技能解封初始篇章-防網站惡攻的天行者(WAF)

前言

[**https://ithelp.ithome.com.tw/articles/10213749**](https://ithelp.ithome.com.tw/articles/10213749)

成本評估

Azure Front Door 依下列定價面向計費：

1. 輸出資料傳輸 (也就是從 Front Door POP 輸出到用戶端的資料)
2. 輸入資料傳輸 (也就是從用戶端輸入 Front Door POP 的資料)
3. 路由規則 (也就是為 Front Door 設定的路由數)。每個路由都是 HTTP/HTTPS 通訊協定、前端主機/網域，以及路徑模式的相異組合。

| 輸出資料傳輸 | 區域 11 | 區域 21 | 區域 31 | 區域 41 | 區域 51 |
| --- | --- | --- | --- | --- | --- |
| 第一個 10 TB / 月 | 每 GB NT$5.110 | 每 GB NT$7.514 | 每 GB NT$15.028 | 每 GB NT$8.416 | 每 GB NT$10.219 |
| 之後的 40 TB (10-50 TB)/月 | 每 GB NT$4.509 | 每 GB NT$6.612 | 每 GB NT$12.804 | 每 GB NT$7.214 | 每 GB NT$8.716 |
| 之後的 100 TB (50-150 TB)/月 | 每 GB NT$3.908 | 每 GB NT$5.711 | 每 GB NT$10.820 | 每 GB NT$6.011 | 每 GB NT$7.364 |
| 每個月超過 150 TB | [連絡我們](https://azure.microsoft.com/zh-tw/overview/sales-number/) | [連絡我們](https://azure.microsoft.com/zh-tw/overview/sales-number/) | [連絡我們](https://azure.microsoft.com/zh-tw/overview/sales-number/) | [連絡我們](https://azure.microsoft.com/zh-tw/overview/sales-number/) | [連絡我們](https://azure.microsoft.com/zh-tw/overview/sales-number/) |

| 1 您會需要支付最低回應大小 2KB 的費用。如需詳細資料，請參閱下方常見問題集。 |
| --- |

| 路由規則 |
| --- |
|  | 每單位價格 | 價格單位 |

|  |  |  |
| --- | --- | --- |
| 前 5 個路由規則 | NT$0.902 | 每小時 |
| 每個額外的路由規則 | NT$0.361 | 每小時 |

| 輸入資料傳輸 |
| --- |
| 每 GB NT$0.301 |

WAF 定價包括每月固定費用和要求處理費用。如原則中所設，每個原則都有月費；自訂規則和受控規則集則有附加元件費用。

| 每單位的原則價格 | | 價格單位 |
| --- | --- | --- |
| NT$150.271 | | 每月 |
| 自訂規則 | 每單位價格 | 價格單位 |
| 規則 | NT$30.055 | 每月 |
| 已處理的要求 | NT$18.033 | 每 1 百萬次要求 |

| 受控規則集 | 每單位價格 | 價格單位 |
| --- | --- | --- |
| 預設規則集 | NT$601.084 | 每月 |
| 已處理的要求 | NT$30.055 | 每 1 百萬次要求 |

FrontDoor Q&A

**什麼是 Azure FrontDoor服務和 Azure 應用程式閘道之間的差異？**

前端和應用程式閘道是第 7 (HTTP/HTTPS) 負載平衡器層級，主要差異FrontDoor是全域服務，而應用程式閘道是區域性服務。 雖然FrontDoor可跨區域不同縮放單位/叢集間的負載平衡，而應用程式閘道則是讓你的縮放單位為VM/容器間來進行。

**Azure FrontDoor服務支援哪些功能？**

Azure **FrontDoor**服務支援動態網站加速 (DSA)、 SSL 卸載和端對端 SSL、 Web 應用程式防火牆、 cookie 型工作階段親和性、 url 路徑型路由等…

