worldskills
Chinese Taipei

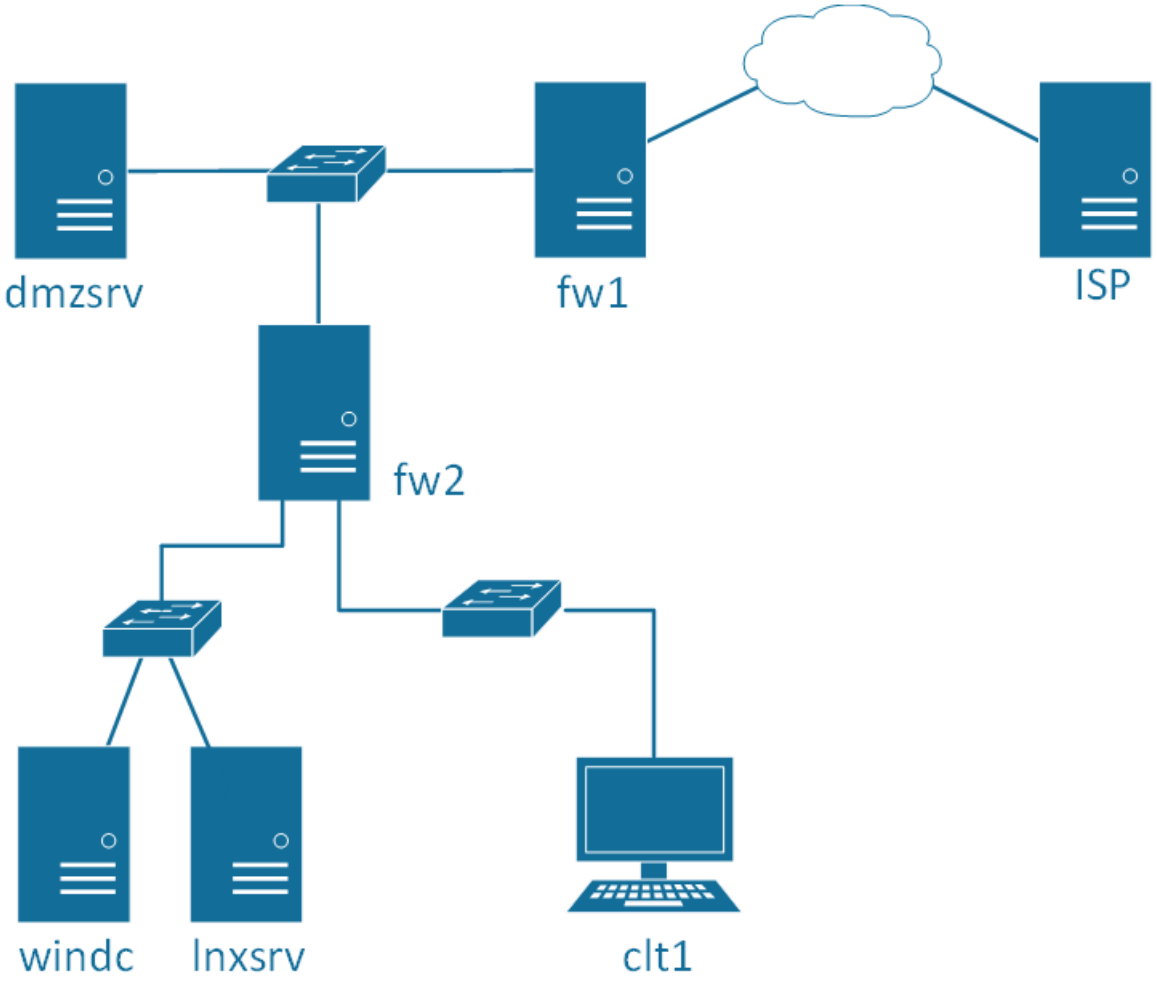
全國技能競賽試題

<39 資訊與網路技術職類>

NSC2019_R2_TP39_TW

第 49 屆全國技能競賽 資訊與網路技術

第一日 Part 1 試題



- 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。

© WorldSkills TW

- 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

新成立的星宇航空公司預計於 2020 年初正式啟航，隨著啟航的到來，

公司的網路環境需由專業人士來維運，因此聘請您來完成這項工作，

接下來您須依照公司的規劃完成各項任務！

※免責聲明：與星宇航空有關著作權的圖文等檔案，僅限於比賽做學術用途使用！

基本設置

- Host 主機不參與整個網路環境，請將其所有網卡 IPv4 及 IPv6 功能關閉
- 試題中不指定 VM 所在的 Host 主機，兩部 Host 主機均須使用，請自行分配系統資源
- 將所有 VM 名稱設定與主機名稱**相同**
    - 若評分時，裁判發現 VM 名稱與主機名稱不同，該台 VM 將**不予評分**！
- 依照附錄 A 設定主機名稱、網卡名稱及相關 IP 位址
- 憑證請統一使用**公司內 CA 服務**發放之憑證，評分時請勿出現憑證錯誤畫面

VMware Workstation Pro

- 確保所有 Windows Server 虛擬機僅能使用電腦製造商信任的軟體啟動

ISP

- 於 PC 建立 Windows Server 2019 虛擬機 ISP
- 設定 DNS 服務，管理 worldskills.tw 之 DNS 紀錄
- 設定 Web 服務，提供網頁於 http://www.worldskills.tw，並建立簡單的頁面
- 設定 Standalone Root CA 服務，效期 6 年，CA 名稱為 TW_ROOTCA
    - 核發 STARLUX-CA 的次要憑證請求
    - 為顧及安全性，不須使用時請關閉此 CA 服務

fw1

- 於 PC 建立 Debian 9 虛擬機 fw1
- 扮演 Router 及 Firewall 角色
