D4-002 結果 12/6/2022

問題一

tb787631.CISSPPT3E.c04.020

Melissa 希望以一種對用戶透明的方式組合她組織中的多個物理網絡，但允許根據網絡服務的需要分配資源。她應該部署什麼類型的網絡？

A、iSCSI

B. 虛擬網絡

C.SDWAN

D、CDN

你回答正確！

虛擬網絡可用於合併現有網絡或將網絡劃分為多個網段。Melissa 可以使用虛擬網絡結合現有網絡，然後使用軟件定義的網絡功能來分配和管理網絡資源。iSCSI 是一種聚合存儲協議。SD-WAN 是一個軟件定義的廣域網，這個問題沒有指定 LAN 或 WAN 技術。CDN 是一種內容分發網絡，有助於應對負載和拒絕服務攻擊。

問題 2

tb787631.CISSPPT3E.c04.019

蘇珊希望通過多個 Internet 服務提供商保護她的通信流量，因為它被發送到她公司的第二個位置。她應該使用什麼技術來保護站點之間始終在線、始終連接的鏈路的流量？

A、FCoE

B.SDWAN

C. 點對點 IPsec VPN

D. Zigbee

你回答正確！

點對點 IPsec VPN 可以提供在兩個站點之間持續建立的安全加密通道，確保 Susan 的流量不會沿其傳輸路徑暴露。FCoE 是 Fibre Channel over Ethernet，一種存儲協議。SD-WAN 是軟件定義廣域網，Zigbee 是低功耗無線協議。這些都不能解決 Susan 的需求。

問題三

tb787631.CISSPPT3E.c04.092

SDN 實施的哪一層使用程序通過 API 傳達對資源的需求？

A. 數據平面

B. 控制平面

C. 應用平面

D. 監控平面

您回答錯誤。

軟件定義網絡 (SDN) 的應用程序平面是應用程序運行的地方，這些應用程序使用應用程序編程接口 (API) 與 SDN 就所需資源進行通信。控制平面接收指令並將它們發送到網絡。最後一個公共平面是設備本身。

問題四

tb787631.CISSPPT3E.c04.035

作為一名信息安全專家，Susan 被要求確定可以訪問其組織的無線網絡的區域，即使它不是預期的。蘇珊應該怎麼做才能確定她所在組織的無線網絡在哪裡可以訪問？

A. 現場調查
B. 戰爭行走
C. 戰車駕駛
D. 設計圖

您回答錯誤。

Wardriving 和 warwalking 都是用於定位無線網絡的過程，但通常不像站點調查那樣詳細和徹底，設計圖是一個虛構的術語。

問題 5

tb787631.CISSPPT3E.c04.064

請參考以下場景：

- 蘇珊正在為她的組織的分支機構設計新的網絡基礎設施。

設置好無線網絡後，Susan 開始著手確保她的網絡即使在發生中斷時也能保持運行。如果發生斷電或其他臨時電源問題，她可以確保她的網絡設備（包括她的路由器、接入點和網絡交換機）繼續運行的最簡單方法是什麼？

A. 購買並安裝一台自動啟動的發電機。

B. 為所有網絡設備部署雙電源。

C. 安裝 UPS 系統以覆蓋所有必須保持在線的網絡設備。

D. 與多個不同的電力公司簽訂冗餘電力合同。

你回答正確！

UPS 系統或不間斷電源設計用於在短暫的電力中斷期間提供備用電源，範圍從電源驟降和電力不足到臨時電源故障。對於更長時間的停電，Susan 仍然需要發電機，如果可能的話，甚至需要來自其他電網或供應商的二次供電，但對於這種特定情況，UPS 將滿足她的需求。當擔心從

一個電源斷電時，雙電源會有所幫助，這對她最關鍵的網絡設備來說是個

好主意，但很少有為接入點或邊緣交換機等邊緣設備配備雙電源。

問題 6

tb787631.CISSPPT3E.c04.077

當以太網上的主機檢測到衝突並發送阻塞信號時，接下來會發生什麼？

A. 允許發送阻塞信號的主機重新發送，而所有其他主機暫停，直到成功接收到該傳輸。

B. 所有主機停止傳輸，每台主機在嘗試再次傳輸之前等待一段隨機時間。

C. 所有主機停止傳輸，每台主機根據最近成功傳輸的時間等待一段時間。

D. 主機等待傳遞令牌，然後在傳遞令牌時恢復傳輸數據。

您回答錯誤。

以太網網絡使用帶衝突檢測 (CSMA/CD) 技術的載波偵聽多路訪問。當

檢測到衝突並發送阻塞信號時，主機在嘗試重傳之前等待一段隨機時間。

問題 7

tb787631.CISSPPT3E.c04.051

哪個 OSI 層包括電氣規範、協議和接口標準？

A. 傳輸層

B. 設備層

C.物理層

D. 數據鏈路層

你回答正確！

物理層包括允許控制吞吐量、處理線路噪聲以及各種其他電氣接口和信號要求的電氣規範、協議和標準。OSI 層沒有設備層。傳輸層連接網絡層和會話層，數據鏈路層將來自網絡層的數據包打包，供運行在物理層上的設備傳輸和接收。

問題 8

tb787631.CISSPPT3E.c04.017

Ben 已將他的網絡配置為不廣播 SSID。為什麼 Ben 會禁用 SSID 廣播，他的 SSID 是如何被發現的？

A. 禁用 SSID 廣播可防止攻擊者發現加密密鑰。SSID 可以從解密的數據包中恢復。

B. 禁用 SSID 廣播對未經授權的人員隱藏網絡。可以使用無線嗅探器發現 SSID。

C. 禁用 SSID 廣播可防止信標幀出現問題。SSID 可以通過重構 BSSID 來恢復。

D. 禁用 SSID 廣播有助於避免 SSID 衝突。可以通過嘗試連接到網絡來發現 SSID。

你回答正確！

禁用 SSID 廣播有助於防止未經授權的人員嘗試連接到網絡。由於 SSID 仍處於活動狀態，因此可以使用無線嗅探器發現它。加密密鑰與 SSID 廣播無關，信標幀用於廣播 SSID，並且可能有多個網絡具有相同的 SSID。

問題 9

tb787631.CISSPPT3E.c04.057

Ben 正在對網絡進行故障排除，發現他所連接的 NAT 路由器的內部網絡為 192.168.xx 子網，其外部 IP 為 192.168.1.40。他遇到了什麼問題？

A. 192.168.xx 是不可路由的網絡，不會傳送到 Internet。
B. 192.168.1.40 不是有效地址，因為它已被 RFC 1918 保留。
C. 使用相同的 IP 範圍不可能進行雙重 NATing。
D. 上游系統無法解封裝他的數據包，他需要改用 PAT。

你回答正確！

對於相同的 IP 範圍，雙重 NAT 是不可能的；NAT 路由器內外不能出現相同的 IP 地址。RFC 1918 地址是保留的，但只是為了不在 Internet 上使用和路由它們，更改為 PAT 不會解決問題。

問題 10

tb787631.CISSPPT3E.c04.026

地址解析協議 (ARP) 和反向地址解析協議 (RARP) 在 OSI 模型的哪一層運行？

A. 第一層

B、第 2 層

C、第 3 層

D. 第 4 層

你回答正確！

ARP 和 RARP 在 OSI 模型的第二層數據鏈路層運行。兩種協議都處理物理硬件地址，這些地址在物理層（第 1 層）之上和網絡層（第 3 層）之下使用，因此屬於數據鏈路層。

問題 11

tb787631.CISSPPT3E.c04.002

在對無線網絡進行安全評估期間，Jim 發現 LEAP 正在使用 WPA 的網絡上使用。吉姆應該提出什麼建議？

A. 繼續使用 LEAP。它為 WPA 網絡提供比 TKIP 更好的安全性。

B. 使用替代協議，如 PEAP 或 EAP-TLS，並在支持的情況下實施 WPA2。

C. 繼續使用 LEAP 來避免身份驗證問題，但轉向 WPA2。

D. 使用替代協議，如 PEAP 或 EAP-TLS，並實施有線等效保密以避免無線安全問題。

你回答正確！

LEAP，即輕量級可擴展身份驗證協議，是一種 Cisco 專有協議，旨在處

理 TKIP 問題。不幸的是，LEAP 也有嚴重的安全問題，不應使用。任何

現代硬件都應支持 WPA2 和 PEAP 或 EAP-TLS 等技術。使用

WEP（WPA 和 WPA2 的前身）將是任何網絡安全性的重大倒退。

問題 12

tb787631.CISSPPT3E.c04.018

在通過接受客戶端請求、更改請求的源地址、將請求映射到客戶端並將修改後的請求發送到它們的目的地來提供 Internet 訪問時，可以使用什麼網絡工具來保護客戶端的身份？

