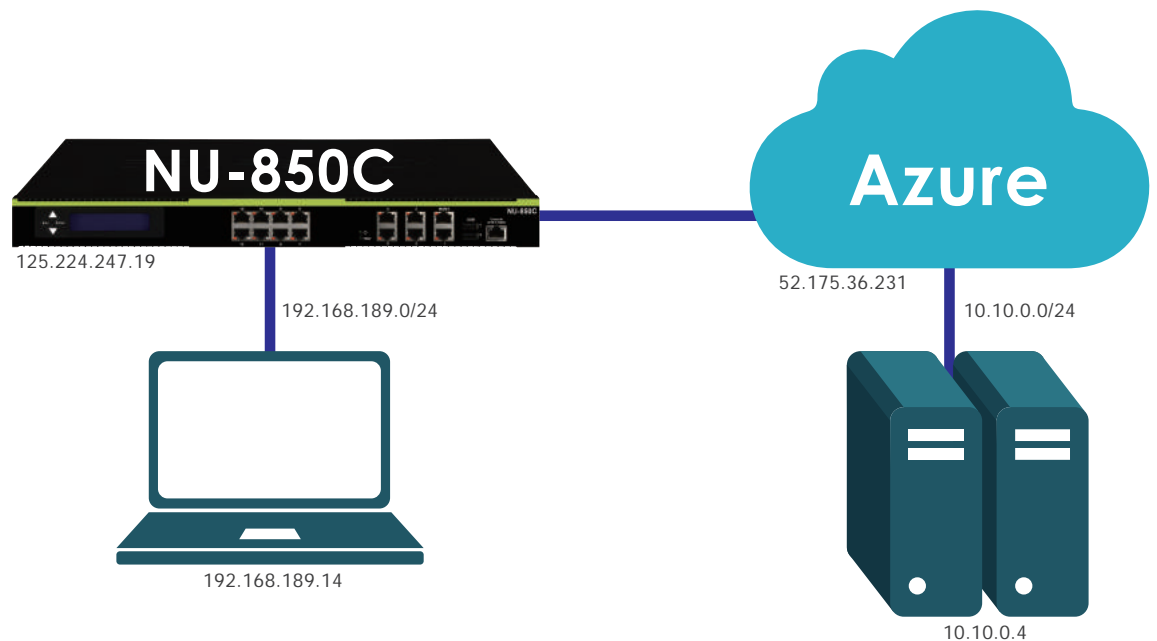


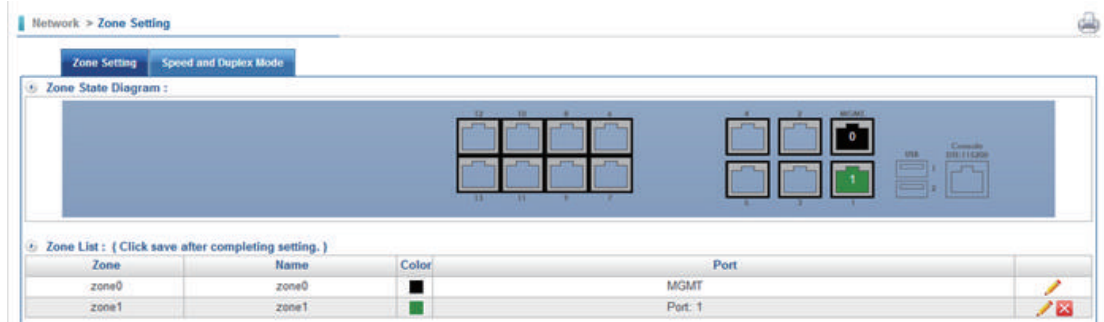
S2S VPN with Azure Route Based



STEP1 - Configuring NU-850C Network

Settings

- 韌體版本 : 9.0.1.2
- Network > Zone Setting , 新增 zone1



台中總公司 04-2705-0888
台中市西屯區西屯路二段256巷6號3F-6

台北分公司 02-2501-1185
台北市中山區松江路129號6F-2

高雄分公司 07-229-8788
高雄市新興區民權一路251號8F-6

免付費專線 0800-666-188

官方網站 | www.sharetech.com.tw

銷售諮詢 | sales@sharetech.com.tw

技術支援 | help@sharetech.com.tw

S2S VPN with Azure Route Based

3. Network > Interface，設定 zone0 IP，並設定網段 192.168.189.126/24。
(注意: 192.168.189.126 在此處為管理 IP)

Network > Interface IPv4

zone0 (zone0) zone1 (zone1) zone2 (zone2) zone3 (zone3)