- 依照附錄 D 建立 3 位使用者
- 為來自內部網路的流量設定 NAT，能透過 39.49.10.10 位址上網

dmzsrv

- 於 PC 建立 Windows Server 2019 虛擬機 dmzsrv
- 設定 DNS 服務，管理 starlux.com 網域**外網**的資源紀錄(Resource Records)

fw2

- 於 PC 建立 Debian 9 虛擬機 fw2
- 扮演 Router 及 Firewall 角色
- 依照附錄 D 建立 3 位使用者
- 請勿使內部網路經過 fw2 後被 NAT，須保持來源為 192.168.0.0/16 網段

windc

- 於 PC 建立 Windows Server 2019 虛擬機 windc
- 設定 AD 網域服務，管理 starlux.com 網域
- 設定 DNS 服務，管理 starlux.com 網域**內網**的資源紀錄(Resource Records)
    - 將其他請求轉送至 ISP
- 設定 Enterprise Sub CA 服務，效期 3 年，名稱為 STARLUX-CA，負責憑證簽發與管理
    - 請透過 TW_ROOTCA 核發此次要憑證
- 新增三個磁碟，將其設為其中一個磁碟損壞後仍可持續運作的模式，並以 40GB 左右的空間提供於 E:\

Active Directory Tasks（包含未來新增至網域中的電腦或使用者）

- 依照附錄 B 建立 200 位使用者
- 為提升使用者登入的安全性，所有網域使用者的密碼須使用長度達 10 個字元以上的密

碼，但不須（IT 群組除外）啟用複雜性原則

- 建立使用者家目錄於 (\\starlux.com\homes\使用者名稱)，使用者只能存取自己的家目錄
    - 使用者登入後於磁碟機 H 掛載使用者家目錄
- 以下 Tasks 除了 windc 外均須自動套用於網域內所有電腦：
    - 啟用本機 Administrator 帳號，並將其名稱修改為 SL_Adm
    - 將桌面背景設為隨身碟裡提供的 starlux_bk.png
- 隱藏登入畫面的開關機按鈕
- 依照附錄 C 建立群組分享資料夾，各群組只能存取自己群組的分享資料夾
    - 使用者登入後於磁碟機 G 掛載群組分享資料夾 (\\starlux.com\群組縮寫)

