配置到Azure的ASA IPsec VTI连接

目录

简介

本文档介绍如何配置到Azure的自适应安全设备(ASA) IPsec虚拟隧道接口(VTI)连接。

先决条件

要求

Cisco 建议您了解以下主题：

- 使用运行ASA 9.8.1或更高版本的公共静态IPv4地址直接连接到互联网的ASA。
- Azure帐户

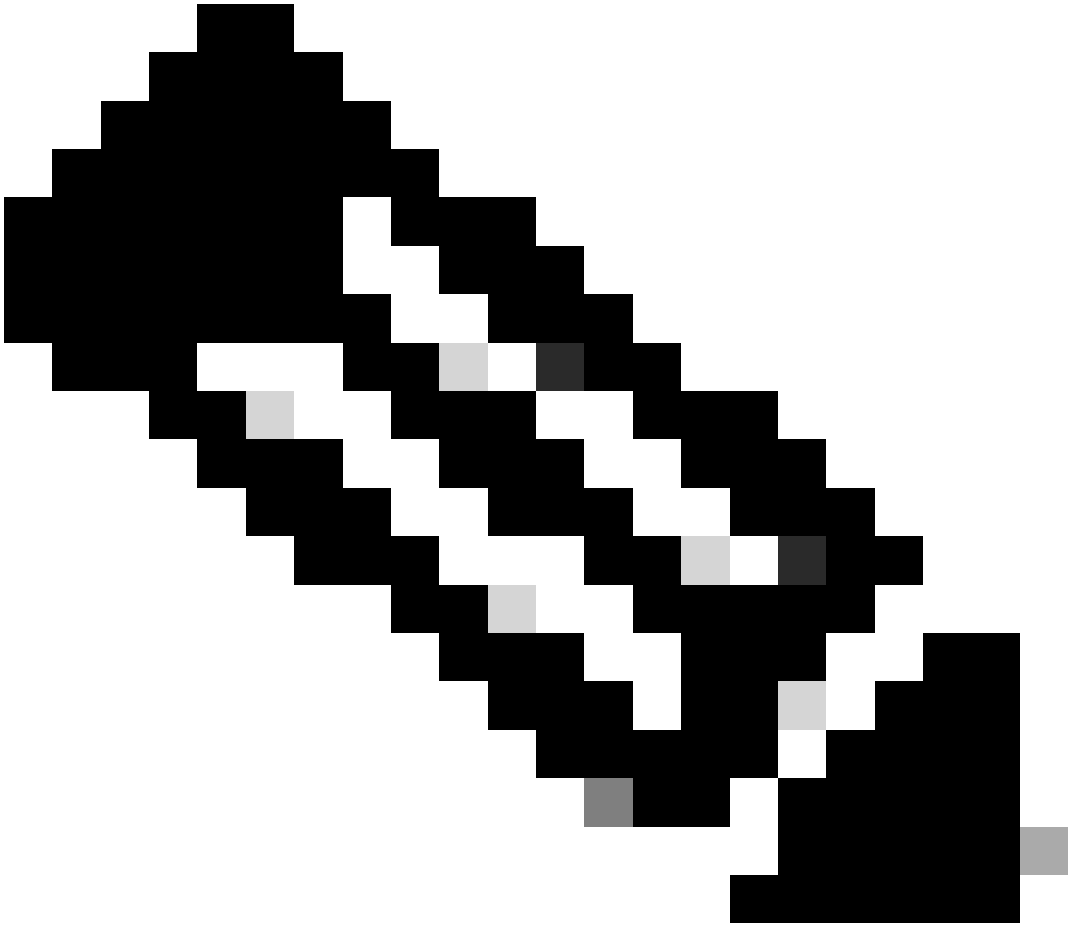
使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

在ASA 9.8.1中，IPsec VTI功能已扩展为使用IKEv2，但是，它仍然限制为通过IPv4的sVTI IPv4。此配置指南是使用ASA CLI界面和Azure门户生成的。Azure门户的配置也可以由PowerShell或API执行。有关Azure配置方法的详细信息，请参阅Azure文档。



