

Configuración de ASA IPsec VTI Connection en Azure

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo configurar una conexión IPsec Virtual Tunnel Interface (VTI) de Adaptive Security Appliance (ASA) a Azure. En ASA 9.8.1, la función IPsec VTI se amplió para utilizar IKEv2; sin embargo, sigue estando limitada a sVTI IPv4 sobre IPv4. Esta guía de configuración se elaboró con el uso de la interfaz CLI de ASA y el portal de Azure. PowerShell o la API también pueden realizar la configuración del portal de Azure. Para obtener más información acerca de los métodos de configuración de Azure, consulte la documentación de Azure.

Nota: Actualmente, VTI sólo se admite en modo de routing de contexto único.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Un ASA conectado directamente a Internet con una dirección IPv4 estática pública que ejecuta ASA 9.8.1 o posterior
- Una cuenta de Azure

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

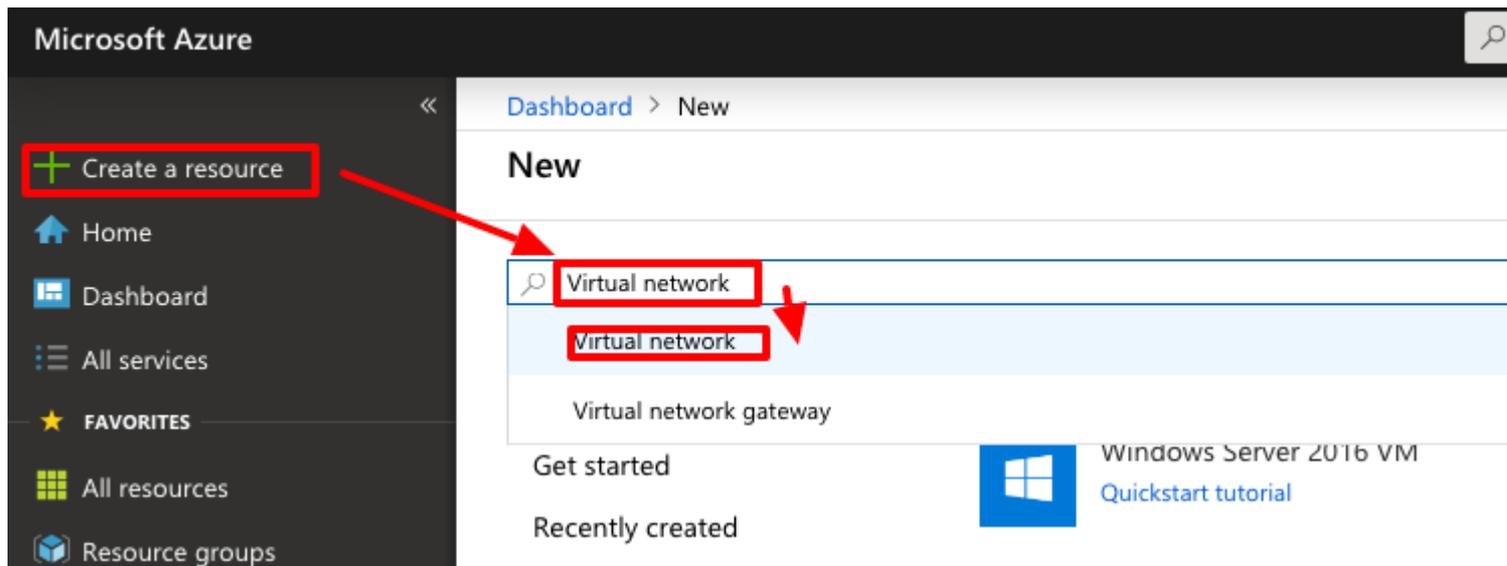
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

En esta guía se supone que la nube de Azure no se ha configurado. Algunos de estos pasos se pueden omitir si los recursos ya están establecidos.

Paso 1. Configure una red en Azure.

Este es el espacio de direcciones de red que vive en la nube de Azure. Este espacio de direcciones debe ser lo suficientemente grande como para albergar subredes dentro de ellas, como se muestra en la imagen.



