AzureへのASA IPsec VTI接続の構成

内容

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。

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静的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

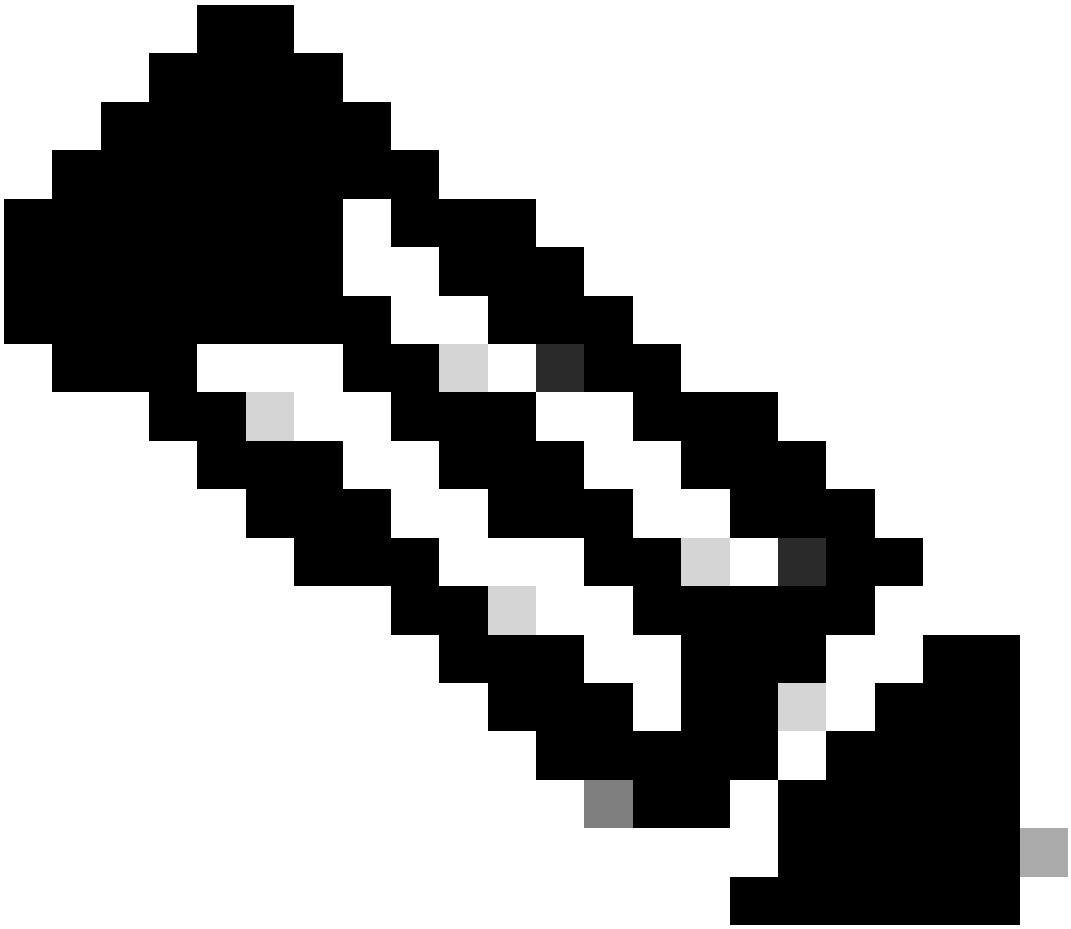
使用するコンポーネント

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。

背景説明

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、依然としてsVTI IPv4 over 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。



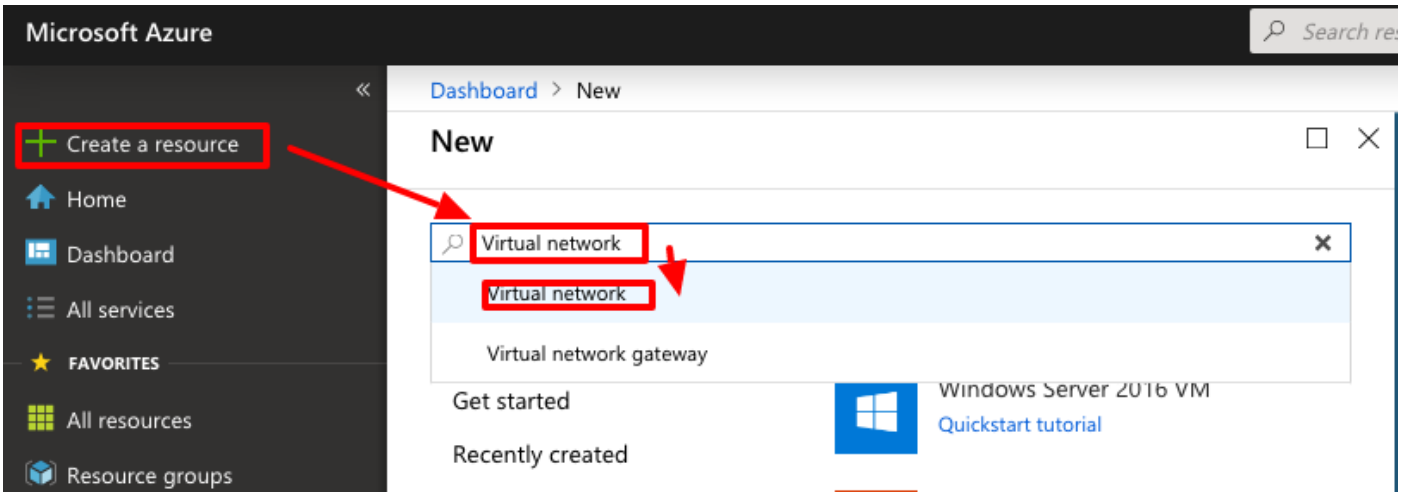
注：現在、VTIはシングルコンテキストルーテッドモードでのみサポートされています。

