共同供應契約軟體標
1130201
定興科技品項簡報檔

DECISION Group Inc.

Agenda

- Central Management System(CMS)

--中央管理系統

- Cyber Forensic System(CFS)

--網路數位內容鑑識系統

- Data Retention Management System(DRMS)

--數據內容彙整管理系統

- ED-CIC網路資訊集納系統
- ED-SSL網路加密封包透視系統
- Forensics E-Detective(FED)

--網路封包解譯鑑識系統

- Forensics Investigation Tookit(FIT)

--離線式網路封包鑑識整合工具

- Network Investigation Toolkit(NIT)

--整合型網路內容鑑識系統

- Remote Access Audit System(RAAS)

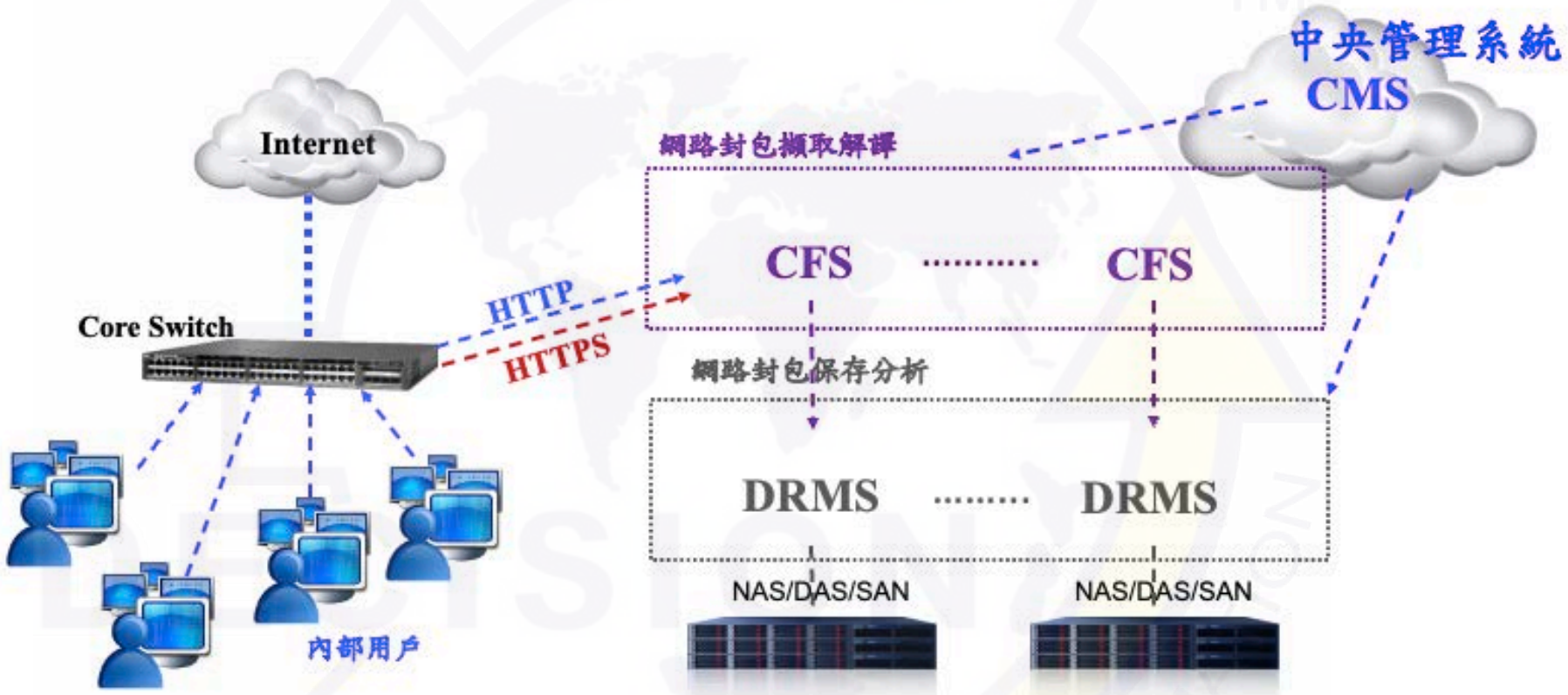
--遠端存取稽核系統

Central Management System (CMS)
中央管理系統

Central Management System(CMS)

