# Configura connessione VTI IPsec ASA ad Azure

## Sommario

roduzione	
erequisiti	
Requisiti	
Componenti usati	
emesse	
onfigurazione	
erifica	
soluzione dei problemi	

## Introduzione

In questo documento viene descritto come configurare una connessione VTI (Virtual Tunnel Interface) di ASA (Adaptive Security Appliance) ad Azure.

# Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- ASA connessa direttamente a Internet con un indirizzo IPv4 statico pubblico con ASA 9.8.1 o versioni successive.
- Un account di Azure

### Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

In ASA 9.8.1, la funzionalità VTI di IPsec è stata estesa per utilizzare IKEv2, ma è ancora limitata a sVTI IPv4 su IPv4. Questa guida alla configurazione è stata prodotta con l'uso dell'interfaccia CLI di ASA e del portale di Azure. La configurazione del portale di Azure può essere eseguita anche da PowerShell o dall'API. Per ulteriori informazioni sui metodi di configurazione di Azure, consultare la documentazione di Azure.



Nota: attualmente la tecnologia VTI è supportata solo in modalità di routing a contesto singolo.

## Configurazione

In questa guida si presume che il cloud di Azure non sia stato configurato. Alcuni di questi passaggi possono essere ignorati se le risorse sono già state stabilite.

Passaggio 1. Configurare una rete in Azure.

Spazio degli indirizzi di rete che risiede nel cloud di Azure. Questo spazio di indirizzi deve essere

sufficientemente ampio da contenere le sottoreti al loro interno, come mostrato nell'immagine.

Microsoft Azure				2	Search re:
	Oashboard > New     New     Oashboard > New     Oashboard	v			
+ Create a resource	New				$\Box \times$
🛧 Home					
📴 Dashboard		k l			×
≣ All services	Virtual networ	k V			
	Virtual networ	'k gateway			
All resources	Get started		Windows Server 2016 VM Quickstart tutorial		
😭 Resource groups	Recently create	d			

<ul> <li>Microsoft Azure</li> </ul>		
All services > Create a resou	nce >	
Marketplace		
Get Started		
Service Providers	A New! Get A	I-generated suggestions
	Ask Al to suggest	products, articles, and solutions for w
Management		$\sim$
Private Marketplace	virtual network	× P
Private Offer Management	Azure benefit eligie e only	Azure services only
		<u> </u>
My Marketplace	Showing 1 to 20 of 8 results for V	rirtual network'. <u>Clear search</u>
Favorites	R	
My solutions	<->	$\leftrightarrow$
Recently created	Virtual network	Virtual network gateway
Relate slass	Microsoft	Microsoft
Private plans	Azure Service	Azure Service
Categories	Create a logical solated section in	The VPN device in your Azure virtual
Naturalian (220)	connect it outvard.	and VNet-to-VNet VPN connections.
Networking (555)		
Security (302)		
Compute (193)	Create 🗸 🗢	Create 🗸 🗢
IT & Management Tools (169)	Virtual network	
Storage (125)	( A A	
On other Table 2049	Virtual network	•

	Nome	Nome dello spazio di indirizzi IP ospitato nel cloud
Moreach Acces     Sense memores works, works, and data (inc)     Central memores     Sense sense      Sense sense sense      Sense sense      Sense sense      Sense sense      Sense sense      Sense sense      Sense sense sense      Sense sense sense      Sense sense sense sense      Sense sense sense sense sense      Sense sense sense sense sense      Sense sense sense sense      Sense sense      Sense sense sense      Sense sense sense	Spazio indirizzi	L'intero intervallo CIDR ospitato in Azure. Nell'esempio viene utilizzato 10.1.0.0/16.
Project details         Server the subscription to measure details, the resource groups like follow to anywork and measure and processory.         Selverytions*	Nome subnet	Il nome della prima subnet creata all'interno della rete virtuale a cui in genere sono collegate le VM. In genere viene creata una subnet denominata default.
Protoco Net Rovers - create Protoco Contract	Intervallo indirizzi subnet	Subnet creata all'interno della rete virtuale.

Passaggio 2. Modificare la rete virtuale per creare una subnet gateway.

