSH
DNS
DHCP

Hostname:
LEI
Operating System:
Windows 10
Network Address:
DHCP
Services:
Internet Client

Internet

Appendix B - Logical Topology



Appendix C - Domain Users

Username	Password	Group	Telephone
Administrator	Skills39	Domain Admins	555-0000
IT01		IT	555-0001
IT02		IT	555-0002
...		IT	...
IT50		IT	555-0050
Sales001		Sales	555-1001
Sales002		Sales	555-1002
...		Sales	...
Sales500		Sales	555-1500
Visitor01		Visitor	555-2001
Visitor02		Visitor	555-2002
...		Visitor	...
Visitor10		Visitor	555-2010