- 可管控多套 CFS及DRMS。
- 可統一控管 CFS及DRMS帳號之認證及授權。
- 單一系統帳號可對不同的前端設備有不同的權限角色。
- 可監控不同的CFS及DRMS之系統狀態，提供包含CPU、RAM、HDD等相關資訊，以及網路封包擷取和資料產生狀況。
- 可針對CFS及DRMS進行關鍵字詞的派送、搜尋，同時搜尋各點設備的資料，快速找到相關的線索及資訊。
- 各點告警訊息將統一送達CMS，並由CMS通知管理人員，管理人員可以即時掌握相關訊息。
- 提供全文檢索功能，可利用中文檢索或條件搜尋等快速的從巨量資料內過濾出所需要的資訊。

Central Management System(CMS)



Cyber Forensic System(CFS)
網路數位內容鑑識系統

Cyber Forensic System(CFS)

- 使用者行為紀錄及內容解譯還原，包含郵件、網頁、FTP、CIFS、Telnet、SQL Command、HTTPS(option)等。
- 使用者網路行為事中告警、事後鑑識/稽核。
- 提供全文檢索及關鍵字搜尋。
- 具備網路流量統計圖表。
- 具備關鍵字告警及個資告警，當設定條件被觸發時會立即發送告警。
- 具備關聯性分析，可利用特定帳號或IP進行使用歷程查詢，以樹狀結構呈現查詢結果。
- 具備原始封包保留功能。

Cyber Forensic System(CFS)

Data Retention Management System (DRMS)
數據內容彙整管理系統

Data Retention Management System(DRMS)

- 可接收來自一套或多套之CFS的解譯資料及原始封包。
- 將來自一套或多套之CFS的資料集中管理。
- 提供條件式搜尋、全文檢索及檔案比對等多種查詢功能。
- 可一次查詢系統內所保存的一套或多套CFS的巨量資料。
- 可依照備份檔案名稱區分來源主機。
- 可同時掛載及查看大量且不同的ISO資料內容。
- 可結合NAS/DAS/SAN等儲存設備保存資料。