Passare alla rete virtuale e aggiungere una subnet del gateway. Nell'esempio viene utilizzato 10.1.1.0/24.

	℅ Search resources, services, and docs (G+/)	🗾 🖓 🛞 🖓 📈 jyoungta@cisco.com 🤮
Home > AZNetworks		Add subnet ×
AZNetworks   Subnetwork	ts ☆ …	
Search «	+ Subnet + Gateway subnet 🔿 Befresh 🛛 🖧 Manage users	Name
Overview		GatewaySubnet
	P Search subprts	Subnet address range * ③
Activity log	Name 🖕 IPv4 🖕 IPv6 ↑↓	10.1.1.0/24 10.1.1.0 - 10.1.1.255 (251 + 5 Azure reserved addresses)
Access control (IAM)     Tags	fault 10.1.0.0/24	Add IPv6 address space ①
X Diagnose and solve problems		NAT gateway 💿
C. 11	$\backslash$	None
Settings	$\langle \rangle$	Network security group
Co Address space		None
𝔅 Connected device	$\mathbf{\lambda}$	Route table
Subnets		None
X Bastion	$\langle \rangle$	
DDoS protection	$\langle \rangle$	SERVICE ENDPOINTS
😨 Firewall		Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more
Microsoft Defender for Cloud		
o Network manager		Services ()
DNS servers	$\mathbf{X}$	V PROCING V
Peerings	$\mathbf{X}$	SUBNET DELEGATION
Service endpoints		Delegate subnet to a service ③
Operation of the second sec		None
Properties		NETWORK POLICY FOR PRIVATE ENDPOINTS
Locks		
Monitoring		Save Cancel

Passaggio 3. Creare un gateway di rete virtuale.

Endpoint VPN ospitato nel cloud. Questo è il dispositivo con cui l'ASA crea il tunnel IPsec. In

questo passaggio viene inoltre creato un IP pubblico assegnato al gateway della rete virtuale. Questo passaggio può richiedere da 15 a 20 minuti.



### Home >

# Marketplace



Tipo di gateway	Selezionare VPN poiché si tratta di una VPN IPSec.	
Tipo VPN	Selezionare Basato su route perché si tratta di una VTI. Quando si esegue una VPN con mappa crittografica, viene utilizzata la VPN basata su criteri.	
SKU	È necessario selezionare VpnGw1 o superiore in base alla quantità di traffico richiesta. Basic non supporta Border Gateway Protocol (BGP).	
Attivata modalità attiva/attiva	Non attivare. Al momento dell'invio, l'ASA non è in grado di originare la sessione BGP da un loopback o nell'interfaccia. Azure consente solo 1 indirizzo IP per il peering BGP.	
Indirizzo IP pubblico	Creare un nuovo indirizzo IP e assegnare un nome alla risorsa.	
Configurazione ASN BGP	Selezionare questa casella per abilitare BGP sul collegamento.	
ASN	Accettate questo valore come default 65515. Si tratta dell'ASN Azure che si presenta.	

Passaggio 4. Creare un gateway di rete locale.

Un gateway di rete locale è la risorsa che rappresenta l'ASA.

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

		Nome	Un nome per l'appliance ASA
Home > Create a resource > Marketplace > Create local network gateware Basics Advanced Review + create A local network gateway is a specific object that repr	ay ··· ×	Indirizzo IP	L'indirizzo IP pubblico dell'interfaccia esterna dell'ASA.
Project details Subscription * Cresec Resource group * Create or Instance details	cells-rig v	Spazio indirizzi	La subnet viene configurata in seguito sulla VTI.
Region *     East US       Name *     ASA       Endpoint ···     Image: Comparison of the second	15 V Steres FQDN 4 V	Configurare le impostazioni BGP	Selezionare questa opzione per abilitare BGP.
192.148.100.0/30 Add additional address range Review + create Previous Next :	> B ···	ASN	Questo ASN è configurato sull'ASA.
		Indirizzo IP peer BGP	L'indirizzo IP è configurato sull'interfaccia VTI dell'ASA.

