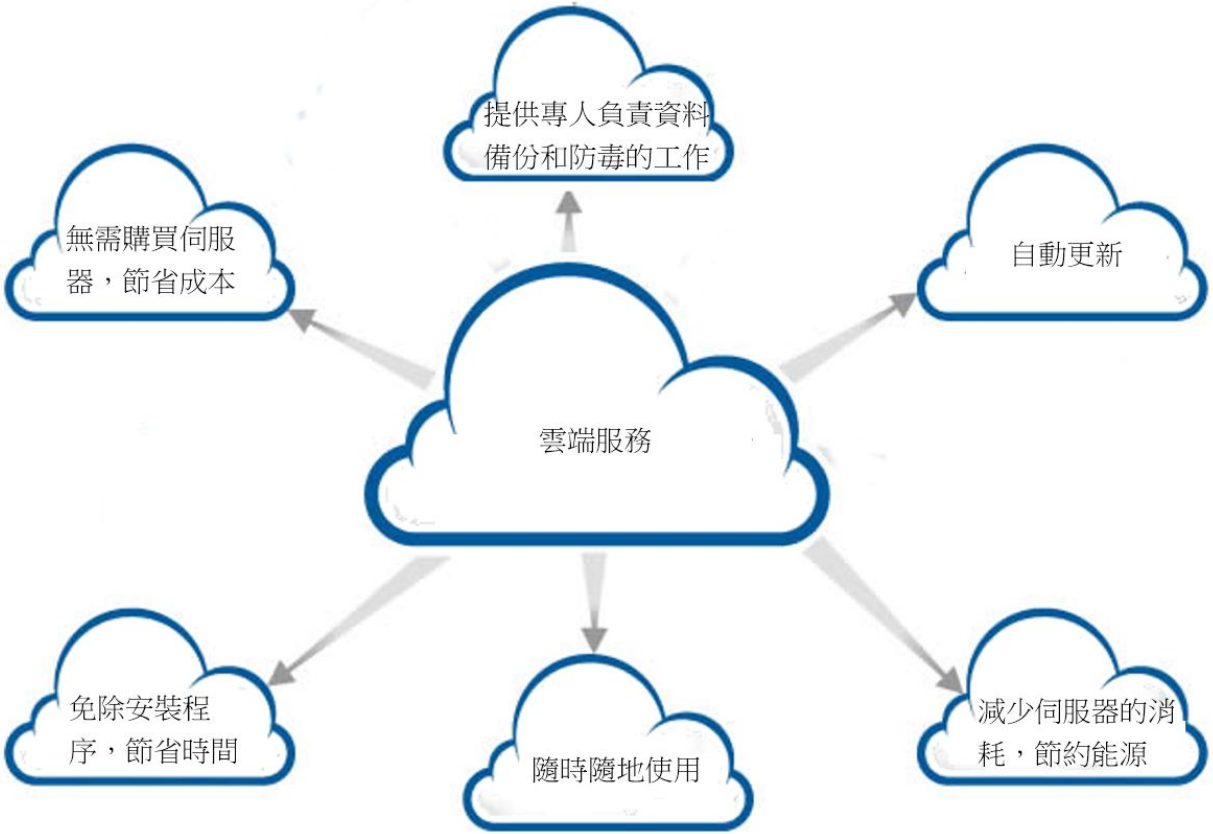
# 技術介紹與應用(雲端服務)

## 第三組

# 雲端服務

基本概念與應用範圍:

指透過網路來提供各種運算資源和服務的模式，而這些運算資源可以包括伺服器、儲存空間、資料庫、網路、軟體和應用程式等。使用者不需要在地端環境自行建立大量的實體軟硬體設備，就可以藉由網路來取用這些相關運算資源。對用戶而言，當用戶的手機儲存空間不夠空間時，雲端服務是幫助用戶儲存圖片，檔案等資料作另一個儲存位置。它應用於 Google Drive，代替用USB。



# 雲端技術的介紹

特點:

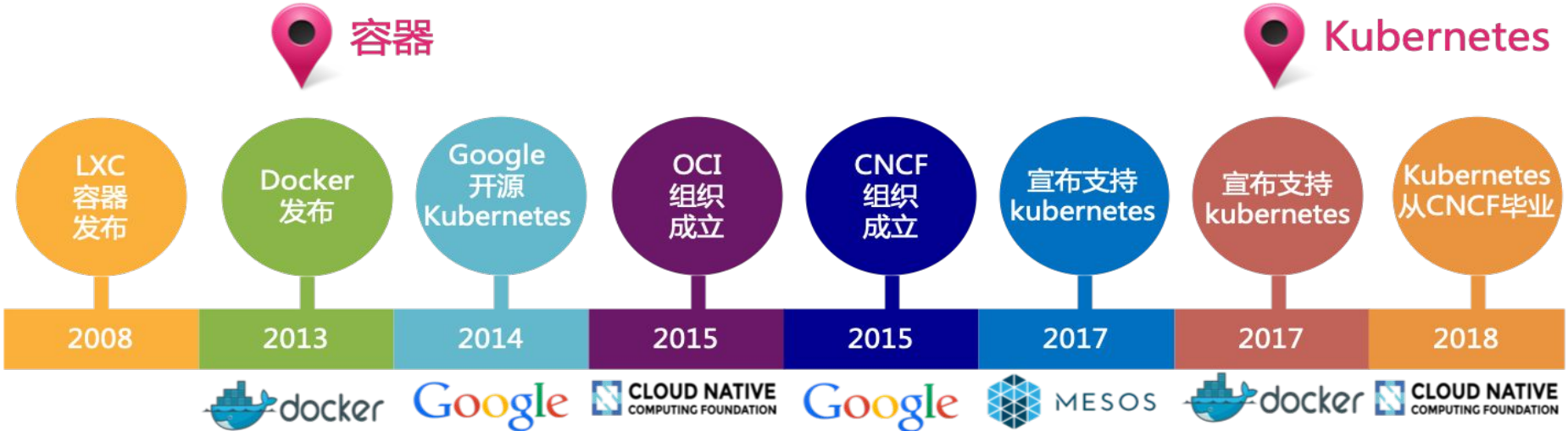
雲端服務是幫助用戶儲存圖片，檔案等資料，以及定時自動與手機同步儲存資料。

技術特性和運作原理:

雲端運算會透過網路(通常是網際網路)，將使用者連至他們申請和存取租用運算服務的雲端平台。中央伺服器會處理用戶端裝置和伺服器間的所有通訊，以利進行資料交換作業。

歷史發展和未來趨勢:

雲端運算是繼1980年代大型電腦到客戶端-伺服器的大轉變之後的又一種巨變。使用者不再需要了解「雲端」中基礎設施的細節，不必具有相應的專業知識，也無需直接進行控制。雲端運算描述了一種基於網際網路的新的IT服務增加、使用和交付模式，通常涉及通過網際網路來提供動態易擴充而且經常是虛擬化的資源。以下是雲計算的歷史。



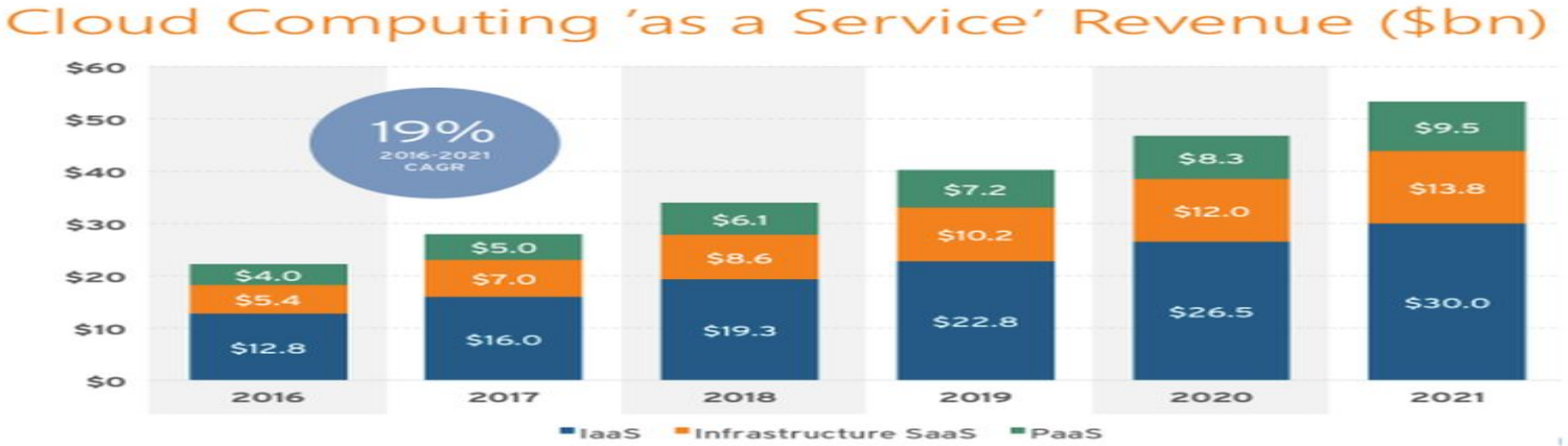
# 雲端技術的優勢

主要優勢和創新點:

雲端技術的主要優勢分別是縮小管理負荷成堆的伺服器和不停運轉的能源會迅速消耗成本，透過自動更新來節省時間。而在雲端技術的創新點的方面，運用多重雲的商業策略能使企業有效降低風險、優化雲端成本並同時改善運算效率，這些優點鼓勵了企業在他們的雲端轉型旅程中採用這項策略。

# 雲端技術的效率和成本：

遷移至雲端能夠讓各種類型和規模的機構能夠加快移動速度、提高靈活性並推動革新。雲端運算的轉變徹底改變了我們的工作、溝通和協同合作方式，而且在現今的數位世界中，變得越來越需要保持競爭力。以下是雲端技術的成本。



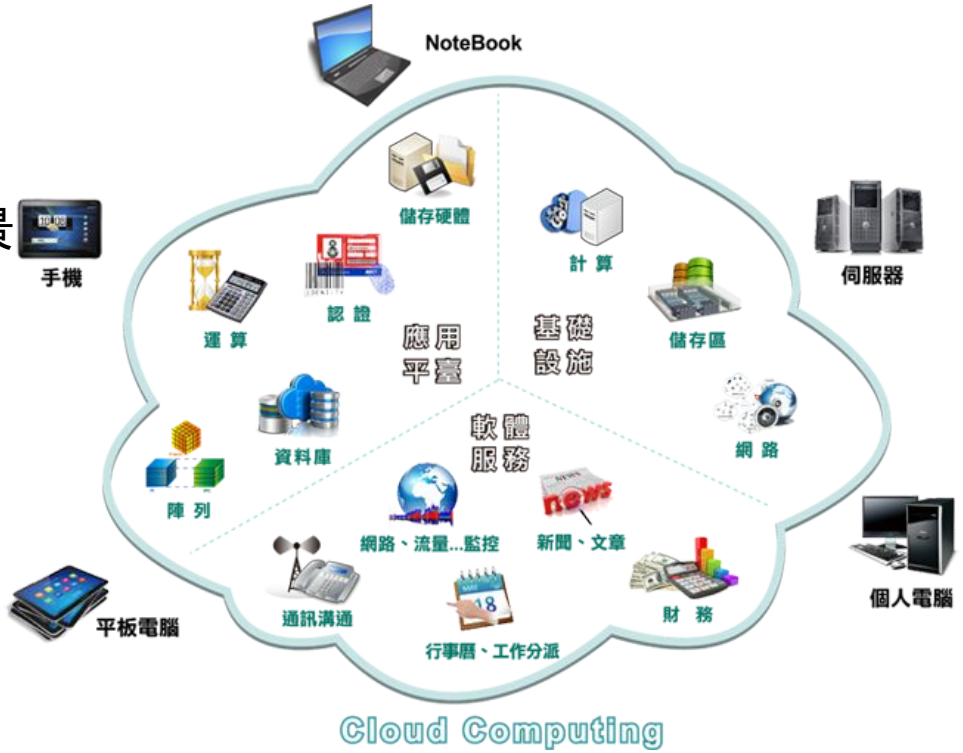
# 雲端技術的應用

具體應用場景或案例:

技術應用的具體應用場在辦公室工作場景

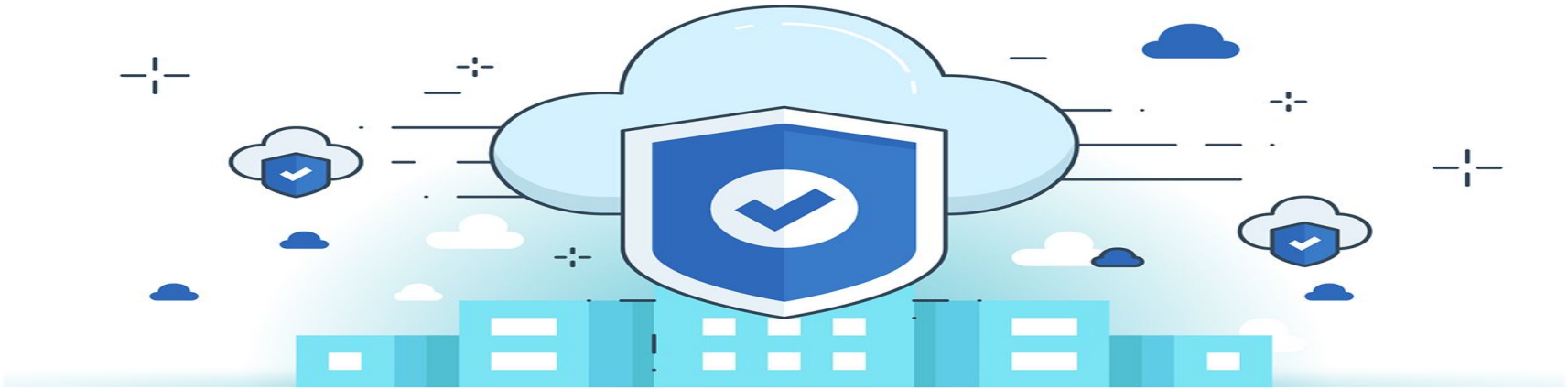
應用場景中的效益和挑戰:

e.g.大數據管理, 5G。



# Q&A

# 網絡安全威脅分析
# （雲端服務）
# 第三組



# 1.1-1.2雲端服務的威脅/來源：

當帳戶遭入侵，攻擊者通常會使用網路釣魚活動來竊取員工密碼，並取得系統和重要公司資產的存取權。硬體和軟體弱點：無論組織使用的是公用還是私人雲端，安裝硬體和軟體的修補程式並保持在最新狀態至關重要。而在內部威脅，人為錯誤是造成安全性缺口的一大原因。

# 1.3雲端服務的嚴重程度和可能性：

雲端出現安全漏洞時，公司都會在試圖恢復時損失金錢、時間和資源。雲端漏洞所導致的停機可能造成嚴重的營運挫敗——雲端中的應用程式和資料，以及與雲端連線的裝置和網路可能會暴露於許多威脅中。

# 1.4針對每種雲端服務威脅的對策威脅的可能性:

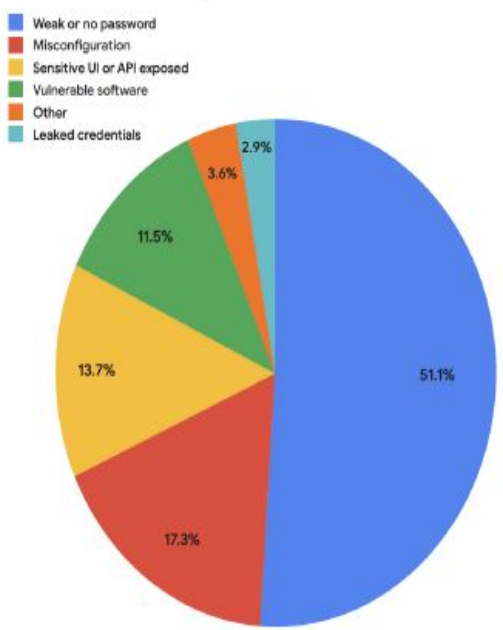
為了應付雲端服務威脅，雲端安全機制是一組網路安全措施，用途是保護雲端應用程式、資料和基礎架構，主要是透過實行安全性政策、做法、控管措施，以及身分與存取權管理和資料遺失防護工具等其他技術，來協助保護雲端環境，防範未經授權的存取、線上攻擊和內部威脅等問題。

# 2. 雲端服務威脅分析

重點:SSH 及 RDP 上的脆弱密碼是導致雲端服務遭受攻擊的主因

根據 Google 所做的資安事件統計，超過半數的雲端入侵事件起因於 SSH 或 RDP 等遠端通訊協定設置過於脆弱的密碼或根本沒設定密碼，駭客得以輕鬆獲取企業的雲端平台權限，進而濫用其雲端資源於挖礦等用途。

- 主要來源是攻擊類型:阻斷服務攻擊(DOS)、憑證外洩、暴力攻擊(Brute-force attack)



