# Configurer le VPN site à site basé sur la route sur le FTD géré par FMC

## Table des matières


- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
  - VTI statique et VTI dynamique
- Limitations et restrictions
  - Limitations générales de VTI (FTD)
  - Prise en charge du protocole de routage (7.x — Mise à jour à partir de 6.7)
  - IPv6 (7.x — Mise à jour à partir de 6.7)
  - Limites supplémentaires VTI dynamiques (7.3+)
  - NAT, QoS et stratégies
  - Algorithmes cryptographiques faibles
  - Licences
- Étapes de configuration sur FMC
  - Valeurs de démonstration en laboratoire
  - Étape 1. Ouverture d'un VPN de site à site
  - Étape 2 : ajout d'une topologie VPN
  - Étape 3. Nom, type et version IKE de la topologie
  - Étape 4. Sélection du périphérique FTD et de VTI
  - Étape 5. Création d'une interface de tunnel virtuel statique
  - Étape 6. Confirmer la création de VTI
  - Étape 7. Configuration de l'homologue (Noeud B — Extranet)
  - Étape 8. Onglet IKE — Sélectionnez ou créez une stratégie IKE
  - Étape 9. (Facultatif) Créez une stratégie IKEv2
  - Étape 10. Authentification IKE
  - Étape 11. Onglet IPsec — Proposition IPsec
  - Étape 12. (Facultatif) Créer une proposition IKEv2 IPsec
  - Étape 13. Sélectionnez la proposition IPsec
  - Étape 14. Confidentialité parfaite et durée de vie
  - Étape 15. Enregistrement de la topologie VPN
  - Étape 16. Configuration de la stratégie de contrôle d'accès (obligatoire)
  - Étape 17. Ajout d'une route statique via VTI
  - Étape 18. Déploiement de la configuration
- Exemple de CLI après déploiement
- Vérifier

À partir de FMC GUI
À partir de FTD CLI
Guide de référence rapide du dépannage
Documents associés
Historique de révision
Le document s'applique

# Introduction

Ce document décrit comment configurer un tunnel VPN site à site basé sur une route statique sur Cisco Secure FTD géré par FMC.

---

# Conditions préalables

## Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Navigation de l'interface utilisateur Web de FMC (périphériques, stratégies, déploiement)
- Fonctionnement VPN IPsec site à site de base (IKE Phase 1/2, établissement de tunnel)
- Routage statique sur FTD (en option BGP/OSPF/EIGRP pour les conceptions basées sur les routes dynamiques)

---

## Composants utilisés

Le VPN basé sur la route utilise des interfaces de tunnel virtuel (VTI) et le routage (statique ou dynamique) au lieu de listes de contrôle d’accès cryptographiques pour déterminer quel trafic est crypté. Ce document se concentre sur l'appairage point à point ou extranet VTI statique (SVTI). Pour les conceptions hub-and-spoke évolutives, reportez-vous à Dynamic VTI (DVTI) dans les documents associés répertoriés à la fin de cet article.

---

Versions des travaux pratiques utilisées dans les exemples :

| Composante | Version |
| --- | --- |
| Cisco Secure Firewall Management Center | 7.4 ou ultérieure (exemples compatibles avec 7.6) |
| Cisco Secure Firewall Threat Defense | 7.4 ou ultérieure (exemples compatibles avec 7.6) |

---

Le VPN basé sur la route VTI statique a été introduit dans FTD 6.7. DVTI, le protocole de routage étendu prend en charge IPv6 VTI et versions ultérieures, et l'évolutivité VTI nécessite FTD 7.3+ / FMC 7.3+. Les différences spécifiques à la version sont indiquées dans la section Limitations et restrictions.

---

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

---

# Informations générales

Le VPN basé sur la route (basé sur VTI) chiffre le trafic qui est routé dans l'interface de tunnel. Contrairement au VPN basé sur une stratégie (crypto-carte), le trafic unique n'est pas sélectionné par l'ACL sur la tête de réseau. Au lieu de cela, la table de routage dirige le trafic vers la VTI. Pour les interfaces VTI statiques, les sélecteurs de trafic IPsec sont en fait de type « any-to-any » (0.0.0.0/0.0.0.0 pour IPv4). Tout paquet acheminé vers l'interface de tunnel est chiffré quel que soit le sous-réseau source/destination, sujet au contrôle d'accès et au routage sur l'homologue.

---

Le VPN basé sur des politiques utilise toujours des ID de proxy/ACL de chiffrement explicites. Le VPN basé sur la route est préférable pour :

- Routage dynamique (BGP, OSPF, EIGRP) sur le tunnel
- Connectivité cloud (AWS, Azure, GCP)
- Gestion simplifiée du domaine de cryptage
- Migration à partir de conceptions de crypto-cartes héritées

---

## VTI statique et VTI dynamique

| Type | Scénario | FTD minimum |
|---|---|---|
| VTI statique (SVTI) | Point à point, homologue extranet, satellite en étoile | 6.7 |
| VTI dynamique (DVTI) | Concentrateur avec plusieurs rayons (modèle virtuel unique sur le concentrateur) | 7.3 |

Ce document couvre l'infrastructure SVTI étape par étape. Pour le hub-and-spoke DVTI avec Multi-SA, référez-vous à Configurer DVTI avec Multi-SA sur le pare-feu sécurisé (ID de document 220322.)

---

## Limitations et restrictions

Consultez les limites de plate-forme actuelles dans le Guide de configuration des périphériques FMC - Directives VPN site à site / VTI pour votre version FMC. Le résumé de la section suivante reflète les sections FMC/FTD 7.4 à 7.6, sauf indication contraire.

---

### Limitations générales de VTI (FTD)

| Limite | Détail |
|---|---|
| Mode tunnel | IPsec uniquement. GRE sur VTI n'est pas pris en charge sur FTD. |
| Mode pare-feu | VTI est pris en charge en mode routé uniquement. |
| Groupage | VTI n'est pas pris en charge sur les déploiements de clusters FTD. |
| HA (actif/veille) | VTI statique est pris en charge dans les paires FTD HA (haute disponibilité). Routage dynamique sur VTI en haute disponibilité : il est possible que standby n'atteigne pas les sous-réseaux via des tunnels VTI créés avec l'unité active IP (planifiez le routage en conséquence). Pour plus de 400 VTI en haute disponibilité, définissez le temps d'attente de l'unité sur 45 secondes. |
| Échelle | Jusqu'à 1 024 VTI statiques et dynamiques par périphérique (7.x). Documentation 6.7 originale citant 100 VTI par interface ; les conseils actuels sont 1024 par périphérique, assurez-vous de vérifier par rapport à votre plate-forme et version. |

| Limite | Détail |
| --- | --- |
| Profils IPsec | 20 profils IPsec uniques maximum (VTI statique). |
| sysopt connection permit-vpn | Ne s'applique pas au VPN basé sur la route. Vous devez configurer des règles de stratégie de contrôle d'accès (ACP) pour le trafic déchiffré dans les deux directions. |
| Paramètres de plateforme | Les interfaces de tunnel VTI ne sont pas prises en charge pour la sélection SNMP ou Syslog dans les paramètres de plate-forme. |
| VPN d’accès à distance | Une interface VTI ne peut pas être utilisée comme interface réseau pour une stratégie VPN d'accès à distance. |

