歡迎學習模組 6：創建聯網環境。

模組概覽

小節目錄

1. 架構需求
2. 創建 AWS 聯網環境
3. 將 AWS 聯網環境連接到互聯網
4. 保護 AWS 聯網環境

演示

- 創建 Virtual Private Cloud

實驗

- 指導實驗：創建 Virtual Private Cloud
- 挑戰實驗：為咖啡館創建 VPC 聯網環境

知識測驗

本模組包含以下章節：

1. 架構需求
2. 創建網路環境
3. 將網絡環境連接到互聯網
4. 保護網路環境

該模組還包括：

- 一個演示，將向您展示如何手動創建 Virtual Private Cloud (VPC)
- 一個指導實驗，您將在其中自行創建 VPC
- 一個挑戰實驗，您將在其中創建 VPC、將私有資源連接到互聯網，以及創建安全層來控制進出 VPC 中私有資源的流量。

最後，您需要完成一個知識測驗，以測試您對本模組中涵蓋的關鍵概念的理解程度。

模組目標

學完本模組後，您應該能夠：

- 說明 Amazon Web Services (AWS) 雲聯網中的 Virtual Private Cloud (VPC) 的基本功能
- 確定如何將 AWS 聯網環境連接到互聯網
- 描述如何在 AWS 聯網環境中隔離資源
- 創建包含子網、互聯網閘道、路由表和安全性群組的 VPC

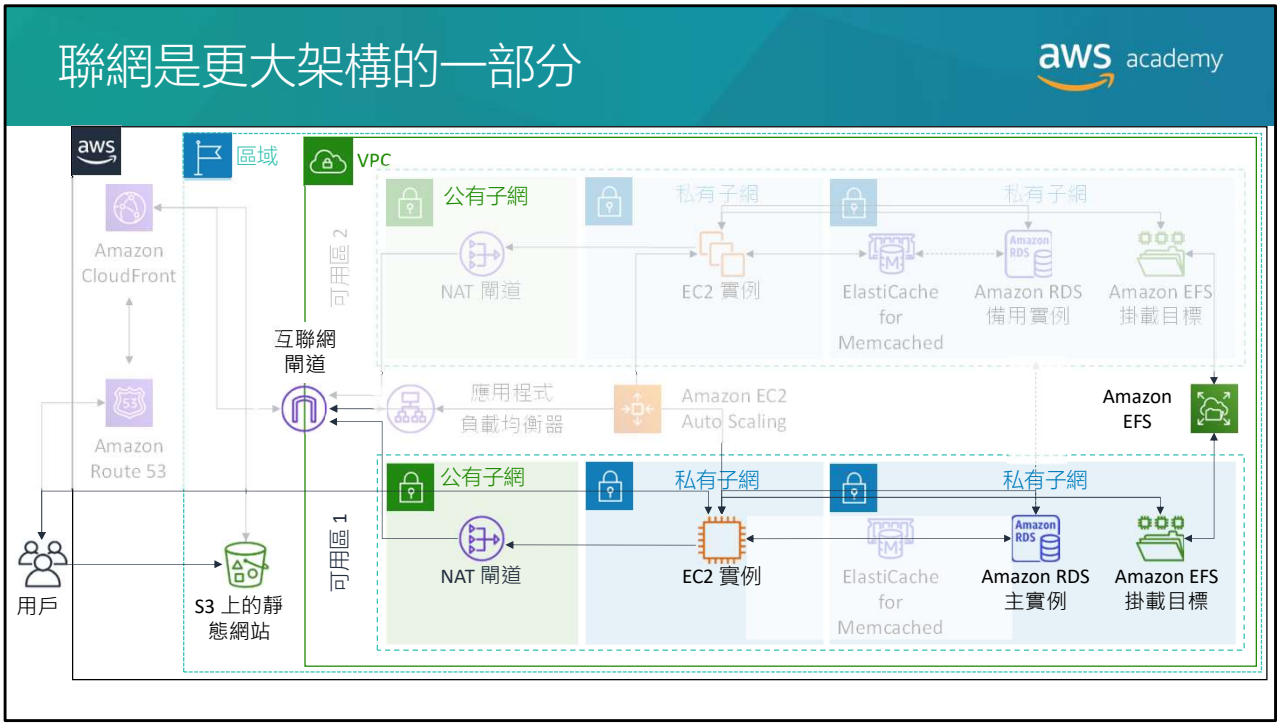
學完本模組後，您應該能夠：

- 說明 Amazon Web Services (AWS) 雲聯網中的 Virtual Private Cloud (VPC) 的基本功能
- 確定如何將 AWS 聯網環境連接到互聯網
- 描述如何在 AWS 聯網環境中隔離資源
- 創建包含子網、互聯網閘道、路由表和安全性群組的 VPC

模組 6：創建聯網環境

第 1 節：架構需求

介紹第 1 節：架構需求。



在本模組中，您將學習如何在 AWS 上設計網路以及如何構建包含子網的 VPC。您還將學習如何將公有子網和私有子網中的實例連接到互聯網。

咖啡館業務要求

咖啡館必須在安全、隔離的網路環境中部署和管理 AWS 資源。

該咖啡館的業務一直在穩步增長。Sofía 和 Nikhil 已經與一些擔任 AWS 顧問的咖啡館常客成為朋友，他們開始討論咖啡館當前的架構。其中有一位常客是 AWS 解決方案架構師 Olivia，他認為需要擴展咖啡館的線上業務。擴展需要額外的伺服器來運行線上下單應用程式，但當前的子網規模太小，無法支援這種增長。因此，他們需要重新構建運行應用程式的網路的某些方面。

在進一步審查咖啡館的架構時，Olivia 還發現了一個漏洞：用於管理應用程式伺服器的 TCP 埠可以通過互聯網訪問。Sofía 解釋說，她和 Nikhil 必須能夠管理和維護伺服器。Olivia 建議他們設置堡壘主機，以減少對伺服器的公開訪問，提高伺服器的安全性。

模組 6：創建聯網環境

第 2 節：創建 AWS 聯網環境

介紹第 2 節：創建 AWS 聯網環境。

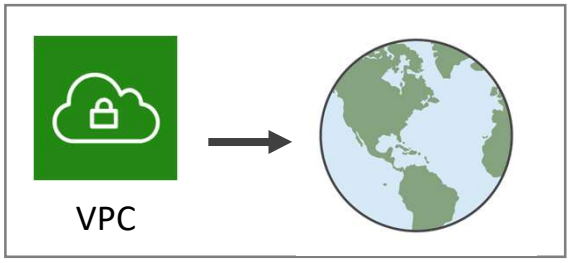
Amazon Virtual Private Cloud (Amazon VPC) 是一項服務，可讓您在 AWS 雲中預置一個邏輯隔離部分（稱為 Virtual Private Cloud 或 VPC），您可以在其中啟動您的 AWS 資源。

