技能解封初始篇章-分散式阻斷洪流攻擊防禦 (DDoS)

前言

<https://ithelp.ithome.com.tw/articles/10213744>

介紹 Microsoft Azure DDoS 服務優勢

1. 簡化設定啟用 Azure DDoS 保護能涵蓋同一個虛擬網路上的所有資源。
2. Always On 流量監視供接近即時的 DDoS 攻擊偵測，且無需任何操作。每當偵測到攻擊後，立即自動降低攻擊的風險。
3. DDoS 保護供進階智慧，可自動設定調整 DDoS 保護。供智慧型流量分析來了解一段時間內的應用程式流量模式。
4. DDoS 保護可啟用Azure 應用程式閘道中WAF功能來防止全面第三/四傳輸網路層攻擊外，也同時避免 Web 應用第七層服務的攻擊如：SQL 插入式攻擊、跨網站指令碼攻擊和工作階段劫持。
5. Web 應用程式防火牆已經過預先設定，可處理 Open Web Application Security Project 認定的前十大常見弱點威脅。
6. 與 Azure 監視原生整合直接能檢視公開攻擊計量和遙測以及其他資源遙測。彈性警示機制會在應用程式受到攻擊時通知所指定的管理者。
7. 攻擊期間可取得以五分鐘為增量的詳細報告，在攻擊結束後取得完整摘要。將 DDoS 風險降低流量記錄串流至離線安全性資訊與事件管理 (SIEM) 系統，以便在攻擊期間進行近乎即時的監視。
8. 若因發生已記錄的 DDoS 攻擊而產生資源費用，可收取服務點數。

**攻擊模式主要有二：**  
頻寬消耗型攻擊

* User Datagram Protocol floods
* ICMP floods
* ping of death

資源消耗型攻擊

* SYN flood
* LAND Attack
* CC Attack
* C&C Attack
* Application level floods

**而實際能防堵方式常見如下：**

* 防火牆(透過規則如：允許或拒絕特定通訊協定，端口或IP Address。當攻擊從不正常IP發出時，可透過拒絕規則阻止從攻擊來源IP發出的需求通訊)
* 交換機(主要是為了能流量控制或IP封包過濾等．．．)
* 路由器(功能同上述能達到像交換機的目的)
* 黑洞導引(將所受攻擊電腦主機通信全發送至一個“黑洞”(簡單說就是一個不存在的主機IP地址)
* 流量清洗(當發生異常大流量攻擊時會被送到DDoS清洗中心，將正常流量和惡意流量分開。而正常流量最後會回流至原來要正常存取瀏覽的網站。如此仍舊可保持正常運作帶來的合法性。

成本評估

DDoS 保護服務有一筆每月固定費外，外加一筆資料處理費。每月的固定費用包含保護 100 項資源的費用。額外保護其他資源會依每月每一項資源的方式加收費用。

DDoS 保護的每月價格 (包含保護 100 項資源的費用)：每月 NT$88,466 超量費用 (超過 100 項資源)：每月每個資源 NT$885。

| 每月處理的資料量 | 每 GB 的價格 |
| --- | --- |
| 0 – 100 TB | NT$1.503 |
| 100 TB – 500 TB | NT$1.203 |
| 500 TB – 1 PB | NT$0.902 |
| 超過 1 PB | [連絡我們](https://azure.microsoft.com/zh-tw/overview/sales-number/) |

\*上述價格以每個月 730 小時計。

補充 Q&A 重點：

1. DDoS 保護內容中如何定義資源？資源是指附加到 IaaS VM、負載平衡器 (傳統及標準負載平衡器)、應用程式閘道 (包含 WAF) 叢集、Service Fabric 或 IaaS 式網路虛擬設備 (NVA) 的公用 IP。未來可能會新增其他受保護的資源。
2. 資料處理包括什麼，以及如何計算這些費用？處理上述受保護資源的資料，是來自在受 DDoS 保護的虛擬網路 (VNET) 上任一 VM 的輸出頻寬。這些 VM 的輸出頻寬總計會加以彙總，然後用於計費。輸出到網際網路的流量也會計入。VNET、VNET 之間，或進入 ExpressRoute 或 VPN 閘道的流量，則不會計入。
3. 如使用 DDoS 保護時間不足一個月，費用是否有所不同？如客戶 DDoS 保護服務有效期間為一整個月，則不論使用量多寡，都必須支付月費。但若服務在當月只有一段時間有效，則只需要針對使用的時數以及產生的資料傳輸超額部分，支付按比例計算的費用。

