《資通安全》

一、隨著 5G 時代的來臨，其所用的網路架構為軟體定義網路（Software Defined Networking, SDN），針對其網路架構及其可能遇到的威脅，請回答下列問題：

(一)請詳述軟體定義網路。（4 分）

(二)請畫圖並詳述 SDN 網路架構。（12 分）

(三)請詳述 SDN 網路各階層所面臨的威脅。（12 分）

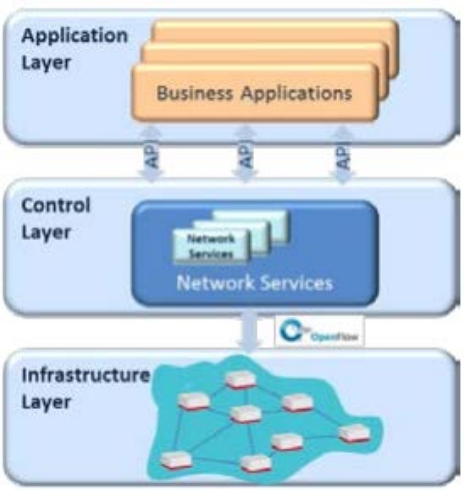
命題意旨	軟體定義網路的概念。
答題關鍵	此題在之前國考出現過數次，然而這次放在資安中主要是因應未來雲端趨勢，可以往虛擬化方向解答。

【擬答】

(一)軟體定義網路：軟體定義網路(SDN)是一個新型的網路架構，實作 SDN 概念最著名的是 OpenFlow 協定，將路由器控制平面自資料平面分離出來，使網路可直接由軟體實作控制，SDN 控制器擁有網路的狀態，故可集中管理整個網路，該架構可以不更動硬體裝置為前提，用軟體方式重新規畫，大幅降低了網路的維護與管理難度並增加彈性。

(二)圖片資料來源(Open Networking Foundation，OFN 基金會)

分為三層：應用層、控制層、基礎建設層(資料層)，傳統網路交換器同時具有控制層和資料層，但 SDN 是將這兩層分開，強化中央管理的部份，提供可程式化的軟體實作網路規劃。



(三)應用層：密碼破解、惡意應用程式；

解決方法：加入控制層對應用程式的存取控管機制。

北向 API：Dos、ARP spoofing attack

控制層：拓樸（Topology）惡意攻擊；

解決方法： 1.主機身分 PKI 驗證 2.驗證主機移動的正確性。

南向 API： Dos、ARP spoofing attack

資料層：可能遭受旁路攻擊、交通轉移；

解決辦法：1.建立靜態轉送規則 2. 關閉攻擊 API 連線的 port。

二、依據「國家資通安全發展方案（110 年至 113 年）」之「善用智慧前瞻科技、主動抵禦潛在威脅」推動策略，發展零信任架構資安防護環境，推動政府機關導入零信任架構，以完善政府網際服務網防禦深廣度。我國政府零信任架構係參考 NIST 零信任架構，同時結合向上集中之防護需求，採取資源門戶之部署方式。請列出並詳述此部署方式之三大核心機制。（24 分）

命題意旨	基於雲端化新型態的資安架構。
答題關鍵	國家資通安全研究院推廣的零信任系統架構與部署方式。
考點命中	《112 高點司法三等．調查局考場特刊》，資通安全第二題。

【擬答】

零信任是因應政府與企業的雲端導入各種 X 即服務型態，邊界定義逐漸模糊，是以個別的資源、使用者和資產本身為主體，而每位使用者在存取企業的每項資源之前，都必須個別通過認證，個別皆通過驗證後，才可以獲取一次性的存取權限。

三大核心機制(參考資料：行政院資通會)

1.身分鑑別：

多因子身分鑑別與身分鑑別聲明，例如：開通帳號與密碼，須使用憑證登入或是手機驗證，機敏機關須使用指紋或是人臉辨識登入。

2.設備鑑別：設備鑑別與設備健康管理。

(1)基於公開金鑰加密系統的信任平台模組(TPM)之設備鑑別。

(2)設備健康管理：持續更新設備狀態，並依設備健康狀態與壽命，換算健康等級。

3.信任推斷：隨時依使用者行為與設備狀態，偵測異常存取，有一套基於分數與情境之信任推斷機制，例如：錯誤次數過多，IP 位址來自境外，登入時間非上班時間或於敏感國際情勢時，可以導入「人工智慧」動態計算信任等級。