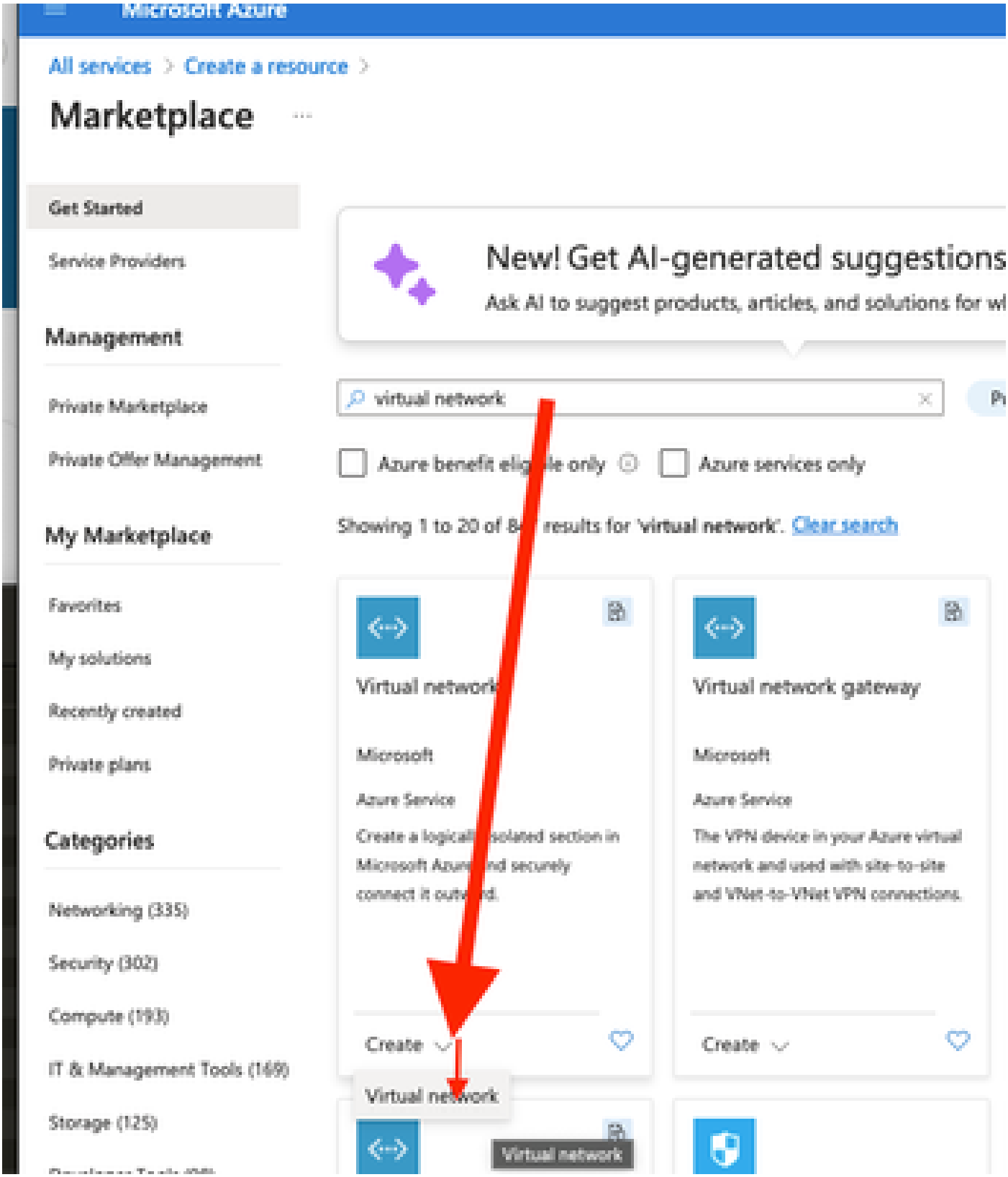
設定

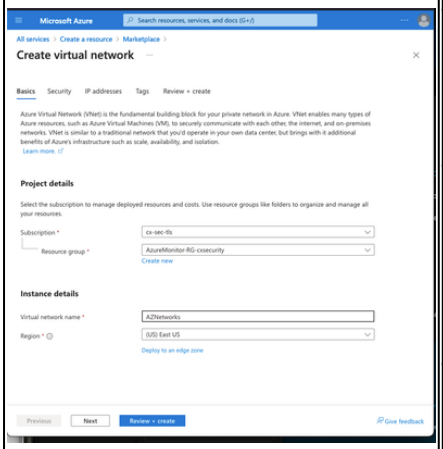
このガイドでは、Azureクラウドが構成されていないことを前提としています。リソースがすでに確立されている場合、これらの手順の一部は省略できます。