本次測試時數精算：

NT$88,466 /30/24=NT$70.4/hr

簡易環境示範

如圖1至圖7所示：

* Azure 訂閱帳戶
* 決定資源放在哪個地區
* 資源群組
* 虛擬網路
* 虛擬網路下資源服務如：虛擬機器型站台服務
* 網路安全群組(Input TCP 80 / 3389 Allow)
* 確認虛擬網路的DDoS防禦為基本型
* 儲存體

圖 1. 檢視英普瑞斯網路安全結界中，Diable-imperis-network的資源群組



圖 2. 目前原有的 10.100.0.0/16 位址空間



圖 3. 因城中資源才剛剛需要被整合故暫時僅有一筆 10.100.1.x/24 的子網路



圖 4. 已連線的資源唯一一張網卡(也就是綁了一台輕量虛擬主機作為網站之用)



圖 5. 這台連接資源本尊就是Windows Server 2016 VM 跑一個測試預設微軟網站

一張含有 文字 的圖片

自動產生的描述

圖 6. 入口網站URL

[http://diablowebsite.southeastasia.cloudapp.azure.com](http://diablowebsite.southeastasia.cloudapp.azure.com/)

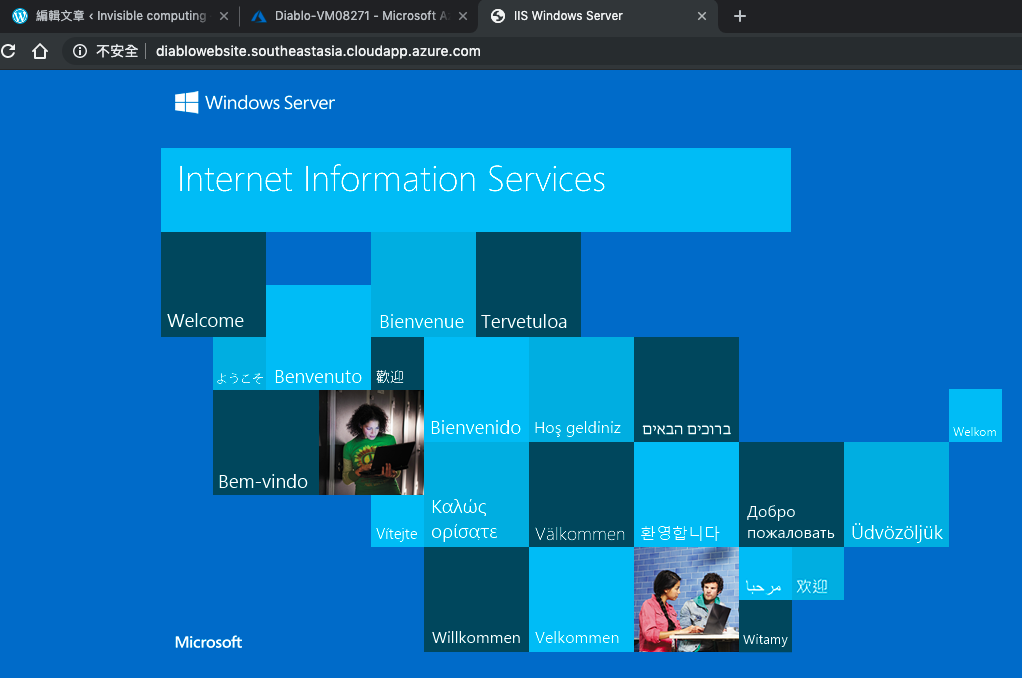
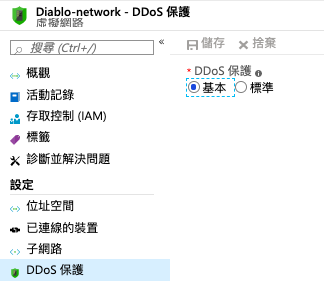