Amazon VPC 讓您能夠控制您的虛擬聯網資源。例如，您可以選擇自己的 IP 位址範圍、創建子網以及配置路由表和網路閘道。您可以在 VPC 中同時使用 IPv4 和 IPv6，實現資源和應用程式安全訪問。

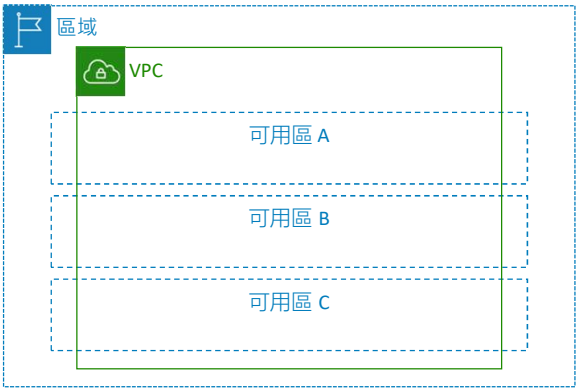
您還可以自訂 VPC 的網路配置。例如，您可以為可訪問公有互聯網的 Web 伺服器創建一個公有子網。您可以將後端系統（例如資料庫或應用程式伺服器）放在不能通過公有互聯網訪問的私有子網中。

最後，您可以使用多個安全層，幫助控制對每個子網中的 Amazon Elastic Compute Cloud (Amazon EC2) 實例的訪問。這些安全層包括安全性群組和網路存取控制清單（網路 ACL）。

VPC 部署



您可以在任何 AWS 區域中部署 VPC。



VPC 可以託管其所在區域中任何可用區的受支持的資源。

VPC 屬於單個 AWS 區域。VPC 跨越區域中的所有可用區，因此它可以託管來自其所在區域內任何可用區的受支持的資源。

無類域間路由 (CIDR)

0.0.0.0/0	= 所有 IP 地址
10.22.33.44/32	= 10.22.33.44
10.22.33.0/24	= 10.22.33.*
10.22.0.0/16	= 10.22.*.*

CIDR	總 IP 地址數
/28	16
...	...
/20	4096
/19	8192
/18	16384
/17	32768
/16	65536

在創建 VPC 時，您可以提供您希望 VPC 中的實例使用的私有 IP 位址集。您以無類域間路由 (CIDR) 塊的形式指定此地址集，例如 10.0.0.0/16。這是您的 VPC 的主要 CIDR 塊。您可以指定 /28（16 個 IP 位址）到 /16（65536 個 IP 位址）之間的塊大小。

Amazon VPC 支援 IPv4 和 IPv6 位址分配，並為它們設定了不同的 CIDR 塊大小限制。預設情況下，所有 VPC 和子網都必須具有 IPv4 CIDR 塊，您不能更改此行為。您可以選擇將 IPv6 CIDR 塊與您的 VPC 關聯。

您的 VPC 可在雙堆疊模式下運行：您的資源可通過 IPv4 和/或 IPv6 進行通信。IPv4 和 IPv6 位址是相互獨立的，因此您必須在 VPC 中分別針對 IPv4 和 IPv6 配置路由和安全設置。

子網：劃分 VPC

- 子網是 VPC 的 IP 位址範圍的分段或分區，您可以在其中分配一組資源
- 子網不是隔離邊界
- 子網是 VPC CIDR 塊的子集
- 子網 CIDR 塊不能重疊
- 每個子網完全位於一個可用區內
- 您可以在每個可用區或本地擴展區中添加一個或多個子網
- AWS 在每個子網中預留五個 IP 地址

例如：具有 CIDR /22 VPC 共包含 1024 個 IP 位址。

您可以將 VPC 劃分為一個或多個子網。子網是 VPC 的 IP 位址範圍的分段或分區，您可以在其中分配一組資源。請務必記住，子網不是應用程式的隔離邊界。相反，它們是存儲路由策略的容器，您將在本模組的下一節中瞭解這些內容。

在創建子網時，需要為子網指定 CIDR 塊，它是 VPC CIDR 塊的子集。子網的 CIDR 塊不能重疊。

儘管每個子網都必須完全位於一個可用區內且不能跨越區域，但每個可用區都可以有一個或多個子網。您可以選擇在本地擴展區中添加子網。當您在本地擴展區中創建子網時，VPC 也會擴展到該本地擴展區。有關如何將 VPC 資源擴展到本地擴展區的更多資訊，請參閱 AWS 文檔中的將 VPC 資源擴展到 AWS 本地擴展區。

由於 VPC 子網映射到特定可用區，因此子網置放是用以確保 Amazon EC2 實例恰當分佈在多個位置的一種方式。

AWS 將預留每個子網 CIDR 塊中的前四個 IP 位址和最後一個 IP 位址。例如，在 CIDR 塊

為 10.0.0.0/24 的子網中，AWS 將預留以下五個 IP 地址：

- 10.0.0.0：網路位址
- 10.0.0.1：VPC 本地路由器
- 10.0.0.2：網域名稱系統 (DNS) 解析
- 10.0.0.3：未來使用
- 10.0.0.255：網路廣播位址

有關 VPC 和子網的更多資訊，請參閱 AWS 文檔中的 VPC 和子網。

VPC 設計最佳實踐

- 為具有唯一路由要求的每組主機的每個可用區創建一個子網。
- 在一個區域內的所有可用區中平均劃分 VPC 網路範圍。
- 不要一次分配所有網路位址。相反，請確保預留一些位址空間 以備將來使用。
- 調整 VPC CIDR 和子網的大小，以支持預期工作負載的顯著增長 。
- 確保 VPC 網路範圍（CIDR 塊）不會與組織的其他私有網路範圍重疊。

在配置任何電腦網路時，請考慮以下通用網路設計原則：

- 為具有唯一路由要求的每組主機的每個可用區創建一個子網。
- 在一個區域內的所有可用區中平均劃分 VPC 網路範圍。
- 不要一次分配所有網路位址。相反，請確保預留一些位址空間以備將來使用。
- 調整 VPC CIDR 和子網的大小，以支援預期工作負載的顯著增長。
- 確保 VPC 網路範圍（CIDR 塊）不會與組織的其他私有網路範圍重疊。

有關設計和調整單個 VPC 大小的更多資訊，請參閱 AWS 單個 VPC 設計。

單個 VPC 部署

在有限的使用案例中，部署一個 VPC 可能是合適的做法：

- 由小型團隊管理的小型單一應用程式
- 高性能計算 (HPC)
- 身份管理

在大多數使用案例中，組織基礎設施主要使用兩種模式：多 VPC 和多帳戶。

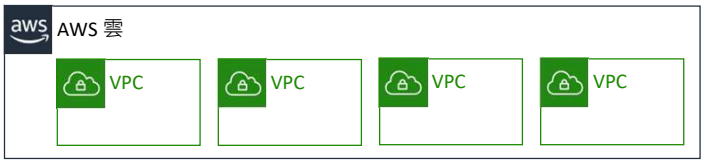
在設計和創建網路環境時，可能適合使用單個 VPC 環境的使用案例數量有限：

- 由小型團隊管理的小型單一應用程式
- 高性能計算 (HPC) 環境（例如物理類比）– 相比跨越多個 VPC 的環境，單個 VPC 環境的延遲更低
- 身份管理環境 – 單個 VPC 可能提供最佳安全性。