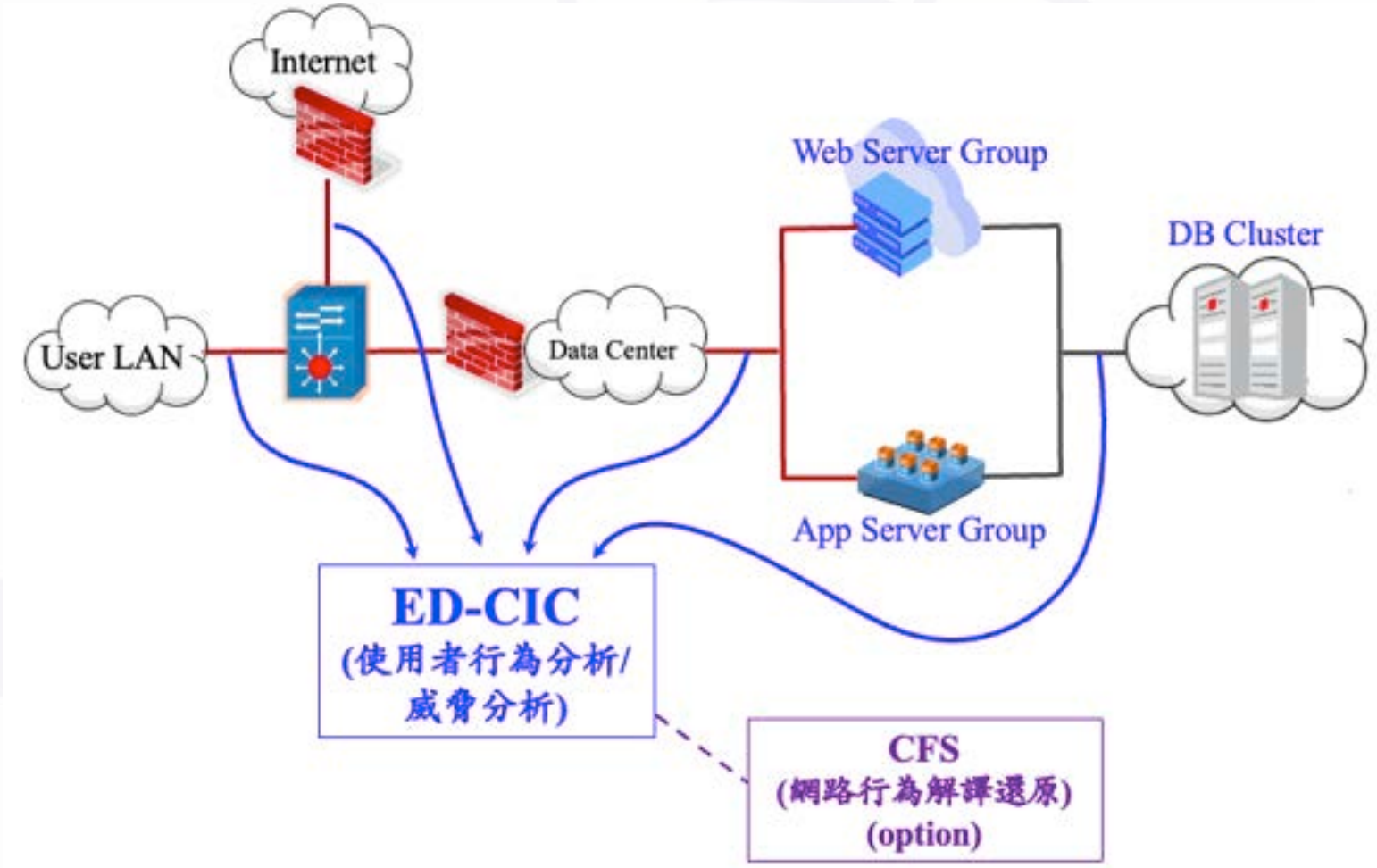
Data Retention Management System(DRMS)

ED-CIC
網路資訊集納系統

ED-CIC

- 為網路行為分析/威脅分析工具。
- 支援導入4Gbps鏡像流量，接收PCAP封包。
- 具備網路深層解析技術(DPI)，內建第七層封包處理功能，只需要將被監控流量導入，可關聯相關資料加以統計分析，提供包含網路行為、封包流向、用量統計等資訊。
- 具備IP/網段/群組之流量排名和分析、TOP N流量統計、攻擊行為統計(option)、攻擊類型統計(option)、嚴重等級統計(option)等視覺化統計圖表 。
- 支援外掛Storage，提供封包保存功能(option)之外，並可以1:1封包複製輸出至其他系統。
- 可將封包輸出至「網路封包鑑識系統CFS」，進行網路內容解譯還原。

