

Configure IKEv2 IPv6 Site-to-Site Tunnel Between ASA and FTD

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[ASA Configuration](#)

[FTD Configuration](#)

[Bypass Access Control](#)

[Configure NAT Exemption](#)

[Verify](#)

[Troubleshoot](#)

[References](#)

Introduction

This document provides a configuration example to set up an IPv6 site to site tunnel between an ASA (Adaptive Security Appliance) and FTD (Firepower Threat Defense) using Internet Key Exchange version 2 (IKEv2) protocol. The setup includes end to end IPv6 network connectivity with ASA and FTD as VPN terminating devices.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics :

- Fundamental knowledge of ASA CLI configuration
- Fundamental knowledge of IKEv2 and IPSEC protocols
- Understanding of IPv6 addressing and routing
- Basic understanding of FTD configuration via FMC

Components Used

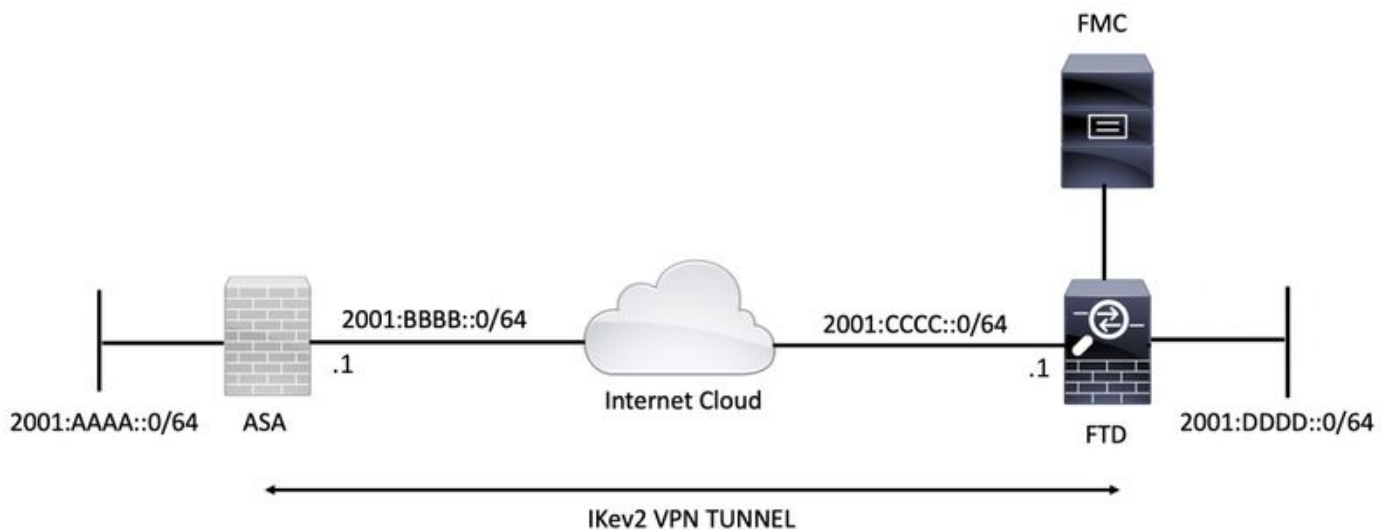
The information in this document is based on a virtual environment, created from devices in a specific lab setup. All of the devices used in this document started with a cleared (default) configuration. If your network is in production, make sure that you understand the potential impact of any command.

The information in this document is based on these software and hardware versions:

- Cisco ASA running 9.6.(4)12
- Cisco FTD running 6.5.0
- Cisco FMC running 6.6.0

Configure

Network Diagram



ASA Configuration

This section describes the configuration required on the ASA.

Step 1. Configure the ASA interfaces.

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ipv6 address 2001:bbbb::1/64
ipv6 enable
```

```
interface GigabitEthernet0/1
nameif inside
security-level 100
ipv6 address 2001:aaaa::1/64
ipv6 enable
```

Step 2. Set an IPv6 default route.

```
ipv6 route outside ::/0 2001:bbbb::2
```

Step 3. Configure the IKEv2 Policy and enable IKEv2 on the outside interface.

