

# 配置到Azure的ASA IPsec VTI連線

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[驗證](#)

[疑難排解](#)

---

## 簡介

本文檔介紹如何配置到Azure的自適應安全裝置(ASA) IPsec虛擬隧道介面(VTI)連線。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 使用運行ASA 9.8.1或更高版本的公共靜態IPv4地址直接連線到網際網路的ASA。
- Azure帳戶

### 採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

在ASA 9.8.1中，IPsec VTI功能已擴展為使用IKEv2，但是，它仍然限制為sVTI IPv4 over IPv4。本配置指南是使用ASA CLI介面和Azure門戶生成的。Azure門戶的配置也可以透過PowerShell或API執行。有關Azure配置方法的詳細資訊，請參閱Azure文檔。



注意：目前，VTI僅在單情景路由模式下受支援。

---

## 設定

本指南假定尚未配置Azure雲。如果已建立資源，則可以跳過其中某些步驟。

步驟 1. 在Azure內配置網路。

這是居住在Azure雲中的網路地址空間。此地址空間必須足夠大，才能容納其中的子網（如圖所示）。

+ Create a resource

Home

Dashboard

All services

FAVORITES

All resources

Resource groups

### New

- Virtual network
- virtual network
- Virtual network gateway

Get started



Windows Server 2016 VM

[Quickstart tutorial](#)

Recently created

# Marketplace

## Get Started

Service Providers

## Management

Private Marketplace

Private Offer Management

## My Marketplace

Favorites

My solutions

Recently created

Private plans

## Categories

Networking (335)

Security (302)

Compute (193)

IT & Management Tools (169)

Storage (125)

Developer Tools (88)



## New! Get AI-generated suggestions

Ask AI to suggest products, articles, and solutions for w

virtual network

Azure benefit eligible only  Azure services only

Showing 1 to 20 of 8 results for 'virtual network'. [Clear search](#)



### Virtual network

Microsoft

Azure Service

Create a logical, isolated section in Microsoft Azure and securely connect it outward.

Create

Virtual network



### Virtual network gateway

Microsoft

Azure Service

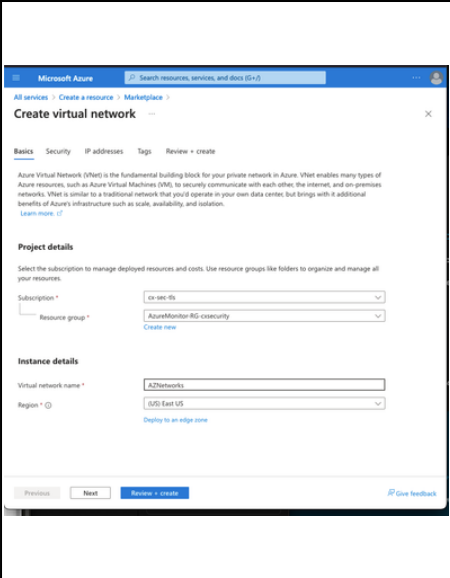
The VPN device in your Azure virtual network and used with site-to-site and VNet-to-VNet VPN connections.

