

# FirePOWER Threat Defense 6.2 VPN to Azure (IKEv2)

This document provides a sample configuration for the connection of Cisco FirePOWER Threat Defense (FTD) device to Azure using IKEv2. This example does not use Border Gateway Protocol (BGP).

*Note: IKEv2 on Azure cannot use a Basic Gateway, thus forcing you to use Route-Based VPN. The FTD device creates a Policy-Based VPN. That would ordinarily be an issue, as Policy-Based works off of a Crypto Map, whereas Route-Based does not. This document will show you how to use a Route-Based Azure VPN, and configure a parameter to force Azure to use Policy-Based Traffic Selectors.*

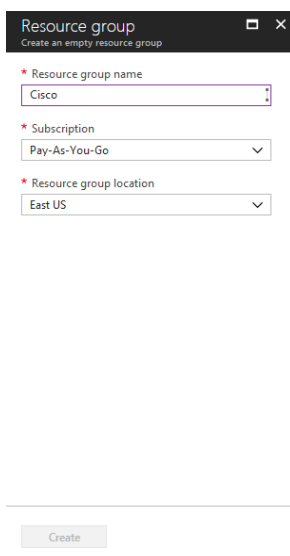
*Note: FirePOWER Management Center (FMC) in Evaluation Mode does not support heavy encryption (AES/3DES) and can only do light encryption (DES). A fully licensed version of the product enables all encryption algorithms.*

**Requirements: Please make sure you have a public IP address to assign to the FTD device.**

## Configure the Azure Environment

I configure the Azure portion first since it takes about 30-45 minutes to receive a public IP address. For all steps, open the respective section and click on the Add button in order to create it new.

1. Create a New Resource Group (For this example I have named mine **Cisco**)



Resource group  
Create an empty resource group

\* Resource group name  
Cisco

\* Subscription  
Pay-As-You-Go

\* Resource group location  
East US

Create

2. Create a new Virtual Network

- a. **Name:** (Example\_VNG) A name of your liking, although something to identify it easily would probably be desired.
- b. **Address Space:** As Desired
  - i. *Please note: this is what would be considered your Protected Networks on the Azure side when you configure the FTD Appliance.*
- c. **Resource Group:** (Cisco) As created in Step 1
- d. **Subnet**
  - i. **Name:** As Desired
  - ii. **Address Range:** Must fit within Address Space (can be smaller subnet)
- e. Click **Create**

Create virtual network

\* Name  
Example\_VNG ✓

\* Address space ⓘ  
10.2.0.0/24 ✓  
10.2.0.0 - 10.2.0.255 (256 addresses)

\* Subscription  
Pay-As-You-Go ▼

\* Resource group  
 Create new  Use existing  
Cisco ▼

\* Location  
East US ▼

Subnet

\* Name  
Example ✓

\* Address range ⓘ  
10.2.0.0/24 ✓  
10.2.0.0 - 10.2.0.255 (256 addresses)

Service endpoints ⓘ  
Disabled Enabled

Pin to dashboard

Create Automation options

3. Create a VPN Gateway (Virtual Network Gateway)
  - a. **Name:** As Desired
  - b. **Gateway Type:** VPN
  - c. **VPN Type:** Route-Based
  - d. **SKU:** Anything but “Basic”
    - i. “VpnGw1” is being used for this example.
  - e. **Virtual Network:** Select the VNet you created in Step 2
  - f. **Location:** East US (eastus) Pick your closest location

Create virtual network gateway... [maximize] [close]

\* Name  
Cisco\_VNG ✓

Gateway type ⓘ  
VPN ExpressRoute

VPN type ⓘ  
Route-based Policy-based

\* SKU ⓘ  
VpnGw1 ▼

Enable active-active mode ⓘ

\* Virtual network ⓘ  
Choose a virtual network >

\* First IP configuration ⓘ  
Create gateway IP configuration... >

Configure BGP ASN

\* Subscription  
Pay-As-You-Go ▼

Resource group ⓘ  
-

\* Location ⓘ  
East US ▼

Pin to dashboard

Create Automation options

Provisioning a virtual network gateway may take up to 45 minutes.

4. Create a Local Network Gateway
  - a. **Name:** As Desired
  - b. **IP Address:** Public IP Address of your local network gateway (Firewall)
    - i. This is the address provided by your ISP that we required in the very beginning.
  - c. **Address Space:** Private/Local Subnet
    - i. Subnet behind the physical on premise device. (NOT Azure Environment)
  - d. **Resource Group:** Cisco (or whichever group you created in Step 1)
  - e. **Location:** East US

Create local network gateway

\* Name  
Cisco\_LNG ✓

\* IP address ⓘ  
111.222.233.244 ✓

Address space ⓘ  
Add additional address range ...