**Azure FrontDoor服務支援哪些通訊協定？**

Azure 的FrontDoor服務支援 HTTP、 HTTPS 和 HTTP/2。

**Azure 前端服務如何支援 HTTP/2？**

只連線到 Azure 前端服務的用戶端使用 HTTP/2 通訊協定支援。 後端集區中的後端的通訊是透過 HTTP/1.1。 預設會啟用 HTTP/2 支援。

**目前支援哪些資源做為後端集區的一部分？**

後端集區可以是儲存體、 Web 網站、 Kubernetes 或其他自訂主機名稱具有公開連線能力所組成。

**什麼是 Azure FrontDoor服務的 POP 位置？**

Azure 的FrontDoor服務都來自 Microsoft 的 Azure CDN 的 POP 相同的位置清單。 完整列表請參閱[從 Microsoft Azure CDN POP 位置](https://docs.microsoft.com/azure/cdn/cdn-pop-locations)。

**Azure FrontDoor服務是否支援靜態或專用的 Ip？**

目前不支援靜態或專用 Ip。

**部署 Azure FrontDoor服務需要多久的時間？ 我的大門仍然運作時正在更新？**

建立新的**FrontDoor**或現有**FrontDoor**任何更新都需要3-5分鐘全域部署。另外補充自訂 SSL 憑證更新部署至全球需要約30分鐘時間。

**什麼是 Azure WAF？**

Azure WAF 是一種 web 應用程式防火牆，可協助保護您的 web 應用程式免于遭受常見的威脅，如 SQL 插入式攻擊、跨網站腳本和其他 web 惡意探索。可自訂受控規則所組成的 WAF 原則以控制對 web 應用程式的存取。

Azure WAF 原則可以套用至裝載于應用程式閘道或 Azure Front 門板服務上的 web 應用程式。

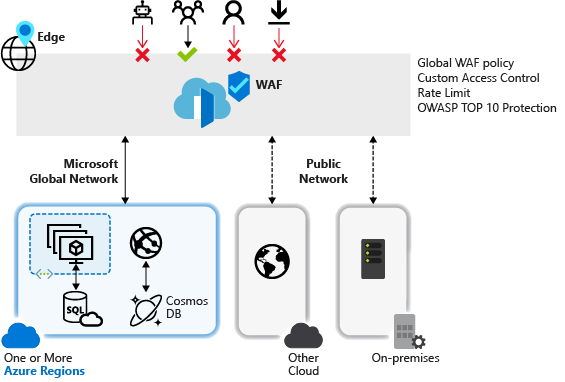
**什麼是適用于 Azure Front 服務的 WAF？**

Azure **FrontDoor**可高度擴充、全域散發的應用程式和內容傳遞網路。 Azure WAF 與**FrontDoor**整合會在進入客戶虛擬網路之前拒絕服務供保護而不犧牲效能。

服務架構

可部署在 Azure 各地資料中心上，啟用網站應用程式防火牆檢查每個網路傳入的要求。防止惡意攻擊來源、禁止接近進入你自家的虛擬網路內，供大規模的整體保護，而不會犧牲效能。

WAF 原則可輕易地連結到你的訂用帳戶中任何前端設定檔和新的規則，只需要幾分鐘的更新生效時間來大幅降低瞬息萬變的威脅風險。



前置作業

需部署兩個在不同 Azure 區域 (如：美國東部和東南亞 ) 中執行的 Web 應用程式個體。此兩組 Web 應用程式個體都會以 A-A Mode 執行，層級不同於 A-S Mode 當發生異常時才會將其中一組作為容錯移轉，A-A Mode 是兩組隨時都能接收流量。

簡易環境示範

* 美國網站主機\*1
* 東南亞網站主機\*1
* 透過 **FrontDoor 全域託管服務串接並透過WAF規則來做保護**

圖1. 網站主機在東南亞 (可以記一下 DNS 名稱等等連網頁可以檢視)

一張含有 文字 的圖片

自動產生的描述

圖2. 確認就是此網站無誤(東南亞)