lnxsrv

- 於 PC 建立 Debian 9 虛擬機 lnxsrv
- 設定 DHCP 服務，配發 192.168.20.101 ~ 192.168.20.200 範圍內的 IP 位址
- 設定 MySQL 服務（請安裝 mariadb-server），帳號為 root，密碼為 Skills39
    - 使用隨身碟中 Booking-sql 資料夾內的檔案（xxx.sql），執行下方指令進行匯入

```
mysql -u root -p Skills39 < xxx.sql
```

clt1

- 於 PC 建立 Windows 10 Enterprise 虛擬機 clt1
- 加入 starlux.com 網域
- 建立本機使用者 Starlux_Public，並於該使用者啟用資訊服務站（Kiosk）模式，開機時自動登入該使用者，登入後自動開啟 Microsoft Edge 並連線至 https://www.starlux.com
    - Edge 須允許分頁模式，為提升安全性，請禁止使用者列印頁面

Appendix A - IP Address Assignment

VM Hostname	OS	Interface Name	IP Address	Default Gateway
ISP	WS 2019	Ethernet0	39.49.10.1/24	N/A*
		LPG8	8.8.8.8/32	
fw1	Debian 9	eth0	39.49.10.10/24	39.49.10.1
			39.49.10.11/24	
		eth1	10.0.0.1/28	N/A*
dmzsrv	WS 2019	Ethernet0	10.0.0.2/28	10.0.0.1
fw2	Debian 9	eth0	10.0.0.3/28	10.0.0.1
		eth1	192.168.10.1/24	N/A*
		eth2	192.168.20.1/24	N/A*
windc	WS 2019	Ethernet0	192.168.10.10/24	192.168.10.1
lnxsrv	Debian 9	eth0	192.168.10.20/24	192.168.10.1
clt1	Windows 10	Ethernet0	Via DHCP	

* 若預設閘道為 N/A，則請勿做任何設定

Appendix B – Active Directory Users

Username	Display Name	Group	Password
IT01 ~ 50	IT01 ~ 50	IT	Skills39
FA001~ 050	Flight Attendant 001 ~ 050	Flight_Attendant	
GS001 ~ 100	Ground Staff 001 ~ 100	Ground_Staff	

Appendix C – Group Share Folders

Share Name	Local Path	Group
\\starlux.com\IT	E:\Share\IT	IT
\\starlux.com\FA	E:\Share\FA	FA
\\starlux.com\GS	E:\Share\GS	GS

Appendix D – fw users

Username	Password
mgt01 ~ 03	Skills39

Certificate Authority 憑證架構

第 49 屆全國技能競賽 資訊與網路技術

第一日 Part 2 試題

※請在時間內完成 Part 1 及 Part 2 試題，兩 Part 將一起評分

ISP

- 設定 Web 服務，提供網頁於 http://www.worldskills.tw，並建立簡單的頁面
    - 若收到目的地為 8.8.8.8 的 http 請求時，在頁面顯示 " Google DNS Test Page "
- 請確認 8.8.8.8 網卡無 L1 signal 狀態
- 阻擋所有來源或目的為 IANA 機構所保留的位址或 Automatic Private IP Addressing（APIPA）位址的流量
- 新增名為 User1 的使用者，扮演外部使用者進行相關測試
    - 請先建立 VPN 設定檔以供評分時測試

fw1

- 透過 39.49.10.11 位址設定相關 NAT Port-Forwarding，讓外部存取 dmzsrv 的對外服務

dmzsrv

- 設定 Web 服務，若以 HTTP 瀏覽須自動導向為 HTTPS，請提供以下站台：
    - 訂位網頁，能夠透過 https://booking.starlux.com 進入網頁
        - 須支援 PHP，請使用隨身碟中 IIS-PHP 資料夾裡提供的檔案安裝
        - 並使用隨身碟中 Booking-web 資料夾內的檔案作為該站台的**首頁**內容
        - 瀏覽網頁時，不需輸入首頁檔名也可正常瀏覽
    - 公司首頁，能夠透過 https://www.starlux.com 進入網頁
        - 使用隨身碟中 www-web 資料夾內的檔案作為首頁內容
- 設定 SSTP VPN 服務，透過 vpn.starlux.com 連線
    - 僅供 VPN 群組（AD 網域）的使用者連線
    - 連線後僅能存取 192.168.10.0/24 網段
    - 配發 192.168.30.39 ~ 192.168.30.49 範圍內的 IP 位址

