

Azure NSG 限制存取外網只允許
Windows Update

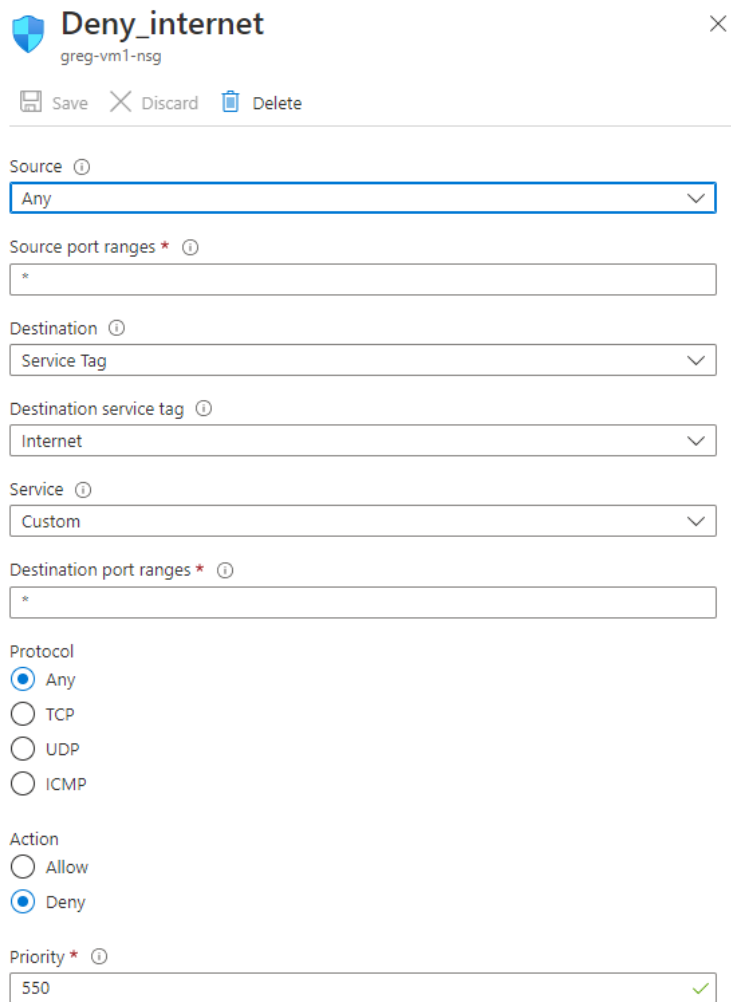
CloudRiches

概述

由於 Azure NSG 無法使用 FQDN 的方式設定規則，所以要透過 Service Tag 去簡化我們的管理工作，如何透過 Service Tag 限制存取外網的同時，只允許 Windows Update。

操作步驟

1. 到 NSG 的 Outbound port rules 把 internet 流量 Deny，優先順序不要使用 100，因為前面還要允許 windows update 流量。