Passaggio 5. Creare una nuova connessione tra il gateway della rete virtuale e il gateway della rete locale, come mostrato nell'immagine.

+ Create a resource	New
🛧 Home	
📴 Dashboard	∠ Connec
i≡ All services	Connec
🛨 FAVORITES	Connection

Home > Create a resource > Marketplace >					
Create connection		×			
Basics Settings Tags Review	+ create				
Create a secure connection to your virtua	I network by using VPN Gateway or ExpressRoute.				
Learn more about VPN Gateway C					
Learn more about expressionate E					
Project details					
Subscription *	cx-sec-tls	$\sim$			
Resource group *	cx-sec-tls-ra	~			
Resource group	Create new				
Instance details					
Connection type * 🕕	Site-to-site (IPsec)	$\sim$			
Name *	VPNTunnel1	~			
Region *	East US	~			
Review + create Previous	Next : Settings > Download a template for automation	Give feedback			

L.

C C A st http://portal azure.com/idecand/idecation (C C C C C C C C C C C C C C C C C C C	🗧 🗧 💼 🔥 Create connecti	on - Microsoft // X Duo Security - Two-Factor Auth X +	~
Central guardel @ Gatting Started @ Lightohy Of @ A K License Grand.   Micros Search resources, services, and does (Gr/)        <	← → C O A == https://	portal.azure.com/#create/Micros: 6년 ☆ 🛛 🕑 🗊 🕃 C: 🕕 🐡	ම එ ≡
Increa       Search resource; services, and docs (G+/)       Image: Imag	실 Getting Started	ghtning GIT	»
Note a resource > Marketplace >         Create connection         Static       Statig       To an event a connection it must be associated to a virtual network gateway >         Static       Statig       Note an event and a connection, it must be associated to a virtual network gateway >       Image: Statig         State day 0'SR) *       Image: Statig       Image: Statig       Image: Statig         State day 0'SR) *       Image: Statig       Image: Statig       Image: Statig         State day 0'SR) *       Image: Statig       Image: Statig       Image: Statig       Image: Statig         State day 0'SR) *       Image: Statig       <	■ Micros 🔎 Search resources, se	rvices, and docs (G+/) E ロ ۞ ⑦ & jyoungt	a@cisco.com
Create connection     Saic:   Sting:   To a vitual network with connection. It must be associated to a vitual network gateway:   Name   Name   Saired kay 0'SQ:   Saired kay 0'SQ:   Saired kay 0'SQ:   Name   Saired kay 0'SQ:   Saired kay 0'SQ:   Name   Saired kay 0'SQ:   Saired kay 0'SQ:   Name   Saired kay 0'SQ:	Home > Create a resource > Marketpla	ace >	
Batic etting Tag Rview + ceale      Characterization and evolution and enconcellon. It must be associated to a virtual network gateway •	Create connection		$\times$
Balici Method   Section Signa   Reverse Natural network what a connection, it must be associated to a virtual network gateway Image: Signa   Interverse gateway Image: Signa   Inclain network gateway Image: Signa   Integrity Image: Signa   Inclain network gateway Image: Signa   Integrity <			
Virtual metwork gateway     To use a virtual network with a connection, it must be associated to a virtual network gateway     Virtual network gateway     ASA     Local network gateway     ASA     Local network gateway     ASA     Shared key (PSK)     Intervine (PAddress)     It E Protocol     It e anable BGP     It e anable BGP     It e anable BGP     It e anable BGP        It e anable BGP   <	Basics Settings Tags Review	+ create	
To use a virtual network with a connection, it must be associated to a virtual network gateway:   Virtual network gateway:   ASA   Local network gateway:   ASA   Shared key (PSK):   Cara network gateway:   KE Protocol   KE Protocol   KE Protocol   KE Protocol   Cara network gateway:   Cara network gateway:   KE Protocol   KE Protocol   Cara network gateway:   Cara network gateway:   KE Protocol   KE Protocol   Cara network gateway:   Cara network gateway:   Cara network gateway:   KE Protocol   Cara network gateway:   Cara network gateway: </td <td>Virtual network gateway</td> <td></td> <td></td>	Virtual network gateway		
