

Configura connessione VTI IPsec ASA ad Azure

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione 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

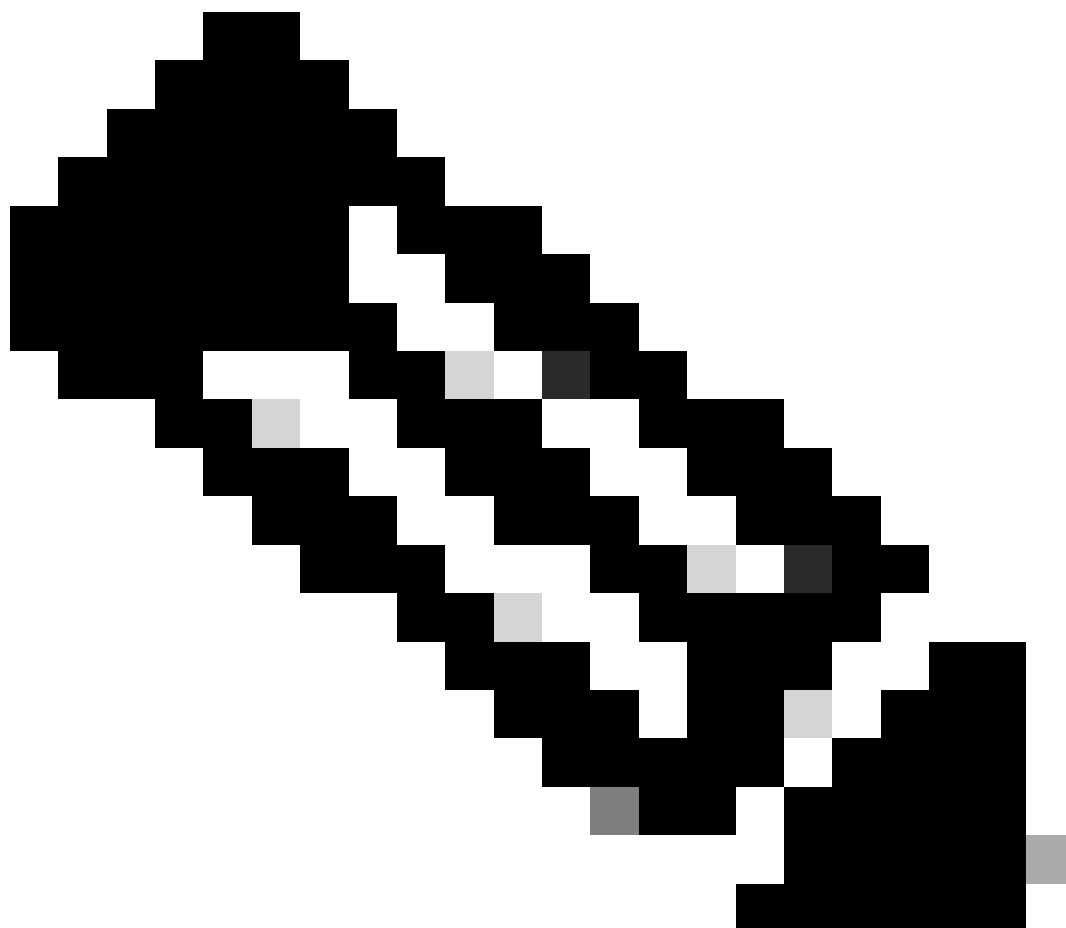
Componenti usati

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.

