Configurer la connexion ASA IPsec VTI à Azure

Table des matières

[Introduction](#)
[Conditions préalables](#)
[Exigences](#)
[Composants utilisés](#)
[Configurer](#)
[Vérifier](#)
[Dépannage](#)

Introduction

Ce document décrit comment configurer une connexion d'interface de tunnel virtuel IPsec (VTI) d'appliance de sécurité adaptatif (ASA) à Azure. Dans ASA 9.8.1, la fonctionnalité IPsec VTI a été étendue pour utiliser IKEv2, mais elle est toujours limitée à sVTI IPv4 sur IPv4. Ce guide de configuration a été produit à l'aide de l'interface de ligne de commande ASA et du portail Azure. La configuration du portail Azure peut également être effectuée par PowerShell ou API. Pour plus d'informations sur les méthodes de configuration Azure, consultez la documentation Azure.

Remarque : actuellement, VTI est uniquement pris en charge en mode routé à contexte unique.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Un ASA connecté directement à Internet avec une adresse IPv4 statique publique qui exécute ASA 9.8.1 ou version ultérieure
- Un compte Azure

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

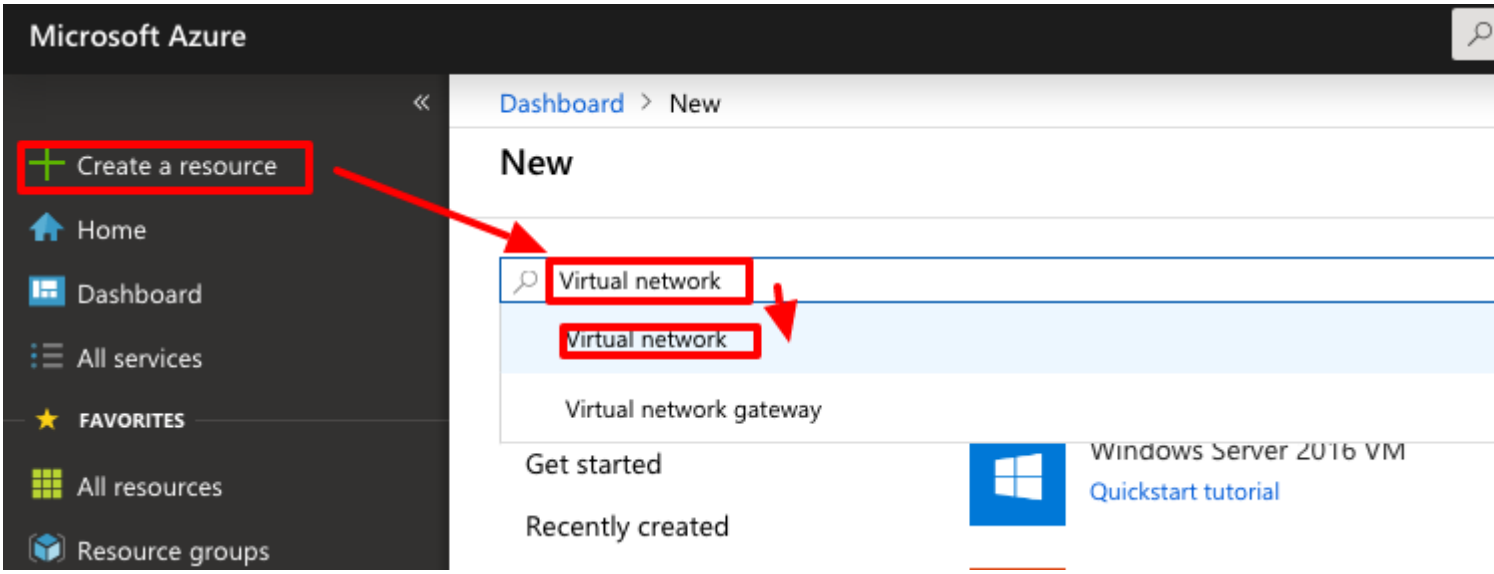
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre lâ€™incidence possible des commandes.

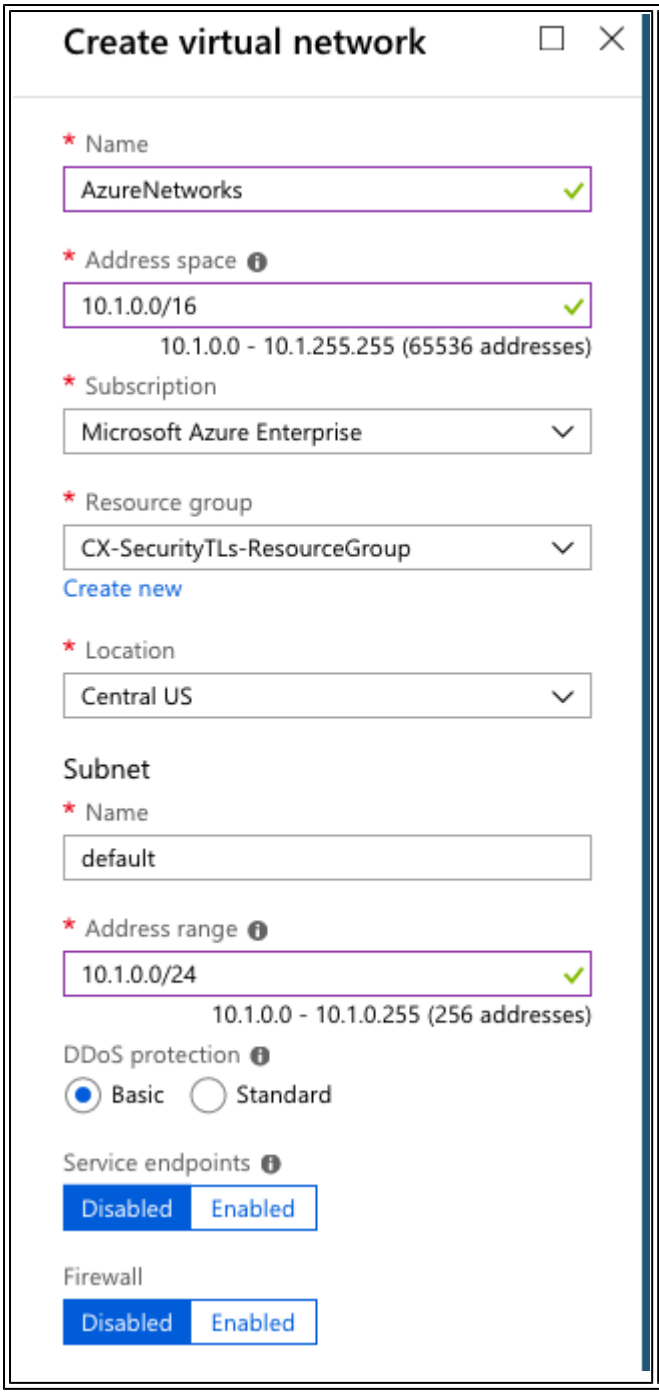
Configurer

Ce guide suppose que le cloud Azure n'a pas été configuré. Certaines de ces étapes peuvent être ignorées si les ressources sont déjà établies.

