

# AzureへのASA IPsec VTI接続の構成

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

---

## はじめに

このドキュメントでは、Azureへの適応型セキュリティアプライアンス(ASA)のIPsec仮想トンネルインターフェイス(VTI)接続を構成する方法について説明します。ASA 9.8.1では、IPsec VTI機能はIKEv2を利用するように拡張されましたが、これはIPv4上のsVTI IPv4に制限されています。この構成ガイドは、ASA CLIインターフェイスとAzure Portalを使用して作成されました。Azureポータルでの構成は、PowerShellまたはAPIでも実行できます。Azureの構成方法の詳細については、Azureのドキュメントを参照してください。



注：現在、VTIはシングルコンテキストルーテッドモードでのみサポートされています。

---

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- ASA 9.8.1以降を実行するパブリックスタティックIPv4アドレスを使用してインターネットに直接接続されたASA
- Azureアカウント

### 使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

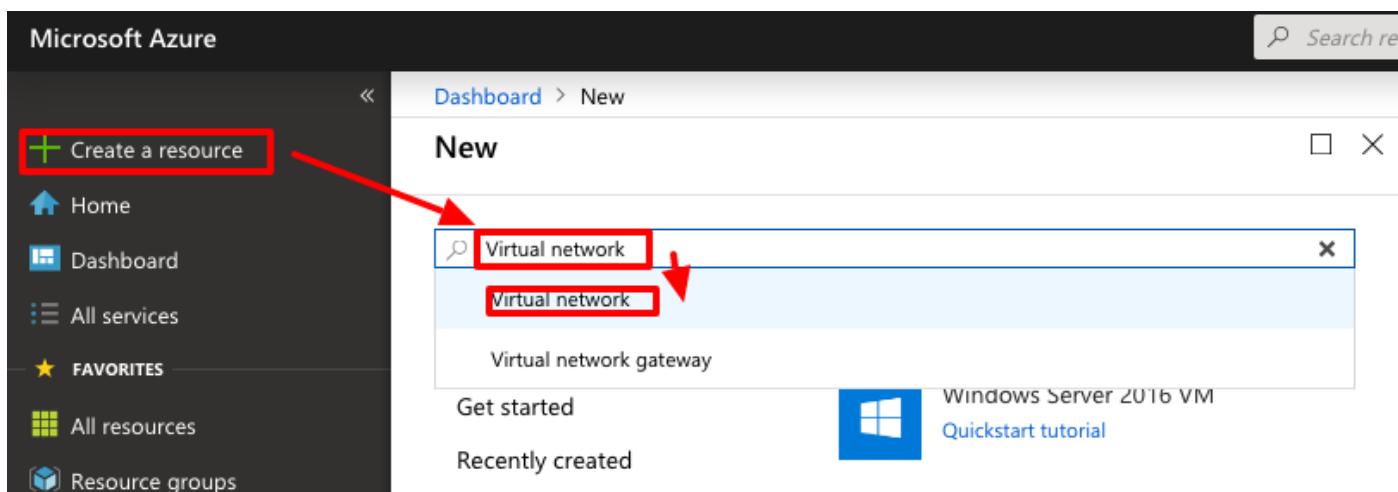
キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 設定

このガイドでは、Azureクラウドが構成されていないことを前提としています。リソースが既に確立されている場合は、これらの手順の一部をスキップできます。

ステップ 1： Azure内でネットワークを構成します。

これは、Azureクラウドに存在するネットワークアドレス空間です。このアドレス空間は、図に示すように、内部のサブネットワークを収容するのに十分な大きさである必要があります。



**Create virtual network**

\* Name: AzureNetworks ✓

\* Address space: 10.1.0.0/16 ✓  
10.1.0.0 - 10.1.255.255 (65536 addresses)

\* Subscription: Microsoft Azure Enterprise ✓

\* Resource group: CX-SecurityTLS-ResourceGroup ✓  
[Create new](#)

\* Location: Central US ✓

Subnet

\* Name: default

\* Address range: 10.1.0.0/24 ✓  
10.1.0.0 - 10.1.0.255 (256 addresses)