ED-CIC

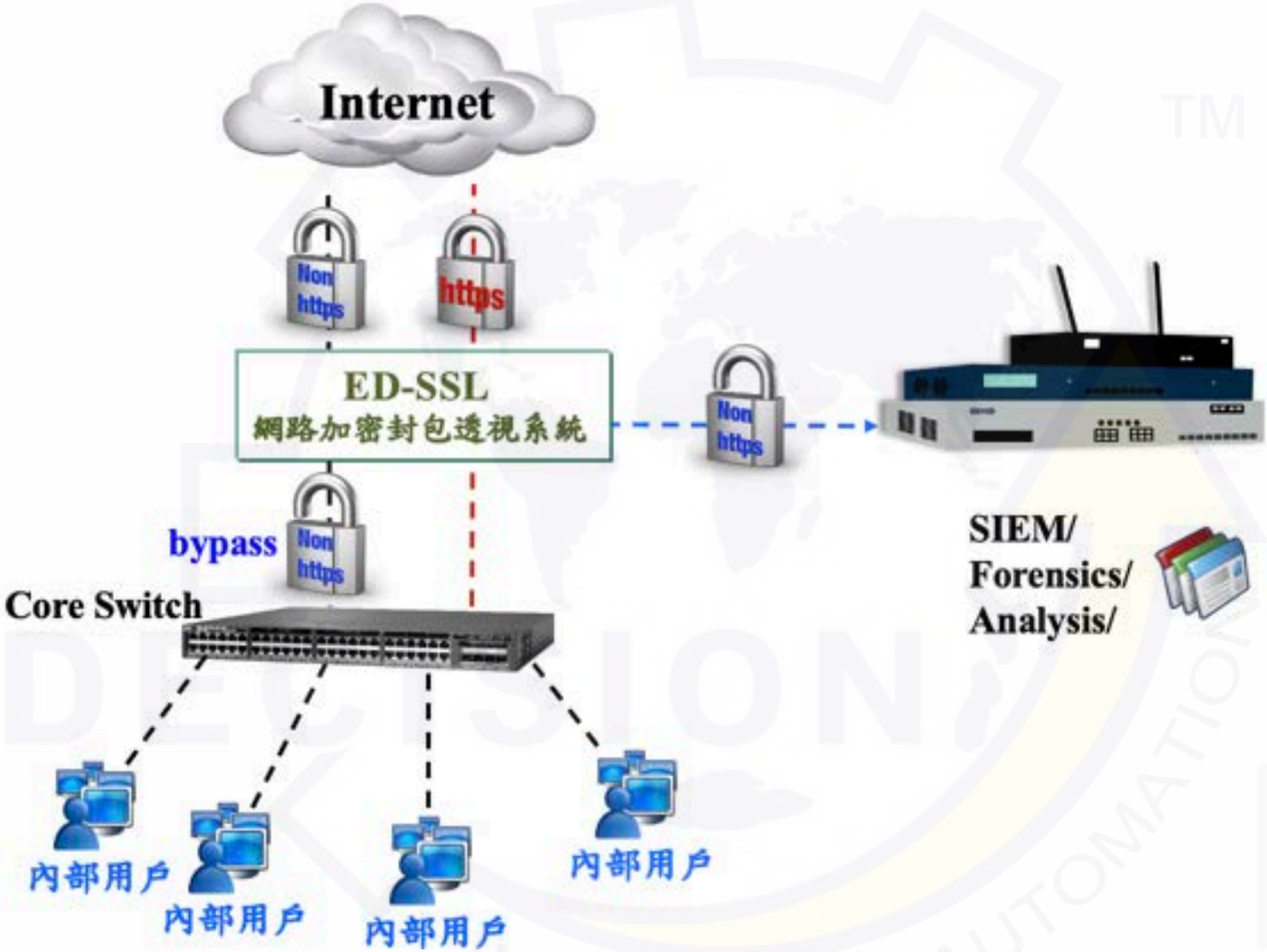

Internet
Web Server Group
DB Cluster
User LAN
Data Center
App Server Group
ED-CIC
(使用者行為分析/
威脅分析)
CFS
(網路行為解譯還原)
(option)

ED-SSL
網路加密封包透視系統

ED-SSL

- 為SSL加密流量監控及檢測專用系統。
- 單一系統作業，統一檢查加解密協議。
- 具備SSL流量可視性。
- 支援內部用戶端對外SSL連線檢測。
- 支援內部伺服器SSL連線檢測。
- 具備流量輸出功能，可將單一來源流量解密後，1：1封包複製給後端被動式資安設備。
- 可整合後端資安設備進行防禦，如防火牆、Anti-Malware、IPS、WAF...等(option)。
- 具備黑名單網站阻絕機制，可於系統建立黑名單，系統偵測到黑名單網站會立刻阻絕。
- 具備白名單排除檢測機制，可於系統建立白名單排除網站檢測。
- 支援SSL 3、TLS 1.0、TLS 1.1、TLS 1.2通訊協定。