ステップ 1： Azure内でネットワークを構成します。

これは、Azureクラウド内に存在するネットワークアドレス空間です。図に示すように、このアドレス空間は、その中に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。

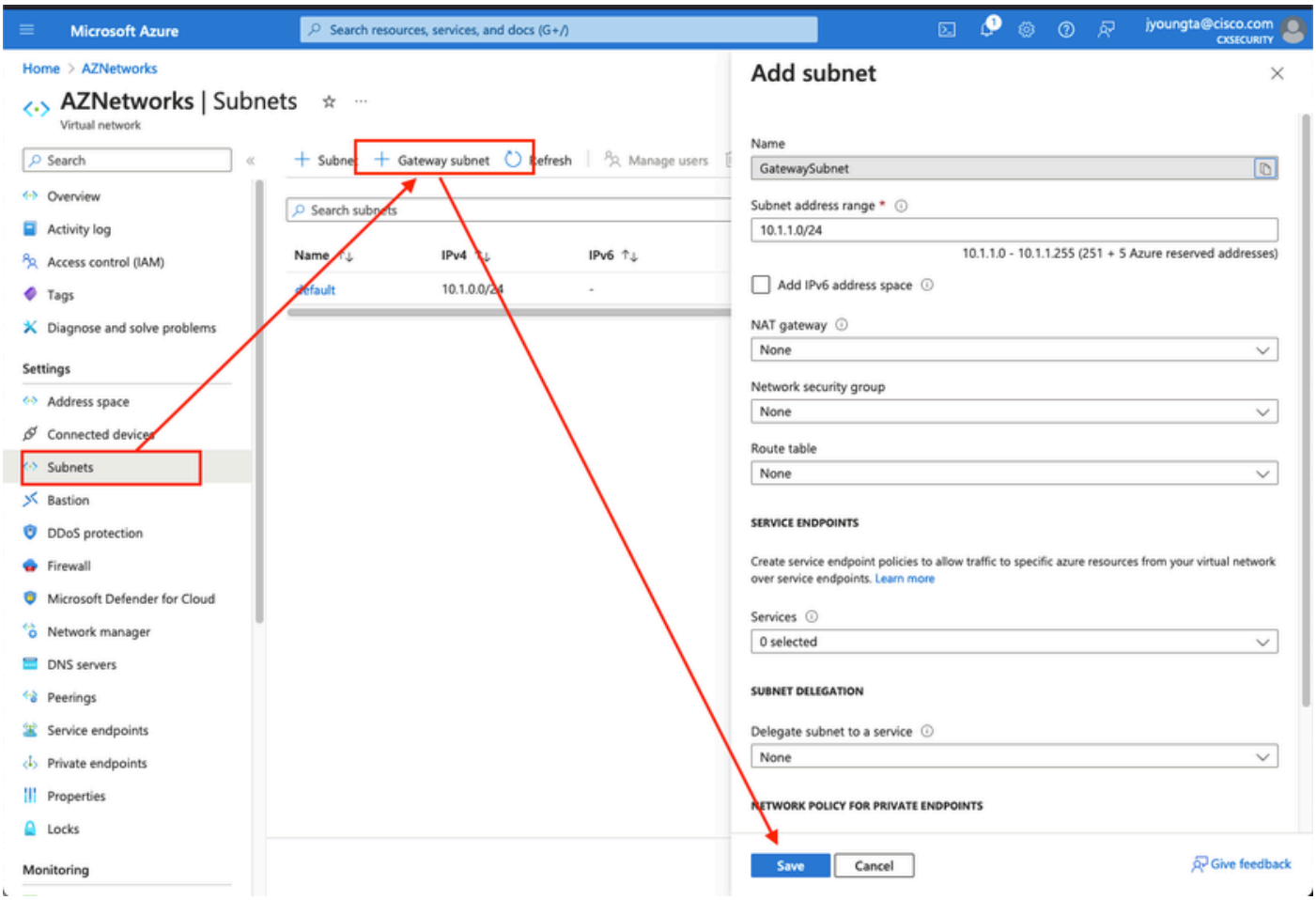



Microsoft Azure
All services > Create a resource >
Marketplace
Get Started
Service Providers
Management
Private Marketplace
Private Offer Management
My Marketplace
Favorites
My solutions
Recently created
Private plans
Categories
Networking (335)
Security (302)
Compute (193)
IT & Management Tools (169)
Storage (125)
New! Get AI-generated suggestions
Ask AI to suggest products, articles, and solutions for wl
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 logically isolated section in Microsoft Azure and securely connect it outward.
Create
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
Virtual network

	[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	AzureでホストされているCIDR範囲全体。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。通常、defaultという名前のサブネットが作成されます。
	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。