Étape 1. Configurez un réseau dans Azure.

Il s'agit de l'espace d'adressage réseau qui réside dans le cloud Azure. Cet espace dâ€™adressage doit être suffisamment grand pour accueillir des sous-réseaux, comme illustré dans lâ€™image.

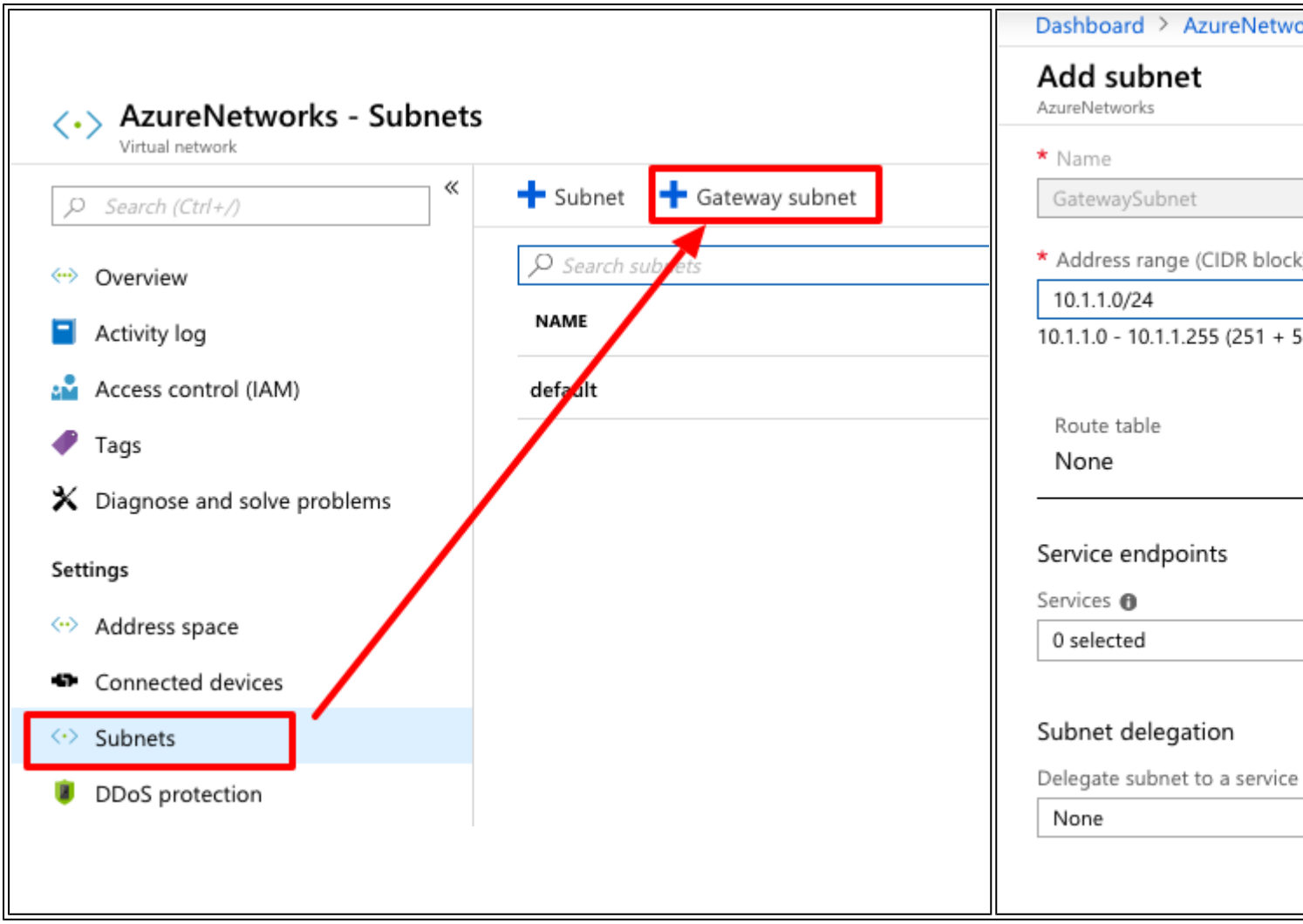




Nom	Nom de l'espace d'adressage IP hébergé dans le cloud
Espace D'Adressage	Toute la gamme CIDR hébergée dans Azure. Dans cet exemple, 10.1.0.0/16 est utilisé
Nom de sous-réseau	Nom du premier sous-réseau créé dans le réseau virtuel auquel les machines virtuelles sont généralement associées
Plage d'adresses de sous-réseau	Un sous-réseau créé dans le réseau virtuel

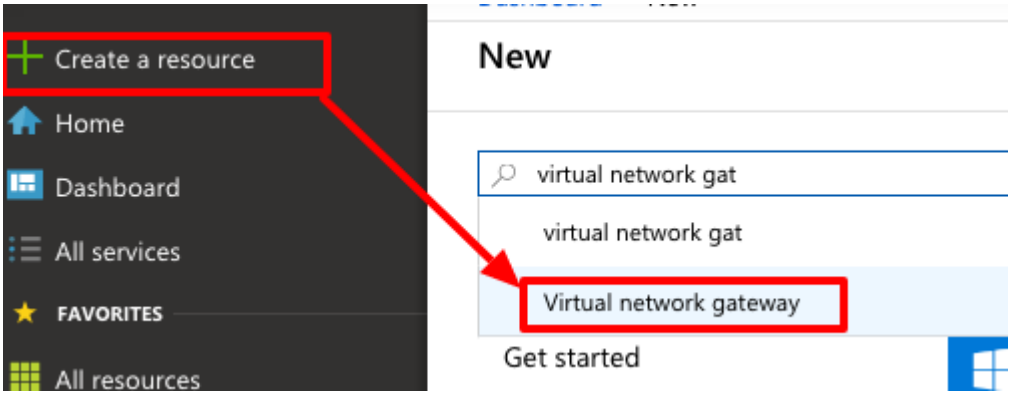
Étape 2. Modifiez le réseau virtuel afin de créer un sous-réseau de passerelle.