但是，對於大多數使用案例而言，都需要多 VPC 環境。您可以在同一區域或不同區域創建多個 VPC。您還可以在同一 AWS 帳戶或不同 AWS 帳戶中創建多個 VPC。

多個 VPC

- 最適合 –
  - 單個團隊或單個企業或組織，例如託管服務提供者
  - 有限團隊，更便於保持標準和管理訪問
- 例外 –
  - 監管和合規性標準可能需要更大規模的工作負載隔離，與企業或組織複雜程度無關



多 VPC 最適合對每個應用程式環境中所有資源的預置和管理保持完全掌控的單一團隊或組織。例如，假設有一個開發大型電子商務應用程式的團隊。當開發人員能夠完全訪問開發和生產環境時，他們可能會使用此模式。管理測試和生產環境中所有資源的託管服務提供者 (MSP) 也通常使用這種模式。

要瞭解有關多 VPC 部署的服務和最佳實踐的更多資訊，請參閱：

- 單區域多 VPC 連接
- 多區域多 VPC 連接

多個帳戶

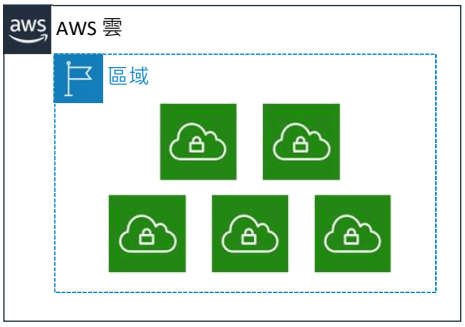
- 最適合 –
  - 大型企業或組織和擁有多個 IT 團隊的企業或組織
  - 預計發展迅速的中型企業或組織
- 為什麼?
  - 在較為複雜的企業或組織中，管理訪問和標準的難度會更大。

如前所述，您可以在同一 AWS 帳戶或不同帳戶中創建多個 VPC。

多帳戶模式最適合企業客戶或跨多個團隊部署應用程式的組織。例如，假設某個組織要支援兩個或多個團隊。他們可能會使用此模式來支援以下開發人員：能夠完全訪問開發環境資源，但對生產環境的存取權限有限或根本沒有許可權。

Amazon VPC 配額

默認配額：每帳戶每區域 5 個 VPC *



* 預設配額為每區域 5 個 VPC，但可以申請增加配額。

注意 Amazon VPC 配額。預設配額為每個區域 5 個 VPC。但是，您可以請求增加此配額。

有關 Amazon VPC 服務限制的更多資訊，請參閱 AWS 文檔中的 Amazon VPC 配額。

第 2 節要點

- 使用 Amazon VPC，您可以預置 VPC，這些 VPC 是 AWS 雲中的邏輯隔離部分，您可以在其中啟動 AWS 資源。
- 一個 VPC 只屬於一個區域，並且被劃分為子網。
- 一個子網屬於一個可用區或本地擴展區。它是 VPC CIDR 塊的子集。
- 您可以在相同區域或不同區域以及相同或不同帳戶中創建多個 VPC。
- 在設計 VPC 時，請遵循最佳實踐。

本模組中這節內容的要點包括：

- 使用 Amazon VPC，您可以預置 VPC，這些 VPC 是 AWS 雲中的邏輯隔離部分，您可以在其中啟動 AWS 資源。
- 一個 VPC 只屬於一個區域，並且被劃分為子網。
- 一個子網屬於一個可用區或本地擴展區。它是 VPC CIDR 塊的子集。
- 您可以在相同區域或不同區域以及相同帳戶或不同帳戶中創建多個 VPC。
- 在設計 VPC 時，請遵循以下最佳實踐：
    - 為具有唯一路由要求的每組主機的每個可用區創建一個子網。
    - 在一個區域內的所有可用區中平均劃分 VPC 網路範圍。
    - 不要一次分配所有網路位址。相反，請確保預留一些位址空間以備將來使用。
    - 調整 VPC CIDR 和子網的大小，以支援預期工作負載的顯著增長。
    - 確保 VPC 網路範圍不會與企業或組織的其他私有網路範圍重疊。

模組 6：創建聯網環境

第 3 節：將 AWS 聯網環境連接到互聯網

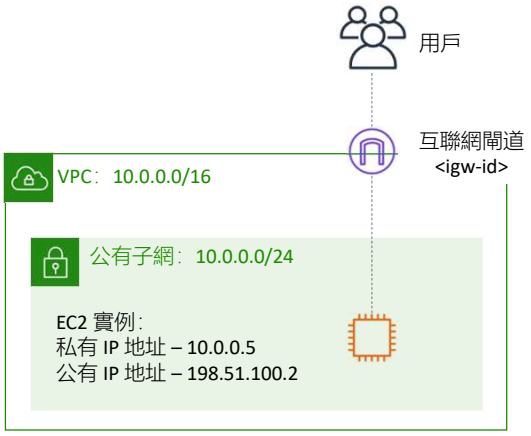
介紹第 3 節：將 AWS 聯網環境連接到互聯網。

創建公有子網

aws academy

互聯網閘道

- 允許 VPC 中的資源與互聯網之間的通信
- 在預設情況下，水準擴展、具有冗餘且高度可用
- 在子網路由表中為 Internet 可路由流量提供一個目標



現在，您已經知道如何為工作負載設計和創建隔離的網路環境，您希望將其連接到互聯網。

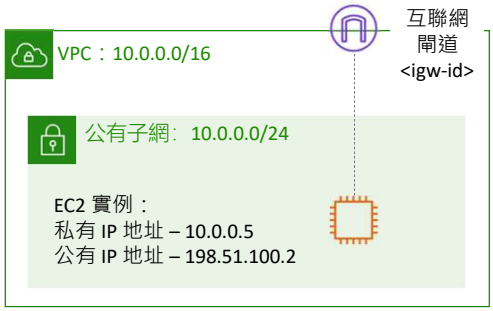
互聯網閘道*是一種 VPC 元件，可允許 VPC 中的資源與互聯網之間進行通信。*它可水準擴展、冗餘且高度可用。互聯網閘道支援 IPv4 和 IPv6 流量。互聯網閘道有兩種用途：首先，它在 VPC 路由表中為互聯網可路由流量提供一個目標。其次，互聯網閘道為已分配公有 IPv4 位址的實例執行網路位址轉譯 (NAT)。