## Prise en charge du protocole de routage (7.x — Mise à jour à partir de 6.7)

La documentation FTD 6.7 d'origine indiquait uniquement BGP. Le FTD actuel prend en charge ces méthodes de routage sur VTI :

| Protocol | Soutien |
| --- | --- |
| Routes statiques | Oui |
| BGP | IPv4 et IPv6 |
| OSPF | OSPFv2 et OSPFv3 |
| EIGRP | IPv4 |

Directives BGP : Lors de l'utilisation de BGP sur VTI, définissez TTL hop count > 1 sur la configuration de routage.

ECMP : Les interfaces VTI statiques en étoile peuvent être placées dans une zone ECMP pour l'équilibrage de charge et le basculement. Dynamic VTI ne prend pas en charge ECMP.

## IPv6 (7.x — Mise à jour à partir de 6.7)

La documentation FTD 6.7 d'origine indiquait IPv4 uniquement et la prise en charge des versions actuelles :

- Adresses IPv6 sur la source du tunnel et les terminaux VTI
- Combinaisons : IPv4 sur IPv4, IPv6 sur IPv6, IPv4 sur IPv6, IPv6 sur IPv4
- Adresses IPv6 statiques et dynamiques sur la source du tunnel

Vérifiez la fonctionnalité homologue et les notes de version FMC avant de déployer IPv6 VTI.

---

## Limites supplémentaires VTI dynamiques (7.3+)

- IKEv2 uniquement (pas IKEv1)
- Topologie Hub and Spoke dans FMC (concentrateur unique recommandé par topologie)
- Pas d'ECMP, pas de QoS, pas de clustering, pas de VRF-in-multi-instance sur DVTI
- 1 000 sessions DVTI maximum par périphérique (selon la plate-forme)
- Le concentrateur DVTI nécessite un adressage en mode bouclé (ou emprunt-IP) dans la plupart des conceptions

---

## NAT, QoS et stratégies

| Stratégie/Fonctionnalité | VTI statique | VTI dynamique |
|---|---|---|
| Politique de contrôle d'accès | Obligatoire (dans les deux sens). | Requis |
| NAT | Le trafic VPN peut être exempté dans l'assistant de topologie ; Les règles NAT peuvent s'appliquer au trafic non VPN. Ne chiffrez pas IKE/ESP de manière incorrecte. | Similaire ; voir options d'exemption NAT FMC |
| QoS | Prise en charge limitée des plates-formes ; DVTI ne prend pas en charge QoS. | Non pris en charge |
| Paramètres de plate-forme (SNMP/Syslog sur VTI) | Non pris en charge. | Non pris en charge |

---

Le texte d'origine de la version 6.7 indique que VTI n'est pas pris en charge dans les stratégies NAT/QoS/Platform Settings. Orientation actuelle : la PPS est obligatoire; SNMP/Syslog sur VTI reste non pris en charge ; La QoS sur DVTI n'est pas prise en charge, consultez FMC pour l'interaction NAT sur votre version.

---

## Algorithmes cryptographiques faibles

Les algorithmes faibles ont été supprimés pour les nouveaux tunnels VPN à partir de FMC/FTD 6.7. Les versions ultérieures conservent des valeurs par défaut de chiffrement fort et celles-ci ne sont pas prises en charge pour les nouvelles configurations de tunnel sur FTD 6.7+ :

---

Stratégie IKE — non prise en charge pour les nouveaux tunnels :

- Chiffrement : 3DES, DES, NULL
- Intégrité: MD5
- PRF : MD5
- Groupes DH : 1, 2, 24

---

Proposition IPsec — non prise en charge pour les nouveaux tunnels :

Chiffrement ESP : DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256

---

Impact de la mise à niveau (version 6.7 ou ultérieure) : La mise à niveau d'un FTD géré par FMC à partir d'une version antérieure à 6.7 peut déclencher un contrôle de prévalidation si une stratégie VPN existante utilise des chiffrements supprimés. Reconfigurez les stratégies IKE/IPsec avec des algorithmes forts avant de procéder à la mise à niveau.

---

| Scénario | Interface utilisateur de configuration | Tunnel après mise à niveau |
|---|---|---|
| Nouvelle installation (6.7+) | Chiffres faibles visibles mais ne peuvent pas être appliqués à FTD 6.7+ | S/O |
| Mise à niveau: FTD utilise uniquement des chiffres faibles | Mise à niveau bloquée jusqu'à reconfiguration | Désactivation du tunnel si forcée |

| Scénario | Interface utilisateur de configuration | Tunnel après mise à niveau |
|---|---|---|
| Mise à niveau: Chiffres faibles/forts mixtes | Mise à niveau bloquée jusqu'à reconfiguration | Le tunnel peut être rétabli si l'homologue utilise des chiffrements forts |
| Licence d'exportation contrôlée (classe C) | DES peut être la seule option sans licence de chiffrement fort | tunnels DES-only |

---

Recommandation : Pour les nouveaux déploiements, utilisez IKEv2, AES-256, SHA-256 ou SHA-512 et le groupe DH 19/20/21 (ou un groupe pris en charge de version supérieure).

---

### Licences

Aucune licence supplémentaire n'est requise au-delà de la capacité FTD de base pour le VPN basé sur la route en mode sous licence ou évaluation. Si les fonctionnalités d'exportation contrôlée (chiffrement fort) ne sont pas activées, seul DES est disponible comme algorithme de chiffrement dans les déploiements restreints.