- *（提醒）此 Server 的 Web 會對 lnxsrv 發起 MySQL 連線！*

fw2

- 設定 DHCP Relay Agent，讓用戶端自 lnxsrv 取得 IP 位址

windc

- 在群組分享資料夾啟用重複資料刪除機制，以避免各群組重複性高的檔案（例如 ISO 檔）佔用磁碟空間

Active Directory Tasks （包含未來新增至網域中的電腦或使用者）

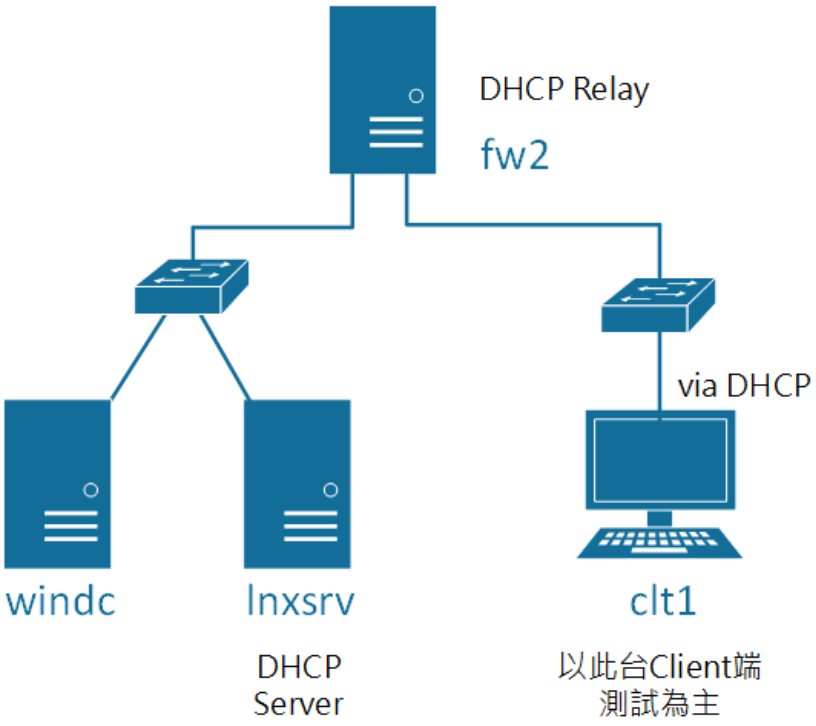
- 以下 Tasks 除了 windc 外均須自動套用於網域內所有電腦：
  - IT 群組的使用者於網域中任意電腦登入後，將取得該電腦的系統管理者權限（等效於本機的 Administrators 群組）
- 將所有使用者的 Edge 瀏覽器首頁設為 www.starlux.com
- 為提升上網的安全性，Ground_Staff 群組的使用者於瀏覽器下載檔案後，禁止執行副檔名為 exe 的檔案（針對使用者預設的 Downloads 的目錄限制即可）
- 為增加空服員的方便性，Flight_Attendant 群組的使用者登入後，自動開啟 Edge 瀏覽器並進入 booking.starlux.com