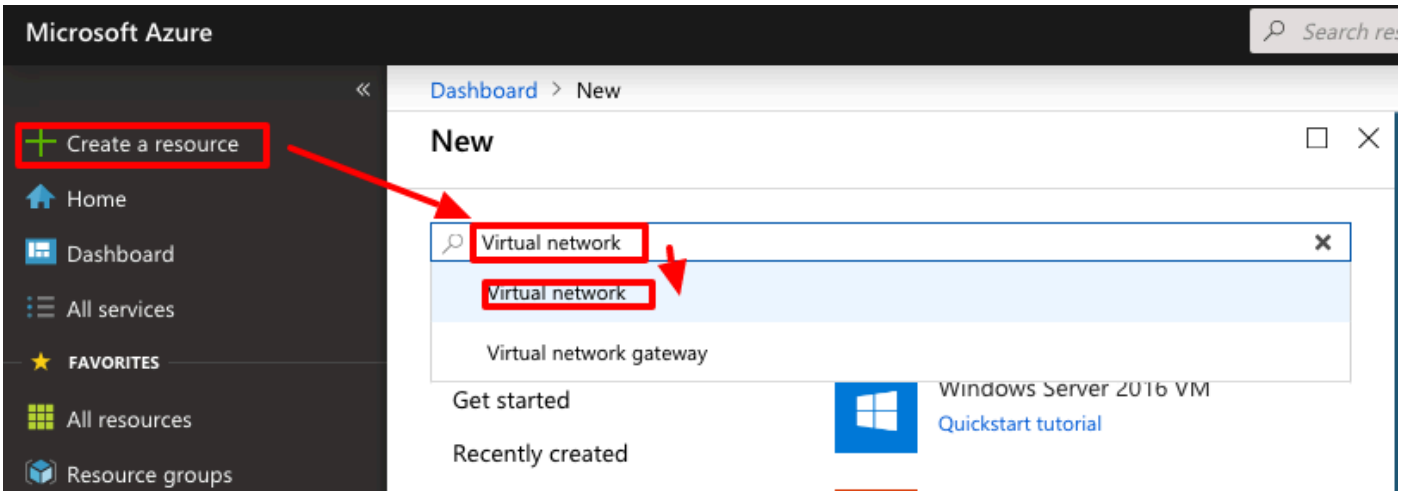
注意：目前，VTI仅在单情景路由模式下受支持。

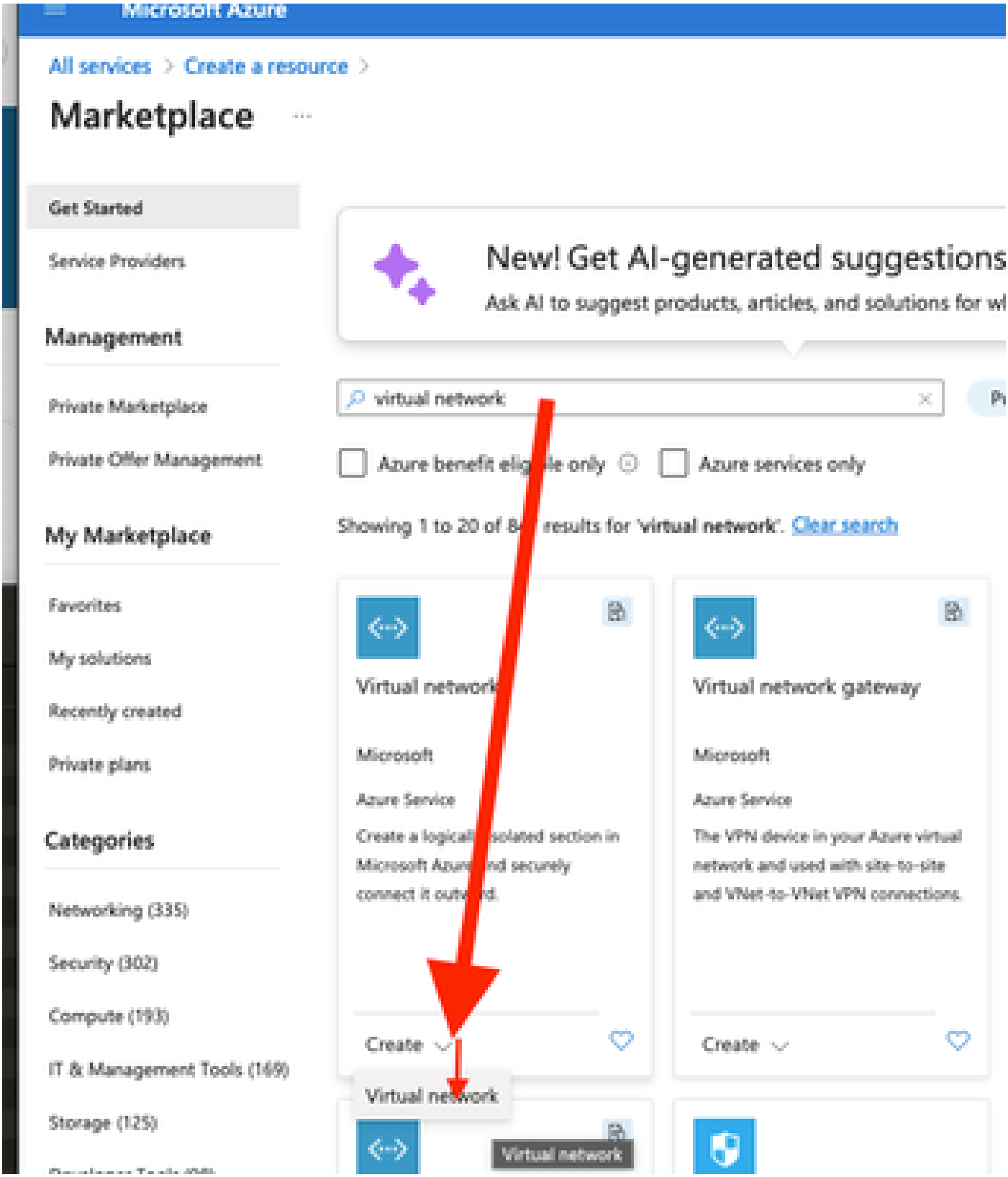
配置

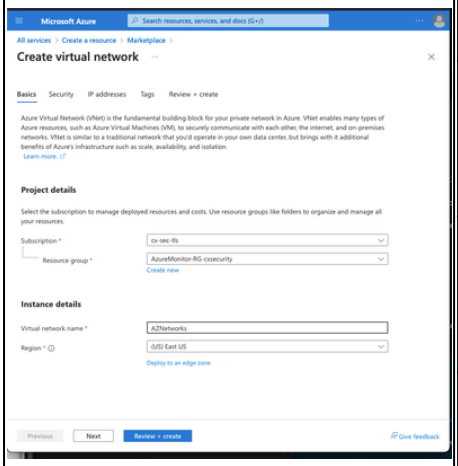
本指南假设Azure云尚未配置。如果已建立资源，则可以跳过其中某些步骤。

步骤1: 在Azure中配置网络。

这是位于Azure云中的网络地址空间。此地址空间必须足够大，才能容纳其中的子网（如图所示）。

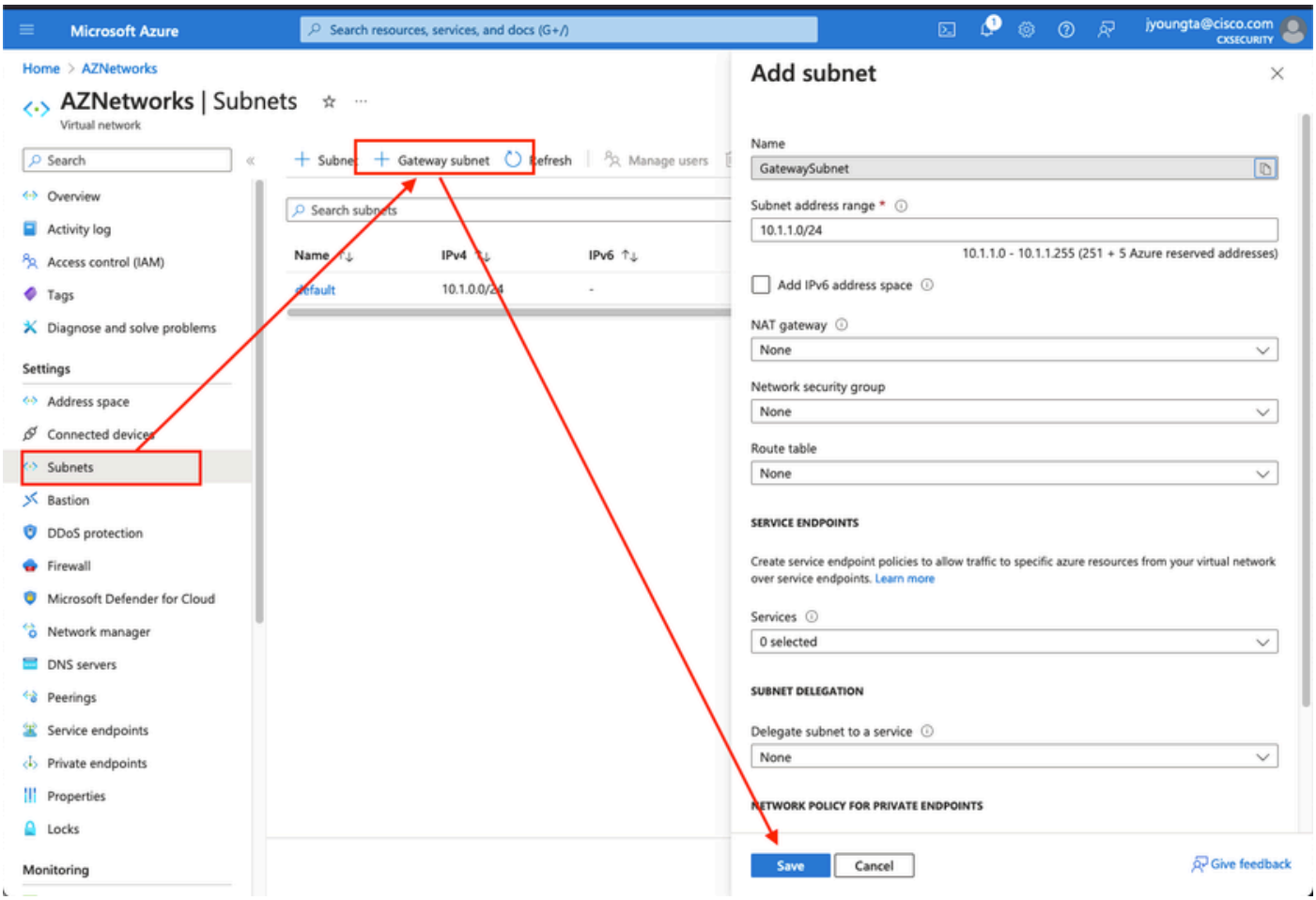

Microsoft Azure
Search re
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
Dashboard > New
New
Virtual network
Virtual network
Virtual network gateway
Get started
Recently created
Windows Server 2016 VM
Quickstart tutorial


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

	名称	云中托管的IP地址空间的名称
	地址空间	Azure中托管的整个CIDR范围。本例中使用的是10.1.0.0/16。
	子网名称	在通常连接VM的虚拟网络内创建的第一个子网的名称。通常创建一个名为default的子网。
	子网地址范围	在虚拟网络中创建的子网。