# 3.雲端服務安全問題來源

雲端環境承受的安全性風險和傳統環境可能會發生的問題類似，例如內部威脅、資料侵害、資料遺失、網路釣魚、惡意軟體、分散式阻斷服務攻擊和 API 有安全漏洞的情況。

不過，大多數機構都有可能會遭遇特定的雲端安全性難題，包括：無法掌握情況、設定錯誤、存取權管理、變動不定的工作負載和法規遵循。

## 雲端安全檢查表

| 檢查項目 |
| --- |
| 1.實體及邏輯網路的屏障 |
| 2.端點的存取控制及管理 |
| 3.非密碼認證機制 |
| 4.憑證的質量控制 |
| 5.密碼重設的流程與機制 |
| 6.即時的異常檢測 |
| 7.事件日誌的完整度與備份、分析 |

資料來源：DIGITIMES，2010/10

# 4.雲端安全問題

在過去12 個月內經歷過安全事件的雲端用戶中，19% 的事件涉及錯誤配置的資源或帳戶。由於特定於提供者的配置設定範圍廣泛，錯誤配置仍然是雲端資安的重大挑戰。不熟悉雲端環境的公司及其員工可能會意外地錯誤配置這些設置，使雲端環境容易受到攻擊。多雲端環境的盛行加劇了這個問題，公司必須為多個不同的雲端供應商正確配置設定。

# 雲端服務案例:

1. **Capital One 數據洩露事件**:

   - 2019年,Capital One遭到黑客攻擊,導致超過10億條客戶信息被盜取。

   - 問題源於該銀行在雲端存儲未妥善配置和保護客戶數據。

2. **Equifax 數據洩露事件**:

   - 2017年,信用報告公司Equifax遭受攻擊,導致1.47億用戶信息遭黑客盜取。

   - 調查發現,是由於Equifax未及時修補軟件漏洞,導致黑客得以入侵。

3. **香港仁安醫院被駭**:

   - 香港仁安醫院的電腦系統2024被駭客惡意攻擊,化驗報告及配血都要改由人手操作

   - 被入侵的原因多是涉事公司無安裝防毒軟體，甚或員工點擊釣魚網站導致。

# 案例解釋:

透過以上三個事件去反映他們的公司在網絡安全上有不足的預防保護措施。例如欠缺定期更新防火牆軟件，修補網絡上的漏洞，不能向客戶提供完善的雲端服務等。為了防範同類事件發生，公司應該從人力培訓做起，例如向員工提供網絡安全的教育，加強他們對網絡安全的意識，定時監督員工處理網絡安全的工作，從而減少人為錯誤。這樣就可以令黑客入侵的威脅減少。而且公司要定期更新防火牆軟件，修補網絡上的漏洞。才能減少發生網絡上的危險。

# 案例來源：

Capital One 數據洩露事件：

https://www.ithome.com.tw/news/139316

Equifax 數據洩露事件：

https://www.bbc.com/zhongwen/trad/chinese-news-51451397

香港仁安醫院被駭：

https://www.worldjournal.com/wj/story/121341/7912981?zh-cn

# Q&A

# 保護措施與模型連繫

# （雲端服務）

## 第三組

# 1.雲端服務的保護措施：

為因應雲端服務的安全，公司會增強端點設備安全、採用強大的憑證策略、使用文件加密等，這些是基本手段。此外，定期評估和維護內部系統、資料複製和備份等也是防止資料遺失、增強系統安全的良策。每年開支約63萬。

# 2.雲端安全與OSI 模型連繫:

1. 物理層:(Physical Layer)
- 負責定義物理設備和介質的特性,如線纜類型、信號特性、連接器等。
- 處理物理媒體上的傳輸。

2. 網絡層:(Network Layer)
- 處理分組交換、邏輯地址、路由和轉發等功能。
- 負責確定資料在網絡上的傳輸路徑。

3. 傳輸層:(Transport Layer)
- 提供端到端的可靠數據傳輸服務。
- 包含差錯控制、流量控制、分段和重裝等功能。

4. 應用層:(Application Layer)
- 最接近用戶的層次,定義應用程序接口。
- 為特定應用程序提供服務,如文件傳輸、電子郵件等。

▲ 圖1-31 OSI 7層架構

# 雲端安全主要影響(OSI)？

## 在營辦方方面:

1. **物理層(Physical Layer)**:
   - 負責定義物理設備和介質的特性,如線纜類型、信號特性、連接器等。

2. **傳輸層(Transport Layer)**:
   - 提供端到端的可靠數據傳輸服務。
   - 包含差錯控制、流量控制、分段和重裝等功能。

3. **數據鏈路層(Data Link Layer)**:
   - 負責可靠的數據幀傳輸,如差錯控制、流量控制等。
   - 提供局域網存取方法。
   - 處理介質訪問和錯誤糾正。