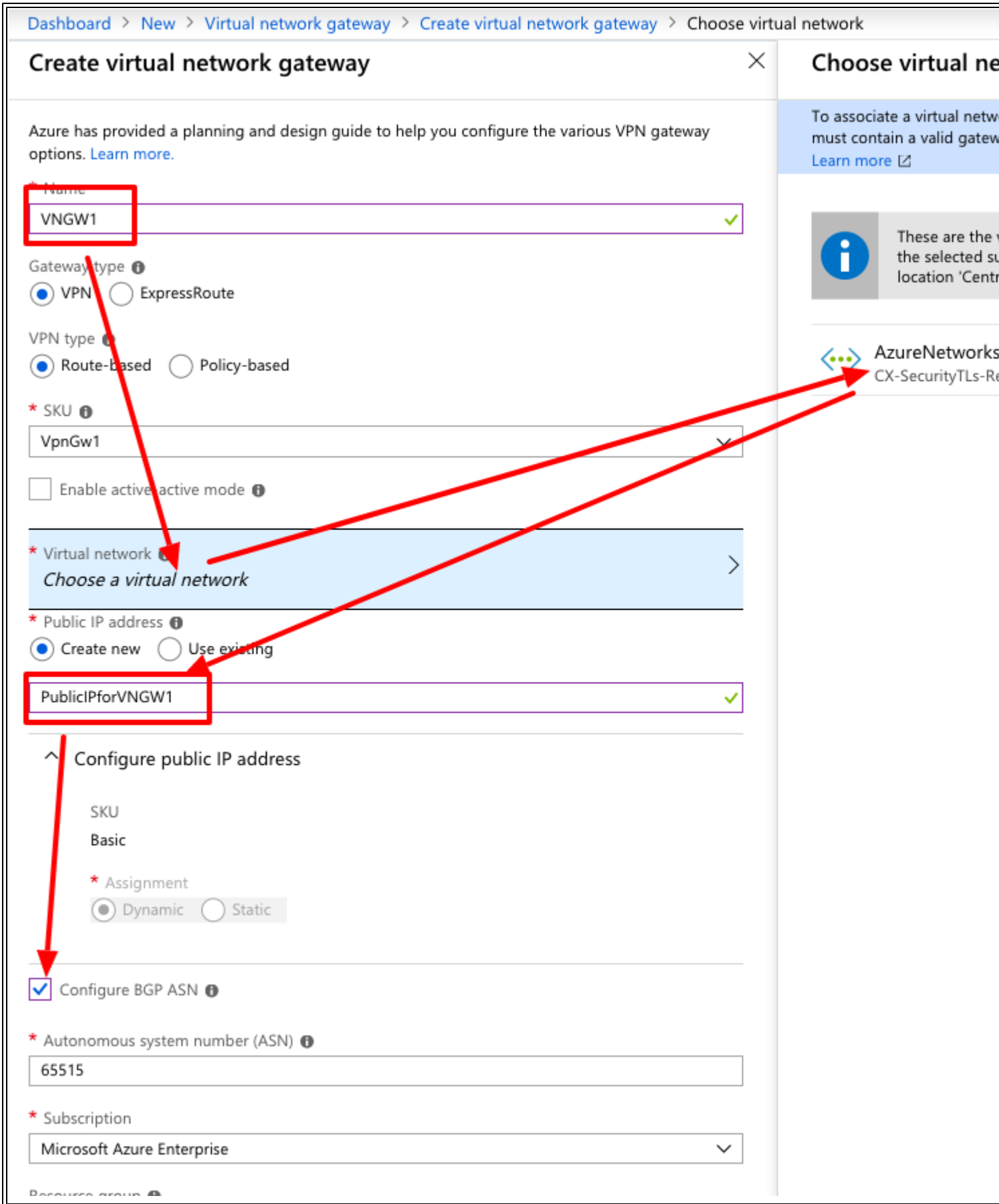
Accédez au **réseau virtuel** et ajoutez un sous-réseau de passerelle. Dans cet exemple, 10.1.1.0/24 est utilisé.



Étape 3. Créez une passerelle de réseau virtuel.

Il s'agit du terminal VPN hébergé dans le cloud. Il s'agit du périphérique avec lequel l'ASA construit le tunnel IPsec. Cette étape crée également une adresse IP publique qui est attribuée à la passerelle de réseau virtuel.