Network interface settings

Interface Name: zone0 Enable: [x] STATIC

MAC address: 00:60:e0:69:f9:a8 MTU: 1500 (1400 ~ 1500)

Visit Control [x] Firewall Protection [x]

Save

IP Address

Name	IP	Mask	Default gateway	Management IP	Edit / Delete
default	192.168.189.126	255.255.255.0	--	[x]	[Edit] [Delete]
14	192.168.14.126	255.255.255.0	--	[x]	[Edit] [Delete]

4. Network > PPPoE，使用 PPPoE 取得 Public IP。新增一個 PPPoE 介面在 zone1 上，並取到 IP：125.224.239.145。

Network > PPPoE

PPPoE

PPPoE List

Name	Interface Name	Enable	Interface	Account	IPv6	IP / MASK	Remote address	Connect State	Connect time	Counter(b/rx)	Detection	Log
pppoe	ppp4001	[x]	zone1	75139012@hinet.net	[x]	125.224.239.145/32	168.95.98.254	Connected	00:07:43	8K / 8K	Log	Log

+ Add Edit Del

5. Network > Route > Designated Gateway，將 PPPoE 設為出口線路。

Network > Route IPv4

Static Routing Designated Gateway Designated Gateway Group Default Gateway Dynamic routing

Edit a designated gateway:

Name: pppoe

Dst IP: (Example: 192.168.1.1 or 192.168.1.0/24)

Gateway: 168.95.98.254 (Example: 192.168.1.1)

Interface: ppp4001 (pppoe)

Line Detection Way: ICMP

Detected IP Address: 8.8.8.8 (Detected IP will be filled in with Gateway)

Detection Frequency: 1 Sec (1-999)

Timeout: 500 ms

Enable Spare Gateway: [x]

Edit

6. Network > Route > Default Gateway，將 PPPoE 設為 Default Gateway。

Network > Route IPv4

Static Routing Designated Gateway Designated Gateway Group Default Gateway Dynamic routing

Edit Default Gateway:

Default Gateway:

Interface: ppp4001 (pppoe)

Assign internet ip: [x] Auto [] Define

Save

S2S VPN with Azure Route Based

7. Policy > Security Policy · 新增一 Policy · 允許 zone0 底下的連線透過 PPPoE 至外部網路。

Policy > Security Policy [IPv4]

Security Policy

Basic Setting

Policy Name:

Source Interface:

Assign Gateway:

Network Address Translation:

Assign Gateway: NAT IP 125.224.247.19

Protocol:

Source: [Change To Define](#)

Destination: [Change To Define](#)

SRC Service Group: Port:

DEST Service Group: Port:

Action:

Policy

Firewall Protection

Policy > Security Policy [IPv4]

Security Policy

Refresh Delete all rules Zero counter Show Source Interface: All 1/1

No.	Policy Name	Source Interface	Services	Source	Destination	Src Port	Des Port	Action	On/Off	NAT	Policy	Edit / Del	Statistics(Packets/Bytes)
1		zone0	ALL	Any	Any					SRC			0 / 0

+ Add

STEP2 - Configuring the Microsoft Azure Virtual Network

1. 建立一個新的 Resource Group - ResourceGroup1

Resource group

Create an empty resource group

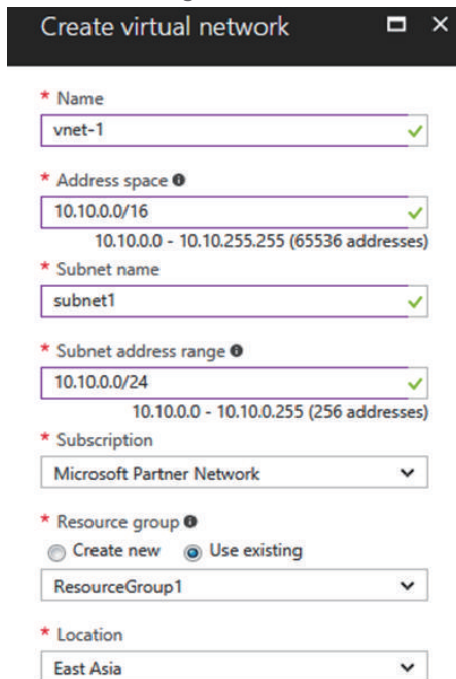
* Resource group name:

* Subscription:

* Resource group location:

S2S VPN with Azure Route Based

2. 新增 Virtual Network，名稱為 vnet-1，Address Space 為 10.10.0.0/16。同時設定其 Subnet，名稱為 subnet1，Range 為 10.10.0.0/24。Resource Group 為剛剛設定的 ResourceGroup1，如下圖所示。



Create virtual network

* Name
vnet-1 ✓

* Address space ⓘ
10.10.0.0/16 ✓
10.10.0.0 - 10.10.255.255 (65536 addresses)

* Subnet name
subnet1 ✓

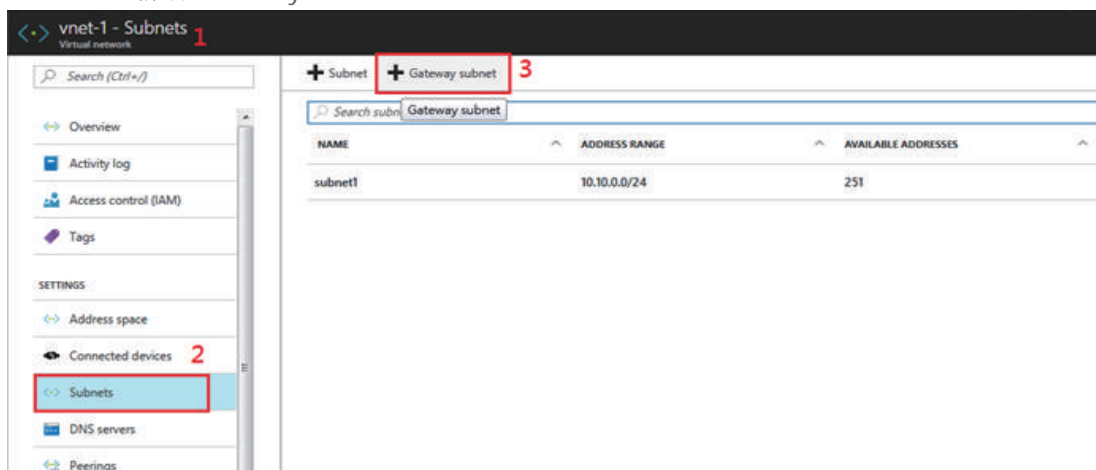
* Subnet address range ⓘ
10.10.0.0/24 ✓
10.10.0.0 - 10.10.0.255 (256 addresses)

* Subscription
Microsoft Partner Network ▼

* Resource group ⓘ
☐ Create new ☒ Use existing
ResourceGroup1 ▼

* Location
East Asia ▼

3. 新增 vnet-1 的 Gateway Subnet。可在 All Resources 裡，找到 vnet-1，點選進來 vnet-1 設定畫面，點選 Subnets，新增 Gateway Subnet。



vnet-1 - Subnets 1

Search (Ctrl+F)

Overview
Activity log
Access control (IAM)
Tags

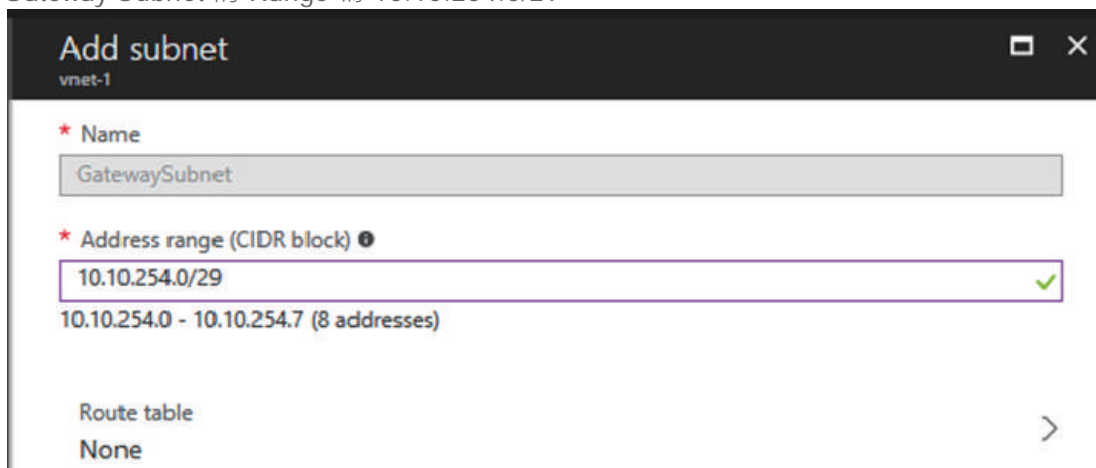
SETTINGS
Address space
Connected devices 2
Subnets
DNS servers
Peerings

