

職能單元代碼	INM3R3518
職能單元名稱	建置安全網路環境
職類別	資訊科技 / 網路規劃與建置管理
職能單元級別	3
工作任務與行為指標	<p>一、 建置網路層安全 (包含虛擬化網路架構)</p> <ol style="list-style-type: none"> 1. 在網路資訊安全人員指導下，建置與測試網路路由通訊協定解決方案。 2. 建置與測試以 IPv4 或 IPv6 為基礎的網路再分布解決方案。 3. 使用路由器作業系統 (OS) 指令建置以減少第三層攻擊。 4. 在交換器上執行以身分為基礎之網路服務 (IBNS) 以提供第二層安全。 5. 利用存取控制系統 (ACS) 做為驗證伺服器執行身分管理。 6. 填寫網路安全防護建置紀錄。 <p>二、 建構入侵防禦系統</p> <ol style="list-style-type: none"> 1. 在網路資訊安全人員指導下，協助評估將路由器、IPS 及防火牆特性進階能力，納入網路資源之威脅事件行動處理 (EAP)。 2. 建置並確認 IPS 特性，以找出威脅並以動態方式阻止其進入網路。 3. 維持、更新與微調 IPS 簽署。 4. 建置與驗證以內容為基礎之存取控制 (CBAC) 以及網路位址轉譯 (NAT)，以動態減少找出的網路威脅。 5. 建置與驗證以區域為基礎之防火牆 (ZFW) 來納入新進應用程式檢查並通知資源定位器 (URL) 過濾，以達到網路安全的提升。 6. 在網路資訊安全人員指導下，協助評估網路功能平台 (NFP) 的特性與功能性，以提供基礎建設保護。 7. 利用路由器的功能來取得管理平面、資料平面與控制平面資訊。

	<p>三、 建置虛擬私有網路 (VPN)【註1】</p> <ol style="list-style-type: none"> 1. 在網路資訊安全人員指導下，協助分析與評估網際網路通訊協定安全性 (IPSec) 與通用路由協議封裝 (IPSec/GRE) 的特性與功能性。 2. 利用憑證授權單位，設定站台對站台VPN之安全連線。 3. 利用動態多點VPN (DMVPN) 的特性與功能性應用，建置與驗證網站對網站VPN作業之安全連線。 4. 以安全封包層協定 (SSL) VPN提供高度安全網路存取，以達到遠端存取連線的特性與效益。 5. 在網路資訊安全人員指導下，協助評估EasyVPN效益，並以動態虛擬通道介面 (DVTI) 建置EasyVPN伺服器，在虛擬通道介面上建立虛擬存取介面。 6. 建置與驗證EasyVPN遠端以便能以路由器及VPN軟體用戶端建立站對站連線。 7. 執行群組加密傳輸 (GET) VPN特性來簡化VPN的供應與管理。 8. 填寫VPN建置紀錄。
工作產出	<ul style="list-style-type: none"> • VPN建置紀錄 • 網路安全防護建置紀錄
職能內涵 (K=knowledge 知識)	<ul style="list-style-type: none"> • 安全性威脅與風險 • NAT 機制、概念與規劃 • 網路服務安全知識 • 防火牆與入侵防禦技術 • OSI 通訊網路架構應用 • 路由通訊協定 • 憑證建置與管理 • 安全防護機制 • 安全性通訊協定、標準與資料加密 • IOS與IP網路模組
職能內涵 (S=skills技能)	<ul style="list-style-type: none"> • 工作文件及記錄撰寫 • 問題解決能力 • 應變管理能力

	<ul style="list-style-type: none">• 規劃與組織能力• 網路安全實作能力• 資訊蒐集能力• 網路工具應用能力• 網路安全技術問題解決能力• 子網路計算能力• 溝通協調能力
說明與補充事項	<ul style="list-style-type: none">• 虛擬私有網路 (VPN): 提供站台對站台以及遠端存取通訊的安全連線。