要將子網設為*公有*，您必須首先創建一個互聯網閘道並將其連接到 VPC。

定向 VPC 資源之間的流量

- 需要使用路由表來定向 VPC 資源之間的流量
- 每個 VPC 有一個主（默認）路由表
- 所有子網都必須與路由表關聯
- 您可以創建自定義路由表

最佳實踐：針對每個子網使用自訂路由表。



公有路由表

目的地	目標
10.0.0.0/16	本地
0.0.0.0/0	<igw-id>

接下來，您必須更新與要連接到互聯網的子閘道聯的路由表。路由表*包含一組稱為*路由*的規則*。路由 用於確定將網路流量的目標去向。

當您創建 VPC 時，它會自動具有一個主路由表。主路由表（以及 VPC 中的每個路由表）最初僅包含一項支持 VPC 中所有資源通信的本地路由。您無法修改路由表中的本地路由。當您在 VPC 中啟動實例時，本地路由會自動覆蓋該實例。您不需要將新實例添加到路由表。您可以為您的 VPC 創建額外的自訂路由表。

VPC 中的每個子網必須與一個路由表相關聯，該路由表會控制此子網的路由。如果您未將子網明確關聯到特定路由表，則該子網將與主路由表建立隱式關聯。一個子網一次只能與一個路由表關聯，但您可以將多個子網與同一個路由表關聯。

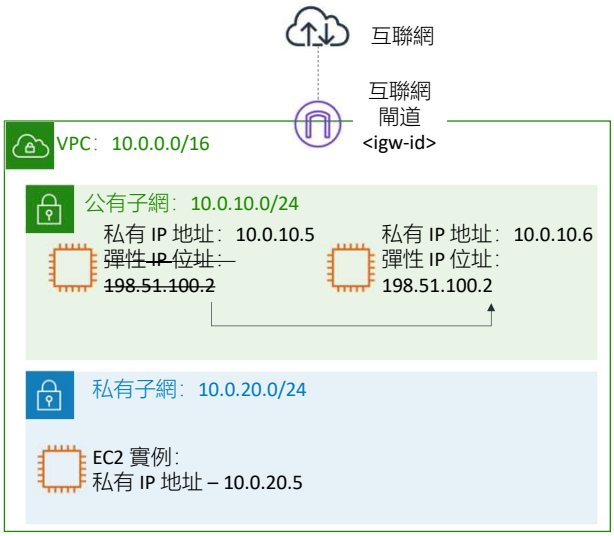
您可以針對每個子網創建自訂路由表，以實現對目標位置的精細路由。

要通過互聯網閘道將非本地流量發送到互聯網，請在與子閘道聯的路由表中創建一個目的地為 **0.0.0.0/0**、目標為 **<igw-id>** 的路由。

將 IP 位址從一個實例重新映射到另一個實例

彈性 IP 地址

- 與您的 AWS 帳戶關聯的靜態公有 IPv4 位址
- 可與實例或彈性網路介面相關聯
- 可以重新映射到帳戶中的另一個實例
- 當負載均衡器不可用時對實現冗余非常有用



接下來，您必須確保您的實例具有公有 IP 位址或彈性 IP 位址。

彈性 IP 位址*是專用於動態雲計算的靜態公有 IPv4 位址*。您可以將彈性 IP 位址與您帳戶中的任意 VPC 的任何實例或彈性網路介面相關聯。借助彈性 IP 位址，您可以迅速將位址重新映射到 VPC 中的其他實例，從而遮罩實例故障。與將彈性 IP 位址與實例直接關聯相比，將彈性 IP 位址與網路介面關聯具有一個優勢。您可以通過一個步驟將網路介面的所有屬性從一個實例移動到另一個實例。

將私有子網連接到互聯網

aws academy

NAT 閘道

- 使私有子網中的實例可以發起到互聯網或其他 AWS 服務的出站流量
- 防止私有實例接收來自互聯網的入站連接請求

公有路由表

目的地	目標
10.0.0.0/16	本地
0.0.0.0/0	<igw-id>

私有路由表

目的地	目標
10.0.0.0/16	本地
0.0.0.0/0	<nat-id>

要將私有子網中的實例連接到互聯網或其他 AWS 服務，您需要一個*網絡地址轉換 (NAT)* 閘道。利用 NAT 閘道，私有子網中的實例可以連接到互聯網或其他 AWS 服務，但會阻止互聯網發起與這些實例的連接。

要創建 NAT 閘道，您必須指定 NAT 閘道所處的公有子網。同時，還必須指定與該 NAT 閘道關聯的彈性 IP 位址。創建 NAT 閘道之後，必須更新與您的一個或多個私有子閘道聯的路由表，以便將流向互聯網的流量指向該 NAT 閘道。這樣，您的私有子網中的實例便可以與互聯網通信。

子網使用案例示例（第 1 個，共 2 個）

資料存儲實例

批次處理實例

後端實例

Web 應用程式實例

花點時間思考下，這些示例中的實例是應該放入公有子網還是私有子網中。

子網使用案例示例（第 2 個，共 2 個）

資料存儲實例 → 私有子網

批次處理實例 → 私有子網

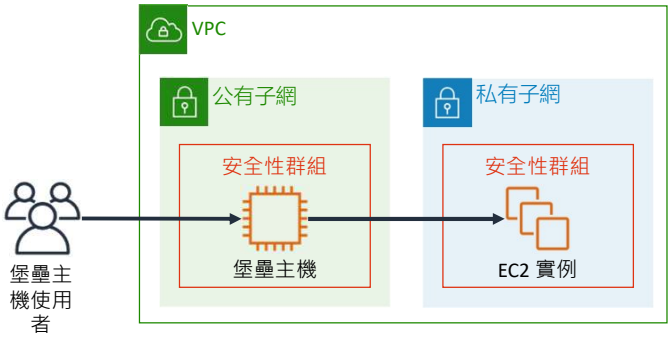
後端實例 → 私有子網

Web 應用程式實例 → 公有子網或私有子網

資料存儲實例、批次處理實例和後端實例應放入私有子網中。您可以將 Web 層實例放入公有子網中。但是，AWS 建議您將 Web 層實例放入*私有*子網中，並將其置於公有子網中的負載等化器之後。在某些環境中，您必須將 Web 應用程式實例直接掛載到彈性 IP 位址（不過您也可以將彈性 IP 位址掛載到負載等化器）。在這些情況下，Web 應用程式實例必須放入公有子網。

堡壘主機

- 用於從外部網路訪問私有網路的伺服器
- 必須儘量減少滲透的可能性



堡壘主機*是用於從外部網路（例如互聯網）訪問私有網路的伺服器。*您可以使用堡壘主機最大限度地降低滲透和潛在攻擊私有網路中的資源的可能性。

例如，假設您希望允許通過 Secure Shell 或 SSH 從外部網路連接到 VPC 私有子網中的 Linux 實例。

您可以使用堡壘主機來降低允許這些外部 SSH 連接到私有子網中實例的風險。堡壘主機通常在 VPC 的公有子網中的 EC2 實例上運行，如本示例所示。私有子網中的 Linux 實例位於安全性群組中，允許從附加到堡壘主機的安全性群組進行 SSH 訪問。堡壘主機使用者連接到堡壘主機，以便他們可以連接到 Linux 實例。