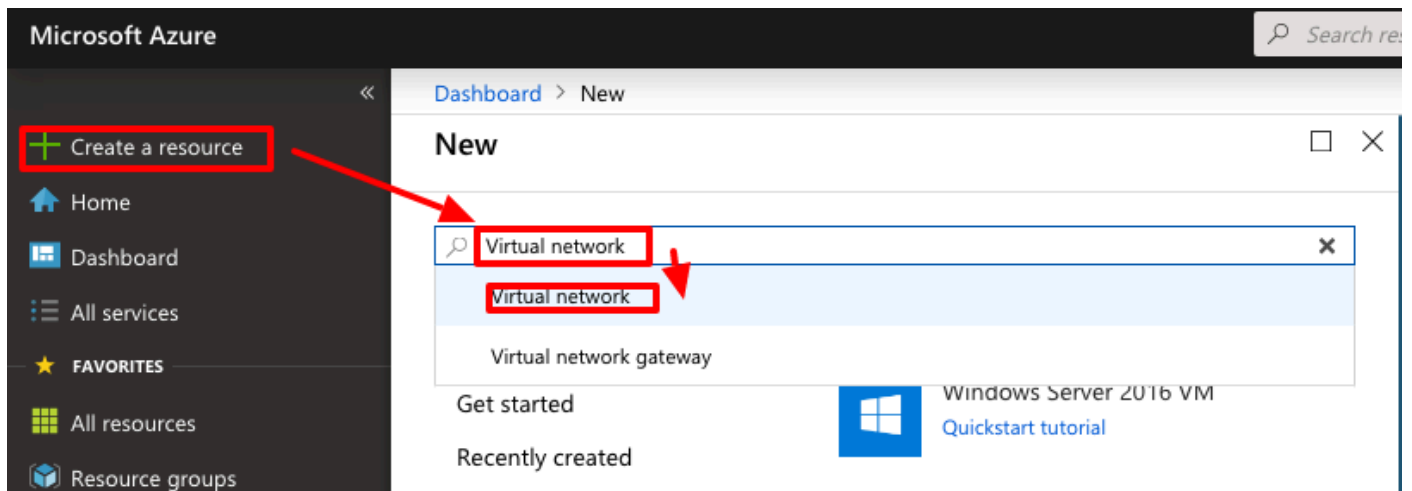
Configurazione

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.



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

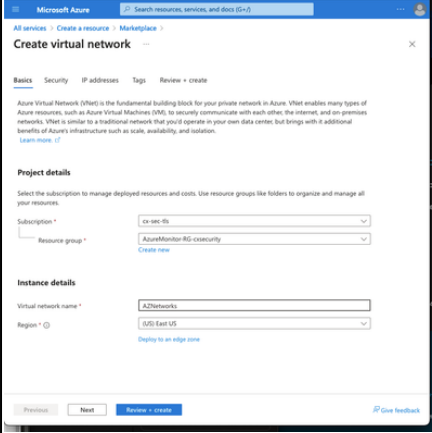
The VPN device in your Azure virtual network and used with site-to-site and VNet-to-VNet VPN connections.