A、開關

B、代理

C、路由器

D、防火牆

你回答正確！

代理是一種網關形式，可為客戶端提供過濾、緩存或其他服務，以保護其

信息免受遠程系統的影響。路由器連接網絡，而防火牆使用規則來限制允

許通過它的流量。交換機用於連接系統，不提供這些功能。

問題 13

tb787631.CISSPPT3E.c04.065

Susan 想為新分支機構所在設施中的設備提供 10 Gb 網絡連接。她有哪些連接選項可以滿足這些速度的結構化佈線？（選擇所有符合條件的。）

A、Cat5e

B、纖維

C.Cat6

D、同軸電纜

你回答正確！

光纖電纜和 Cat6 電纜都可以以 10 Gb 的速度運行。Cat5e 和同軸電纜

不符合這些速度。

問題 14

tb787631.CISSPPT3E.c04.098

Chris 正在建立一個酒店網絡，需要確保每個房間或套房內的系統可以相互連接，但其他套房或房間內的系統不能。同時，他需要保證酒店所有系統都能上網。他應該推薦什麼解決方案作為最有效的業務解決方案？

A. 每個房間的 VPN
B. VLAN
C. 港口安全
D. 防火牆

你回答正確！

VLAN 可用於在邏輯上分隔網絡端口組，同時仍提供對上行鏈路的訪問。

每個房間的 VPN 會產生大量的支持開銷以及額外的費用。端口安全用於限制哪些系統可以連接到端口，但它不提供系統之間的網絡安全。最後，雖然防火牆可能有效，但它們會增加費用和復雜性，而不會比 VLAN 解決方案增加任何好處。

問題 15

tb787631.CISSPPT3E.c04.034

克里斯在旅行時使用蜂窩熱點提供互聯網訪問。如果他在他的 PC 在其組織的企業網絡上時讓熱點連接到他的 PC，他可能會導致什麼安全問題？

A. 流量可能無法正確路由，從而暴露敏感數據。

B. 他的系統可以充當從互聯網到本地網絡的橋樑。

C. 他的系統可能是反射型 DDoS 攻擊的入口。

D. 如果出現安全問題，安全管理員可能無法確定他的 IP 地址。

您回答錯誤。

當工作站或其他設備同時連接到安全網絡和非安全網絡（如 Internet）時，

它可能充當橋樑，繞過位於公司網絡邊緣的安全保護。流量路由不當導致

敏感數據暴露的可能性不大，因為流向內部系統和網絡的流量不太可能路

由到外部網絡。反射 DDoS 攻擊用於隱藏身份而不是連接到內部網絡，

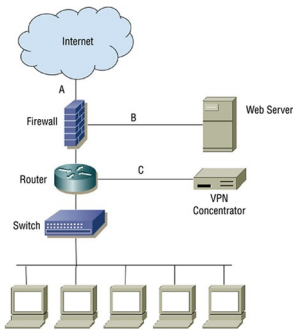
託管系統的安全管理員應該能夠確定他的系統使用的本地和無線 IP 地址。

問題 16

tb787631.CISSPPT3E.c04.013

請參考以下場景和圖表：

- Chris 正在為他的組織設計分層網絡安全。



圖中顯示了哪種類型的防火牆設計？

A. 單層防火牆

B. 兩層防火牆

C. 三層防火牆

D. 四層防火牆

您回答錯誤。

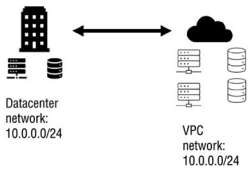
圖中的防火牆後面有兩個保護區，使其成為雙層防火牆設計。

問題 17

tb787631.CISSPPT3E.c04.074

請參考以下場景：

- Ben 是一家組織的信息安全專家，該組織正在用雲託管的虛擬機替換其物理服務器。隨著組織構建其虛擬環境，它正在轉向混合雲運營模式，其中一些系統和服務保留在其本地數據中心，而其他系統和服務則託管在雲中。下圖顯示了本地數據中心和雲 VPC 的網絡 IP 範圍，您在回答問題時應考慮這些範圍。



數據中心和專有網絡配置的子網最容易出現什麼問題？

A. IP 地址衝突

B. 路由循環

C.MAC 地址衝突

D、以上所有

你回答正確！

在設計扁平網絡時，為現場和雲託管數據中心使用相同的 IP 範圍可能會

有所幫助，但即使在 10.0.0.0/24 範圍這樣大的空間中，也必須仔細管理

和分配地址。如果地址管理不當，可能會出現衝突，從而中斷生產服務。

除非手動更改地址或在不更改其 MAC 地址的情況下複製虛擬機，否則

不應出現 MAC 地址衝突。問題中沒有任何建議路由問題。

問題 18

tb787631.CISSPPT3E.c04.023

本為一家小型連鎖咖啡店提供網絡和安全服務。這家咖啡連鎖店希望為顧客提供安全、免費的無線網絡。如果 Ben 不需要擔心協議支持問題，以下哪項是 Ben 允許客戶安全連接到他的無線網絡而無需用戶帳戶的最佳選擇？

A. 在 PSK 模式下使用 WPA2。
B. 在 SAE 模式下使用 WPA3。
C. 在企業模式下使用 WPA2。
D. 使用強制門戶。

您回答錯誤。

WPA3 的新 SAE（對等同步身份驗證）模式改進了 WPA2 的 PSK 模式，

允許在沒有企業用戶帳戶的情況下在客戶端和無線網絡之間進行安全身份

驗證。如果 Ben 需要擔心對 WPA3 的支持，而 WPA3 可能不適用於所

有可能想要連接的系統，他可能不得不選擇 WPA2。強制門戶通常與開

放訪客網絡一起使用，企業模式需要用戶帳戶。

問題 19

tb787631.CISSPPT3E.c04.033

以下哪項不是聚合協議的示例？

A.MIME

B、FCoE

C、iSCSI

D、網絡電話

你回答正確！

以太網光纖通道 (FCoE)、互聯網小型計算機系統接口 (iSCSI) 和互聯網

協議語音 (VoIP) 都是融合協議的示例，它們將專用協議與標準協議（如

TCP/IP）相結合。MIME，多用途 Internet 郵件擴展，不是一個聚合協議。

問題 20

tb787631.CISSPPT3E.c04.022

在安全評估期間，Jim 發現與他合作的組織使用多層協議來處理 SCADA 系統，並且最近將 SCADA 網絡連接到組織生產網絡的其餘部分。對於通過 TCP/IP 進行的串行數據傳輸，他應該關心什麼？

A. 現在連接到網絡的 SCADA 設備現在可以通過網絡受到攻擊。

B. TCP/IP 上的串口數據無法加密。

C、串口數據不能在 TCP 包中攜帶。

D. TCP/IP 的吞吐量允許對串行設備進行簡單的拒絕服務攻擊。

您回答錯誤。

DNP3 等多層協議允許 SCADA 和其他系統使用基於 TCP/IP 的網絡進行通信。許多 SCADA 設備從未設計為暴露在網絡中，將它們添加到可能不安全的網絡中會產生重大風險。可以在 TCP 數據包上使用 TLS 或其他加密，這意味著甚至可以保護串行數據。串行數據可以通過 TCP 數據

包進行傳輸，因為 TCP 數據包不關心它們的內容；它只是另一個有效載

荷。最後，TCP/IP 沒有設計的特定吞吐量，因此吞吐量問題是設備級問

題。

問題 21

tb787631.CISSPPT3E.c04.043

Ben 部署了一個 1000BaseT 千兆位網絡，需要在一棟大型建築物中鋪設電纜。如果 Ben 直接從該建築物中的一個交換機運行他的鏈路到另一個交換機，根據 1000BaseT 規範，Ben 可以覆蓋的最大距離是多少？

A、2 公里

B、500 米

C. 185 米

D、100 米

你回答正確！

1000BaseT 能夠根據其規格運行 100 米。對於更長的距離和外部運行，

現代網絡中通常使用光纖電纜。

問題 22

tb787631.CISSPPT3E.c04.084

Steve 的任務是在 IP 網絡上實施網絡存儲協議。他可能會在其實施中使用哪種以存儲為中心的融合協議？

A、MPLS

B、FCoE

C、SDN

D、網絡電話

你回答正確！

以太網光纖通道允許通過以太網網絡進行光纖通道通信，允許使用現有的高速網絡來傳輸存儲流量。這避免了為光纖通道實施定制電纜設備的成本。

MPLS，即多協議標籤交換，用於高性能網絡；VoIP 是 IP 語音；SDN 是軟件定義網絡。

問題 23

tb787631.CISSPPT3E.c04.086

以下哪項以正確的順序顯示了 OSI 模型的層，從第 1 層到第 7 層？按照適當的順序放置此處顯示的 OSI 模型的層，從第 1 層到第 7 層。

A. 第 1 層 = 數據鏈路；第 2 層 = 物理層；第 3 層 = 網絡；第 4 層 = 傳輸；第 5 層 = 會話；第 6 層 = 演示；第 7 層 = 應用程序

B. 第 1 層 = 物理層；第 2 層 = 數據鏈路；第 3 層 = 網絡；第 4 層 = 傳輸；第 5 層 = 會話；第 6 層 = 演示；第 7 層 = 應用程序

C. 第 1 層 = 物理層；第 2 層 = 數據鏈路；第 3 層 = 網絡；第 4 層 = 傳輸；第 5 層 = 會話；第 6 層 = 應用程序；第 7 層 = 演示

D. 第 1 層 = 物理；第 2 層 = 數據鏈路；第 3 層 = 網絡；第 4 層 = 會話；第 5 層 = 傳輸；第 6 層 = 演示；第 7 層 = 應用程序

你回答正確！

OSI 層從第 1 層到第 7 層的順序如下：

1.身體的

2.數據鏈接

3.網絡

4.運輸

5.會議

6.推介會

7.應用

問題 24

tb787631.CISSPPT3E.c04.041

作為滲透測試練習的一部分，Melissa 使用 ping 實用程序檢查遠程系統是否正常運行。如果她不想看到自己的 ping 數據包，她應該從數據包嗅探器的日誌中過濾掉什麼協議？

