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:

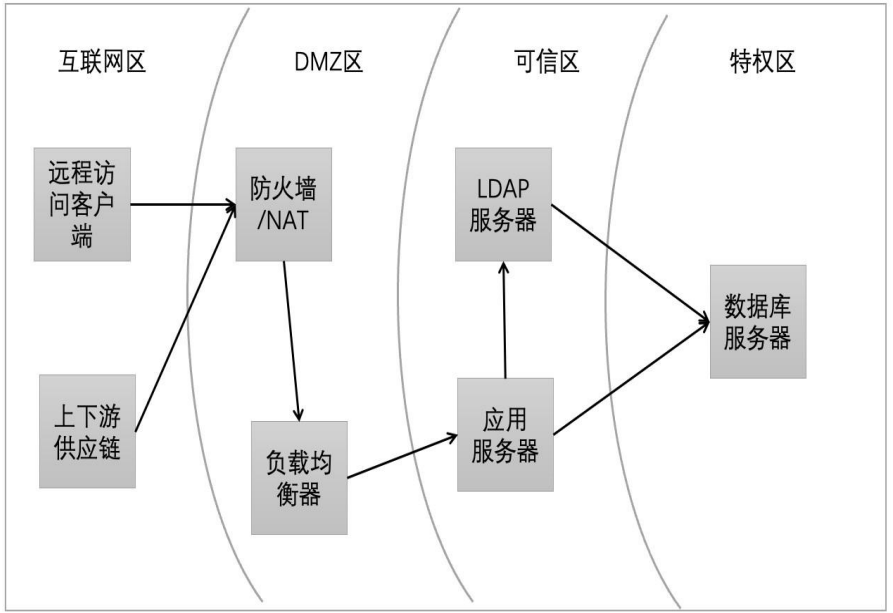
網絡架構模型,也就是OSI(開放式系統互連)模型和TCP/IP模型,它們定義了網絡通信的各個層次,並提供了網絡設備和協議之間的連接機制

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。

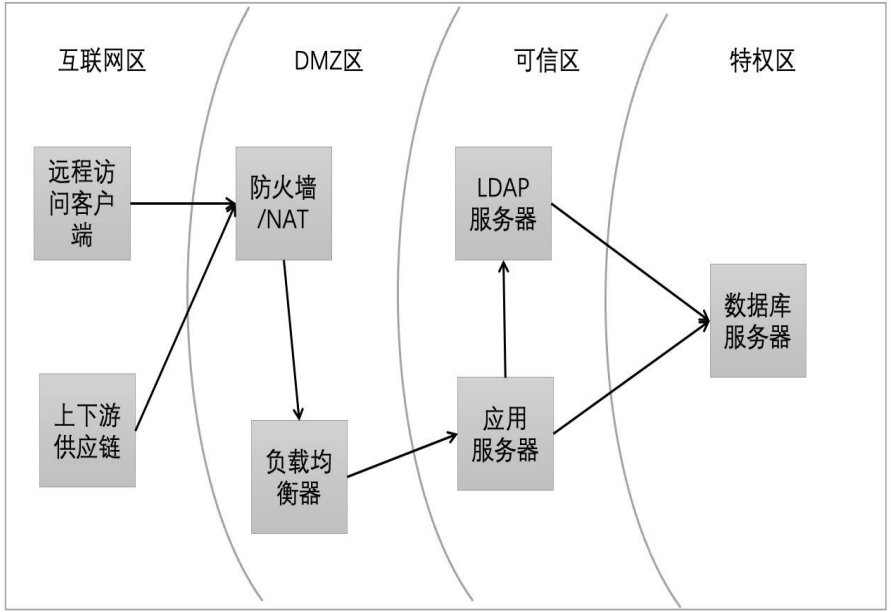
- TCP/IP模型的各層通常直接對應到OSI相應的層次,但並非完全一一對應。

- 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。



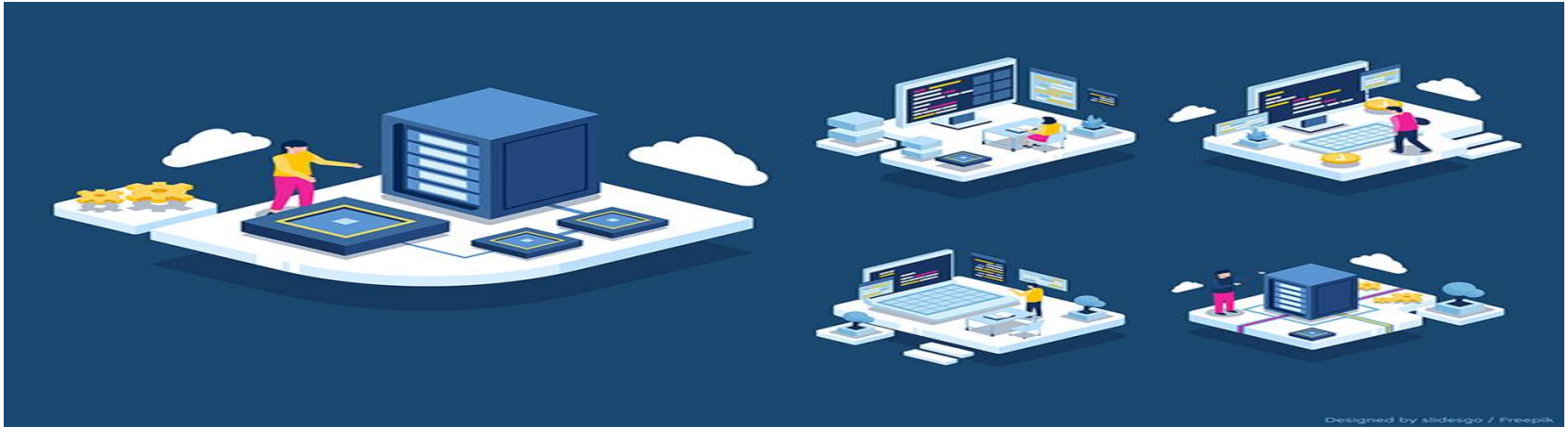
針對網絡接口層的專門防禦措施或技術(步驟)：

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。



Q&A