

Konfigurieren der ASA IPsec VTI-Verbindung zu Azure

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie eine Adaptive Security Appliance (ASA) IPsec Virtual Tunnel Interface (VTI)-Verbindung mit Azure konfigurieren. In ASA 9.8.1 wurde die IPsec-VTI-Funktion auf IKEv2 erweitert. Sie ist jedoch weiterhin auf sVTI IPv4 über IPv4 beschränkt. Dieser Konfigurationsleitfaden wurde unter Verwendung der ASA CLI-Schnittstelle und des Azure-Portals erstellt. Die Konfiguration des Azure-Portals kann auch über PowerShell oder API erfolgen. Weitere Informationen zu den Azure-Konfigurationsmethoden finden Sie in der Azure-Dokumentation.

Anmerkung: Derzeit wird VTI nur im Routing-Modus mit einem Kontext unterstützt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Eine direkt mit dem Internet verbundene ASA mit einer öffentlichen statischen IPv4-Adresse, auf der ASA 9.8.1 oder höher ausgeführt wird.
- Ein Azure-Konto

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

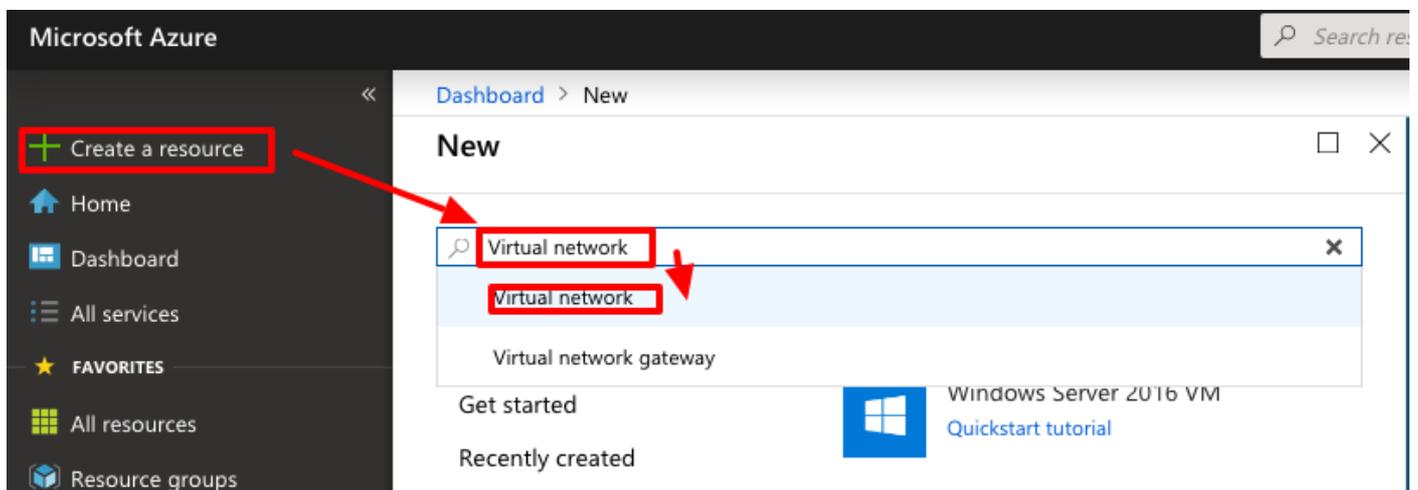
Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konfigurieren

In diesem Leitfaden wird davon ausgegangen, dass die Azure-Cloud nicht konfiguriert wurde. Einige dieser Schritte können übersprungen werden, wenn die Ressourcen bereits eingerichtet sind.

Schritt 1: Konfigurieren Sie ein Netzwerk in Azure.

Dies ist der Netzwerkadressraum, der sich in der Azure-Cloud befindet. Dieser Adressraum muss groß genug sein, um in ihm Subnetzwerke unterzubringen, wie im Bild gezeigt.



Name Ein Name für den in der Cloud gehosteten IP-Adressbereich

Adressraum Der gesamte CIDR-Bereich wird in A gehostet. In diesem Beispiel wird 10.1.0.0/16 verwendet

Subnet Der Name des ersten Subnetzes, da ize innerhalb des virtuellen Netzwerkes e wird, mit dem VMs normalerweise verbunden sind.

Subnet

Z-Adressbereich Ein innerhalb des virtuellen Netzwerkes erstelltes Subnetz

h

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

Schritt 2: Ändern Sie das virtuelle Netzwerk, um ein Gateway-Subnetz zu erstellen.

Navigieren Sie zum **virtuellen Netzwerk**, und fügen Sie ein Gateway-Subnetz hinzu. In diesem Beispiel wird 10.1.1.0/24 verwendet.

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

Schritt 3: Erstellen eines virtuellen Netzwerk-Gateways

Dies ist der VPN-Endpunkt, der in der Cloud gehostet wird. Dies ist das Gerät, mit dem die ASA den IPsec-Tunnel erstellt. Bei diesem Schritt wird auch eine öffentliche IP erstellt, die dem virtuellen Netzwerk-Gateway zugewiesen wird.

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

New

virtual network gat

Virtual network gateway

Get started 

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.