

# Configurer un VPN site à site sur FTD géré par FDM

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Définition des réseaux protégés](#)

[Configuration d'un VPN site à site](#)

[Configuration ASA](#)

[Vérifier](#)

[Dépannage](#)

[Problèmes de connectivité initiaux](#)

[Problèmes spécifiques au trafic](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit comment configurer un VPN site à site sur Firepower Threat Defense (FTD) géré par FirePower Device Manager (FDM).

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base du VPN
- Expérience avec FDM
- Expérience avec la ligne de commande ASA (Adaptive Security Appliance)

### Composants utilisés

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

- Cisco FTD 6.5
- ASA 9.10(1)32
- IKEv2

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.

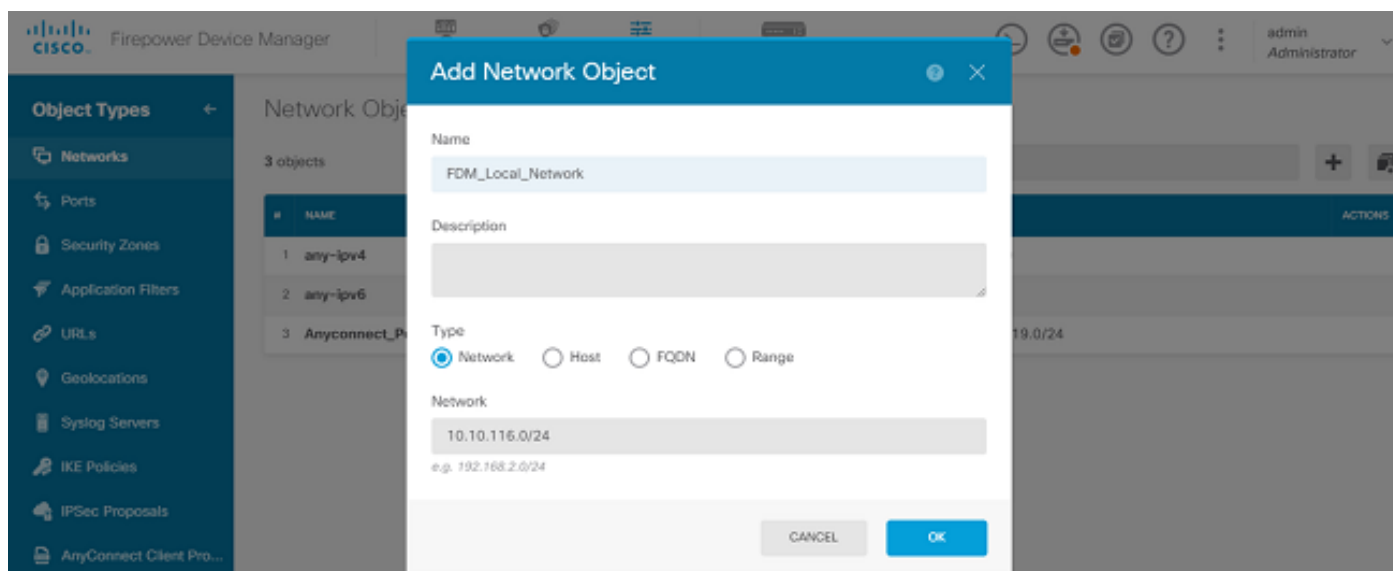
## Configurer

Commencez par la configuration sur FTD avec FDM.