```
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 14
prf sha256
lifetime seconds 86400
```

```
crypto ikev2 enable outside
```

Step 4. Configure the Tunnel Group.

```
tunnel-group 2001:cccc::1 type ipsec-l2l
tunnel-group 2001:cccc::1 ipsec-attributes
ikev2 remote-authentication pre-shared-key cisco123
ikev2 local-authentication pre-shared-key cisco123
```

Step 5. Create the objects and the Access Control List (ACL) to match the interesting traffic.

```
object-group network local-network
network-object 2001:aaaa::/64
```

```
object-group network remote-network
network-object 2001:dddd::/64
```

```
access-list CRYPTO_ACL extended permit ip object-group local-network object-group remote-network
```

Step 6. Configure the identity Network Address Translation (NAT) rules for the interesting traffic.

```
nat (inside,outside) source static local-network local-network destination static remote-network
remote-network no-proxy-arp route-lookup
```

Step 7. Configure the IKEv2 IPsec Proposal.

```
crypto ipsec ikev2 ipsec-proposal ikev2_aes256
protocol esp encryption aes-256
protocol esp integrity sha-1
```

Step 8. Set the Crypto Map and apply it to the outside interface.

```
crypto map VPN 1 match address CRYPTO_ACL
crypto map VPN 1 set peer 2001:cccc::1
crypto map VPN 1 set ikev2 ipsec-proposal ikev2_aes256
crypto map VPN 1 set reverse-route
```