---

## Étapes de configuration sur FMC

Ces étapes sont configurées dans un VPN site à site basé sur une route statique (VTI) entre un FTD (Node A) et un homologue extranet tel qu'un ASA (Node B) :

---

### Valeurs de démonstration en laboratoire

| Paramètre | Valeur |
|---|---|
| Nom de topologie | VTI-ASA |
| Version IKE | IKEv2 |
| Nom VTI | VTI-ASA |

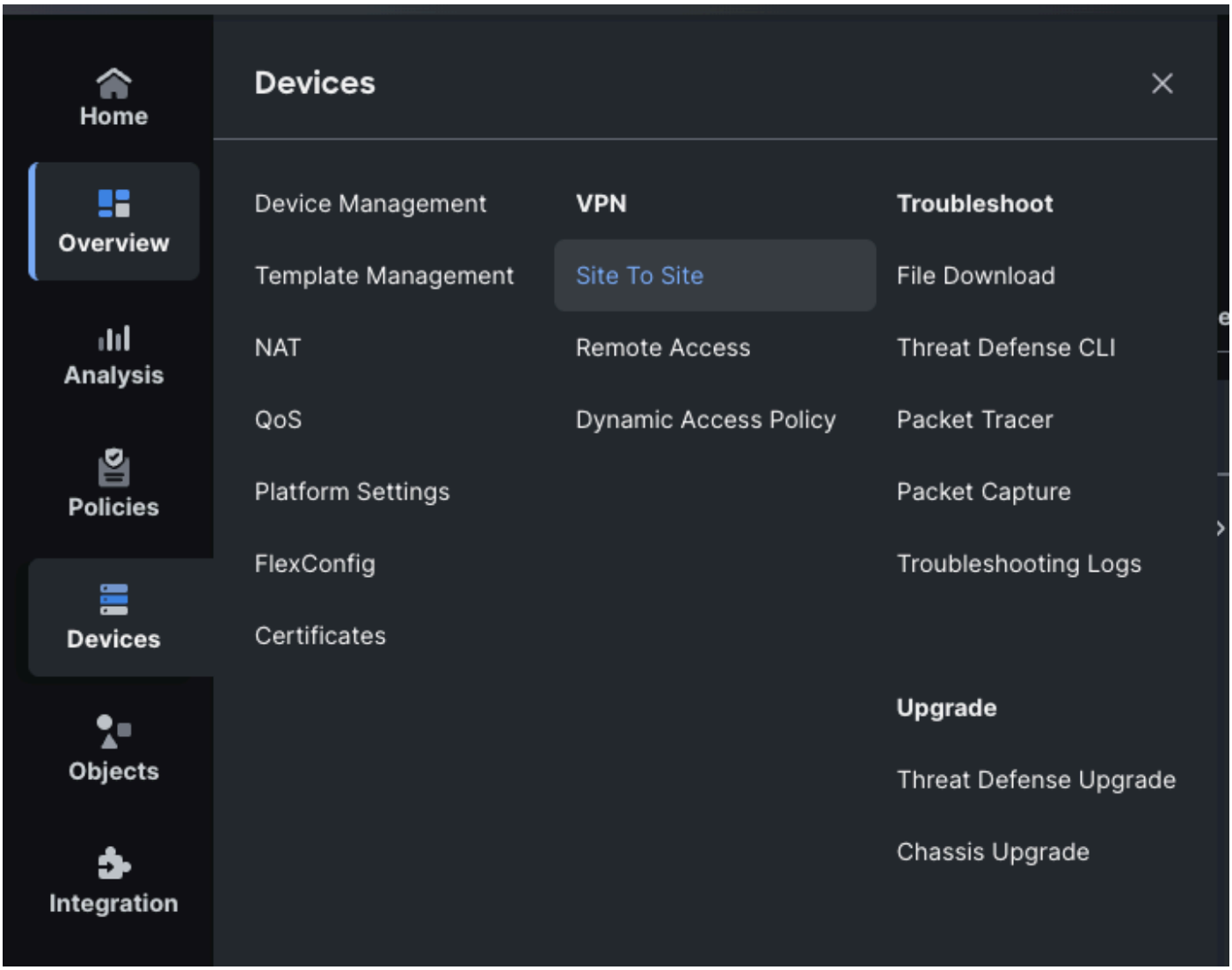
| Paramètre | Valeur |
| --- | --- |
| Zone VTI | Zone VTI |
| ID de tunnel | 1 |
| IP VTI (FTD) | 192.168.100.1/30 |
| Source du tunnel | GigabitEthernet0/0 (externe) |
| Périphérique homologue | Extranet ASA |
| Nom de pair | Homologue ASA |
| IP du terminal homologue | 10.106.67.252 |
| Nom de la stratégie IKE | ASA-IKEv2-Policy |
| Nom de proposition IPsec | Stratégie ASA-IPSec |
| PSK (travaux pratiques uniquement) | (utiliser une clé forte en production) |

---

## Étape 1. Ouverture d’un VPN de site à site

1. Accédez à Périphériques > VPN > Site à site

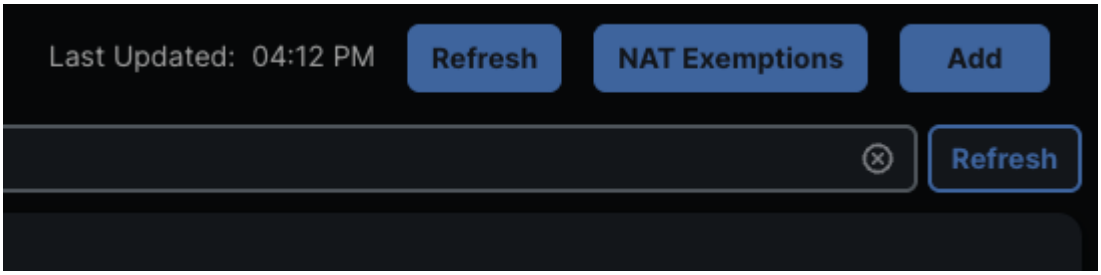
---




## Étape 2 : ajout d’une topologie VPN

1. Cliquez sur Add VPN et choisissez Firewall Threat Defense Device (ou Secure Firewall Threat Defense Device, selon la version de l'interface utilisateur FMC).