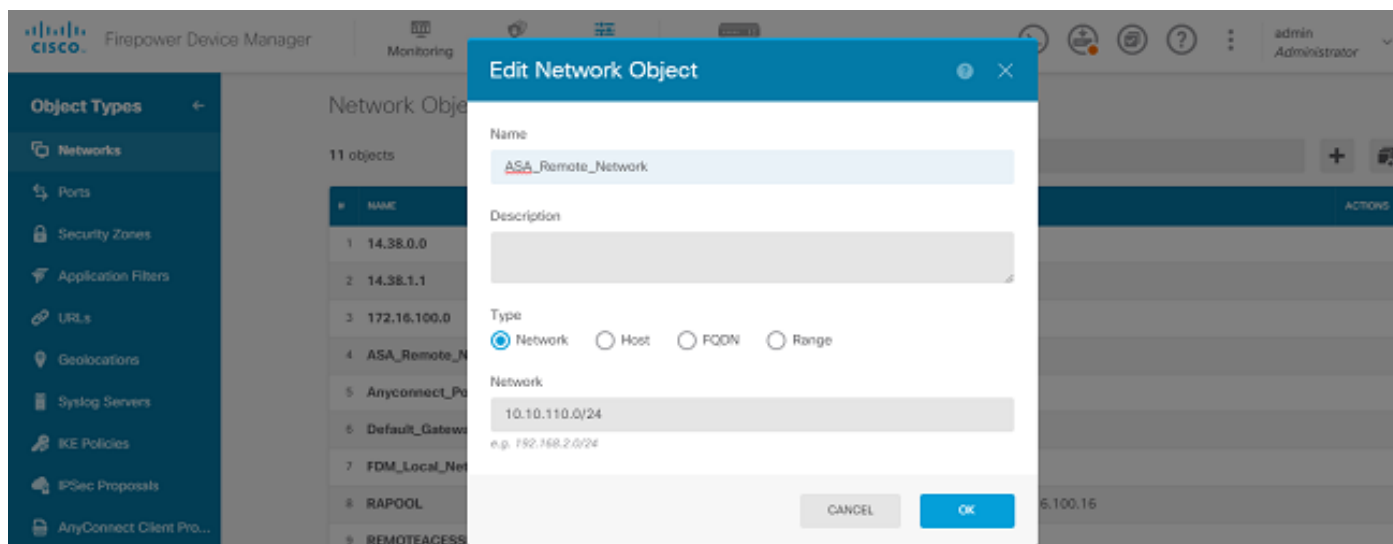
### Définition des réseaux protégés

Accédez à Objets > Réseaux > Ajouter un nouveau réseau.

Configurez les objets pour les réseaux LAN à partir de l'interface utilisateur FDM. Créez un objet pour le réseau local derrière le périphérique FDM, comme illustré dans l'image.



Créez un objet pour le réseau distant derrière le périphérique ASA, comme illustré dans l'image.



## Configuration d'un VPN site à site

Accédez à Site-to-Site VPN > Create Site-to-Site Connection.

Suivez les instructions de l'assistant Site-to-Site sur FDM, comme illustré dans l'image.

The screenshot displays the Cisco Firepower Device Manager (FDM) interface. At the top, the navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: firepower'. The main content area shows a network diagram with an 'Inside Network' connected to a 'Cisco Firepower Threat Defense for VMWa...' device. The device has interfaces 0/0, 0/1, 0/2, and 0/5. It is connected to an 'ISP/WAN/Gateway' which is in turn connected to an 'Internet' cloud. Services like 'DNS Server', 'NTP Server', and 'Smart License' are shown on the Internet side.

Below the diagram is a grid of configuration cards:

- Interfaces:** Connected, Enabled 3 of 4. [View All Interfaces](#)
- Smart License:** Registered. [View Configuration](#)
- Site-to-Site VPN:** There are no connections yet. [View Configuration](#) (highlighted with a red box)
- Remote Access VPN:** Configured, 1 connection | 1 Group Policy. [View Configuration](#)
- Advanced Configuration:** Includes: FlexConfig, Smart CLI. [View Configuration](#)
- System Settings:** Management Access, Logging Settings, DHCP Server, DNS Server, Management Interface, Hostname, NTP, Cloud Services, Reboot/Shutdown, Traffic Settings, URL Filtering Preferences.

At the bottom, the 'Device Summary' page for 'Site-to-Site VPN' is shown. It features a search bar and a table with columns: #, NAME, LOCAL INTERFACE, LOCAL NETWORKS, REMOTE NETWORKS, NAT EXEMPT, ICE V1, ICE V2, and ACTIONS. The table is currently empty, and a message states: 'There are no Site-to-Site connections yet. Start by creating the first Site-to-Site connection.' A red box highlights the 'CREATE SITE-TO-SITE CONNECTION' button.

