

Configuration du tunnel site à site IPv6 IKEv2 entre ASA et FTD

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configuration ASA](#)

[Configuration FTD](#)

[Ignorer le contrôle d'accès](#)

[Configurer l'exemption NAT](#)

[Vérification](#)

[Dépannage](#)

[Références](#)

Introduction

Ce document fournit un exemple de configuration pour configurer un tunnel de site à site IPv6 entre un ASA (Adaptive Security Appliance) et FTD (Firepower Threat Defense) à l'aide du protocole Internet Key Exchange version 2 (IKEv2). La configuration inclut une connectivité réseau IPv6 de bout en bout avec ASA et FTD comme périphériques de terminaison VPN.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances fondamentales de la configuration de l'interface de ligne de commande ASA
- Connaissances fondamentales des protocoles IKEv2 et IPSEC
- Compréhension de l'adressage et du routage IPv6
- Compréhension de base de la configuration FTD via FMC

Components Used

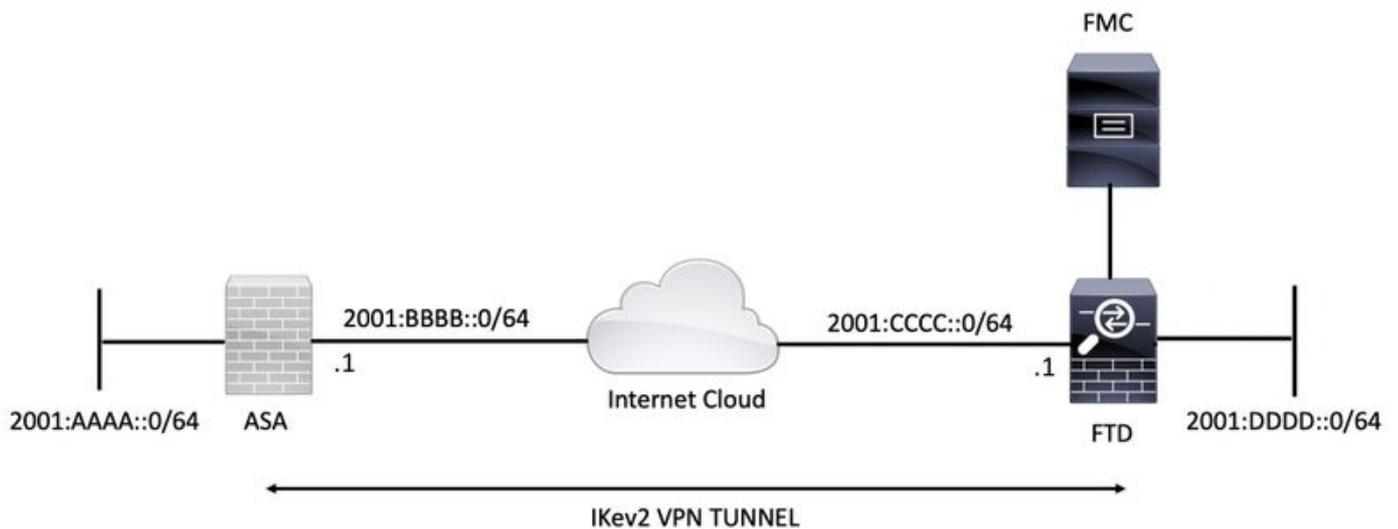
Les informations de ce document sont basées sur un environnement virtuel, créé à partir de périphériques dans une configuration de travaux pratiques spécifique. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en production, assurez-vous de bien comprendre l'impact potentiel de toute commande.

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ASAv exécutant 9.6.1(4)12
- Cisco FTDv 6.5.0
- Cisco FMCv exécutant 6.6.0

Configuration

Diagramme du réseau



Configuration ASA

Cette section décrit la configuration requise sur l'ASA.

Étape 1. Configurer les interfaces ASA.

```
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
```

Étape 2. Définissez une route IPv6 par défaut.

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

Étape 3. Configurez la stratégie IKEv2 et activez IKEv2 sur l'interface externe.