---




---

## Étape 3. Nom, type et version IKE de la topologie

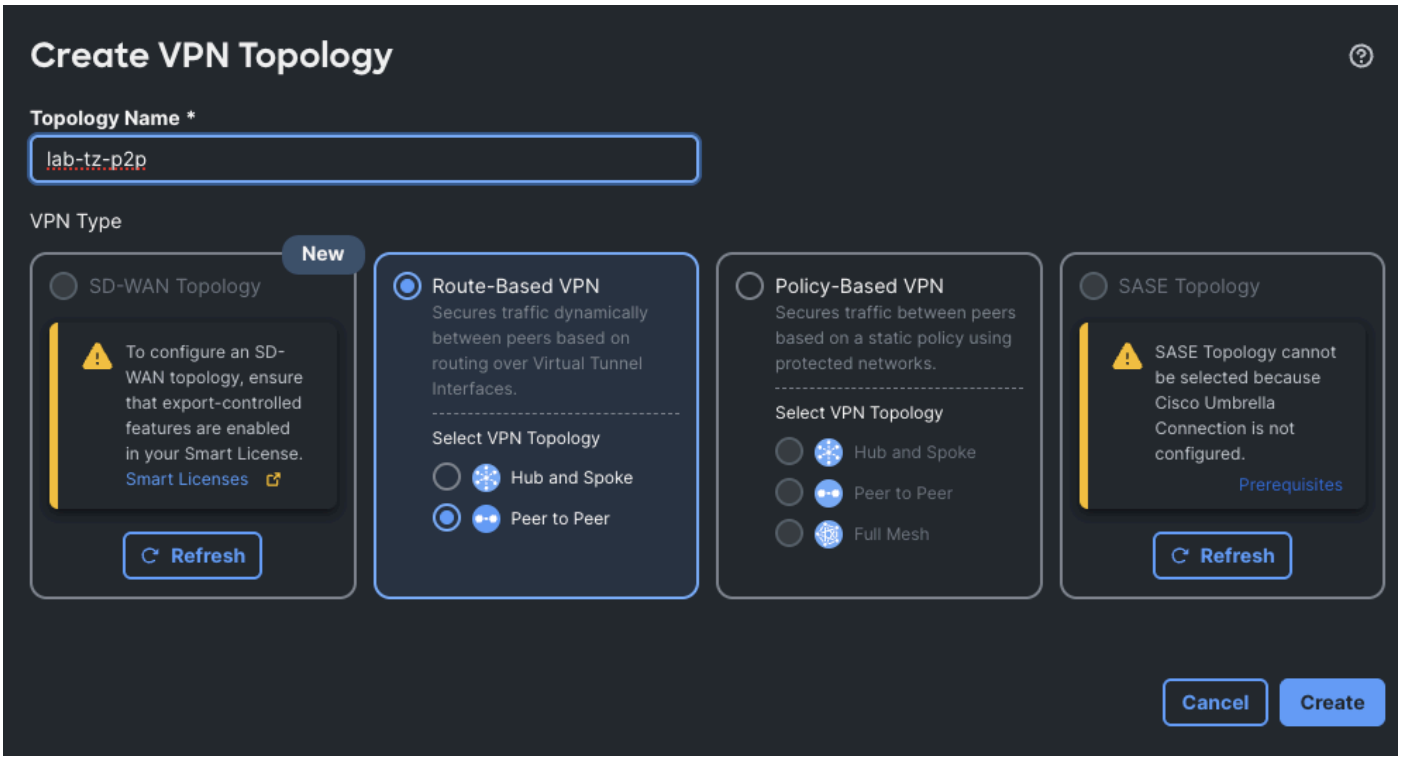
1. Indiquez un nom de topologie et sélectionnez le type VPN Route Based (VTI). Choisissez la version IKE (recommandé : IKEv2.)

- Nom de topologie : VTI-ASA
- type : Basé sur la route (VTI)
- Version IKE : IKEv2

---

Remarque : IKEv1 ne prend pas en charge les périphériques compatibles CC/UCAPL. Cisco recommande IKEv2 pour les nouvelles conceptions.

---

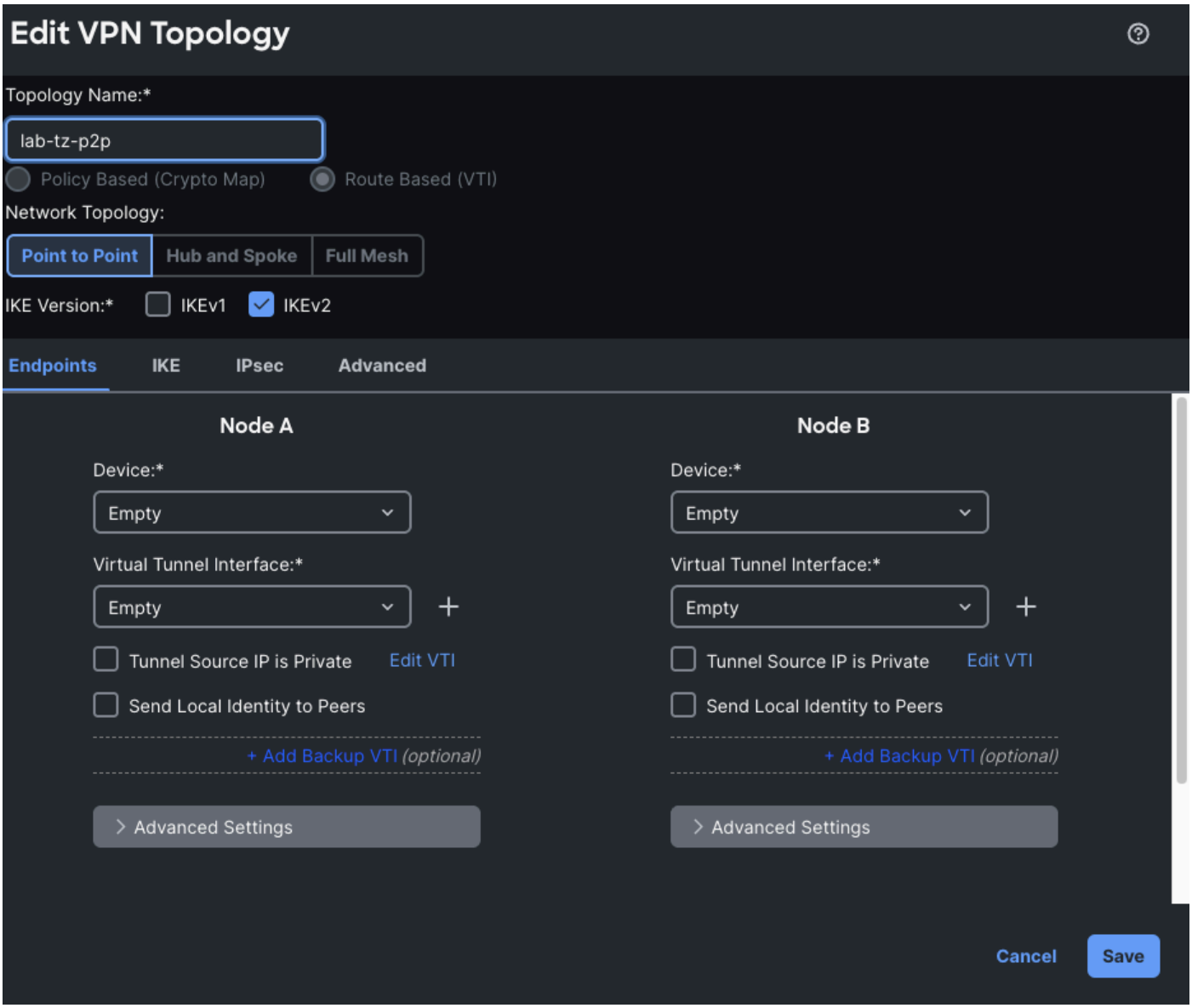



---

## Étape 4. Sélection du périphérique FTD et de VTI

1. Sélectionnez le périphérique FTD pour le noeud A.
2. Ajoutez une nouvelle interface de tunnel virtuel (cliquez sur +) ou sélectionnez une interface VTI existante. Pour le concentrateur en étoile avec DVTI sur le concentrateur, le

concentrateur utilise Dynamic VTI.