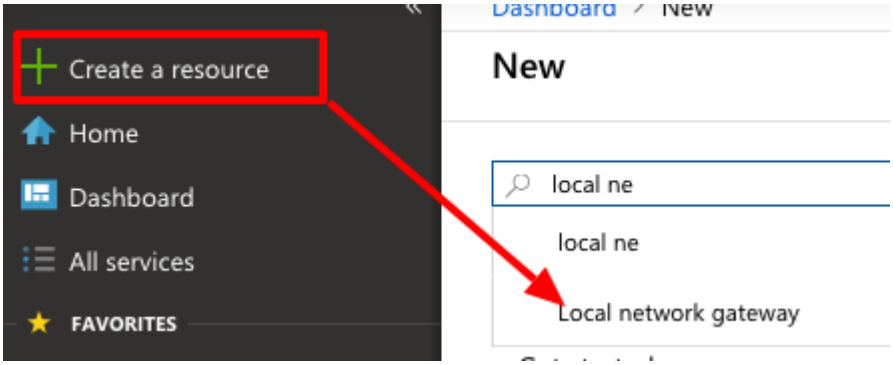


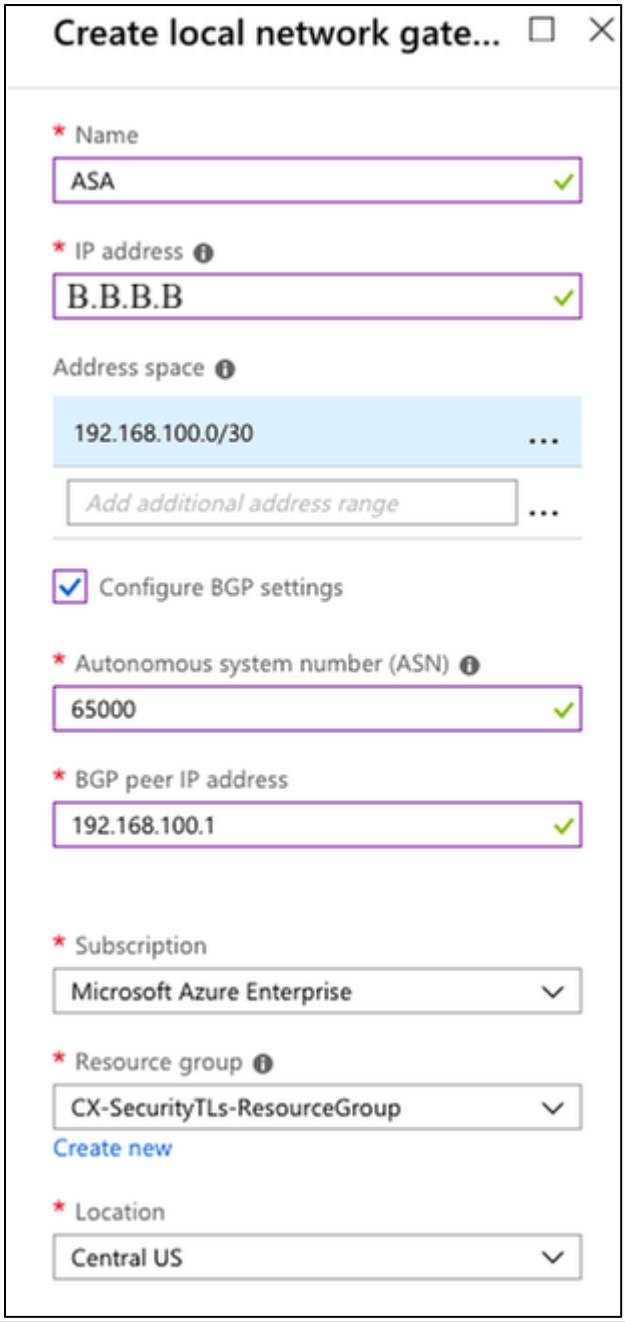
Nom	Nom de la passerelle de réseau virtuel
Type de passerelle	Sélectionnez VPN, car il s'agit d'un VPN IPsec
Type de VPN	Sélectionnez Basé sur la route, car il s'agit d'une interface VTI. La méthode basée sur la s lorsqu'un VPN de crypto-carte est effectué
RÉFÉRENCE	Vous devez sélectionner VpnGw1 ou supérieur en fonction du volume de trafic requis. Ba

	charge BGP
Activé en mode actif/actif	Ne pas activer. Au moment de la publication, l'ASA n'a pas la capacité d'approvisionner l d'un bouclage ou à l'intérieur de l'interface. Azure autorise uniquement 1 adresse IP pour
Adresse IP publique	Créez une nouvelle adresse IP et attribuez un nom à la ressource
Configuration du réseau ASN BGP	Cochez cette case pour activer BGP sur la liaison
ASN	Conservez le 65515 par défaut. Il s'agit de l'ASN Azure se présente comme

Étape 4. Créez une passerelle de réseau local.

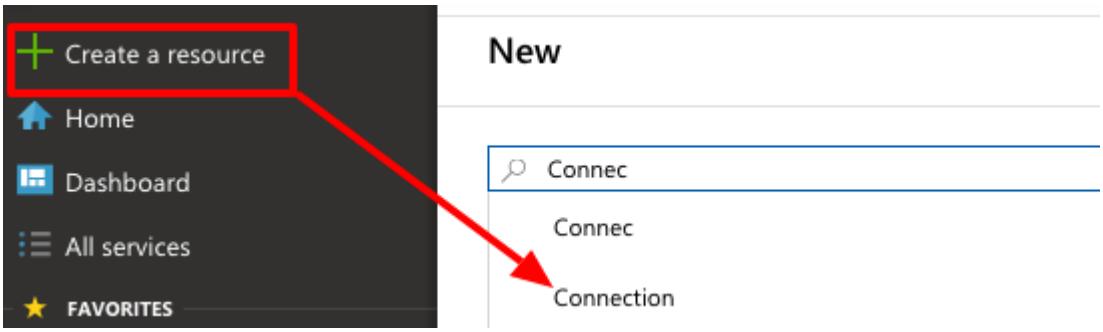
Une passerelle de réseau local est la ressource qui représente l'ASA.