+ Subnet + Gateway subnet 3

Search subnet Gateway subnet

NAME	ADDRESS RANGE	AVAILABLE ADDRESSES
subnet1	10.10.0.0/24	251

4. Gateway Subnet 的 Range 為 10.10.254.0/29。



Add subnet
vnet-1

* Name
GatewaySubnet

* Address range (CIDR block) ⓘ
10.10.254.0/29 ✓
10.10.254.0 - 10.10.254.7 (8 addresses)

Route table
None >

S2S VPN with Azure Route Based

5. 新增 Virtual Network Gateway。設定如下圖，名稱為 vnet-1-gw，VPN type 為 Policy-based，Virtual Network 套用剛剛設定的 vnet-1，接著需點選 Public IP Address 進入下一步的設定。

Create virtual network gateway...

* Name
vnet-1-gw

Gateway type
VPN ExpressRoute

VPN type
Route-based Policy-based

* SKU
VpnGw1

* Virtual network
vnet-1

* Public IP address
Choose a public IP address

* Subscription
Microsoft Partner Network

Resource group
ResourceGroup1

☐ Pin to dashboard

Create Automation options

Provisioning a virtual network gateway may take up to 45 minutes.

6. 進入 Public IP 的設定畫面，依下圖步驟新增 vnet-1-gw。

Choose public IP address

Dynamic public IP addresses that are not in use won't have an IP address assigned to them.

No public IP addresses found in the selected subscription and location 'East Asia'.

+ Create new 1

No results

Create public IP address

* Name
vnet-1-gw 2

S2S VPN with Azure Route Based

7. 設定完成後，如下圖，按下 Create，等候約 30 分。

The screenshot shows the 'Create virtual network gateway' form in the Azure portal. The form is titled 'Create virtual network gate...' and has a close button. The fields are as follows:

- Name:** vnet-1-gw (with a green checkmark)
- Gateway type:** VPN (selected), ExpressRoute
- VPN type:** Route-based (selected), Policy-based
- SKU:** VpnGw1 (selected from a dropdown)
- Virtual network:** vnet-1 (selected from a dropdown)
- Public IP address:** (new) vnet-1-gw (selected from a dropdown, highlighted with a dashed blue border)
- Subscription:** Microsoft Partner Network (selected from a dropdown)
- Resource group:** ResourceGroup1
- Pin to dashboard:** ☐
- Create:** A blue button to create the gateway.
- Automation options:** A link to view automation options.

8. 部署完成後，可以得到 Public IP: 23.97.68.169。

The screenshot shows the 'vnet-1-gw' resource page in the Azure portal. The page has a left sidebar with navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, SETTINGS, and Configuration. The main content area shows the 'Essentials' section with the following details:

Property	Value
Resource group (change)	ResourceGroup1
Location	East Asia
Subscription (change)	Microsoft Partner Network
Subscription ID	64503c1e-49c5-4a9d-87b9-443787bb71e5
SKU	VpnGw1
Gateway type	VPN
VPN type	Route-based
Virtual network	vnet-1
Public IP address	23.97.68.169 (vnet-1-gw)

S2S VPN with Azure Route Based

9. 新增 Local Network Gateway。名稱為 OnpremNetwork1，IP Address 為 NU-850C 的 Public IP 125.224.239.145，Address Space 為 NU-850C zone0 下的網段 192.168.189.0/24，Resource Group 為 ResourceGroup1。

Create local network gateway

*

Name

OnpremNetwork1

✓

*

IP address

125.224.239.145

✓

Address space

192.168.189.0/24

...

Add additional address range

...