A、UDP

B、TCP

C、知識產權

D、ICMP

你回答正確！

Ping 使用 ICMP（Internet 控制消息協議）來確定係統是否響應以及原始系統和遠程系統之間有多少躍點。Melissa 只需要過濾掉 ICMP 就不會看到她的 ping。

問題 25

tb787631.CISSPPT3E.c04.070

在故障排除過程中，與 Alyssa 交談的支持技術人員表示該問題是第 3 層問題。以下哪個可能的問題不是第 3 層問題？

A. TTL 不匹配

B. MTU 不匹配

C. 不正確的 ACL

D. 斷網線

你回答正確！

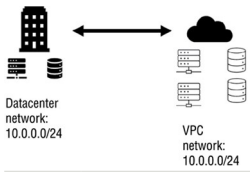
網絡電纜損壞是第 1 層問題。如果您遇到這樣的問題並且不確定，請尋找具有不同情況或一組假設的答案。在這裡，您有三個問題發生在網絡（第 3 層）上，所有這些問題都具有軟件或協議含義。網絡電纜損壞是完全不同類型的問題，應該突出顯示。不過要小心！考試可能會給你兩個可能有效的答案供你選擇，所以努力擺脫兩個最不可能的答案，把時間花在剩下的選項上。

問題 26

tb787631.CISSPPT3E.c04.073

請參考以下場景：

- Ben 是一家組織的信息安全專家，該組織正在用雲託管的虛擬機替換其物理服務器。隨著組織構建其虛擬環境，它正在轉向混合雲運營模式，其中一些系統和服務保留在其本地數據中心，而其他系統和服務則託管在雲中。下圖顯示了本地數據中心和雲 VPC 的網絡 IP 範圍，您在回答問題時應考慮這些範圍。



Ben 希望確保他的雲託管基礎架構即服務環境中的實例到實例（系統到系統）流量是安全的。他可以做些什麼來完全確保虛擬化網絡流量不被捕獲和分析？

A. 防止在所有主機上安裝數據包嗅探器。

B. 禁用所有虛擬網絡接口的混雜模式。

C. 禁止使用任何虛擬水龍頭。

D. 加密主機之間的所有流量。

您回答錯誤。

在基礎架構即服務（IaaS）環境中，提供雲環境的公司擁有所有虛擬機和網絡的最終控制權。因此，要保護數據，最好的選擇是對數據進行加密。

不幸的是，Ben 無法完全確保他的環境中的流量不會被捕獲，並且必須依賴雲託管提供商來確保這一點。雖然防止安裝數據包嗅探器和竊聽器並確保不能啟用混雜模式在您控制的環境中是有用的習慣，但這不會在雲環境中提供相同的控制。

問題 27

tb787631.CISSPPT3E.c04.095

5e 類電纜的額定最大速度是多少？

A. 5 Mbps

B. 10 Mbps

C. 100 Mbps

D. 1000 Mbps

你回答正確！

Category 5e cable is rated for speeds up to 1000 Mbps. If you need a faster network connection, you can consider Cat6 or higher copper cables or move to fiber where speeds can be much higher.

Question 28

tb787631.CISSPPT3E.c04.048

Cameron is worried about distributed denial-of-service attacks against his company's primary web application. Which of the following options will provide the most resilience against large-scale DDoS attacks?

A. A CDN

B. Increasing the number of servers in the web application server cluster

C. Contract for DDoS mitigation services via the company's ISP

D. Increasing the amount of bandwidth available from one or more ISPs

You Answered Incorrectly.

與任何其他解決方案相比，由主要提供商運營的內容分發網絡或 CDN

可以更輕鬆地處理大規模 DDoS 攻擊。通過 ISP 使用 DDoS 緩解技術是

下一個最有用的功能，其次是帶寬的增加和 Web 應用程序集群中服務器

數量的增加。

問題 29

tb787631.CISSPPT3E.c04.049

有四種常見的 VPN 協議。列出的哪個組包含所有常見的 VPN 協議？

A. PPTP、LTP、L2TP、IPsec
B. PPP、L2TP、IPsec、VNC
C. PPTP、L2F、L2TP、IPsec
D. PPTP、L2TP、IPsec、SPAP

您回答錯誤。

PPTP、L2F、L2TP 和 IPsec 是最常見的 VPN 協議。TLS 也用於越來

越多的 VPN 連接，並且可能會出現在 CISSP 考試的某個時刻。PPP 是

撥號協議，LTP 不是協議，SPAP 是有時與 PPTP 一起使用的 Shiva 密

碼驗證協議。

問題 30

tb787631.CISSPPT3E.c04.078

馬克擔心他的網絡電纜的物理安全性。如果沒有專用設備，哪種類型的網絡連接最難竊聽？

A. 無線網絡

B、藍牙

C、Cat5/Cat6 雙絞線

D、光纖

您回答錯誤。

光纜是所列網絡類型中最難在沒有專用設備的情況下捕獲數據的類型。如

果可以訪問光纖電纜和專用設備對其進行竊聽，或者可以訪問光纖電纜的

端點和光學分路器，仍然可以獲得訪問權限。在任何一種情況下，當電纜

被切斷、拼接或斷開連接時都可能會出現中斷，並且許多攻擊者將無法訪

問、沒有技能或需要這樣做的工具。可以使用標準無線網卡和工具捕獲

WiFi 和藍牙流量，使用商用工具可以輕鬆捕獲雙絞線以太網電纜傳輸的

數據。

問題 31

tb787631.CISSPPT3E.c04.025

802.11n 使用什麼速度和頻率範圍？

A. 僅 5 GHz

B. 900 MHz 和 2.4 GHz

C. 2.4 GHz 和 5 GHz

D. 僅 2.4 GHz

你回答正確！

802.11n 可以在 2.4 和 5 GHz 頻率範圍內運行。900 MHz 範圍經常用於

電話和非 WiFi 無線網絡以及其他業餘無線電用途。知道有多個範圍可用 ，

並且它們可能會根據正在使用的接入點數量以及可能對該頻段造成乾擾的

其他設備是否在該區域中而表現不同，這對於無線網絡部署可能很重要。

第 32 題

tb787631.CISSPPT3E.c04.068

Selah 的網絡團隊被要求確定一種技術，使他們能夠通過像對待代碼一樣對待網絡來動態改變組織的網絡。她應該推薦哪種類型的架構？

A. 遵循 5-4-3 規則的網絡

B. 融合網絡

C. 軟件定義網絡

D. 基於管理程序的網絡

你回答正確！

軟件定義網絡提供了一種可以定義和配置為代碼或軟件的網絡架構。這將使 Selah 的團隊能夠根據組織要求快速更改網絡。5-4-3 規則是用於依賴中繼器或集線器的網絡的舊設計規則。融合網絡承載多種類型的流量，如語音、視頻和數據。基於管理程序的網絡可能是軟件定義的，但它也可以使用作為虛擬機運行的傳統網絡設備。

問題 33

tb787631.CISSPPT3E.c04.001

Gary 想要分發一個大文件並且更喜歡點對點 CDN。以下哪項是此類技術最常見的示例？

A. CloudFlare

B. BitTorrent

C. 亞馬遜 CloudFront

D. Akamai 邊緣

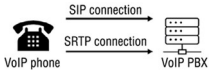
您回答錯誤。

BitTorrent 是點對點 (P2P) 內容分發網絡的一個示例。除了不太合法的用途外，它通常用於合法目的來分發大型文件，如 Linux ISO 和其他免費分發的軟件包和文件。CloudFlare、CloudFront 和 Akamai 的 Edge 都是託管 CDN。

第 34 題

tb787631.CISSPPT3E.c04.100

Mikayla 正在審查她的組織的 VoIP 環境配置，並找到一個顯示以下設計的圖表。她應該表達什麼擔憂？



A. 語音連接未加密，可以收聽。

B. 此圖中沒有安全問題。

C. 會話初始化連接未加密，可以查看。

D. 會話初始化和語音數據連接都是未加密的，可以被捕獲和分析。

您回答錯誤。

此圖顯示使用 SIP 而不是 SIPS，這意味著會話初始化協議未加密。幸運的是，語音數據通過安全實時傳輸協議或 SRTP 進行了加密。除了 SRTP 之外，Mikayla 還應該考慮使用 SIPS。

問題 35

tb787631.CISSPPT3E.c04.027

以下哪項是允許通過 TCP 裝載存儲的融合協議，並且經常用作光纖通道的低成本替代方案？

A、MPLS
B、SDN
C、網絡電話
D、iSCSI

你回答正確！

iSCSI 是一種融合協議，允許通過傳統網絡技術提供與位置無關的文件服務。它的成本低於傳統的光纖通道。VoIP 是 IP 語音，SDN 是軟件定義網絡，MPLS 是多協議標籤交換，一種使用路徑標籤而不是網絡地址的技術。