Create



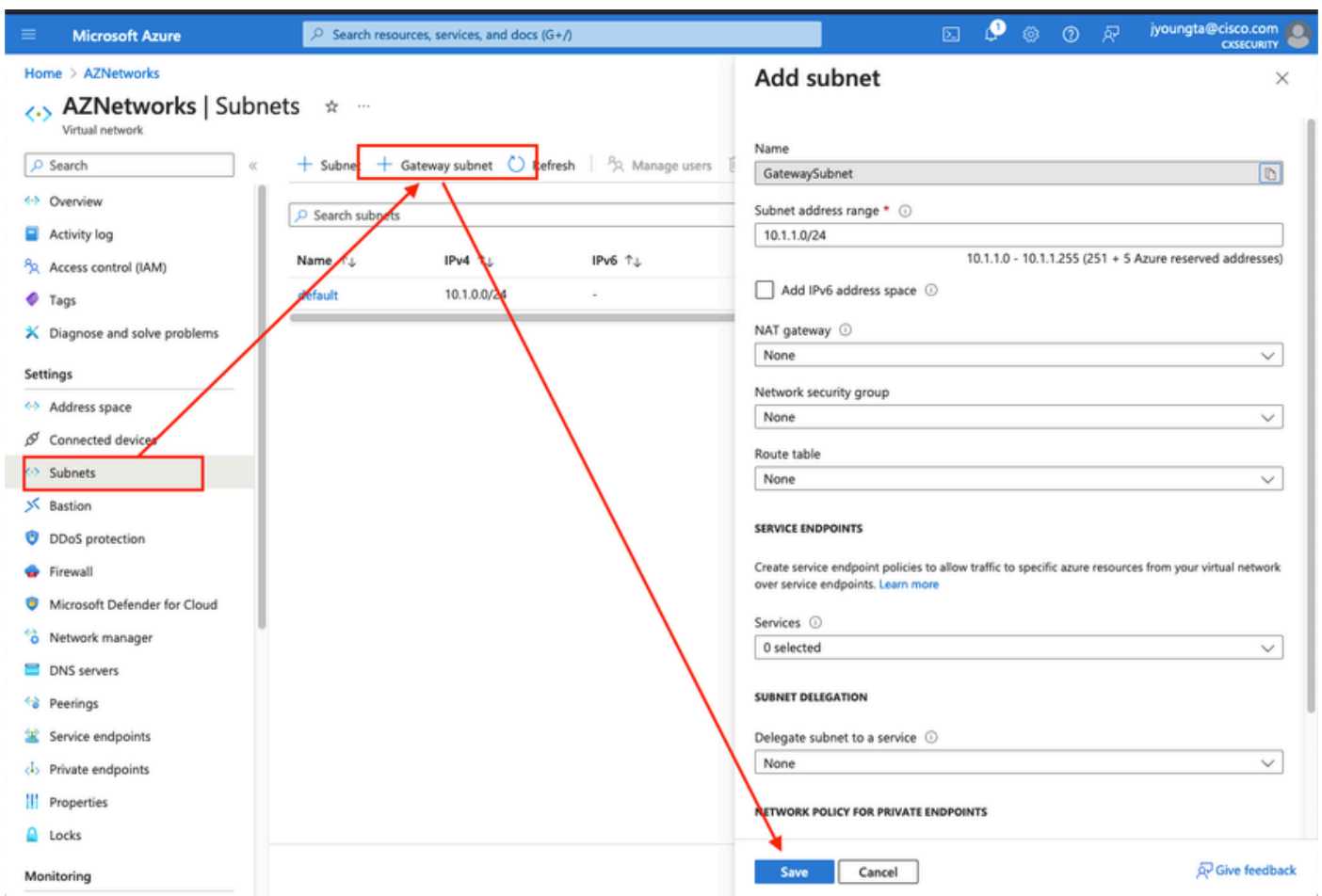
Virtual network



	Nome	Nome dello spazio di indirizzi IP ospitato nel cloud
	Spazio indirizzi	L'intero intervallo CIDR ospitato in Azure. Nell'esempio viene utilizzato 10.1.0.0/16.
	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.
	Intervallo indirizzi subnet	Subnet creata all'interno della rete virtuale.

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

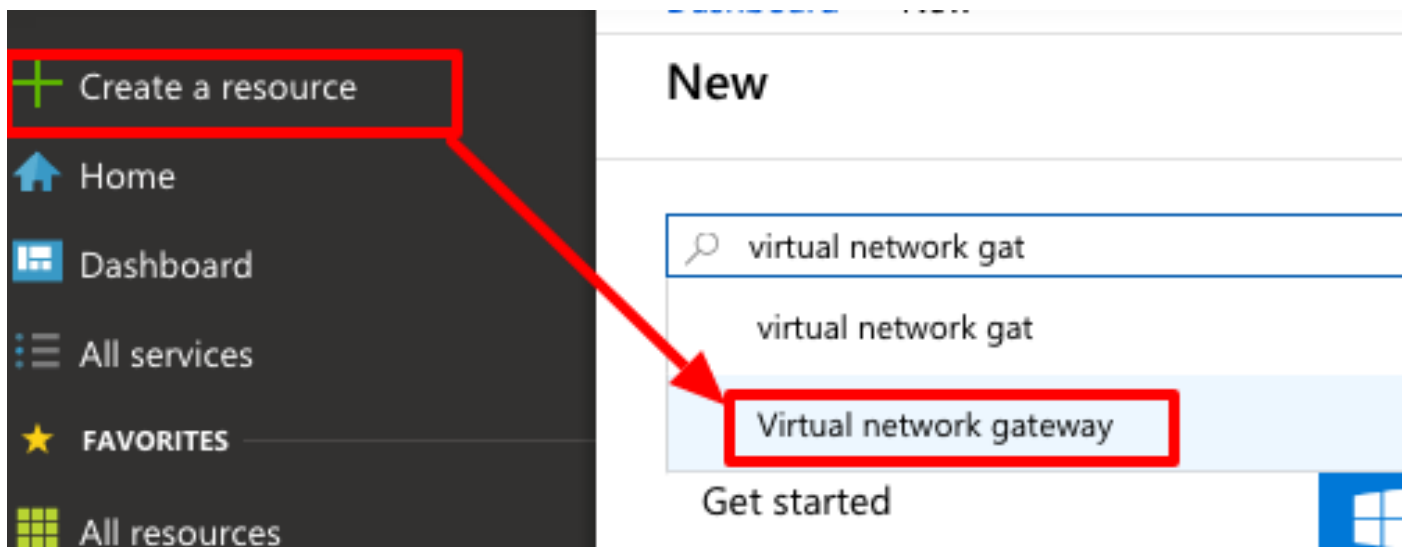
Passare alla rete virtuale e aggiungere una subnet del gateway. Nell'esempio viene utilizzato 10.1.1.0/24.