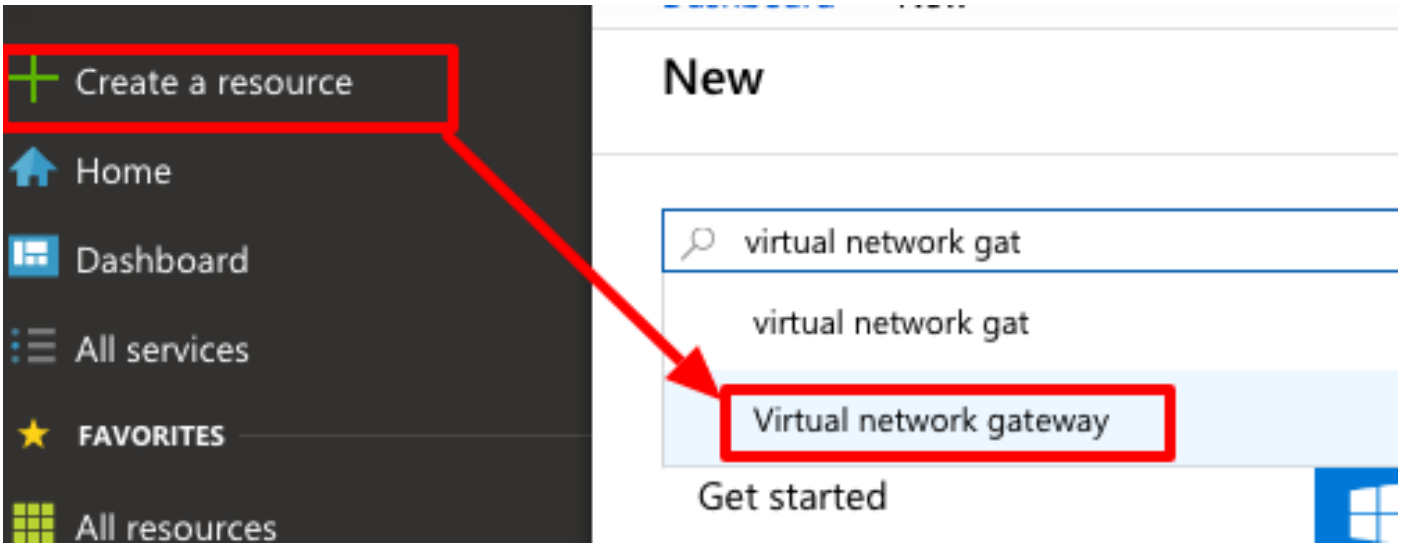
仮想ネットワークに移動し、ゲートウェイサブネットを追加します。この例では、10.1.1.0/24が使用されます。

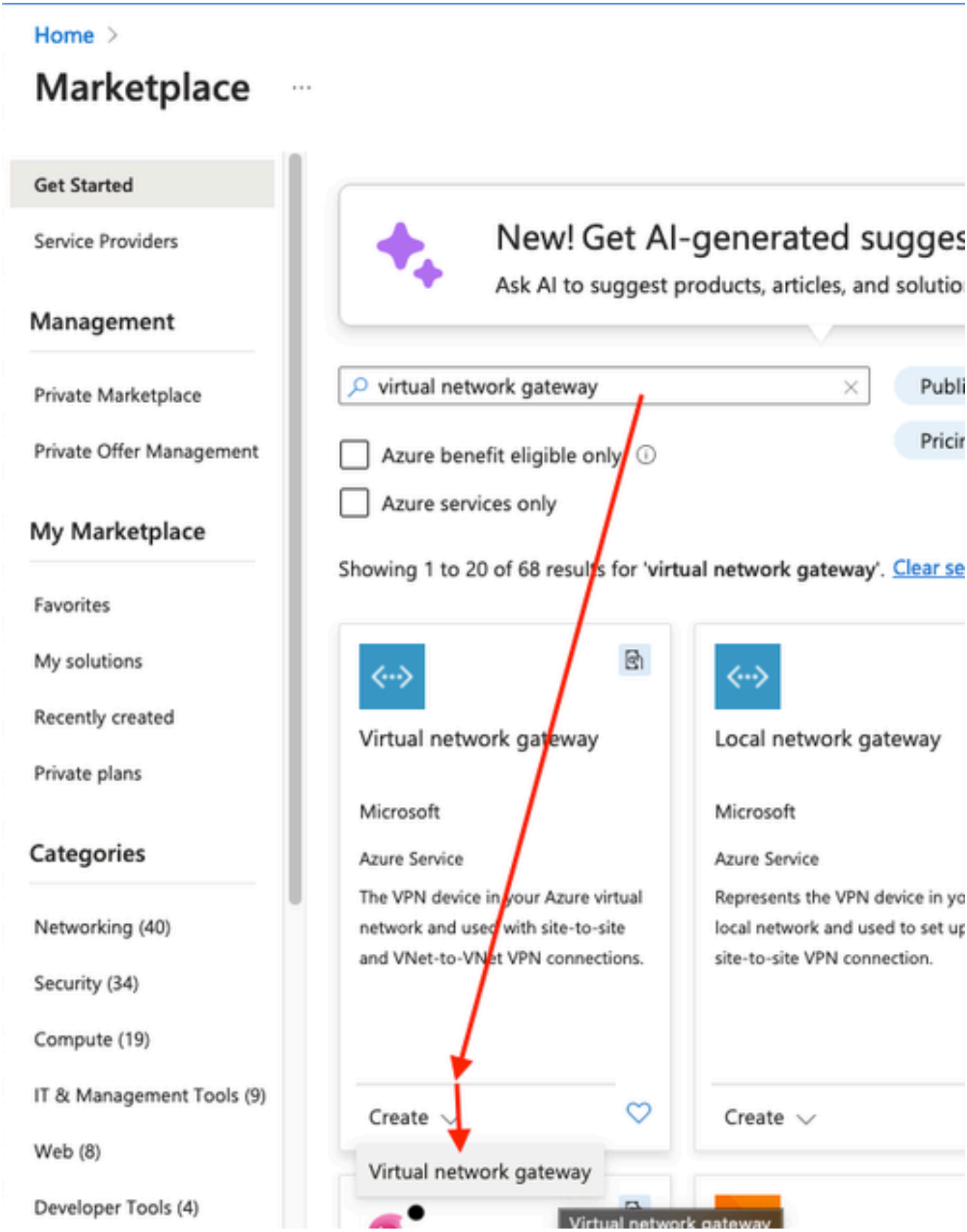


ステップ 3： 仮想ネットワークゲートウェイを作成します。

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

を構築する際に使用するデバイスです。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。 この手順の完了には15 ~ 20分かかります。



