# 配置到Azure的ASA IPsec VTI連線

目錄			
<u>簡介</u>			
<u>必要條件</u>			
<u>需求</u>			
<u>採用元件</u>			
<u>背景資訊</u>			
<u>設定</u>			
<u>驗證</u>			
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)。



<ul> <li>Microsoft Azure</li> </ul>		
All services > Create a resou	rce >	
Marketplace		
•		
Get Started		
Service Providers	🔶 New! Get A	Al-generated suggestions
	Ask Al to sugges	t products, articles, and solutions for w
Management		
Private Marketplace	virtual network	× P
Private Offer Management	Azure benefit eligiele only	Azure services only
-		U,
My Marketplace	Showing 1 to 20 of 8 results for '	virtual network'. <u>Clear search</u>
Favorites		
My solutions	<>	<>
Recently created	Virtual network	Virtual network gateway
Brinste stars	Microsoft	Microsoft
Private plans	Azure Service	Azure Service
Categories	Create a logical solated section in	The VPN device in your Azure virtual
1	Microsoft Azure and securely connect it outverd.	network and used with site-to-site and VNet-to-VNet VPN connections.
Networking (333)		
Security (302)	1 🗡	
Compute (193)	Create 🗸 🗢	Create 🗸 🗢 🗢
IT & Management Tools (169)	Virtual nework	
Storage (125)		
Development To als (0.8)	Virtual network	•

Moreourf Asure     Starth resource; univer, and dec (5r,1)     Water Sono > Create a resource > Marketplace >     Create a virtual network ×	名稱	雲中託管的IP地址空間的名稱		
Basics Security (P-addresses Togs Review+ oracle     Aner Varual Mitseler, (Merc) site Madaeweet Judiding Mock Norycommunicate with each state. White multies many types of     Aner reviews: a Machari Varual Mitseler, (Merc) and Machari Mitseler, (Merc) and Machari Mitseler, (Merc) and Machari Machari Mitseler, (Merc) and Machari Mitseler, (Merc) and Machari Machari Mitseler, (Merc) and Machari Machari Mitseler, (Merc) and Machari Machi Machari Machari Machari Machari Machari Machari Machari Machari	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。		
your morent. SuburyIsten * (n see. 6) Resource group * Austrationative RG casecutry Create rowe Instance details What intervers same * <u>Alternoots</u> Region * O <u>Deping to an edge core</u>	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。		
Press. Not Revenues and Revenues	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。

Microsoft Azure	Search resources, services, and docs (G+/)	国 🖓 ③ ⑦ 反 jyoungta@cisco.com 🤐
Home > AZNetworks	A	dd subnet ×
AZNetworks   Subnet Virtual network	ts ☆ …	
	+ Subne: + Gateway subnet 🕐 Kefresh   🖄 Manage users 💈	me iatewaySubnet
Overview	Search subpots	bnet address range * 💿
Activity log	10	0.1.1.0/24
Access control (IAM)	Name 1↓ IPv6 ↑↓	10.1.1.0 - 10.1.1.255 (251 + 5 Azure reserved addresses)
🔷 Tags	otfault 10.1.0.0/24 -	Add IPv6 address space 🛈
X Diagnose and solve problems	NA	T gateway 🛈
Settings	N	lone
Address space	Net	twork security group
Ø Connected device		ione V
Subnets	Roy	ute table
✓ Bastion		vuie v
ODoS protection	SER	RVICE ENDPOINTS
😨 Firewall	Cre	ate service endpoint policies to allow traffic to specific azure resources from your virtual network
Microsoft Defender for Cloud	ove	er service endpoints. Learn more
O Network manager	Ser	nvices ①
DNS servers		selected
* Peerings	SUE	BNET DELEGATION
Service endpoints	Def	legate subnet to a service ①
Private endpoints	N	lone V
Properties		
Locks	ner.	TWORK POLICY FOR PRIVATE ENDPOINTS
Hadada		Save Cancel O-Give feedback
Monitoring		

