## 一、拓撲基礎設施層

##### **1.1 核心架構**

|  |  |  |
| --- | --- | --- |
| **組件** | **部署位置** | **功能說明** |
| 雙核心路由器 + 核心交換器 | 區域總部 | 提供高可用內部主幹傳輸與路由分流，支援多VLAN微分割與叢集高可用架構 |
| MPLS主線 + SD-WAN備援 + IPSec加密 | 區域總部 ↔ 各分行 | 建立安全、優先級分類的跨地區通道（MPLS主線 / SD-WAN備援），支援QoS設定（VLAN10為交易最高優先）與AES加密通訊 |
| 分行邊界路由器 + NGFW防火牆 | 各分行出口處 | 邊界路由與防火牆流量過濾，支援VLAN延伸、端點分段、應用層封包檢查與入侵防護 |
| 分層交換架構 | 各分行內部 | 核心交換器（L3）→ 樓層交換器（L2）→ 接入層，支援PoE、IP語音與網管介接 |
| 無線控制器 | 各分行機房 | 集中管理AP、實施SSID區隔（員工/ATM）與802.1X認證 |
| 雙ISP備援出口 | 各據點邊界 | 提供主要與備援網路路由（例如MPLS + 4G/LTE），並透過BGP路由自動切換，確保連線不中斷 |

##### **1.2 關鍵設備清單**

|  |  |  |  |
| --- | --- | --- | --- |
| 設備 | 部屬點 | 規格要求 | 高可用設計 |
| 雙核心路由器 | 區域總部 | 支援 BGP/OSPF，路由冗餘切換 | 雙電源、雙主控備援 |
| 核心交換器 | 區域總部 | L3 多層交換，支援虛擬堆疊與 VLAN 微分割 | 模組化堆疊設計 |
| NGFW防火牆（總部HA） | 區域總部邊界 | 次世代防火牆，支援 IPS/IDS、TLS 1.3 | 主備模式 (HA Pair) |
| 分行邊界防火牆 | 各分行入口 | 次世代防火牆，支援 VLAN 延伸、安全策略下發 | 單點高可用 |
| 分行無限控制器 | 各分行內部 | 管理員工/ATM SSID、配合 NAC/802.1X | 冗餘路由支援 |
| 存取交換器 | 各分行辦公區 | 24埠 GbE，支援 802.1X、PoE+ | STP 防迴圈 |
| 資料庫防火牆 | 區域總部系統層 | SQL協定解析、資料層封包稽核 | Inline 模式備援 |
| WAF應用防火牆 | DMZ區 | 保護外部網站與 API、具備Bot防禦能力 | 雙實例部署 |
| DLP機制 | 區域總部出口 | 機敏資料偵測與封鎖、與 SIEM 整合 | 高效能模式運行 |
| 虛擬伺服器叢集 | 區域總部系統層 | 支援 VMHA、分區虛擬化（交易/內部） | 自動故障遷移 |
| 備份NAS | 區域總部 | 支援每日排程快照、資料加密 | RAID5+遠端複寫 |

## 二、系統層拓撲

**2.1 系統區段架構**

|  |  |  |  |
| --- | --- | --- | --- |
| 網路區段(VLAN) | 包含系統 | 隔離要求 | 資安控制 |
| 交易區 (VLAN10) | 核心銀行系統、支付閘道、加密資料庫 | 與辦公區與DMZ區完全隔離，僅允許 TLS 1.3 加密通訊 | * 微分割 (Micro-segmentation) * 資料庫防火牆 (DB Firewall) * 零信任通道驗證 |
| 辦公區 (VLAN20) | 郵件伺服器、檔案伺服器 | 限定協議通訊 (如SMTP/SMB)，可受控連外（Web Proxy） | * DLP控管外傳資料 * 使用者行為分析（UEBA） |
| DMZ區 (VLAN30) | 對外網站、API服務 | 僅開放必要端口（如 HTTPS 443、API Gateway 入口） | * WAF 防護與 Bot 攻擊阻擋 * API 金鑰驗證與速率限制 * 定期弱點掃描與修補管理 |