DDoS protection:  Basic  Standard

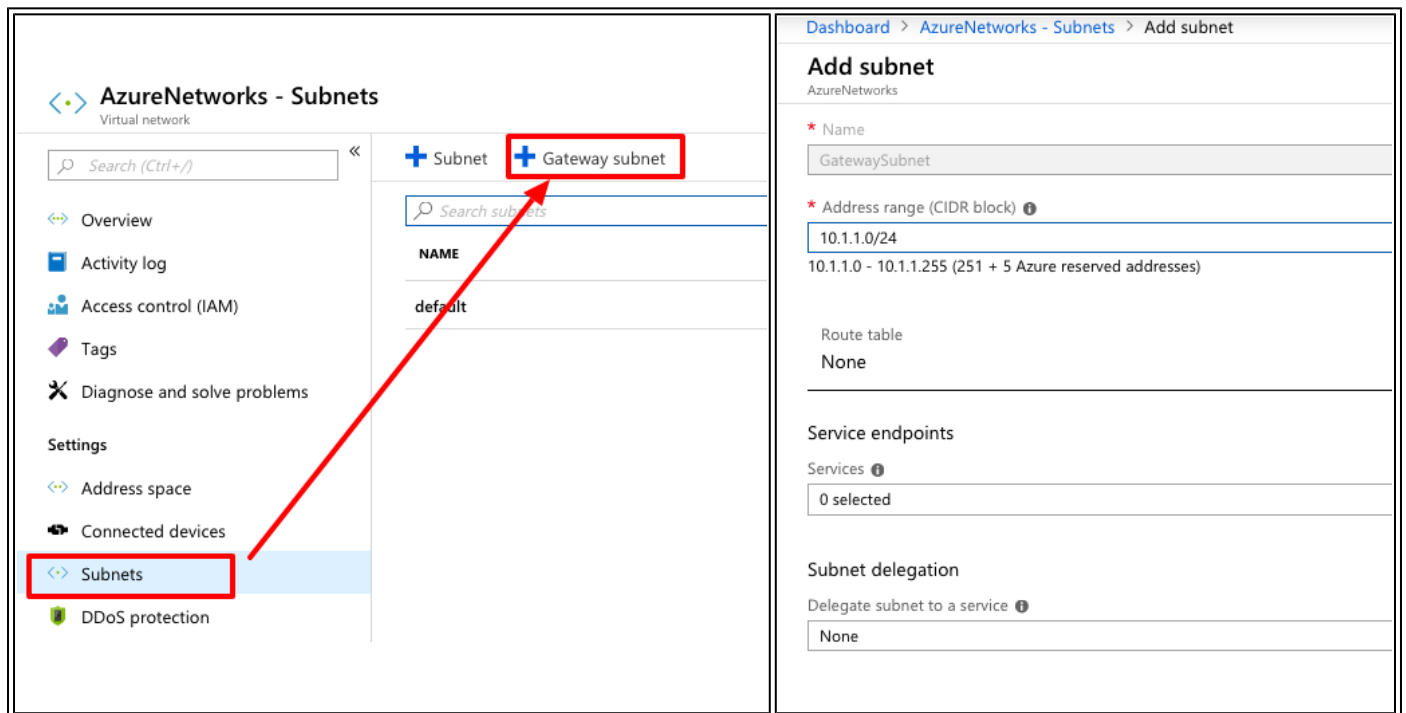
Service endpoints:  Disabled  Enabled

Firewall:  Disabled  Enabled

[名前(Name)]	クラウドでホストされるIPアドレス空間の名前
アドレス空間	CIDRの範囲全体がAzureでホストされています。この例では、10.1.0.0/16が使用されます
サブネット名	通常VMが接続される仮想ネットワーク内で作成される最初のサブネットの名前
サブネットアドレス範囲	仮想ネットワーク内に作成されたサブネット