```
crypto map VPN interface outside
```

FTD Configuration

This section provides instructions to configure an FTD using FMC.

Define the VPN Topology

Step 1. Navigate to **Devices > VPN > Site To Site**.

Select 'Add VPN' and choose 'Firepower Threat Defense Device', as shown in this image.

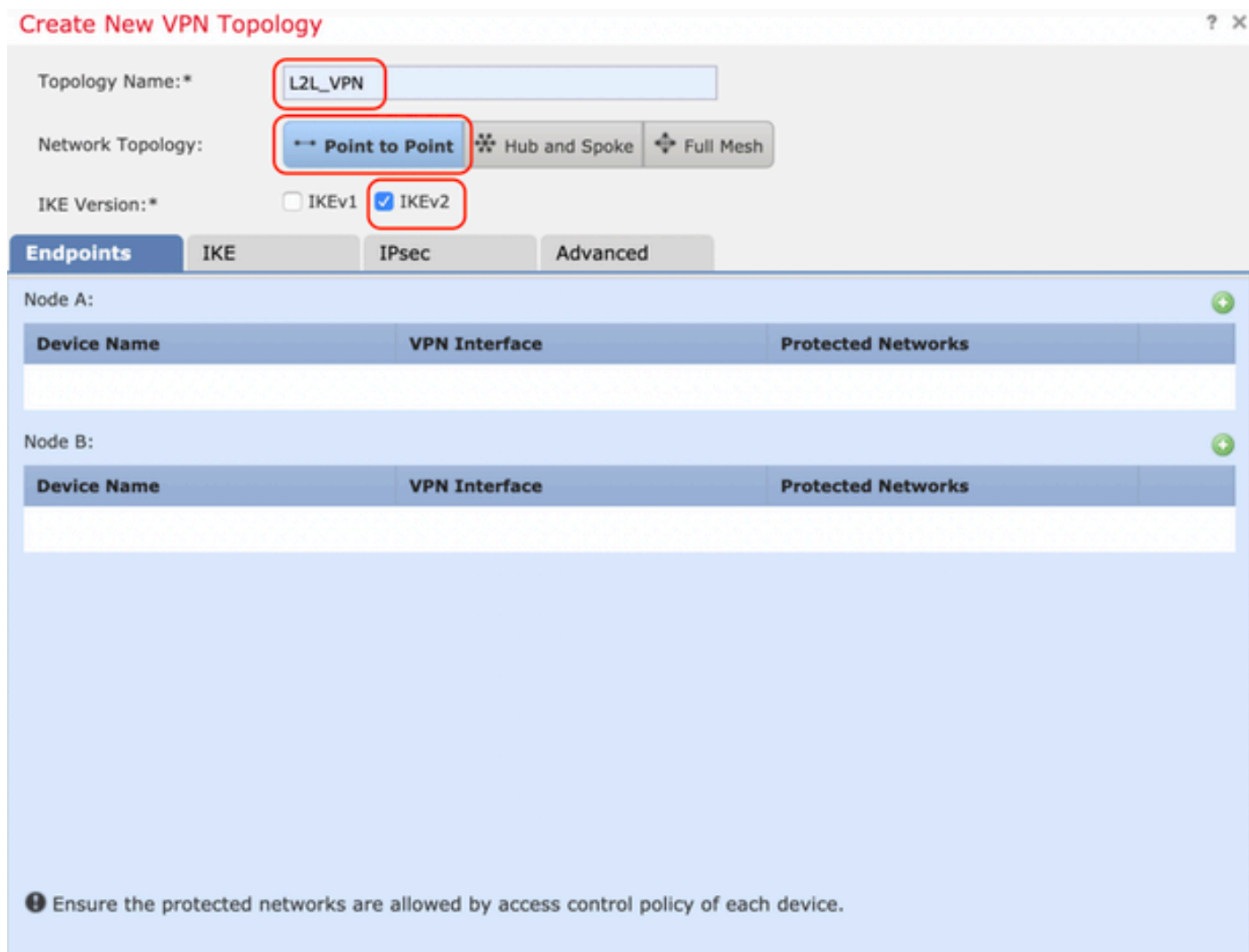


Step 2. 'Create New VPN Topology' box appears. Give the VPN an easily identifiable name.

Network Topology: Point to Point

IKE Version: IKEv2

In this example, when selecting endpoints Node A is the FTD. Node B is the ASA. Click on the green plus button to add devices to the topology.



Step 3. Add the FTD as the first endpoint.

Choose the interface where the crypto map is applied. The IP address should auto-populate from the device configuration.

Click the green plus icon under Protected Networks to select subnets that are encrypted via this VPN tunnel. In this example, 'Local Proxy' network object on FMC comprises of IPv6 subnet '2001:DDDD::/64'.

Edit Endpoint

? X

Device:*

FTDv

Interface:*

OUTSIDE

IP Address:*

2001:CCCC::1

This IP is Private

Connection Type:

Bidirectional

Certificate Map:

Protected Networks:*

Subnet / IP Address (Network) Access List (Extended)



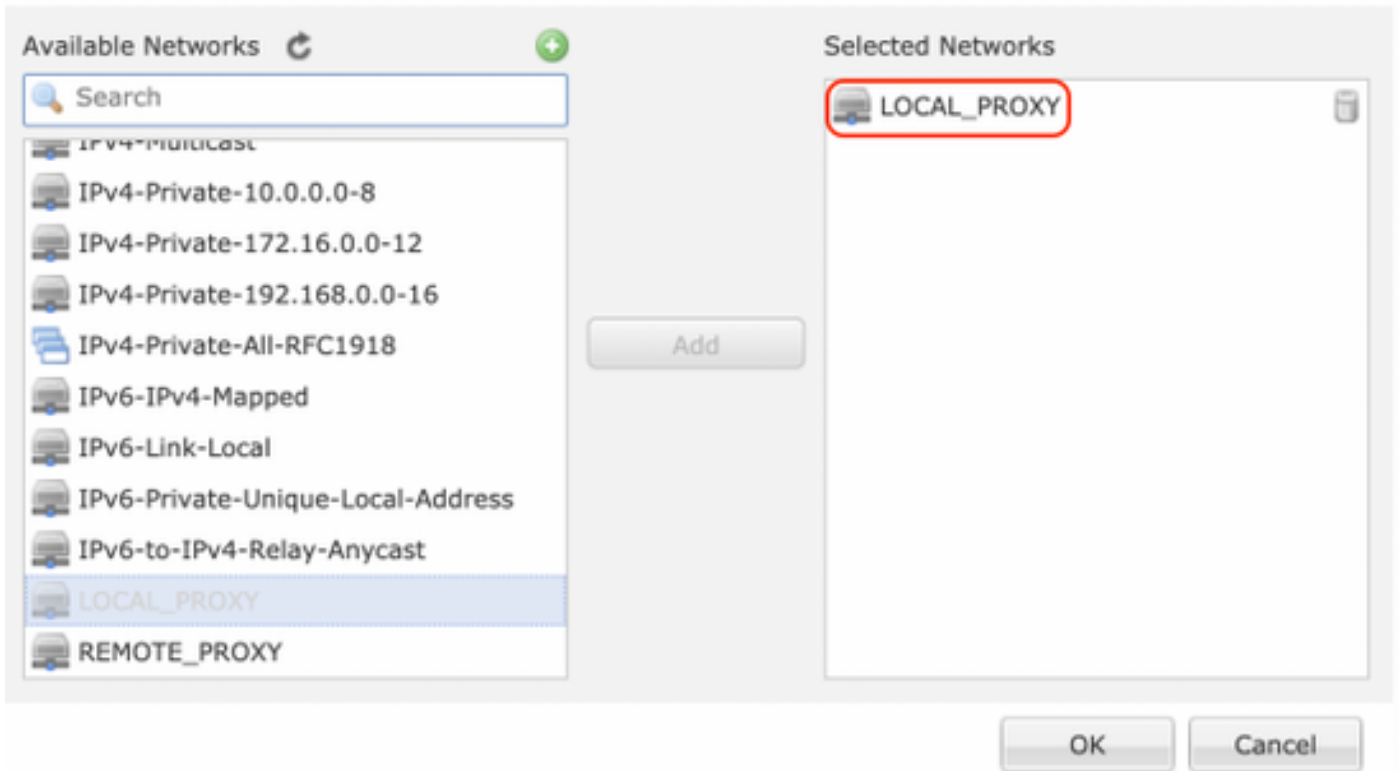
LOCAL_PROXY



OK

Cancel

Network Objects



With the above step, the FTD endpoint configuration is complete.

Step 4. Click the green plus icon for Node B which is an ASA in the configuration example. Devices that are not managed by the FMC are considered Extranet. Add a device name and IP address.

Step 5. Select the green plus icon to add protected networks.

Edit Endpoint ? X

Device:* Extranet

Device Name:* ASA

IP Address:* Static Dynamic
2001:BBBB::1

Certificate Map: +

Protected Networks:*
 Subnet / IP Address (Network) Access List (Extended)

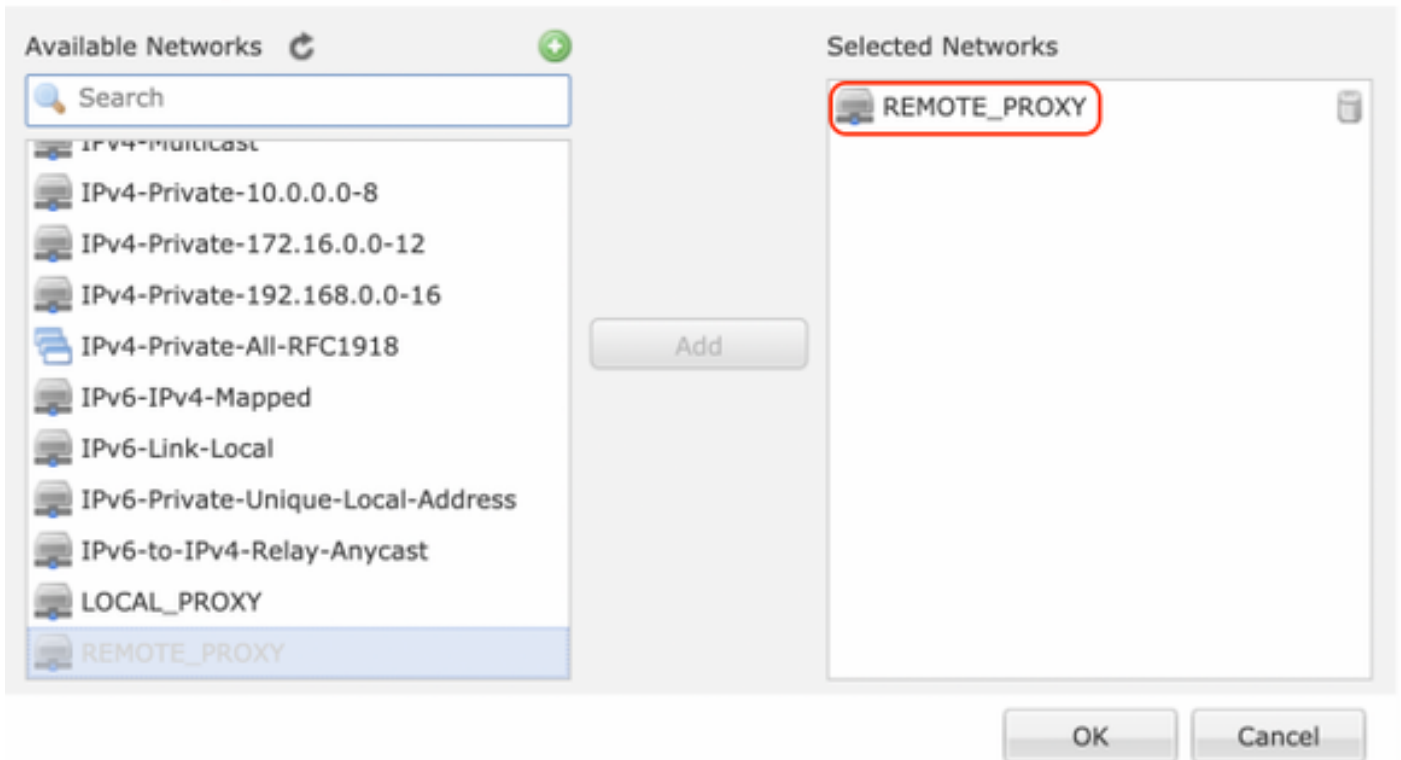
REMOTE_PROXY

OK Cancel

Step 6. Select the ASA subnets that need to be encrypted and add them to the selected networks.

'Remote Proxy' is the ASA subnet '2001:AAAA::/64' in this example.

Network Objects



Configure IKE Parameters

