技能解封初始篇章-安全閘門重鎮(NSG & ASG)

前言

網路安全性群組中的安全性規則能讓您篩選可在虛擬網路子網路及網路介面中流入和流出的網路流量類型。

前置作業：

* 如果尚未註冊過 Azure 可以來免費試用一個月200美金額度。
* 如用入口網站透過 https://portal.azure.com ，用你註冊申請的 Azure 帳戶登入。
* 如想使用 PowerShell 實測，可透過 Azure Cloud Shell 並切換成 PowerShell 執行命令或從你自己的電腦執行 PowerShell。(需要安裝針對 Azure 所屬的 PowerShell 模組)
* 最後如想用 CLI 實測，則可透過 Azure Cloud Shell 切換成 CLI 模式執行命令或從你自己的電腦執行 CLI。(需要安裝針對 Azure 所屬 CLI 模組)

成本評估

網路安全群組與應用程式安全群組(完全免費僅需注意本身單一訂閱下對於此資源的數量限制)

一張含有 文字 的圖片

自動產生的描述

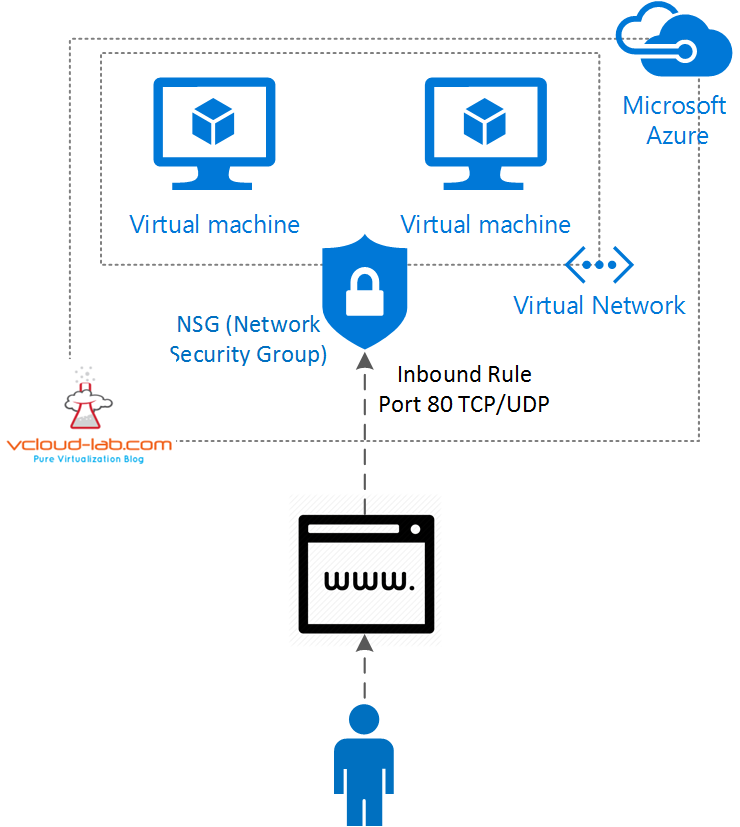
**安全群組 Q&A**

* 預設安全性規則會封鎖來自網際網路的輸入存取，並只允許來自虛擬網路進入流量。 如需要允許來自網際網路流量進入則變更優先序高於預設規則安全性規則即可。
* 如果有對等互連的虛擬網路，**VIRTUAL\_NETWORK** 服務標籤預設會自動開啟適用於對等互連虛擬網路的前置詞。 如需虛擬網路對等互連相關問題進行處理可透過 **ExpandedAddressPrefix** 清單中檢視前置詞。
* 有效安全性規則生效須在有 NSG 已關聯至 VM 的網路介面或子網路且 VM 處於執行中。
* 如沒有 NSG 關聯至網路介面或子網路且以將 Public IP 指派給 VM，則預設所有連接埠全開並可任意地點對它進行進出存取。