圖 7. 目前為預設基本型的 DDoS 防禦



**實驗環境**

如圖8至圖30所示：

圖 8. 找到DDoS Protection Plan服務並選擇屬於適合您現行資源環境下的地區

一張含有 文字 的圖片

自動產生的描述

圖 9.回到你所要做進階DDoS保護的虛擬網路,改為標準後套用剛剛設置的計畫

一張含有 文字 的圖片

自動產生的描述

圖 10.儲存等待生效

一張含有 文字 的圖片

自動產生的描述

圖 11.完成後就會提醒您可以到計量服務針對Public IP服務做DDoS監視

一張含有 文字 的圖片

自動產生的描述

圖 12.以下有這麼多的DDoS參數列表(列出如圖12-15之多)

一張含有 文字 的圖片

自動產生的描述

圖 13.

一張含有 文字 的圖片

自動產生的描述

圖 14.

一張含有 文字 的圖片

自動產生的描述

圖 15.

一張含有 文字 的圖片

自動產生的描述

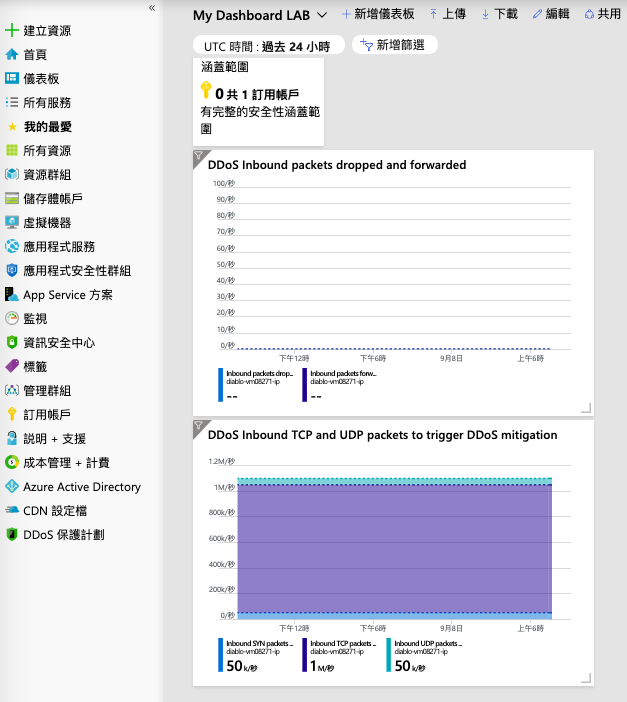
官方建議的標準遙測計量如下：

* **捨棄的標籤名稱** (如：**捨棄的傳入封包 DDoS**)：DDoS 保護系統捨棄/清除的封包數目。
* **轉送的標籤名稱** (如：**轉送的輸入封包 DDoS**)：DDoS 系統轉送到目的地 VIP 的封包數目 – 未篩選的流量。
* **沒有標籤名稱** (如：**輸入封包 DDoS**)：進入清除系統的封包總數 – 表示捨棄和轉總的封包總和。

針對受保護資源的每個公用 IP 位址套用三個自動調整風險降低措施 (TCP SYN、TCP 及 UDP)。 客戶可依需求環境選取檢視原則閾值**以觸發 DDoS 風險降低措施的輸入 TCP 封包**並**觸發 DDoS 風險降低措施的輸入 UDP 封包**計量**彙總**輸入為 ‘Max’

設置完成並訂選至儀表板上(上述因為屬於計量範疇如果不了解如何設置容小弟後續會有更詳細的篇章說明)

圖 16.釘選至儀表板方便登入即刻了解狀況(上面預設是一天更新一次,可以縮短至30分鐘)



補充另外有個重要的設置在未來需要調用分析時可以用上，我們叫它做DDoS 攻擊風險降低報告

它主要是用 Netflow 通訊協定進行資料彙整以供有關資源攻擊的詳細資訊。每當公用 IP 資源遭受攻擊時，將在啟動風險降低措施後，立即產生風險降低報告。

每隔五分鐘就會產生一份增量報告及整個風險降低期間，產生一份風險降低後續報告。 目的是確保在 DDoS 攻擊持續進行較長時間的情況下，客戶將能夠每五分鐘檢視最新的風險降低報告快照集，並在攻擊風險降低結束後，檢視完整摘要。

