Configure Policy-Based and Route-Based VPN from ASA and FTD to Microsoft Azure

Contents

Introduction
Concepts
Prerequisites
Requirements
Components Used
Configure
IKEv1
IKEv2 Route-based with VTI on ASA Code 9.8(1) or later
IKEv1 configuration on FTD
IKEv2 Route-based with Policy-based Traffic Selectors
Verify
Phase 1
IKEv2
IKEv1
Phase 2
Troubleshoot
IKEv1
IKEv2

Introduction

This document outlines the concepts and configuration necessary to implement a site to site VPN on Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) Next Generation Firewall to connect to Microsoft Azure Cloud Services.

Concepts

VPN Encryption Domain: The IP addresses range IPSec allows to participate in the VPN tunnel. The encryption domain is defined using a local traffic selector and remote traffic selector to specify what local and remote subnet ranges are captured and encrypted by IPSec. There are two methods to define the VPN's encryption domain: route-based or policy-based traffic selectors.

Route-based: The encryption domain is set to allow any traffic which enters the IPSec tunnel. IPSec Local and remote traffic selectors are set to 0.0.0.0. This means that any traffic routed into the IPSec tunnel is encrypted regardless of the source/destination subnet.

ASA supports route-based VPN with the use of Virtual Tunnel Interfaces (VTIs) in version 9.8 and later.

FTD does not support route-based VPN at the time of writing this document.
**Policy-based:** The encryption domain is set to encrypt only specific IP ranges for both source and destination. Policy-based local traffic selectors and remote traffic selectors identify what traffic to encrypt over IPSec.

ASA supports policy-based VPN with crypto maps in version 8.2 and later.

Microsoft Azure supports route-based, policy-based, or "route-based" with simulated policy-based traffic selectors. Azure currently restricts what IKE(Internet Key Exchange) version you are able to configure based upon the VPN selected method. Route-based requires IKEv2 and policy-based requires IKEv1. This means that if IKEv2 is used, then route-based in Azure must be selected and ASA must use a Virtual Tunnel Interface, but if the ASA only supports crypto maps due to code version, then Azure must be configured for route-based with policy-based traffic selectors. This is accomplished in the Azure portal via PowerShell script deployment to implement an option which Microsoft calls UsePolicyBasedTrafficSelectors as explained here: [https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps)

To summarize from the ASA and FTD configuration perspective:

- For ASA/FTD configured with a crypto map, Azure must be configured for policy-based VPN or route-based with UsePolicyBasedTrafficSelectors.
- For ASA configured with a virtual tunnel interface, Azure must be configured for route-based VPN.
- For FTD we don't currently support virtual tunnel interface (VTI) or Routed Based VPN.

**Prerequisites**

**Requirements**

- For IKEv2 route-based VPN using VTI on ASA: ASA code version 9.8(1) or later. **Azure must be configured for route-based VPN**
- For IKEv1 policy-based VPN using crypto map on ASA and FTD: ASA code version 8.2 or later and FTD 6.2.0 or later. **Azure must be configured for policy-based VPN**
- For IKEv2 route-based VPN using crypto map on ASA with policy-based traffic selectors: ASA code version 8.2 or later configured with a crypto map. **Azure must be configured for route-based VPN with UsePolicyBasedTrafficSelectors.**
- Firepower Management Center (FMC) knowledge for FTD management and configuration.

**Components Used**

- Cisco ASA
- Microsoft Azure
- Cisco Firepower Threat Defense
- Cisco Firepower Management Center

**Configure**

Complete the configuration steps below. Choose either to configure IKEv1, IKEv2 Route Based with VTI, or IKEv2 Route Based w/ Use Policy-Based Traffic Selectors (crypto map on ASA).
IKEv1

For a site to site IKEv1 VPN from ASA to Azure, follow the below ASA configuration. Ensure that you configure a policy-based tunnel in the Azure portal. Crypto maps are used on ASA for this example.

Reference this Cisco document for full IKEv1 on ASA configuration info.