ステップ2：ゲートウェイサブネットを作成するために仮想ネットワークを変更します。

仮想ネットワークに移動し、ゲートウェイサブネットを追加します。この例では、10.1.1.0/24が使用されます。

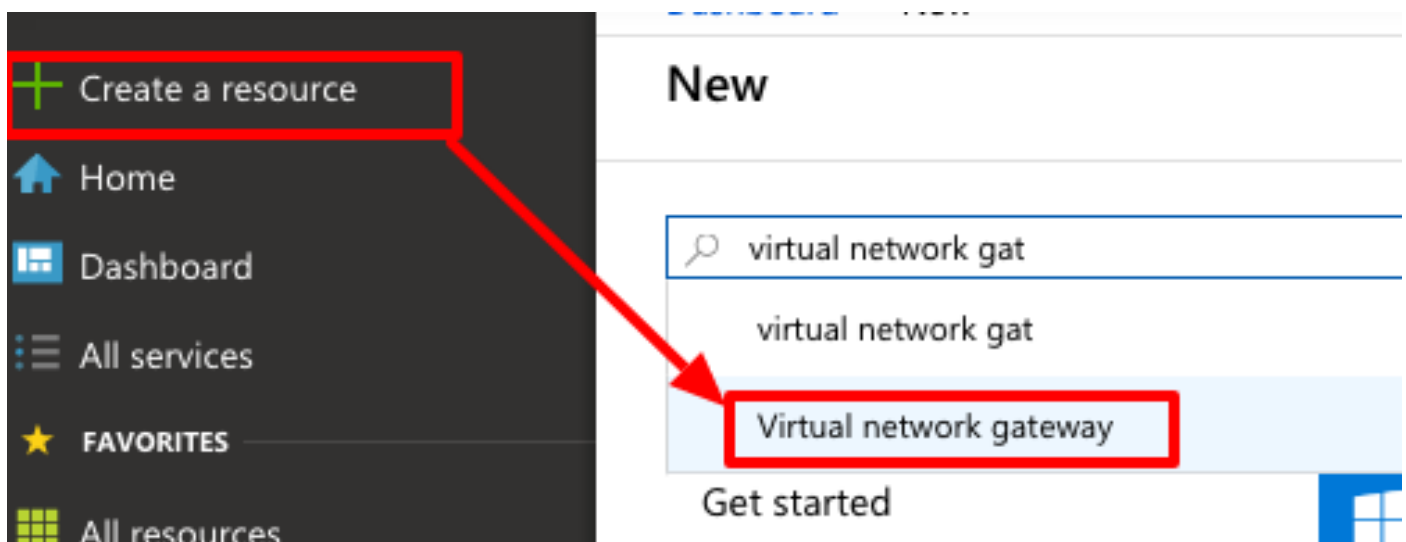


The screenshot shows the Azure portal interface for configuring a virtual network. On the left, the 'Subnets' menu item is highlighted with a red box. In the center, the '+ Gateway subnet' button is highlighted with a red box and an arrow pointing to the 'Add subnet' form on the right. The 'Add subnet' form shows the following configuration:

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

ステップ3：仮想ネットワークゲートウェイを作成します。

これは、クラウドでホストされているVPNエンドポイントです。これは、ASAがIPsecトンネルを構築するデバイスです。この手順では、仮想ネットワークゲートウェイに割り当てられるパブリックIPも作成します。



The screenshot shows the Azure portal 'New' page. The 'Create a resource' button is highlighted with a red box. A red arrow points from this button to the search results for 'virtual network gat'. The search results show 'Virtual network gateway' highlighted with a red box. Below the search results, there is a 'Get started' link and a Windows logo.

Dashboard > New > Virtual network gateway > Create virtual network gateway > Choose virtual network