ED-SSL


Internet
Non https
https
ED-SSL
網路加密封包透視系統
Non https
bypass
Non https
Core Switch
SIEM/
Forensics/
Analysis/
內部用戶
內部用戶
內部用戶
內部用戶

Forensics E-Detective (FED)
網路封包解譯鑑識系統

FED

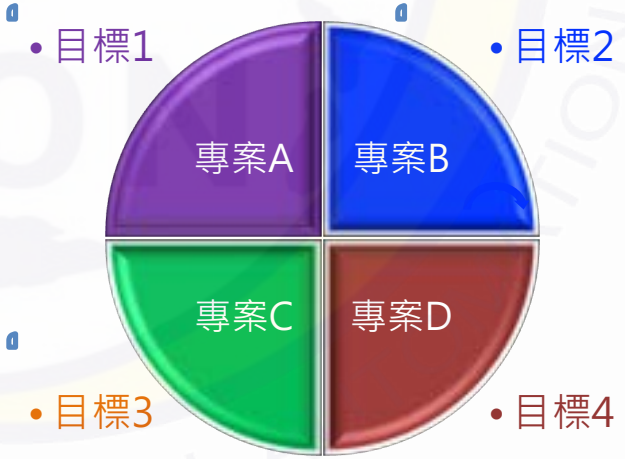
- 適用於專案型或任務型網路封包鑑識，可安裝於輕便型獨立主機，做為可攜式之網路封包鑑識工具，接收解譯還原online或offline網路封包。
- 具備「有線網路封包」、「有線網路之HTTPS / SSL加密網路連線封包(option)」及「離線網路封包」等網路封包擷取處理模式。
- Online模式下，可利用Sniffer Mode或是Man-in-the-middle(MITM)方式擷取封包。
- Offline模式下，可匯入原始封包檔進行網路封包解析。
- 在任務需求下，可保留原始封包檔並匯出。
- 可針對不同任務建立不同專案，專案各自獨立。不同目標的網路封包各自保留於獨立區域，避免資料互相混雜。
- 具備全文檢索及條件式搜尋。

FED

離線網路封包 ·

有線網路封包·

有線網路之·
HTTPS/SSL加密網路
連線封包(option)