Step 1. Enable IKEv1 on the outside interface.

Cisco-ASA(config)#crypto ikev1 enable outside

Step 2. Create an IKEv1 policy that defines the algorithms/methods to be used for hashing, authentication, Diffie-Hellman group, lifetime, and encryption.

Note: The phase 1 IKEv1 attributes listed below are provided best-effort from this publicly available Microsoft document. For further clarification please reach out to Microsoft Azure support.

Cisco-ASA(config)#crypto ikev1 policy 1
!The 1 in the above command refers to the Policy suite priority (1 highest, 65535 lowest)
Cisco-ASA(config-ikev1-policy)#authentication pre-share
Cisco-ASA(config-ikev1-policy)#encryption aes
Cisco-ASA(config-ikev1-policy)#hash sha
Cisco-ASA(config-ikev1-policy)#group 2
Cisco-ASA(config-ikev1-policy)#lifetime 28800

Step 3. Create a tunnel group under the IPsec attributes and configure the peer IP address and the tunnel pre-shared key.

Cisco-ASA(config)#tunnel-group 192.168.1.1 type ipsec-l2l
Cisco-ASA(config)#tunnel-group 192.168.1.1 ipsec-attributes
Cisco-ASA(config-tunnel-ipsec)#ikev1 pre-shared-key cisco
! Note the IKEv1 keyword at the beginning of the pre-shared-key command.

Step 4. Create an access list that defines the traffic to be encrypted and tunneled. In this example, the traffic of interest is the traffic from the tunnel that is sourced from the 10.2.2.0 subnet to the 10.1.1.0. It can contain multiple entries if there are multiple subnets involved between the sites.

In Versions 8.4 and later, objects or object groups can be created that serve as containers for the networks, subnets, host IP addresses, or multiple objects. Create two objects that have the local and remote subnets and use them for both the crypto Access Control List (ACL) and the NAT statements.

Cisco-ASA(config)#object network 10.2.2.0_24
Cisco-ASA(config-network-object)#subnet 10.2.2.0 255.255.255.0
Cisco-ASA(config)#object network 10.1.1.0_24
Cisco-ASA(config-network-object)#subnet 10.1.1.0 255.255.255.0

Cisco-ASA(config)#access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24
Step 5. Configure the Transform Set (TS), which must involve the keyword IKEv1. An identical TS must be created on the remote end as well.

**Note:** The phase 2 IPSec attributes listed below are provided best-effort from this publicly available Microsoft document. For further clarification please reach out to Microsoft Azure support.

```
Cisco-ASA(config)#crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac
```

Step 6. Configure the crypto map and apply to the outside interface, which has these components:

- The peer IP address
- The defined access list that contains the traffic of interest
- The TS
- The config below does not set PFS since publicly available Azure documentation states that PFS is disabled for IKEv1 in Azure. An optional Perfect Forward Secrecy (PFS) setting, which creates a new pair of Diffie-Hellman keys that are used in order to protect the data (both sides must be PFS-enabled before Phase 2 comes up), can be enabled via use of this config: crypto map outside_map 20 set pfs
- The phase 2 IPSec lifetimes set below are based upon publicly available Azure documentation, for further clarification please contact Microsoft Azure support

```
Cisco-ASA(config)#crypto map outside_map 20 match address 100
Cisco-ASA(config)#crypto map outside_map 20 set peer 192.168.1.1
Cisco-ASA(config)#crypto map outside_map 20 set ikev1 transform-set myset
Cisco-ASA(config)#crypto map outside_map 20 set security-association lifetime seconds 3600
Cisco-ASA(config)#crypto map outside_map 20 set security-association lifetime kilobytes 102400000
Cisco-ASA(config)#crypto map outside_map interface outside
```

Step 7. Ensure that the VPN traffic is not subjected to any other NAT rule. Create a NAT exemption rule:

```
Cisco-ASA(config)#nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static 10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup
```