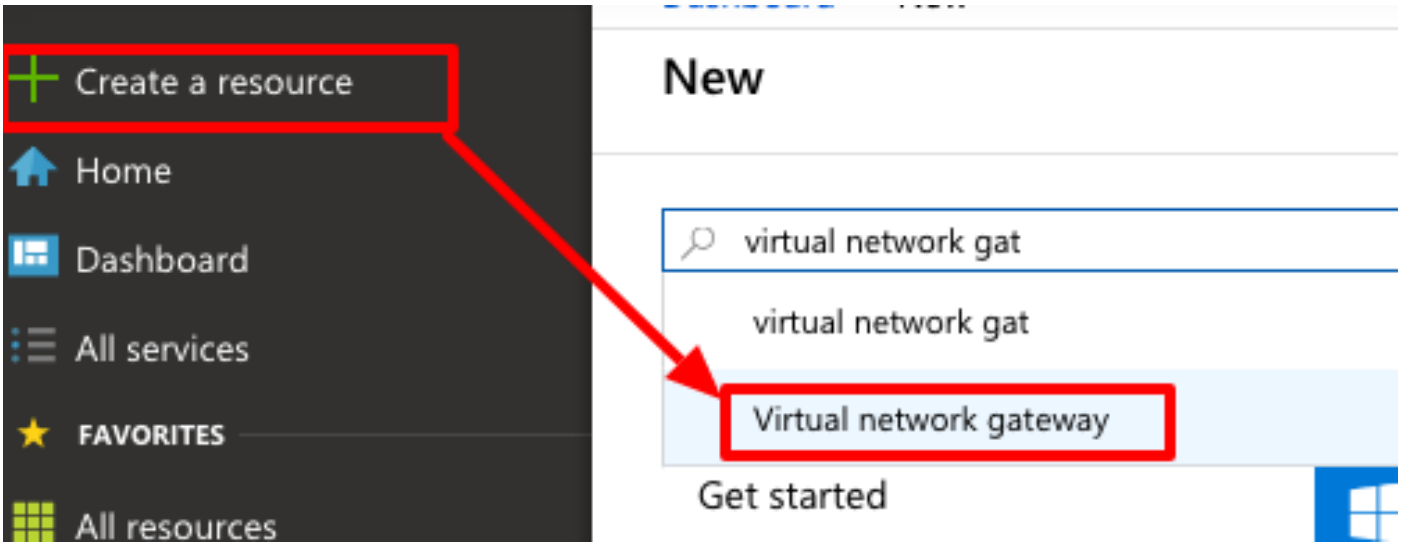
第二步： 修改虚拟网络以创建网关子网。

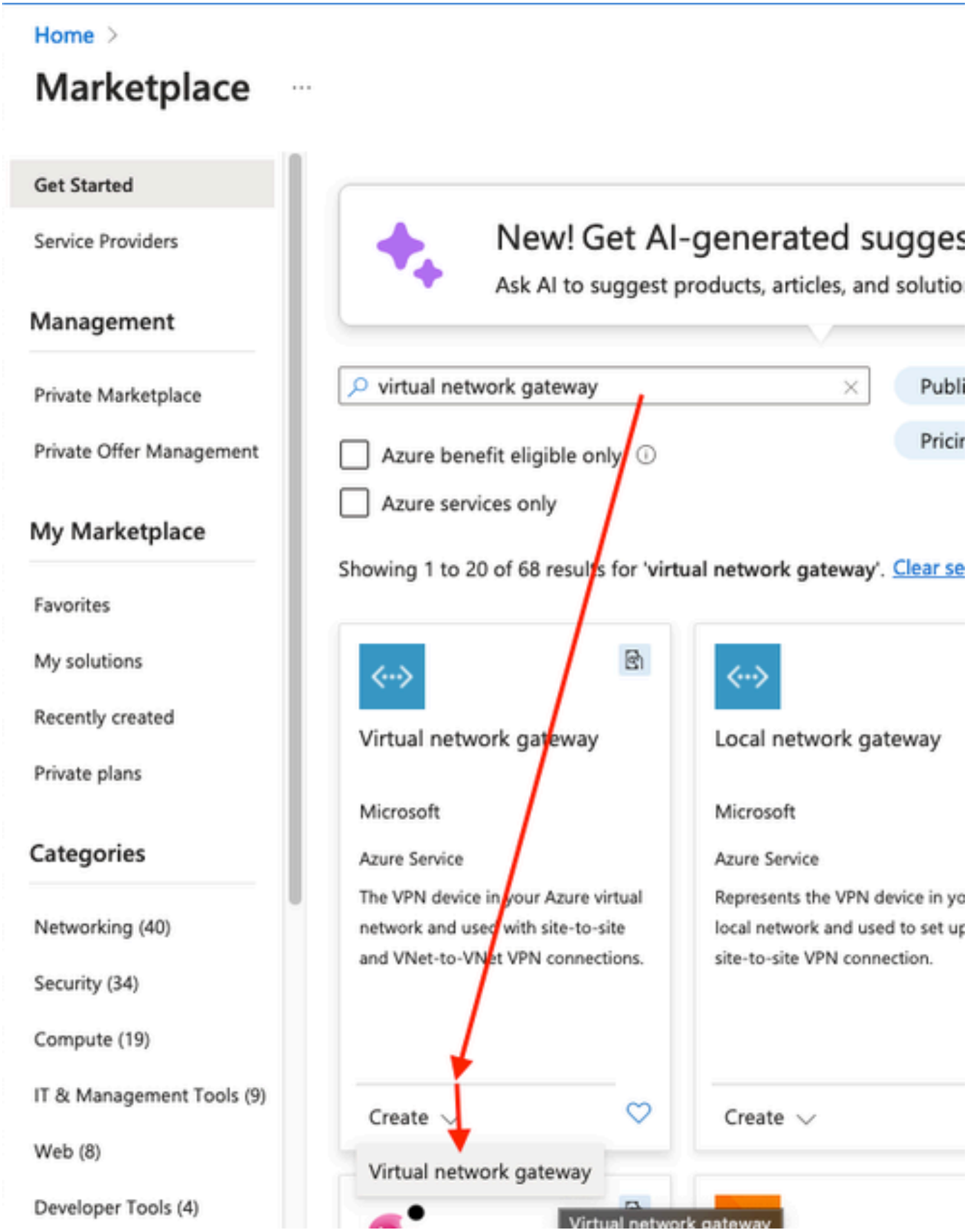
导航到虚拟网络并添加网关子网。本例中使用的是10.1.1.0/24。



第三步： 创建虚拟网络网关。

这是托管在云中的VPN终端。这是ASA用来构建IPSec隧道的设备。此步骤还会创建分配给虚拟网络网关的公共IP。 完成此步骤可能需要15 – 20分钟。


Create a resource
Home
Dashboard
All services
FAVORITES
All resources
New
virtual network gat
virtual network gat
Virtual network gateway
Get started