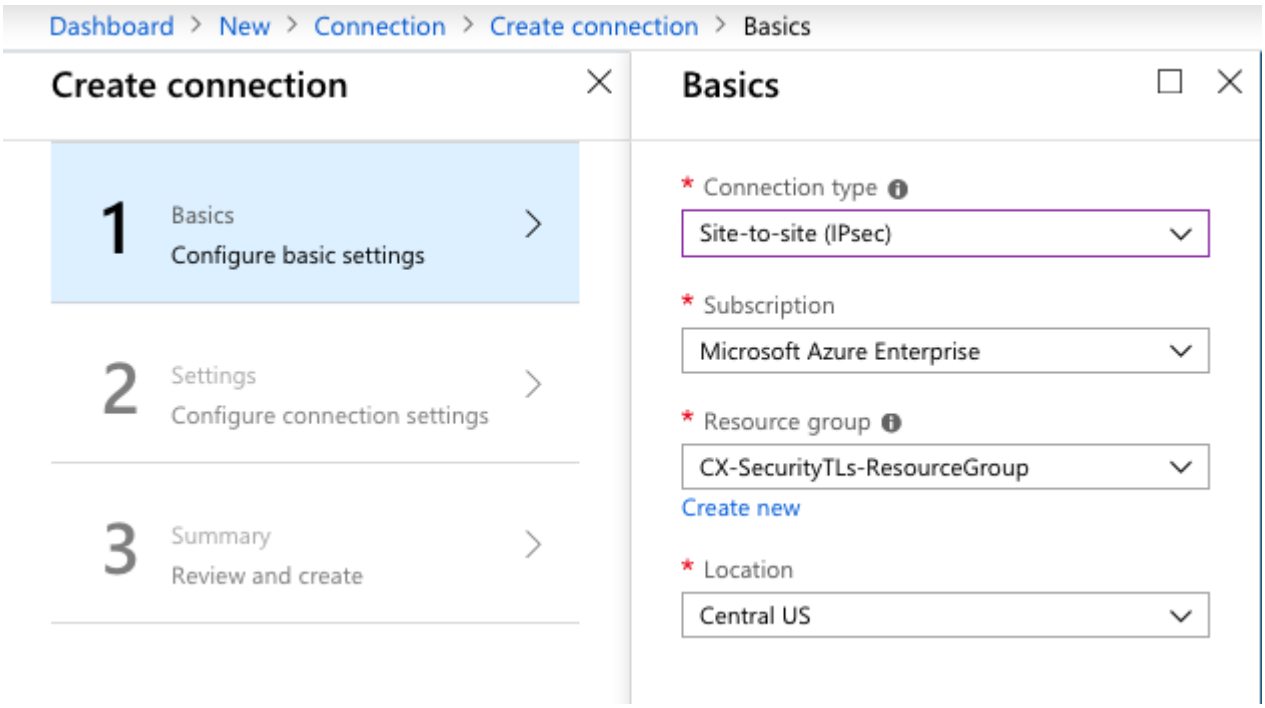


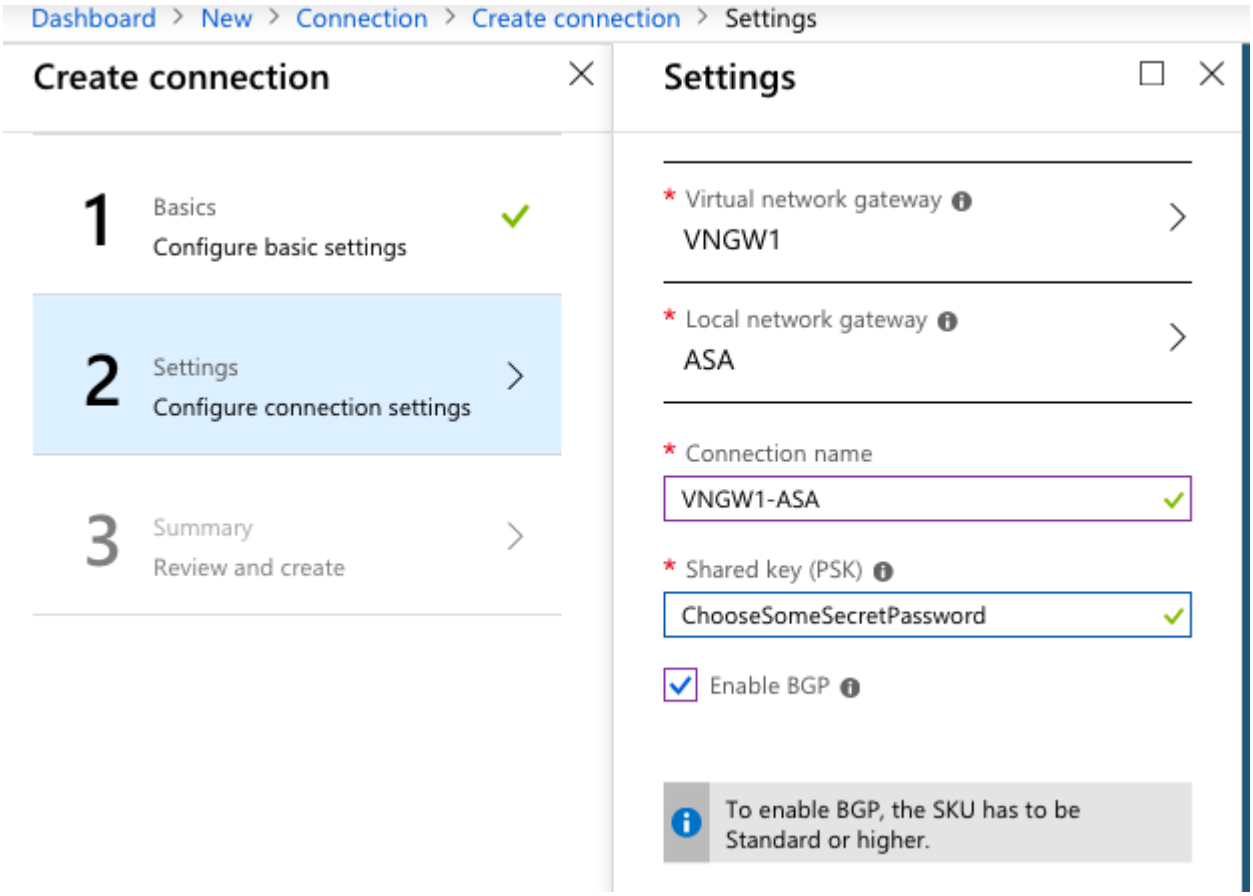


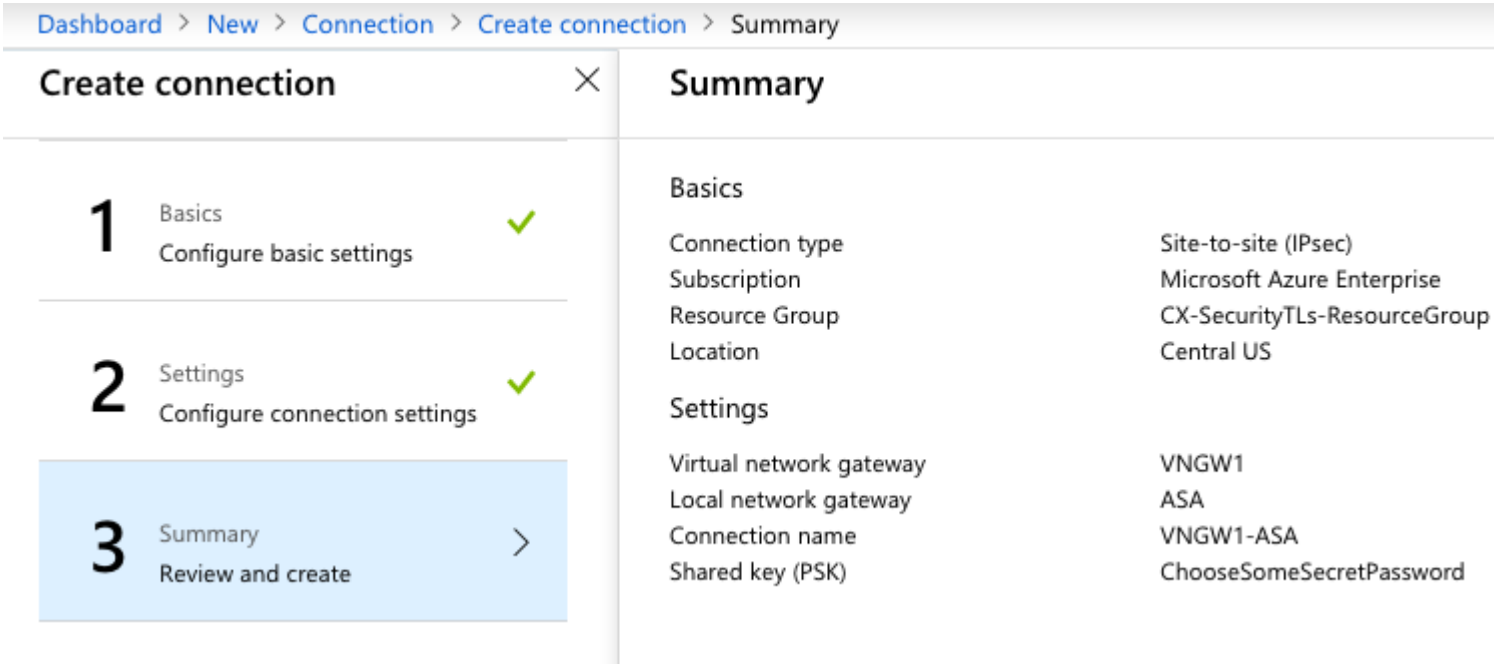
Nom	Un nom pour l'ASA
Adresse IP	Adresse IP publique de l'interface externe de l'ASA
Espace D'Adressage	Le sous-réseau est configuré sur le VTI ultérieurement
Configuration des paramètres BGP	Cochez cette case pour activer BGP
ASN	Cet ASN est configuré sur l'ASA
Adresse IP de l'homologue BGP	L'adresse IP est configurée sur l'interface ASA VTI

Étape 5. Créez une nouvelle connexion entre la passerelle de réseau virtuel et la passerelle de réseau local, comme illustré dans l'image.




Dashboard > New > Connection > Create connection > Basics
Create connection
1
Basics
Configure basic settings
2
Settings
Configure connection settings
3
Summary
Review and create
Basics
* Connection type
Site-to-site (IPsec)
* Subscription
Microsoft Azure Enterprise
* Resource group
CX-SecurityTLs-ResourceGroup