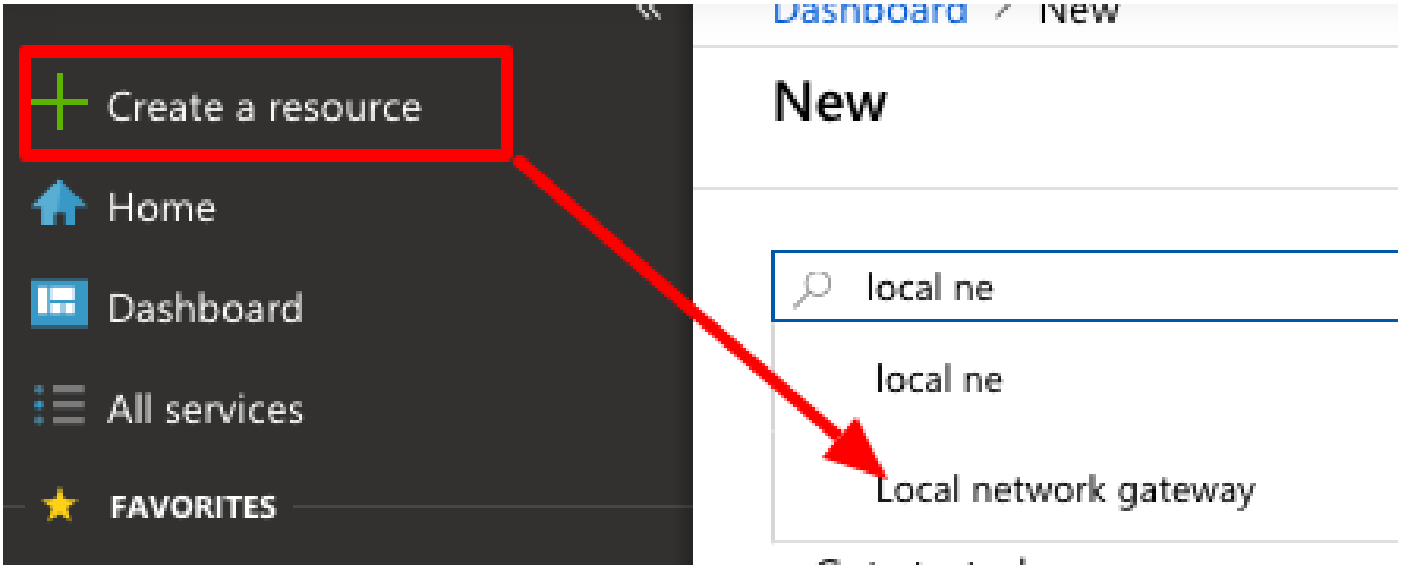


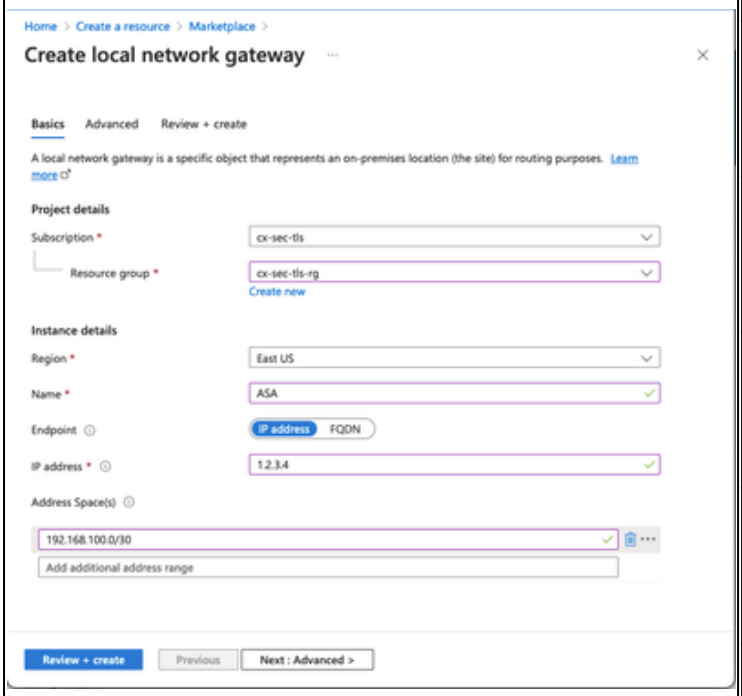
[名前(Name)]	仮想ネットワークゲートウェイの名前

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はサポートしていません ボーダーゲートウェイプロトコル(BGP)。
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。ポスティングの時点で、ASAにはループバックからBGPセッションを調達する機能がありません インターフェイス内に配置しますAzureでは、BGPピアリングにIPアドレスを1つしか使用できません。
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、自身を表すASN Azureです。