clt1

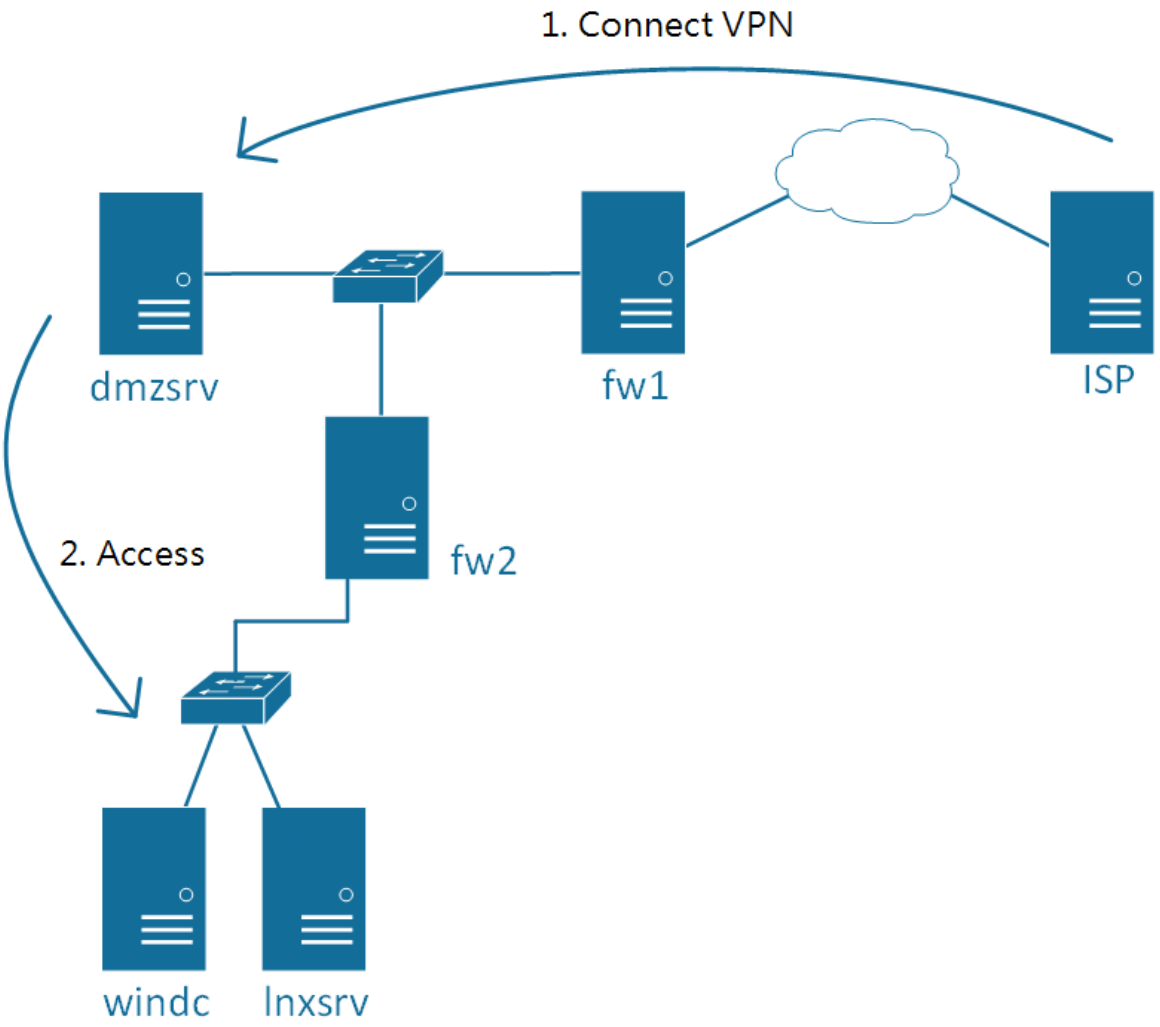
- 完成試題要求後，應可成功連線至 http://www.worldskills.tw 及 8.8.8.8

