配置到Azure的ASA IPsec VTI连接

Ħ	录
<u>简</u> :	<u>ዮ</u>
<u>先</u>)	<u> </u>
	<u>要求</u>
	<u>使用的组件</u>
背	
配	
<u>验</u> ì	<u>r</u>
故	章 <u>排除</u>

简介

本文档介绍如何配置到Azure的自适应安全设备(ASA) IPsec虚拟隧道接口(VTI)连接。

先决条件

要求

Cisco 建议您了解以下主题:

- 使用运行ASA 9.8.1或更高版本的公共静态IPv4地址直接连接到互联网的ASA。
- Azure帐户

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

背景信息

在ASA 9.8.1中,IPsec VTI功能已扩展为使用IKEv2,但是,它仍然限制为通过IPv4的sVTI IPv4。 此配置指南是使用ASA CLI界面和Azure门户生成的。Azure门户的配置也可以由PowerShell或 API执行。有关Azure配置方法的详细信息,请参阅Azure文档。



注意:目前,VTI仅在单情景路由模式下受支持。

配置

本指南假设Azure云尚未配置。如果已建立资源,则可以跳过其中某些步骤。

步骤1:在Azure中配置网络。

这是位于Azure云中的网络地址空间。此地址空间必须足够大,才能容纳其中的子网(如图所示)。



 Microsoft Azure 		
All services > Create a resou	rce >	
Marketplace		
•		
Get Started		
Service Providers	A 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	•

Moreoufl Assum Statch resource, savines, and doct (5-/) Mill sarioton - > Charles a resource - > Markingbae -> Create survitual network ×	名称	云中托管的IP地址空间的名称	
Basic Security IP addresses Tags Review + oracle Asser Visual Network (Netric tare for detailerented building block for granners used and advect that advect the internet, and on premise that are struct to a building block for granners used at a building block for granners used at a building block for granners and the advect that adve	地址空 间	Azure中托管的整个CIDR范围。本例中使用的是 10.1.0.0/16。	
your movers. Suburytion * ca set dh Resurve group * Aunstholour MC cascurity Crain now Instance details Whul Interork same *Affetenots. Region * Digit dat US Digits are using nome	子网名 称	在通常连接VM的虚拟网络内创建的第一个子网的名称。 通常创建一个名为default的子网。	
Promoti Team Constanting	子网地 址范围	在虚拟网络中创建的子网。	

第二步:修改虚拟网络以创建网关子网。

导航到虚拟网络并添加网关子网。本例中使用的是10.1.1.0/24。

Microsoft Azure	Search resources, services, and docs (G+/)	国家 🖓 ③ ⑦ 戻 jyoungta@cisco.com 🤐
Home > AZNetworks		Add subnet ×
AZNetworks Subnet Virtual network	ts 🛪 …	
© Search «	+ Subnet + Gateway subnet C Refresh 8 Manage users	Name
(c) Ourning	1	GatewaySubnet
•• Overview	P Search subjects	Subnet address range * 🕕
Activity log	Name L IPv4 L IPv6 ↑	10.1.1.0/24 10.1.1.0 - 10.1.1.255 (251 + 5 Azure reserved addresses)
Access control (IAM)	1010004	Add IPv6 address space
Tags	eraut IV. I.V.Vyde	
X Diagnose and solve problems		NAT gateway ()
Settings		
Address space	$\langle \rangle$	None
S Connected devices		Deute deble
Subnets		None
✓ Bastion		
DDoS protection		SERVICE ENDPOINTS
😔 Firewall	$\mathbf{\lambda}$	Create service endpoint policies to allow traffic to specific azure resources from your virtual network
Microsoft Defender for Cloud		over service endpoints. Learn more
S Network manager		Services ①
DNS servers		0 selected V
A Peerings		SUBNET DELEGATION
Senire endnoints	\mathbf{N}	Delegate subset to a consise (i)
Drivate endpoints		None V
U Dependier		
Properties		NETWORK POLICY FOR PRIVATE ENDPOINTS
LOCKS		
Monitoring		Save Cancel Q Give feedback

第三步: 创建虚拟网络网关。

这是托管在云中的VPN终端。这是ASA用来构建IPSec隧道的设备。此步骤还会创建分配给虚拟网络网关的公共IP。 完成此步骤可能需要15 – 20分钟。



Home >

Marketplace



名称

网关类型	选择VPN,因为这是IPsec VPN。				
VPN类型	选择Route-based,因为这是VTI。加密映射VPN完成后,使用基于策略的。				
SKU	需要根据所需的流量量选择VpnGw1或更高版本。基本不支持 边界网关协议(BGP)				
已启用主用/主用模式	不启用。在发布时,ASA没有从环回获取BGP会话的功能 或接口内部。Azure仅允许BGP对等的1个IP地址。				
公共 IP 地址	创建新的IP地址并为资源指定名称。				
配置BGP ASN	选中此框可在链路上启用BGP。				
ASN	将此项保留为默认65515。这是ASN Azure展示自身。				

第四步: 创建本地网络网关。

本地网络网关是代表ASA的资源。

	"	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 ···· ×			名称	ASA的名称
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 C			IP Address	ASA外部接口的公用 IP地址。
Project details Subscription * Resource group * Instance details	cx-sec-tis-rg ~		地址空间	稍后将在VTI上配置 子网。
Region * [Name * [Endpoint ①	East US ASA P address FQDN		配置BGP设 置	选中此复选框可启 用BGP。
IP address * ③ Address Space(s) ③ 192.168.100.0/30 Add additional address range	1214 V		ASN	此ASN在ASA上配 置。
Review + create Previous	Next : Advanced >		BGP对等体 IP地址	IP地址在ASA VTI接 口上配置。

第五步: 在虚拟网络网关和本地网络网关之间创建新连接, 如图所示。

+ 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	n - Microsoft JLX Duo Security - Two-Factor Auth X +	~
← → C O A == https://p	oortal.azure.com/#create/Micros: 68 ☆ 🛛 📀 👔 🕻 🛈 🚸	ම ර ≡
실 Getting Started ⊕ Getting Started 🧧 Lig	htning GIT ⊕ ASA License Gener	»
■ Micros P Search resources, ser	vices, and docs (G+/) 🗵 🗘 🐵 🕐 😥 iyoungt	a@cisco.com
Home > Create a resource > Marketpla	ce >	
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 * 🕕	VNGW1 V	
Local network gateway * 🕡	ASA	
Shared key (PSK) * ①	······ ✓	
IKE Protocol ①	○ IKEv1 ● IKEv2	
Use Azure Private IP Address ①		
Enable BGP ①		
1 To enable BGP, the SKU has to be Star	idard 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 ①	Encryption * Integrity/PRF * DH Group *	
	GCMAES256 V SHA384 V DHGroup14 V	
IKE Phase 2(IPsec) ③	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 \bigcirc	Enable Disable	
DPD timeout in seconds *	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 🛛 👌 Refre	🕹 Download 🛛 💍 Refresh							
Showing only top 200 i	Showing only top 200 records, click Download above to see all.							
Scope		Virtual machine (j	/oungta-ubuntu-azure)					
Network interface		jyoungta-ubuntu	ı-azur956		~			
Effective routes								
SOURCE Tu	STATE	Ϋ́υ	ADDRESS PREFIXES	\uparrow_{\downarrow}	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		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	-		

故障排除

当前没有故障排除此配置的特定可用资料。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。