4. 網絡層:(Network Layer)
   - 處理分組交換、邏輯地址、路由和轉發等功能。
   - 負責確定資料在網絡上的傳輸路徑。

## 在用戶方面:

1. **應用層(Application Layer)**:
   - 最接近用戶的層次,定義應用程序接口。
   - 為特定應用程序提供服務,如文件傳輸、電子郵件等。

2. 網絡層:(Network Layer)
   - 處理分組交換、邏輯地址、路由和轉發等功能。
   - 負責確定資料在網絡上的傳輸路徑。

# 針對網絡層的專門防禦措施或技術

可添加包括防火牆(Firewall):
在雲端環境中部署高性能、可配置的防火牆,對進出流量進行嚴格的訪問控制和監控。

利用虛擬專用網(VPN):
可以保護在線隱私權並保護資訊不受黑客、網絡監控等。

網絡監控和入侵檢測(IDS)
- 部署網絡流量監控和預防系統實時監測和分析網絡活動。
- 及時發現和阻止網絡層面的異常行為或攻擊。

安全配置和更新(Security update):
- 確保雲端網絡設備和軟件的安全配置和及時更新,修補已知漏洞。
- 制定網絡設備和軟件的安全基線和標準。

# 3.雲端安全與TCP/IP模型連繫:

1. **網絡接口層(Network Interface Layer)**:
   - 在雲端環境中,這一層的安全主要涉及虛擬網卡、交換機、路由器等網絡設備的安全配置和管理。
   - 確保網絡接口層設備的安全補丁更新、配置檢查等措施。

2. **網際網路層(Internet Layer)**:
   - 這一層對應於 OSI 模型的網絡層,雲端安全重點在於防火牆、路由、IP 地址管理等。
   - 確保網際網路層的訪問控制、網路隔離、入侵檢測等安全防護。

3. **傳輸層(Transport Layer)**:
   - 這一層對應於 OSI 模型的傳輸層,雲端安全重點在於 TCP/UDP 協議的安全性。
   - 確保傳輸層的端到端加密、身份驗證、DDoS 防禦等安全機制。

4. **應用層(Application Layer)**:
   - 這一層對應於 OSI 模型的應用層,雲端安全重點在於應用程序本身的安全性。
   - 確保應用層的身份和訪問管理、代碼審核、數據加密等安全實踐。

# 雲端安全主要影響(TCP/IP)

**網絡接口層(Network Interface Layer)**:

1. **虛擬網卡安全**:
   - 確保雲端虛擬機器使用安全隔離的虛擬網卡,避免跨虛擬機器的網絡攻擊。
   - 對虛擬網卡進行安全配置,如禁用非必要的功能、配置ACL規則等。
   - 定期檢查虛擬網卡的安全性設置,及時修復發現的漏洞。

2. **交換機安全**:
   - 採用安全的交換機配置,如開啟端口安全、VLAN隔離等功能。
   - 加強對交換機的訪問控制,只允許授權的管理人員訪問。
   - 確保交換機軟件版本及時更新,修補已知的安全漏洞。

3. **網絡設備管理安全**:
   - 採用集中化的網絡設備管理平台,對雲端網絡設備進行統一的安全管理。
   - 實施基於角色的訪問控制(RBAC),限制網絡管理人員的操作權限。
   - 對網絡設備的配置變更、操作日誌等進行持續監控和審計。