Virtual network gateway* VISUI   Local network gateway* ASA   Shared key (PSK)* Image: Shared key (PSK)*   IKE Protocol IKEV1   IKE Protocol IKEV1   IKE Protocol IKEV1   Ite Azure Private IP Address Image: Shared key   IPsec / IKE policy Image: Shared key   Ite Phase 1 Image: Shared key   Ite Phase 2(IPsec) Image: Shared key   Ite Phase 2(IPsec) Image: Shared key   IPsec Sha lifetime in seconds * Image: Shared key   Ite policy based traffic selector Image: Shared key   Ite policy based traffic selector Image: Shared key   Ip policy based traffic selector Image: Shared key   Ite policy based traffic selector Image: Shared key   Ite policy based traffic selector Image: Shared key   Ite policy based traffic selector Image: S	To use a virtual network with a connection	n, it must be associated to a virtual network gateway.	
Local network gateway* ASA   Shared key (PSK)* Image: Constraint of the second of	Virtual network gateway * 🕕	VNGW1 V	
Shared key (PSK)*      IKE Protocol      IKE Protocol      IKE Protocol      IKE Protocol      IKE Protocol      Ike Vaure Private IP Address      Imable BGP      Imable BGP      Imable BGP, the SKU has to be Standard or higher.     IPsec / IKE policy      Imable BGP, the SKU has to be Standard or higher.     IPsec / IKE policy      Imable BGP, the SKU has to be Standard or higher.     IPsec / IKE policy      Imable BGP, the SKU has to be Standard or higher.     IPsec / IKE policy      Imable BGP, the SKU has to be Standard or higher.     IPsec / IKE policy      Imable BGP, the SKU has to be Standard or higher.     Imable Default      Image: Standard or higher.     Image: Standa	Local network gateway * 🕕	ASA	
IKE Protocol   IKE Protocol   Ise Azure Private IP Address   Ise Azure	Shared key (PSK) * 🕕	······ ··· ··· ··· ··· ·· ·· ·· ·· ·· ·	
Use Azure Private IP Address   Enable BGP   C   Enable BGP, the SKU has to be Standard or higher.     I'' To enable BGP, the SKU has to be Standard or higher.     I''' To enable BGP, the SKU has to be Standard or higher.     I'''' To enable BGP, the SKU has to be Standard or higher.     I''''''''''''''''''''''''''''''''''''	IKE Protocol ①	○ IKEv1 ● IKEv2	
Enable BGP ()     Enable BGP ()     I or enable BGP, the SKU has to be Standard or higher.     Psec / IKE policy ()     Default (utor)     ()     I or enable BGP, the SKU has to be Standard or higher.     I match in the outpatient of the outpat	Use Azure Private IP Address ①		
I nadle bor o   I no enable BGP, the SKU has to be Standard or higher.     IPsec / IKE policy O     IPsec / IKE policy O     IKE Phase 1 O     Encryption*        IKE Phase 2(IPsec) O     IPsec SA lifetime in KiloBytes* O     IPsec SA lifetime in seconds* O     IPsec SA lifetime in seconds* O     Image: Connection Mode O	Enable RGR		
To enable BGP, the SKU has to be Standard or higher.     IPsec / IKE policy ③     Default Custom <ul> <li>Psec / IKE policy ③</li> <li>Percuryption *</li> <li>Integrity/PRF *</li> <li>DH Group *</li> <li>GCMAES256 ○</li> <li>SHA384 ○</li> <li>DHGroup14 ○</li> </ul> IKE Phase 1 ③   Encryption *   Integrity/PRF *   DH Group *   GCMAES256 ○   SHA384 ○   DHGroup14 ○        IKE Phase 2(IPsec) ③   IPsec SA lifetime in Kilo8ytes * ③   0   IPsec SA lifetime in seconds * ③   27000   Use policy based traffic selector ③   Enable Disable   DPD timeout in seconds * ③   45   Connection Mode ③	Enable bor 🕁		
IPsec / IKE policy ()       Default Custom         IPsec / IKE policy ()       ()         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 *       Integrity/PRF *       DH Group *         IKE Phase 2(IPsec) ()       IPsec Encryption *       IPsec Integrity *       PFS Group *         IFsec SA lifetime in KiloBytes * ()       ()       ()       ()         IPsec SA lifetime in seconds * ()       27000       ()       ()         DPD timeout in seconds * ()       (45       ()       ()         OPD timeout in seconds * ()       ()       ()       ()       ()	To enable BGP, the SKU has to be Sta	ndard or higher.	
IPsec / IKE policy ①              Cefault Custom          IPsec / IKE policy ①              Cefault Custom          IWen 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 ⑦ SHA384 ⑦ DHGroup14 ⑦             IKE Phase 2(IPsec) ②         IKE Phase 2(IPsec) ③              IPsec Encryption * IPsec Integrity * PFS Group *                  AES256 ⑦ SHA256 ⑦ None ⑦          IPsec SA lifetime in KiloBytes * ③              0	•		