Client 運作模式

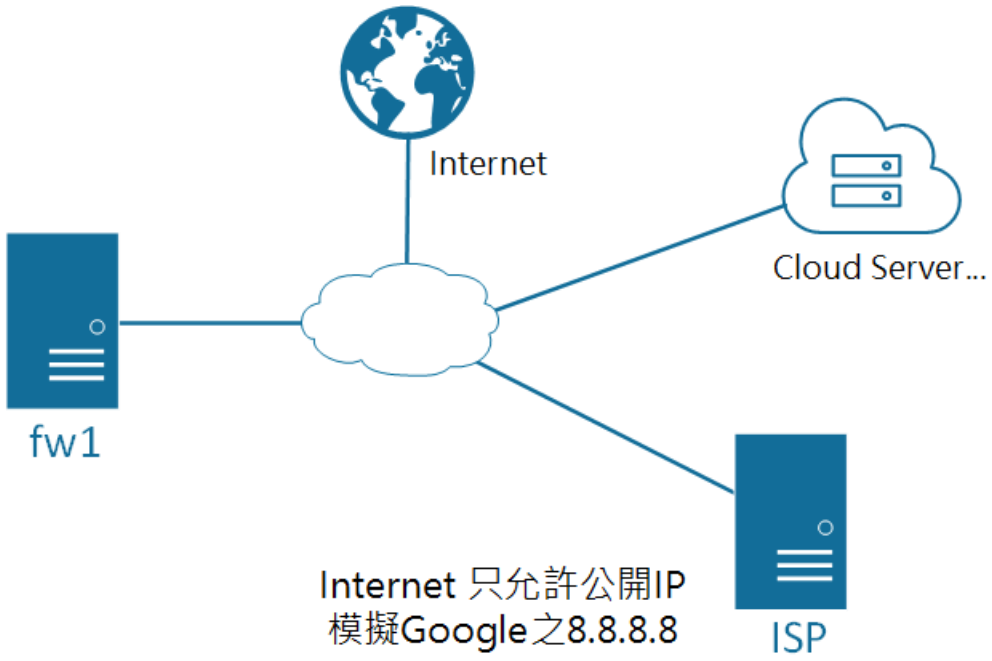
DHCP 服務架構



VPN 流量方向

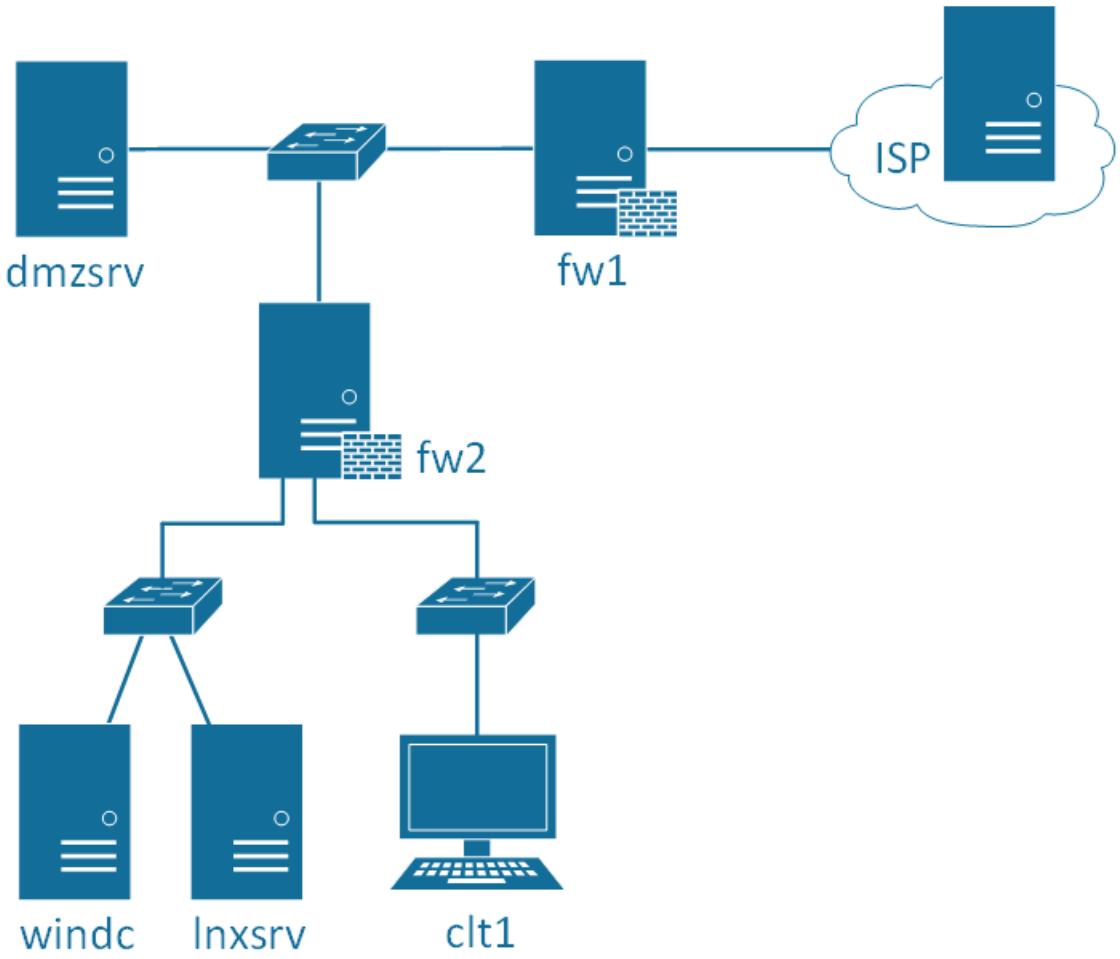


Internet 網際網路



第 49 屆全國技能競賽 資訊與網路技術

第二日 Part 1 試題



- 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。
- 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。
- 今日之工作項目將延續昨日之部分情境，部分資訊請選手自行參考昨日的試題
- 有關防火牆之設定，請採用**最嚴謹**的方式設定，且**所有方向**均須考慮！

dmzsrv

- *（提醒）此 Server 的 Web 會對 lnxsrv 發起 MySQL 連線！*

fw1

- 透過 iptables，設定如下的存取控制：
  1. 來自 Internet 的連線，僅允許存取 dmzsrv 對外的服務，並可正常建立連線
  2. 內部網路對 Internet 的存取，不進行限制，並可正常建立連線
  3. 允許本機所有對外提供的服務
  4. 除必要或返程連線外，禁止轉送或於本機發起任何連線至內部網路
  5. 封鎖其他未經允許的連線
  - 系統重新啟動後，需保留所有防火牆規則及流量統計資訊

fw2

- 請勿使內部網路經過 fw2 後被 NAT，須保持來源為 192.168.0.0/16 網段
- 透過 iptables，設定如下的存取控制：
  1. 除 MySQL 連線外，禁止轉送或於本機發起任何連線至內部網路
  2. 來自內部網路的連線不進行限制，並可正常建立連線
  3. 允許 VPN 連線到 192.168.10.0/24 及 VPN 認證所需的連線
  4. 允許監控服務所需的連線
  5. 封鎖其他未經允許的連線
  - 系統重新啟動後，需保留所有防火牆規則及流量統計資訊

windc

- 依照附錄 A 建立 10 位 AD 使用者
- 在 DNS 服務中，所有 dmzsrv 對外提供的服務所需的資源紀錄，在**內網**一律使用**外部 IP**
  例如：booking.starlux.com -> 39.49.10.11
- 在 E:\data 建立分享資料夾，提供於\\starlux.com\data，僅有 IT 群組能存取

lnxsrv

- 設定 Icinga2 監控服務，透過 https://monitor.starlux.com:81 連線，可使用帳號密碼 icingaadmin/Skills39 進入
  - 監控 booking.starlux.com 網站的狀態