Create new
* Location
Central US


Dashboard > New > Connection > Create connection > Settings
Create connection
1
Basics
Configure basic settings
2
Settings
Configure connection settings
3
Summary
Review and create
Settings
* Virtual network gateway
VNGW1
* Local network gateway
ASA
* Connection name
VNGW1-ASA
* Shared key (PSK)
ChooseSomeSecretPassword
Enable BGP
To enable BGP, the SKU has to be Standard or higher.



Étape 6. Configurer l'ASA.

Tout d'abord, activez IKEv2 sur l'interface externe et configurez les stratégies IKEv2.

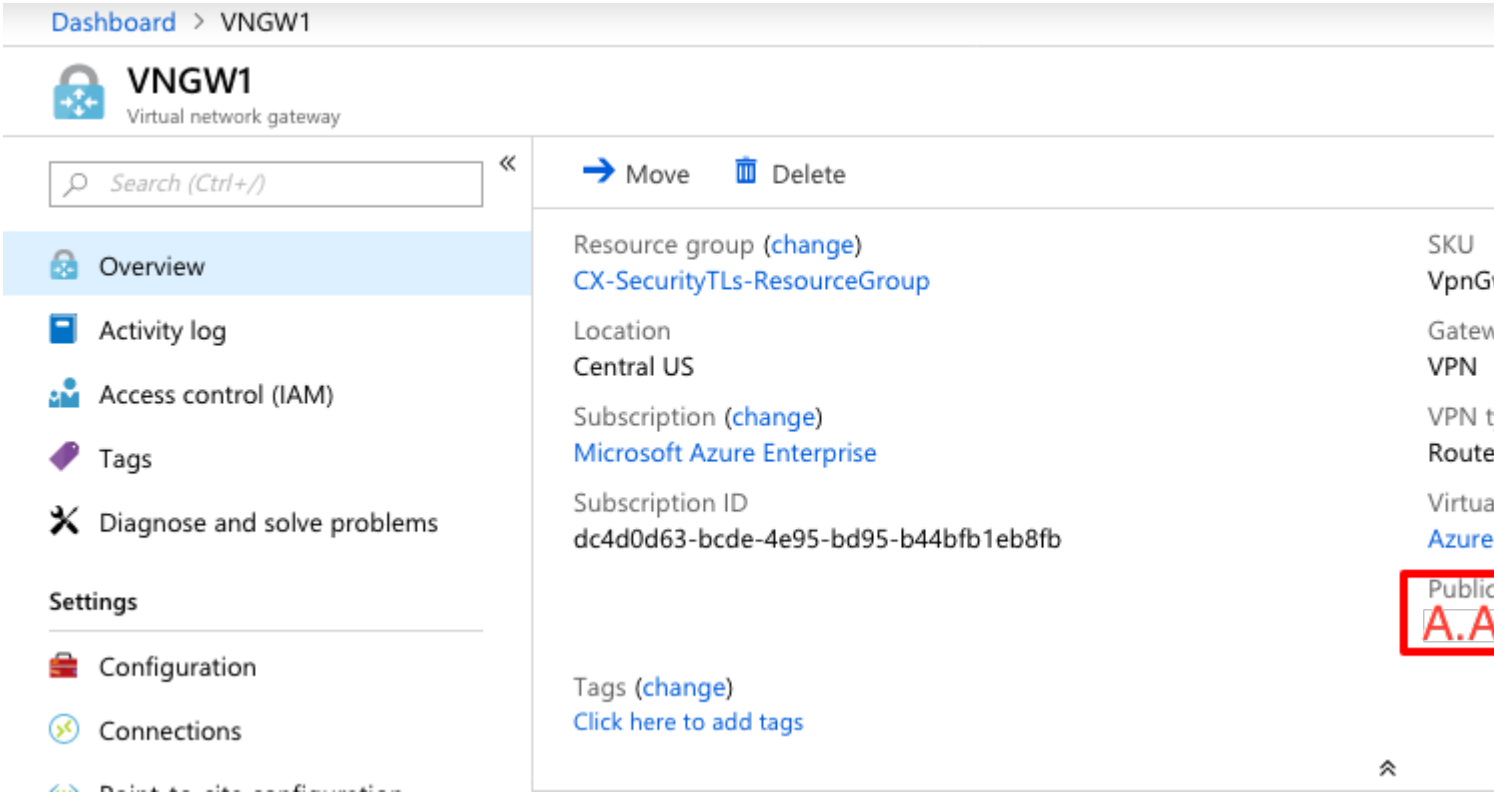
```
crypto ikev2 policy 10
 encryption aes-gcm-256 aes-gcm-192 aes-gcm
 integrity null
 group 14 5 2
 prf sha512 sha384 sha256 sha
 lifetime seconds 86400
crypto ikev2 policy 20
 encryption aes-256 aes-192 aes
 integrity sha512 sha384 sha256 sha
 group 14 5 2
 prf sha512 sha384 sha256 sha
 lifetime seconds 86400
crypto ikev2 enable outside
```