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.



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

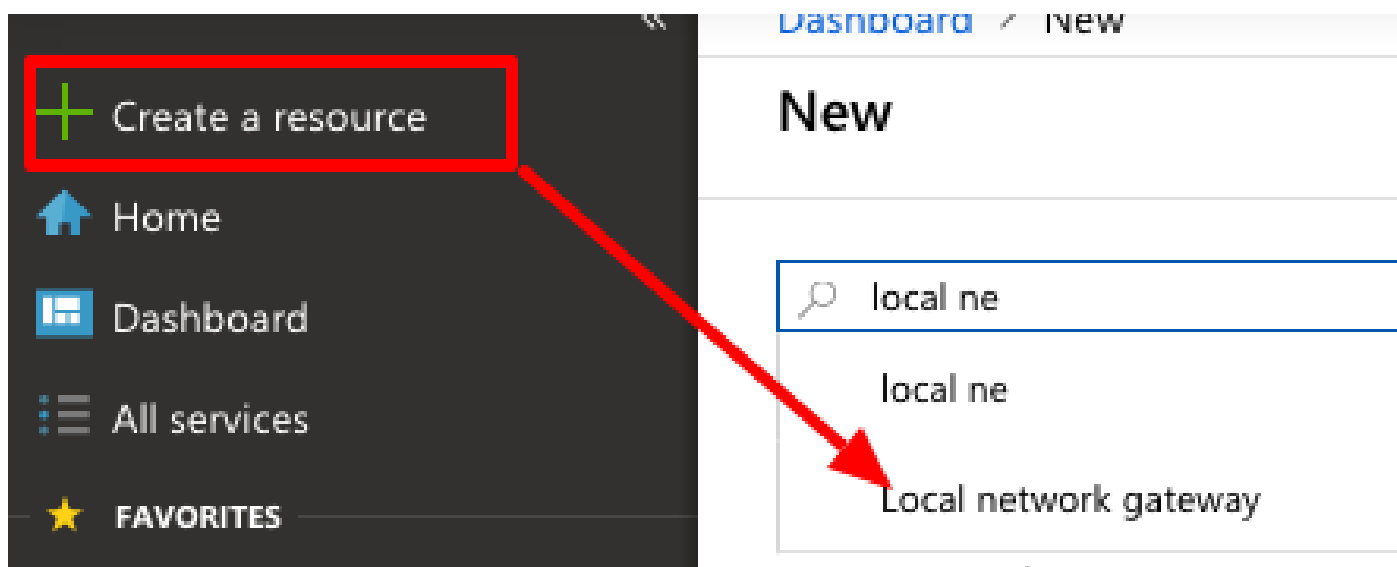
Nome

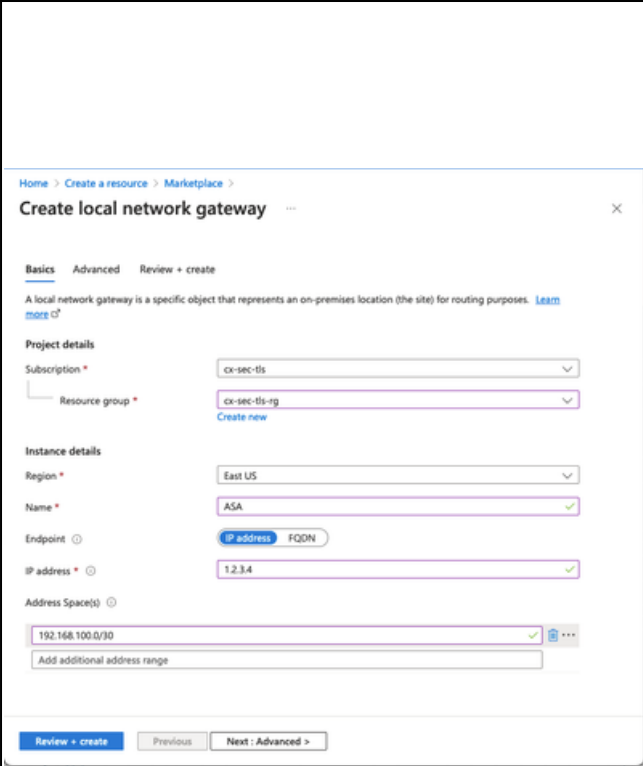
Nome del gateway di rete virtuale

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.

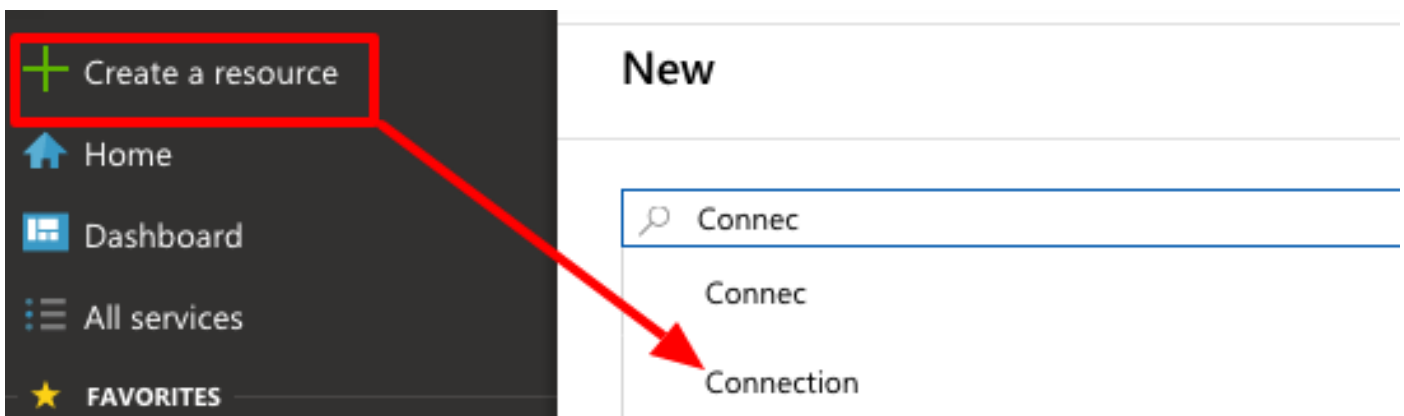
Passaggio 4. Creare un gateway di rete locale.

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



	<p>Nome</p>	<p>Un nome per l'appliance ASA</p>
	<p>Indirizzo IP</p>	<p>L'indirizzo IP pubblico dell'interfaccia esterna dell'ASA.</p>
	<p>Spazio indirizzi</p>	<p>La subnet viene configurata in seguito sulla VTI.</p>
	<p>Configurare le impostazioni BGP</p>	<p>Selezionare questa opzione per abilitare BGP.</p>
	<p>ASN</p>	<p>Questo ASN è configurato sull'ASA.</p>
	<p>Indirizzo IP peer BGP</p>	<p>L'indirizzo IP è configurato sull'interfaccia VTI dell'ASA.</p>

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



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						

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 - 255.255.255.255/65535
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): (0.0.0.0/0.0.0.0/0/0)  
    remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)  
    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:
```

```
spi: 0x74E90416 (1961427990)
```

```
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
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 defi
* 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	0		32768	i <<<

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
B     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
C     B.B.B.A 255.255.255.224 is directly connected, outside
L     B.B.B.B 255.255.255.255 is directly connected, outside
C     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
C     192.168.100.0 255.255.255.252 is directly connected, AZURE
L     192.168.100.1 255.255.255.255 is directly connected, AZURE
```

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.

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	-

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).