Attribuez à la connexion site à site un nom de profil de connexion facilement identifiable.

Choisissez l'interface externe correcte pour le FTD, puis choisissez le réseau local qui doit être chiffré sur le VPN site à site.

Définissez l'interface publique de l'homologue distant. Sélectionnez ensuite le réseau d'homologues distants qui est chiffré sur le VPN site à site, comme illustré dans l'image.

## Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name

RTPVPN-ASA

**LOCAL SITE**

Local VPN Access Interface

outside (GigabitEthernet0/0)

Local Network

+ FDM\_Local\_Network

**REMOTE SITE**

Static  Dynamic

Remote IP Address

14.36.137.82

Remote Network

+ ASA\_Remote\_Network

CANCEL NEXT

Sur la page suivante, choisissez le bouton Edit pour définir les paramètres Internet Key Exchange (IKE) comme indiqué dans l'image.

## IKE Policy

**i** IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

IKE Version 2



IKE Policy

Globally applied

EDIT...

IKE Version 1



IPSec Proposal

Custom set selected

EDIT...

Cliquez sur le bouton Create New IKE Policy comme indiqué dans l'image.

Filter

AES-GCM-NULL-SHA i

AES-SHA-SHA i

DES-SHA-SHA i

Create New IKE Policy

OK

Ce guide utilise les paramètres suivants pour l'échange initial IKEv2 :

Cryptage AES-256

Intégrité SHA256

Groupe DH 14

PRF SHA256

# Add IKE v2 Policy



Priority

1

Name

RTPVPN-ASA

State



Encryption

AES256 ×



Diffie-Hellman Group

14 ×



Integrity Hash

SHA256 ×



Pseudo Random Function (PRF) Hash

SHA256 ×



Lifetime (seconds)

86400

*Between 120 and 2147483647 seconds.*

CANCEL

OK

Une fois de retour sur la page principale, choisissez le bouton Edit pour la proposition IPsec. Créez une nouvelle proposition IPsec comme illustré dans l'image.

# Select IPSec Proposals



Filter

SET DEFAULT

 AES-GCM *in Default Set*



 AES-SHA



 DES-SHA-1



Create new IPSec Proposal

CANCEL

OK

Ce guide utilise les paramètres suivants pour IPSec :

Cryptage AES-256

Intégrité SHA256

## Add IKE v2 IPsec Proposal



Name

ASA-IPSEC

Encryption

AES256

Integrity Hash

SHA256

CANCEL

OK

Définissez l'authentification sur clé pré-partagée et saisissez la clé pré-partagée (PSK) utilisée aux deux extrémités. Dans ce guide, le PSK de Cisco est utilisé comme illustré dans l'image.



## Authentication Type

Pre-shared Manual Key

Certificate

## Local Pre-shared Key

•••••

## Remote Peer Pre-shared Key

•••••

Définissez l'interface NAT Exempt interne. Si plusieurs interfaces internes sont utilisées, une règle NAT Exempt manuelle doit être créée sous Politiques > NAT.

---

### Additional Options

#### NAT Exempt

inside (GigabitEthernet0/1) ▼ ⓘ

#### Diffie-Hellman Group for Perfect Forward Secrecy

No Perfect Forward Secrecy (turned off) ▼ ⓘ

---

BACK

NEXT

Sur la dernière page, un résumé de la connexion de site à site s'affiche. Assurez-vous que les adresses IP correctes sont sélectionnées et que les paramètres de cryptage appropriés sont

utilisés, puis cliquez sur le bouton Terminer. Déployez le nouveau VPN de site à site.

La configuration ASA est complétée par l'utilisation de l'interface de ligne de commande.