#### 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。



#### Home >

# Marketplace



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。

	"	Dashboard / New
+ Create a resource		New
🛧 Home		
🔲 Dashboard		,
E All services		local ne
🛨 FAVORITES		Local network gateway

Home > Create a resource > Marketplace > Create local network gateway ··· ×			名稱	ASA的名稱
Basics Advanced Review + create A local network gateway is a specific object that represents an on-premises location (the site) for routing purposes. Learn more O			IP 位址	ASA外部介面的公用 IP地址。
Project details Subscription * Resource group * Instance details	α-sec-tis     ∨       α-sec-tis-rg     ∨       Create new		地址空間	稍後將在VTI上配置 子網。
Region * Name * Endpoint ①	East US V ASA V (P address) FQDN		配置BGP設 定	選中此選項可啟用 BGP。
IP address * () Address Space(s) () 192.168.100.0/30 Add additional address range	     		ASN	此ASN是在ASA上 配置的。
Review + create Previous	Next : Advanced >		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 a resource	New
🛧 Home	
📴 Dashboard	
∃ All services	Connec
🛨 FAVORITES	Connection

Home > Create a resource > Marketplace >						
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 2						
Learn more about expressionate in						
Project details						
Subscription *	cx-sec-tls	$\sim$				
Resource group *	cx-sec-tis-ra					
Resource group	Create new					
Instance details						
Connection type * ①	Site-to-site (IPsec)	$\sim$				
Name *	VPNTunnel1	~				
Region *	East US	$\sim$				
Review + create Previous	Next : Settings > Download a template for automation	Give feedback				

L.

🗧 🕘 🗧 🔝 🔥 Create connectio	on - Microsoft // X Duo Security - Two-Factor Auth X +	~
← → C O A == https://	portal.azure.com/#create/Micros 😚 🏠 🗢 💽 🛃 🕻 🕕 🏶	බ එ ≡
실 Getting Started	ghtning GIT   ASA License Gener 🕀 ASA License Gener 🔀 Cisco SecureX	»
■ Micros P Search resources, ser	vices, and docs (G+/) 🗵 🗘 🍥 🖓 įyoungta	
Home > Create a resource > Marketpla	ice >	
Create connection		$\times$
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 * 🕕	VNGW1 V	
Local network gateway * 🕕	ASA	
Shared key (PSK) * ①	······	
IKE Protocol ③	○ IKEv1 ● IKEv2	
Use Azure Private IP Address 🕕		
Enable BGP ①	✓	
1 To enable BGP, the SKU has to be Star	ndard or higher.	
IPsec / IKE policy ①	Default Custom	
	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 ③	Encryption * Integrity/PRF * DH Group *	
	GCMAES256 V SHA384 V DHGroup14 V	
IKE Phase 2(IPsec)	IPsec Encryption * IPsec Integrity * PFS Group *	
	AES256 V SHA256 V None V	
IPsec SA lifetime in KiloBytes * 🛈	0	
IPsec SA lifetime in seconds * ①	27000	
Use policy based traffic selector $\ \ \odot$	Enable Disable	
DPD timeout in seconds * ④	45 🗸	
Connection Mode ①	Default      InitiatorOnly      ResponderOnly	
Review + create Previous	Next : Tags > Download a template for automation	Give feedback

Dashboard > Resource groups > CX-SecurityTLs-ResourceGroup > jyoungta-ubuntu-azure - Diagnose and solve problems > Effective routes								
Effective routes								
🛓 Download 🛛 👌 Refres	🚽 Download 🛛 👌 Refresh							
Showing only top 200 re	ecords, c	lick Download abov	e to see all.					
Scope		Virtual machine (jy	oungta-ubuntu-azure)					
Network interface		jyoungta-ubuntu	-azur956		~			
Effective routes								
SOURCE T	STATE	$\uparrow_{\Downarrow}$	ADDRESS PREFIXES	¢ψ	NEXT HOP TYPE	$\uparrow \downarrow$ NEXT HOP TYPE IP ADDRESS $\uparrow \downarrow$		
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		10.0.0/8		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)。