圖 17.到Public IP服務的刀鋒功能視窗設置診斷



透過收集 DDoSMitigationReports 記錄涵蓋到以下增量及攻擊風險降低後續報告的欄位資訊

* 攻擊媒介
* 流量統計資料
* 丟棄封包的原因
* 涉及的通訊協定
* 前 10 個來源國家/地區或區域
* 前 10 個來源的 ASN

而收集攻擊風險降低流程記錄可讓你在接近即時DDoS 攻擊間，查看丟棄的流量、轉寄的流量及其他相關資料點。 DDoSMitigationFlowLogs 記錄涵蓋到以下增量及攻擊風險降低後續報告的欄位資訊

* 來源 IP
* 目的地 IP
* 來源連接埠
* 目的地連接埠
* 通訊協定類型
* 在風險降低期間所採取的動作

圖 18 .可以把Log傳送至以下三種服務位置，大多時候我會放置Log分析中，但礙於測試成本期限示範放置儲存空間中(此也預先設置)



可透過此breakingpoint服務機構做DDoS攻擊測試，來應對這些挑戰，各企業需要一種應用和安全測試解決方案已驗證網路和網路設備的穩定、準確和品質。

在這種情況下，BreakingPoint應運而生。通過模擬真實合 法的流量、分散式阻斷攻擊（DDoS）、漏洞、惡意軟體、 模糊測試，BreakingPoint可以檢驗各企業機構的安全基礎 架構，減少近80%的網路退化風險並將防止攻擊安全程度提 升近70%。

