

職能單元代碼	INM3R1500v2
職能單元名稱	為安全網路環境組態網路裝置
領域類別	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、執行第二層安全機制</p> <ol style="list-style-type: none"> 1. 使用路由器作業系統 (OS) 指令組態以減少第二層攻擊。 2. 在交換器上執行以身分為基礎的網路服務 (IBNS) 以提供第二層安全機制。 3. 利用存取控制系統 (ACS) 做為驗證伺服器執行身分管理。 <p>二、組態路由器 OS 入侵防禦系統 (OS-IPS) 以減輕網路資源威脅 <small>【註1】</small></p> <ol style="list-style-type: none"> 1. 評估路由器 OS-IPS 防火牆特性的進階能力，納入網路資源威脅事件的行動處理 (EAP)。 2. 組態並確認 IPS 特性以找出威脅，並以動態方式阻止威脅侵入網路。 3. 維持、更新與微調 IPS 攻擊特徵碼 (Signature)。 4. 組態與驗證以背景為基礎的存取控制 (CBAC) 與網路位址轉譯 (NAT)，以便動態減少找出的網路威脅。 5. 組態與驗證區域為基礎的防火牆 (ZFW)，以增加新進應用程式檢查並通知資源定位器 (URL) 過濾以提升網路安全。 <p>三、組態虛擬私有網路 (VPN) 建立站台對站台與遠端存取通訊的安全連線</p> <ol style="list-style-type: none"> 1. 分析並評估網際網路安全協定 (IPsec) 與通用路由協定封裝 (IPsec / GRE) 特性與功能。 2. 利用憑證授權單位設定站台對站台 VPN 的安全連線。 3. 分析動態多點 VPN (DMVPN) 特性與功能。 4. 組態與驗證網站對網站 VPN 作業的安全連線。 5. 運用安全通訊協定 (SSL) VPN 提供高度安全網

	<p>路存取以達遠端存取連線特性與效益【註2】。</p> <p>6. 評估 <u>EasyVPN 效益</u>【註3】，並以動態虛擬通道介面 (DVTI) 配置 EasyVPN 伺服器建立虛擬存取介面。</p> <p>7. 組態與驗證 EasyVPN 遠端，以透過路由器與 VPN 軟體用戶端建立站對站連線。</p> <p>8. 執行群組加密傳輸 (GET) VPN 特性以簡化 VPN 供應與管理。</p> <p>四、執行網路基礎保護 (NFP)</p> <ol style="list-style-type: none"> 1. 評估 NFP 特性與功能以提供基礎建設保護。 2. 利用路由器 OS 功能取得管理平面、資料平面與控制平面。
職能內涵 (K=knowledge 知識)	<p>一、IOS 與 IP 網路模組</p> <p>二、網路拓撲與架構及元件</p> <p>三、網路標準與協定</p> <p>四、區域網路 (LAN) 與廣域網路 (WAN) 運作</p> <p>五、威脅防護策略之相關網路安全防護知識</p> <p>六、架設與加強防火牆</p> <p>七、NAT 概念與規劃</p> <p>八、安全連線與遠端存取通訊</p> <p>九、安全性通訊協定如 SSL</p> <p>十、穿隧協定知識</p> <p>十一、VPN 技術方法</p> <p>十二、佈署方案之重點</p> <p>十三、路由器作業與問題類型</p>
職能內涵 (S=skills 技能)	<p>一、溝通協調能力</p> <p>二、分析現行網路資源威脅與解決策略</p> <p>三、規劃與設計組態網路裝置作業流程</p> <p>四、評估與選擇網路安全裝置</p> <p>五、執行與評量網路安全要求</p> <p>六、資訊科技應用能力</p>
評量設計參考	<p>一、評量證據</p> <ol style="list-style-type: none"> 1. 能評估網路安全系統要求。 2. 能減少網路安全威脅。

	<ol style="list-style-type: none">3. 能規劃 VPN 安全連線。4. 能評估與執行 NFP。5. 能利用第二層與第三層裝置，設計、執行與驗證網路安全系統。6. 能規劃、驗證與解決 VLAN 切換與切換間通訊。7. 能規劃、驗證與解決路由器作業與相關問題。8. 熟悉運用網路安全概念與技術。 <p>二、評量情境與資源</p> <ol style="list-style-type: none">1. 評量情境須儘量符合實務工作現場環境。2. 相關軟體與硬體設備。3. 相關規格書與作業文件。4. 評量流程與技巧須在文化方面要合宜，適合受評者的溝通技能等級、語言與讀寫算能力之工作。 <p>三、評量方法</p> <ol style="list-style-type: none">1. 宜採用多種評量方式來評量實務技能與知識。2. 以口頭或書面提問，評量受評者所需知識與技能。3. 運用目標提問方式評量所需知識。4. 觀察受評者安裝、配置與測試新或更新的網路。5. 評估受評者提供的工作文件紀錄。
說明與補充事項	<p>【註1】威脅：如阻斷服務 (DoS)、IP 詐騙、網址造假、媒體存取控制 (MAC) 詐騙、通訊埠掃描、監聽等。</p> <p>【註2】遠端存取連線特性與效益：如彈性與成本效益認可、桌面支援成本降低、成本與管理複雜度降低、威脅保護等。</p> <p>【註3】EasyVPN 效益：如佈署彈性、使用與維護簡單、可交互運作性提升、生產力增加等。</p>

更新紀錄

2021 年修訂職能內容。