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

```
crypto ikev2 enable outside
```

Étape 4. Configurez le groupe de tunnels.

```
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
```

Étape 5. Créez les objets et la liste de contrôle d'accès (ACL) pour qu'ils correspondent au trafic intéressant.

```
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
```

Étape 6. Configurez les règles NAT (Identity Network Address Translation) pour le trafic intéressant.

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

Étape 7. Configurez la proposition IPsec IKEv2.

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

Étape 8. Définissez la carte de chiffrement et appliquez-la à l'interface externe.

```
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
```

Configuration FTD

Cette section fournit des instructions pour configurer un FTD à l'aide de FMC.

Définir la topologie VPN

Étape 1. Accédez à **Périphériques > VPN > Site To Site**.

Sélectionner 'Ajouter un VPN' et choisissez 'Firepower Threat Defense Device', comme illustré dans cette image.

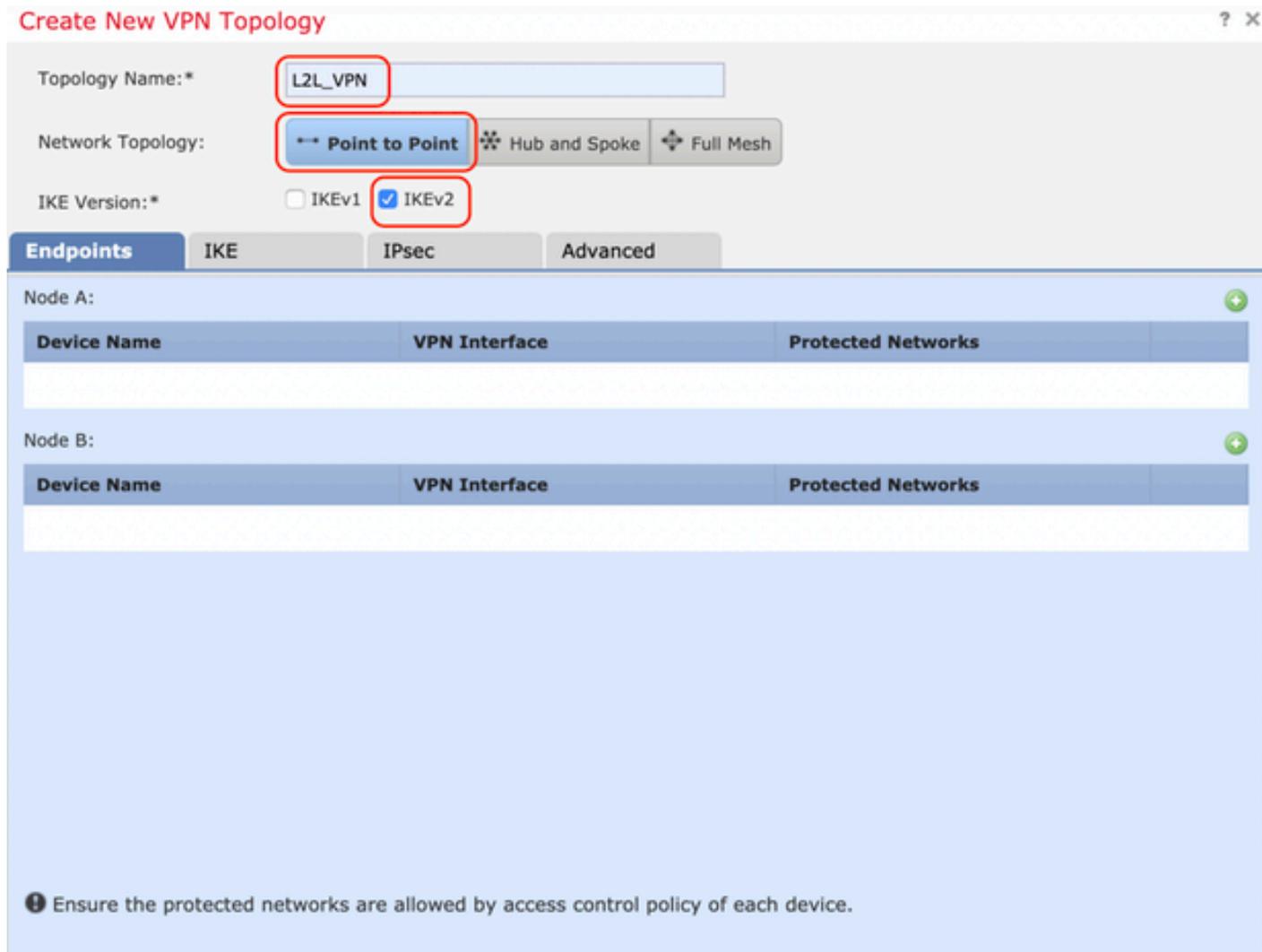


Étape 2. La zone Créer une topologie VPN apparaît. Donnez au VPN un nom facilement identifiable.

Topologie du réseau : Pointez vers Point

Version IKE : IKEv2

Dans cet exemple, lors de la sélection des points de terminaison, le noeud A est le FTD. Le noeud B est l'ASA. Cliquez sur le bouton vert plus pour ajouter des périphériques à la topologie.



Étape 3. Ajoutez le FTD comme premier point de terminaison.

Sélectionnez l'interface à laquelle la crypto-carte est appliquée. L'adresse IP doit être renseignée automatiquement à partir de la configuration du périphérique.

Cliquez sur l'icône verte plus sous Réseaux protégés pour sélectionner les sous-réseaux chiffrés via ce tunnel VPN. Dans cet exemple, l'objet réseau 'Proxy local' sur FMC comprend le sous-réseau IPv6 '2001:DDDD::/64'.

Edit Endpoint



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)