Configure BGP settings

\* Subscription  
Pay-As-You-Go

\* Resource group ⓘ  
 Create new  Use existing  
Cisco

\* Location  
East US

Pin to dashboard

[Create](#) [Automation options](#)

## Azure PowerShell Portion

You have to declare the following variables (VNG, LNG, and IPsec Policy) to leverage inside the single command you need to run, in order to enable the Policy-Based Traffic Selectors (even though we are still in a Route-Based VPN, as created in Step 3).

*NOTE: If you lose your PowerShell connection or you do not commit to completing steps 5-8 immediately, you will lose the variables you declared and will have to start over prior to running the Step 8 command.*

*Note: I am using the fully licensed FMC, therefore, I am going to use AES. If you are using an evaluation license, you must use DES and not AES. You may use the Encryption Algorithms of your liking aside from that limitation*

### 5. Declare your IPsec Policy Variable (\$ipsec)

```
PS Azure:\> $ipsec = New-AzureRmIpsecPolicy -IkeEncryption AES256 -  
IkeIntegrity SHA256 -DhGroup DHGroup24 -IpsecEncryption AES256 -  
IpsecIntegrity SHA256 -PfsGroup PFS24 -SALifeTimeSeconds 3600 -  
SADataSizeKilobytes 1024000000
```

### 6. Declare your VNG (\$vng) Variable

- The name that you will use will be the same VNG you created in Step 3 (Cisco\_VNG in my case). Must be typed EXACTLY as seen in Azure portal.

```
PS Azure:\> $vng = Get-AzureRmVirtualNetworkGateway -Name Cisco_VNG -  
ResourceGroupName Cisco
```

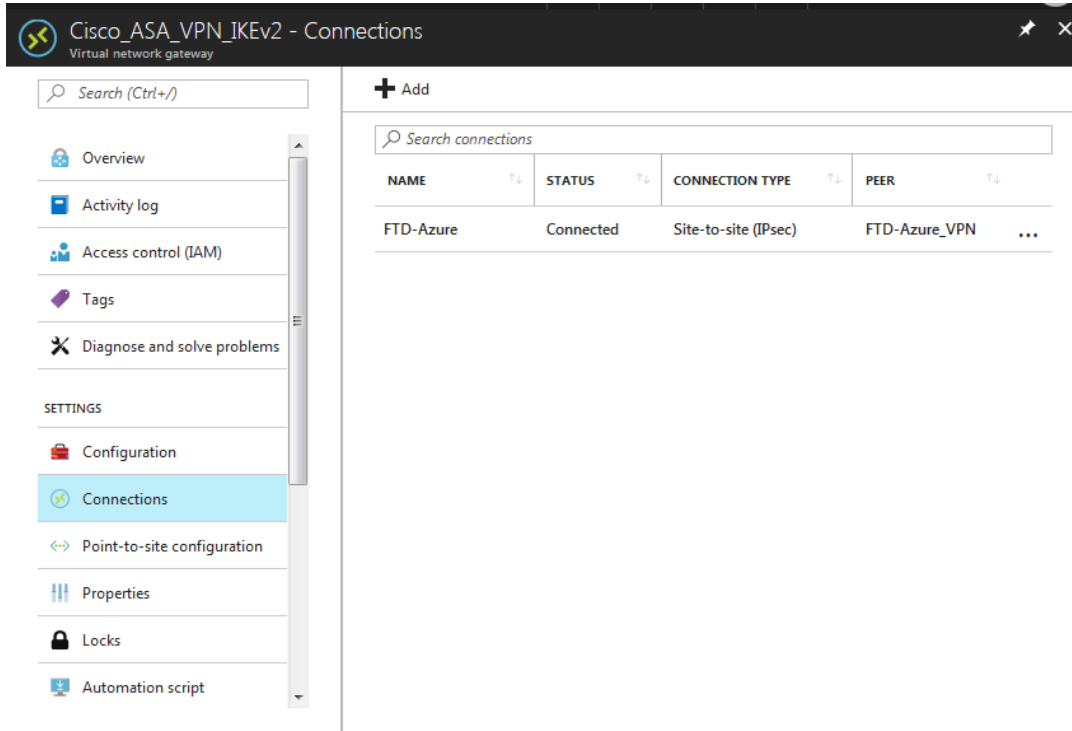
### 7. Declare your LNG (\$lng) Variable

```
PS Azure:\> $lng = Get-AzureRmLocalNetworkGateway -Name Cisco_VNG -  
ResourceGroupName Cisco
```