儘管您可以調整此架構來滿足自己的要求，但堡壘主機應該是 Linux 實例的唯一 SSH 流量來源。

有關此架構的更多資訊，請參閱博客文章 How to Record SSH Sessions Established Through a Bastion Host。要瞭解如何在 AWS 上的 VPC 環境中部署 Linux 堡壘主機，請完成 AWS 中的 Linux 堡壘主機 Quick Start。

演示：
創建 Virtual Private Cloud

現在，您的講師可能會選擇演示如何使用 Amazon VPC 手動創建包含子網、互聯網閘道和路由表的 VPC。

第 3 節要點

- 互聯網閘道允許 VPC 中的實例與互聯網進行通信。
- 路由表 控制來自子網或閘道的流量。
- 彈性 IP 地址是靜態公有 IPv4 位址，可以與實例或彈性網路介面關聯。它們可以重新映射到您帳戶中的另一個實例。
- NAT 閘道使私有子網中的實例可以發起到互聯網或其他 AWS 服務的出站流量。
- 堡壘主機是用於從外部網路（例如互聯網）訪問私有網路的伺服器。

本模組中這節內容的要點包括：

- 互聯網閘道允許 VPC 中的實例與互聯網進行通信。
- 路由表控制來自子網或閘道的流量。
- 彈性 IP 位址是靜態公有 IPv4 位址，可以與實例或彈性網路介面關聯。它們可以重新映射到您帳戶中的另一個實例。
- NAT 閘道使私有子網中的實例可以發起到互聯網或其他 AWS 服務的出站流量。
- 堡壘主機是用於從外部網路（例如互聯網）訪問私有網路的伺服器。

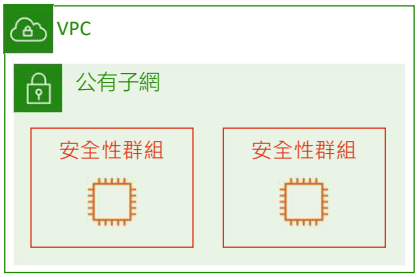
模組 6：創建聯網環境

第 4 節：保護 AWS 聯網環境

介紹第 4 節：保護 AWS 聯網環境

安全性群組

- 有狀態防火牆，可控制出入 AWS 資源的入站和出站流量
- 在實例或網路介面級別運行



現在，您已經知道如何設計和部署網路環境並將其連接到互聯網，您必須隔離您的應用程式和工作負載。

您可以通過來實現隔離：將託管您應用程式或工作負載的 EC2 實例部署到附加到您 VPC 的安全性群組中。

安全性群組是在實例或網路介面級別運行的有狀態防火牆。

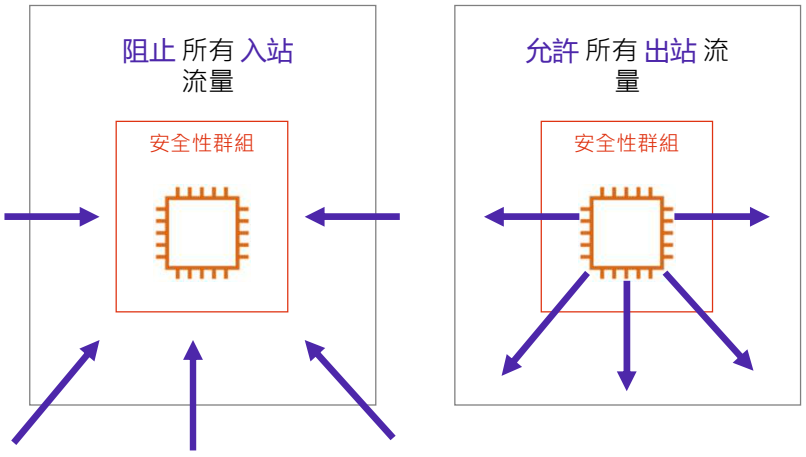
有狀態意味著，自動允許返回流量，不受規則影響。例如，假設您通過家用電腦對您的實例發起了互聯網控制消息協定 (ICMP) *ping* 命令。如果入站安全性群組規則允許 ICMP 流量，則系統會跟蹤有關連接的資訊（包括埠資訊）。實例對 ping 命令的回應流量不會作為新請求進行跟蹤，而是作為已建立的連接進行跟蹤。即使出站安全性群組規則限制了出站 ICMP 流量，也將允許從實例流出。

安全性群組規則控制出入您的 AWS 資源的入站和出站流量。您應該嚴格配置這些規則，以限制流量並僅在需要時允許訪問。流量可以受任何互聯網協定、服務埠以及源或目標 IP 位址（單個 IP 位址或 CIDR 塊）的限制。

並非所有的流量流都會被跟蹤。假設一個安全性群組規則允許所有流量（即 0.0.0.0/0）的傳輸控制協議 (TCP) 或使用者資料包通訊協定 (UDP) 流。另一個方向還有一個允許響

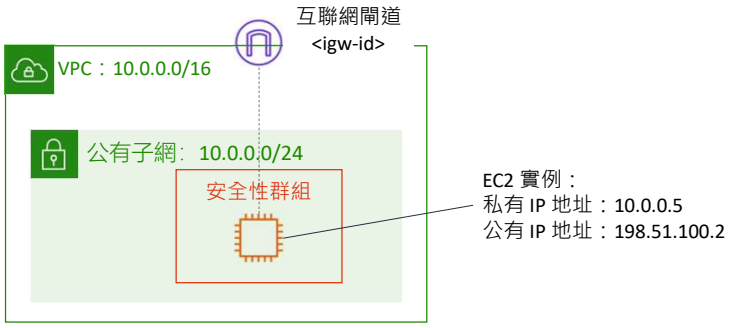
應流量的相應規則。在這種情況下，不會跟蹤該流量流。因此，允許回應流量基於允許回應流量的入站或出站規則流動，而不是基於跟蹤資訊流動。

默認安全性群組



當您創建一個安全性群組時，它沒有入站規則。這意味著，您必須向安全性群組添加入站規則，以允許來自另一台主機的入站流量進入您的實例。默認情況下，安全性群組包含*允許所有出站流量*的出站規則。您可以刪除該規則並添加只允許特定出站流量的出站規則。如果您的安全性群組沒有出站規則，則系統將不允許來自您實例的任何出站流量。