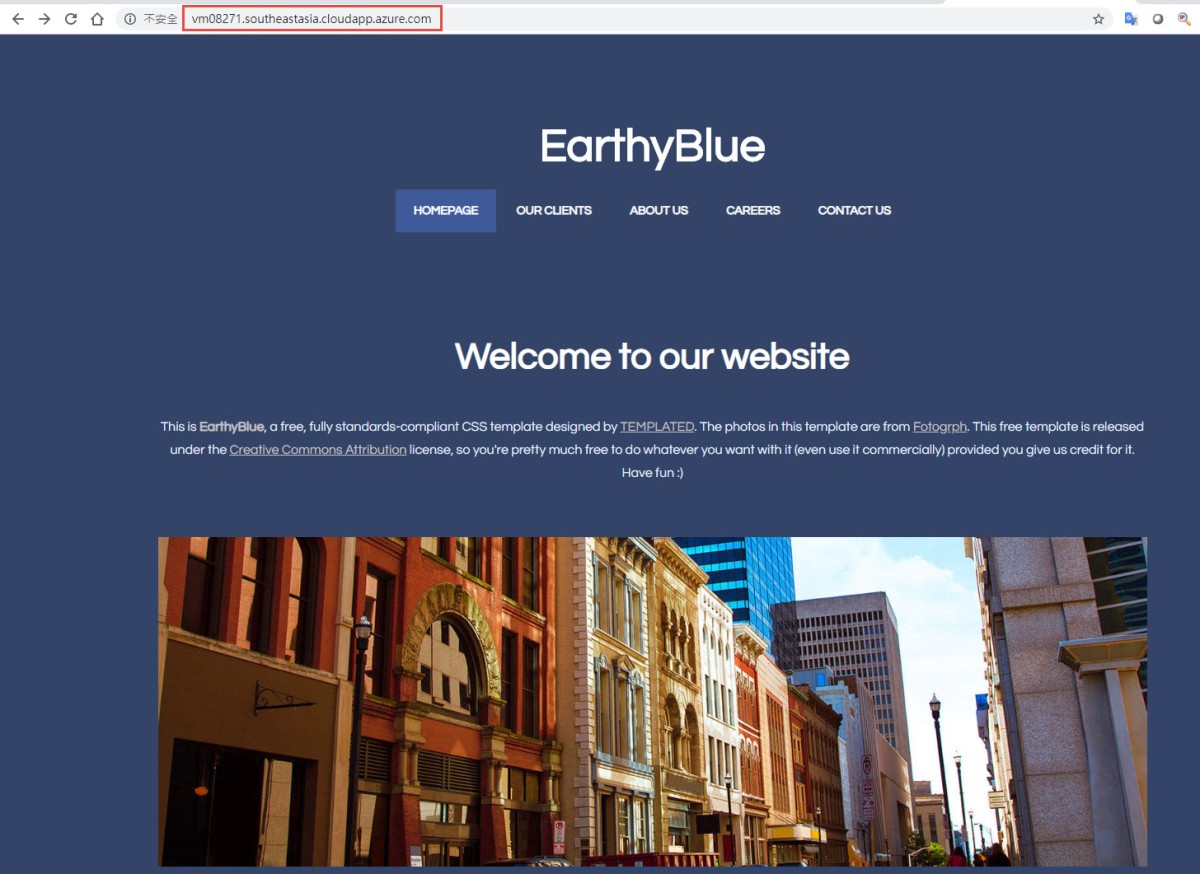


圖3. 網站主機在美國 (可以記一下 DNS 名稱等等連網頁可以檢視)

一張含有 文字 的圖片

自動產生的描述

圖4. 確認就是此網站無誤(美國)