Step 1. Under the IKE tab, specify the parameters to use for the IKEv2 initial exchange. Click the green plus icon to create a new IKE policy.

Edit VPN Topology



Topology Name:* L2L_VPN

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:* preshared_sha_aes256_dh14_3

Authentication Type: Pre-shared Automatic Key

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

IKEv2 Settings

Policy:* Ikev2_Policy

Authentication Type: Pre-shared Manual Key

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

Save Cancel

Step 2. In the new IKE policy, specify a priority number as well as the lifetime of phase 1 of the connection. This guide uses these parameters for the initial exchange:

Integrity (SHA256),
Encryption (AES-256),
PRF (SHA256), and
Diffie-Hellman Group (Group 14).

All IKE policies on the device will be sent to the remote peer regardless of what is in the selected policy section. The first one the remote peer matches will be selected for the VPN connection.

[Optional] Choose which policy is sent first using the priority field. Priority 1 is sent first.

Edit IKEv2 Policy

Name:*

Ikev2_Policy

Description:

Priority:

(1-65535)

Lifetime:

86400

seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

- MD5
- SHA
- SHA512
- SHA256
- SHA384
- NULL

Add

Selected Algorithms

SHA256

Save

Cancel

Edit IKEv2 Policy



Name:*

Description:

Priority: (1-65535)

Lifetime: seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

- AES
- AES-256
- DES
- 3DES
- AES-192
- AES-GCM
- AES-GCM-192
- AES-GCM-256
- NULL

Add

Selected Algorithms

- AES-256

Save

Cancel

Edit IKEv2 Policy



Name:*

Description:

Priority: (1-65535)

Lifetime: seconds (120-2147483647)

- Integrity Algorithms
- Encryption Algorithms
- PRF Algorithms**
- Diffie-Hellman Group

Available Algorithms

- MDS
- SHA
- SHA512
- SHA256
- SHA384

Add

Selected Algorithms

- SHA256

Save

Cancel

Edit IKEv2 Policy



Name:*

Description:

Priority:

Lifetime: seconds (120-2147483647)

Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group

Available Groups

- 1
- 2
- 5
- 14
- 15
- 16
- 19
- 20
- 21

Selected Groups

- 14

Add

Save Cancel

Step 3. Once the parameters have been added, select the above-configured policy, and choose the authentication type.