服務架構

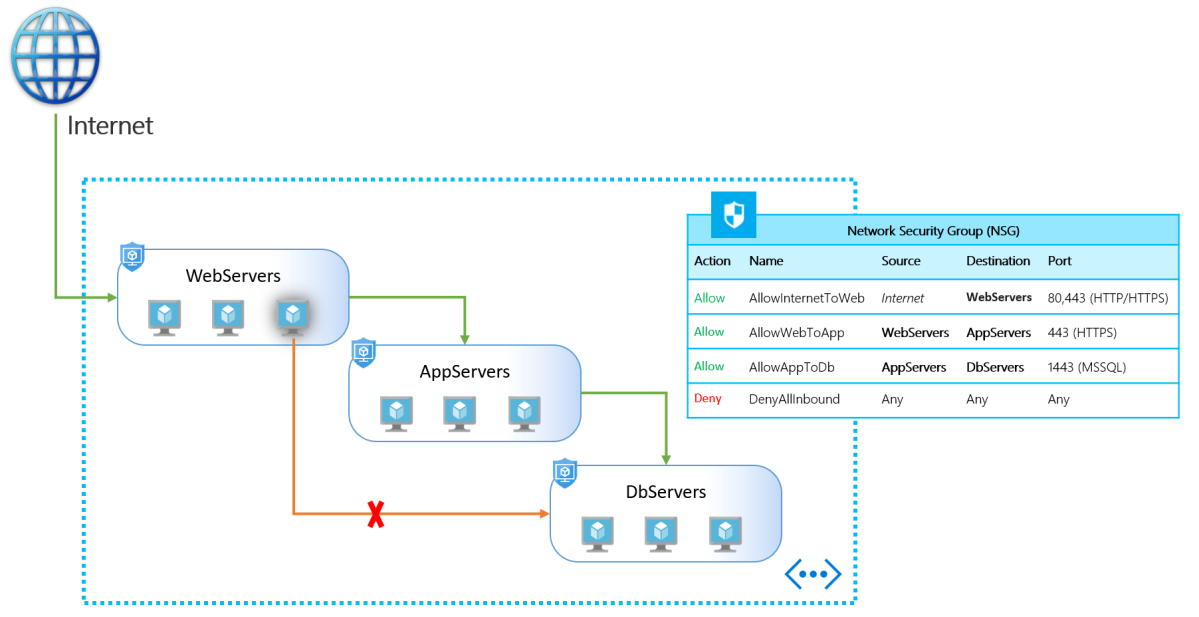
**網路安全群組架構**

透過 NSG 當作一道進出入開關的閥門針對來源到目的以及什麼協定及連接埠範圍作明確的規則限制，圖中範例就是兩台 VM 作為對外網站服務並僅允許http 80 Port 連線進入(就是像白名單其實沒有寫到的則一律把封包 Drop 掉)



**應用程式安全架構**

從圖中可以得知原本套用至目的端主機需要一台台重複套用可以透過ASG群組標籤直接將相同性質的後端主機服務直接套用即可，除了管理面上設置方便很多外，還可以在同一組NSG分別擁有不同的存取限制需求都能分別套用至不同目標主機中。