特定的配置或安全設置如何抵禦網路攻擊？通過模擬任意 流量，在最真實的環境下驗證和優化網路，BreakingPoint 讓問題迎刃而解。

此外，它還對安全基礎架構進行大規模 檢測，從而確保可用性，更大靈活性和快速的網路測試。

breakingpoint服務關鍵特性

模擬300多項真實的應用程序協議，允許定製和操作任何協議，包含原始數據，高速生成具實際協議重要性的混合協議。

支持檢測超過37,000種攻擊和惡意軟體並同時從單一埠傳輸各類流量包括：合法流量、DDoS和惡意軟體。

即時更新所訂購的應用協定和威脅情報（ATI）確保用戶掌握最新應用程序和威脅。

右邊註冊網站有免費5GB攻擊流量 <https://breakingpoint.cloud/trial>

圖 19 . 建立新帳戶

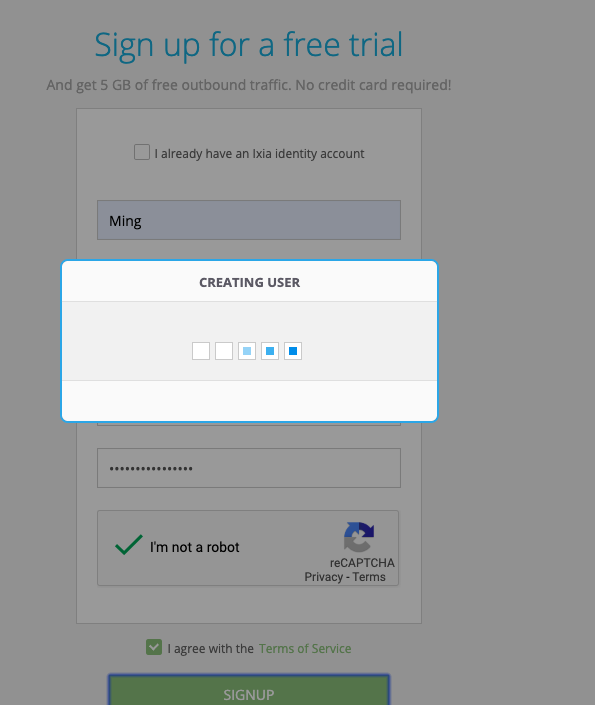


圖 20 .開始試用

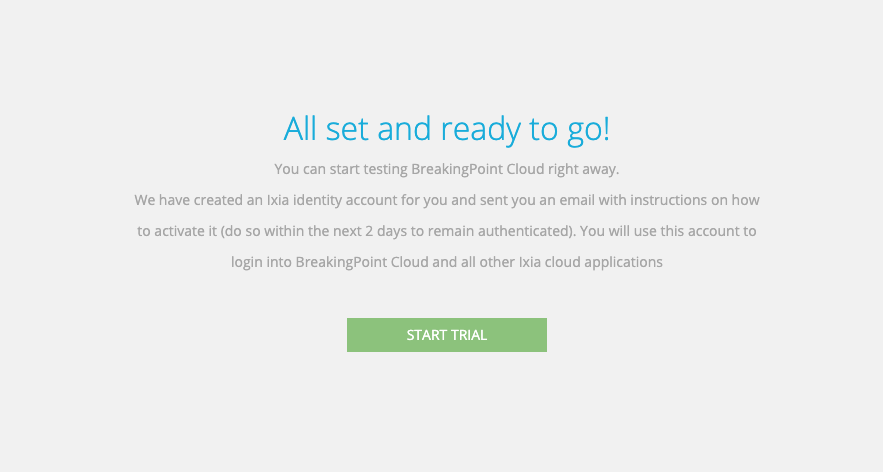


圖 21 .同意與Azure訂閱綁定並需要允許微軟帳戶存取

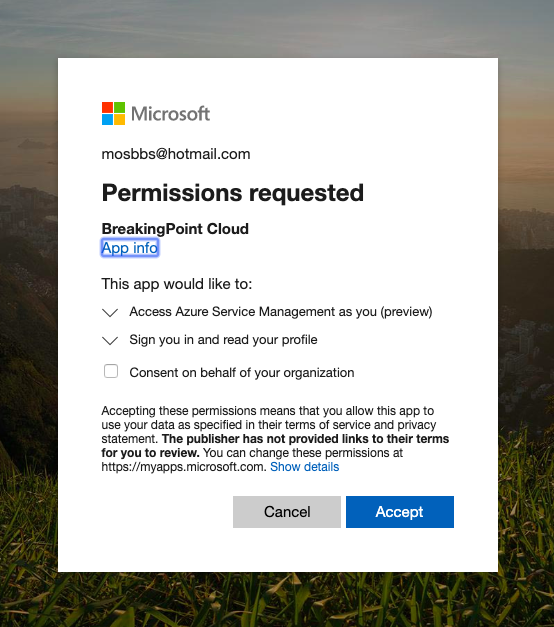


圖 22.驗證綁定成功啟用(可能需要一兩分鐘的時間)

一張含有 文字 的圖片

自動產生的描述

圖 23 .選擇指定的攻擊方式，能在免費5GB範疇內的限制我選用TCP SYN Flood也就是惡意用戶利用三向交握在正常TCP程序中可跳過傳送最後的ACK訊息或在SYN裡透過欺騙來源IP，讓伺服器送SYN-ACK到假造的IP Addree，但實際上是永遠不會收到ACK而不斷耗竭。