Select the Pre-shared Manual Key option. For this guide, the pre-shared key '**cisco123**' is used.

Edit VPN Topology



Topology Name:*

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:*

Authentication Type:

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

IKEv2 Settings

Policy:*

Authentication Type:

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

Configure IPSEC Parameters

Step 1. Move to the IPsec tab and create a new IPsec Proposal by clicking the pencil icon to edit the transform set.

Edit VPN Topology

? X

Topology Name:*

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints | IKE | **IPsec** | Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode:

Transform Sets:

IKEv1 IPsec Proposals	IKEv2 IPsec Proposals*
tunnel_aes256_sha	Ikev2__IPSec_Proposal

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

Modulus Group:

Lifetime Duration*: Seconds (Range 120-2147483647)

Lifetime Size: Kbytes (Range 10-2147483647)

— **ESPv3 Settings**

Save Cancel

Step 2. Create a new IKEv2 IPsec Proposal by selecting the green plus icon and input the phase 2 parameters as shown below:

ESP Hash: SHA-1

ESP Encryption : AES-256

Edit IKEv2 IPsec Proposal



Name:*

Ikev2__IPSec_Proposal

Description:

ESP Hash

ESP Encryption

Available Algorithms

- SHA-512
- SHA-384
- SHA-256
- SHA-1
- MD5
- NULL

Selected Algorithms

SHA-1

Add

Save

Cancel

Edit IKEv2 IPsec Proposal



Name:*

Description:

ESP Hash

ESP Encryption

Available Algorithms

- AES-GCM-256
- AES-256
- AES-GCM-192
- AES-192
- AES-GCM
- AES
- 3DES
- DES
- AES-GMAC-256

Add

Selected Algorithms

- AES-256**

Save **Cancel**

Step 3. Once the new IPsec proposal has been created, add it to the selected transform sets.

IKEv2 IPsec Proposal



Available Transform Sets

- AES-GCM
- AES-SHA
- DES_SHA-1
- Ikev2__IPSec_Proposal**

Add

Selected Transform Sets

- Ikev2__IPSec_Proposal**

OK **Cancel**

Step 4. The newly selected IPsec proposal is now listed under the IKEv2 IPsec Proposals.

If needed, the phase 2 lifetime and PFS can be edited here. For this example, the lifetime is set as default and PFS disabled.

Edit VPN Topology ? X