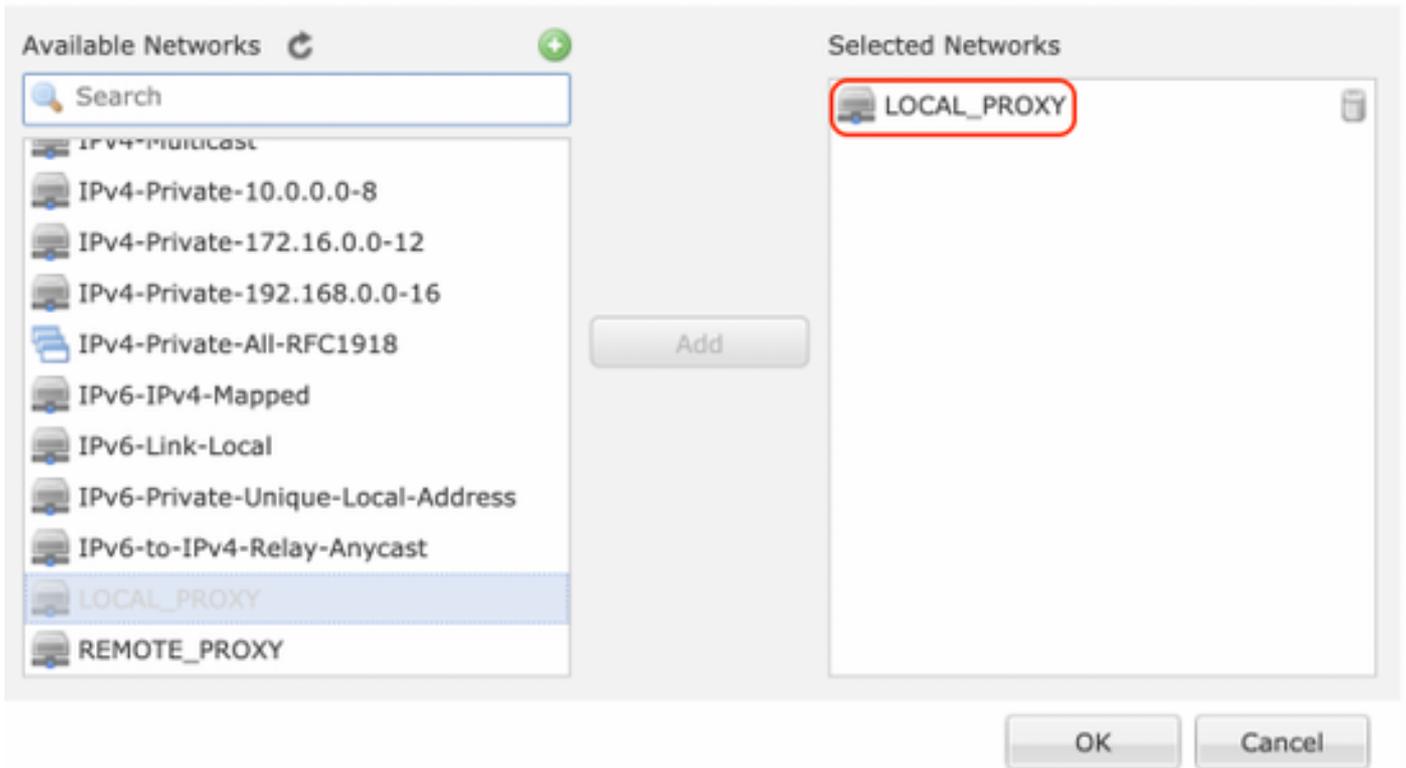


LOCAL_PROXY

OK

Cancel

Network Objects



À l'étape ci-dessus, la configuration du point de terminaison FTD est terminée.

Étape 4. Cliquez sur l'icône verte plus pour le noeud B qui est un ASA dans l'exemple de configuration. Les périphériques qui ne sont pas gérés par le FMC sont considérés comme extranet. Ajoutez un nom de périphérique et une adresse IP.

Étape 5. Sélectionnez l'icône verte plus pour ajouter des réseaux protégés.