**Note:** When multiple subnets are used, you must create object groups with all of the source and destination subnets and use them in the NAT rule.

```
Cisco-ASA(config)#object-group network 10.x.x.x_SOURCE
Cisco-ASA(config-network-object-group)#network-object 10.4.4.0 255.255.255.0
Cisco-ASA(config-network-object-group)#network-object 10.2.2.0 255.255.255.0
Cisco-ASA(config)#object network 10.x.x.x_DESTINATION
Cisco-ASA(config-network-object-group)#network-object 10.3.3.0 255.255.255.0
Cisco-ASA(config-network-object-group)#network-object 10.1.1.0 255.255.255.0
Cisco-ASA(config)#nat (inside,outside) 1 source static 10.x.x.x_SOURCE 10.x.x.x_SOURCE destination static 10.x.x.x_DESTINATION 10.x.x.x_DESTINATION no-proxy-arp route-lookup
```

**IKEv2 Route-based with VTI on ASA Code 9.8(1) or later**

For a site to site IKEv2 Route Based VPN on ASA code, follow the configuration below. Ensure
that Azure is configured for route-based VPN and do not configure UsePolicyBasedTrafficSelectors in the Azure portal. A Virtual Tunnel Interface will be configured on ASA.

Reference [this Cisco document](#) for full ASA VTI configuration info.

Step 1. Enable IKEv2 on the outside interface:

```
Cisco-ASA(config)#crypto ikev2 enable outside
```

Step 2. Add an IKEv2 phase 1 policy.

**Note:** Microsoft has published conflicting information regarding the particular IKEv2 phase 1 encryption, integrity, and lifetime attributes used by Azure. The attributes listed below are provided best-effort from [this publicly available Microsoft document](#). Conflicting IKEv2 attribute information from Microsoft is [visible here](#). For further clarification please reach out to Microsoft Azure support.

```
Cisco-ASA(config)#crypto ikev2 policy 1
Cisco-ASA(config-ikev2-policy)#encryption aes
Cisco-ASA(config-ikev2-policy)#integrity sha
Cisco-ASA(config-ikev2-policy)#group 2
Cisco-ASA(config-ikev2-policy)#lifetime seconds 28800
```

Step 3. Add an IKEv2 phase 2 IPsec Proposal. Specify the security parameters in the crypto IPsec ikev2-ipsec-proposal configuration mode:

```
protocol esp encryption {des | 3des | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | null}
protocol esp integrity {md5 | sha-1 | sha-256 | sha-384 | sha-512 | null}
```

**Note:** Microsoft has published conflicting information regarding the particular phase 2 IPsec encryption and integrity attributes used by Azure. The attributes listed below are provided best-effort from [this publicly available Microsoft document](#). Conflicting phase 2 IPsec attribute information from Microsoft is [visible here](#). For further clarification please reach out to Microsoft Azure support.

```
Cisco-ASA(config)#crypto ipsec ikev2 ipsec-proposal SET1
Cisco-ASA(config-ipsec-proposal)#protocol esp encryption aes
Cisco-ASA(config-ipsec-proposal)#protocol esp integrity sha-1
```

Step 4. Add an IPsec profile specifying:

- The previously configured ikev2 phase 2 IPSec proposal
- The phase 2 IPsec lifetime (optional) in seconds and/or kilobytes
- The Perfect Forwarding Secrecy (PFS) group (optional)

**Note:** Microsoft has published conflicting information regarding the particular phase 2 IPsec lifetime and pfs attributes used by Azure. The attributes listed below are provided best-effort from [this publicly available Microsoft document](#). Conflicting phase 2 IPsec attribute information from Microsoft is [visible here](#). For further clarification please reach out to Microsoft Azure support.
Step 5. Create a tunnel group under the IPsec attributes and configure the peer IP address and the IKEv2 local and remote tunnel pre-shared key:

Step 6. Create a Virtual Tunnel Interface specifying:

- a new tunnel interface number: interface tunnel [number]
- a new tunnel interface name: nameif [name]
- a non-existant IP address to exist on the tunnel interface: ip address [ip-address] [mask]
- tunnel source interface where the VPN will terminate locally: tunnel source interface [int-name]
- the Azure gateway IP address: tunnel destination [Azure Public IP]
- IPSec IPv4 mode: tunnel mode ipsec ipv4
- the IPSec profile to use for this VTI: tunnel protection ipsec profile [profile-name]

Step 7. Create a static route to point traffic into the tunnel. To add a static route, enter the following command:
route if_name dest_ip mask gateway_ip [distance]

The dest_ip and mask is the IP address for the destination network in the Azure cloud, for instance 10.0.0.0/24. The gateway_ip needs to be any IP address (existant or non-existant) on the tunnel interface subnet, such as 169.254.0.2. The purpose of this gateway_ip is to point traffic into the tunnel interface, but the particular gateway IP itself is not important.

IKEv1 configuration on FTD

For a site to site IKEv1 VPN from FTD to Azure, we need to have previously registered the FTD device to FMC.

Step 1. Create a Site to Site policy. Go to the FMC dashboard, navigate to "Devices" click on "VPN" and select "Site to Site".
Step 2. Create a new policy. Click on "Add VPN" dropdown menu and select "Firepower Threat Defense device".

Step 3. On the "Create new VPN Topology" window, specify your "Topology Name", check the "IKEV1" protocol checkbox and click on the "IKE" tab. For the purpose of this example, preshared keys is used as authentication method.

Click on the "Authentication Type:" dropdown menu, and select "Pre-shared manual key". Type the manual pre-shared key on the "Key" and "Confirm Key" text fields.
Step 4. Configure the ISAKMP policy or Phase 1 parameters by creating a new one. On the same window, click on the green plus button to add a new ISAKMP policy. Specify the name of the policy and select the desired Encryption, Hash, Diffie-Hellman Group, Lifetime and Authentication Method and click on "Save".
Step 5. Configure the IPsec policy or phase 2 parameters by going to the "IPsec" tab, select "Static" on the "Crypto Map Type" checkbox. Click on the "edit pencil" icon from the "IKEV1 IPsec Proposals" at the "Transform Sets:" option.
Step 6. Create a new IPsec proposal. On the "IKEv1 IPSec Proposal" window, click on the green plus button to add a new one. Specify the name of the policy and it's desired parameters for ESP Encryption and ESP Hash algorithms and click on "Save".
Step 7. On the "IKEV1 IPsec Proposal" window, add your new IPsec policy to the "Selected Transform Sets" section and click "OK".
Step 8. Back on the "IPSec" tab, configure the desired Lifetime Duration and Size.

Step 9. Select the Encryption Domain/Traffic Selectors/Protected Networks by going to the "Endpoints" tab. On the "Node A" section click on the green plus button to add a new one. In this example Node A is used as the local subnets to the FTD.
Step 10. On the “Add Endpoint” window, specify the FTD to use on the “Device” dropdown along with its physical interface and IP address to use.

Step 11. To specify the local traffic selector, go to the “Protected Networks” option and click on the green plus button to create a new object.

Step 12. On the “Network Objects” window, click on the green plus button next to the “Available Networks” text to create a new local traffic selector object.

Step 13. On the "New Network Object" window, specify the name of the object and select accordingly host/network/range/FQDN. Then, click on "Save".
Step 14. Add the object to the "Selected Networks" section on the "Network Objects" window and click "OK". Click "OK" on the "Add Endpoint" window.

Step 15. Define the Node B endpoint, which on this example, it is the Azure endpoint. On the "Create New VPN Topology" window, go to the "Node B" section and click on the green plus button to add the remote endpoint traffic selector. Specify "Extranet" for all VPN peer endpoints that are not managed by the same FMC as Node A. Type the name of the device (locally
significant only) and its IP address.

Step 16. Create the remote traffic selector object. Go to the "Protected Networks" section and click on the green plus button to add a new object.