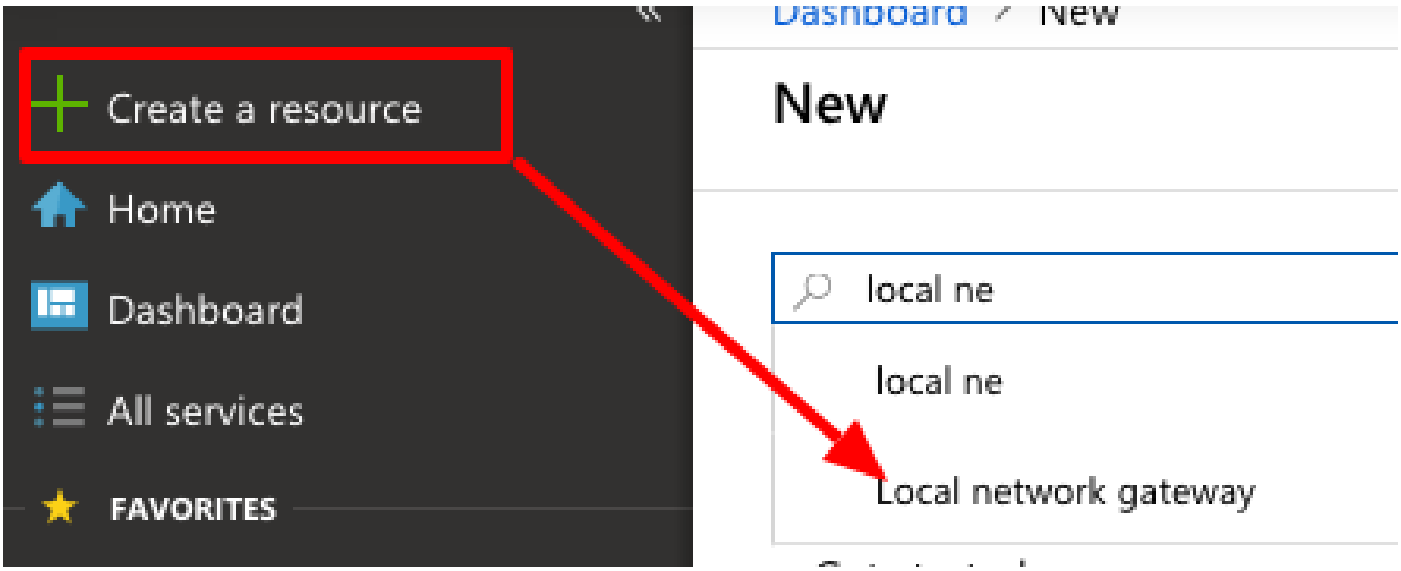


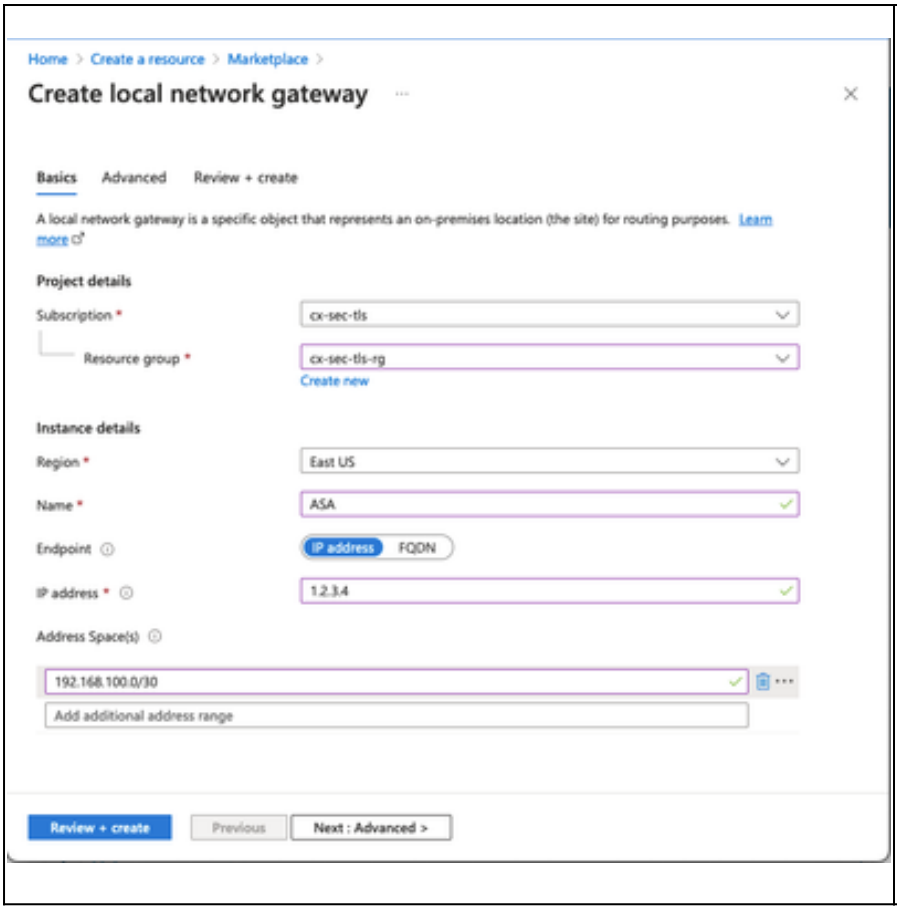
名称	虚拟网络网关的名称

网关类型	选择VPN，因为这是IPsec VPN。
VPN类型	选择Route-based，因为这是VTI。加密映射VPN完成后，使用基于策略的。
SKU	需要根据所需的流量量选择VpnGw1或更高版本。基本不支持 边界网关协议(BGP)
已启用主用/主用模式	不启用。在发布时，ASA没有从环回获取BGP会话的功能 或接口内部。Azure仅允许BGP对等的1个IP地址。
公共 IP 地址	创建新的IP地址并为资源指定名称。
配置BGP ASN	选中此框可在链路上启用BGP。
ASN	将此项保留为默认65515。这是ASN Azure展示自身。