一張含有 文字, 大自然, 夜空 的圖片

自動產生的描述

圖5. 首要任務須先從WAF原則開始建立，並啟用原則

一張含有 文字 的圖片

自動產生的描述

圖6. 可以針對實際WAF的作用進行模式選擇，另外當異常回報則可重導向至指定網頁

一張含有 文字 的圖片

自動產生的描述

圖7. 對於受控原則屬於微軟控制我們只能選擇對不同情境下最佳的選擇，大多就預設

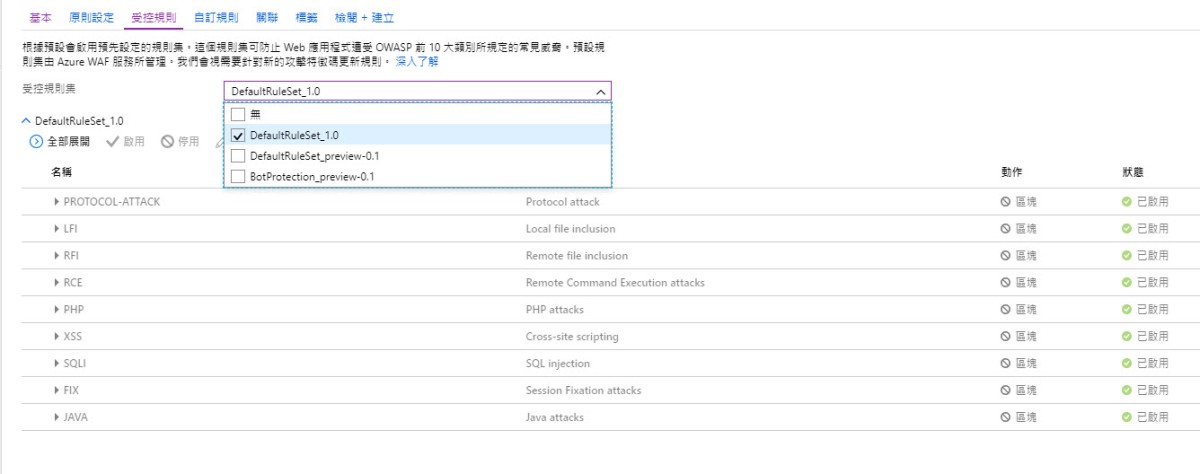


圖8. 本次規則驗證，小弟選擇透過地理區來區分如果是台灣來的連線一律阻擋，台灣以外則正常顯示頁面

一張含有 文字 的圖片

自動產生的描述

圖9. 原則設立驗證完成

一張含有 桌 的圖片

自動產生的描述

一張含有 文字 的圖片

自動產生的描述

圖10. WAF Policy 服務建立完成

一張含有 文字 的圖片

自動產生的描述

圖11. 確認一下剛剛的設定(原則)

一張含有 文字 的圖片

自動產生的描述

圖12. 確認一下剛剛的設定(受控規則)

一張含有 桌 的圖片

自動產生的描述

圖13. 確認一下剛剛的設定(自訂規則)

一張含有 文字 的圖片

自動產生的描述

圖14. 開始要建立真正的重頭戲 FrontDoor 服務 (地區只是要找個地方指定馾實際上就是全域服務)