問題 36

tb787631.CISSPPT3E.c04.037

Casey 被要求確定 Zigbee 網絡流量是否可以在傳輸過程中得到保護。Zigbee 使用什麼安全機制來保護數據流量？

A. 3DES 加密

B、AES 加密

C、ROT13 加密

D. Blowfish 加密

你回答正確！

Zigbee 使用 AES 來保護網絡流量，提供完整性和機密性控制。它不使用 3DES，而 ROT13 是一種簡單的旋轉密碼，您可能會在麥片盒或秘密解碼器環中找到它。

問題 37

tb787631.CISSPPT3E.c04.004

Selah 和 Nick 的 PC 通過同時傳輸來同時發送流量。哪個網絡術語描述了網絡上可能受同一問題影響的系統範圍？

A. 子網

B. 超網

C. 衝突域

D.廣播域

你回答正確！

衝突域是一組系統，如果它們同時傳輸可能會導致衝突。衝突域外的系統

如果同時發送則不會引起衝突。這一點很重要，因為衝突域中的系統數量

增加了由於衝突增加而導致網絡擁塞的可能性。廣播域是一組可以相互接

收廣播的系統。子網是網絡的邏輯劃分，而超網則由兩個或多個網絡組成 。

問題 38

tb787631.CISSPPT3E.c04.061

Selah 的組織在桌面 PC 所在的交換機上部署了 VoIP 電話。這會產生什麼安全問題，什麼解決方案會有所幫助？

A. VLAN 跳躍；使用物理上分開的開關。

B、VLAN 跳躍；使用加密。

C. 來電顯示欺騙；MAC 過濾。

D. 拒絕服務攻擊；在網絡之間使用防火牆。

你回答正確！

當設備共享相同的交換機基礎設施時，可以實現語音和計算機 VLAN 之

間的 VLAN 跳躍。使用物理上獨立的交換機可以防止這種攻擊。加密對

VLAN 跳躍沒有幫助，因為它依賴於交換機需要讀取的標頭數據（而且

這是未加密的），而來電顯示欺騙是 VoIP 系統的固有問題。拒絕服務始

終是可能的，但這並不是特定的 VoIP 問題，如果它位於必須允許通過的

端口上，防火牆可能無法阻止該問題。

第 39 題

tb787631.CISSPPT3E.c04.038

Sue modifies her MAC address to one that is allowed on a network that uses MAC filtering to provide security. What is the technique Sue used, and what nonsecurity issue could her actions cause?

A. Broadcast domain exploit, address conflict
B. Spoofing, token loss
C. Spoofing, address conflict
D. Sham EUI creation, token loss

You Answered Incorrectly.

The process of using a fake MAC (Media Access Control) address is

called spoofing, and spoofing a MAC address already in use on the

network can lead to an address collision, preventing traffic from reaching one or both systems. Tokens are used in token ring networks, which are outdated, and EUI refers to an Extended Unique Identifier, another term for MAC address, but token loss is still not the issue. Broadcast domains refer to the set of machines a host can send traffic to via a broadcast message.

Question 40

tb787631.CISSPPT3E.c04.080

端點安全系統部署最常見的挑戰是什麼？

A. 妥協
B. 數據量
C. 監控網絡上的加密流量
D. 處理非 TCP 協議

您回答錯誤。

端點安全解決方案因其可以創建的數據量巨大而面臨挑戰。當每個工作站

都生成有關事件的數據時，這可能是大量數據。端點安全解決方案在正確

實施時應該減少妥協的數量，並且它們還可以通過在本地主機上解密後監

控流量來提供幫助。最後，非 TCP 協議在現代網絡中相對少見，這使得

端點安全系統實現中相對少見。

問題 41

tb787631.CISSPPT3E.c04.054

分段、排序和錯誤檢查都發生在與 SSL、TLS 和 UDP 關聯的 OSI 模型的哪一層？

A. 傳輸層
B. 網絡層
C.會話層
D. 表現層

您回答錯誤。

傳輸層提供設備之間的邏輯連接，包括端到端的傳輸服務以確保數據的傳

送。傳輸層協議包括 TCP、UDP、SSL 和 TLS。

問題 42

tb787631.CISSPPT3E.c04.069

Jason 知道使用 OSI 模型的協議在數據從一層移動到另一層時依賴於封裝。當數據向上流動到 OSI 層時，每一層都添加了什麼？

A.信息被添加到標題中。

B. 信息被添加到數據的主體中。

C. 數據用新的密鑰加密。

D. 提供完美前向保密的安全信封

你回答正確！

封裝添加到上一層提供的數據的頁眉（有時添加到頁腳）。數據的主體沒有被修改，加密可能會發生但並不總是發生。

問題 43

tb787631.CISSPPT3E.c04.079

Rich 想將他的網絡連接到距離他當前位置半英里的建築物。沿途有樹木和地形特徵，但有一條道路從樹木之間穿過到另一個位置。哪種類型的傳輸介質最適合此類部署？

A. 每 200 到 300 碼帶有中繼器的以太網電纜

B. WiFi 定向天線

C. 光纖電纜

D. LiFi 系統

你回答正确！

Buried fiber-optic cable is best suited to long distances, particularly when there are trees or other obstacles blocking line of sight that may interfere with WiFi or LiFi deployments. Ethernet’s distance limitations mean that repeaters would need to be powered, and there is no description of other structures or power along the path.

Question 44

tb787631.CISSPPT3E.c04.021

Which email security solution provides two major usage modes: (1) signed messages that provide integrity, sender authentication, and nonrepudiation; and (2) an enveloped message mode that provides integrity, sender authentication, and confidentiality?

A. S/MIME
B. MOSS
C. PEM
D. DKIM

You Answered Correctly!

S/MIME 支持簽名郵件和安全信封方法。雖然可以使用其他工具複製

S/MIME 的功能，但安全信封是 S/MIME 特定的概念。MOSS（即

MIME 對象安全服務）和 PEM 都可以提供身份驗證、機密性、完整性和

不可否認性，而 DKIM（即域密鑰識別郵件）是一種域驗證工具。

問題 45

tb787631.CISSPPT3E.c04.007

Michele 想用安全的替代品來替代 FTP 流量。她應該選擇什麼安全協議？

A、TFTP

B、HFTPS

C、安全 FTP

D、SFTP

你回答正確！

FTP/S 和 SFTP 通常用作替代不安全的 FTP 服務。SFTP 具有使用

SSH 進行傳輸的優勢，可以輕鬆使用現有的防火牆規則。TFTP 是簡單

的 FTP，是一種不安全的快速傳輸方法，通常用於為網絡設備傳輸文件 ，

以及其他用途。HFTPS 和 SecFTP 就是針對這個問題補的。

問題 46

tb787631.CISSPPT3E.c04.081

127.0.0.1 是什麼類型的地址？

A. 公共 IP 地址

B. RFC 1918 地址

C. APIPA 地址

D.環回地址

您回答錯誤。

IP 地址 127.0.0.1 是一個環回地址，將解析為本地機器。公共地址是非

RFC 1918，非保留地址。RFC 1918 地址是保留的，包括 10.xxx 等範

圍 APIPA 地址是在找不到 DHCP 服務器時使用的自分配地址。

問題 47

tb787631.CISSPPT3E.c04.066

數據流出現在 OSI 模型的哪三層？

A. 申請、演示和會議

B. 演示、會話和傳輸

C. 物理、數據鏈路和網絡

D. 數據鏈路、網絡和傳輸

您回答錯誤。

數據流與應用層、表示層和會話層相關聯。一旦它們到達傳輸層，它們就

變成段 (TCP) 或數據報 (UDP)。從那裡，它們被轉換為網絡層的數據包 、

數據鏈路層的幀和物理層的位。

問題 48

tb787631.CISSPPT3E.c04.042

Selah 希望在她的網絡上提供基於端口的身份驗證，以確保客戶端在使用網絡之前必須進行身份驗證。什麼技術是滿足此要求的合適解決方案？

答：802.11a

B. 802.3

C.802.15.1

D、802.1x

你回答正確！

802.1x 提供基於端口的身份驗證，可與 EAP（可擴展身份驗證協議）等

技術一起使用。802.11a 是無線標準，802.3 是以太網標準，802.15.1

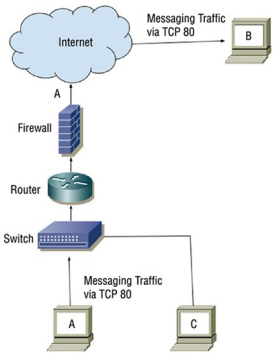
是最初的藍牙 IEEE 標準。

問題 49

tb787631.CISSPPT3E.c04.029

請參考以下場景和圖表：

- Selah 的組織多年來一直使用一種流行的消息傳遞服務。最近，人們對消息傳遞的使用提出了擔憂。



根據圖表，消息傳遞流量最有可能使用哪種協議？

A.鬆弛

B、HTTP

C、SMTP

D、HTTPS

你回答正確！

使用 TCP 端口 80 表明消息服務正在使用 HTTP 協議。Slack 是一種通過 HTTPS 運行的消息服務，它使用端口 443。SMTP 是一種使用端口 25 的電子郵件協議。