Create



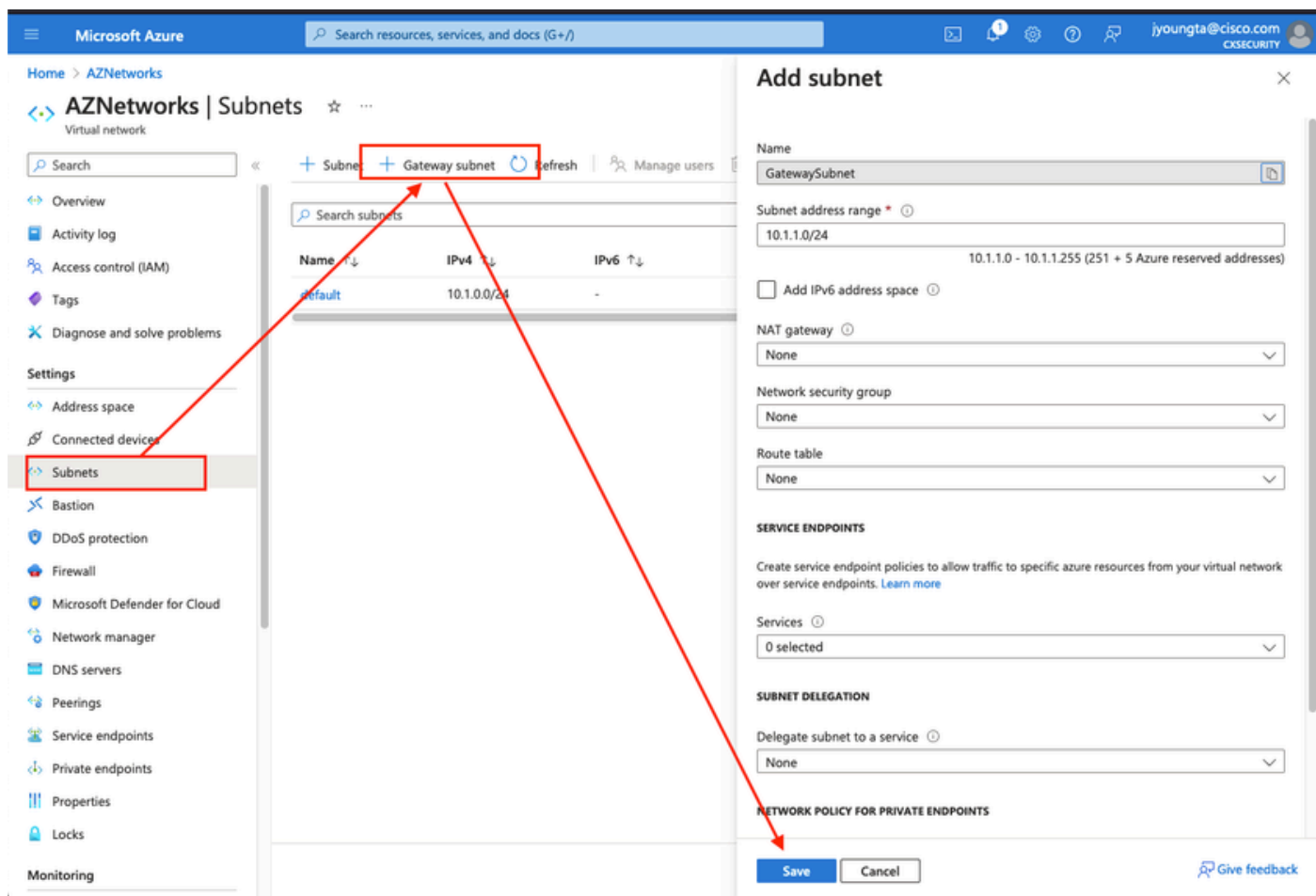
Virtual network



	名稱	雲中託管的IP地址空間的名稱
	地址空間	Azure中託管的整個CIDR範圍。本例中使用的是10.1.0.0/16。
	子網名稱	虛擬網路中建立的第一個子網名稱，VM通常連線到該虛擬網路。通常建立名為default的子網。
	子網地址範圍	在虛擬網路中建立的子網。

步驟 2. 修改虛擬網路以建立網關子網。

導航到虛擬網路並增加網關子網。本例中使用的是10.1.1.0/24。



步驟 3. 建立虛擬網路網關。

這是託管在雲中的VPN終端。這是ASA用來構建IPSec隧道的裝置。此步驟還會建立分配給虛擬網路網關的公共IP。完成此步驟可能需要15 – 20分鐘。

- + Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources

## New

virtual network gat

virtual network gat

Virtual network gateway

Get started



Home >

# Marketplace

## Get Started

Service Providers

## Management

Private Marketplace

Private Offer Management

## My Marketplace

Favorites

My solutions

Recently created

Private plans

## Categories

Networking (40)

Security (34)

Compute (19)

IT & Management Tools (9)

Web (8)

Developer Tools (4)



## New! Get AI-generated sugges

Ask AI to suggest products, articles, and solution

virtual network gateway

Publi

Prici

Azure benefit eligible only ⓘ

Azure services only

Showing 1 to 20 of 68 results for 'virtual network gateway'. [Clear se](#)



### Virtual network gateway

Microsoft

Azure Service

The VPN device in your Azure virtual network and used with site-to-site and VNet-to-VNet VPN connections.

Create

Virtual network gateway



### Local network gateway

Microsoft

Azure Service

Represents the VPN device in yo local network and used to set up site-to-site VPN connection.