Create virtual network □ ×

*** Name**
 ✓

*** Address space** ⓘ
 ✓
 10.1.0.0 - 10.1.255.255 (65536 addresses)

*** Subscription**
 ▾

*** Resource group**
 ▾
[Create new](#)

*** Location**
 ▾

Subnet

*** Name**

*** Address range** ⓘ
 ✓
 10.1.0.0 - 10.1.0.255 (256 addresses)

DDoS protection ⓘ
 Basic Standard

Service endpoints ⓘ

Firewall

Nombre	Nombre del espacio de direcciones IP alojado en la nube
Espacio de dirección	Todo el intervalo CIDR hospedado en Azure. En este ejemplo, se utiliza 10.1.0.0/16
Nombre de subred	El nombre de la primera subred creada dentro de la red virtual a la que normalmente están conectadas las VM
Intervalo de direcciones de subred	Una subred creada dentro de la red virtual

Paso 2. Modifique la red virtual para crear una subred de gateway.

Vaya a la **red virtual** y agregue una subred de gateway. En este ejemplo, se utiliza 10.1.1.0/24.

AzureNetworks - Subnets
Virtual network

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Address space
- Connected devices
- Subnets**
- DDoS protection

+ Subnet **+ Gateway subnet**

Search subnets

NAME
default

Add subnet
AzureNetworks

- Name: GatewaySubnet
- Address range (CIDR block): 10.1.1.0/24
10.1.1.0 - 10.1.1.255 (251 + 5)
- Route table: None
- Service endpoints: 0 selected
- Subnet delegation: None

Paso 3. Cree un gateway de red virtual.

Se trata del terminal VPN alojado en la nube. Este es el dispositivo con el que ASA construye el túnel IPsec. Este paso también crea una IP pública que se asigna al gateway de la red virtual.

Create a resource

- Home
- Dashboard
- All services
- FAVORITES
- All resources

New

virtual network gat

virtual network gat

Virtual network gateway

Get started

Create virtual network gateway

Azure has provided a planning and design guide to help you configure the various VPN gateway options. [Learn more.](#)

Name

Gateway type
 VPN ExpressRoute

VPN type
 Route-based Policy-based

* SKU

Enable active active mode

* Virtual network

* Public IP address
 Create new Use existing

Configure public IP address

SKU

Basic

* Assignment

Dynamic Static

Configure BGP ASN

* Autonomous system number (ASN)

* Subscription

Required groups

Choose virtual ne

To associate a virtual network with a VPN gateway, the virtual network must contain a valid gateway subnet. [Learn more](#)

These are the virtual networks in the selected subscription and location 'Central US'.

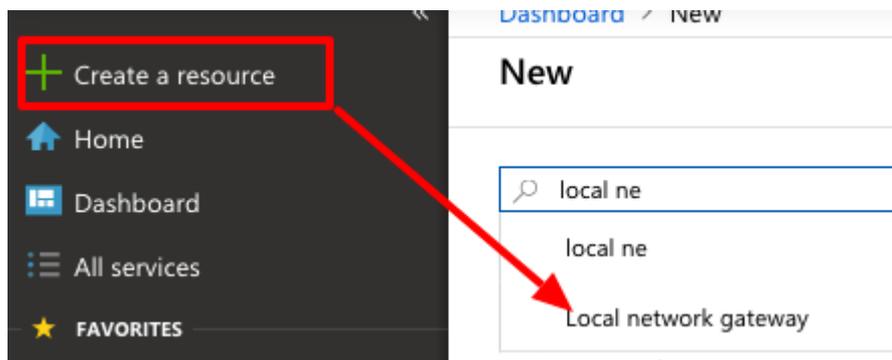
AzureNetworks
 CX-SecurityTls-Res

Nombre	Nombre del gateway de red virtual
Tipo de gateway	Seleccione VPN, ya que es una VPN IPsec.
Tipo de VPN	Seleccione Basado en ruta porque es un VTI. Se utiliza basado en políticas cuando se realiza cifrado criptográfico
SKU	Es necesario seleccionar VpnGw1 o superior en función de la cantidad de tráfico necesario

	BGP
Activado el modo activo/activo	No activar. En el momento de la publicación, ASA no tiene la capacidad de originar la sesión loopback o dentro de la interfaz. Azure solo permite 1 dirección IP para el peering BGP
Dirección IP pública	Cree una nueva dirección IP y asigne un nombre al recurso
Configuración de ASN de BGP	Marque esta casilla para habilitar BGP en el link
ASN	Deje este valor como 65515 predeterminado. Este es el ASN Azure que se presenta como

Paso 4. Cree un gateway de red local.