### 8. Create the VNG Connection

```
PS Azure:\> New-AzureRmVirtualNetworkGatewayConnection -Name (As Desired) -  
ResourceGroupName Cisco -VirtualNetworkGateway1 $vng -LocalNetworkGateway2  
$lng -Location eastus -ConnectionType IPsec -IpsecPolicies $ipsec  
-UsePolicyBasedTrafficSelectors $True -SharedKey 'cisco123'
```

9. Once this command has been completed, you can verify that it created the VNG Connection by clicking on connections on the left hand side under the VNG menu itself.
  - a. It will not say Connected under Status at this point as the VPN will not yet be established



10. Please proceed to the FMC as you are finished with the Azure portion.

## Configure the FTD Device via the FMC

I am assuming that your FTD device is already connected to your FMC at this point. We will only do basic configuration to get the VPN up and running.

11. Enable inside and outside interfaces with IP addressing scheme
  - a. This is where you use the FTD Public IP address from the requirements on the Outside interface.
  - b. The Inside Interface can be any private IP addressing you desire.

FTD5525

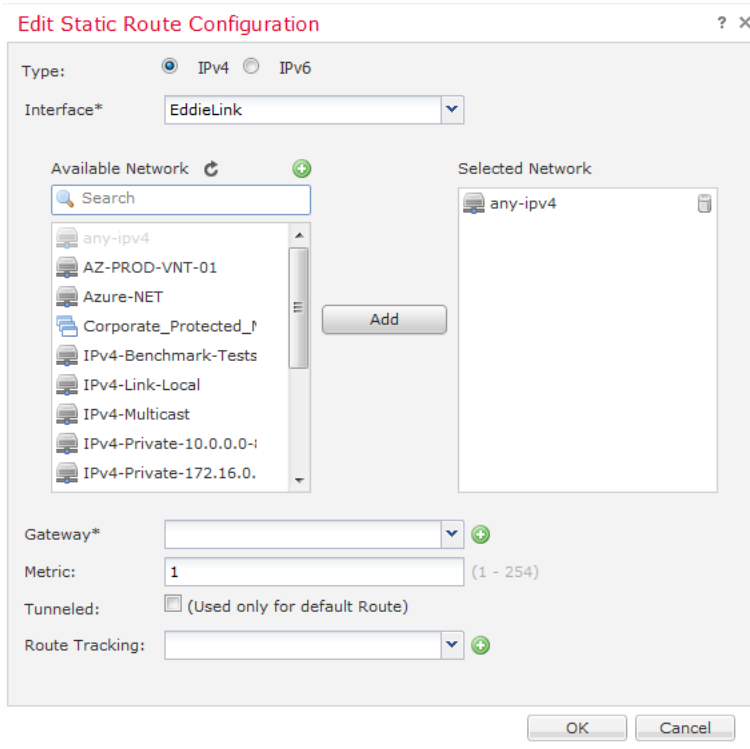
Cisco ASA5525-X Threat Defense

Save Cancel

Status	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
●	GigabitEthernet0/0		Physical			
●	GigabitEthernet0/1	EddieLink	Physical	Outside		FTD Public IP Address
●	GigabitEthernet0/2		Physical			
●	GigabitEthernet0/3		Physical			
●	GigabitEthernet0/4		Physical			
●	GigabitEthernet0/5		Physical			
●	GigabitEthernet0/6		Physical			
●	GigabitEthernet0/7	Corporate	Physical	Inside		FTD Local IP Address
●	Diagnostic0/0	diagnostic	Physical			