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。

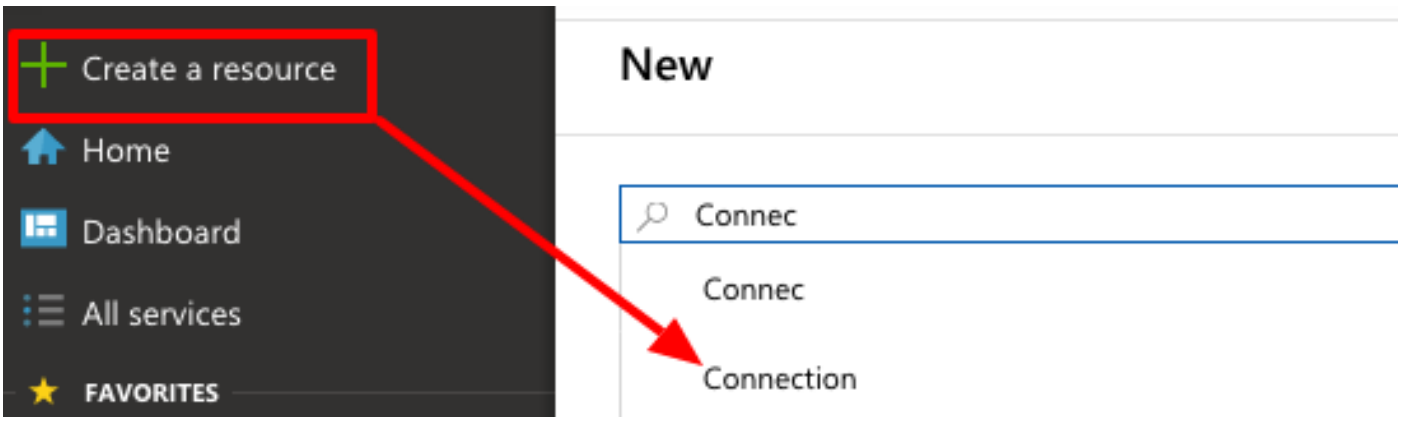
ローカルネットワークゲートウェイは、ASAを表すリソースです。

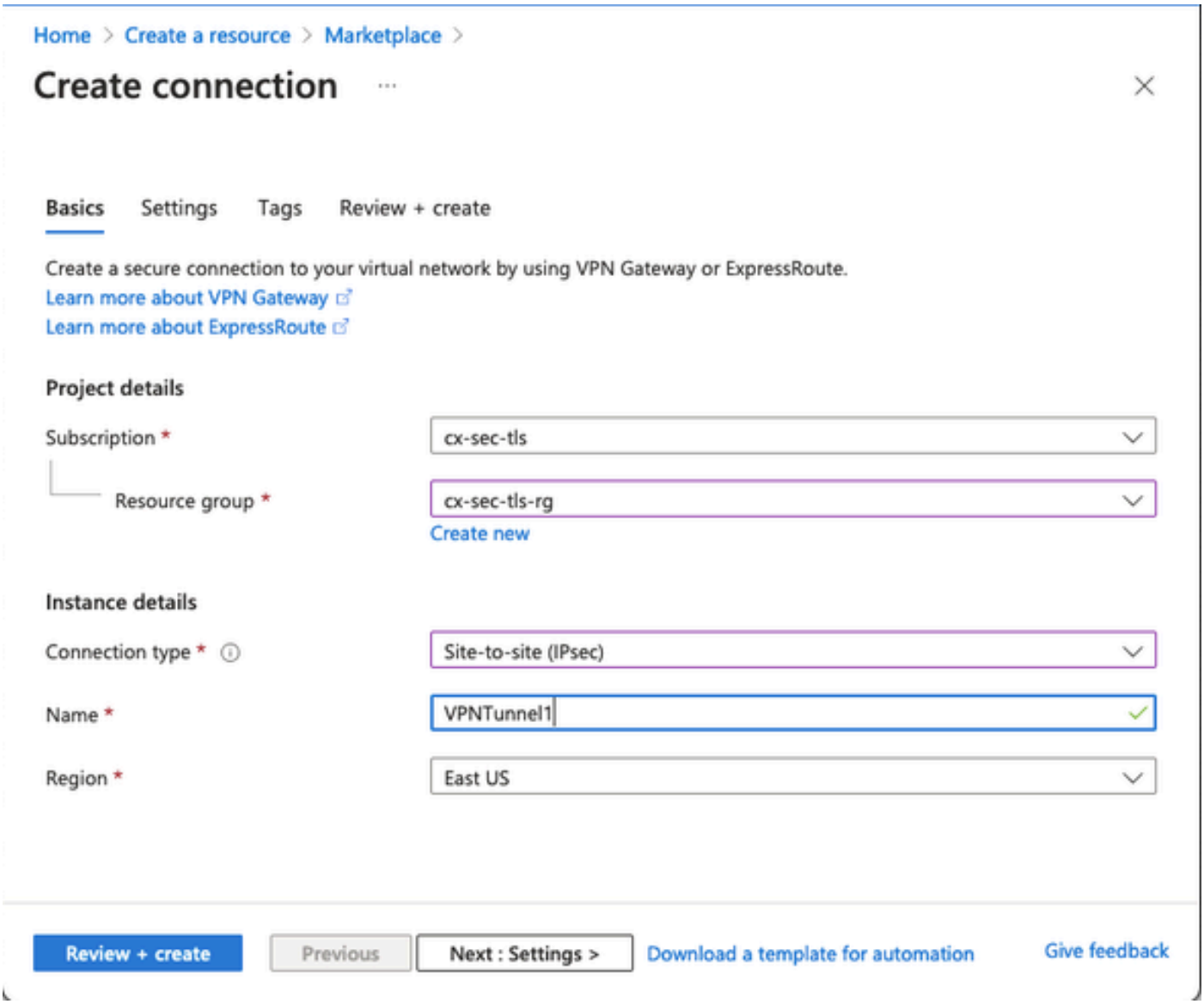


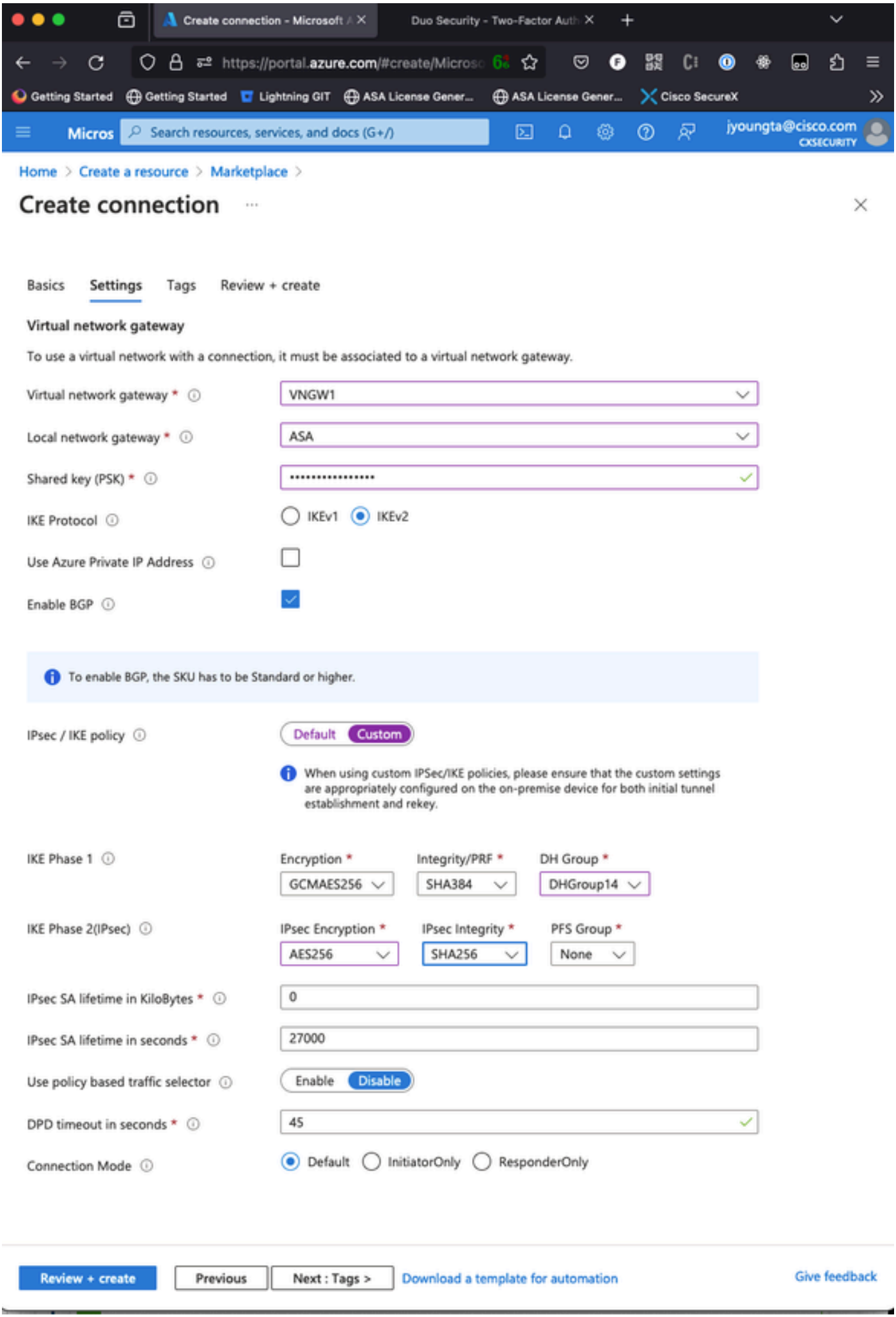


[名前(Name)]	ASAの名前
IP アドレス	ASAの外部インターフェイスのパブリックIPアドレス。
アドレス空間	サブネットは、後でVTIで設定します。
BGPの設定	BGPを有効にするには、これをオンにします。
ASN	このASNはASAで設定されます。
BGPピアのIPアドレス	IPアドレスはASA VTIインターフェイスで設定されます。