Un gateway de red local es el recurso que representa el ASA.



Create local network gate... □ ×

*** Name**
 ✓

*** IP address** ⓘ
 ✓

Address space ⓘ
 ...
 ...

Configure BGP settings

*** Autonomous system number (ASN)** ⓘ
 ✓

*** BGP peer IP address**
 ✓

*** Subscription**
 ▼

*** Resource group** ⓘ
 ▼
[Create new](#)

*** Location**
 ▼

Nombre	Un nombre para el ASA
IP Address	La dirección IP pública de la interfaz exterior del ASA
Espacio de dirección	La subred se configura en el VTI más tarde
Configurar los parámetros de BGP	Marque esta opción para activar BGP
ASN	Este ASN está configurado en el ASA
Dirección IP de peer BGP	La dirección IP se configura en la interfaz VTI de ASA

Paso 5. Cree una nueva conexión entre la puerta de enlace de red virtual y la puerta de enlace de red local, como se muestra en la imagen.

- + Create a resource
- ↑ Home
- 📊 Dashboard
- ☰ All services
- ★ FAVORITES

New

- Connec
- Connection

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 ▾

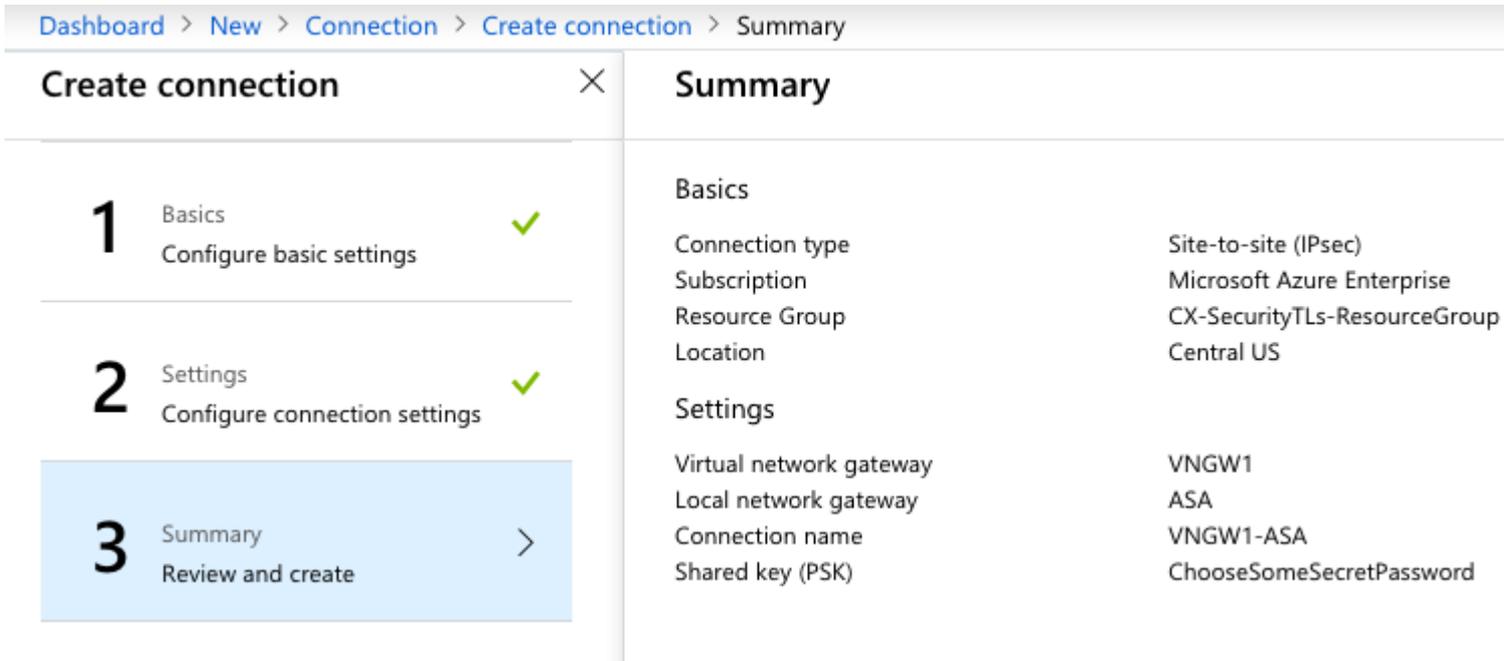
Create connection

- 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 ⓘ

i To enable BGP, the SKU has to be Standard or higher.



Paso 6. Configuración del ASA.

