

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 de Interfaz de túnel virtual (VTI) IPsec Adaptive Security Appliance (ASA) a Azure. En ASA 9.8.1, la función IPsec VTI se amplió para utilizar IKEv2; sin embargo, todavía se limita a sVTI IPv4 sobre IPv4. Esta guía de configuración se produjo con el uso de la interfaz CLI de ASA y el Portal de Azure. La configuración del portal de Azure también puede realizarla PowerShell o API. Para obtener más información sobre 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:

- 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.

The information in this document was created from the devices in a specific lab environment. All of

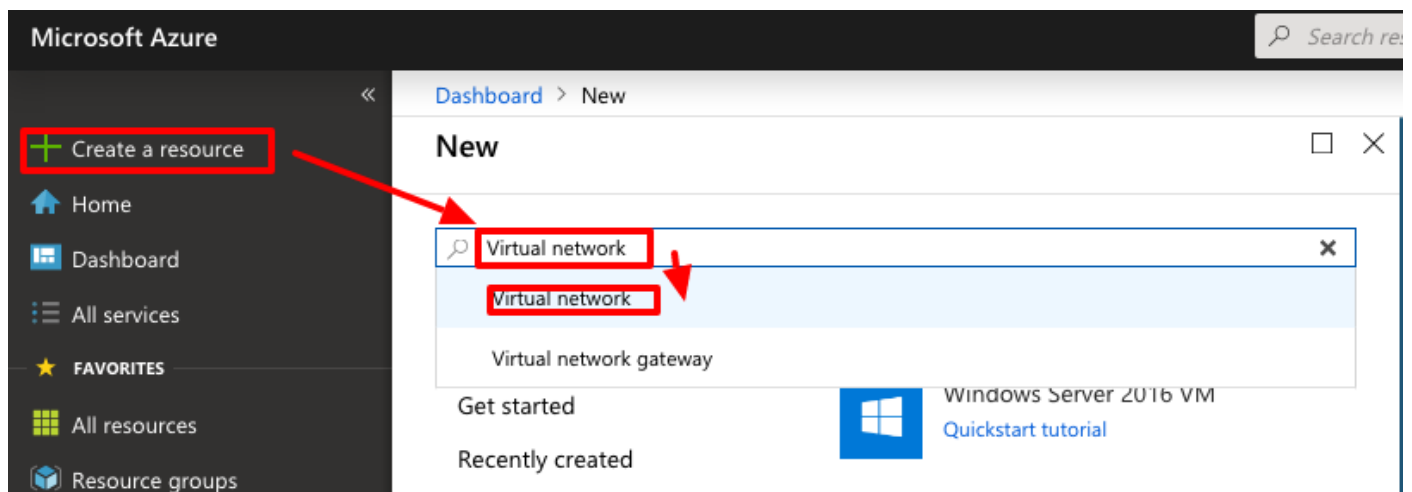
the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

En esta guía se asume 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 dentro de Azure.

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



Nombre	Nombre del espacio de dirección
Espacio de dirección	IP alojado en la nube Toda la gama CIDR alojada en Azure. En este ejemplo, se utilizó 10.1.0.0/16
Nombre de subred	El nombre de la primera subred creada dentro de la red virtual que se suelen conectar las VM
Intervalo de direcciones de subred	Una subred creada dentro de la red virtual

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

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

Navegue hasta 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

Paso 3. Cree un Virtual Network Gateway.

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

-  Create a resource
-  Home
-  Dashboard
-  All services
-  FAVORITES
-  All resources

New

virtual network gat

virtual network gat

Virtual network gateway

Get started 