Create

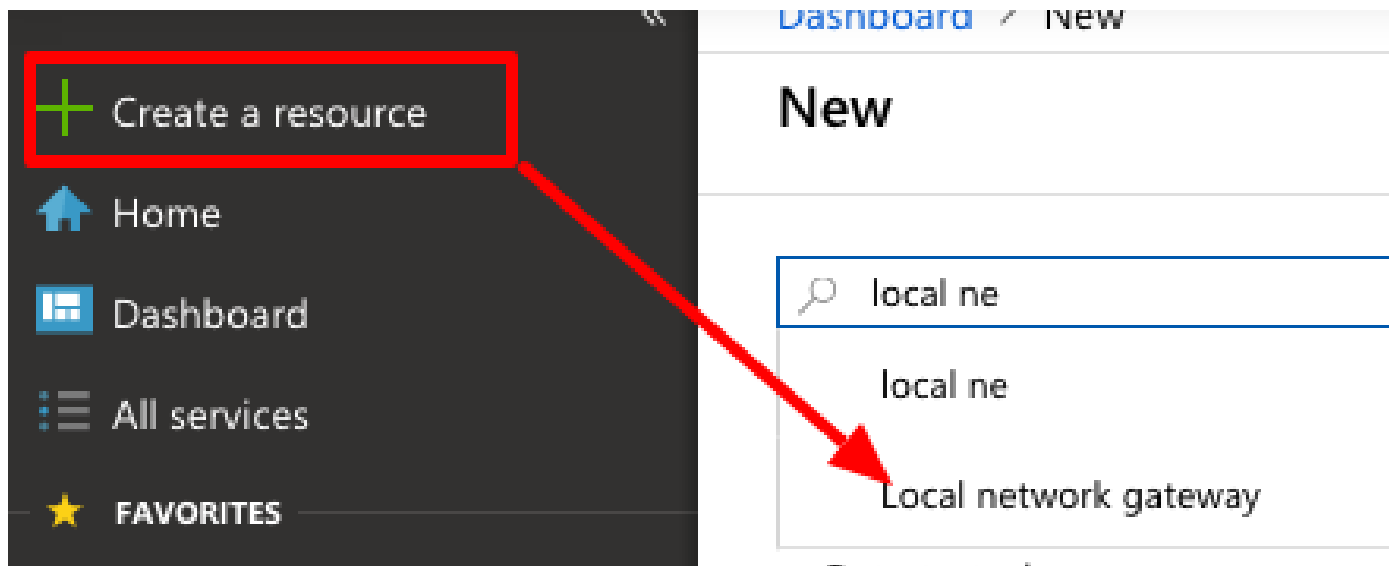
名稱

虛擬網路閘道的名稱

閘道型別	選擇VPN，因為這是IPSec VPN。
VPN型別	選擇Route-based，因為這是VTI。加密對映VPN完成後，使用基於策略的。
SKU	需要根據所需的流量量選擇VpnGw1或更高版本。Basic不支援邊界網關協定(BGP)。
啟用的主用/主用模式	請勿啟用。在發佈時，ASA沒有從環回中獲取BGP會話的功能或介面內部。Azure僅允許BGP對等使用1個IP地址。
公用IP位址	建立新的IP位址並為資源指定名稱。
配置BGP ASN	選中此框可在鏈路上啟用BGP。
ASN	保留此為預設65515。這是自我展示的ASN Azure。