Deny_internet greg-vm1-nsg ×

Save Discard Delete

Source ⓘ
Any ▼

Source port ranges * ⓘ
*

Destination ⓘ
Service Tag ▼

Destination service tag ⓘ
Internet ▼

Service ⓘ
Custom ▼

Destination port ranges * ⓘ
*

Protocol
 Any
 TCP
 UDP
 ICMP

Action
 Allow
 Deny

Priority * ⓘ
550 ✓

2. 允許 Windows Update 流量，要設定 2 個 Service Tag Rule。

allow_update_2

greg-vm1-nsg

Save Discard Delete

Source: Any

Source port ranges: *

Destination: Service Tag

Destination service tag: AzureUpdateDelivery

Service: HTTPS

Destination port ranges: 443

Protocol: TCP

Action: Allow

Priority: 540

Name: allow_update_2

allow_update_1

greg-vm1-nsg

Save Discard Delete

Source: Any

Source port ranges: *

Destination: Service Tag

Destination service tag: AzureFrontDoor.FirstParty

Service: HTTP

Destination port ranges: 80

Protocol: TCP

Action: Allow

Priority: 530

Name: allow_update_1

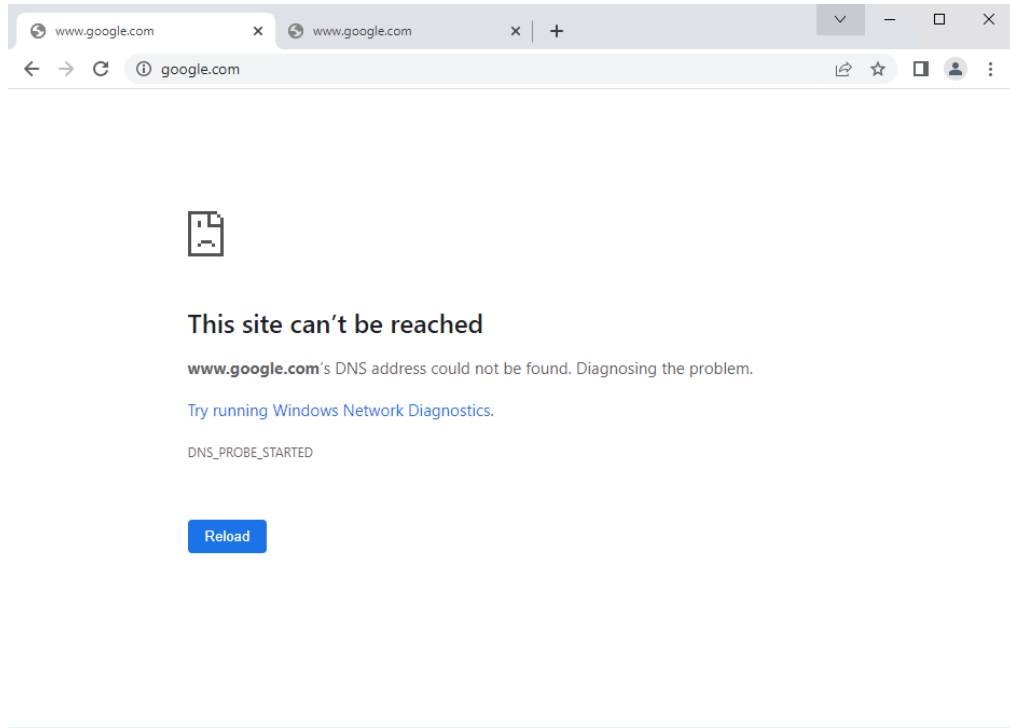
Inbound port rules **Outbound port rules** Application security groups Load balancing

Network security group greg-vm1-nsg (attached to network interface: greg-vm146)
Impacts 1 subnets, 1 network interfaces

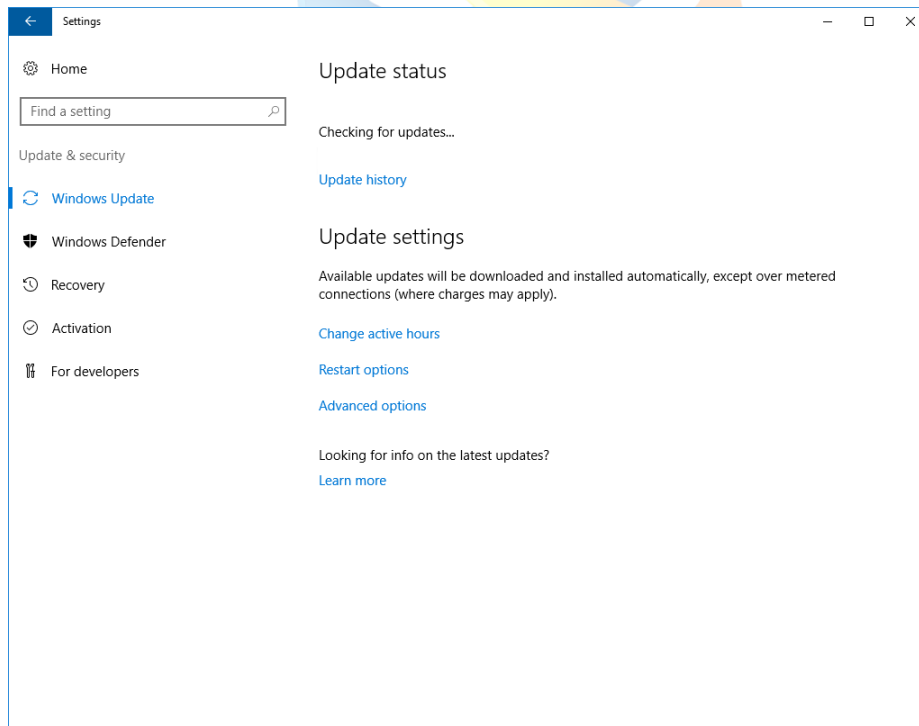
Add outbound port rule

Priority	Name	Port	Protocol	Source	Destination	Action	
530	allow_update_1	80	TCP	Any	AzureFrontDoor.FirstParty	Allow	***
540	allow_update_2	443	TCP	Any	AzureUpdateDelivery	Allow	***
550	Deny_internet	Any	Any	Any	Internet	Deny	***
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	***
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow	***
65500	DenyAllOutBound	Any	Any	Any	Any	Deny	***

3. 連線到 VM 上，開啟瀏覽器確認無法開啟網頁，如：www.google.com



4. 點選 Windows Update, 確認可以成功更新。



雲馥聯繫資訊

雲馥數位股份有限公司

地址：241 新北市三重區重新路四段 12 號 12 樓

電話：+ 886 2 2595 1865

傳真：+ 886 2 2595 8973

網址：<https://www.cloudriches.com>

電子郵件：service@cloudriches.com

服務電話：+ 886 2 2595 6218

服務平台：<https://portal.cloudriches.com>



CloudRiches