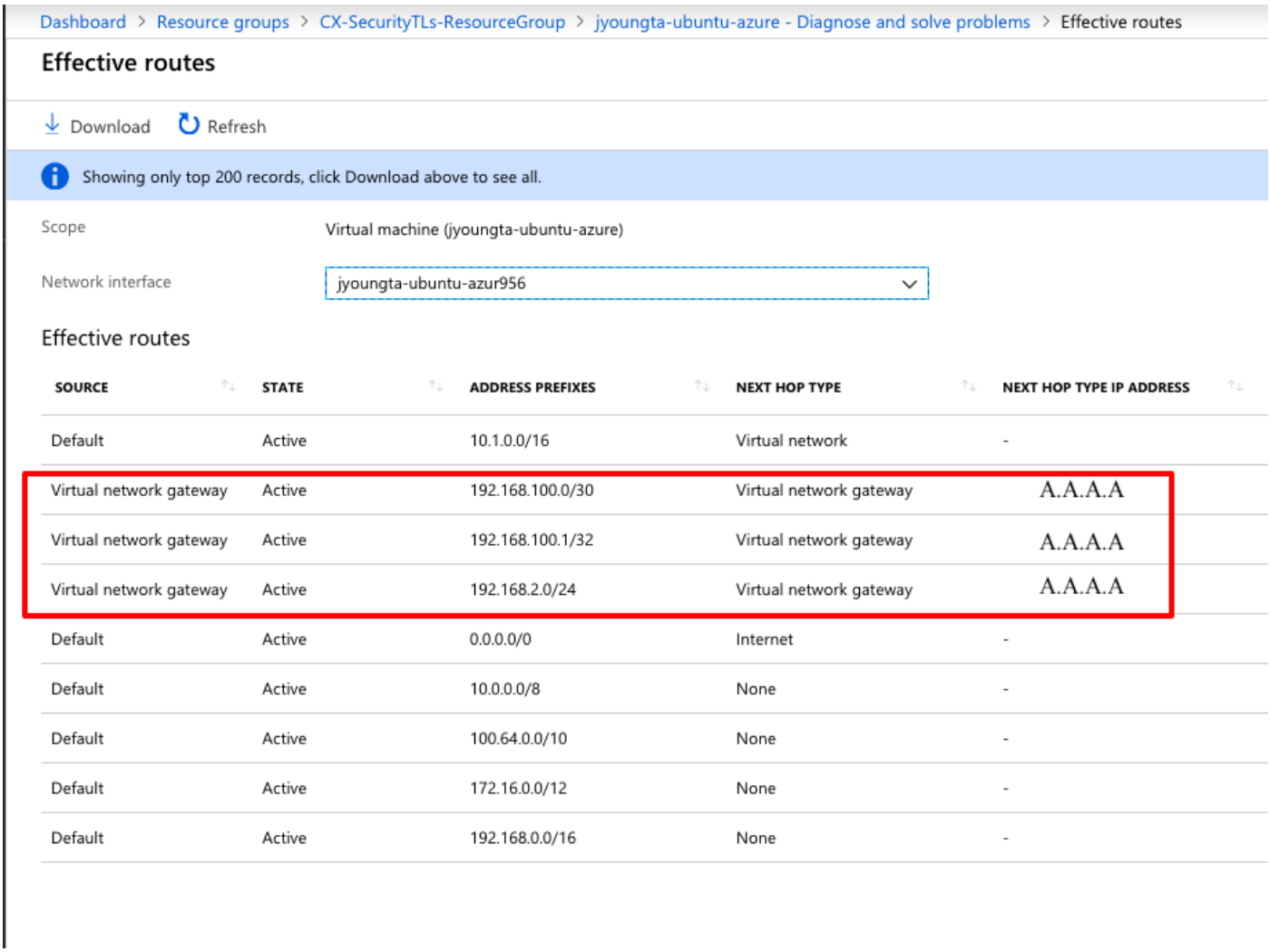
ステップ 5： 図に示すように、仮想ネットワークゲートウェイとローカルネットワークゲートウェイの間に新しい接続を作成します。




Home > Create a resource > Marketplace >
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 *
cx-sec-tls
Resource group *
cx-sec-tls-rg
Create new
Instance details
Connection type *
Site-to-site (IPsec)
Name *
VPNTunnel1
Region *
East US
Review + create
Previous
Next : Settings >
Download a template for automation
Give feedback


Create connection - Microsoft
Duo Security - Two-Factor Auth
https://portal.azure.com/#create/Microsc
Getting Started
Getting Started
Lightning GIT
ASA License Gener...
ASA License Gener...
Cisco SecureX
Micros
Search resources, services, and docs (G+/)
jyoungta@cisco.com
CXSECURITY
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 *
VNGW1
Local network gateway *
ASA
Shared key (PSK) *
IKE Protocol
IKEv1
IKEv2
Use Azure Private IP Address
Enable BGP
To enable BGP, the SKU has to be Standard or higher.
IPsec / IKE policy
Default
Custom
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 *
GCMAES256
Integrity/PRF *
SHA384
DH Group *
DHGroup14
IKE Phase 2(IPsec)
IPsec Encryption *
AES256
IPsec Integrity *
SHA256
PFS Group *
None
IPsec SA lifetime in KiloBytes *
0
IPsec SA lifetime in seconds *
27000
Use policy based traffic selector
Enable
Disable
DPD timeout in seconds *
45
Connection Mode
Default
InitiatorOnly
ResponderOnly
Review + create
Previous
Next : Tags >
Download a template for automation
Give feedback

手順 6： ASA の設定



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。