Topology Name:* L2L_VPN

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints IKE **IPsec** Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

tunnel_aes256_sha Ikev2_IPSec_Proposal

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

Modulus Group:

Lifetime Duration*: 28800 Seconds (Range 120-2147483647)

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

ESPv3 Settings

Save Cancel

You must either configure the below steps to Bypass Access Control or Create Access Control Policy rules to allow VPN subnets through FTD.

Bypass Access Control

If `sysopt permit-vpn` is not enabled then an access control policy must be created to allow the VPN traffic through the FTD device. If `sysopt permit-vpn` is enabled skip creating an access control policy. This configuration example uses the "Bypass Access Control" option.

The parameter `sysopt permit-vpn` can be enabled under the Advanced > Tunnel.

Caution: This option removes the possibility to use the Access Control Policy to inspect traffic coming from the users. VPN filters or downloadable ACLs can still be used to filter user traffic. This is a global command and applies to all VPNs if this checkbox is enabled.

Edit VPN Topology



Topology Name:*

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints IKE IPsec **Advanced**

IKE
IPsec
Tunnel

NAT Settings

Keepalive Messages Traversal
Interval: Seconds (Range 10 - 3600)

Access Control for VPN Traffic

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Certificate Map Settings

Use the certificate map configured in the Endpoints to determine the tunnel

Use the certificate OU field to determine the tunnel

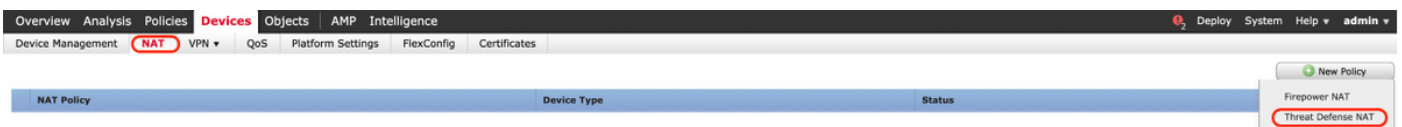
Use the IKE identity to determine the tunnel

Use the peer IP address to determine the tunnel

Configure NAT Exemption

Configure a NAT Exemption statement for the VPN traffic. NAT exemption must be in place to prevent VPN traffic from matching another NAT statement and incorrectly translating VPN traffic.

Step 1. Navigate to **Devices > NAT** and create a new policy by clicking **New Policy > Threat Defense NAT**.



New Policy



Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