12. Create a basic route

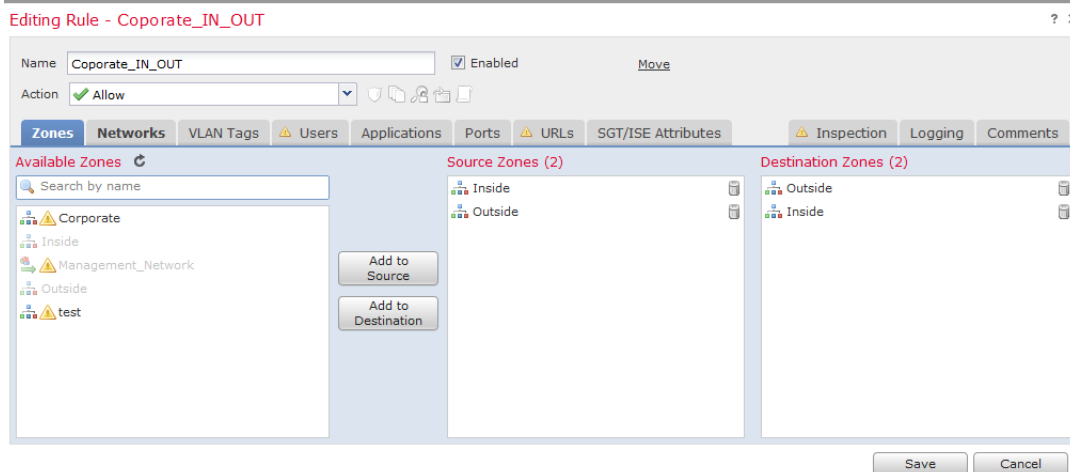
- a. **Interface:** The Outside Interface
- b. **Selected network:** any-ipv4
- c. **Gateway:** Next hop



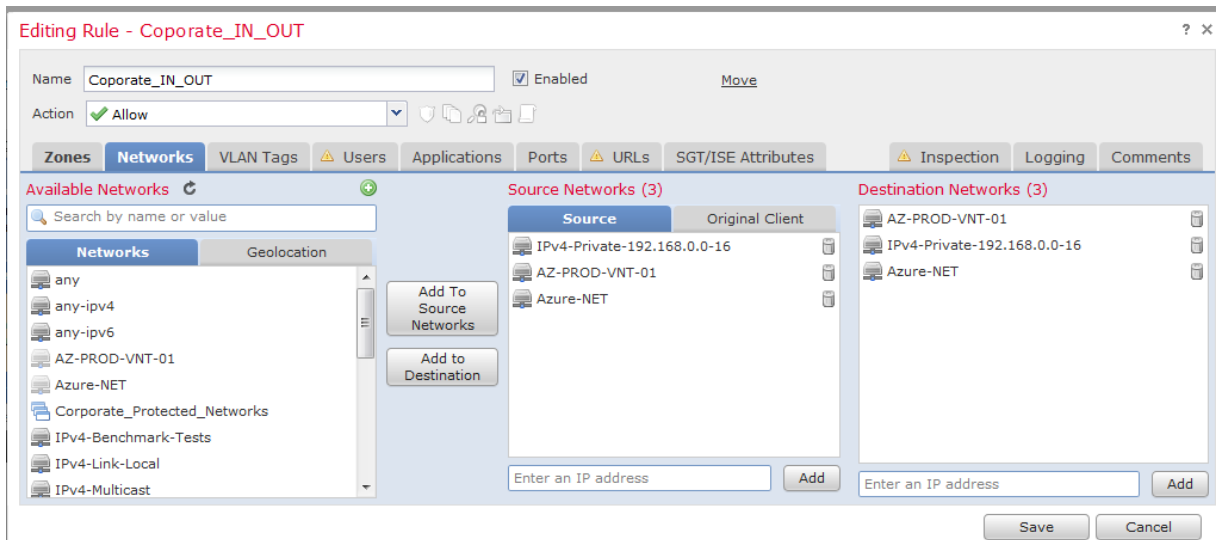
13. Create a "PermitAll" ACL

*Do not judge my typo! 😊 (Coporate)*

- a. **Action:** Allow
- b. **Source Zones:** *Outside* (Do not Add Inside)
- c. **Destinations Zones:** *Inside* (Do not Add Outside)



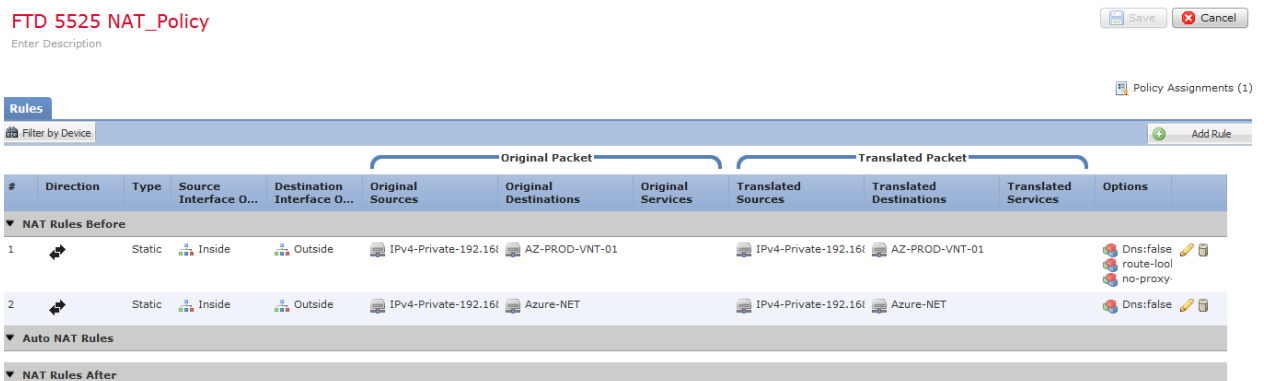
tion



- e. Under Networks:
  - i. Source IP: Azure Address Space
  - ii. Destination IP:
- f. Click 'Save'
  - i. Make sure the policy is assigned to device under Policy Assignments.