三、學者 Pipkin 指出資安事故指標為有可能、極有可能、明確等三種不同類別，用以檢查某個事件是否成為一個可能的事故或稱為嫌疑事故（Incident Candidate），請回答下列問題：（每小題 12 分，共 24 分）

（一）依據資訊安全原則，請列出至少三項並詳述如何確認發生真實資安事故。

（二）當真實資安事故發生時，資訊安全相關人員必須立刻啟動應對的事故回應計畫（Incident Response Plan）。請列出至少四項事故處理應該採取的行動並詳述之。

命題意旨	資安事故判定與回應計劃。
答題關鍵	本題重點在於資安事故法的法理，但是並非只有法理可以解決資安問題，可以根據各指標企業，如：中華電信、證卷交易所和大型金融機構發生過的案例切入即可。

【擬答】

(一)根據台北市政府資通安全事件通報與應變，發生於本府各機關之事件，系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅者。因此若發生一件資安事件，可以根據 C.I.A 三原則進行審查：

1.機密性：是否有機密資料、個資或是國安資料外流於公眾。

2.完整性：是否有資料遭到竄改或是存取權限異常，未按照既定政策執行。

3.可用性：系統是否能繼續運作，若不能繼續運作影響的系統功能範圍與公共生活多寡。

(二)根據國家資通安全通報應變作業

1.即時阻斷：應就資安事件發生原因、影響等級、可能影響範圍、 可能損失、是否需要支援等項目逐一盤查，保留被入侵或破壞相關證據，並「即時採取適當措施」，避免災情擴大。

2.找出攻擊手法：查詢國家資通安全通報應變網站、系統弱點(病毒)資料庫或聯絡技術支援單位(或廠商)等方式，尋求解決方案。如無法解決，應迅速向主管機關或國家資通安全會報反應，請求提供相關技術支援。

3.降低損害：依訂定之緊急應變計畫，實施緊急應變處置，並持續監控與追蹤管制。

4.進行復原：視資安事件損壞程度啟動備援計畫、異地備援或備援中心等應變措施，盡速恢復日常運作，提供正常服務。

5.盤點事件影響範圍：評估資安事件對業務運作造成之衝擊，並進行損害管制。
6.事後法律行動：資安事件如涉及刑責，應做好相關證據保全工作，如：日誌、連線紀錄和存取權限，以聯繫檢警調單位協助偵查。

四、為防範各種不同的網路弱點及達到資安通報的機制，請回答下列問題：（每小題 12 分，共 24 分）
（一）請詳述 CVE（Common Vulnerabilities and Exposures）、NVD（National Vulnerability Database）及 CPE（Common Platform Enumeration）之意義為何？並說明 CVE、NVD 及 CPE 彼此之間的運作情形。
（二）請詳述資通安全弱點通報機制（Vulnerability Alert and Notification System）及其運作方法。

命題意旨	弱點通報編碼與通報機制。
答題關鍵	此題是以往 OWSAP 的變形考題，OWSAP 是將 CVE 通報，以 CVSS(弱點通用評價)整理分組，而此題則是考 CVE 漏洞命名與如何查詢，考點仍大同小異。

【擬答】
(一)
1.CVE：是一個與資訊安全有關的資料庫，描述各種資安弱點，以標準編號作為識別。
格式為: CVE-YYYY-NNNN，YYYY 為年份，NNNN 為流水號。
2.CPE：用於識別軟體、硬體、作業系統等資訊資產的弱點標準化方式，主要分廠商、產品、版本、更新等等。
格式：cpe:2.3:a:microsoft:internet_explorer:10.0.1:edu:*:*:*:*:*:*
3.NVD：美國國家弱點資料庫，將收錄 CVE 弱點資料庫，可載入 CPE 字典，可以找到相關產品的 CVE 漏洞。
(二)(參考：國家資通安全研究院)
資通安全弱點通報機制：結合資訊資產與弱點管理，掌握風險並協助機關落實資通安全管理法之資產盤點與風險評估。
運作方法：
1.確認資訊資產弱點：蒐集使用之軟硬體資訊，將所使用之資訊資產設備與美國國家弱點資料庫進行比對，當使用資訊設備存在重大弱點時，應得應變處理。
2.降低重大弱點管控與追蹤之成本：利用自動化比對方式進行盤點目前機關資訊設備資產存在弱點使用情形，提供機關相關弱點資訊與自我檢查機制。
3.追蹤資訊資產弱點修補情形：依照各分級機關訂定之風險值門檻，進行弱點評估與修補作業。
4.強化安全性更新落實情形：搭配更新已安裝安全性清單，以協助確認資產之安全性更新已完成與缺漏項目，更精準呈現弱點修補情形。