FTDv

Selected Devices

FTDv

Step 2. Click on **Add Rule**.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

NAT_Exempt

Enter Description

Policy Assignments (1)

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
▼ NAT Rules Before											
▼ Auto NAT Rules											
▼ NAT Rules After											

Step 3. Create a new Static Manual NAT Rule.

Reference the inside and outside interfaces for the NAT rule. Specifying the interfaces at Interface Objects tab prevents these rules to affect traffic from other interfaces.

Navigate to the Translation tab and select the source and destination subnets. As this is a NAT exemption rule, ensure the original source/destination and the translated source/destination are the same.

Add NAT Rule

? X

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects: **Translation** PAT Pool Advanced

Original Packet

Original Source:* +

Original Destination: +

Original Source Port: +

Original Destination Port: +

Translated Packet

Translated Source: +

Translated Destination: +

Translated Source Port: +

Translated Destination Port: +

Click the Advanced tab and enabled **no-proxy-arp** and **route-lookup**.

Add NAT Rule

? X

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects: Translation **Advanced** PAT Pool

Translate DNS replies that match this rule

Fallthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Unidirectional

Save this rule and confirm the final NAT statement in the NAT list.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

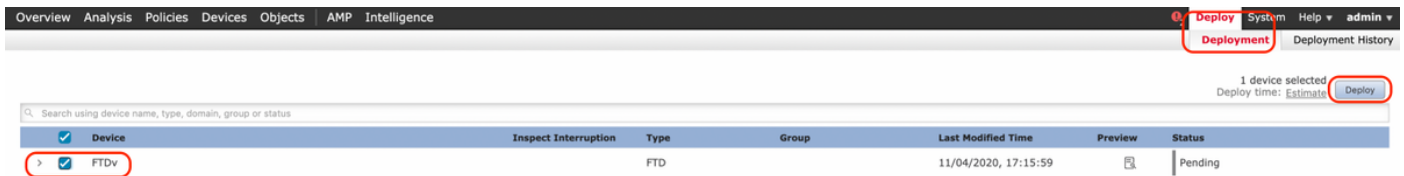
Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates Show Warnings Save Cancel

NAT_Exempt
Enter Description Policy Assignments (1)

Rules Filter by Device Add Rule

#	Direction	Type	Original Packet			Translated Packet			Options
			Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	
1		Static	LAN	WAN	LOCAL_PROXY	REMOTE_PROXY	LOCAL_PROXY	REMOTE_PROXY	Dns: false route-lookup no-proxy-arp

Step 4. Once the configuration is complete, save and deploy the configuration to the FTD.



Verify

Initiate interesting traffic from the LAN machine or you can run the below packet-tracer command on the ASA.