簡易環境示範

圖1. 檢視原來已經準備好在同一地區的兩台虛擬機器並已經啟用IIS網站服務

一張含有 桌 的圖片

自動產生的描述

圖2. 確認第一台無套用NSG規則

一張含有 文字 的圖片

自動產生的描述

圖3.  確認第二台無套用NSG規則

一張含有 文字 的圖片

自動產生的描述

圖4. 瀏覽第一台虛擬機器預設網站確認服務正常

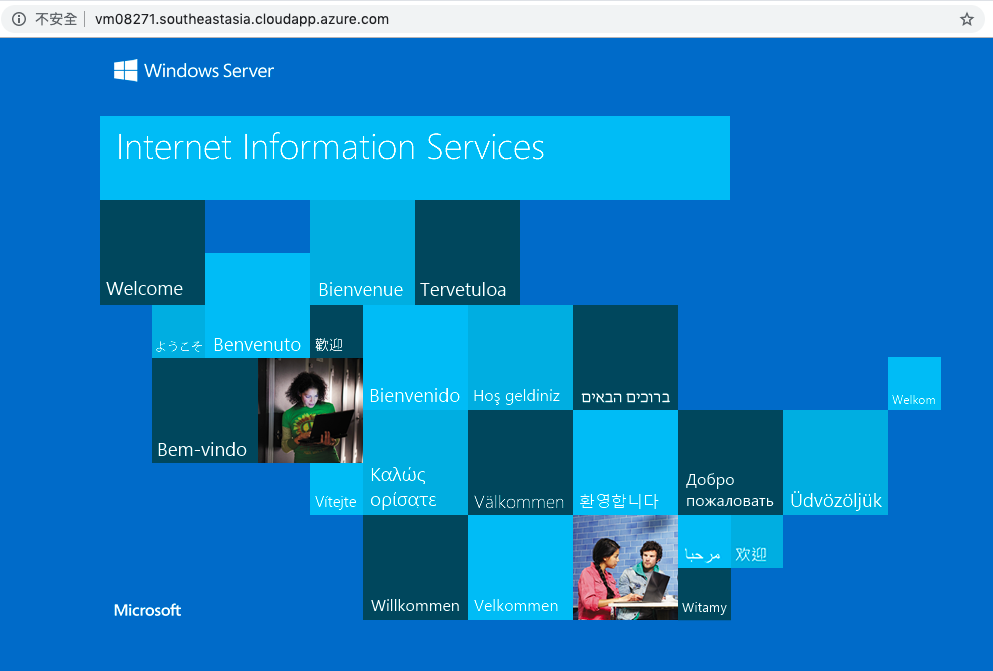


圖5.  瀏覽第二台虛擬機器預設網站確認服務正常

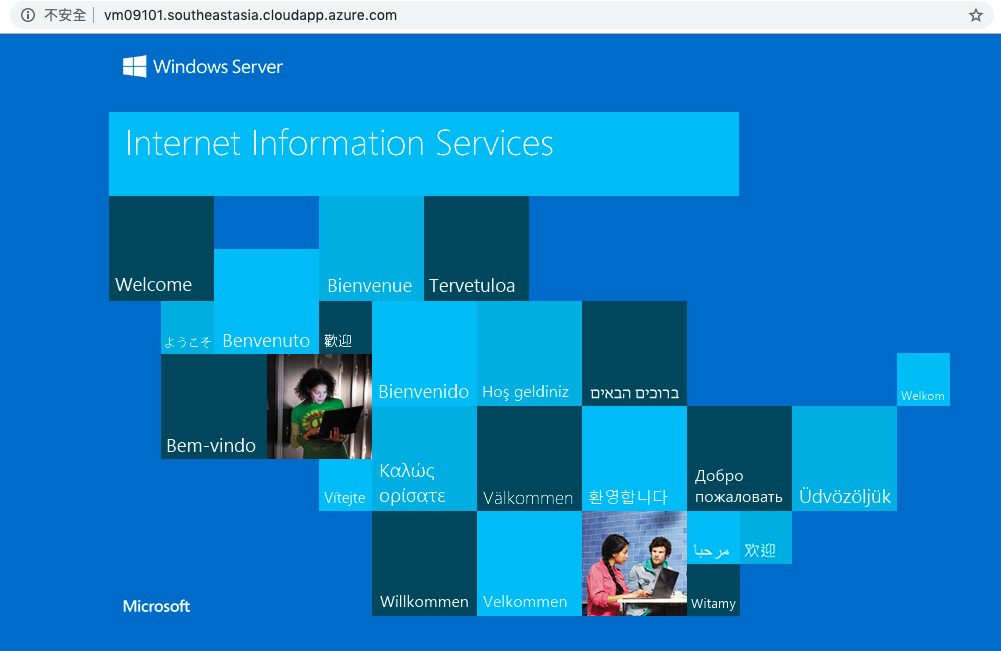


圖6.  確認現行我自己的電腦對外Public IP (請記住它)

一張含有 文字 的圖片

自動產生的描述

圖7.  開始正題找到 ASG 服務並選擇與虛擬機器相同地區

一張含有 文字 的圖片

自動產生的描述

圖8. ASG 建立完成

一張含有 文字 的圖片

自動產生的描述

圖9.  先前準備好的 NSG 並原有就建立好 RDP 與 Http 是 Any 允許狀態

一張含有 文字, 收據, 螢幕擷取畫面 的圖片

自動產生的描述

圖10.  我們改變一下把第一條 RDP 規則來源 IP 縮限僅允許剛剛所記住的 Public IP 才能允許，另外目的端也從原來 Any 改成剛剛建立好的 ASG

一張含有 桌 的圖片

自動產生的描述

圖11.  此 RDP 規則已經套用 ASG 完成

一張含有 桌 的圖片

自動產生的描述

圖12.  回到第一台虛擬機器進到網路切換到應用程式安全群組並選擇剛剛所設置的 ASG

一張含有 文字 的圖片

自動產生的描述

圖13. 套用完成(第二台方式亦同故不在重複呈現)