##### **2.2 系統通訊流程：跨分行交易流程**

1. **終端認證：**分行櫃員電腦 → 802.1X認證 → AD域控
2. **交易發起：**終端 → 交易區VLAN → 區域總部核心系統（加密通道）
3. **資料庫存取：**交易內容會觸發核心系統查詢加密資料庫，透過資料庫防火牆過濾指令，確保存取行為合法。
4. **風險檢查與行為分析：**經SIEM即時分析交易模式（異常行為觸發阻斷）

##### **2.3 備援設計**

1. **異地備份**：交易資料同步至總部+雲端（AWS S3 Glacier加密存儲）
2. **故障轉移**：核心系統叢集化（如Oracle RAC），VIP自動切換

## 三、基礎設施資安防護規劃

### A. 網路安全架構

1. **邊界防護**：
2. **遠端存取安全**：
3. **內部網路防護**：

### B. 端點安全

1. **終端防護**：
2. **行動設備管理**：

### C. 資料安全

1. **資料傳輸**：
2. **資料儲存**：

## 四、應用系統資安規劃

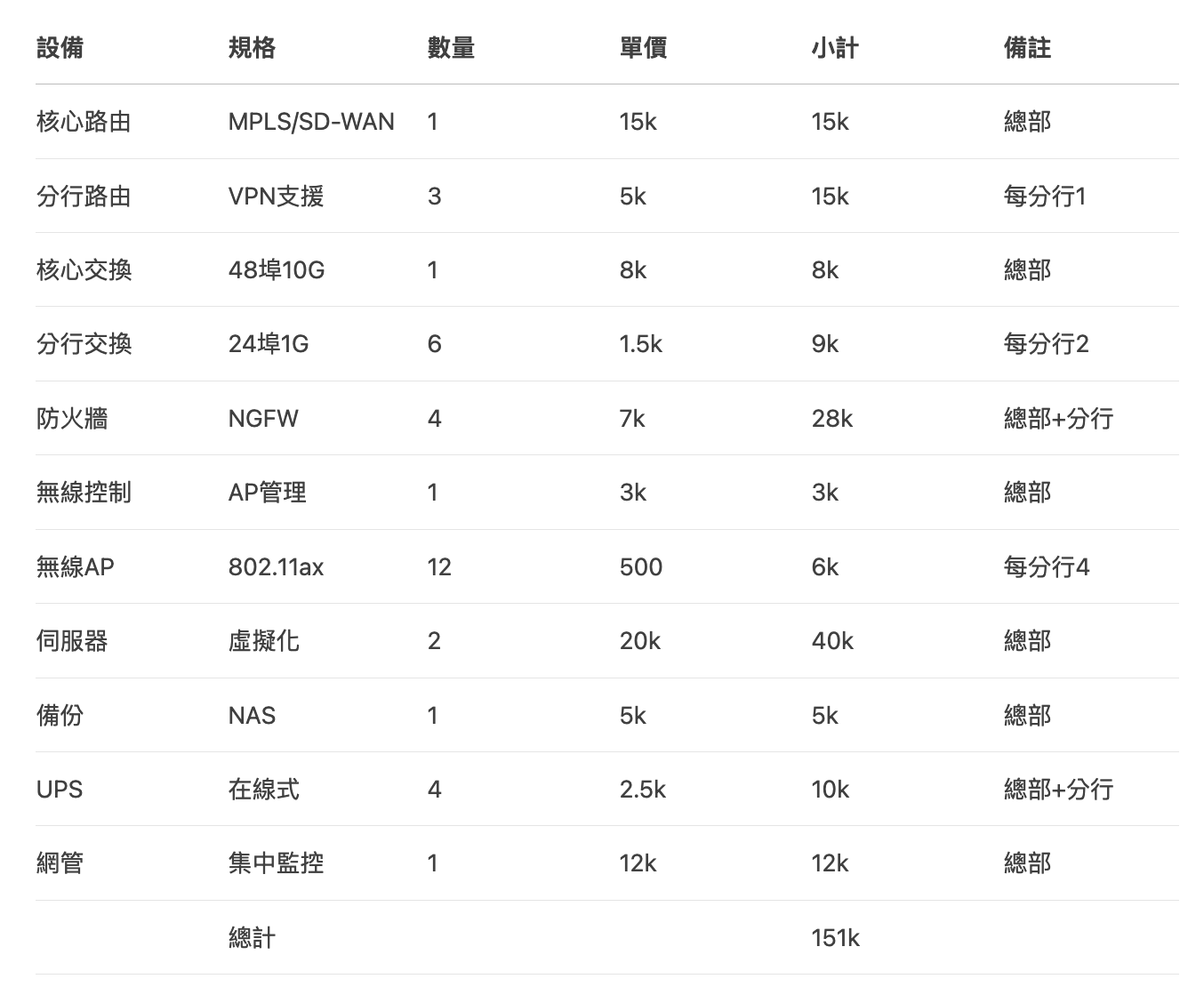
### A. 交易系統安全架構

1. **多層防護**：
2. **存取控制**：

### B. 交易流程安全控制

1. **身份驗證**：
2. **交易完整性**：
3. **異常檢測**：

## 五、預算估算



## 六、實施與維護計畫

### A. 實施計畫（建置階段）

1. 專案啟動與角色分工
   * 專案管理人（PM）：主導進度、預算、與資安策略整合。
   * 網路團隊：負責拓撲設計、設備部署（路由器、交換器、無線控制器等）。
   * 資安團隊：主責NGFW、防火牆、DLP、WAF、DB防火牆設定與測試。
   * 系統團隊：建置虛擬伺服器叢集、備份NAS、集中監控平台。
2. 階段性部署計畫

(1) 時間導向的分期目標規劃

|  |  |
| --- | --- |
| 階段 | 重點工作項目 |
| 第一階段 | * 建置基礎網路架構 * 部署核心安全設備（NGFW、防火牆、IPS） * 上線基本監控系統 |