IKE Phase 1 ○       Encryption *       Integrity/PRF *       DH Group *         IKE Phase 1 ○       Encryption *       Integrity/PRF *       DH Group *         IKE Phase 2(IPsec) ○       IPsec Encryption *       IPsec Integrity *       PFS Group *         IKE Phase 2(IPsec) ○       IPsec Encryption *       IPsec Integrity *       PFS Group *         IRE Phase 2(IPsec) ○       IPsec Encryption *       IPsec Integrity *       PFS Group *         IPsec SA lifetime in KiloBytes * ○       0       IPsec SA lifetime in seconds *       27000         Use policy based traffic selector ○       Enable Disable       ✓         DPD timeout in seconds * ○       45       ✓         O       Default ○ InitiatorOnly ○ ResponderOnly	IPsec / IKE policy ①	Default Custom	
establishment and rekey. IKE Phase 1 ① Encryption * Integrity/PRF * DH Group * GCMAES256 ✓ SHA384 ✓ DHGroup14 ✓ IKE Phase 2(IPsec) ③ IPsec Encryption * IPsec Integrity * PFS Group * AES256 ✓ SHA256 ✓ None ✓ IPsec SA lifetime in KiloBytes * ④ 0 IPsec SA lifetime in seconds * ④ 27000 Use policy based traffic selector ④ Enable Disable DPD timeout in seconds * ④ 45 Connection Mode ④ Default ④ InitiatorOnly ⑥ ResponderOnly		When using custom IPSec/IKE policies, please ensure that the custom settings are appropriately configured on the on-premise device for both initial tunnel	
IKE Phase 1 ()       Encryption *       Integrity/PRF *       DH Group *         IKE Phase 2(IPsec) ()       IPsec Encryption *       IPsec Integrity *       PFS Group *         IKE Phase 2(IPsec) ()       IPsec Encryption *       IPsec Integrity *       PFS Group *         IPsec SA lifetime in KiloBytes * ()       0       Integrity *       None ()         IPsec SA lifetime in seconds * ()       27000       Integrity *       Image: Same ()         Use policy based traffic selector ()       Enable ()       Enable ()       Image: Same ()         DPD timeout in seconds * ()       45       ()       Image: Same ()       Image: Same ()         Connection Mode ()       O       Default ()       InitiatorOnly ()       ResponderOnly		establishment and rekey.	
GCMAES256        SHA384        DHGroup14          IKE Phase 2(IPsec) ①       IPsec Encryption *       IPsec Integrity *       PFS Group *         IPsec SA lifetime in KiloBytes * ①       0       IPsec SA lifetime in seconds *       0         IPsec SA lifetime in seconds * ①       27000       IPsebe       IPsebe         DPD timeout in seconds * ①       Imsebe       IPsebe       Imsebe         OPD timeout in seconds * ①       45       Imsebe       Imsebe         Operault ①       InitiatorOnly ②       ResponderOnly	IKE Phase 1 ①	Encryption * Integrity/PRF * DH Group *	
IKE Phase 2(IPsec) ③       IPsec Encryption *       IPsec Integrity *       PFS Group *         IPsec SA lifetime in KiloBytes * ④       0         IPsec SA lifetime in seconds * ④       27000         Use policy based traffic selector ④       Enable Disable         DPD timeout in seconds * ④       45         Connection Mode ④       Default ◯ InitiatorOnly ◯ ResponderOnly		GCMAES256 V SHA384 V DHGroup14 V	
AES256       SHA256       None         IPsec SA lifetime in KiloBytes*       0         IPsec SA lifetime in seconds*       27000         Use policy based traffic selector       Enable         DPD timeout in seconds*       45         Connection Mode       O	IKE Phase 2(IPsec)	IPsec Encryption * IPsec Integrity * PFS Group *	
IPsec SA lifetime in KiloBytes * ①       0         IPsec SA lifetime in seconds * ①       27000         Use policy based traffic selector ①       Enable Disable         DPD timeout in seconds * ①       45         Connection Mode ①       Default ○ InitiatorOnly ○ ResponderOnly		AES256 V SHA256 V None V	
IPsec SA lifetime in seconds * ①       27000         Use policy based traffic selector ①       Enable Disable         DPD timeout in seconds * ①       45         Connection Mode ①       Default O InitiatorOnly O ResponderOnly	IPsec SA lifetime in KiloBytes * 🕕	0	
Use policy based traffic selector   Enable Disable  DPD timeout in seconds   45  Connection Mode  Default  InitiatorOnly  ResponderOnly	IPsec SA lifetime in seconds *	27000	
DPD timeout in seconds * ③     45     ✓       Connection Mode ③     ● Default ○ InitiatorOnly ○ ResponderOnly	Use policy based traffic selector 🕕	Enable Disable	
Connection Mode   Default  Default  Default  ResponderOnly	DPD timeout in seconds * ①	45 🗸	
	Connection Mode ①	Default      InitiatorOnly      ResponderOnly	
Paview + create Previour Next - Tage > Download a template for automation Give feedback	Review + create Previous	Next : Tags > Download a template for automation	Give feedback
Neview v create Previous Previous Download a template for automation			