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) +

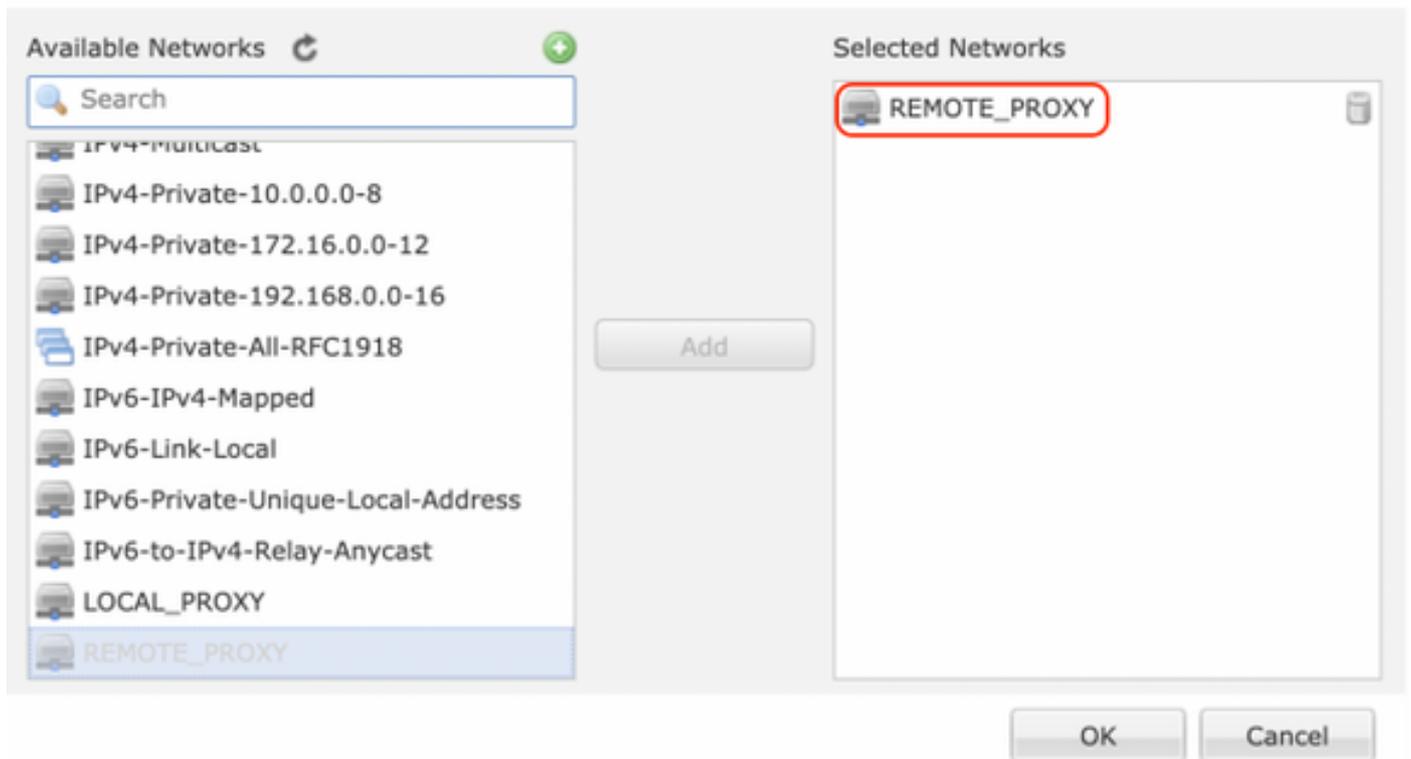
REMOTE_PROXY

OK Cancel

Étape 6. Sélectionnez les sous-réseaux ASA à chiffrer et ajoutez-les aux réseaux sélectionnés.

'Remote Proxy' est le sous-réseau ASA '2001:AAAA::/64' dans cet exemple.

Network Objects



Configurer les paramètres IKE

Étape 1. Sous l'onglet IKE, spécifiez les paramètres à utiliser pour l'échange initial IKEv2. Cliquez sur l'icône verte plus pour créer une nouvelle stratégie IKE.

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

Étape 2. Dans la nouvelle stratégie IKE, spécifiez un numéro de priorité ainsi que la durée de vie de la phase 1 de la connexion. Ce guide utilise les paramètres suivants pour l'échange initial :
Intégrité (SHA256),
Cryptage (AES-256),
PRF (SHA256), et
Groupe Diffie-Hellman (Groupe 14).

Toutes les stratégies IKE du périphérique seront envoyées à l'homologue distant, quelle que soit la section de stratégie sélectionnée. La première que l'homologue distant recherche sera sélectionnée pour la connexion VPN.

[Facultatif] Choisissez la stratégie qui est envoyée en premier à l'aide du champ de priorité. La priorité 1 est envoyée en premier.

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:*

Ikev2_Policy

Description:

Priority:

(1-65535)

Lifetime:

86400

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

Selected Algorithms

- SHA256

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 Groups

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

Add

Selected Groups

- 14

Save Cancel

Étape 3. Une fois les paramètres ajoutés, sélectionnez la stratégie configurée ci-dessus et choisissez le type d'authentification.

Sélectionnez l'option Clé manuelle prépartagée. Pour ce guide, la clé pré-partagée 'cisco123' est utilisée.