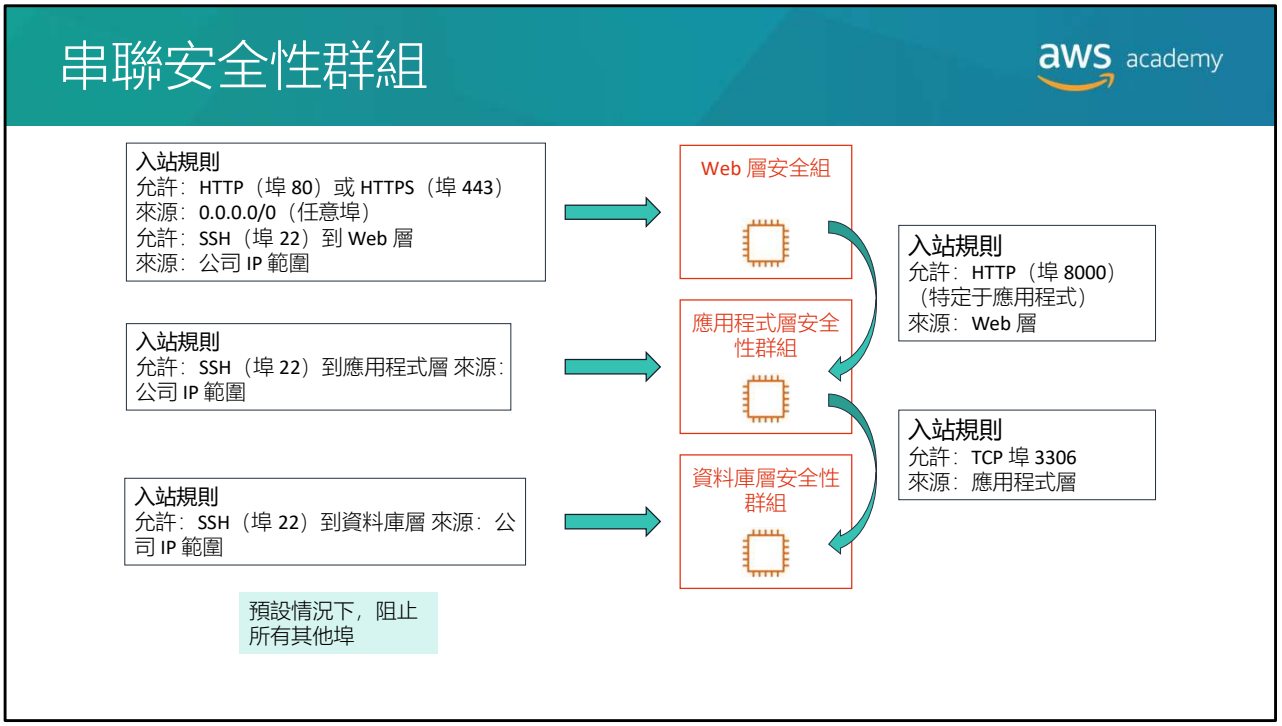
自訂安全性群組



入站				
類型	協議	埠範圍	源	目的地
HTTP	TCP	80	任何位置	允許 Web 訪問

創建自訂安全性群組時，您可以指定*允許*規則，但不可以指定*拒絕*規則。例如，當您為托管 Web 應用程式的實例創建公有子網時，最後一步是創建允許向這些實例發送 HTTP 流量的安全性群組。

在做出允許流量的決定之前評估所有規則。

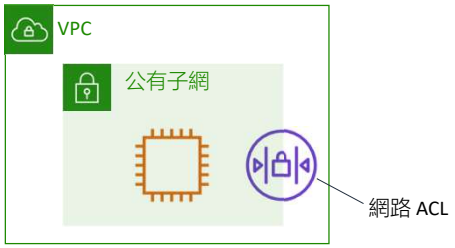


大多數雲組織創建的安全性群組都會為每個功能層設置入站規則。此示例顯示了典型的三層應用程式中的安全性群組鏈。入站和出站規則的設置方式為，僅允許流量從頂層流向底層，然後再流回。安全性群組將充當防火牆，防止分層中的安全性漏洞自動為受影響的用戶端提供針對所有資源的子網範圍存取權限。

安全性群組可以配置為針對不同類別的實例設置不同的規則。思考下這個 Web 應用程式的傳統三層架構的示例。用於 Web 伺服器的組將具有對互聯網開放的埠 80 (HTTP) 或埠 443 (HTTPS)。用於應用程式伺服器的組將具有僅供 Web 伺服器組訪問的埠 8000（特定于應用程式）。用於資料庫伺服器的組將具有僅對應用程式伺服器組開放的埠 3306 (MySQL)。這三個組均允許埠 22 (SSH) 上的管理訪問，但只能從客戶的公司網路訪問。此機制可以實現高度安全應用程式的部署。

網路存取控制清單（網路 ACL）

- 在子網級別運行
- 預設情況下允許所有入站和出站流量
- 無狀態防火牆，要求針對入站和出站流量設置顯式規則



網路存取控制清單（網路 ACL）*是 VPC 的可選安全層。*它充當防火牆，用於控制進出一個或多個子網的流量。 要向您的 VPC 添加額外的安全層，您可以使用類似於安全性群組的規則設置網路 ACL。

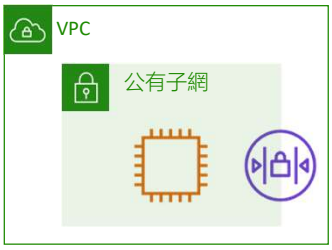
您的 VPC 中的每個子網都必須與一個網路 ACL 相關聯。如果您沒有將某個子網與一個網路 ACL 顯式關聯，則該子網將自動與預設網路 ACL 關聯。您可以將網路 ACL 與多個子閘道聯。但是，一個子網一次只能與一個網路 ACL 關聯。當您將一個網路 ACL 與一個子閘道聯時，之前的關聯將被刪除。

網路 ACL 有單獨的入站和出站規則，每項規則都可以允許或拒絕流量。您的 VPC 自動帶有可修改的預設網路 ACL。預設情況下，它允許所有入站和出站 IPv4 流量以及 IPv6 流量（如果適用）。