步驟 4. 建立本地網路網關。

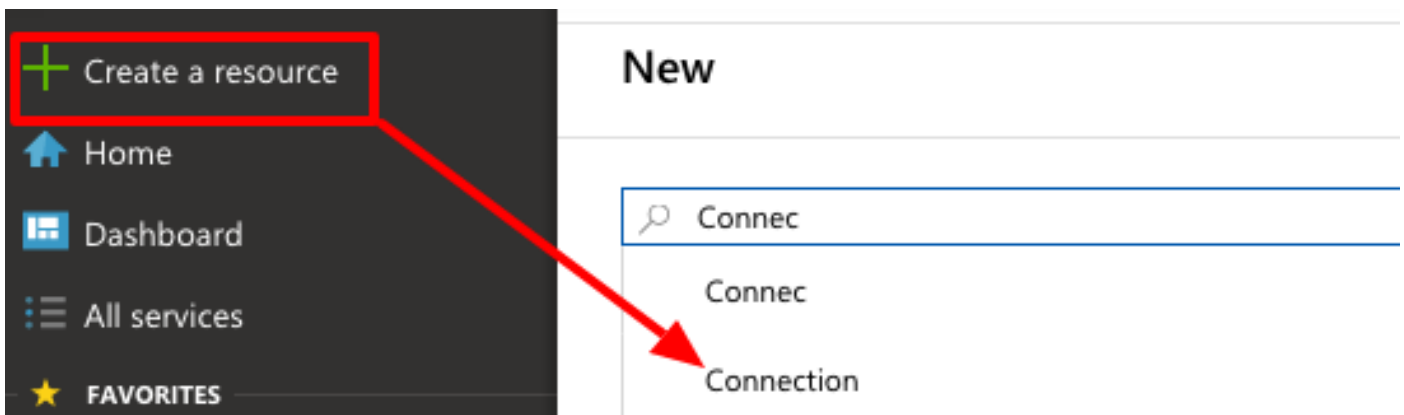
本地網路網關是代表ASA的資源。





	名稱	ASA的名稱
	IP 位址	ASA外部介面的公用IP地址。
	地址空間	稍後將在VTI上配置子網。
	配置BGP設定	選中此選項可啟用BGP。
	ASN	此ASN是在ASA上配置的。
	BGP對等體IP地址	IP地址在ASA VTI介面上配置。

步驟 5. 在虛擬網路網關和本地網路網關之間建立新連線，如圖所示。



# Create connection ...



**Basics** Settings Tags Review + create

Create a secure connection to your virtual network by using VPN Gateway or ExpressRoute.

[Learn more about VPN Gateway](#)

[Learn more about ExpressRoute](#)

## Project details

Subscription \*

Resource group \*  [Create new](#)

## Instance details

Connection type \*

Name \*

Region \*

**Review + create**

Previous

**Next : Settings >**

[Download a template for automation](#)

[Give feedback](#)

Home > Create a resource > Marketplace >

## Create connection



Basics Settings Tags Review + create

### Virtual network gateway

To use a virtual network with a connection, it must be associated to a virtual network gateway.

Virtual network gateway *	<input type="text" value="VNGW1"/>
Local network gateway *	<input type="text" value="ASA"/>
Shared key (PSK) *	<input type="text" value="....."/>
IKE Protocol	<input type="radio"/> IKEv1 <input checked="" type="radio"/> IKEv2
Use Azure Private IP Address	<input type="checkbox"/>
Enable BGP	<input checked="" type="checkbox"/>

**i** To enable BGP, the SKU has to be Standard or higher.

IPsec / IKE policy  Default  Custom

**i** When using custom IPsec/IKE policies, please ensure that the custom settings are appropriately configured on the on-premise device for both initial tunnel establishment and rekey.

IKE Phase 1	Encryption *	<input type="text" value="GCM_AES256"/>	Integrity/PRF *	<input type="text" value="SHA384"/>	DH Group *	<input type="text" value="DHGroup14"/>	
	IKE Phase 2(IPsec)	IPsec Encryption *	<input type="text" value="AES256"/>	IPsec Integrity *	<input type="text" value="SHA256"/>	PFS Group *	<input type="text" value="None"/>
	IPsec SA lifetime in KiloBytes *	<input type="text" value="0"/>	IPsec SA lifetime in seconds *	<input type="text" value="27000"/>	Use policy based traffic selector	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	DPD timeout in seconds *
Connection Mode	<input checked="" type="radio"/> Default <input type="radio"/> InitiatorOnly <input type="radio"/> ResponderOnly						

## Effective routes

Download Refresh

Showing only top 200 records, click Download above to see all.

Scope Virtual machine (jyoungta-ubuntu-azure)

Network interface jyoungta-ubuntu-azur956

### Effective routes

SOURCE	STATE	ADDRESS PREFIXES	NEXT HOP TYPE	NEXT HOP TYPE IP ADDRESS
Default	Active	10.1.0.0/16	Virtual network	-
Virtual network gateway	Active	192.168.100.0/30	Virtual network gateway	A.A.A.A
Virtual network gateway	Active	192.168.100.1/32	Virtual network gateway	A.A.A.A
Virtual network gateway	Active	192.168.2.0/24	Virtual network gateway	A.A.A.A
Default	Active	0.0.0.0/0	Internet	-
Default	Active	10.0.0.0/8	None	-
Default	Active	100.64.0.0/10	None	-
Default	Active	172.16.0.0/12	None	-
Default	Active	192.168.0.0/16	None	-

## 疑難排解

目前沒有特定資訊可用於對此組態進行疑難排解。

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。