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

Configurer les paramètres IPSEC

Étape 1. Passez à l'onglet IPsec et créez une proposition IPsec en cliquant sur l'icône représentant un crayon pour modifier le jeu de transformation.

Edit VPN Topology



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**

Étape 2. Créez une proposition IPsec IKEv2 en sélectionnant l'icône verte plus et en entrant les paramètres de phase 2 comme indiqué ci-dessous :

Hachage ESP : SHA-1

Cryptage ESP : 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

Étape 3. Une fois la nouvelle proposition IPsec créée, ajoutez-la aux jeux de transformation sélectionnés.

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

Étape 4. La proposition IPsec nouvellement sélectionnée est maintenant répertoriée dans les propositions IPsec IKEv2.

Si nécessaire, la durée de vie de la phase 2 et le PFS peuvent être modifiés ici. Dans cet exemple, la durée de vie est définie par défaut et PFS désactivé.

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 tunnel_aes256_sha IKEv2 IPsec Proposals* Ikev2_IPSec_Proposal

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

Modulus Group: [dropdown]

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

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

ESPv3 Settings

Save Cancel

Vous devez configurer les étapes ci-dessous pour contourner le contrôle d'accès ou créer des règles de stratégie de contrôle d'accès pour autoriser les sous-réseaux VPN via FTD.

Ignorer le contrôle d'accès

Si `sysopt permit-vpn` n'est pas activé, une stratégie de contrôle d'accès doit être créée pour autoriser le trafic VPN via le périphérique FTD. Si `sysopt permit-vpn` est activé, ignorez la création d'une stratégie de contrôle d'accès. Cet exemple de configuration utilise l'option "Bypass Access Control".