Étape 6. Configurez un jeu de transformation IPsec et un profil IPsec.

```
crypto ipsec ikev2 ipsec-proposal AZURE-PROPOSAL
 protocol esp encryption aes-256
 protocol esp integrity sha-256
crypto ipsec profile AZURE-PROPOSAL
 set ikev2 ipsec-proposal AZURE-PROPOSAL
```

Étape 8. Configurez le groupe de tunnels.

Récupérez l'adresse IPv4 publique de la passerelle réseau virtuelle créée à l'étape 3, comme illustré dans l'image.



Ensuite, configurez sur l'ASA une politique de groupe et un groupe de tunnels avec la clé pré-partagée définie à l'étape 3.

```
group-policy AZURE internal
group-policy AZURE attributes
 vpn-tunnel-protocol ikev2
tunnel-group A.A.A.A type ipsec-l2l
tunnel-group A.A.A.A general-attributes
 default-group-policy AZURE
tunnel-group A.A.A.A ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

Étape 9. Configurez l'interface du tunnel.

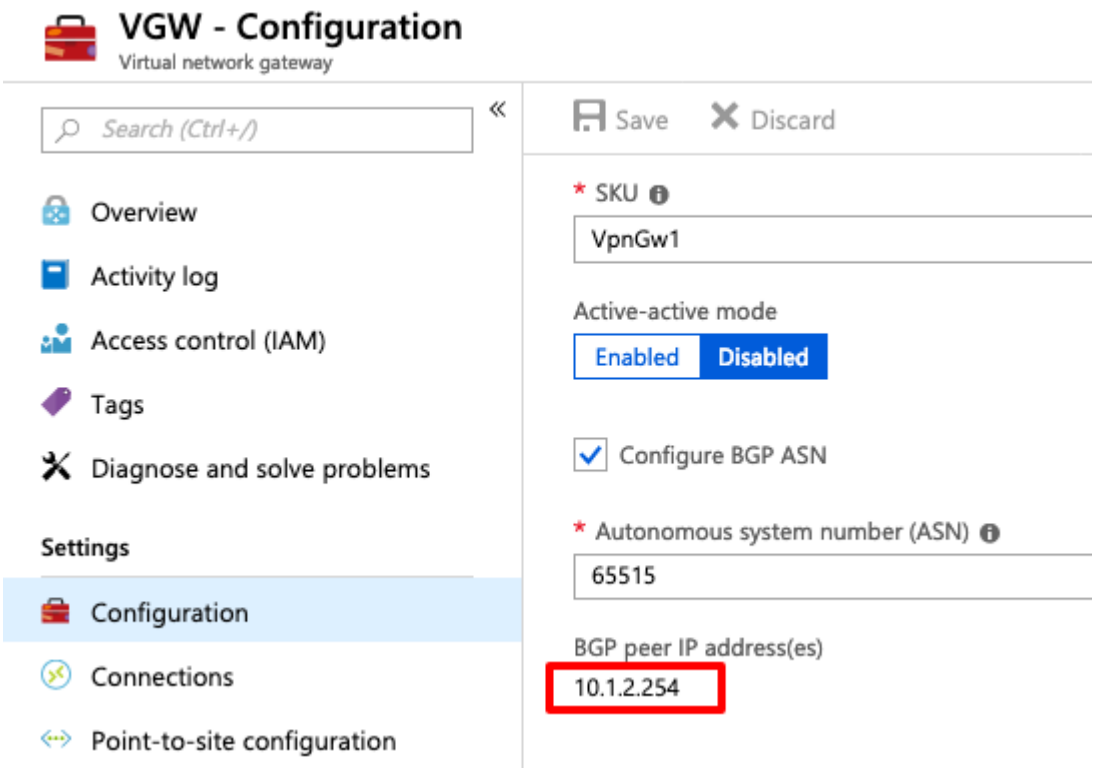
À l'étape 4 (configuration de la passerelle réseau locale), une adresse réseau et une adresse IP pour la connexion BGP ont été configurées. Il s'agit de l'adresse IP et du réseau à configurer sur le VTI.

```
interface Tunnel1
 nameif AZURE
 ip address 192.168.100.1 255.255.255.252
 tunnel source interface outside
 tunnel destination A.A.A.A
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile AZURE-PROPOSAL
 no shutdown
```

Étape 10.

Option 1. Configurez le routage dynamique. Échangez des routes avec Azure à l'aide de BGP.

Localisez l'adresse IP du routeur BGP dans Azure pour afficher la configuration de la passerelle réseau virtuelle créée à l'étape 3. Dans cet exemple, il s'agit de 10.1.2.254.



Sur l'ASA, configurez une route statique qui pointe vers 10.1.2.254 via le tunnel VTI. Dans cet exemple, 192.168.100.2 se trouve dans le même sous-réseau que le VTI. Bien qu'aucun périphérique ne dispose de cette adresse IP, l'ASA installe la route qui pointe vers l'interface VTI.