第 50 題

tb787631.CISSPPT3E.c04.055

Windows `ipconfig` 命令顯示以下信息：

- BC-5F-F4-7B-4B-7D

什麼術語描述了這一點，通常可以從中收集到什麼信息？

A. IP 地址，系統的網絡位置

B. MAC 地址，網卡廠商

C.MAC 地址，使用的媒體類型

D. IPv6 客戶端 ID，網絡接口卡的製造商

你回答正確！

機器訪問控制 (MAC) 地址是機器用於第 2 層通信的硬件地址。MAC 地址包括一個組織唯一標識符 (OUI)，用於標識製造商。MAC 地址是可以

更改的，所以這並不能保證準確性，但一般情況下您可以通過 MAC 地址

來判斷設備是哪個廠家生產的。

問題 51

tb787631.CISSPPT3E.c04.011

VPN 後端認證服務常用的協議有以下哪一種？

A.HTTPS

B. 半徑

C、ESP

D.AH

你回答正確！

遠程訪問撥入用戶服務 (RADIUS) 協議最初設計用於支持撥號調製解調

器連接，但仍常用於基於 VPN 的身份驗證。HTTPS 不是身份驗證協議 。

ESP 和 AH 都是 IPsec 協議，但不為其他系統提供認證服務。

問題 52

tb787631.CISSPPT3E.c04.093

以下哪項不是多層協議的缺點？

A. 他們可以允許繞過過濾器和規則。

B. 他們可以在更高的 OSI 級別上運行。

C. 他們可以允許隱蔽通道。

D. 它們可以允許繞過網段邊界。

您回答錯誤。

多層協議的常見缺點是它們可以繞過過濾器，允許或創建隱蔽通道，並允

許繞過網段邊界。在更高 OSI 層級運行的能力通常被認為是一種優勢。

問題 53

tb787631.CISSPPT3E.c04.083

哪種類型的網絡設備最常用於將端點系統分配給 VLAN？

A. 防火牆

B、路由器

C、開關

D. 樞紐

您回答錯誤。

端點系統到 VLAN 的分配通常由網絡交換機執行。

問題 54

tb787631.CISSPPT3E.c04.072

ICMP、RIP、網絡地址轉換都發生在 OSI 模型的哪一層？

A. 第一層

B、第 2 層

C、第 3 層

D. 第 4 層

你回答正確！

ICMP、RIP 和網絡地址轉換都發生在第 3 層，即網絡層。

問題 55

tb787631.CISSPPT3E.c04.096

5G 網絡相對於 4G 網絡的兩大優勢是什麼？（選擇所有符合條件的。）

A、抗干擾特性

B. 加強用戶身份保護

C.相互認證能力

D. 多因素認證

你回答正確！

5G 技術包括新的相互身份驗證功能和對用戶身份的額外保護。它沒有特

定的抗干擾安全功能，也沒有專門使用多因素身份驗證。

問題 56

tb787631.CISSPPT3E.c04.005

Sarah 正在手動查看 TCP 流量的數據包捕獲，並發現系統在短時間內重複發送的 TCP 數據包中設置了 RST 標誌。這個標誌在 TCP 包頭中是什麼意思？

A. RST 標誌的意思是“休息”。服務器需要流量來短暫暫停。

B. RST 標誌表示“中繼設置”。數據包將被轉發到數據包中設置的地址。

C. RST 標誌表示“恢復標準”。通信將以正常格式恢復。

D. RST 表示“重置”。TCP 會話將斷開。

你回答正確！

RST 標誌用於重置或斷開會話。它可以通過新的三向握手重新啟動連接來恢復。

問題 57

tb787631.CISSPPT3E.c04.087

Valerie 在其網絡上的交換機上啟用端口安全。她最有可能試圖阻止哪種類型的攻擊？

A.IP 欺騙

B、MAC 聚合

C. CAM 表氾濫

D、VLAN 跳躍

你回答正確！

Valerie 很可能試圖通過防止在單個端口上使用大量 MAC 地址來防止

CAM 表泛洪。如果 CAM 表泛洪成功，交換機將不知道將流量發送到哪

裡，而是將所有流量發送到每個端口，從而可能將流量暴露給攻擊者。側

重於硬件 (MAC) 地址的端口安全無法阻止 IP 欺騙和 VLAN 跳躍。MAC

aggregation 是針對這個問題補的。

問題 58

tb787631.CISSPPT3E.c04.047

以下哪個選項包含 OSI 模型第 6 層中存在的標准或協議？

A. NFS、SQL 和 RPC

B. TCP、UDP 和 TLS

C. JPEG、ASCII 和 MIDI

D. HTTP、FTP 和 SMTP

你回答正確！

第 6 層，表示層，通過對數據進行格式化和標準化，將來自應用層的數

據轉換為其他系統可以理解的格式。這意味著 JPEG、ASCII 和 MIDI 等

標準用於數據的表示層。傳輸層使用 TCP、UDP 和 TLS；

NFS、SQL、RPC 運行在 Session 層；HTTP、FTP、SMTP 是應用層

協議。

問題 59

tb787631.CISSPPT3E.c04.063

請參考以下場景：

- 蘇珊正在為她的組織的分支機構設計新的網絡基礎設施。

Susan 知道她需要為她的客戶實施 WiFi 網絡，並希望收集有關客戶的信息，例如他們的電子郵件地址，而不必向他們提供無線網絡密碼或密鑰。什麼類型的解決方案可以提供這種功能組合？

A.南汽

B. 強制門戶

C. 預共享密鑰

D. WPA3 的 SAE 模式

您回答錯誤。

強制門戶是一種流行的解決方案，您可能在酒店和咖啡店熟悉它。它們將

從客戶那裡收集數據的能力與開放網絡相結合，因此客戶數據不會被加密 。

這避免了分發網絡密碼的需要，但意味著如果客戶擔心安全，他們必須確保他們自己的流量是加密的。

問題 60

tb787631.CISSPPT3E.c04.039

Joanna 希望部署 4G LTE 作為遠程站點設備的帶外管理解決方案。以下哪項安全功能不是 4G 服務提供商通常提供的？

A. 加密能力
B. 基於設備的認證
C. 安全服務用戶的專用塔和天線
D. 基於 SIM 的身份驗證

你回答正確！

While security features vary from provider to provider, encryption, device-based authentication (for example, using certificates), and SIM-based authentication are all common options for 4G connectivity solutions.

Joanna should work with her provider to determine what capabilities are available and assess whether they meet her needs.

Question 61

tb787631.CISSPPT3E.c04.003

Ben has connected his laptop to his tablet PC using an 802.11ac connection. What wireless network mode has he used to connect these devices?

A. Infrastructure mode
B. Wired extension mode
C. Ad hoc mode
D. Standalone mode

You Answered Correctly!

Ben 使用的是 ad hoc 模式，它直接連接兩個客戶端。很容易將其與獨立模式混淆，後者使用無線接入點連接客戶端，而不是像中央網絡那樣連接到有線資源。基礎架構模式將端點連接到中央網絡，而不是直接相互連接。最後，有線擴展模式使用無線接入點將無線客戶端鏈接到有線網絡。

第 62 題

tb787631.CISSPPT3E.c04.082

Susan 正在為需要使用藍牙的組織用戶編寫最佳實踐聲明。她知道藍牙存在許多潛在的安全問題，並希望盡可能提供最佳建議。蘇珊應該包括以下哪幾組指導？

A. 使用藍牙內置的強加密，更改設備上的默認 PIN，關閉發現模式，並在未使用時關閉藍牙。

B. 僅將藍牙用於非機密活動，更改設備上的默認 PIN，關閉發現模式，並在不使用時關閉藍牙。

C. 使用藍牙內置的強加密，使用擴展（8 位或更長）藍牙 PIN，關閉發現模式，並在不使用時關閉藍牙。

D. 僅將藍牙用於非機密活動，使用擴展（八位或更長）藍牙 PIN，關閉發現模式，並在不使用時關閉藍牙。

你回答正確！

由於藍牙不提供強加密，因此它只能用於非機密活動。藍牙 PIN 是四位代碼，通常默認為 0000。將其關閉並確保您的設備未處於發現模式有助於防止藍牙攻擊。

問題 63

tb787631.CISSPPT3E.c04.010

Brian 正在為 PPP 連接選擇身份驗證協議。他想選擇一個選項來加密用戶名和密碼，並使用質詢/響應對話框防止重放。他還想定期重新驗證遠程系統。他應該使用哪種協議？

A.PAP

B. CHAP

C、EAP

D.飛躍

你回答正確！

PPP 服務器使用質詢握手身份驗證協議或 CHAP 對遠程客戶端進行身份驗證。它加密用戶名和密碼，並在連接時使用防止重放攻擊的技術執行定期重新驗證。LEAP 提供重新驗證但專為 WEP 而設計，而 PAP 發送未加密的密碼。EAP 是可擴展的並用於 PPP 連接，但它不直接處理列出的項目。

第 64 題

tb787631.CISSPPT3E.c04.046

Chris 想為他正在設計的設備使用低功耗個人區域網絡無線協議。以下哪種無線協議最適合創建小型低功耗設備，這些設備可以在建築物或房間內相對較短的距離內相互連接？

A. 無線網絡

B、Zigbee

C、NFC

D、紅外線

你回答正確！

Zigbee 專為此類低功耗物聯網網絡而設計，將是 Chris 的最佳選擇。某

些版本的藍牙也被設計為在低功耗模式下運行，但藍牙不在這個答案列表

中。WiFi 需要更多功率，NFC 距離很近，無法在建築物或房間內工作，

紅外線需要視線，因此很少使用。

問題 65

tb787631.CISSPPT3E.c04.099

在取證調查期間，Charles 能夠確定連接到受感染網絡的系統的媒體訪問控制 (MAC) 地址。Charles 知道 MAC 地址與製造商或供應商相關聯，並且是系統指紋的一部分。MAC 地址屬於哪個 OSI 層？