# 針對網絡接口層的專門防禦措施或技術

1. 設備配置安全:確保網絡設備(如路由器、交換機等)的安全配置,禁用不必要的服務和協議,設置強密碼等。

2. 漏洞管理:定期掃描和修補網絡設備及系統的安全漏洞,以減少被攻擊者利用的風險。

3. 身份驗證和訪問控制:針對重要資源實施嚴格的身份驗證和訪問控制,防止未授權的存取。

4. 日誌記錄和監控:詳細記錄網絡活動日誌,並對其進行分析和監控,以便及時發現和應對異常情況。

5. 入侵檢測與防禦系統(IDS/IPS):部署IDS/IPS系統,實時監測網絡流量,並對可疑活動發出警報。IPS系統還可以主動阻擋或緩解一些攻擊。

# 4.雲端安全與網絡架構模型連繫:

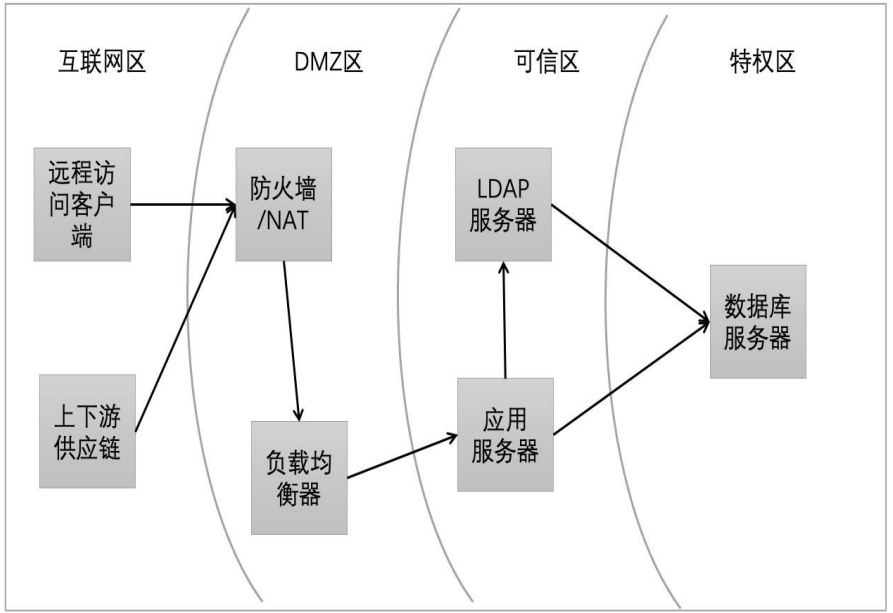
網絡架構模型,也就是OSI(開放式系統互連)模型和TCP/IP模型,它們定義了網絡通信的各個層次,並提供了網絡設備和協議之間的連接機制

兩種模型的連繫:

- TCP/IP模型更貼近現實網絡實現,OSI模型則提供了更詳細的理論指導。

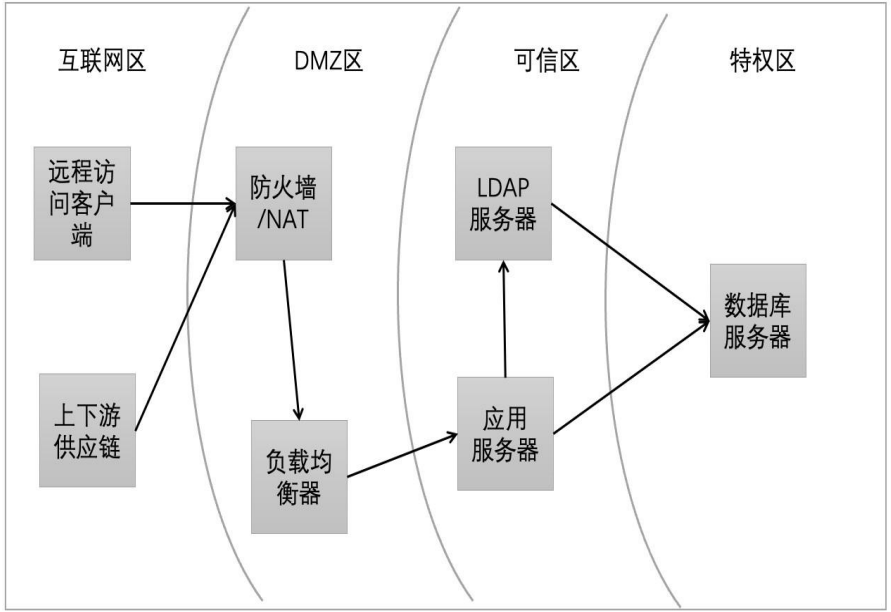
- TCP/IP模型的各層通常直接對應到OSI相應的層次,但並非完全一一對應。

- 網絡設備和協議的設計和實現通常會參考兩種模型,以確保網絡通信的標準化和互操作性。



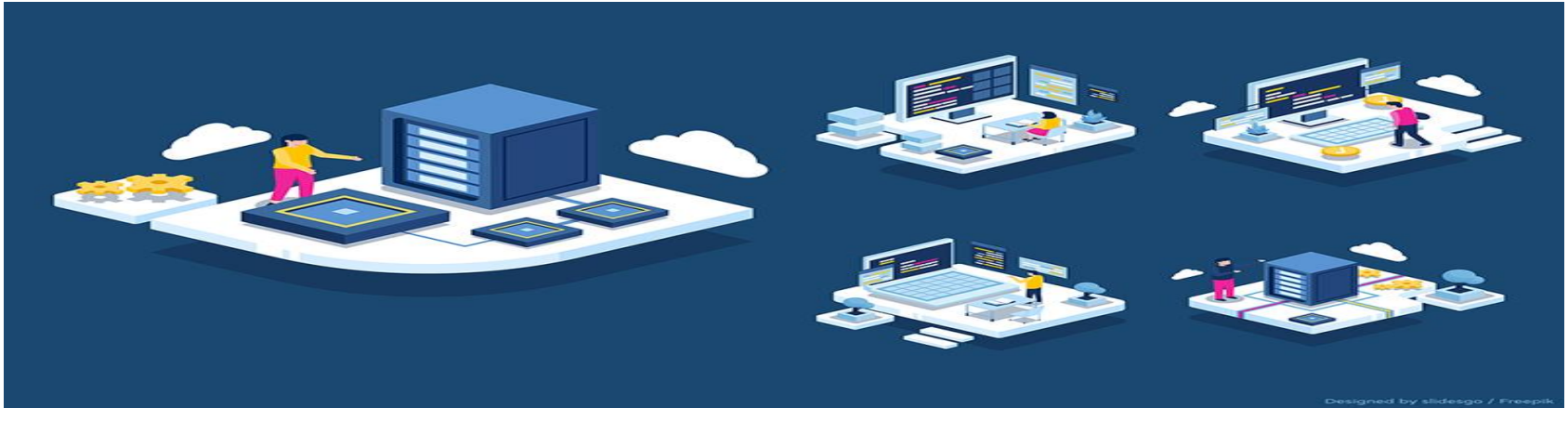
# 針對網絡接口層的專門防禦措施或技術(步驟):

1. 首先，透過在互聯網區的上下遊供應鏈或遠程訪問客戶端傳送信號給防火牆。
2. 然後，防火牆再傳送數據給負載均衡器。
3. 最後，負載均衡器可以傳送數據給服務器或直接傳送至數據庫服務器。



# 針對網絡接口層的專門防禦措施或技術:

1. 軟件配置安全:確保有安全的軟件(例如防火牆，負載均衡器)，去過濾和檢查該軟件有沒有病毒入侵風險。
2. 定期掃描客戶的雲端裡所儲存的數據和資料。作出保護和備份。
3. 在客戶提取雲端的資料前，必須要確定客戶的身分以及進行雙重認證，以便保護雲端安全和減少入侵的風險。
4. 定期派人檢查雲端機房，令雲端服務能夠繼續長時間服務。



# 針對網絡接口層的專門防禦措施或技術(例子):

1.雲端安全需要綜合的安全策略，包括適當的存取控制、加密、持續監控，請專業的安全機構進行全方位的審計、教育培訓等方面的措施，以確保雲端環境的安全性和穩定性。例如對關鍵資料進行端對端加密，如果要使用加密，加密金鑰的安全管理至關重要，保留金鑰備份，最好不要保存在雲端。例如預防配置錯誤這樣的基本漏洞，雲端安全風險將大大降低。最後，無論是個人用戶、中小企業用戶或企業級雲端用戶，確保網路和設備盡可能安全是非常重要的。(**SlowMist 慢霧團隊**)

2.專案方需確認客戶端僅透過安全的API 存取雲端服務，避免注入攻擊、跨網站腳本等惡意活動。使用API 也可以在存取雲端服務之前對客戶端進行身份驗證和資料檢驗，以確保存取安全和資料安全。考慮到個人電腦作為客戶端的安全防護能力較弱，不建議透過個人電腦直接呼叫API 對系統進行資料存取和維運，而是透過雲端上虛擬桌面或安全的跳板機來完成相關的存取。(**Beosin 團隊**)

# Q&A