## 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:

## Choose virtual network

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

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

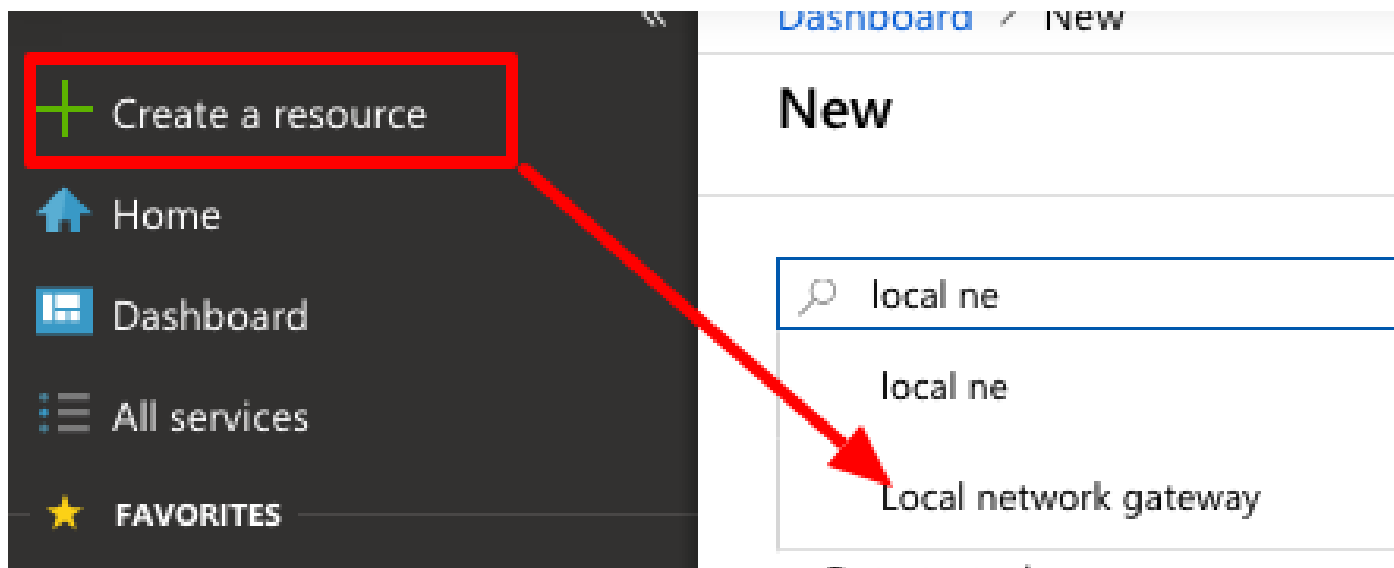
AzureNetworks  
CX-SecurityTLs-Resour...

[名前(Name)]	仮想ネットワークゲートウェイの名前
ゲートウェイタイプ	これはIPsec VPNであるため、VPNを選択します
VPNタイプ	これはVTIであるため、Route-basedを選択します。ポリシーベースは、クリプトマップVPNが実行されるときに使用されます
SKU	必要なトラフィック量に基づいてVpnGw1以上を選択する必要があります。BasicはBGPをサポートしていません
有効なアクティブ/アクティブモード	有効にしないでください。ポストイングの時点では、ASAはループバックまたはインターフェイス内からBGPセッションを発信する機能を持っていません。Azureでは、BGPピアリングに対して1つのIPアドレスのみが許可されます

パブリックIPアドレス	新しいIPアドレスを作成し、リソースに名前を割り当てます
BGP ASNの設定	リンクでBGPを有効にするには、このチェックボックスをオンにします
ASN	これをデフォルトの65515のままにしておきます。これは、ASN Azureが自身を次のように表示します。

ステップ 4：ローカルネットワークゲートウェイを作成します。

ローカルネットワークゲートウェイは、ASAを表すリソースです。



**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  
 ▾

[名前(Name)]	ASAの名前
IP アドレス	ASAの外部インターフェイスのパブリック IPアドレス
アドレス空間	サブネットは後でVTIに設定されます
BGPの設定	BGPを有効にするには、これをオンにします
ASN	このASNはASAで設定されます
BGPピアのIPアドレス	IPアドレスがASA VTIインターフェイスに設定されている

ステップ 5： 図に示すように、仮想ネットワークゲートウェイとローカルネットワークゲートウェイの間に新しい接続を作成します。

- + 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 ⓘ



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

### Create connection

- 1 Basics  
Configure basic settings ✓
- 2 Settings  
Configure connection settings ✓
- 3 Summary  
Review and create >

### Summary

<b>Basics</b>	
Connection type	Site-to-site (IPsec)
Subscription	Microsoft Azure Enterprise
Resource Group	CX-SecurityTLs-ResourceGroup
Location	Central US
<b>Settings</b>	
Virtual network gateway	VNGW1
Local network gateway	ASA
Connection name	VNGW1-ASA
Shared key (PSK)	ChooseSomeSecretPassword

手順 6 : ASA の設定.