一張含有 文字 的圖片

自動產生的描述

圖 24 .選擇指定攻擊的IP以我的Azure VM為目標

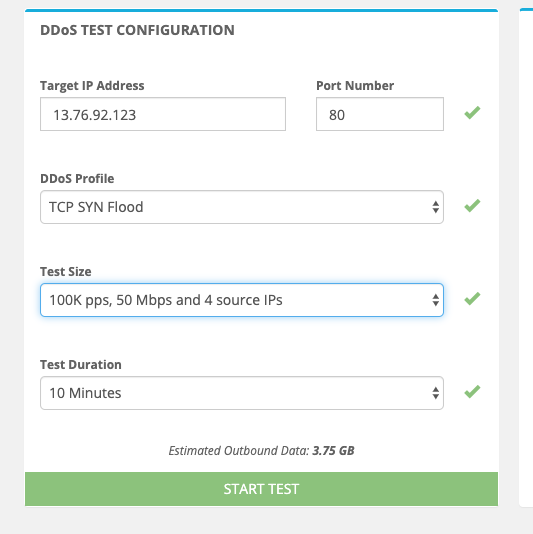


圖 25 .測試中

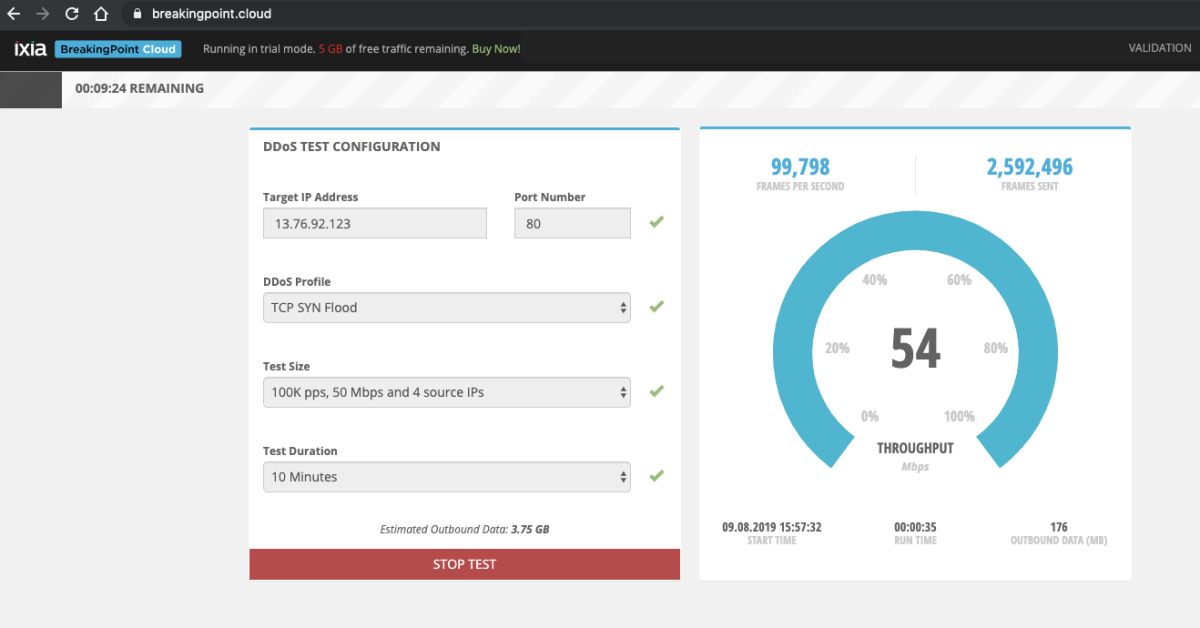


圖 26 .測試完成

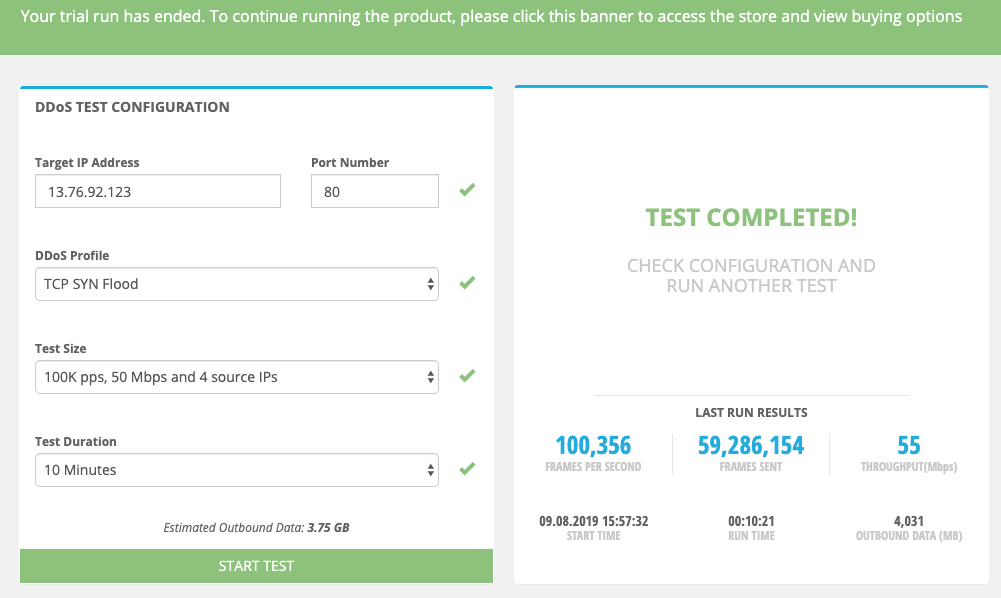


圖 27.從圖中看到所監視在右上角處已經功能運作把不正常的流量做丟棄