```
route AZURE 10.1.2.254 255.255.255.255 192.168.100.2 1
```

Configurez ensuite le protocole BGP sur l'ASA. Le réseau 192.168.2.0/24 est l'interface interne de l'ASA et une route qui est propagée dans le cloud. En outre, les réseaux configurés dans Azure sont annoncés à l'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
```

Option 2. Configurer le routage statique : configurez les routes de manière statique sur ASA et Azure. Configurez l'ASA pour envoyer le trafic aux réseaux Azure sur le tunnel VTI.

```
route AZURE 10.1.0.0 255.255.0.0 192.168.100.2 1
```

Modifiez la passerelle de réseau local créée à l'étape 4 avec les réseaux qui existent derrière l'ASA et le sous-réseau sur l'interface du tunnel et ajoutez les préfixes sous la section « Ajouter des espaces réseau supplémentaires ».

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Étape 1. Vérifiez qu'une session IKEv2 est établie avec **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
```

Étape 2. Vérifiez qu'une SA IPsec est également négociée à l'aide de la commande **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#
```

Étape 3. Vérifiez la connectivité sur le tunnel vers le routeur distant BGP avec l'utilisation de **ping et ping tcp** afin de valider le routage de couche 3 et la connectivité de couche 4 pour BGP ou les ressources de point d'extrémité si vous utilisez le routage statique.

<#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#
```

Étape 4. Lorsque vous utilisez BGP. Vérifiez la connectivité BGP, les routes reçues et annoncées à Azure et la table de routage de l'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
```

Étape 5. Envoyez une requête ping à un périphérique via le tunnel. Dans cet exemple, il s'agit d'une machine virtuelle Ubuntu qui s'exécute dans Azure.

<#root>

ciscoasa# p

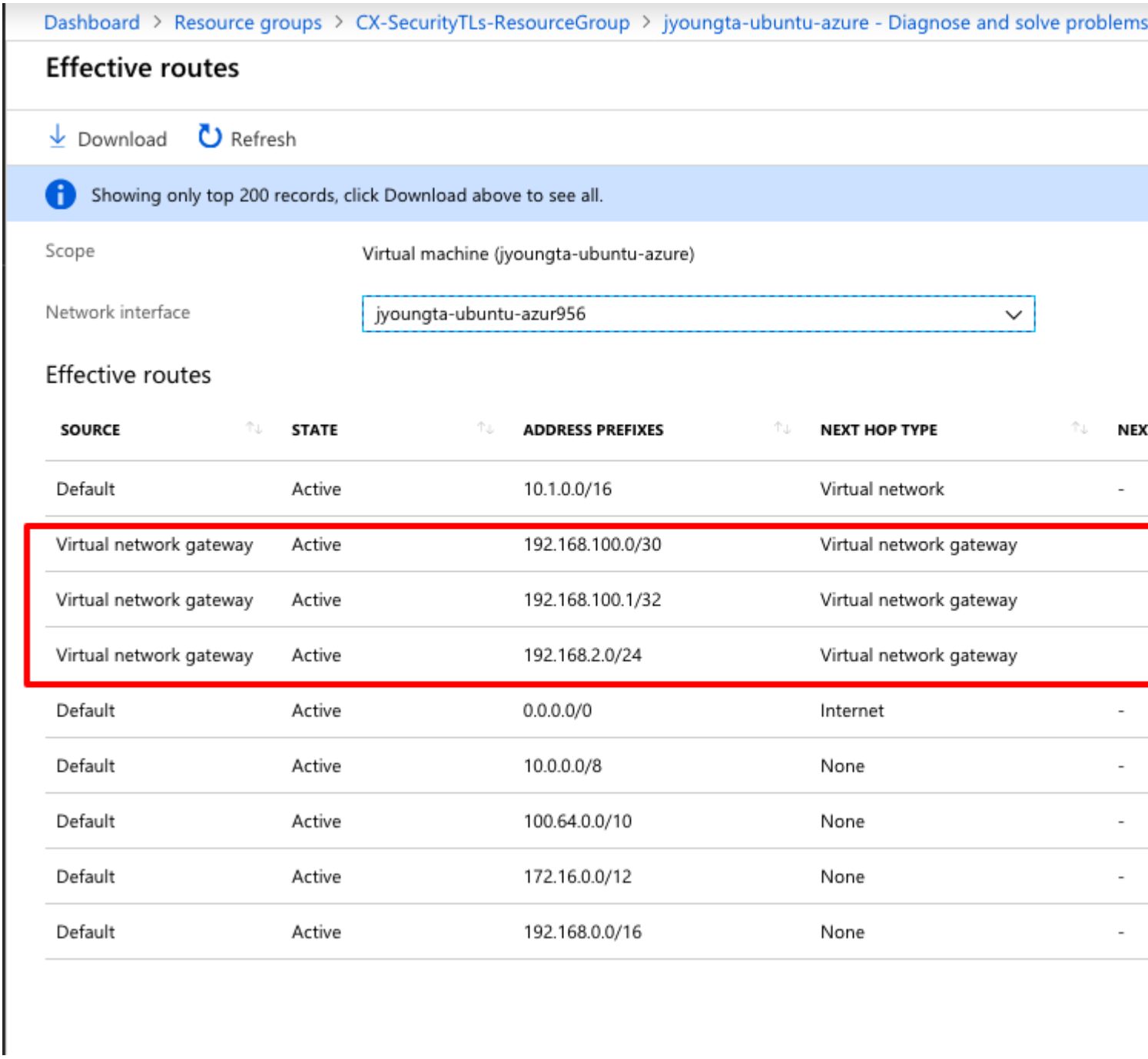
ing 10.1.0.4

```
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
```

Affichez maintenant les routes effectives sur la machine virtuelle distante. Elles doivent afficher les routes annoncées par l'ASA vers le cloud, comme indiqué dans l'image.



Dépannage

Aucune information spécifique n'est actuellement disponible pour dépanner cette configuration.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.