## Étape 5. Création d’une interface de tunnel virtuel statique

1. Définissez les nouveaux paramètres VTI et cliquez sur OK.

| Champ | Exemple |
| --- | --- |
| Nom | VTI-ASA |
| Description | Tunnel VTI avec extranet ASA |

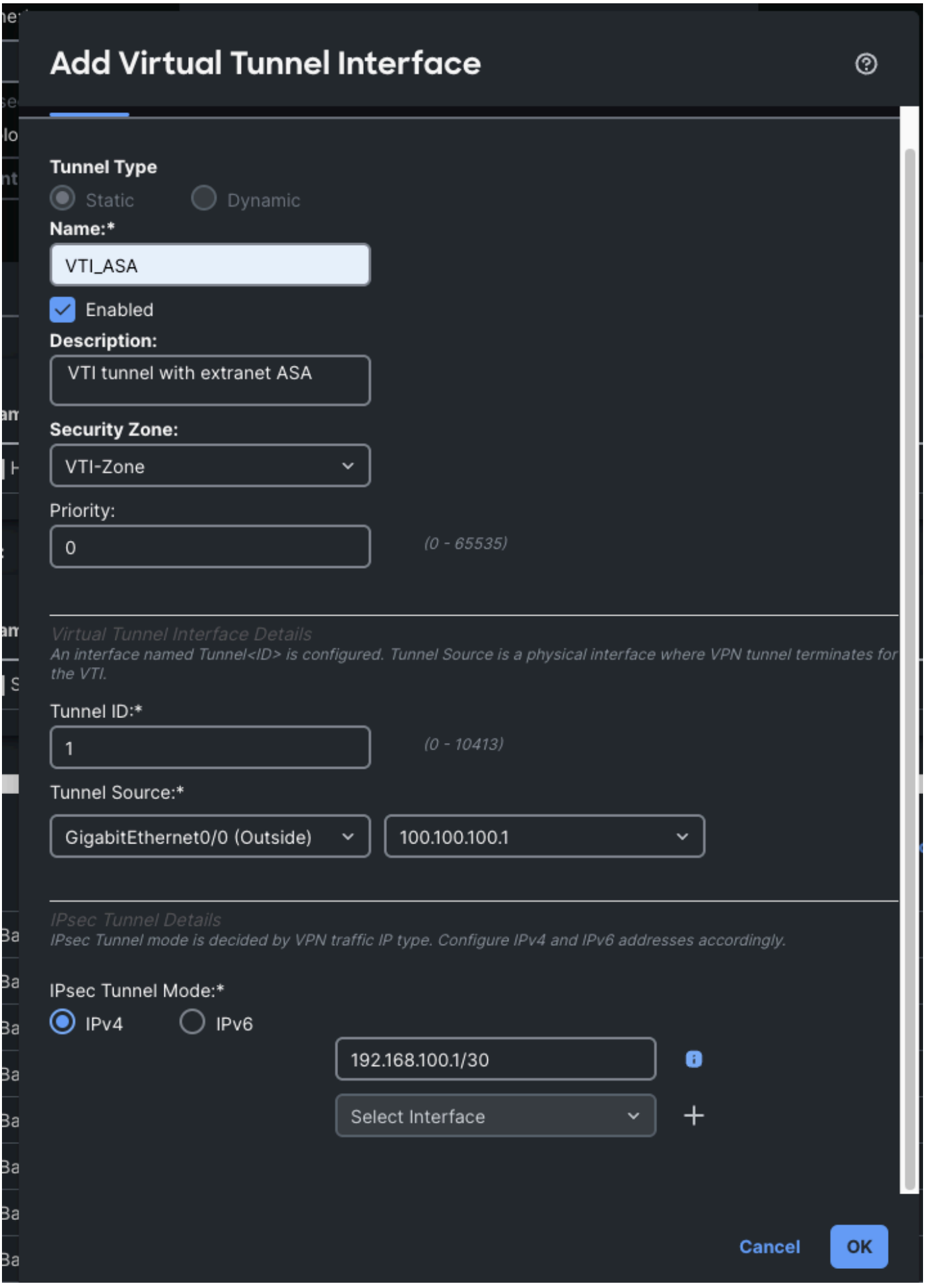
| Champ | Exemple |
| --- | --- |
| Zone de sécurité | Zone VTI |
| ID de tunnel | 1 |
| Adresse IP | 192.168.100.1/30 |
| Source du tunnel | GigabitEthernet0/0 (externe) |
| Mode tunnel | ipsec ipv4 |

---

2.

- Attribuez la VTI à une zone de sécurité dédiée utilisée dans les règles ACP.
- Pour IPv6, sélectionnez le mode de tunnel et l'adressage appropriés (7.x).
- N'utilisez pas d'interface emprunt-IP comme adresse source du tunnel.

---


Add Virtual Tunnel Interface
Tunnel Type
Static
Dynamic
Name:*
VTI_ASA
Enabled
Description:
VTI tunnel with extranet ASA
Security Zone:
VTI-Zone
Priority:
0
(0 - 65535)
Virtual Tunnel Interface Details
An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.
Tunnel ID:*
1
(0 - 10413)
Tunnel Source:*
GigabitEthernet0/0 (Outside)
100.100.100.1
IPsec Tunnel Details
IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.
IPsec Tunnel Mode:*
IPv4
IPv6
192.168.100.1/30
Select Interface
Cancel
OK

## Étape 6. Confirmer la création de VTI

1. Cliquez sur OK sur la confirmation que le VTI a été créé.

---

## Étape 7. Configuration de l’homologue (Noeud B — Extranet)

1. Sélectionnez le VTI créé à l’étape 5. Configurez le noeud B (homologue) :

---

| Champ | Exemple |
|---|---|
| Type de périphérique | Extranet |
| Nom du périphérique | Homologue ASA |
| Adresse IP du terminal | 10.106.67.252 |

---

2. Configurez les réseaux protégés pour les sous-réseaux derrière chaque homologue. Les réseaux protégés définissent le trafic qui peut utiliser le VPN ; Le VPN basé sur la route nécessite toujours des routes pointant vers le VTI.

Facultatif (7.x) :

- Activez NAT Traversal si un périphérique NAT existe entre des homologues.
- Exemptez le trafic VPN de la fonction NAT dans l'assistant de topologie si nécessaire.
- Envoyer l'IP d'interface de tunnel virtuel aux homologues lorsque l'homologue a besoin de l'IP VTI pour le routage (commun avec BGP/OSPF).