Le paramètre `sysopt permit-vpn` peut être activé sous Advanced > Tunnel.

Attention : Cette option supprime la possibilité d'utiliser la stratégie de contrôle d'accès pour inspecter le trafic provenant des utilisateurs. Les filtres VPN ou les listes de contrôle d'accès téléchargeables peuvent toujours être utilisés pour filtrer le trafic utilisateur. Il s'agit d'une commande globale qui s'applique à tous les VPN si cette case est activée.

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

Configurer l'exemption NAT

Configurez une instruction NAT Exemption pour le trafic VPN. L'exemption NAT doit être en place pour empêcher le trafic VPN de correspondre à une autre instruction NAT et de traduire incorrectement le trafic VPN.

Étape 1. Accédez à **Périphériques > NAT** et créez une nouvelle stratégie en cliquant sur **Nouvelle stratégie > Défense contre les menaces NAT**.



New Policy



Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

FTDv

Selected Devices

FTDv

Étape 2. Cliquez sur **Ajouter une règle**.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

NAT_Exempt

Enter Description

Show Warnings Show Cancel

Policy Assignments (1)

Filter by Device

| # | 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 | | | | | | | | | | | |

Étape 3. Créez une nouvelle règle NAT manuelle statique.

Référez-vous aux interfaces interne et externe pour la règle NAT. La spécification des interfaces dans l'onglet Objets d'interface empêche ces règles d'affecter le trafic provenant d'autres interfaces.

Accédez à l'onglet Traduction et sélectionnez les sous-réseaux source et de destination. Comme il s'agit d'une règle d'exemption NAT, assurez-vous que la source/destination d'origine et la source/destination traduite sont identiques.

Add NAT Rule



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: +

Cliquez sur l'onglet Avancé et activez **no-proxy-arp** et **route-lookup**.

Add NAT Rule



NAT Rule: Insert:

Type: Enable

Description:

Interface Objects: Translation PAT Pool **Advanced**

Translate DNS replies that match this rule

Falthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Unidirectional

Enregistrez cette règle et confirmez l'instruction NAT finale dans la liste NAT.

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

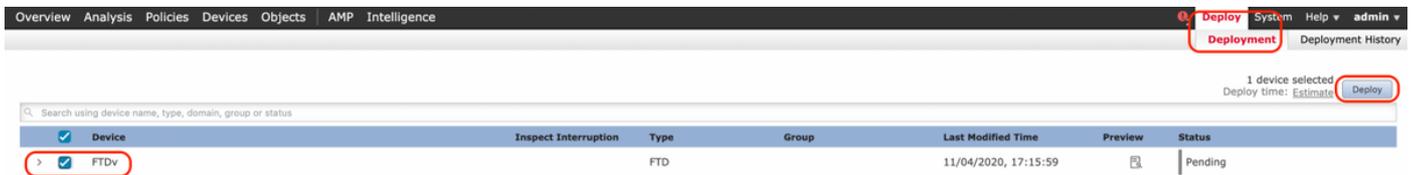
Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates Show Warnings Save Cancel

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 |

Étape 4. Une fois la configuration terminée, enregistrez et déployez la configuration sur le FTD.



Vérification

Lancez un trafic intéressant à partir de la machine LAN ou exécutez la commande packet-tracer ci-dessous sur l'ASA.

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

Remarque: Ici Type = 128 et Code=0 représente ICMPv6 “ Echo Request ”.

La section ci-dessous décrit les commandes que vous pouvez exécuter sur ASA ou FTD LINA CLI pour vérifier l'état du tunnel IKEv2.

Voici un exemple de sortie de l'ASA :

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

IKEv2 SAs:

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

```
Tunnel-id Local                               Remote
          Status                               Role
6638313 2001:bbbb::1/500                       2001:cccc::1/500
          READY    INITIATOR
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
```

Dépannage

Pour résoudre les problèmes d'établissement du tunnel IKEv2 sur ASA et FTD, exécutez les commandes de débogage suivantes :

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

Voici un exemple de débogages IKEv2 qui fonctionnent pour référence :

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

Références

<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>