A. 應用層

B.會話層

C.物理層

D. 數據鏈路層

你回答正確！

MAC 地址及其組織上唯一的標識符在數據鏈路層用於識別網絡上的系統 。

應用層和會話層不關心物理地址，而物理層涉及電氣連接和處理物理接口

而不是尋址。

第 66 題

tb787631.CISSPPT3E.c04.059

Jim 的組織使用傳統的 PBX 進行語音通信。其內部通信可能面臨的最常見的安全問題是什麼？他應該提出什麼建議來預防它？

A. 竊聽、加密

B. 中間人攻擊，端到端加密

C. 竊聽、人身安全

D. Wardialing，部署一個 IPS

您回答錯誤。

Traditional private branch exchange (PBX) systems are vulnerable to

eavesdropping because voice communications are carried directly over

copper wires. Since standard telephones don’t provide encryption (and

you’re unlikely to add encrypted phones unless you’re the NSA),

physically securing access to the lines and central connection points is the best strategy available.

Question 67

tb787631.CISSPPT3E.c04.085

Michelle is told that the organization that she is joining uses an SD-WAN controller architecture to manage their WAN connections. What can she assume about how the network is managed and controlled? (Select all that apply.)

A. The network uses predefined rules to optimize performance.

B. The network conducts continuous monitoring to support better performance.

C. The network uses self-learning techniques to respond to changes in the network.

D. 所有連接均由組織的主要互聯網服務提供商管理。

您回答錯誤。

SD-WAN 實施通常執行所有這些功能，結合通過自學習和機器智能技術進行監視和響應的主動數據收集，然後應用預定義的規則來採取行動以使網絡按預期運行。SD-WAN 並不暗示或要求所有連接都由組織的主要互

聯網服務提供商管理。事實上，SD-WAN 通常用於處理多個 ISP，以實

現故障轉移和冗餘。

第 68 題

tb787631.CISSPPT3E.c04.009

Frank 負責確保他的組織擁有可靠、受支持的網絡硬件。以下哪項不是網絡管理員在確保網絡持續運行時普遍關心的問題？

A. 如果設備有供應商支持
B. 如果設備在保修期內
C. 主要設備是否支持冗餘電源
D. 如果所有設備都支持冗餘電源

你回答正確！

大多數網絡包括許多邊緣設備，如無線接入點和邊緣交換機。這些設備通

常有一個單一的電源來平衡成本和可靠性，如果它們發生故障，將被簡單

地更換。路由器和核心交換機等更關鍵的設備通常配備冗餘電源，以確保

在某個組件出現故障時網絡的較大部分不會出現故障。當然，確保設備得

到支持以便它們獲得更新並且它們在保修期內都是可支持網絡的常見做法。

第 69 題

tb787631.CISSPPT3E.c04.094

按順序放置 TCP/IP 模型的以下層，從應用層開始向下移動堆棧。

1. 應用層
2. 網絡接入層
3. 網絡層
4. 傳輸層

A、1、2、3、4
B、1、4、2、3
C.1、4、3、2
D.4、1、3、2

你回答正確！

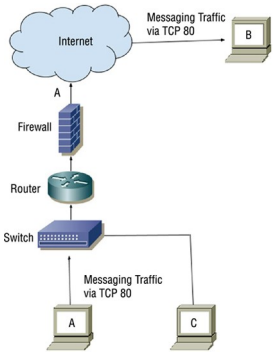
按順序，這些層是：應用層、傳輸層、Internet 層和網絡訪問層。

第 70 題

tb787631.CISSPPT3E.c04.031

請參考以下場景和圖表：

- Selah 的組織多年來一直使用一種流行的消息傳遞服務。最近，人們對消息傳遞的使用提出了擔憂。



Selah 的公司如何才能最好地滿足內部系統 A 和 C 用戶對安全消息傳遞的需求？

A. 使用第三方消息服務。

B. 實施和使用本地託管服務。

C. 使用 HTTPS。

D. 停止使用消息傳遞，而是使用更安全的電子郵件。

您回答錯誤。

如果業務需要消息傳遞，則使用本地消息傳遞服務器是最佳選擇。這可以防止流量傳輸到第三方服務器，並可以提供額外的好處，例如日誌記錄、存檔和控制安全選項（如使用加密）。

第 71 題

tb787631.CISSPPT3E.c04.032

當允許使用多層協議時，以下哪些缺點是值得關注的？

A. 可以在更高層使用一系列協議。

B. 允許隱蔽通道。

C. 過濾器無法繞過。

D. 加密不能合併到多層。

你回答正確！

多層協議為安全從業者帶來了三個主要問題：它們可以隱藏隱蔽通道（因

此隱蔽通道是允許的），過濾器可以被隱藏在分層協議中的流量繞過，以

及網絡段設置的邏輯邊界可以在某些情況下被繞過情況。多層協議允許在

不同層進行加密，並支持更高層的一系列協議。

第 72 題

tb787631.CISSPPT3E.c04.024

Alicia 的公司使用 SMS 消息提供數字代碼來實施多因素身份驗證。關於此設計，Alicia 可能想表達的主要安全問題是什麼？

A. SMS 消息未加密。

B. SMS 消息可以被發件人欺騙。

C. SMS 消息可能被多個電話接收。

D. SMS 消息可能存儲在接收電話上。

你回答正確！

SMS messages are not encrypted, meaning that they could be sniffed and captured. While using two factors is more secure than a single factor, SMS is one of the less secure ways to implement two-factor authentication because of this. SMS messages can be spoofed, can be received by more than one phone, and are typically stored on the recipient's phone. The primary threat here, however, is the unencrypted message itself.

Question 73

tb787631.CISSPPT3E.c04.050

Wayne wants to deploy a secure voice communication network. Which of the following techniques should he consider? (Select all that apply.)

A. Use a dedicated VLAN for VoIP phones and devices.

B. Require the use of SIPS and SRTP.

C. Require the use of VPN for all remote VoIP devices.

D. Implement a VoIP IPS.

You Answered Correctly!