網路 ACL 是*無狀態的*，這意味著在處理請求後，不會保留有關請求的資訊。必須通過規則顯式允許返回流量。

自訂網路 ACL

建議
僅限特定網路安全要求



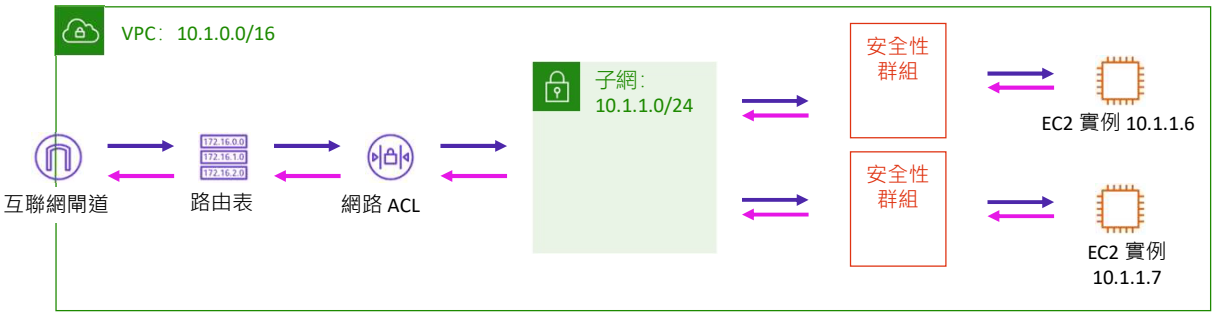
Nacl-11223344

入站:
規則 # 100：SSH 172.31.1.2/32 允許
規則 # *：所有流量 0.0.0.0/0 拒絕

出站:
規則 # 100：自訂 TCP 172.31.1.2/31 允許
規則 # *：所有流量 0.0.0.0/0 拒絕

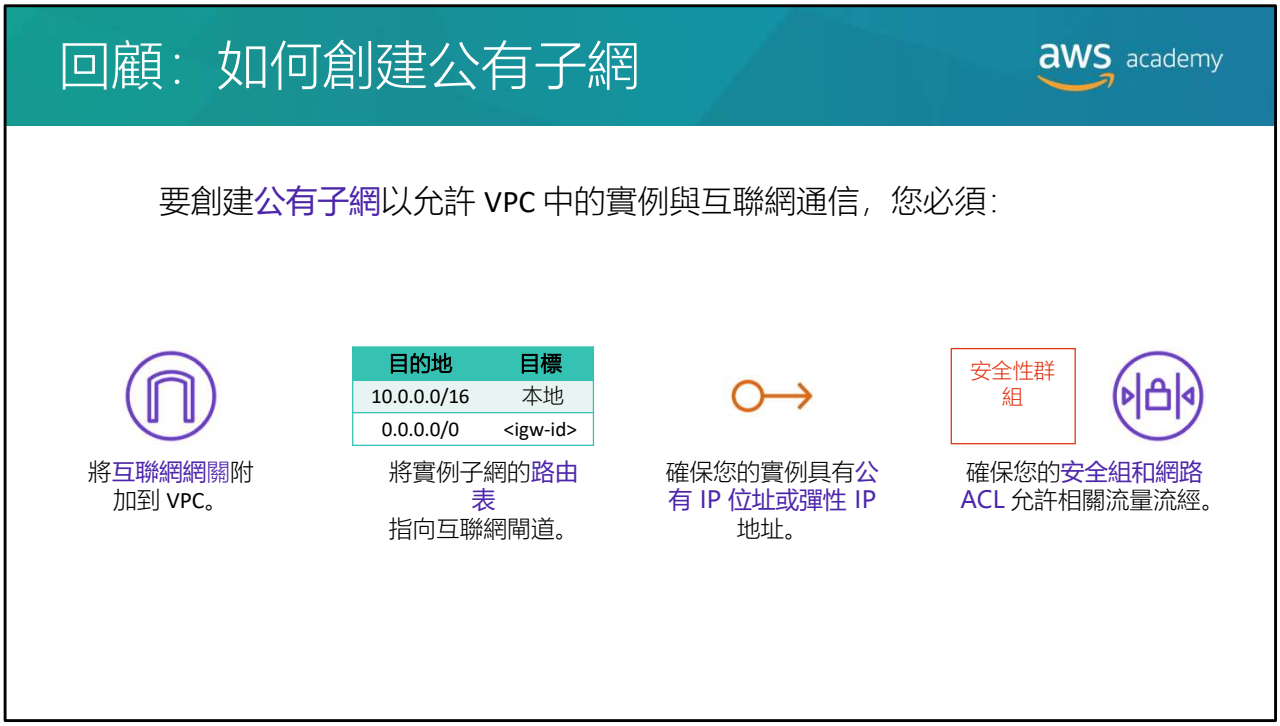
您可以創建*自定義*網絡 ACL 並將其與子網相關聯。預設情況下，每個自定義網絡 ACL 將拒絕所有入站和出站流量，直至您添加相關規則。

使用多層防護構建基礎設施



作為最佳實踐，您應該使用多層防護保障您的基礎設施安全。通過在 VPC 中運行基礎設施，您可以控制將哪些實例對互聯網開放。您可以定義安全性群組和網路 ACL，以便分別在基礎設施和子網級別進一步保護您的基礎設施。此外，您應該使用防火牆在作業系統級保障您的實例安全，並遵循其他安全性最佳實踐。

在同時實施網路 ACL 和安全性群組作為控制流量的深度防禦方法時，即使某項控制措施的配置出現錯誤的情況下，主機也不會遭遇不需要的流量。



回顧一下，要創建公有子網以允許 VPC 中的實例與互聯網進行通信，您必須：

- 將互聯網閘道附加到 VPC。
- 將路由添加到您子網的路由表，該路由表將流向互聯網的流量定向到互聯網閘道
- 確保您的實例具有公有 IP 位址或彈性 IP 位址
- 確保您的安全性群組和網路 ACL 允許相關流量流經

第 4 節要點

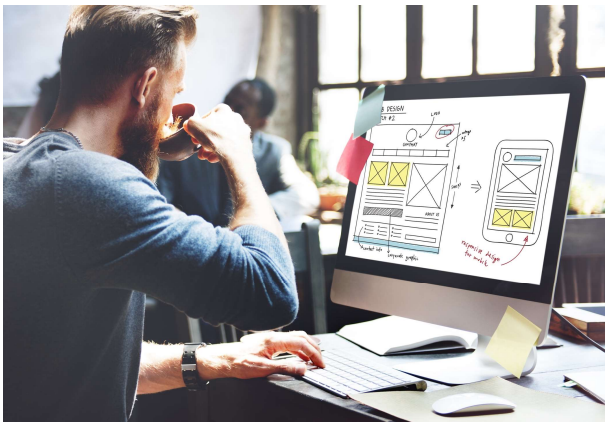
- 安全性群組是在實例級別運行的有狀態防火牆
- 網路 ACL 是在子網級別運行的無狀態防火牆
- 當您設置入站和出站規則以允許流量從架構的頂層流向底層時，您可以將安全組串聯在一起來隔離安全性漏洞
- 您應使用多層防護構建基礎設施

本模組中這節內容的要點包括：

- 安全性群組是在實例級別運行的有狀態防火牆
- 網絡 ACL 是在子組級別運行的無狀態防火牆
- 當您設置入站和出站規則以允許流量從架構的頂層流向底層時，您可以將安全性群組串聯在一起來隔離安全性漏洞
- 您應使用多層防護構建基礎設施

模組 6 – 指導實驗：創建 Virtual Private Cloud

aws academy



您現在將完成模組 6 – 指導實驗：創建 Virtual Private Cloud。

指導實驗：任務

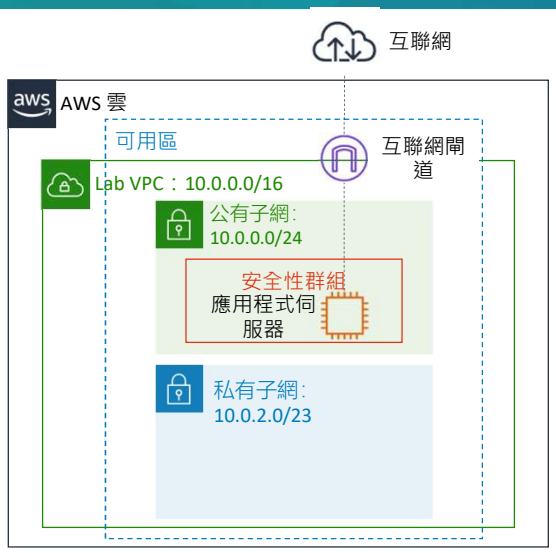
使用 Amazon VPC 手動創建 VPC，其中包括：

- 公有子網和私有子網
- 一個互聯網閘道
- 一個路由表，包含將流向互聯網的流量定向至互聯網閘道
- 一個針對公有子網中 EC2 實例的安全性群組
- 一個測試 VPC 的應用程式伺服器