Primero, habilite IKEv2 en la interfaz externa y configure las políticas 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
```

Paso 6. Configure un conjunto de transformación IPsec y un perfil 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
```

Paso 8. Configure el grupo de túnel.

Recupere la dirección IPv4 pública de la puerta de enlace de red virtual creada en el paso 3, como se muestra en la imagen.

Dashboard > VNGW1

VNGW1
Virtual network gateway

Search (Ctrl+)

Move Delete

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Connections

Resource group (change)
CX-SecurityTLs-ResourceGroup

Location
Central US

Subscription (change)
Microsoft Azure Enterprise

Subscription ID
dc4d0d63-bcde-4e95-bd95-b44bfb1eb8fb

Tags (change)
Click here to add tags

SKU
VpnG
Gatew
VPN
VPN t
Route
Virtua
Azure
Public
A.A

A continuación, configure en ASA una política de grupo y un grupo de túnel con la clave previamente compartida definida en el paso 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 *****
```

Paso 9. Configure la interfaz de túnel.

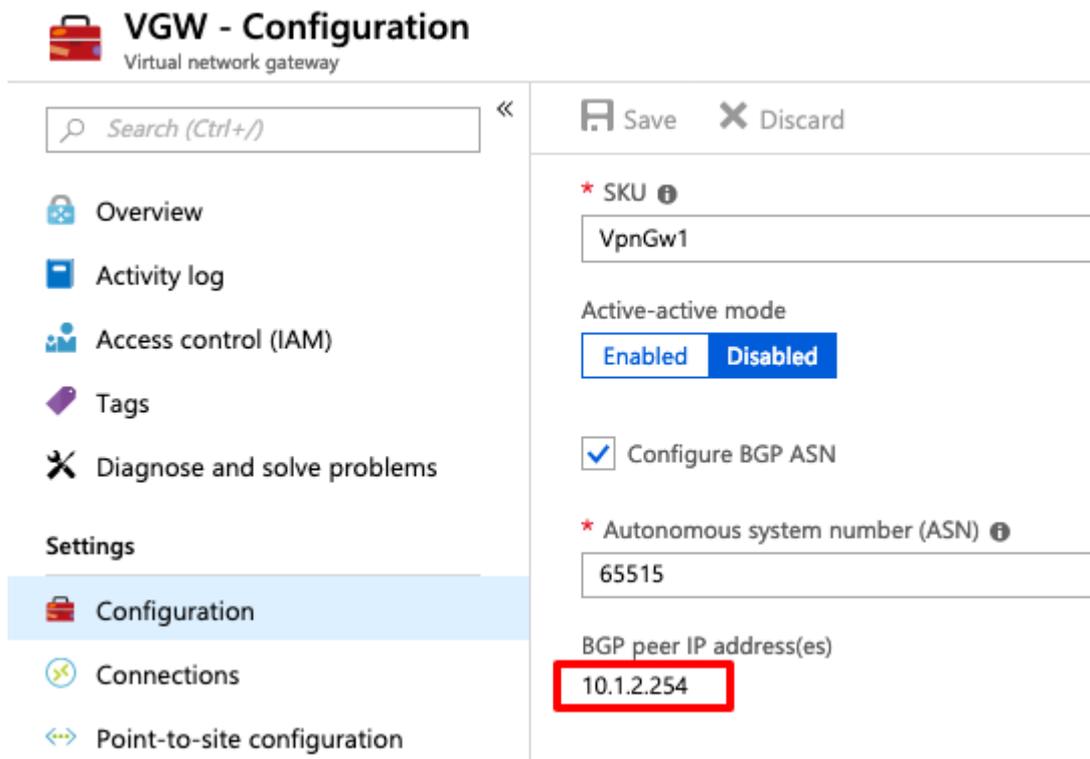
En el paso 4 (configurar la puerta de enlace de red local) se configuró una dirección de red y una dirección IP para la conexión BGP. Se trata de la dirección IP y la red que se configurarán en el VTI.