Step 17. On the "Network Objects" window, click on the green plus button next to the "Available Networks" text to create a new object. On the "New Network Object" window, specify the name of the object and select accordingly host/range/network/FQDN and click on "Save".
Step 18. Back on the "Network Objects" window, add your new remote object to the "Selected Networks" section and click "OK". Click "Ok" on the "Add Endpoint" window.

Step 19. On the "Create New VPN Topology" window you can see now both nodes with their correct traffic selectors/protected networks. Click on "Save".
Step 20. On the FMC dashboard, click on "Deploy" at the top righ pane, select the FTD device and click "Deploy".

Step 21. On the command line interface, VPN configuration will look the same as the one for ASA devices.

**IKEv2 Route-based with Policy-based Traffic Selectors**

For a site to site IKEv2 VPN on ASA with crypto maps, follow the configuration below. Ensure that Azure is configured for route-based VPN *AND* UsePolicyBasedTrafficSelectors must be configured in the Azure portal through the use of PowerShell.

*This document* from Microsoft describes the configuration of UsePolicyBasedTrafficSelectors in conjunction with Route-Based Azure VPN mode. Without this step being completed, ASA with crypto maps fail to establish the connection due to a mismatch in the traffic selectors received from Azure.

Reference *this Cisco document* for full ASA IKEv2 w/ crypto map config information

Step 1. Enable IKEv2 on the outside interface:
Step 2. Add an IKEv2 phase 1 policy.

**Note:** Microsoft has published conflicting information regarding the particular IKEv2 phase 1 encryption, integrity, and lifetime attributes used by Azure. The attributes listed below are provided best-effort from this publicly available Microsoft document. Conflicting IKEv2 attribute information from Microsoft is visible here. For further clarification please reach out to Microsoft Azure support.

```cisco
Cisco-ASA(config)#crypto ikev2 enable outside
```

Step 3. Create a tunnel group under the IPsec attributes and configure the peer IP address and the IKEv2 local and remote tunnel pre-shared key:

```cisco
Cisco-ASA(config)#crypto ikev2 policy 1
Cisco-ASA(config-ikev2-policy)#encryption aes
Cisco-ASA(config-ikev2-policy)#integrity sha
Cisco-ASA(config-ikev2-policy)#group 2
Cisco-ASA(config-ikev2-policy)#lifetime seconds 28800
```

Step 4. Create an access list that defines the traffic to be encrypted and tunneled. In this example, the traffic of interest is the traffic from the tunnel that is sourced from the 10.2.2.0 subnet to the 10.1.1.0. It can contain multiple entries if there are multiple subnets involved between the sites.

In Versions 8.4 and later, objects or object groups can be created that serve as containers for the networks, subnets, host IP addresses, or multiple objects. Create two objects that have the local and remote subnets and use them for both the crypto Access Control List (ACL) and the NAT statements.

```cisco
Cisco-ASA(config)#object network 10.2.2.0_24
Cisco-ASA(config-network-object)#subnet 10.2.2.0 255.255.255.0
Cisco-ASA(config)#object network 10.1.1.0_24
Cisco-ASA(config-network-object)#subnet 10.1.1.0 255.255.255.0
Cisco-ASA(config)#access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24
```

Step 5. Add an IKEv2 phase 2 IPsec Proposal. Specify the security parameters in the crypto IPsec ikev2 ipsec-proposal configuration mode:

```cisco
protocol esp encryption {des | 3des | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | null}
protocol esp integrity {md5 | sha-1 | sha-256 | sha-384 | sha-512 | null}
```

**Note:** Microsoft has published conflicting information regarding the particular phase 2 IPSec encryption and integrity attributes used by Azure. The attributes listed below are provided best-effort from this publicly available Microsoft document. Conflicting phase 2 IPSec attribute
information from Microsoft is visible here. For further clarification please reach out to Microsoft Azure support.

