Configure ASA IPsec VTI Connection to Azure

Contents

<u>Prerequisites</u>	
Requirements	
Components Used	
Background Information	
Configure	
Verify	
Troubleshoot	

Introduction

This document describes how to configure an Adaptive Security Appliance (ASA) IPsec Virtual Tunnel Interface (VTI) connection to Azure.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- An ASA connected directly to the Internet with a public static IPv4 address that runs ASA 9.8.1 or later.
- An Azure account

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

In ASA 9.8.1, the IPsec VTI feature was extended to utilize IKEv2, however, it is still limited to sVTI IPv4 over IPv4. This configuration guide was produced with the use of the ASA CLI interface and the Azure Portal. The configuration of the Azure portal can also be performed by PowerShell or API. For more information about the Azure configuration methods, refer to the Azure documentation.



Note: Currently, VTI is only supported in single-context, routed mode.

Configure

This guide assumes that the Azure cloud has not been configured. Some of these steps can be skipped if the resources are already established.

Step 1. Configure a network within Azure.

This is the network address space that lives in the Azure Cloud. This address space must be large enough in order to accommodate sub-networks within them as shown in the image.



 Microsoft Azure 		
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 outvard.	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	•

E Klonech Acore (7: Seech resources, services, and dates (5x) 🔕	Name	A Name for the IP Address Space Hosted in the Cloud
All anvies : Conta remove : Maingline : Create virtual network - Keisa Scorty Padoross tap Review - create	Address	The whole CIDR range hosted in Azure. In this example,
And Virtual Network (Netry is the fundamental building block for your private methods in Auxo. Whet enables many types of Anore monoses, such as Anar Virtual Madhene (MB) is sociedly communicate with such other, the interact, and on-present benefits of Anars Initiative Centre and a such association of a social social social social social social latent social Anars Initiative Centre and a social availability, and instations.	Space	10.1.0.0/16 is used.
Project details Serve the advorging to the meager deployed resources and cash, the resource groups, like folders to organize and meager all point resource groups. Selvergrins* If serve for advorging the folders to organize and meager all point resource groups. Measure groups* If serve for advorging the folders to organize and measure advorging the folders to organize and measure advorging the folders to organize and measure advorging the folders to organize advorging the folders to	Subnet Name	The name for the first subnet created within the virtual network to which VMs are usually attached. A subnet called default is usually created.
Protect Nort Record a cetals. If Gas Institute	Subnet Address range	A subnet created within the Virtual Network.

Step 2. Modify the Virtual Network in order to create a Gateway Subnet.

Navigate to the **Virtual network** and add a gateway subnet. In this example, 10.1.1.0/24 is used.

Microsoft Azure	≫ Search resources, services, and docs (G+/)	اين پېرونه کې 🕲 😥 🖾 🗵 🖾 🕹
Home > AZNetworks	A	dd subnet ×
AZNetworks Subnets Virtual network	S ☆ …	
	+ Subne + Gateway subnet 🕐 Kefresh 🖄 Manage users 💈 🕼	me iatewaySubnet
Overview	Search subnets Sub	bnet address range * 💿
Activity log	10	0.1.1.0/24
Access control (IAM)	Name ↓ IPv4 ↓ IPv6 ↑↓	10.1.1.0 - 10.1.1.255 (251 + 5 Azure reserved addresses)
🗳 Tags	Afault 10.1.0.0/24 -	Add IPv6 address space ①
× Diagnose and solve problems	NA	iT gateway ⊙
Settions	N	lone v
A Address source	Net	twork security group
Autress space	N	lone v
b Connected devices	Roy	ute table
Subnets	N	lone 🗸
>> Bastion	SER	RVICE ENDPOINTS
DDoS protection		
😨 Firewall	ove	rate service endpoint policies to allow traffic to specific azure resources from your virtual network er service endpoints. Learn more
Microsoft Defender for Cloud	Ser	rvices ①
o Network manager		selected
DNS servers		
1 Peerings	SUB	BNET DELEGATION
Service endpoints	Del	legate subnet to a service ①
(I) Private endpoints	N	lone v
Properties	Art	TWORK POLICY FOR PRIVATE ENDPOINTS
Locks		
Monitoring		Save Cancel & Give feedback
L		

Step 3. Create a Virtual Network Gateway.