```
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
```

Paso 10.

Opción 1. Configure el enrutamiento dinámico. Intercambie rutas con Azure con el uso de BGP.

Busque la dirección IP del router BGP en Azure para ver la configuración del gateway de red virtual creado en el paso 3. En este ejemplo es 10.1.2.254.



The screenshot shows the 'VGW - Configuration' page in the Azure portal. The left sidebar contains navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and Settings. Under Settings, 'Configuration' is selected. The main content area shows the configuration for 'VpnGW1'. The 'SKU' is 'VpnGW1'. The 'Active-active mode' is set to 'Enabled'. The 'Configure BGP ASN' checkbox is checked. The 'Autonomous system number (ASN)' is '65515'. The 'BGP peer IP address(es)' field contains '10.1.2.254', which is highlighted with a red box.

En el ASA, configure una ruta estática que apunte a 10.1.2.254 fuera del túnel VTI. En este ejemplo, 192.168.100.2 está dentro de la misma subred que el VTI. Aunque ningún dispositivo tenga esa dirección IP, el ASA instala la ruta que señala la interfaz VTI.

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

A continuación, configure BGP en ASA. La red 192.168.2.0/24 es la interfaz interna del ASA y una ruta que se propaga a la nube. Además, las redes configuradas en Azure se anuncian al 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
```

Opción 2. Configure el ruteo estático: configure rutas estáticamente en ASA y Azure. Configure ASA para enviar tráfico a las redes de Azure a través del túnel VTI.

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

Modifique la puerta de enlace de red local creada en el paso 4 con las redes que existen detrás del ASA y la subred en la interfaz de túnel y agregue los prefijos en la sección "Agregar espacios de red adicionales".

Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

Paso 1. Verifique que se haya establecido una sesión IKEv2 con **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
```

Paso 2. Verifique que una SA IPsec también se negocie con el uso 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#
```

Paso 3. Verifique la conectividad a través del túnel al router remoto BGP con el uso de **ping** y **ping tcp** para validar el ruteo de capa 3 y la conectividad de capa 4 para BGP o los recursos de punto final si utiliza el ruteo estático.

```
<#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#

Paso 4. Cuando utiliza BGP. Verifique la conectividad BGP, las rutas recibidas y anunciadas a Azure y la tabla de ruteo del 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
```

Paso 5. Haga ping a un dispositivo a través del túnel. En este ejemplo, es una máquina virtual de Ubuntu que se ejecuta en 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

Para ver las rutas efectivas en la VM remota ahora, deben mostrar las rutas que ASA anunció a la nube, como se muestra en la imagen.

Dashboard > Resource groups > CX-SecurityTLs-ResourceGroup > jyoungta-ubuntu-azure - Diagnose and solve problems

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
Default	Active	10.1.0.0/16	Virtual network	-
Virtual network gateway	Active	192.168.100.0/30	Virtual network gateway	-
Virtual network gateway	Active	192.168.100.1/32	Virtual network gateway	-
Virtual network gateway	Active	192.168.2.0/24	Virtual network gateway	-
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	-

Troubleshoot

Actualmente no hay información específica disponible para resolver problemas de esta configuración.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).