14. Create a NAT exemption Rule

- a. **Source Interface:** Inside
- b. **Destination Outside:** Outside
- c. **Original Sources:** Private IP Addresses (Local Environment)
- d. **Original Destinations:** Azure's Virtual Network Address Space, not Range
- e. **Translated Sources:** Private IP Addresses (Local Environment)
- f. **Translated Destinations:** Azure's Virtual Network Address Space, not Range



15. Create a Site-to-Site VPN Connection

- a. Click on **Add VPN -> Firepower Threat Defense Device**
  - i. **Topology Name:** As Desired



- ii. **Network Topology:** Point-to-Point
- iii. **IKE Version:** IKEv2
- b. Click on Plus sign next to Node A
  - i. **Device:** <Choose your FTD Device> (FTD5525 in my case)
  - ii. **Interface:** (Outside FTD Interface)
  - iii. **IP Address:** Public IP address assigned to Outside Interface
  - iv. **Protected Networks:** Local Network on FTD Side
  - v. **Connection Type:** Leave as Bidirectional (You need to play both Initiator & Responder role)

**Add Endpoint** ? x

Device:\* FTD5525

Interface:\* EddieLink

IP Address:\* 66.195.117.9

This IP is Private

Connection Type: Bidirectional

Certificate Map: +

Protected Networks:\* +

OK Cancel

- a. Click on Plus sign next to Node B
  - i. **Device:** Extranet
  - ii. **Device Name:** As Desired
  - iii. **IP Address:** Public IP assigned to Azure VNG (hoping it's been 45 minutes by this point and you have been assigned an IP address)

- iv. **Protected Networks:** Virtual Network Address Space (declared in Step 2)

The screenshot shows a dialog box titled "Add Endpoint". It has a title bar with a question mark and a close button. The dialog contains the following fields:

- Device:\***: A dropdown menu with "Extranet" selected.
- Device Name:\***: An empty text input field.
- IP Address:\***: A text input field containing "Example:10.1.1.1".
- Certificate Map:**: A dropdown menu with a plus sign icon to its right.
- Protected Networks:\***: A large empty text area with a plus sign icon to its right.

At the bottom of the dialog are two buttons: "OK" and "Cancel".

16. Configure IKEv2 Settings

- a. **Policy:** Click on Plus sign
  - i. **Integrity:** AES256
  - ii. **Encryption:** SHA256
  - iii. **PRF Algorithm:** SHA256
  - iv. **Diffie-Hellman Group:** 24
  - v. **Lifetime:** 28800
- b. **Authentication Type:** Pre-Shared Manual Key
- c. **Key:** I used cisco123 (hopefully you use something a little bit more secure)

## Create New VPN Topology

Topology Name:\* AzureVPN

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:\*  IKEv1  IKEv2

Endpoints IKE IPsec Advanced

**IKEv1 Settings**

Policy:\* preshared\_sha\_aes256\_dh5\_5

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:\* 24 Characters (Range 1-127)

**IKEv2 Settings**

Policy:\* AES-GCM-NULL-SHA

Authentication Type: Pre-shared Manual Key

Key:\*

Confirm Key:\*

Enforce hex-based pre-shared key only

### 17. Configure IPsec Settings

- a. **IKEv2 Mode:** Tunnel
- b. **Transform Sets:** Create a new set with AES256/SHA256
- c. **Lifetime Duration:** 3600
- d. **Lifetime Size:** 1024000000
- e. **Perfect Forward Secrecy (PFS) Checkbox:** Check and select the Modulus Group 24 which was specified in your PowerShell '\$ipsec' Policy.

### 18. Deploy configuration out to device

- a. Wait until deployment to device is completed prior to continuing

### 19. While in CLI enter the system support diagnostic-cli command

20. Check both phases by entering the command line interface of your FTD device and running your show commands

21. ISAKMP keepalives not supported by Azure, turn off on FMC.