在本實驗中，您將使用 Amazon VPC 手動創建具有以下元件的 VPC：

- 公有子網和私有子網
- 一個互聯網閘道
- 一個路由表，包含將流向互聯網的流量定向至互聯網閘道
- 一個針對公有子網中 EC2 實例的安全性群組
- 一個測試 VPC 的應用程式伺服器

指導實驗：最終產品



該圖總結了您完成實驗後將會構建的內容。

大約 30 分鐘

現在可以開始指導實驗了。

指導實驗總結：要點

完成這個指導實驗之後，您的講師可能會帶您討論此指導實驗的要點。

模組 6 – 挑戰實驗：為咖啡館創建 VPC 聯網環境

您現在將完成模組 6 – 挑戰實驗：為咖啡館創建 VPC 聯網環境。

業務需求：安全的聯網環境

Sofía 和 Nikhil 已將咖啡館的資料庫層與 Web 應用程式層分開。他們還將資料庫資源從公有子網移動到了私有子網。

Mateo 建議他們通過與資料庫實例相互獨立的私有子網中運行咖啡館的應用程式伺服器，以便增強安全性。

Sofía 和 Nikhil 成功創建了一個雙層架構，他們在這個架構中將咖啡館的資料庫層與 Web 應用程式層分開。他們還將資料庫資源從公有子網移動到了私有子網。

Mateo 建議他們在與資料庫實例相互獨立的私有子網中運行咖啡館的應用程式伺服器，來增強 VPC 的安全性。

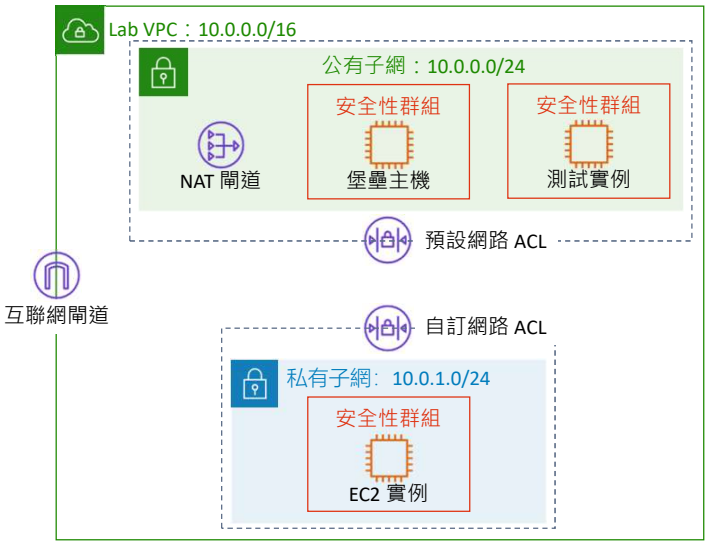
挑戰實驗：任務

1. 創建公有子網
2. 創建堡壘主機
3. 為堡壘主機分配彈性 IP 位址
4. 測試與堡壘主機的連接
5. 創建私有子網
6. 創建 NAT 閘道
7. 在私有子網中創建 EC2 實例
8. 為 SSH 傳遞配置 SSH 用戶端
9. 測試與堡壘主機的 SSH 連接
10. 創建網路 ACL
11. 測試自定義網路 ACL

在本挑戰實驗中，您將完成以下任務：

1. 創建公有子網
2. 創建堡壘主機
3. 為堡壘主機分配彈性 IP 位址
4. 測試與堡壘主機的連接
5. 創建私有子網
6. 創建 NAT 閘道
7. 在私有子網中創建 EC2 實例
8. 為 SSH 傳遞配置 SSH 用戶端
9. 測試與堡壘主機的 SSH 連接
10. 創建網路 ACL
11. 測試自定義網路 ACL

挑戰實驗：最終產品



該圖總結了您完成實驗後將會構建的內容。

現在可以開始挑戰實驗了。

挑戰實驗總結：要點

完成這個挑戰實驗之後，您的講師可能會帶您討論此挑戰實驗的要點。

模組 6：創建聯網環境

模組總結

現在來回顧下本模組，並對知識測驗和對實踐認證考試問題的討論進行總結。

模組總結

aws academy

總體來說，您在本模組中學習了如何：

- 說明 AWS 雲聯網中 VPC 的基本功能
- 確定如何將 AWS 聯網環境連接到互聯網
- 描述如何在 AWS 聯網環境中隔離資源
- 創建包含子網、互聯網閘道、路由表和安全性群組的 VPC

總體來說，您在本模組中學習了如何：

- 說明 AWS 雲聯網中 VPC 的基本功能
- 確定如何將 AWS 聯網環境連接到互聯網
- 描述如何在 AWS 聯網環境中隔離資源
- 創建包含子網、互聯網閘道、路由表和安全性群組的 VPC

完成知識測驗

現在可以完成本模組的知識測驗。

樣題

aws academy

您有一個應用程式，在單個可用區中的多個 Amazon Elastic Compute Cloud (Amazon EC2) 實例上運行。該應用程式通過互聯網調用協力廠商應用程式設計發展介面 (API)。

如何為協力廠商 API 提供單個 IP 位址以添加到訪問安全列表中？

A. 為實例分配彈性 IP 位址。
B. 為實例分配公有 IP 地址。
C. 將實例置於 NAT 閘道之後。
D. 將實例置於 Network Load Balancer 之後。

思考答案選項，並根據之前突出顯示的關鍵字排除錯誤選項。

正確答案是 C： *"將實例置於 NAT 閘道之後。"* 可以排除選項 A 和 B，因為應用程式最終將擁有多個公有 IP 位址，而安全列表只需要一個 IP 位址。也可以排除選項 D，因為 Network Load Balancer 也將擁有多個 IP 位址。選項 C 是正確的，因為 NAT 閘道可以通過單個 IP 位址訪問。

其他資源

- VPC 和子網
- 從一個到多個：VPC 設計的演進
- AWS 單個 VPC 設計
- AWS re:Invent 2018：您的虛擬資料中心：VPC 基礎知識和連接選項
- AWS 聯網基礎知識

如果您想瞭解有關本模組所涵蓋主題的更多資訊，下面這些其他資源可能會有所幫助：

- VPC 和子網
- 從一個到多個：VPC 設計的演進
- AWS 單個 VPC 設計
- AWS re:Invent 2018：您的虛擬資料中心：VPC 基礎知識和連接選項
- AWS 聯網基礎知識

感謝您完成本模組的學習。