This is the VPN endpoint that is hosted in the cloud. This is the device that the ASA builds the IPsec tunnel with. This step also creates a public IP which is assigned to the Virtual network gateway. This step can take 15 - 20 minutes to complete.



Home >

Marketplace



Name Name for the Virtual Network Gateway

Gateway Type	Select VPN as this is an IPsec VPN.
VPN Type	Select Route-based because this is a VTI. Policy-based is used when a crypto map VPN is done.
SKU	Need to select VpnGw1 or greater based on the amount of traffic needed. Basic does not support Border Gateway Protocol (BGP).
Enabled active/active mode	Do not enable. At the time of posting, the ASA does not have the capability to source the BGP session from a loopback or inside the interface. Azure only allows 1 IP address for the BGP peering.
Public IP address	Create a new IP address and assign a name to the resource.
Configure BGP ASN	Check this box to enable BGP on the link.
ASN	Leave this as the default 65515. This is the ASN Azure that presents itself.

Step 4. Create a Local Network Gateway.

A Local network gateway is the resource that represents the ASA.

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

Home > Create a resource > Marketplace >	Name	A Name for the ASA
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 of	IP Address	The public IP address of the ASA's outside interface.
Project details Subscription * CX-sec-tis CX-sec-tis-tg Create new Create new	Address Space	The subnet is configured on the VTI later.
Instance details Region * East US Name * ASA Instance details Region * East US Instance details Instance	Configure BGP Settings	Check this to enable BGP.
Address Space(s) ③ 192.168.100.0/30 Add additional address range	ASN	This ASN is configured on the ASA.
Review + create Previous Next : Advanced >	BGP peer IP address	The IP address is configured on the ASA VTI interface.

Step 5. Create a new connection between the Virtual network gateway and the Local network gateway as shown in the image.

+ Create a resource	New
🛧 Home	
📴 Dashboard	,○ Connec
E All services € E All services	Connec
- 🛨 FAVORITES	Connection

Home > Create a resource > Marketplace >						
Create connection	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 connecti	on - Microsoft // × Duo Security	- Two-Fact	tor Auth × +					~	
← → C O A == https://	portal.azure.com/#create/Microso	<mark>6</mark> 8 ☆	S 🕞	89 87	C:	•		ப்	≡
실 Getting Started 🕀 Getting Started 🔽 Li	ghtning GIT 🕀 ASA License Gener	⊕ asa i	License Gener	×c	sco Secu	ıreX			»
■ Micros 🖉 Search resources, se	rvices, and docs (G+/)		0 ®	0	8	jyoungta	ecisco costo	.com URITY	0
Home > Create a resource > Marketpl	ace >								
Create connection								>	<
Basics Settings Tags Review	+ create								
Virtual network gateway									
To use a virtual network with a connection	n, it must be associated to a virtual ne	twork gat	eway.						
Virtual network gateway * 🕕	VNGW1					\sim			
Local network gateway * 🕕	ASA					\sim			
Shared key (PSK) * ①						~			
IKE Protocol	() IKEv1 () IKEv2								
Lice Anura Private IP Address									
Enable BGP ()									
To apple BCD the SVII has to be Sta	ndard or biobor								
To enable boy, the SKO has to be sta	ndard or nigher.								
IPsec / IKE policy ①	Default Custom								
	When using custom IPSec/IKE pol are appropriately configured on t	licies, pleas	se ensure that the	custon	n settings al tunnel				
	establishment and rekey.	ine on pres		201111110	ar consider				
IKE Phase 1 ①	Encryption * Integrity/PF	te •	DH Group *						
	GCMAES256 V SHA384	\sim	DHGroup14	~					
IKE Phase 2(IPsec)	IPsec Encryption * IPsec Integ	prity *	PFS Group *						
	AES256 V SHA256	\sim	None 🗸]					
IPsec SA lifetime in KiloBytes * 🕕	0								
IPsec SA lifetime in seconds *	27000								
Use policy based traffic selector ①	Enable Disable								
DPD timeout in seconds * ①	45					~			
Connection Mode ①	Default InitiatorOnly	Respon	nderOnly						
Review + create Previous	Next : Tags > Download a to	emplate fo	or automation				Give f	eedba	ack

Step 6. Configure the ASA.

in order to validate layer 3 routing and layer 4 connectivity for BGP or the endpoint resources if you use static routing.