Passaggio 6 Configurare l'appliance ASA

che punti alla porta 10.1.2.254 del tunnel VTI. Nell'esempio, 192.168.100.2 è all'interno della stessa subnet della VTI. Anche se nessun dispositivo ha questo indirizzo IP, l'ASA installa il percorso che punta all'interfaccia VTI.

route AZURE 10.1.2.254 255.255.255.255 192.168.100.2 1

Quindi, configurare BGP sull'appliance ASA. La rete 192.168.2.0/24 è l'interfaccia interna dell'ASA e un percorso propagato nel cloud. Inoltre, le reti configurate in Azure vengono annunciate all'appliance ASA.

router bgp 65000 bgp log-neighbor-changes bgp graceful-restart address-family ipv4 unicast neighbor 10.1.2.254 remote-as 65515 neighbor 10.1.2.254 ebgp-multihop 255 neighbor 10.1.2.254 activate network 192.168.2.0 network 192.168.100.0 mask 255.255.255.252 no auto-summary no synchronization exit-address-family

Opzione 2. Configura routing statico: configura in modo statico le route sia su ASA che su Azure. Configurare l'appliance ASA per inviare il traffico alle reti di Azure tramite il tunnel VTI.

route AZURE 10.1.0.0 255.255.0.0 192.168.100.2 1

Modificare il gateway di rete locale creato nel passaggio 4 con le reti esistenti dietro l'ASA e la subnet sull'interfaccia del tunnel, quindi aggiungere i prefissi nella sezione Add Additional Network Spaces (Aggiungi spazi di rete aggiuntivi).

## Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Passaggio 1. Verificare che sia stata stabilita una sessione IKEv2 con il comando show crypto ikev2 sa.

<#root>

ciscoasa# show crypto ikev2 sa

IKEv2 SAs: Session-id:6, Status:UP-ACTIVE, IKE count:1, CHILD count:1 Tunnel-id Local Remote 2006974029 B.B.B.B. /500 A.A.A.A/500 READY INITIATOR Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK Life/Active Time: 86400/4640 sec Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535 remote selector 0.0.0.0/0 - 255.255.255/65535 ESP spi in/out: 0x74e90416/0xba17723a

Passaggio 2. Verificare che anche un'associazione di protezione IPsec venga negoziata con l'utilizzo del comando show crypto ipsec sa.