*

Subscription

Microsoft Partner Network

▼

*

Resource group

Create new

Use existing

ResourceGroup1

▼

*

Location

East Asia

▼

10. 在 All Resources 找到 OnpremNetwork1，點選 Connections，新增一 Connection。

OnpremNetwork1 - Connections

Local network gateway

Search (Ctrl+I)

Overview

Activity log

Access control (IAM)

Tags

SETTINGS

Configuration

Connections

Properties

+ Add

Search connections

NAME	STATUS
No results	

7

S2S VPN with Azure Route Based

11. 此連線名稱為 vnet-1-onprem-Conn，Virtual Network Gateway 是剛設定的 vnet-1-gw，Local Network Gateway 為 OnpremNetwork1，PSK 是要建立 VPN Tunnel 所使用到的 Preshare Key。

Add connection
OnpremNetwork1

* Name
vnet-1-onprem-Conn ✓

Connection type
Site-to-site (IPsec) ▼

* Virtual network gateway
vnet-1-gw >

* Local network gateway
OnpremNetwork1 🔒

* Shared key (PSK)
123456abc ✓

Subscription
Microsoft Partner Network ▼

Resource group
ResourceGroup1 🔒

Create new

Location
East Asia ▼

12. 為了測試 VPN 是否正常運作，新增一個 Virtual Machine，並安裝 Ubuntu Server 14.04 LTS，步驟如下，Virtual Network 選擇 vnet-1，Subnet 選擇 subnet1。

Create virtual machine

1 Basics
Configure basic settings >

2 Size
Choose virtual machine size >

3 Settings
Configure optional features >

4 Summary
Ubuntu Server 14.04 LTS >

Basics

* Name
vm ✓

VM disk type
HDD ▼

* User name
jamie ✓

* Authentication type
SSH public key Password

* Password
..... ✓

* Confirm password
..... ✓

Subscription
Microsoft Partner Network ▼

* Resource group
Create new Use existing
ResourceGroup1 ▼

Location
East Asia ▼

OK

S2S VPN with Azure Route Based

Create virtual machine

1 Basics
Done

2 Size
Choose virtual machine size

3 Settings
Configure optional features

4 Summary
Ubuntu Server 14.04 LTS

Choose a size

Browse the available sizes and their features

4,109.03 TWD/MONTH (ESTIMATED)		8,633.59 TWD/MONTH (ESTIMATED)		18,144.39 TWD/MONTH (ESTIMATED)	
A0 Standard		A1 Standard		A2 Standard	
1 Core	0.75 GB	1 Core	1.75 GB	2 Cores	3.5 GB
1 Data disks	1x500 Max IOPS	2 Data disks	2x500 Max IOPS	4 Data disks	4x500 Max IOPS
Load balancing		Load balancing		Load balancing	
461.69 TWD/MONTH (ESTIMATED)		1,385.07 TWD/MONTH (ESTIMATED)		2,770.14 TWD/MONTH (ESTIMATED)	

Create virtual machine

1 Basics
Done

2 Size
Done

3 Settings
Configure optional features

4 Summary
Ubuntu Server 14.04 LTS

Settings

Storage

Use managed disks

No Yes

Network

Virtual network

vnet-1

Subnet

subnet1 (10.10.0.0/24)

Public IP address

(new) vm-ip

Network security group (firewall)

(new) vm-nsg

Extensions

Extensions

No extensions

High availability

Availability set

9

S2S VPN with Azure Route Based

13. 安裝完成後，可以看到此 vm 被分配到 IP 10.10.0.4。

STEP3 - Configuring the NU-850C IPSec Tunnel

1. VPN > IPSec Tunnel > Add

2. 開始設定

2.1 勾選 Enable

2.2 輸入 Tunnel Name，Azure_PolicyBased_VPN

2.3 輸入 Local IP Address，PPPoE IP 125.224.239.145

2.4 輸入 Azure 的 Public IP 23.97.68.169 (STEP 2，第 8 點)

2.5 輸入 Local Subnet 192.168.189.0/24

2.6 輸入 Remote Subnet 10.10.0.0/24 (STEP 2，第 2 點)

S2S VPN with Azure Route Based

2.7 IKE 選擇 v1

2.8 Connection Type 勾選 Main

2.9 Preshare Key 輸入在 Azure 設定的 PSK · 123456abc (STEP 2 · 第 11 點)

2.10 ISAKMP 選擇 aes / sha1 / DH Group 2

2.11 Local ID · Remote ID 皆為 IP Address

2.12 IKE SA Lifetime 為 8HR

2.13 IPsec 選擇 aes / sha1

2.14 PFS 為 No

2.15 IPsec SA Lifetime 為 1HR

IKE Setting (Phase1)

IKE ☐ v1 ☒ v2

Connection Type ☒ Main ☐ Aggressive

Preshare Key

ISAKMP DH Group ☐ Auto Matching

Local ID ☒ IP Address ☐ Domain Name

Remote ID ☒ IP Address ☐ Domain Name

IKE SA Lifetime Hour(s)