---

## Étape 8. Onglet IKE — Sélectionnez ou créez une stratégie IKE

1. Ouvrez l'onglet IKE et sélectionnez une stratégie IKEv2 existante ou cliquez sur + pour en créer une nouvelle.

---

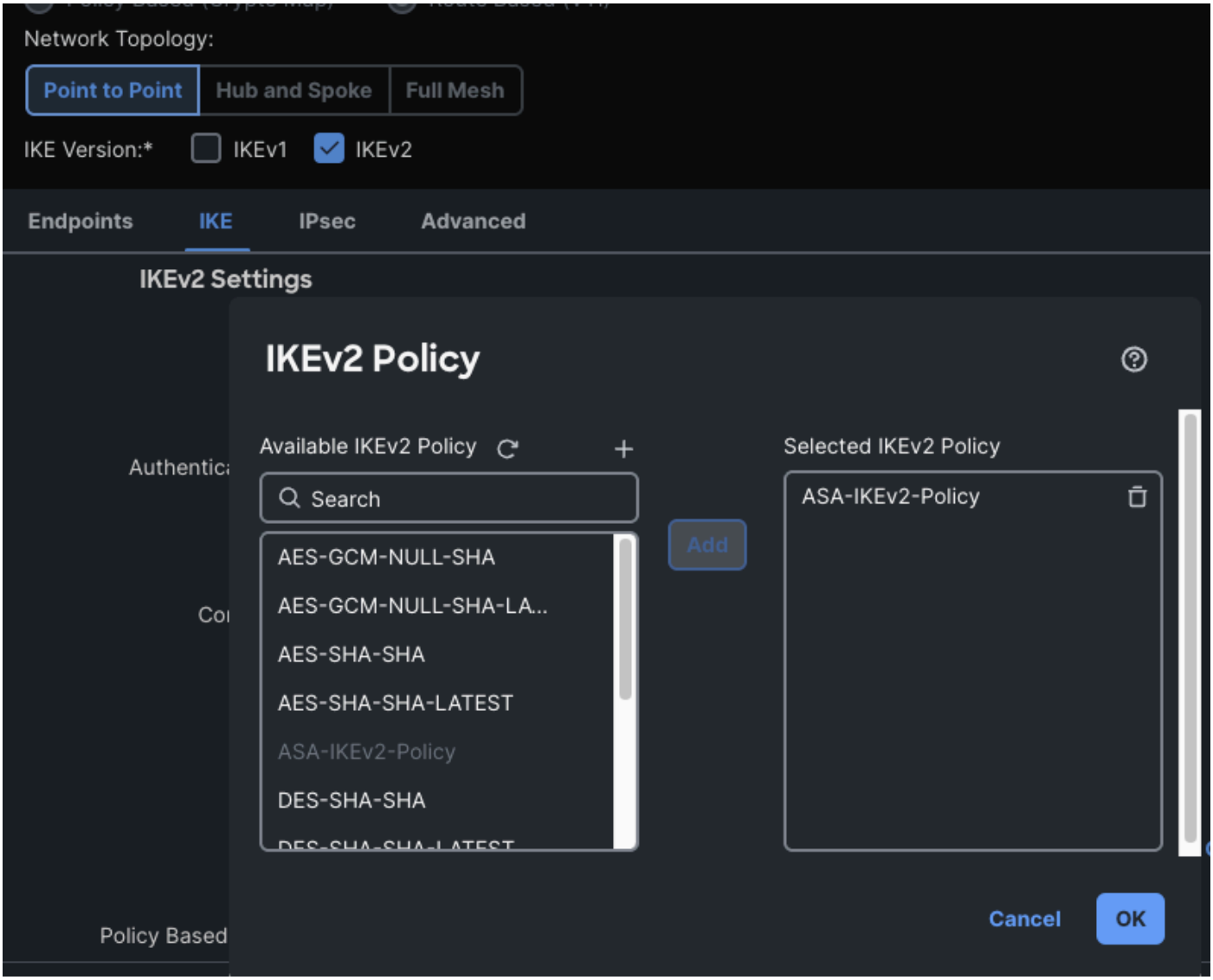
## Étape 9. (Facultatif) Créez une stratégie IKEv2

| Champ | Exemple recommandé |
|---|---|
| Nom | ASA-IKEv2-Policy |
| Intégrité | SHA-512 (ou SHA-256) |
| Chiffrement | AES-256 |
| PRF | SHA-512 (ou SHA-256) |
| Groupe DH | 21 (ou 19/20 par politique) |

---

1. Cliquez sur Save.

---




---

## Étape 10. Authentification IKE

1. Sélectionnez la stratégie IKE. Sélectionnez le type d'authentification :

- Clé manuelle pré-partagée : Entrez et confirmez la clé (travaux pratiques/démonstration uniquement ; utiliser une clé prépartagée forte en production.)
- Clé automatique pré-partagée : disponible lorsque les deux terminaux sont gérés par le même FMC.
- Certificat : pour l'authentification basée sur PKI.

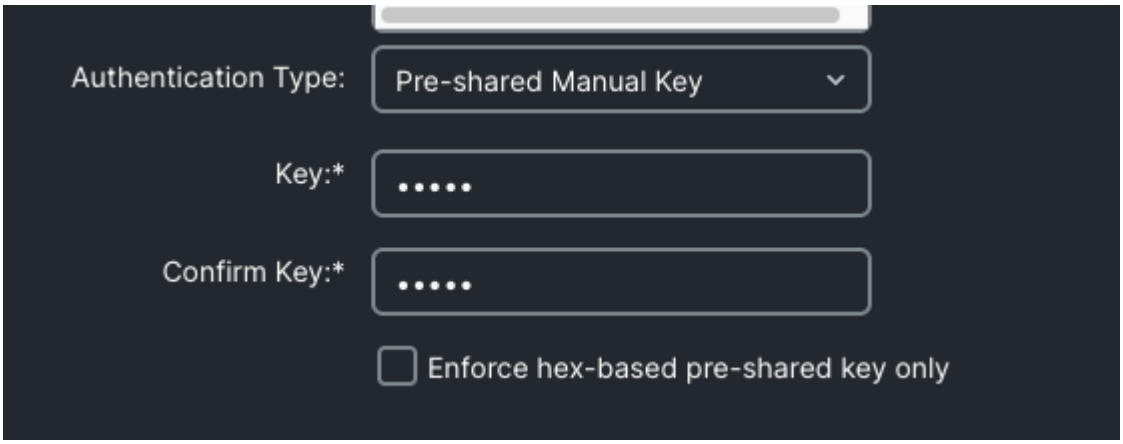
---

Exemple (travaux pratiques) :