一張含有 文字 的圖片

自動產生的描述

圖14. 再確認一次在允許的 Public IP 下做RDP連線登入均正常一張含有 文字, 螢幕擷取畫面, 監視器, 室內 的圖片

自動產生的描述

圖15. 切至4G網路上網讓對外的 Public IP  變更

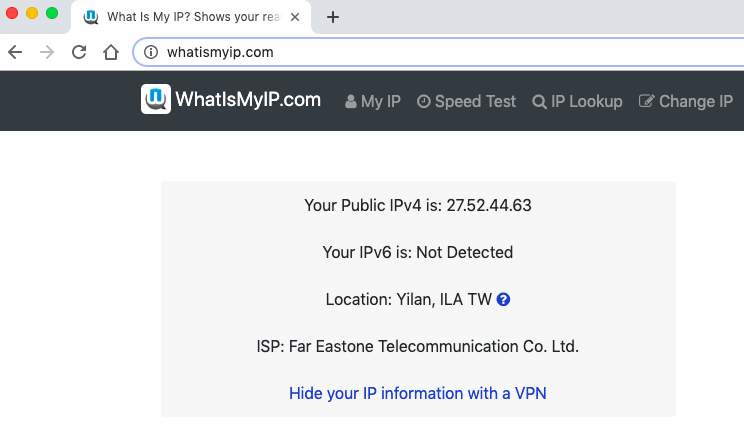
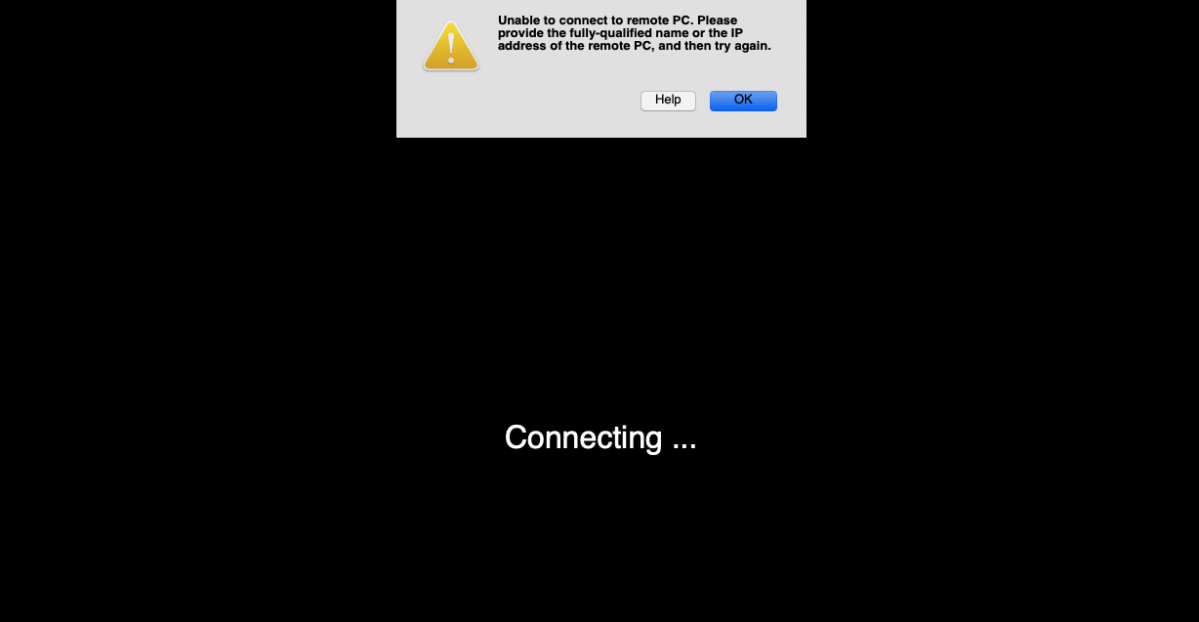


圖16. 再重新做 RDP 連線就發現封包已經被終止不被允許



**進階流量分析檢視設置示範**

圖17.  再來是進階的設定示範，在剛剛的 NSG 服務的刀鋒視窗最下面有流程紀錄檔設置需做啟用並把 Log 放置指定儲存體帳戶中，而流量分析部份也需要啟用 Log 分析服務才能讓 NSG 的 Log能有效的被產出視覺顯示

一張含有 文字 的圖片

自動產生的描述

圖18.  另外診斷紀錄會是 NSG 故障排除的部份也需要設置並選擇丟到剛剛 Log 分析的地方

一張含有 文字 的圖片

自動產生的描述

圖19. 診斷設置完成



圖20. 流量紀錄也已啟用完成



圖21. 再到網路監看員服務確認是否啟用了所想要監視的地區如：我這邊的示範為東南亞

一張含有 文字 的圖片

自動產生的描述

圖22. 最後點選流量分析(圖中也很明顯告知它是需要時間做資料搜集分析的)故要等待

一張含有 文字 的圖片

自動產生的描述

圖23. 初步檢視畫面如下就會包含到可視化的網路進出流量以及每個流量的分析狀態



圖24. 這是點選左上的地圖功能就可以視覺化整個網路封包狀態



圖25. 不過其實我為了測試要有流量RDP與瀏覽網站都是連線中的….這以下的所有網路資料應該並非即時目前看來不是正確地顯示，明天再來檢視看看嘍！

一張含有 文字 的圖片

自動產生的描述