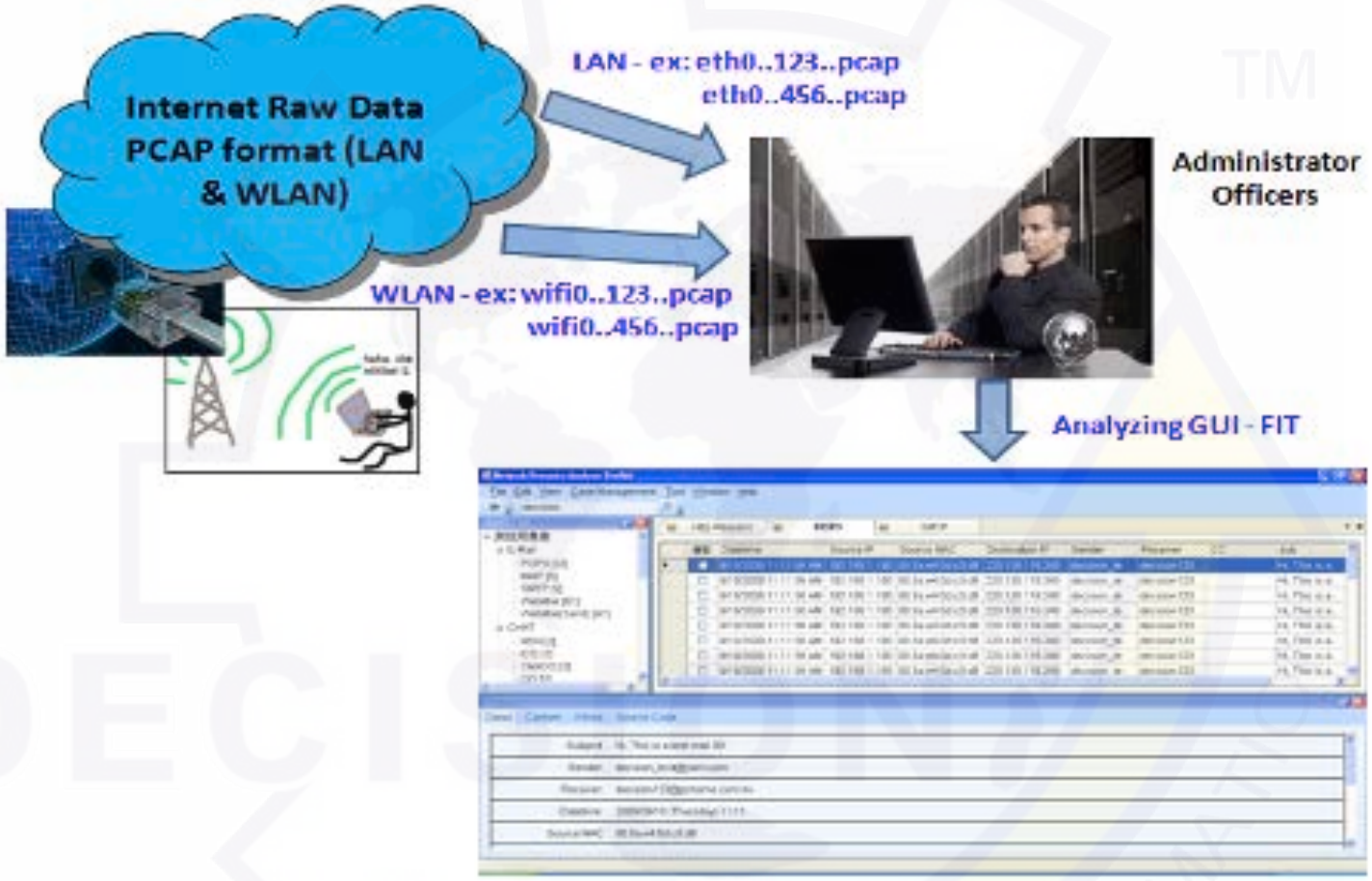


Forensics Investigation Toolkit (FIT)
離線式網路封包鑑識整合工具

FIT

- 支援微軟作業系統，可在Windows平台上執行。
- 提供「手動匯入」模式，可針對現有封包檔案以手動匯入方式進行解析。
- 以專案方式進行管理，用於區別不同用途或目的之專案。
- 以樹狀結構方式呈現物件清單，包含「通訊協定解析結果」及「封包連結數」等，可透過頁籤(Tab)切換檢視資料。
- 提供特定專案解析還原資料之各通訊協定數量。
- 提供連線清單及連線細節資訊。
- 提供以帳號或IP為主的關聯性分析。
- 針對HTTP上傳/下載、FTP及網路芳鄰等，具備圖片還原功能，可以圖片牆方式檢視，並可查閱各圖片之紀錄資訊。
- 可輸入關鍵字、帳號、IP位址，針對當前專案進行資料檢索。