- 使用 ICMP 監控 fw1 主機

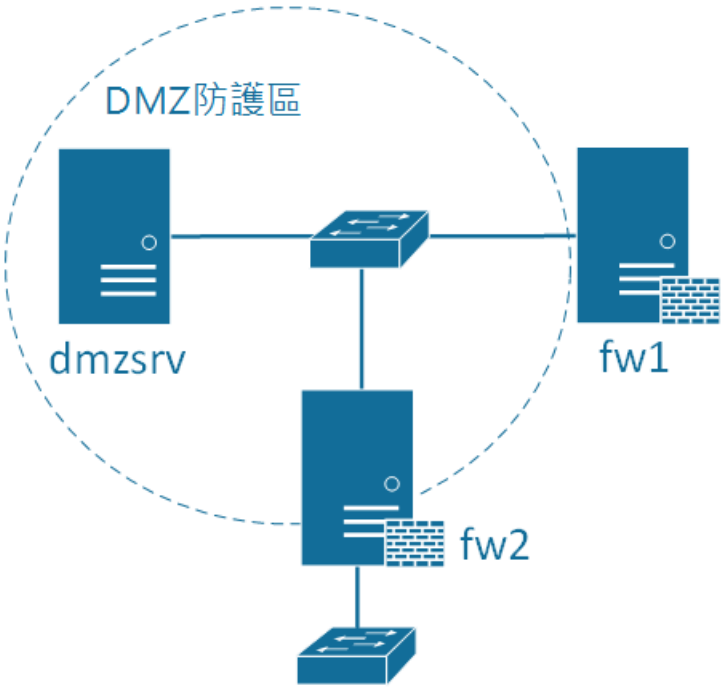
clt1

- 完成防火牆之存取控制後，既有服務應正常運作，評分時透過此台主機進行相關測試！

Appendix A – Active Directory Users

Username	Group	Password
MGT01 ~ 10	Management	Skills39

DMZ



第 49 屆全國技能競賽 資訊與網路技術

第二日 Part 2 試題

※請在時間內完成 Part 1 及 Part 2 試題，兩 Part 將一起評分

ISP

- 扮演測試 SSH 及相關防火牆設定，如須預先設定相關設定，請選手於評分前先將設定設好，若評分時無法執行可能導致部分項目失分

fw1

- 建立一個名為 rc1 的本機使用者
- 設定防火牆的存取控制 LOG：
  - 將 SSH 連線 Log，紀錄至：
    /var/log/fw_ssh.log
  - 將所有遭到封鎖的連線 Log，紀錄至：
    /var/log/fw_deny.log
  - 系統重新啟動後，需保留所有防火牆規則及流量統計資訊
- 將防火牆的連線 Log 同步至 lnxsrv 主機
- 於 /list_deny.sh 新增一個 Script，執行後會列出最後 6 筆被封鎖的連線 LOG，且只允許 rc1 使用者執行該腳本
- 設定 SSH 服務，對外提供於 Port 2019，僅允許 rc1 使用者連線，且於連線參數中執行任何指令均無視，連線後自動執行上述腳本，執行後自動中斷連線！
- 當使用者登入後，其他使用者（可包含自己）的終端介面會顯示：
  - 範例：

```
mgt01 logged in...
Have a nice day !
```

```
USERNAME logged in...
Have a nice day !
```

fw2

- 設定防火牆的存取控制 LOG：
  - 將所有遭到封鎖的連線 Log，紀錄至：
    /var/log/fw_deny.log
  - 系統重新啟動後，需保留所有防火牆規則及流量統計資訊
- 將防火牆的連線 Log 同步至 lnxsrv 主機

windc

- 將群組分享資料夾改以 AES 加密的方式提供檔案分享服務

lnxsrv

- 為提升安全性，當 root 使用者登入後，若閒置超過 1 分鐘時，將自動登出終端介面
- 加入 starlux.com 網域，網域使用者將可登入本機
- 僅允許 IT、Management 兩群組的網域使用者於終端介面登入
- 將 /data 與 windc 的分享資料夾 \\starlux.com\data 同步，並僅允許 IT 群組存取
- 將來自 fw1 及 fw2 的 Log 分別記錄於：
  - From fw1：/data/fw1/ssh.log 及 /data/fw1/deny.log
  - From fw2：/data/fw2/deny.log
  - 以上所有日誌，IT 群組的網域使用者須能夠讀取

clt1

- 完成試題要求後，既有或新增的服務應能夠繼續存取使用！

Log 運作架構