第四步： 创建本地网络网关。

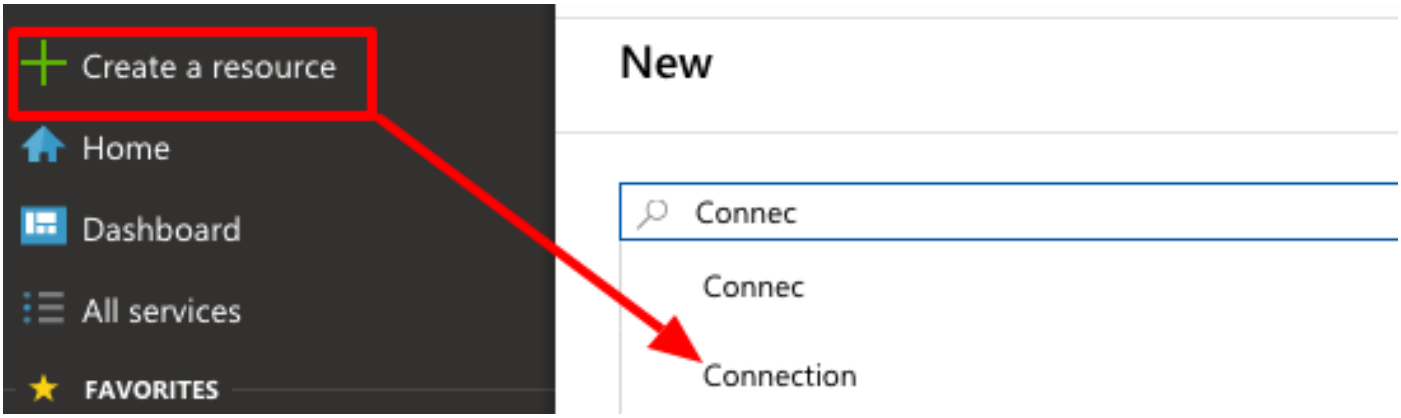
本地网络网关是代表ASA的资源。

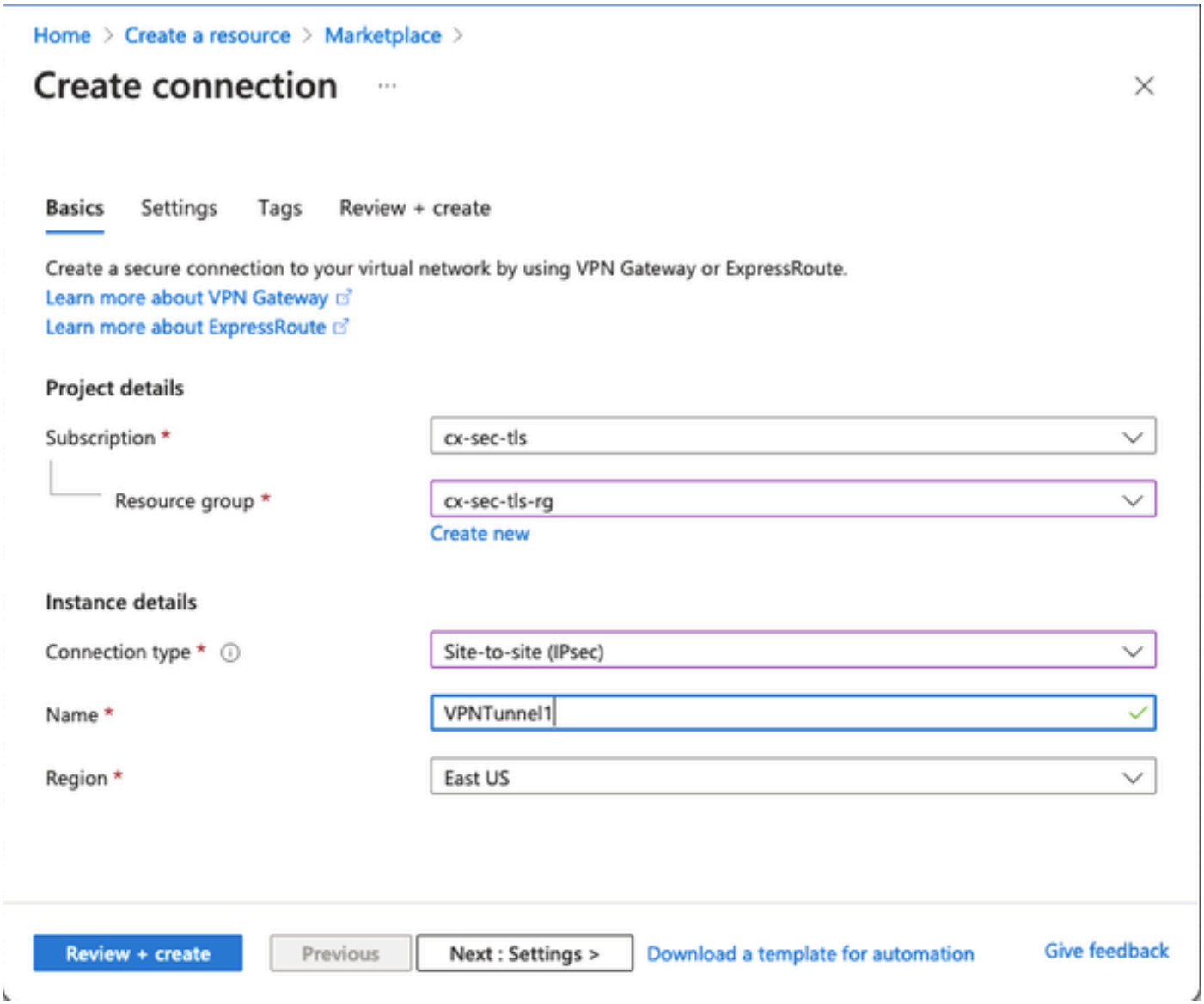


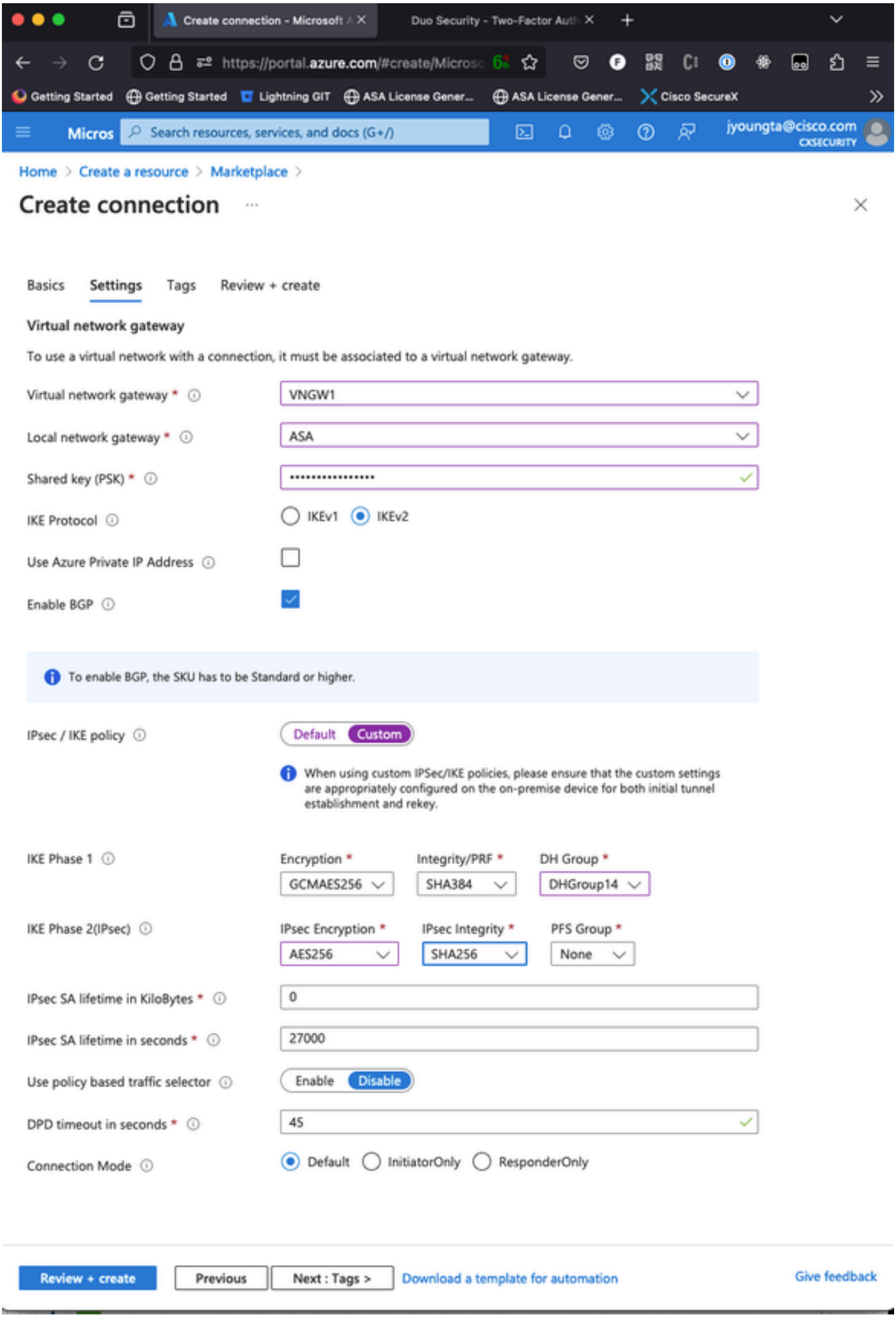


名称	ASA的名称