Wayne 應該考慮為 VoIP 設備使用專用 VLAN，以幫助將它們與其他聯

網設備分開，並且他還應該要求使用 SIPS 和 SRTP，這兩種安全協議

都可以加密他的 VoIP 流量。如果正在使用 SIPS 和 SRTP，則不需要為

所有遠程 VoIP 設備使用 VPN，並且大多數組織中的典型部署並不是用

於 VoIP 的特定 IPS。

第 74 題

tb787631.CISSPPT3E.c04.088

Alaina 希望確保系統在允許進入網絡之前符合她的網絡安全設置，並希望確保她能夠盡可能地測試和驗證系統設置。她應該部署什麼類型的 NAC 系統？

A. 預准入、無客戶端 NAC 系統
B. 入院後、基於客戶的 NAC 系統
C. 預准入、基於客戶端的 NAC 系統
D. 入院後無客戶端 NAC 系統

你回答正確！

基於客戶端的預准入 NAC 系統將在系統被允許進入網絡之前使用客戶端

對其進行測試，該客戶端比無客戶端模型可以確定更多關於系統的信息。

客戶端已經聯網後的准入後測試和無客戶端版本在無法為系統安裝客戶端

時很有用。

第 75 題

tb787631.CISSPPT3E.c04.090

Angela 需要在以下協議之間進行選擇以進行安全身份驗證，並且不想創建不必要的技術複雜性。她應該選擇哪種身份驗證協議，為什麼？

A. EAP，因為它默認提供強加密

B. LEAP，因為它提供頻繁的重新認證和 WEP 密鑰的更改

C. PEAP，因為它提供加密並且不會遭受與 LEAP 相同的漏洞

D. EAP-TLS

您回答錯誤。

在這三個答案中，PEAP 是最好的解決方案。它將 EAP 封裝在 TLS 隧

道中，提供強大的加密。LEAP 是 Cisco 專有協議，最初設計用於幫助

處理 WEP 中的問題。LEAP 的保護已被擊敗，使其成為一個糟糕的選擇 。

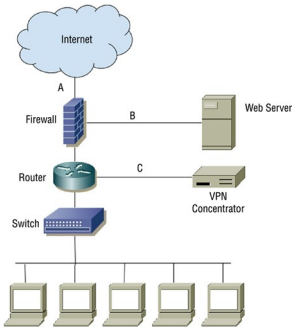
EAP-TLS 是安全的，但需要客戶端證書，因此難以部署和管理。

第 76 題

tb787631.CISSPPT3E.c04.015

請參考以下場景和圖表：

- Chris 正在為他的組織設計分層網絡安全。



如果 Chris 想阻止針對 Web 服務器的跨站腳本攻擊，那麼什麼設備最好，他應該把它放在哪裡？

A. 防火牆，位置 A

B. IDS，位置 A

C. IPS，位置 B

D. 一個 WAF，位置 C

你回答正確！

入侵保護系統可以掃描流量並阻止已知和未知的攻擊。Web 應用程序防

火牆或 WAF 也是一種合適的技術，但將其放置在位置 C 只能防止通過

組織的 VPN 進行的攻擊，而 VPN 只能由受信任的用戶使用。防火牆通

常沒有識別和阻止跨站點腳本攻擊的能力，而 IDS 系統只能監視而不能

阻止攻擊。

第 77 題

tb787631.CISSPPT3E.c04.097

VXLAN 在數據中心環境中起到什麼作用？

A. 它消除了以太網電纜最大距離的限制。

B. 它允許多個子網存在於同一 IP 空間中，主機使用相同的 IP 地址。

C. 它通過第 3 層網絡隧道傳輸第 2 層連接，將它們延伸到底層第 3 層網絡。

D、以上所有

你回答正確！

VXLAN 通過第 3 層網絡建立第 2 層連接隧道，本質上是將 LAN 擴展到

它可能無法正常運行的距離或網絡上。它不會消除以太網電纜的距離限制

，

也不會允許多個子網使用相同的 IP 空間——這需要 NAT 或其他重新映

射地址的技術來避免衝突。

第 78 題

tb787631.CISSPPT3E.c04.016

Susan 正在部署一個路由協議，該協議維護一個目標網絡列表，其中包含到這些網絡的跳數距離以及應將流量發送到它們的方向。她使用什麼類型的協議？

A. 鏈路狀態協議

B. 鏈路距離協議

C. 目的地度量協議

D. 距離矢量協議

您回答錯誤。

距離矢量協議使用包括到遠程網絡的跳躍方向和距離在內的度量來做出決

策。鏈路狀態路由協議考慮到遠程網絡的最短距離。目標度量和鏈路距離

協議不存在。

第 79 題

tb787631.CISSPPT3E.c04.062

請參考以下場景：

- 蘇珊正在為她的組織的分支機構設計新的網絡基礎設施。

Susan 想為該位置的內部網絡地址使用一組不可路由的 IP 地址。根據您對安全網絡設計原則和 IP 網絡的了解，以下哪些 IP 範圍可用於該目的？（選擇所有符合條件的。）

A.172.16.0.0/12

B.192.168.0.0/16

C.128.192.0.0/24

D.10.0.0.0/8

你回答正確！

RFC 1918 將三個地址範圍定義為私有（不可路由）IP 地址範圍：

10.0.0.0/8、172.16.0.0/12 和 192.168.0.0/16。這些都可行，但許多組

織將 192.168.0.0/16 範圍用於較小的站點，或者選擇為多個遠程站點劃

分出 10.0.0.0/8 範圍的部分。

問題 80

tb787631.CISSPPT3E.c04.028

Chris 正在構建一個以太網網絡，並且知道他需要使用他的 1000BaseT 網絡跨越 150 多米的距離。他應該使用什麼網絡技術來幫助解決這個問題？

A、在 100 米前安裝中繼器、交換機或集中器。

B. 使用 Category 7 電纜，它具有更好的屏蔽性能以實現更高的速度。

C. 安裝網關處理距離。

D. 使用 STP 電纜以高速處理更長的距離。

你回答正確！

中繼器、交換機或集中器將放大信號，確保 1000BaseT 的 100 米距離

限制不是問題。如果網絡協議發生變化，網關將很有用，而 Cat7 電纜適

用於距離更短的 10 Gbps 網絡。STP 電纜限制為 155 Mbps 和 100 米 ，

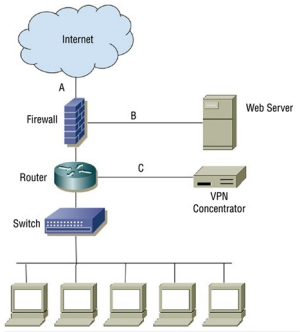
這會給 Chris 帶來網絡問題。

問題 81

tb787631.CISSPPT3E.c04.014

請參考以下場景和圖表：

- Chris 正在為他的組織設計分層網絡安全。



如果 VPN 授予遠程用戶與本地工作站相同的網絡和系統資源訪問權限，Chris 應該提出什麼安全問題？

A. VPN 用戶將無法訪問網絡服務器。

B. 沒有額外的安全問題；VPN 集中器的邏輯網絡位置與工作站的邏輯網絡位置相匹配。

C. Web 服務器流量不受狀態檢查。

D. VPN 用戶應該只能從受管理的 PC 連接。

你回答正確！

連接到受保護網絡的遠程 PC 需要符合與內部網絡所需的安全設置和標準。VPN 集中器在邏輯上將遠程用戶置於防火牆後面的保護區中，但這意味著用戶工作站（和用戶）必須以與本地工作站相同的方式受到信任。

問題 82

tb787631.CISSPPT3E.c04.045

Kathleen 所在的公司已將大多數員工轉移到遠程工作，並希望確保他們用於語音、視頻和基於文本的協作的多媒體協作平台是安全的。以下哪個安全選項將提供最佳用戶體驗，同時為通信提供適當的安全性？

A. 協作平台的所有使用都需要基於軟件的 VPN 連接到公司網絡。

B. 要求所有通信都使用 SIPS 和 SRTP。

C. 對協作平台的所有流量使用 TLS。

D. 將安全的 VPN 端點部署到每個遠程位置並使用點對點 VPN 進行通信。

您回答錯誤。

大多數現代應用程序在整個通信過程中都支持 TLS，允許客戶端安全地連接到服務並加密通信。VPN，無論是軟件還是硬件形式，都將更加複雜和笨拙。基於軟件的 VPN 會更靈活，而基於硬件的 VPN 會更昂貴、

更複雜。SIPS 和 SRTP 適用於 VoIP 環境，但通常不是 Microsoft

Teams、Zoom 或 WebEx 等現代多媒體協作平台的完整解決方案。

問題 83

tb787631.CISSPPT3E.c04.052

本正在設計一個 WiFi 網絡，並被要求為該網絡選擇最安全的選項。他應該選擇哪種無線安全標準？

一、WPA2

B、WPA

C、WEP

D.WPA3

你回答正確！

WPA3 是 WPA2 的替代品，它增加了安全功能，包括一種稱為同步對等

身份驗證的新模式，它用更安全的選項取代了 WPA2 的預共享密鑰模式 。

總的來說，它提供了安全改進，但由於硬件和軟件完全支持它的時間，可

能不會立即實施。WPA2 取代了 WPA 和 WEP，成為部署最廣泛的無線

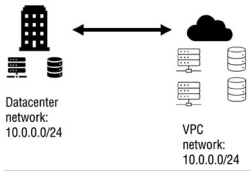
安全標準。

問題 84

tb787631.CISSPPT3E.c04.075

請參考以下場景：

- Ben 是一家組織的信息安全專家，該組織正在用雲託管的虛擬機替換其物理服務器。隨著組織構建其虛擬環境，它正在轉向混合雲運營模式，其中一些系統和服務保留在其本地數據中心，而其他系統和服務則託管在雲中。下圖顯示了本地數據中心和雲 VPC 的網絡 IP 範圍，您在回答問題時應考慮這些範圍。



Ben 希望使用多個互聯網服務提供商 (ISP) 連接到他的雲 VPC，以確保可靠的訪問和帶寬。他可以使用什麼技術來管理和優化這些連接？

A、FCoE

B、VXLAN

C.SDWAN

D. LiFi

你回答正確！

軟件定義的廣域網或 SD-WAN 通常用於管理多個 ISP 和其他連接選項，以確保速度、可靠性和帶寬設計目標均得到滿足。Ben 可以使用 SD-WAN 功能來實現他的目標，使他的混合雲環境取得成功。以太網光纖通

道 (FCoE) 是一種存儲協議；VXLAN 用於可擴展的虛擬 LAN，而不是

WAN；而 LiFi 使用可見光和紅外線來傳輸數據。

問題 85

tb787631.CISSPPT3E.c04.012

Isaac 希望確保他的 VoIP 會話初始化是安全的。他應該確保啟用和需要什麼協議？

A、SVOIP

B、PBSX

C.SIPS

D、SRTP

你回答正確！

SIPS 是 VoIP 會話初始化協議的安全版本，添加了 TLS 加密以保證會話

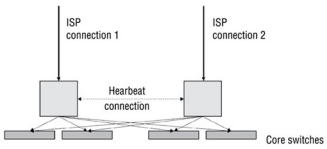
初始化過程的安全。SVOIP 和 PBSX 不是真正的協議，但 SRTP 是實

時傳輸協議 RTP 的安全版本。

問題 86

tb787631.CISSPPT3E.c04.089

Derek 想要部署冗餘核心路由器，如圖所示。什麼樣的高可用集群模型會給他提供最大的吞吐量？



A.主動/主動

B、線下互動

C、主動/被動

D、近線

您回答錯誤。

主動/主動對可以使用兩個設備的全部吞吐量能力，但正常的部署模型將設計為單個設備的最大吞吐量，以避免在其中一個設備出現故障時中斷。

主動/被動設計只能處理單個設備的吞吐量，並允許輔助設備保持運行準備狀態，但在需要時才傳遞流量。在線交互是一個術語，通常用於描述過濾電源而不是通過電源的 UPS 系統，而近線是一個術語，用於描述不在線但可以相對快速檢索的備份。