- Policy (politique) : ASA-IKEv2-Policy

- Authentification: Clé manuelle pré-partagée

---




---

## Étape 11. Onglet IPsec — Proposition IPsec

1. Ouvrez l'onglet IPsec. Sélectionnez ou créez une proposition IKEv2 IPsec (cliquez sur Edit ou sur +).

---

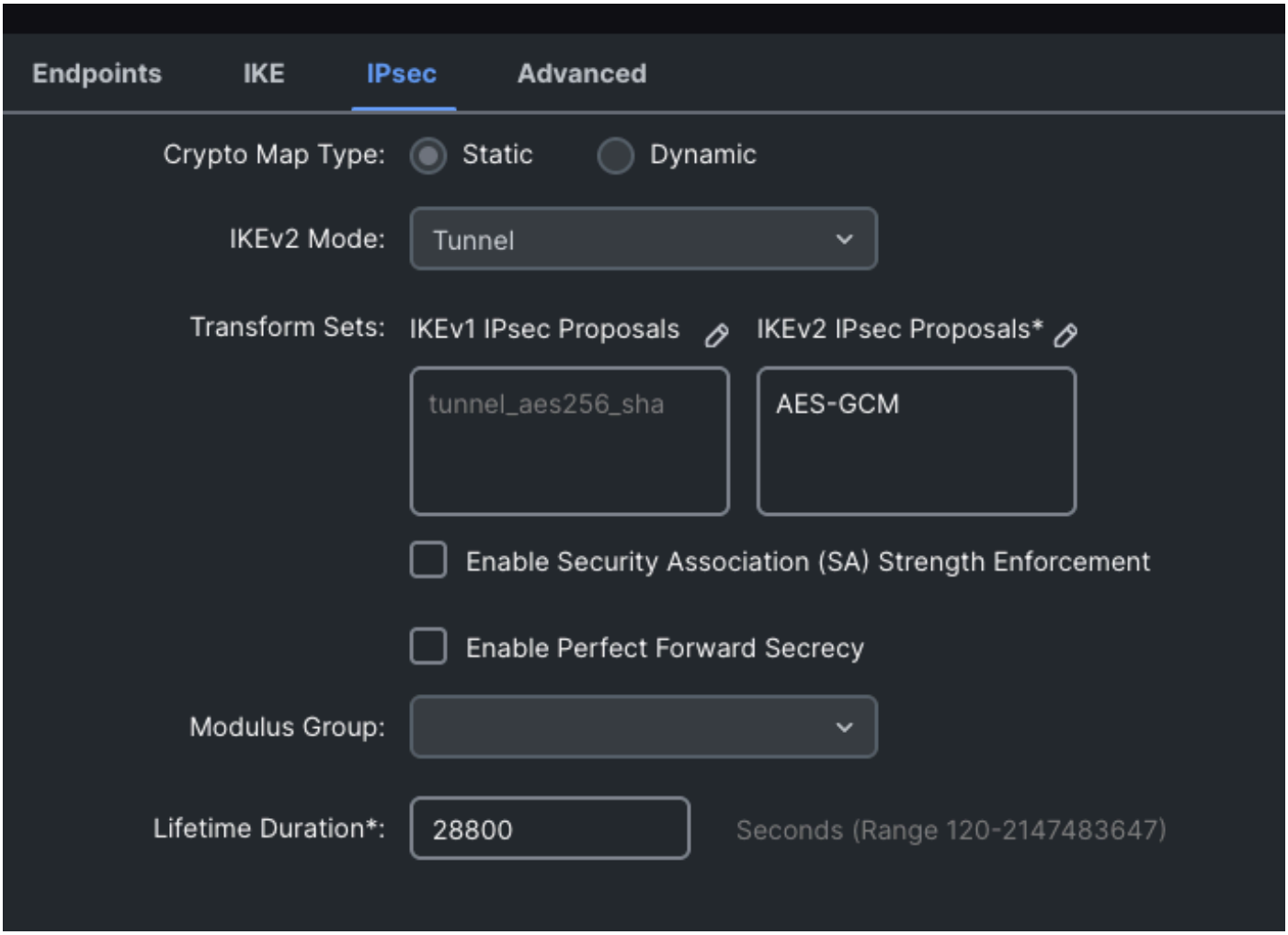
## Étape 12. (Facultatif) Créer une proposition IKEv2 IPsec

| Champ | Exemple recommandé |
|---|---|
| Nom | Stratégie ASA-IPSec |
| Hachage ESP | SHA-512 (ou SHA-256) |
| Cryptage ESP | AES-256 |

---

1. Cliquez sur Save.

---




---

## Étape 13. Sélectionnez la proposition IPsec

1. Choisissez la proposition et cliquez sur OK.

---

## Étape 14. Confidentialité parfaite et durée de vie

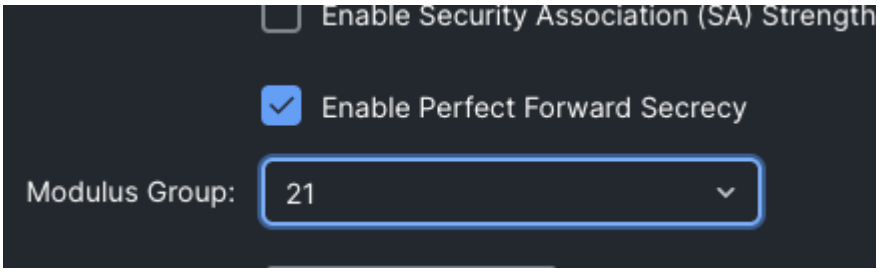
1. Configurez le PFS et les durées de vie facultatives :

---

| Champ | Exemple |
|---|---|
| Confidentialité parfaite | Groupe 21 |

| Champ | Exemple |
| --- | --- |
| Durée De Vie | 28800 secondes (par défaut) |
| Taille de vie | 4608000 Ko (par défaut) |

2. Adaptez-vous aux exigences des homologues et aux normes de chiffrement organisationnelles.




## Étape 15. Enregistrement de la topologie VPN

Vérifiez le résumé et cliquez sur Save.

## Étape 16. Configuration de la stratégie de contrôle d’accès (obligatoire)

1. Accédez à Stratégies > Contrôle d'accès > Contrôle d'accès. Modifiez la stratégie appliquée au FTD.

Remarque : sysopt connection permit-vpn - La stratégie de contournement du contrôle d'accès pour le trafic VPN décrypté ne fonctionne pas avec le VPN basé sur la route. Configurez des règles Allow explicites pour le trafic traversant la zone VTI dans les deux directions. Le tableau suivant fournit l'exemple de création de règles.

| Direction | Zone source | Zone De Repos | Réseaux sources | Réseaux Dest |
| --- | --- | --- | --- | --- |
| Interne → Distant | Dans la zone | Zone VTI (ou zone de sortie) | Dans le réseau | Réseau distant |

| Direction | Zone source | Zone De Repos | Réseaux sources | Réseaux Dest |
|---|---|---|---|---|
| Distant → Interne | Zone VTI | Dans la zone | Réseau distant | Dans le réseau |

---

2. Ajustez les noms de zone en fonction de votre conception. Des règles bidirectionnelles sont requises pour une connectivité complète.