#### <#root>

```
ciscoasa# show crypto ipsec sa
interface: AZURE
    Crypto map tag: __vti-crypto-map-3-0-1, seq num: 65280, local addr: B.B.B.B
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0/0/0)
      current_peer: A.A.A.A
#pkts encaps: 240,
#pkts encrypt: 240, #pkts digest: 240
#pkts decaps: 377
, #pkts decrypt: 377, #pkts verify: 377
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 240, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: B.B.B.B/500, remote crypto endpt.: A.A.A.A/500
      path mtu 1500, ipsec overhead 78(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: BA17723A
      current inbound spi : 74E90416
    inbound esp sas:
```

```
SA State: active
```

```
transform: esp-aes-256 esp-sha-256-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, VTI, }
slot: 0, conn_id: 1722, crypto-map: __vti-crypto-map-3-0-1
sa timing: remaining key lifetime (kB/sec): (3962863/24100)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0xFFFFFFFF 0xFFFFFFFF
outbound esp sas:
spi: 0xBA17723A (3122098746)
SA State: active
```

transform: esp-aes-256 esp-sha-256-hmac no compression in use settings ={L2L, Tunnel, IKEv2, VTI, } slot: 0, conn\_id: 1722, crypto-map: \_\_vti-crypto-map-3-0-1 sa timing: remaining key lifetime (kB/sec): (4008947/24100) IV size: 16 bytes replay detection support: Y Anti replay bitmap: 0x00000000 0x00000001

ciscoasa#

Passaggio 3. Verificare la connettività sul tunnel al router remoto BGP con l'uso di ping e ping tcp per convalidare il routing di livello 3 e la connettività di livello 4 per BGP o le risorse dell'endpoint se si usa il routing statico.

#### <#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:
!!!!!
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:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 41/42/42 ms
ciscoasa#
```

Passaggio 4. Quando si usa BGP, verificare le route di connettività BGP ricevute e annunciate ad

Azure e la tabella di routing dell'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 O BGP filter-list cache entries using O bytes of memory BGP using 1640 total bytes of memory BGP activity 14/10 prefixes, 17/12 paths, scan interval 60 secs AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd Neiahbor V 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 Network Next Hop Metric LocPrf Weight Path \*> 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 в 10.1.0.0 255.255.0.0 [20/0] via 10.1.1.254, 01:03:33 S 10.1.2.254 255.255.255.255 [1/0] via 192.168.100.2, AZURE С B.B.B.A 255.255.255.224 is directly connected, outside B.B.B.B 255.255.255.255 is directly connected, outside L 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 192.168.100.1 255.255.255.255 is directly connected, AZURE 1

Passaggio 5. Eseguire il ping di un dispositivo sul tunnel. In questo esempio è una macchina virtuale Ubuntu in esecuzione 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

Visualizzare ora i percorsi effettivi sulla VM remota. Devono mostrare i percorsi annunciati dall'ASA al cloud, come mostrato nell'immagine.

	Dashboard > Resource groups > CX-SecurityTLs-ResourceGroup > jyoungta-ubuntu-azure - Diagnose and solve problems > Effective routes						
	Effective routes						
	🕹 Download 🛛 Download	sh					
	Showing only top 200	records, c	lick Download abov	e to see all.			
	Scope		Virtual machine (jy	oungta-ubuntu-azure)			
	Network interface		jyoungta-ubuntu	i-azur956		~	
	Effective routes						
	SOURCE 1	STATE	Ťψ	ADDRESS PREFIXES	¢↓	NEXT HOP TYPE	↑↓ NEXT HOP TYPE IP ADDRESS ↑↓
	Default	Active		10.1.0.0/16		Virtual network	-
ſ	Virtual network gateway	Active		192.168.100.0/30		Virtual network gateway	A.A.A
I	Virtual network gateway	Active		192.168.100.1/32		Virtual network gateway	A.A.A
l	Virtual network gateway	Active		192.168.2.0/24		Virtual network gateway	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	-

# Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

### Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).