技能解封初始篇章-對空對地的坦克巨塔(Firewall)

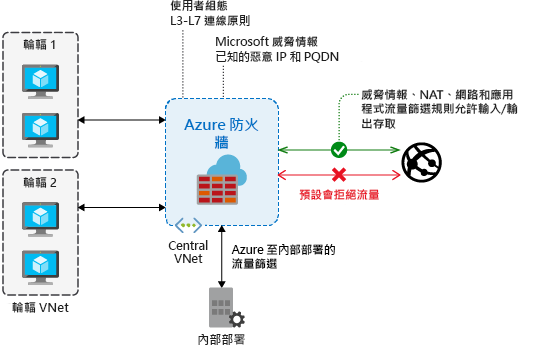
前言

Azure 防火牆是一個全託管的網路層級的資安服務，涵蓋範圍是以您的 Azure 虛擬網路下的資源為主要保護範圍。涵蓋 L4-L7 的 FaaS(Firewall as a Service)防火牆即服務，同時符合內建就有的高可用以及不受限的擴展延展。

Azure 防火牆本身具有以下重要特色：  
\* 防火牆本身就具高可用性。  
\* 支援可用性區域。(可減少負載平衡服務設置，同時可跨多個可用性區域提升保護)  
\* 不受限的水平擴展。  
\* 應用程式 FQDN 過濾防護。  
\* 網路流量篩選。  
\* 威脅情報警示並可直接 Drop 已知的惡意IP流量。(此判斷來自微軟的威脅情報判別)  
\* 來源與目的網路位址轉譯。(SNAT/DNAT)  
\* Azure Monitor 集中整合記錄分析。

如圖中所示，透過對整個虛擬網路的保護下都能夠判別L4-L7層的流量是否為惡意再作進一步的防護動作讓後端的虛擬機器真正在上面對外的應用服務都能夠安全無虞。

圖一.



Azure Firewall 把玩前成本計價須知

**防火牆部署 (固定費用)**

每個防火牆部署 NT$37.568/小時

**資料處理 (變動費用)**

每 GB NT$0.481 由防火牆處理。

Azure Firewall Q&A

**Azure 防火牆部署方式是什麼？**

可將Azure 防火牆部署在任何虛擬網路上，但一般用戶通常會將其部署當一個虛擬網路中心，在以中樞和支點方式與其他虛擬網路對等互連。 接著就可從對等互連的虛擬網路設定預設路由，指向此虛擬網路防火牆中心。

我們本身支援全域 VNet 對等互連，但不建議使用，因為跨區連線會發生效能和延遲問題。 為了達到最佳效能, 請為每個區域部署一個防火牆。

**Azure 防火牆主要有哪些規則概念？**

* 應用程式規則：設定可從子網存取的完整功能變數名稱 (Fqdn)。
* 網路規則：設定包含來源位址、通訊協定、目的地埠及目的地位址的規則。
* NAT 規則:設定 DNAT 規則以允許連入連接。

**Azure 防火牆運作方式與市集中如 ：NVA 服務有何不同？**

Azure 防火牆是一種基本防火牆，可處理特定客戶實例但並非取代。 建議可以視需求混合使用協力廠商 NVA 和 Azure 防火牆。使用首重相輔相成。

**應用程式閘道 WAF 與 Azure 防火牆有什麼不同？**

Web 應用程式防火牆 (WAF) 是應用程式閘道中一個功能，可供 Web 集中式進入保護，避免遭到常見惡意攻擊。Azure 防火牆可針對非 HTTP/S 通訊協定如： RDP、SSH、FTP 等..協定供輸入保護、為所有通訊協定 / 連接埠供輸出網路層級保護以及為輸出 HTTP/S 供 Web 層級保護。

**網路安全性群組 (NSG) 和 Azure 防火牆有什麼不同？**

Azure 防火牆可補足網路安全性群組功能。 兩者結合時，可供更好的”深度防禦“網路安全性。 網路安全性群組供分散式網路層流量篩選，可限制虛擬網路內資源的流量。

Azure 防火牆完全具狀態的集中式網路防火牆即服務，可跨不同訂用帳戶和虛擬網路，供網路層級和應用程式層級的保護。

**如何使用我的服務端點設定 Azure 防火牆？**

要安全存取 PaaS 服務，建議使用服務端點。 你可選擇在Azure 防火牆子網路中啟用服務端點，並在已連線的支點虛擬網路上停用它。 如此你就可享有這兩項功能的好處 — 服務端點安全性和所有流量的集中記錄。