Cisco-ASA(config)#crypto ipsec ikev2 ipsec-proposal SET1
Cisco-ASA(config-ipsec-proposal)#protocol esp encryption aes
Cisco-ASA(config-ipsec-proposal)#protocol esp integrity sha-1

Step 6. Configure a crypto map and apply to the outside interface, which contains these components:

• The peer IP address
• The defined access list that contains the traffic of interest
• The IKEv2 phase 2 IPSec Proposal
• The phase 2 IPSec lifetime in seconds
• An optional Perfect Forward Secrecy (PFS) setting, which creates a new pair of Diffie-Hellman keys that are used in order to protect the data (both sides must be PFS-enabled before Phase 2 comes up)

Note: Microsoft has published conflicting information regarding the particular phase 2 IPSec lifetime and PFS attributes used by Azure. The attributes listed below are provided best-effort from this publicly available Microsoft document. Conflicting phase 2 IPSec attribute information from Microsoft is visible here. For further clarification please reach out to Microsoft Azure support.

Cisco-ASA(config)#crypto map outside_map 20 match address 100
Cisco-ASA(config)#crypto map outside_map 20 set peer 192.168.1.1
Cisco-ASA(config)#crypto map outside_map 20 set ikev2 ipsec-proposal myset
Cisco-ASA(config)#crypto map outside_map 20 set security-association lifetime seconds 27000
Cisco-ASA(config)#crypto map outside_map 20 set security-association lifetime kilobytes unlimited
Cisco-ASA(config)#crypto map outside_map 20 set pfs none
Cisco-ASA(config)#crypto map outside_map interface outside

Step 8. Ensure that the VPN traffic is not subjected to any other NAT rule. Create a NAT exemption rule:

Cisco-ASA(config)#nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static 10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup

Note: When multiple subnets are used, you must create object groups with all of the source and destination subnets and use them in the NAT rule.

Cisco-ASA(config)#object-group network 10.x.x.x_SOURCE
Cisco-ASA(config-network-object-group)#network-object 10.4.4.0 255.255.255.0
Cisco-ASA(config-network-object-group)#network-object 10.2.2.0 255.255.255.0

Cisco-ASA(config)#object-group network 10.x.x.x_DESTINATION
Cisco-ASA(config-network-object-group)#network-object 10.3.3.0 255.255.255.0
Cisco-ASA(config-network-object-group)#network-object 10.1.1.0 255.255.255.0

Cisco-ASA(config)#nat (inside,outside) 1 source static 10.x.x.x_SOURCE 10.x.x.x_SOURCE destination static 10.x.x.x_DESTINATION 10.x.x.x_DESTINATION no-proxy-arp route-lookup
Verify

After completing the configuration on both ASA and the Azure gateway, Azure initiates the VPN tunnel. You can verify that the tunnel builds correctly with the following commands.

**Phase 1**

Verify the phase 1 security association has built with the following command:

**IKEv2**

Below, an IKEv2 SA built from local outside interface IP 192.168.1.2 on UDP port 500, to the remote destination IP 192.168.2.2 is shown. There is also a valid child SA built for encrypted traffic to flow over.

Cisco-ASA# show crypto ikev2 sa

IKEv2 SAs:

Session-id:44615, Status:UP-ACTIVE, IKE count:1, CHILD count:1

<table>
<thead>
<tr>
<th>Tunnel-id Local</th>
<th>Status</th>
<th>Role</th>
<th>Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>3208253</td>
<td>READY</td>
<td>INITIATOR</td>
<td>192.168.2.2/500</td>
</tr>
<tr>
<td>Life/Active Time: 86400/142 sec</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*-->Child sa: local selector 192.168.0.0/0 - 192.168.0.255/65535
remote selector 192.168.3.0/0 - 192.168.3.255/65535
ESP spi in/out: 0x9b60edc5/0x8e7a2e12

**IKEv1**

Below, an IKEv1 SA built with ASA as the initiator to peer IP 192.168.2.2 with a remaining lifetime of 86388 seconds is shown.