FIT



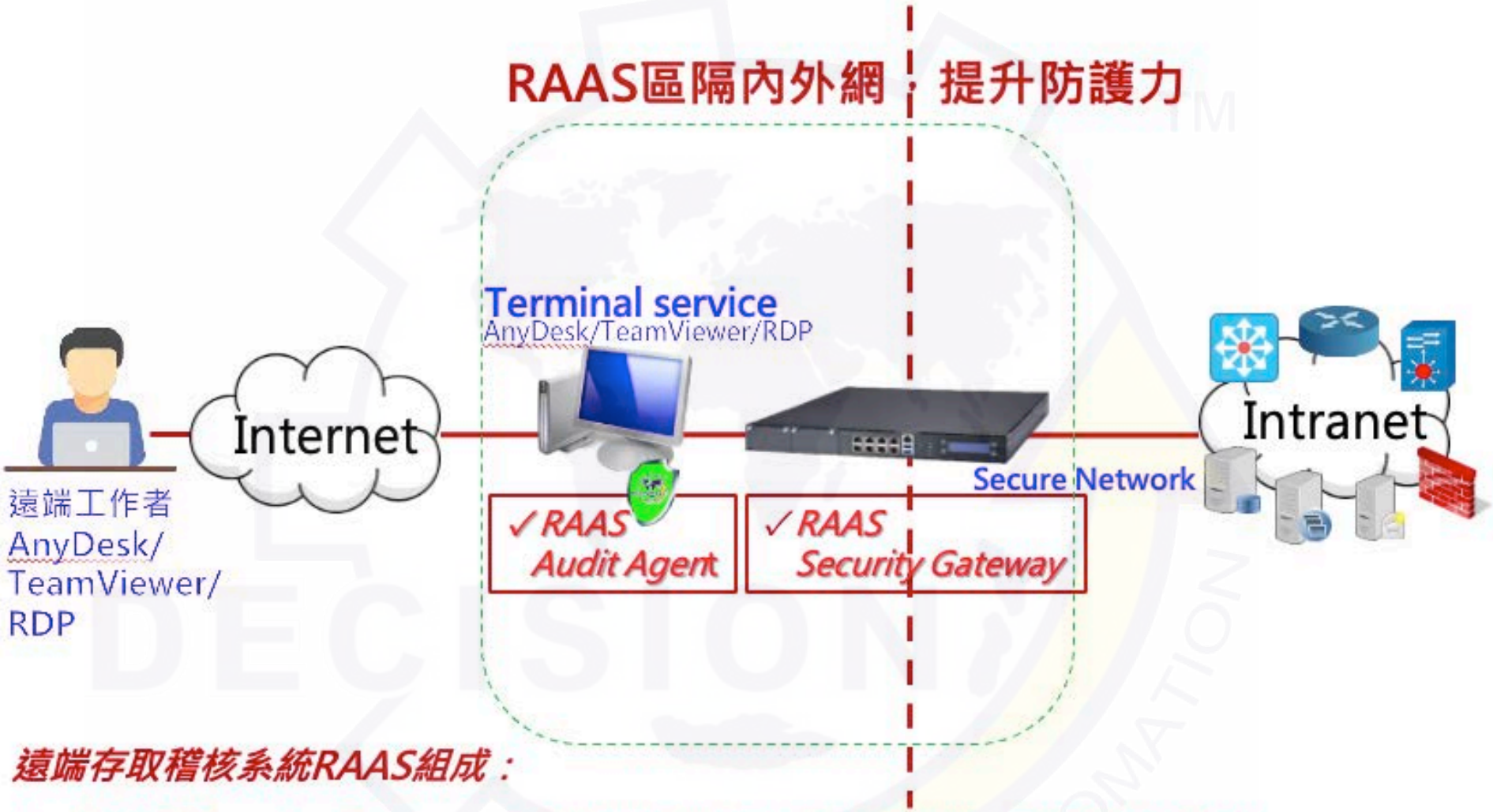
Forensics Investigation Toolkit (FIT)

Remote Access Audit System (RAAS)
遠端存取稽核系統

Remote Access Audit System(RAAS)

- 適用「資通安全管理法施行細則第4條」及「行政院資通安全處110/3/2函(請各機關加強遠端存取控制機制..)」
- 遠端維護、遠距辦公之遠端存取 授權/管理/監控/稽核。
- 遠端存取帳號/時間/設備管制。
- 遠端桌面連線操作錄影及封包側錄。
- 遠端桌面操作即時監看、遠端桌面連線即時阻斷。
- 遠端存取事件告警、遠端桌面連線使用軌跡紀錄保存。
- 支援AnyDesk/TeamViewer/RDP等中繼工作站。
- 區分網路為內部及外部，提高管理強度，降低使用風險。

Remote Access Audit System(RAAS)



遠端存取稽核系統RAAS組成：

- ✓ *RAAS Security Gateway--安裝在遠端桌面跟內部之間，可安裝在VM上*
- ✓ *RAAS Audit Agent--跟遠端桌面安裝在一起*

謝謝指教