**是否有任何防火牆資源群組的限制？**

防火牆、子網路、VNet 和公用 IP 位址全都必須在相同的資源群組中。

**為什麼 Azure 防火牆需要/26 個子網大小？**

**Azure 防火牆**在調整規模時布建更多虛擬機器 instance。 /26 位址空間可確保防火牆有足夠的 IP 位址可容納調整。

前置作業

虛擬子網路需指定名稱為AzureFirewallSubnet (並不能與其他資源混用)

欲先建立一組使用者自定路由 (UDR)

簡易實驗環境示範

圖1. 確認防火牆子網路已經預先建立

一張含有 桌 的圖片

自動產生的描述

圖2. 目前沒有任何防火牆服務

一張含有 文字 的圖片

自動產生的描述

圖3. 可以有支援區域備援(剛好LAB手癢就來個1,2)吧



圖4. 選擇已有的虛擬網路(剛剛有防火牆子網路的),另外也會有一組對外Public IP



圖5. 建立完成

一張含有 文字 的圖片

自動產生的描述

圖6. 威脅情報預設是警示,要攔截請選擇最右邊

一張含有 文字 的圖片

自動產生的描述

圖7. 檢視一下要能來做測試標的的虛擬機器,包含公私有IP記一下

一張含有 文字 的圖片

自動產生的描述

圖8. 將UDR新增一筆路由下一跳到防火牆做判別

一張含有 文字 的圖片

自動產生的描述

圖9. 原本虛擬機器的子網路套用都是預設路由,但是我們要讓防火牆擋在進出網際網路中間故需要把下一站的路由位置改到防火牆私有IP上

一張含有 文字 的圖片

自動產生的描述

圖10. 我們從此虛擬網路的網卡中檢視有效路由就可以看到中間那行到網際網路已經被我的UDR取代了

一張含有 桌 的圖片

自動產生的描述

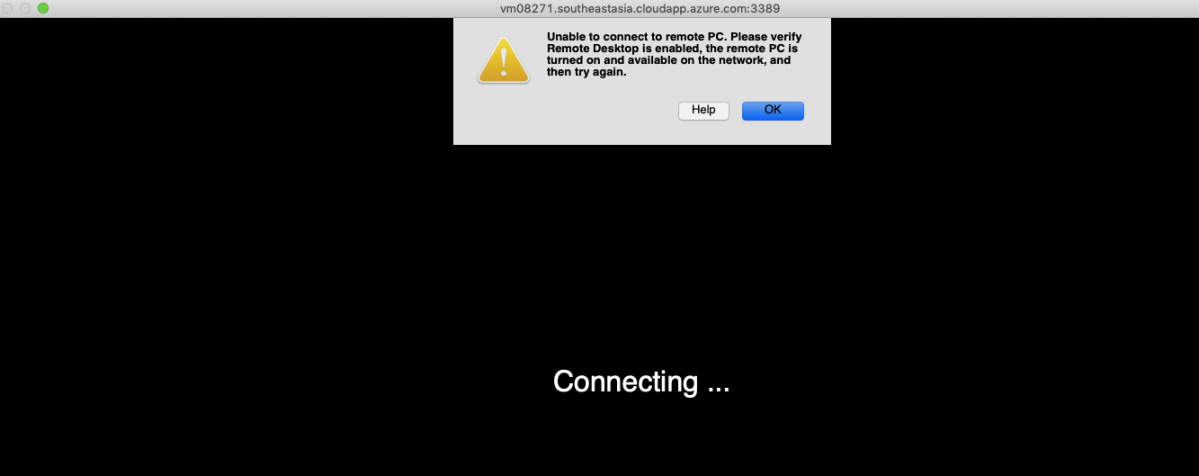
圖11. 因為已經被防火牆取代RDP也斷了….記得剛剛不是有DNAT嗎！

圖12. 設定我們要測試的主角拿一個Amazon的URL作為Deny為例(因為我們是Azure……哈哈)