Cisco-ASA# sh crypto ikev1 sa detail

IKEv1 SAs:

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 192.168.2.2
   Type : L2L  Role : initiator
   Rekey : no  State : MM_ACTIVE
   Encrypt : aes  Hash : SHA
   Auth : preshared  Lifetime: 86400
   Lifetime Remaining: 86388

**Phase 2**

Verify the phase 2 IPSec security association has built with: show crypto ipsec sa peer [peer-ip]
Cisco-ASA# show crypto ipsec sa peer 192.168.2.2
peer address: 192.168.2.2
Crypto map tag: outside, seq num: 10, local addr: 192.168.1.2

access-list VPN extended permit ip 192.168.0.0 255.255.255.0 192.168.3.0 255.255.255.0
local ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
current_peer: 192.168.2.2

#pkts ecaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.1.2/500, remote crypto endpt.: 192.168.2.2/500
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 8E7A2E12
current inbound spi : 9B60EDC5

inbound esp sas:
spi: 0x9B60EDC5 (2606820805)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 182743040, crypto-map: outside
sa timing: remaining key lifetime (kB/sec): (4193279/28522)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000001F

outbound esp sas:
spi: 0x8E7A2E12 (2390371858)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 182743040, crypto-map: outside
sa timing: remaining key lifetime (kB/sec): (3962879/28522)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

4 packets are sent and 4 are received over the IPSec SA with no errors. One inbound SA with SPI 0x9B60EDC5 and one outbound SA with SPI 0x8E7A2E12 are installed as expected.

You can also verify that data is being passed over the tunnel by checking the vpn-sessiondb l2l entries:

Cisco-ASA#show vpn-sessiondb l2l

Session Type: LAN-to-LAN
Bytes Tx: and Bytes Rx: show sent and received data counters over the IPSec SA.

Troubleshoot

Step 1. Verify interesting traffic for the VPN is being received by ASA on the inside interface destined for Azure’s private network. For testing, you can configure a continuous ping from an inside client and configure a packet capture on ASA to verify it is received:

   capture [cap-name] interface [if-name] match [protocol] [src-ip] [src-mask] [dest-ip] [dest-mask]

   show capture [cap-name]

Cisco-ASA#capture inside interface inside match ip host [local-host] host [remote-host]
Cisco-ASA#show capture inside

2 packets captured

   1: 18:50:42.835863       192.168.0.2 > 192.168.3.2: icmp: echo request
   2: 18:50:42.839128       192.168.3.2 > 192.168.0.2: icmp: echo reply

2 packets shown

If reply traffic from Azure is seen, then the VPN is properly built and sending/receiving traffic.

If source traffic is missing, verify that your sender is properly routing to the ASA.

If source traffic is seen but reply traffic from Azure is missing, continue on to verify why.

Step 2. Verify that the interesting traffic received on ASA inside interface is properly processed by ASA and routed into the VPN:

   To simulate an ICMP echo request:

   Full packet-tracer usage guidelines can be found here:

Cisco-ASA# packet-tracer input inside icmp 192.168.0.2 8 0 192.168.3.2 detail

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
   Forward Flow based lookup yields rule:
in id=0x7f6c19af0a0, priority=13, domain=capture, deny=false
  hits=3, user_data=0x7f6c19af9b0, cs_id=0x0, l3_type=0x0
  src mac=0000.0000.0000, mask=0000.0000.0000
  dst mac=0000.0000.0000, mask=0000.0000.0000
  input_ifc=inside, output_ifc=any

Phase: 2
Type: ACCESS-LIST
Subtype:
  Result: ALLOW
  Config: Implicit Rule
  Additional Information:
  Forward Flow based lookup yields rule:
  in id=0x7f6c195971f0, priority=1, domain=permit, deny=false
    hits=32, user_data=0x0, l3_type=0x8
    src mac=0000.0000.0000, mask=0100.0000.0000
    dst mac=0000.0000.0000, mask=0100.0000.0000
    input_ifc=inside, output_ifc=any