---

## Étape 17. Ajout d'une route statique via VTI

1. Accédez à Périphériques > Gestion des périphériques. Modifiez le périphérique FTD.
2. Ouvrez Routing > Static Route. Cliquez sur Add Route.

---

| Champ | Exemple |
|---|---|
| Interface | VTI-ASA |
| Réseau | Réseau distant |
| Passerelle | 192.168.100.2 (IP VTI homologue) |

---

3. Utilisez l'adresse IP du tunnel homologue comme passerelle, à moins que votre conception n'utilise un autre tronçon suivant accessible via l'interface VTI.

4. Pour le routage dynamique, configurez BGP, OSPF, ou EIGRP sur le VTI au lieu (ou en plus) des routes statiques.

5. ECMP (facultatif, 7.x) : Placez plusieurs VTI statiques dans une zone ECMP et configurez les routes statiques ECMP pour le partage de charge.

---

## Étape 18. Déploiement de la configuration

1. Naviguez jusqu'à Déployer > Déploiement (ou Déployer > Gestionnaire de déploiement, selon la version de FMC). Sélectionnez le FTD et cliquez sur Déployer. Attendez la réussite du déploiement avant de procéder à la vérification.

---

# Exemple de CLI après déploiement

Une fois le déploiement réussi, la configuration CLI FTD ressemble à :

```
crypto ikev2 policy 1
 encryption aes-256
 integrity sha512
 group 21
 prf sha512
 lifetime seconds 86400
crypto ikev2 enable Outside

crypto ipsec ikev2 ipsec-proposal CSM_IP_1
 protocol esp encryption aes-256
 protocol esp integrity sha-512

crypto ipsec profile FMC_IPSEC_PROFILE_1
 set ikev2 ipsec-proposal CSM_IP_1
 set pfs group21

group-policy .DefaultS2SGroupPolicy internal
group-policy .DefaultS2SGroupPolicy attributes
 vpn-idle-timeout 30
 vpn-idle-timeout alert-interval 1
 vpn-session-timeout none
 vpn-session-timeout alert-interval 1
 vpn-filter none
 vpn-tunnel-protocol ikev1 ikev2

tunnel-group 10.106.67.252 type ipsec-l2l
tunnel-group 10.106.67.252 general-attributes
 default-group-policy .DefaultS2SGroupPolicy
tunnel-group 10.106.67.252 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****

interface Tunnel1
 description VTI Tunnel with Extranet ASA
 nameif VTI-ASA
 ip address 192.168.100.1 255.255.255.252
 tunnel source interface Outside
 tunnel destination 10.106.67.252
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
```

---

Les noms réels des objets et les numéros de stratégie varient selon le déploiement FMC.

---

# Vérifier

## À partir de FMC GUI

1. Ouvrez Périphériques > VPN > Site à site et sélectionnez la topologie.
2. Utilisez Check Status ou le tableau de bord de surveillance site à site pour afficher l'état du tunnel.

---



Remarque : L'état du tunnel VPN FMC ne peut pas être mis à jour en temps réel sur toutes les versions (des intervalles de plusieurs minutes ont été documentés). Vérifiez avec CLI si l'interface utilisateur graphique présente un état ambigu. Vérifications CLI équivalentes (il est possible que FMC puisse les exécuter pour l'état).

---

```
show crypto ipsec sa peer <Peer_IP>
show vpn-sessiondb detail l2l filter ipaddress <Peer_IP>
```

---

## À partir de FTD CLI

```
show running-config crypto
show running-config interface Tunnel
show running-config route
show crypto ikev2 sa detailed
show crypto ipsec sa detailed
show crypto ipsec sa peer <Peer_IP>
show vpn-sessiondb detail l2l
show vpn-sessiondb detail l2l filter ipaddress <Peer_IP>
```

---

Pour les homologues existants qui utilisent toujours IKEv1 :

```
show crypto ikev1 sa detailed
```

---

Vérification du routage :

```
show route
show bgp summary
show ospfv3 neighbor
```

---

Remplacez les commandes par celles qui correspondent à votre protocole de routage configuré.

## Guide de référence rapide du dépannage

| Symptôme | Cause Commune | Action |
|---|---|---|
| Échec IKE | Non-concordance PSK, UDP 500/4500 bloqué, non-concordance de chiffrement | Comparer la politique/proposition IKE avec l'homologue ; vérification de NAT-T |
| IPsec activé, aucun trafic | Règle ACP manquante | Ajouter des règles d'autorisation pour la zone VTI dans les deux directions |
| IPsec activé, aucun trafic | Route statique manquante ou incorrecte | Vérifier la route via VTI vers le réseau protégé à distance |
| Désactivation du tunnel après la mise à niveau FMC | Chiffres faibles supprimés | Reconfigurer IKE/IPsec avec AES-256/SHA-256+ |
| BGP n'appairage pas sur VTI | TTL/zone de sécurité | Définir le saut de durée de vie > 1 ; Vérifier l'accessibilité IP VTI |
| L'interface utilisateur graphique s'affiche, l'interface CLI apparaît | Délai d'actualisation du statut FMC | Utiliser CLI ; redéployer en cas d'obsolescence |

## Documents associés

- Configuration du tunnel VPN site à site basé sur la route sur FTD géré par FMC (Cisco.com) — ID de document 216276
- Configuration de DVTI avec Multi-SA sur Secure Firewall — ID de document 220322
- Guide de configuration des périphériques FMC 7.6 - VPN de site à site
- Exemple d'utilisation DVTI — Hub and Spoke avec OSPF/BGP
- Instructions relatives aux interfaces de tunnel virtuel (Defense Orchestrator / FMC)
- Configuration de la transmission tunnel partagée dynamique ASA/AnyConnect (référence pour les concepts de routage FQDN)

---

## Historique de révision

| Révision | Date | Commentaires |
|---|---|---|
| 7.0 | 28-juil-2026 | Mise à jour complète : Marquage du pare-feu sécurisé, limitations 7.x (échelle VTI OSPF/EIGRP/IPv6/1024), liaisons croisées DVTI, accent ACP, fautes de frappe corrigées, vérification/dépannage étendu |
| 6.0 | 24/09/2024 | Présentation et mise en forme mises à jour (Cisco.com) |
| 5.0 | 27-juin-2024 | Limitations et mise à jour des références DVTI (Cisco.com) |
| 1.0 | 23-nov-2020 | Première publication |

---

## Le document s'applique

- Cisco Secure Firewall Threat Defense (FTD)
- Cisco Secure Firewall Management Center (FMC)
- VPN site à site basé sur la route statique (SVTI)
- Homologues extranet (ASA, périphériques IPsec tiers)

---

Ne couvre pas : VTI de cluster FTD, tunnels GRE ou procédure Hub and Spoke DVTI complète (voir Document ID 220322.)

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.