IPsec Setting (Phase 2)

IPsec ☐ Auto Matching

Perfect Forward Secrecy (PFS) ☒ No ☐ Yes

IPsec SA Lifetime Hour(s)

☒ Dead Peer Detection Delay Seconds Time out Seconds

☐ Drop SMB Protocol

3. 設定完成且 Tunnel 建立後，如下圖所示。

VPN > IPsec Tunnel

IPsec Tunnel

IPsec Tunnel and Status :

Tunnel Name	Local IP Address	Local Interface	Local Subnet	Status	Remote IP	Remote Subnet	phase 1	phase 2	Operation time	Enable	Switch	Edit / Del	Log
Azure_RouteBased_VPN	125.224.239.145	ppp4001	192.168.189.0/24		23.97.68.169	10.10.0.0/24	aes-sha1	aes-sha1	00:00:06	<input checked="" type="checkbox"/>	-		

4. Policy > IPsec Policy · 新增 IPsec Policy。

Policy > IPsec Policy

IPsec Policy

No.	Policy Name	Services	Path	Source	Destination	Port	Action	On/Off	Policy	Edit / Del	Statistics(Packets/Bytes)
-----	-------------	----------	------	--------	-------------	------	--------	--------	--------	------------	---------------------------

S2S VPN with Azure Route Based

5. 允許連線至 Azure Virtual Network，Path 選擇 'To IPSec'，Destination 可選擇 'IPSec Any' 或是 Azure_PolicyBased_VPN (10.10.0.0/24)。

Policy > IPsec Policy IPv4

IPsec Policy

Basic Setting :

Policy Name: [Text Box]

Protocol: ALL

Path: To IPSec

Source: Any [Change To Define]

Destination: IPSec Any [Change To Define]

Service Port or Group: User Defined Port [Text Box]

Action: Permit

Policy :

Schedule: None

QoS: None

[Add]

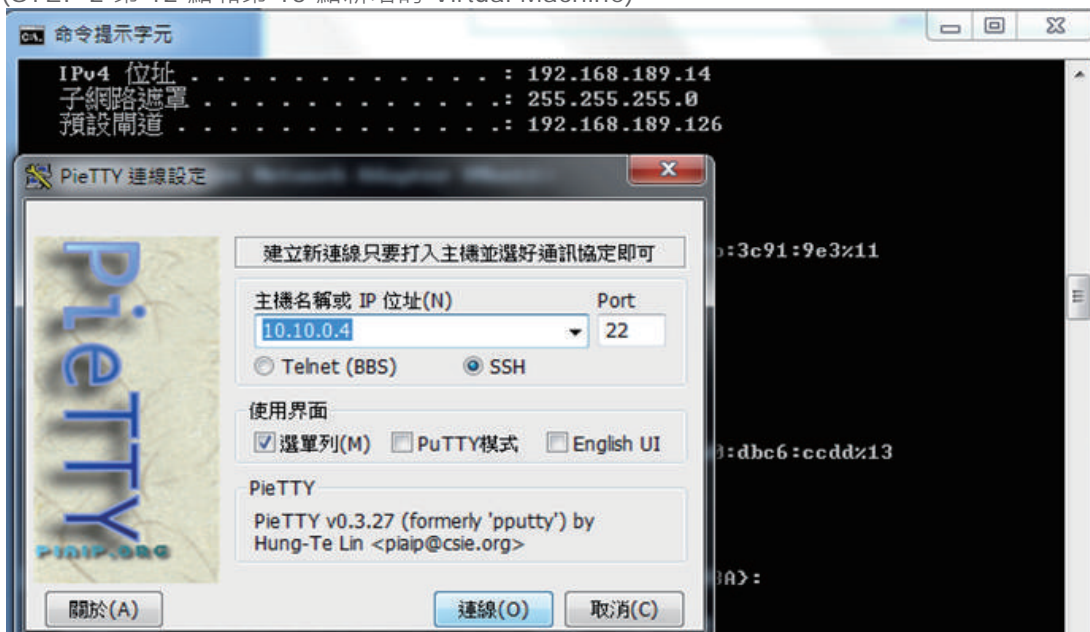
6. 新增後如下

No.	Policy Name	Services	Path	Source	Destination	Port	Action	On/Off	Policy	Edit / Del	Statistics(Packets/Bytes)
1	Azure Policy	ANY	To IPSec	Any	IPSec Any		[Icon]	[Icon]		[Icon]	0 / 0

[Add]

