Configure ASA IPsec VTI Connection to Azure

Contents

Introduction
Prerequisites
Requirements
Components Used
Configure
Verify
Troubleshoot

Introduction

This document describes how to configure an Adaptive Security Appliance (ASA) IPsec Virtual Tunnel Interface (VTI) connection to Azure. In ASA 9.8.1, the IPsec VTI feature was extended to utilize IKEv2, however, it still is limited to sVTI IPv4 over IPv4. This configuration guide was produced with the use of the ASA CLI interface and the Azure Portal. The configuration of the Azure portal might also be performed by PowerShell or API. For more information about the Azure configuration methods, refer to the Azure documentation.

Note: Currently, VTI is only supported in single-context, routed mode.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- An ASA connected directly to the Internet with a public static IPv4 address running ASA 9.8.1 or later
- An Azure account

Components Used

This document is not restricted to specific software and hardware versions.

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. If your network is
live, ensure that you understand the potential impact of any command.

**Configure**

This guide assumes that the Azure cloud hasn't been configured, some of these steps can be skipped if the resources are already established.

Step 1. Configure a network within Azure.

This is the network address space that will live in the Azure Cloud. This address space should be large enough in order to accommodate sub-networks within them as shown in the image.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A name for the IP address space hosted in the cloud</td>
<td></td>
</tr>
<tr>
<td>The whole CIDR range hosted in Azure</td>
<td>In this example, 10.1.0.0/16 is used</td>
</tr>
<tr>
<td>The name for the first subnet created within the virtual network to which VMs are usually attached</td>
<td></td>
</tr>
<tr>
<td>A subnet created within the Virtual Network</td>
<td></td>
</tr>
</tbody>
</table>
Step 2. Modify the Virtual Network in order to create a Gateway Subnet.

Navigate to the **Virtual network** and add a gateway subnet. In this example, 10.1.1.0/24 is used.
Step 3. Create a Virtual Network Gateway.

This is the VPN endpoint that is hosted in the cloud. This is the device that the ASA will build the IPsec tunnel with. This step also creates a public IP which is assigned to the Virtual network gateway.