```
packet-tracer input inside icmp 2001:aaaa::23 128 0 2001:dddd::33 detail
```

Note : Here Type = 128 and Code=0 represents ICMPv6 “Echo Request”.

The below section describes the commands that you can run on ASA or FTD LINA CLI to check the status of the IKEv2 tunnel.

This is an example of an output from the ASA:

```
ciscoasa# show crypto ikev2 sa
```

```
IKEv2 SAs:
```

```
Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local Status Role Remote
6638313 2001:bbbb::1/500
READY INITIATOR 2001:cccc::1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/224 sec
Child sa: local selector 2001:aaaa::/0 - 2001:aaaa::ffff:ffff:ffff:ffff/65535
remote selector 2001:dddd::/0 - 2001:dddd::ffff:ffff:ffff:ffff/65535
ESP spi in/out: 0xa0fd3fe6/0xd95ecdb8
```

```
ciscoasa# show crypto ipsec sa detail
```

```
interface: outside
```

```
Crypto map tag: VPN, seq num: 1, local addr: 2001:bbbb::1
```

```
access-list CRYPTO_ACL extended permit ip 2001:aaaa::/64 2001:dddd::/64
local ident (addr/mask/prot/port): (2001:aaaa::/64/0/0)
remote ident (addr/mask/prot/port): (2001:dddd::/64/0/0)
current_peer: 2001:cccc::1
```

```
#pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 11
#pkts decaps: 11, #pkts decrypt: 11, #pkts verify: 11
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #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
#pkts no sa (send): 0, #pkts invalid sa (rcv): 0
#pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
#pkts invalid prot (rcv): 0, #pkts verify failed: 0
#pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
```

#pkts invalid pad (rcv): 0,
#pkts invalid ip version (rcv): 0,
#pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
#pkts replay failed (rcv): 0
#pkts min mtu frag failed (send): 0, #pkts bad frag offset (rcv): 0
#pkts internal err (send): 0, #pkts internal err (rcv): 0

local crypto endpt.: 2001:bbbb::1/500, remote crypto endpt.: 2001:cccc::1/500
path mtu 1500, ipsec overhead 94(64), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: D95ECDB8
current inbound spi : A0FD3FE6

inbound esp sas:

spi: 0xA0FD3FE6 (2700951526)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 1937408, crypto-map: VP
sa timing: remaining key lifetime (kB/sec): (4055040/28535)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

outbound esp sas:

spi: 0xD95ECDB8 (3646868920)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 1937408, crypto-map: VPN
sa timing: remaining key lifetime (kB/sec): (4193280/28535)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

ciscoasa# **show vpn-sessiondb detail l2l filter name 2001:cccc::1**

Session Type: LAN-to-LAN Detailed

Connection : 2001:cccc::1
Index : 473 IP Addr : 2001:cccc::1
Protocol : IKEv2 IPsec
Encryption : IKEv2: (1)AES256 IPsec: (1)AES256
Hashing : IKEv2: (1)SHA256 IPsec: (1)SHA1
Bytes Tx : 352 Bytes Rx : 352
Login Time : 12:27:36 UTC Sun Apr 12 2020
Duration : 0h:06m:40s

IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:

Tunnel ID : 473.1
UDP Src Port : 500 UDP Dst Port : 500
Rem Auth Mode: preSharedKeys
Loc Auth Mode: preSharedKeys
Encryption : AES256 Hashing : SHA256
Rekey Int (T): 86400 Seconds Rekey Left(T): 86000 Seconds
PRF : SHA256 D/H Group : 14
Filter Name :

IPsec:

Tunnel ID : 473.2

Local Addr	: 2001:aaaa::/64/0/0		
Remote Addr	: 2001:dddd::/64/0/0		
Encryption	: AES256	Hashing	: SHA1
Encapsulation	: Tunnel		
Rekey Int (T)	: 28800 Seconds	Rekey Left(T)	: 28400 Seconds
Rekey Int (D)	: 4608000 K-Bytes	Rekey Left(D)	: 4608000 K-Bytes
Idle Time Out	: 30 Minutes	Idle TO Left	: 23 Minutes
Bytes Tx	: 352	Bytes Rx	: 352
Pkts Tx	: 11	Pkts Rx	: 11

Troubleshoot

To troubleshoot IKEv2 tunnel establishment issues on ASA and FTD, run the following debug commands:

```
debug crypto condition peer <peer IP>
debug crypto ikev2 protocol 255
debug crypto ikev2 platform 255
```

Here is a sample working IKEv2 debugs for reference:

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debug.html>

References

<https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/119425-configure-ipsec-00.html>

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/81824-common-ipsec-trouble.html>

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/vpn/asa-95-vpn-config/vpn-site2site.html>