IP Address	ASA外部接口的公用IP地址。
地址空间	稍后将在VTI上配置子网。
配置BGP设置	选中此复选框可启用BGP。
ASN	此ASN在ASA上配置。
BGP对等体IP地址	IP地址在ASA VTI接口上配置。

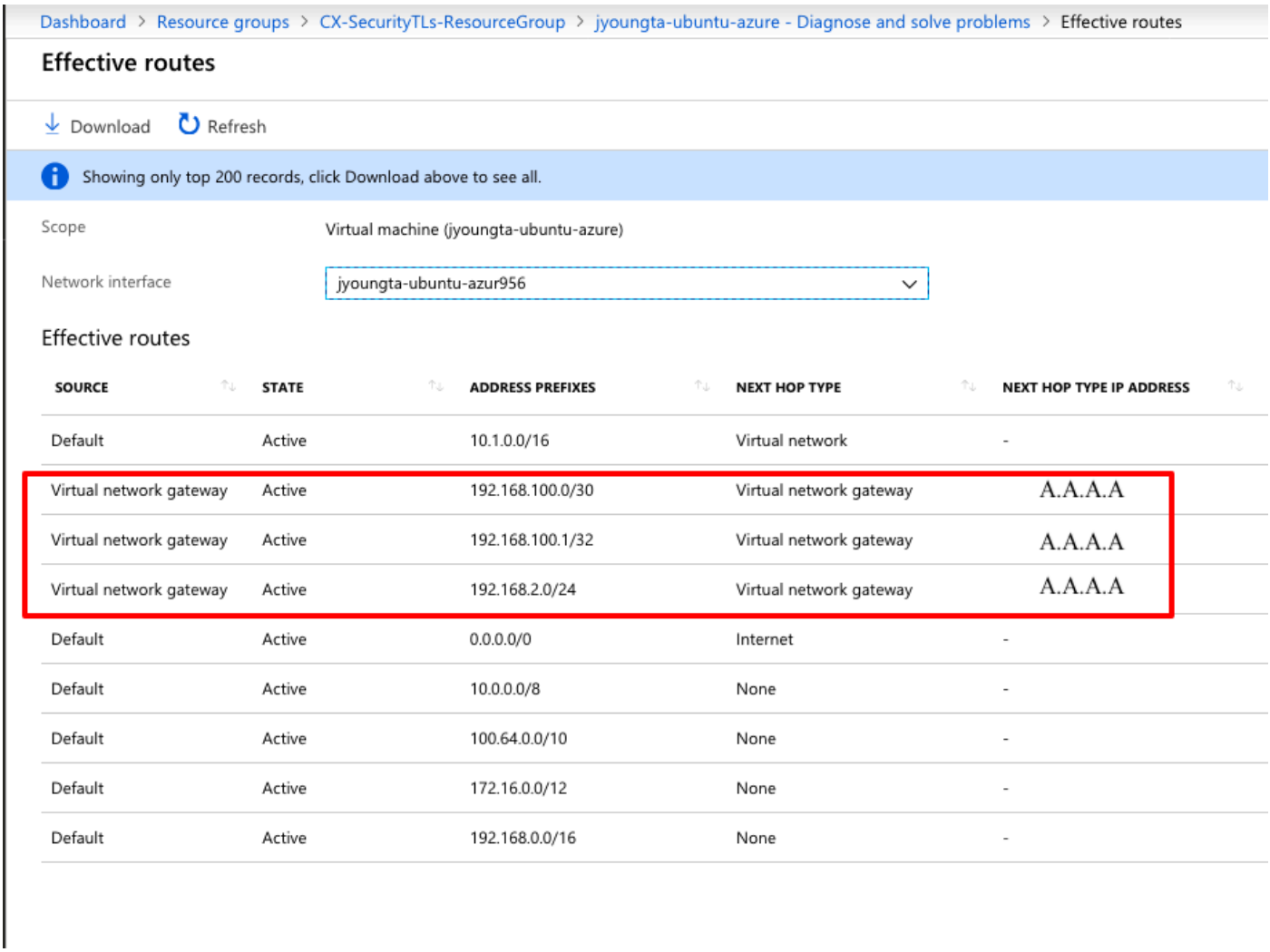
第五步： 在虚拟网络网关和本地网络网关之间创建新连接，如图所示。




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

第六步：配置ASA。



故障排除

当前没有故障排除此配置的特定可用资料。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。