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 192.168.1.1 using egress ifc outside

Phase: 4
Type: NAT
Subtype: per-session
  Result: ALLOW
  Config:
  Additional Information:
  Forward Flow based lookup yields rule:
  in id=0x7f6c19250290, priority=0, domain=nat-per-session, deny=true
    hits=41, user_data=0x0, reverse, use_real_addr, flags=0x0, protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
    input_ifc=any, output_ifc=any

Phase: 5
Type: IP-OPTIONS
Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Forward Flow based lookup yields rule:
  in id=0x7f6c1987c120, priority=0, domain=inspect-ip-options, deny=true
    hits=26, user_data=0x0, reverse, flags=0x0, protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
    input_ifc=inside, output_ifc=any

Phase: 6
Type: QOS
Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Forward Flow based lookup yields rule:
  in id=0x7f6c19a60280, priority=70, domain=qos-per-class, deny=false
    hits=30, user_data=0x7f6c19a5c030, reverse, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 7
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7f6c1983ab50, priority=66, domain=inspect-icmp-error, deny=false
  hits=27, user_data=0x7f6c1987afc0, cs_id=0x0, use_real_addr, flags=0x0, protocol=1
  src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, tag=any, dscp=0x0
  input_ifc=inside, output_ifc=any

Phase: 8
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
out id=0x7f6c19afe1a0, priority=70, domain=encrypt, deny=false
  hits=2, user_data=0x13134, cs_id=0x7f6c19349670, reverse, flags=0x0, protocol=0
  src ip/id=192.168.0.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=192.168.3.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
  input_ifc=any, output_ifc=outside

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 43, packet dispatched to next module
Module information for forward flow ...
snp_fp_tracer_drop
snp_fp.inspect_ip_options
snp_fp.inspect_icmp
snp_fp.adjacency
snp_fp.encrypt
snp_fp.fragment
snp_ifc.stat

Module information for reverse flow ...

Result:
input-interface: inside
input-line-status: up
output-interface: outside
output-line-status: up
Action: allow

Note in the output above that NAT is seen exempting traffic (no translation takes effect). Verify no NAT translation is occurring on the interesting traffic.

Also verify the "output-interface:" is correct--it should be either the physical interface where crypto map is applied or it should be the virtual tunnel interface.
Ensure that there are no access list drops seen.

If VPN phase shows ENCRYPT: ALLOW, the tunnel is already built and you should see IPSec SA installed with encaps.

Step 2.1 If ENCRYPT:ALLOW seen in packet-tracer above

Verify IPsec SA is installed and encrypting traffic using "show crypto ipsec sa"

Perform a capture on outside interface to verify that encrypted packets are being sent from ASA and encrypted responses are received from Azure

Step 2.1 If ENCRYPT:DROP seen in packet-tracer above

VPN tunnel is not yet established but should be in negotiation. This is an expected condition when first bringing the tunnel up. Run debugs to view the tunnel negotiation process and identify where and if a failure is occurring:

First, verify the correct version of ike is being triggered and that the ike-common process shows no relevant errors:

Cisco-ASA#debug crypto ike-common 255

If no ike-common debug output is seen when interesting traffic is initiated, this means traffic is being dropped before reaching the crypto process or crypto ikev1/ikev2 is not enabled on the box. Double check the crypto config and packet drops

If ike-common debug shows the crypto process is being triggered, debug the IKE configured version to view tunnel negotiation messages and identify where the failure occurs in tunnel-building with Azure:

**IKEv1**

Full [ikev1 debug procedure and analysis is here](#).

Cisco-ASA#debug crypto ikev1 127
Cisco-ASA#debug crypto ipsec 127

**IKEv2**

Full [ikev2 debug procedure and analysis is here](#).

Cisco-ASA#debug crypto ikev2 platform 127
Cisco-ASA#debug crypto ikev2 protocol 127
Cisco-ASA#debug crypto ipsec 127