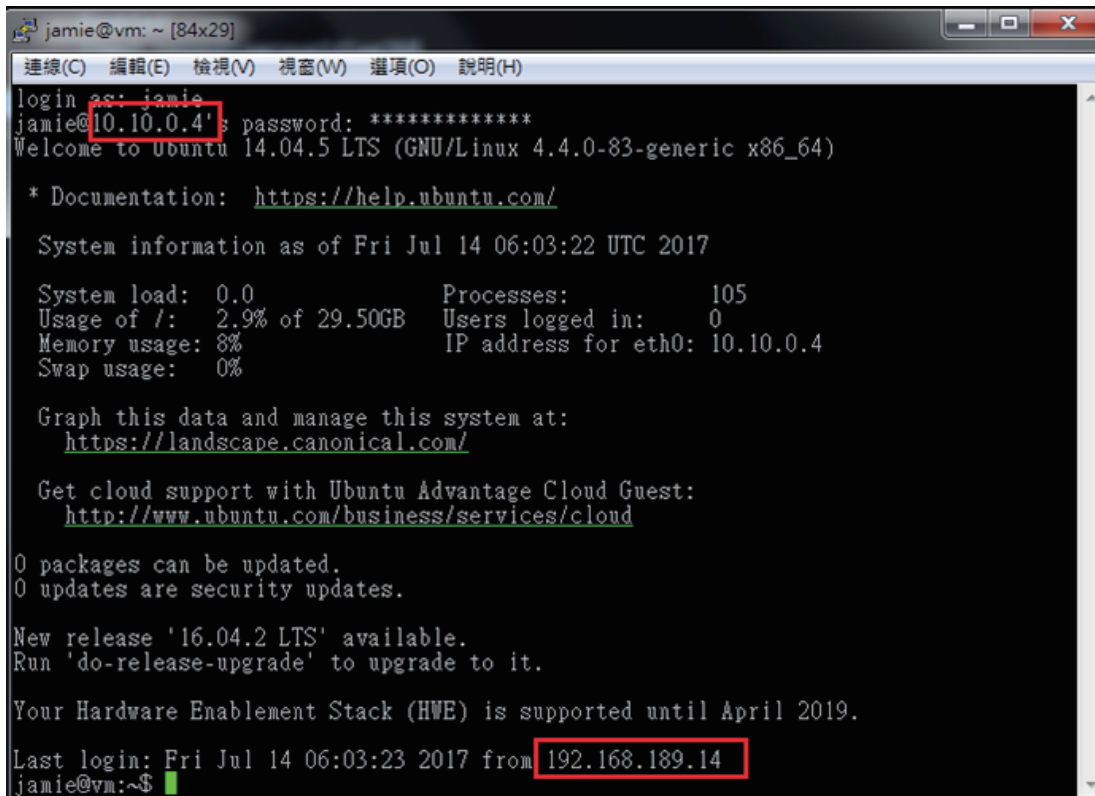
STEP 4 - Test

1. 透過 zone0 底下 PC 192.168.189.14 (Gateway 192.168.189.126)，經由 VPN 連到 10.10.0.4:22 (STEP 2 第 12 點和第 13 點新增的 Virtual Machine)。