| 第二階段 | * 實施進階安全控制（WAF、DLP、DB防火牆） * 強化應用系統安全 * 推動員工資安意識培訓 |
| 第三階段 | * 執行全面安全評估與滲透測試 * 導入持續改進機制（SOAR、UEBA） * 完成資安認證（如ISO 27001） |

(2) 技術導向的執行順序

* 網路與基礎設施建置
* 安全設備整合與策略規劃
* 監控、備份、與虛擬化平台實施
* 測試、模擬攻擊與風險評估
* 安全認證準備與文件化作業

### B. 維護計畫（營運階段）

### 1. 日常維運與監控

* 安全監控作業：
* 設備與日誌管理：

### 2. 定期維護與更新機制

|  |  |  |
| --- | --- | --- |
| **項目** | **頻率** | **說明** |
| 安全補丁與更新 | 每月 | 包含韌體、作業系統與資安設備特徵碼 |
| 安全評估 | 每季 | 檢討防火牆規則、存取權限與風險清單 |
| 滲透測試 | 每年 | 搭配資安稽核與認證所需 |
| 備份還原測試 | 每月 | 確保資料異地備援與可用性 |

C. 資安強化與持續改善

### 1. 零信任與多層防禦實施

* 對關鍵系統施行角色導向存取控制（RBAC）
* 實施多因子驗證與ZTA（Zero Trust Architecture）

### 2. 自動化偵測與事件回應

* 部署SOAR平台整合SIEM，實現自動回應流程
* UEBA技術辨識內部異常行為並進行風險評分

### 3. 端點與行動設備控管

* 所有裝置均部署EDR/XDR，具備隔離與回應能力
* MDM機制防範資料外洩，支援遠端鎖定與抹除

D. 合規與稽核計畫

### 1. 資安法規與標準對應

* ISO/IEC 27001： 系統性資訊安全管理機制
* PCI DSS v4.0： 資料加密、存取控管與稽核要求
* 金管會與地方法規： 包含災難復原、存取紀錄與監控要求

### 

組員名稱以及負責工作：

113EP8011 陳開威：系統資安規劃與預算估計

113EP8012 楊曼翎：基礎設施資安防護規劃

113EP8014 胡語庭：整體實施與維護計劃

113EP8020 羅慧榆：網路拓樸圖建構

113EP8011 陳開威：系統資安規劃與預算估計