まず、外部インターフェイスでIKEv2を有効にし、IKEv2ポリシーを設定します。

```
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
```

手順 6 : IPsecトランスフォームセットとIPsecプロファイルを設定します。

```
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
```

ステップ 8 : トンネルグループを設定します。

図に示すように、手順3で作成した仮想ネットワークゲートウェイのパブリックIPv4アドレスを取得します。



Dashboard > VNGW1

**VNGW1**  
Virtual network gateway

Search (Ctrl+/)

Move Delete

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Connections

Print to site configuration

Resource group (change)  
[CX-SecurityTls-ResourceGroup](#)

SKU  
VpnGw1

Location  
Central US

Gateway type  
VPN

Subscription (change)  
[Microsoft Azure Enterprise](#)

VPN type  
Route-based

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

Virtual network  
[AzureNetworks](#)

Public IP address  
**A.A.A.A**(PublicIPforVNGW1)

Tags (change)  
[Click here to add tags](#)

次に、ステップ3で定義した事前共有キーを使用して、ASAでグループポリシーとトンネルグループを設定します。

```
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 *****
```

ステップ 9： トンネル インターフェイスを設定します。

ステップ4: ( ローカルネットワークゲートウェイの設定 ) BGP接続のネットワークアドレスとIPアドレスが設定されました。これは、VTIで設定するIPアドレスとネットワークです。

```
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
```

ステップ 10：

オプション 1ダイナミックルーティングを設定します。BGPを使用してAzureとルートを交換します。

AzureでBGPルーターのIPアドレスを見つけて、手順3で作成した仮想ネットワークゲートウェイの構成を表示します。この例では10.1.2.254です。

**VGW - Configuration**  
Virtual network gateway

Search (Ctrl+/)

Save Discard

\* SKU ⓘ  
VpnGw1

Active-active mode  
Enabled Disabled

Configure BGP ASN

\* Autonomous system number (ASN) ⓘ  
65515

BGP peer IP address(es)  
10.1.2.254

ASAで、VTIトンネルから10.1.2.254を指すスタティックルートを設定します。この例では、192.168.100.2はVTIと同じサブネット内にあります。そのIPアドレスを持つデバイスがなくても、ASAはVTIインターフェイスをポイントするルートをインストールします。

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

次に、ASAでBGPを設定します。ネットワーク192.168.2.0/24はASAの内部インターフェイスであり、クラウドに伝播されるルートです。また、Azureで設定されたネットワークはASAにアドバタイズされます。

```
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
```

オプション 2スタティックルーティングの設定：ASAとAzureの両方でルートを静的に設定します。VTIトンネルを介してAzureネットワークにトラフィックを送信するようにASAを設定します。

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

ASAの背後にあるネットワークとトンネルインターフェイスのサブネットを使用して、手順4で作成したローカルネットワークゲートウェイを変更し、「追加のネットワークスペースの追加」セクションでプレフィックスを追加します。

## 確認

ここでは、設定が正常に機能しているかどうかを確認します。

ステップ 1： show crypto ikev2 saを使用して、IKEv2セッションが確立されていることを確認します。

<#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

ステップ 2： show crypto ipsec saコマンドを使用して、IPSec SAもネゴシエートされていることを確認します。

<#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#
```

ステップ 3 : pingおよびping tcpを使用してBGPリモートルータへのトンネルを介した接続を確認し、BGPのレイヤ3ルーティングおよびレイヤ4接続、またはスタティックルーティングを使用している場合はエンドポイントリソースを検証します。

```
<#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#
```

ステップ 4 : BGPを使用する場合。BGP接続、Azureに対して受信およびアドバタイズされたルート、およびASAのルーティングテーブルを確認します。

```
<#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
```

ステップ 5 : トンネルを介してデバイスにpingを実行します。この例では、Azureで実行される Ubuntu VMです。

```
<#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
```

リモートVM上の有効なルートを今すぐ表示します。図に示すように、ASAがクラウドにアドバタイズしたルートを表示する必要があります。

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

### 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

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	-

## トラブルシュート

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。



## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。