<#root> ciscoasa# ping 10.1.2.254 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.1.2.254, timeout is 2 seconds: 11111 Success rate is 100 percent (5/5), round-trip min/avg/max = 40/42/50 ms ciscoasa# ping tcp 10.1.2.254 179 Type escape sequence to abort. No source specified. Pinging from identity interface. Sending 5 TCP SYN requests to 10.1.2.254 port 179 from 192.168.100.1, timeout is 2 seconds: 11111 Success rate is 100 percent (5/5), round-trip min/avg/max = 41/42/42 ms ciscoasa#

Step 4. When you use BGP, verify BGP connectivity routes received and advertised to Azure and the routing table of the ASA.

<#root>

ciscoasa#

show bgp summary

BGP router identifier 192.168.100.1, local AS number 65000 BGP table version is 6, main routing table version 6 4 network entries using 800 bytes of memory 5 path entries using 400 bytes of memory 2/2 BGP path/bestpath attribute entries using 416 bytes of memory 1 BGP AS-PATH entries using 24 bytes of memory 0 BGP route-map cache entries using 0 bytes of memory 0 BGP filter-list cache entries using 0 bytes of memory BGP using 1640 total bytes of memory BGP activity 14/10 prefixes, 17/12 paths, scan interval 60 secs Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 10.1.2.254 4 65515 73 60 6 0 0

01:02:26 3

ciscoasa#

show bgp neighbors 10.1.2.254 routes

BGP table version is 6, local router ID is 192.168.100.1 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, r RIB-failure, S Stale, m multipath Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Weight Path *> 10.1.0.0/16 10.1.2.254 0 65515 i <<< This is the virtual network def: 192.168.100.0/30 10.1.2.254 0 65515 i r> 192.168.100.1/32 10.1.2.254 0 65515 i Total number of prefixes 3 ciscoasa# show bgp neighbors 10.1.2.254 advertised-routes BGP table version is 6, local router ID is 192.168.100.1 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, r RIB-failure, S Stale, m multipath Origin codes: i - IGP, e - EGP, ? - incomplete Metric LocPrf Weight Path Network Next Hop *> 192.168.2.0 0.0.0.0 0 32768 i <<< These are the routes being advert *> 192.168.100.0/30 0.0.0.0 32768 i 0 <<< Total number of prefixes 2 ciscoasa# ciscoasa# show route Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, + - replicated route Gateway of last resort is 10.1.251.33 to network 0.0.0.0 S* 0.0.0.0 0.0.0.0 [1/0] via B.B.B.C, outside 10.1.0.0 255.255.0.0 [20/0] via 10.1.1.254, 01:03:33 в 10.1.2.254 255.255.255.255 [1/0] via 192.168.100.2, AZURE S B.B.B.A 255.255.255.224 is directly connected, outside С L B.B.B.B 255.255.255.255 is directly connected, outside С 192.168.2.0 255.255.255.0 is directly connected, inside L 192.168.2.2 255.255.255.255 is directly connected, inside С 192.168.100.0 255.255.255.252 is directly connected, AZURE

L 192.168.100.1 255.255.255 is directly connected, AZURE

Step 5. Ping a device over the tunnel. In this example, it is an Ubuntu VM that runs in Azure.

```
<#root>
ciscoasa# p
ing 10.1.0.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.0.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/42/50 ms
```

View the effective routes on the remote VM now. They must show the routes the ASA advertised to the cloud as shown in the image.

Dashboard > Resource groups > CX-SecurityTLs-ResourceGroup > jyoungta-ubuntu-azure - Diagnose and solve problems > Effective routes							
Effective routes	Effective routes						
🛓 Download 🛛 Download							
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	$\uparrow \downarrow$ NEXT HOP TYPE IP ADDRESS $\uparrow \downarrow$				
Default Active	e 10.1.0.0/16	Virtual network	-				
Virtual network gateway Active	e 192.168.100.0/30	Virtual network gateway	A.A.A.A				
Virtual network gateway Active	e 192.168.100.1/32	Virtual network gateway	A.A.A.A				
Virtual network gateway Active	e 192.168.2.0/24	Virtual network gateway	A.A.A.A				
Default Active	e 0.0.0.0/0	Internet	-				
Default Active	e 10.0.0/8	None	-				
Default Active	e 100.64.0.0/10	None	-				
Default Active	e 172.16.0.0/12	None	-				
Default Active	e 192.168.0.0/16	None	-				

Troubleshoot

There is currently no specific information available to troubleshoot this configuration.