一張含有 文字 的圖片

自動產生的描述

圖14. 一開始的組態流程設置畫面

一張含有 文字 的圖片

自動產生的描述

圖15. 先從前端要被連線的URL命名，另外是否需要Cookies紀錄相同的來源指定同一台後端主機(預設是關閉)，最後套用剛剛設置的Policy

一張含有 文字 的圖片

自動產生的描述

圖16. 後端集區就把本次要測試的兩台主機的網站FQDN網址加進去並給予優先序與權重比例

一張含有 桌 的圖片

自動產生的描述

圖17. 作法同上述



圖18. 確認後端都已經設置完畢狀態均顯示已啟用

一張含有 文字 的圖片

自動產生的描述

圖19. 最後設置規則Http/s均要另外綁定前端對外的FQDN，包含是否需要快取等．．

一張含有 文字 的圖片

自動產生的描述

圖20. 上述三階段流程均設置完畢

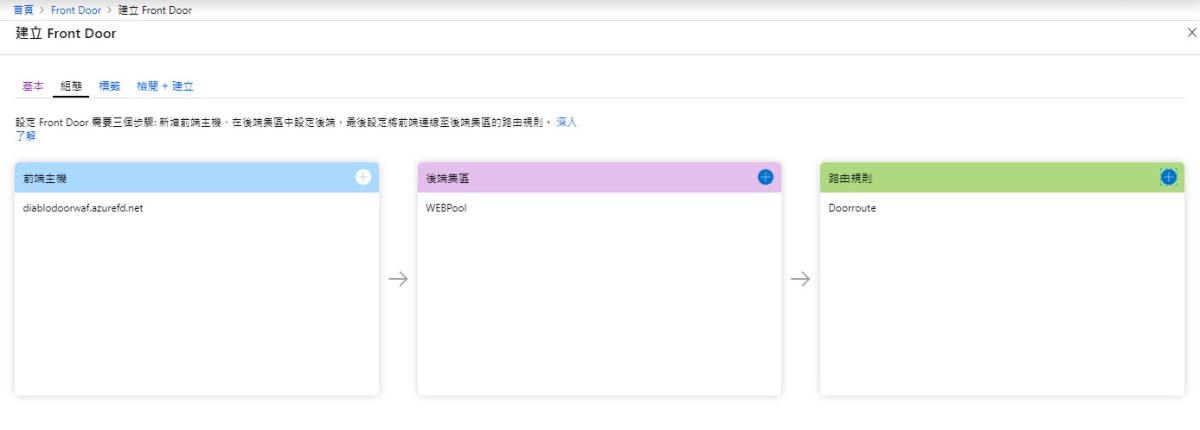


圖21. 確認設置驗證無誤

一張含有 文字 的圖片

自動產生的描述

圖22. 建立Frontdoor服務完成

一張含有 文字 的圖片

自動產生的描述

圖23. 需要等個五分鐘後再試，不然後端還沒真正Ready會說找不到，從台灣連到Frontdoor 網址測試的確是有套用到規則被封鎖掉

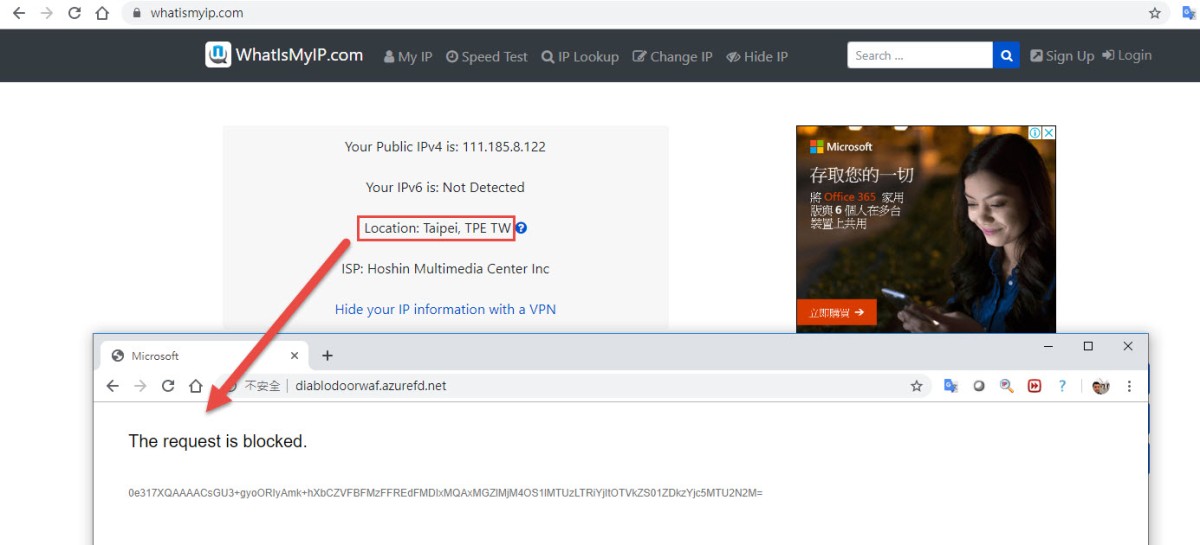


圖24. 透過美國的虛擬機來當作用戶連Frontdoor 網址測試則沒有問題能正常顯示網站

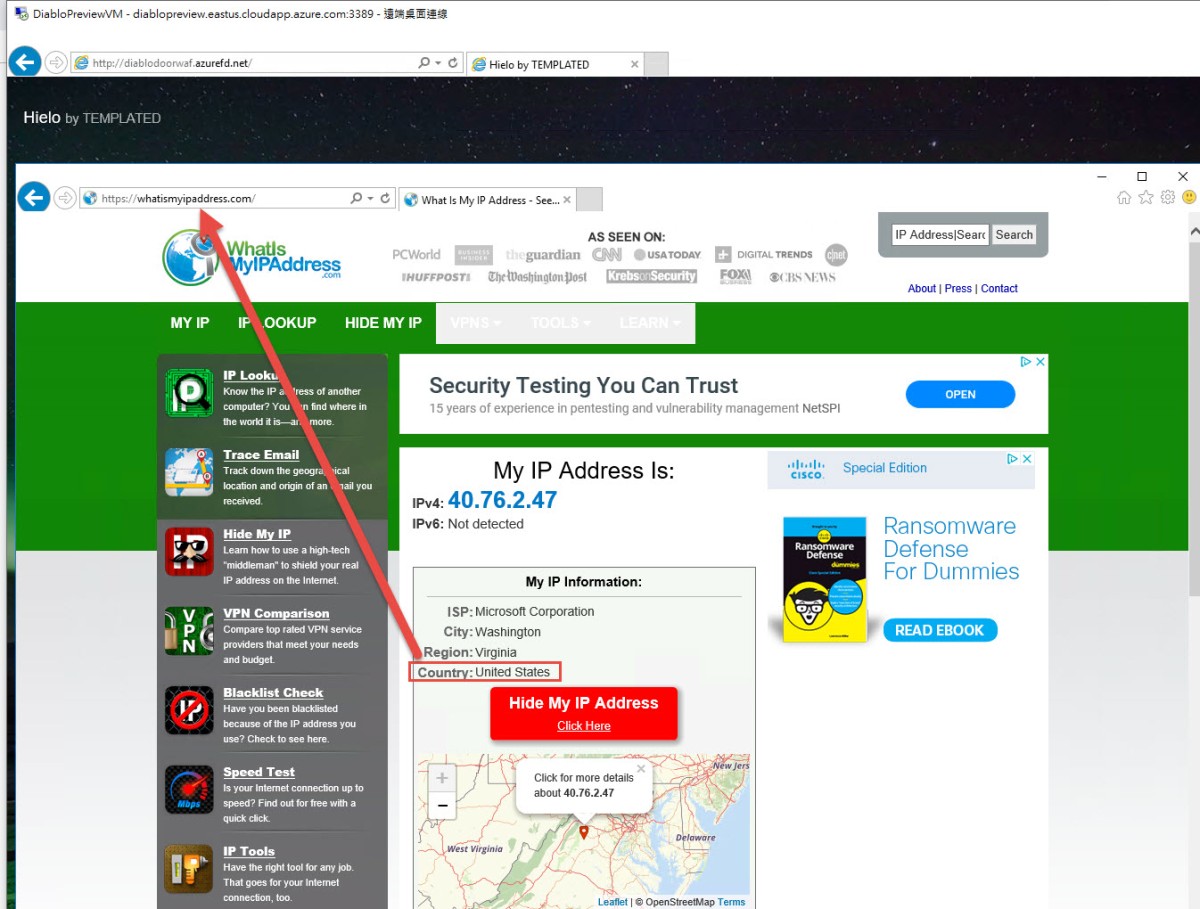


圖25. 因為中間有多次的連線測試所以也看到這段時間的Request集中的連線數變多，沒有問題