問題 87

tb787631.CISSPPT3E.c04.056

Chris 被要求在實施 PEAP 和 LEAP 之間進行選擇以進行無線身份驗證。他應該選擇什麼，為什麼？

A. LEAP，因為它修復了 TKIP 的問題，從而提高了安全性

B. PEAP，因為它實現了 CCMP 以確保安全

C. LEAP，因為它實現了 EAP-TLS 用於端到端會話加密

D. PEAP，因為它可以提供一個封裝 EAP 方法的 TLS 隧道，保護整個會話

您回答錯誤。

PEAP 為 EAP 方法提供加密並可以提供身份驗證。它不實施 WPA2 標準中包含的 CCMP。LEAP 具有危險的不安全性，由於自 2000 年代初以來一直可用的攻擊工具，因此不應使用。

問題 88

tb787631.CISSPPT3E.c04.006

Gary 正在部署無線網絡，並希望部署最快的無線技術。他應該使用以下哪一種無線網絡標準？

答：802.11a

B、802.11g

C、802.11n

D.802.11ac

你回答正確！

他應該選擇 802.11ac，支持理論速度高達 3.4 Gbps。802.11n 最高支持

600 Mbps，802.11g 和 802.11 a 只能支持 54 Mbps。

問題 89

tb787631.CISSPPT3E.c04.053

凱瑟琳在一個城鎮中有兩個主要位置，她希望這兩個環境看起來像同一個本地網絡。每個位置都部署了路由器、交換機和無線接入點。哪種技術最適合讓她讓這兩個設施看起來位於同一網段？

A.SDWAN
B、VXLAN
C.VMWAN
D、iSCSI

您回答錯誤。

VXLAN 是一種封裝協議，可在可路由網絡中承載 VLAN，使兩個不同的

網絡位置看起來在同一網段上，儘管距離和網絡存在差異。SD-WAN 是

一種軟件定義的廣域網，是一種管理和控制廣域網連接的方式。iSCSI

是一種基於 IP 的存儲協議，而 VMWAN 就是為了解決這個問題。

問題 90

tb787631.CISSPPT3E.c04.040

SMTP、HTTP 和 SNMP 都發生在 OSI 模型的哪一層？

A. 第 4 層

B、第 5 層

C、第 6 層

D. 第 7 層

你回答正確！

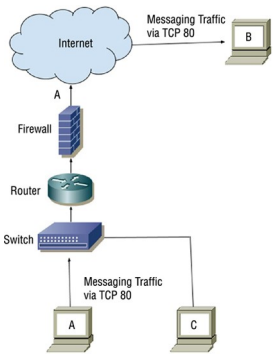
特定於應用程序的協議在第 7 層處理，即 OSI 模型的應用程序層。

問題 91

tb787631.CISSPPT3E.c04.030

請參考以下場景和圖表：

- Selah 的組織多年來一直使用一種流行的消息傳遞服務。最近，人們對消息傳遞的使用提出了擔憂。



從 A 向 B 發送內部通信會引起什麼安全問題？

A. 防火牆不保護系統 B.

B. 系統 C 可以看到系統 A 到 B 的廣播流

量。

C. 它通過未加密的協議傳輸。

D. 消息傳遞不提供不可否認性。

你回答正確！

HTTP 流量通常通過 TCP 80 發送。未加密的 HTTP 流量可以在 A 和 B 之間的任何點輕鬆捕獲，這意味著所選的消息傳遞解決方案無法為組織的企業通信提供機密性。

問題 92

tb787631.CISSPPT3E.c04.058

B 類網絡的默認子網掩碼是什麼？

A.255.0.0.0

B.255.255.0.0

C.255.254.0.0

D.255.255.255.0

你回答正確！

B 類網絡擁有 2^16 個系統，其默認網絡掩碼為 255.255.0.0。

問題 93

tb787631.CISSPPT3E.c04.060

通過 WiFi 和 LiFi 進行無線通信的技術區別是什麼？

A. LiFi 不易受電磁干擾。

B. LiFi 不能用於提供寬帶速度。

C. WiFi 不易受電磁干擾。

D. WiFi 不能用於提供寬帶速度。

你回答正確！

LiFi 使用可見光和紅外線高速傳輸數據。雖然 LiFi 部署尚未廣泛發生，

但它們已在一些實際應用中取得初步成功。LiFi 和 WiFi 可以提供寬帶速

度，而 WiFi 與 LiFi 不同，容易受到 EM 干擾。

問題 94

tb787631.CISSPPT3E.c04.071

在檢查她的組織的網絡時，安吉拉發現它正遭受廣播風暴的困擾，並且承包商、訪客和組織的管理人員都在同一網段上。Angela 應該推薦什麼設計更改？

A. 要求對所有用戶進行加密。

B. 在網絡邊界安裝防火牆。

C. 啟用生成樹環路檢測。

D. 根據功能要求對網絡進行分段。

你回答正確！

網絡分段可以減少性能問題，並通過限制分段中的系統數量來減少廣播風

暴的可能性。這減少了每個系統可見的廣播流量，並可以減少擁塞。分段

還可以通過分離不需要能夠訪問彼此系統的功能組來幫助提供安全性。在

邊界安裝防火牆只會幫助入站和出站流量，而不是跨網絡流量。生成樹循

環預防有助於防止以太網網絡中的循環（例如，當您通過每個交換機上的

兩個端口將交換機插入交換機時），但它不會解決不是由循環或安全問題

引起的廣播風暴。加密可能有助於防止功能組之間出現一些問題，但不會

阻止它們掃描其他系統，

問題 95

tb787631.CISSPPT3E.c04.067

Lucca 希望保護在生產中使用但不再受支持且無法修補以免受網絡攻擊的端點。他應該怎麼做才能最好地保護這些設備？

A. 在設備上安裝防火牆。

B. 禁用所有服務並打開設備上的端口。

C. 在設備前面放置一個硬件網絡安全設備。

D. 將設備從網絡中拔出，因為它們無法得到適當的保護。

你回答正確！

如果設備仍需要投入生產但無法打補丁，Lucca 的最佳選擇是使用單獨

的安全設備來保護它們。簡單地在設備上安裝防火牆或禁用它向網絡公開

的所有服務可能很誘人，但某些設備可能沒有可用的防火牆軟件，即使有 ，

底層操作系統也可能在其實現中存在漏洞甚至防火牆也無法保護的網絡堆

棧或其他軟件。拔掉保護所需的設備並不能解決讓它們保持在線的需要。

問題 96

tb787631.CISSPPT3E.c04.044

MAC 克隆試圖繞過有線網絡的哪些安全控制？

A. 港口安全

B、VLAN 跳躍

C. 802.1q 集群

D. Etherkiller 預防

您回答錯誤。

端口安全可防止無法識別或未經許可的系統根據其 MAC 地址連接到網

絡端口。克隆一個允許的或合法的 MAC 地址試圖繞過它。VLAN 跳躍和

802.1q 中繼攻擊試圖通過封裝數據包來訪問其他子網，因此它們將被解

包並定向到其他子網。Etherkiller 預防不是安全設置或控制。

問題 97

tb787631.CISSPPT3E.c04.008

Jake 被告知他的網絡存在第 3 層問題。以下哪項與 OSI 模型中的第 3 層相關？

A. IP 地址

B. TCP 和 UDP 協議

C、MAC 地址

D. 通過硬件發送和接收位

您回答錯誤。

網絡層或第 3 層使用 IP 地址進行邏輯尋址。TCP 和 UDP 協議用於傳輸

層，即第 4 層。硬件地址用於第 2 層，即數據鏈路層，通過硬件發送和

接收位是在物理層（第 1 層）完成的。

問題 98

tb787631.CISSPPT3E.c04.036

IPsec 可以為安全通信提供哪些功能？

A. 加密、訪問控制、不可否認性和消息認證。

B. 協議融合、內容分發、微分段和網絡虛擬化

C. 加密、授權、不可否認和消息完整性檢查

D. 微分段、網絡虛擬化、加密和消息認證

你回答正確！

IPsec 或 Internet 協議安全性可以使用公鑰密碼術提供加密、訪問控制、不可否認性和消息身份驗證。它不提供授權、協議收斂、內容分發或列出的其他項目。

問題 99

tb787631.CISSPPT3E.c04.091

當衛星互聯網是唯一可用的選擇時，需要高性能互聯網連接的系統經常關心的問題是什麼？

A. 安全

B. 與 LiFi 等協議的兼容性

C. 與 Zigbee 等協議的兼容性

D. 延遲

你回答正確！

大多數現有的衛星互聯網系統都有相對較高的延遲。較新的低地球軌道衛星（如 Starlink）似乎提供比高軌道更好的延遲，但延遲和對天氣乾擾的敏感性都是基於衛星的系統的常見問題。

第 100 題

tb787631.CISSPPT3E.c04.076

WPA2 的 Counter Mode Cipher Block Chaining Message Authentication Mode Protocol (CCMP) 基於哪種常見的加密方案？

已

B、3DES

C、AES

D、TLS

你回答正確！

WPA2 的 CCMP 加密方案是基於 AES 的。在撰寫本書時，還沒有任何針對 WPA2 的實際攻擊。DES 已被成功攻破，3DES 和 TLS 均未用於 WPA2。