一張含有 文字 的圖片

自動產生的描述

圖13. 另外也設定一筆指定對外能解析DNS紀錄的來源

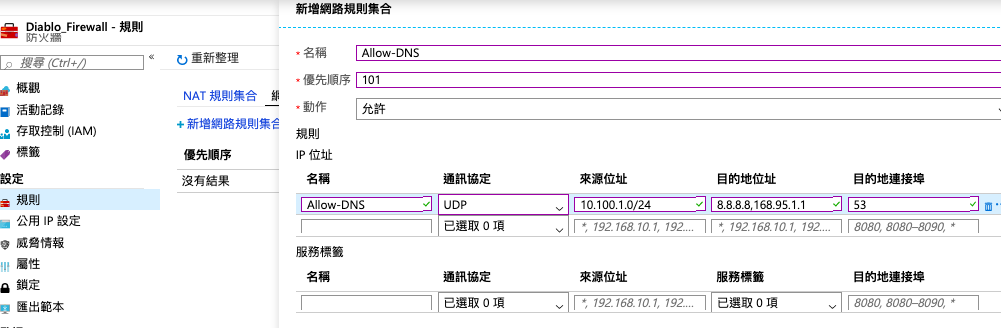


圖14. 因為已經變成從防火牆發起,DNS也需要從虛擬機器的網卡上變更

一張含有 文字 的圖片

自動產生的描述

圖15. 最後設定剛剛提到的DNAT,需要透過防火牆來找到後端指定的連線主機位置

一張含有 文字 的圖片

自動產生的描述

**PS：生肖都需要幾分鐘的時間,另外提醒每一組的規則都需要等另一個規則生效後再去儲存不然就會顯示衝突失敗**

圖16. 最後就又可以在RDP連線登入進去剛剛的虛擬機器桌面

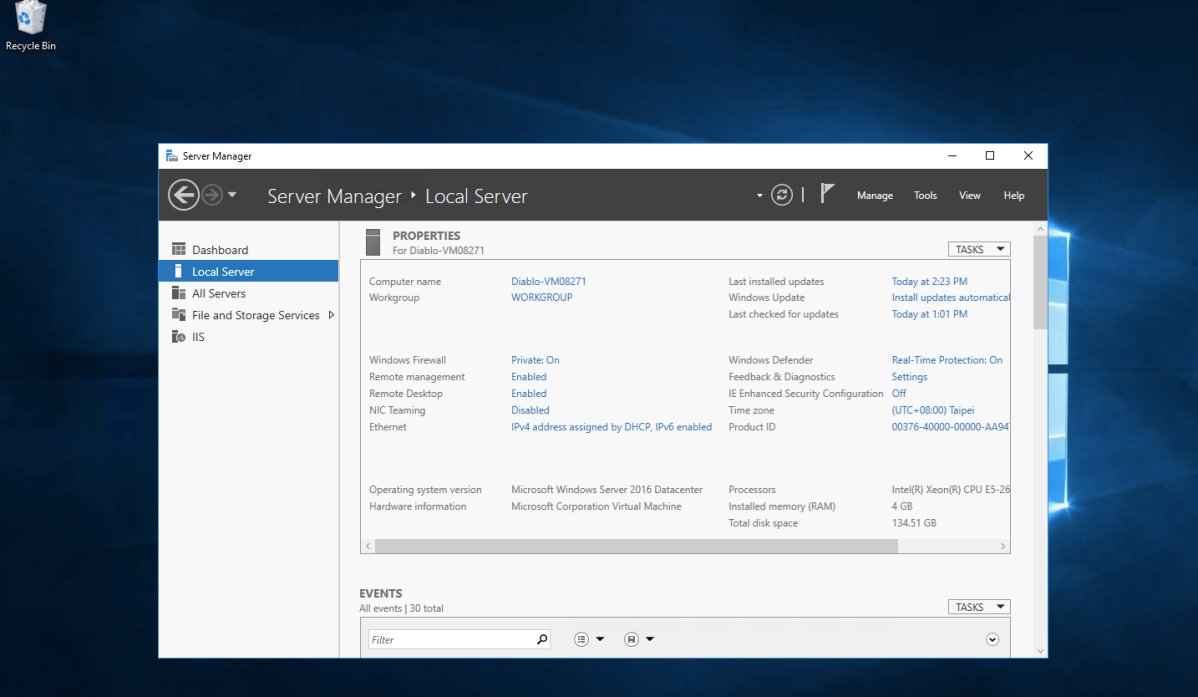


圖17. 最後測試amazon.com的網址也的確被防火牆做阻擋

一張含有 文字 的圖片

自動產生的描述