S2S VPN with Azure Route Based

2. 可連線成功，表示 Tunnel 正常運作。



A terminal window titled 'jamie@vm: ~ [84x29]' showing a successful login for user 'jamie' at IP '10.10.0.4'. The system is Ubuntu 14.04.5 LTS. The terminal output includes system information, update status, and hardware enablement details. The IP address '192.168.189.14' is highlighted in the last login line.

```
jamie@vm: ~ [84x29]
連線(C) 編輯(E) 檢視(V) 視窗(W) 選項(O) 說明(H)
login as: jamie
jamie@10.10.0.4's password: *****
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-83-generic x86_64)

* Documentation:  https://help.ubuntu.com/

System information as of Fri Jul 14 06:03:22 UTC 2017

System load:  0.0              Processes:    105
Usage of /:   2.9% of 29.50GB   Users logged in:  0
Memory usage: 8%              IP address for eth0: 10.10.0.4
Swap usage:  0%

Graph this data and manage this system at:
  https://landscape.canonical.com/

Get cloud support with Ubuntu Advantage Cloud Guest:
  http://www.ubuntu.com/business/services/cloud

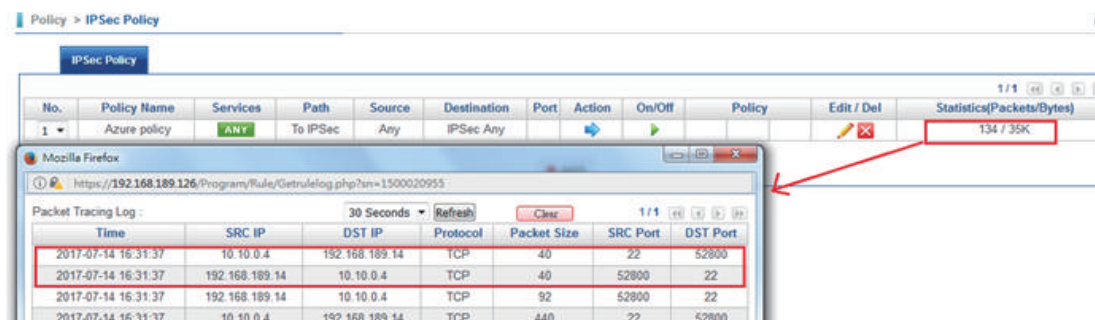
0 packages can be updated.
0 updates are security updates.

New release '16.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2019.

Last login: Fri Jul 14 06:03:23 2017 from 192.168.189.14
jamie@vm:~$
```

3. Policy > IPSec Policy，點選 Statistics，可看到封包記錄。

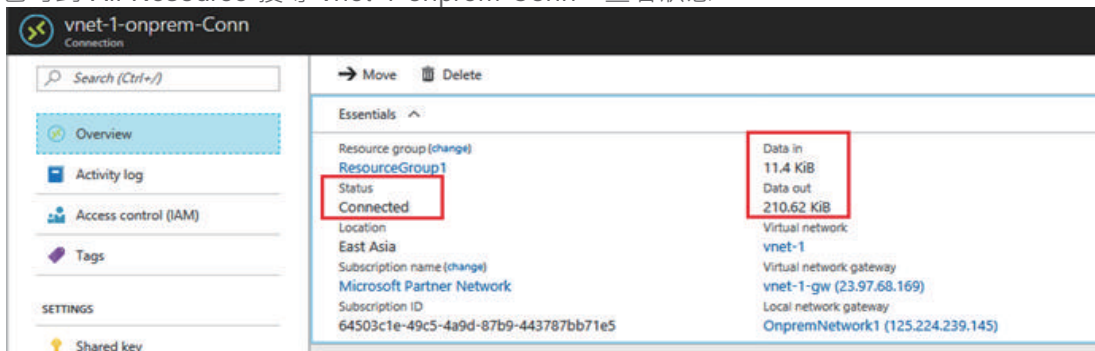


The screenshot shows the 'IPSec Policy' page in the Azure portal. The 'Statistics' tab is selected, displaying a table of packet tracing logs. The table has columns for Time, SRC IP, DST IP, Protocol, Packet Size, SRC Port, and DST Port. The data shows successful connections between 10.10.0.4 and 192.168.189.14.

No.	Policy Name	Services	Path	Source	Destination	Port	Action	On/Off	Policy	Edit / Del	Statistics(Packets/Bytes)
1	Azure policy	ANY	To IPSec	Any	IPSec Any						134 / 35K

Time	SRC IP	DST IP	Protocol	Packet Size	SRC Port	DST Port
2017-07-14 16:31:37	10.10.0.4	192.168.189.14	TCP	40	22	52800
2017-07-14 16:31:37	192.168.189.14	10.10.0.4	TCP	40	52800	22
2017-07-14 16:31:37	192.168.189.14	10.10.0.4	TCP	92	52800	22
2017-07-14 16:31:37	10.10.0.4	192.168.189.14	TCP	440	22	52800

4. 也可到 All Resource 搜尋 vnet-1-onprem-Conn，查看狀態。



The screenshot shows the 'vnet-1-onprem-Conn' resource page in the Azure portal. The 'Overview' tab is selected, displaying the status of the connection. The status is 'Connected'. The page also shows details about the resource group, location, and subscription.

Resource group: ResourceGroup1
Status: **Connected**
Location: East Asia
Subscription name: Microsoft Partner Network
Subscription ID: 64503c1e-49c5-4a9d-87b9-443787bb71e5

Data in: 11.4 KiB
Data out: 210.62 KiB
Virtual network: vnet-1
Virtual network gateway: vnet-1-gw (23.97.68.169)
Local network gateway: OnpremNetwork1 (125.224.239.145)