## Configuration ASA

1. Activez IKEv2 sur l'interface externe de l'ASA :

```
Crypto ikev2 enable outside
```

2. Créez la stratégie IKEv2 qui définit les mêmes paramètres configurés sur le FTD :

```
Crypto ikev2 policy 1  
Encryption aes-256  
Integrity sha256  
Group 14  
Prf sha256  
Lifetime seconds 86400
```

3. Créez une stratégie de groupe qui autorise le protocole IKEv2 :

```
Group-policy FDM_GP internal  
Group-policy FDM_GP attributes  
Vpn-tunnel-protocol ikev2
```

4. Créez un groupe de tunnels pour l'adresse IP publique FTD homologue. Faites référence à la stratégie de groupe et spécifiez la clé pré-partagée :

```
Tunnel-group 172.16.100.10 type ipsec-l2l  
Tunnel-group 172.16.100.10 general-attributes  
Default-group-policy FDM_GP  
Tunnel-group 172.16.100.10 ipsec-attributes  
ikev2 local-authentication pre-shared-key cisco  
ikev2 remote-authentication pre-shared-key cisco
```

5. Créez une liste de contrôle d'accès définissant le trafic à chiffrer : (FTDSubnet 10.10.116.0/24)

(ASASubnet 10.10.110.0/24) :

```
Object network FDMSubnet
  Subnet 10.10.116.0 255.255.255.0
Object network ASASubnet
  Subnet 10.10.110.0 255.255.255.0
Access-list ASAtoFTD extended permit ip object ASASubnet object FTDSubnet
```

6. Créez une proposition IKEv2 IPsec qui fait référence aux algorithmes spécifiés sur le FTD :

```
Crypto ipsec ikev2 ipsec-proposal FDM
  Protocol esp encryption aes-256
  Protocol esp integrity sha-256
```

7. Créez une entrée de crypto-carte qui lie la configuration :

```
Crypto map outside_map 20 set peer 172.16.100.10
Crypto map outside_map 20 match address ASAtoFTD
Crypto map outside_map 20 set ikev2 ipsec-proposal FTD
Crypto map outside_map 20 interface outside
```

8. Créez une instruction d'exemption NAT qui empêche le trafic VPN d'être NATTED par le pare-feu :

```
Nat (inside,outside) 1 source static ASASubnet ASASubnet destination static FDMSubnet FDMSubnet
no-proxy-arp route-lookup
```

## Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Tentative d'initialisation du trafic via le tunnel VPN. Avec l'accès à la ligne de commande de l'ASA ou du FTD, cela peut être fait avec la commande `packet tracer`. Lorsque vous utilisez la commande `packet-tracer` pour activer le tunnel VPN, il doit être exécuté deux fois afin de vérifier si le tunnel s'active. La première fois que la commande est émise, le tunnel VPN est hors service et

la commande packet-tracer échoue avec VPN encrypt DROP. N'utilisez pas l'adresse IP interne du pare-feu comme adresse IP source dans le traceur de paquets car cela échoue toujours.

```
firepower# packet-tracer input inside icmp 10.10.116.10 8 0 10.10.110.10
```

```
Phase: 9
Type: VPN
Subtype: encrypt
Result: DROP
Config:
Additional Information:
```

```
firepower# packet-tracer input inside icmp 10.10.116.10 8 0 10.10.110.10
```

```
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 172.16.100.1 using egress ifc outside
```

```
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static |s2sAc1SrcNwgV4|c9911223-779d-11ea-9c1b-5ddd47126971 |s2sAc1SrcNwgV4
Additional Information:
NAT divert to egress interface outside
Untranslate 10.10.110.10/0 to 10.10.110.10/0
```

```
Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group NGFW_ONBOX_ACL global
access-list NGFW_ONBOX_ACL advanced trust object-group |acSvcg-268435457 ifc inside any ifc outside any
access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy
access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule
object-group service |acSvcg-268435457
service-object ip
Additional Information:
```

```
Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static |s2sAc1SrcNwgV4|c9911223-779d-11ea-9c1b-5ddd47126971 |s2sAc1SrcNwgV4
Additional Information:
Static translate 10.10.116.10/0 to 10.10.116.10/0
```

```
Phase: 9
Type: VPN
Subtype: encrypt
Result: ALLOW
```

Config:  
Additional Information:

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

Afin de surveiller l'état du tunnel, accédez à l'interface de ligne de commande du FTD ou de l'ASA.

À partir de l'interface de ligne de commande FTD, vérifiez les phases 1 et 2 à l'aide de la commande `show crypto ikev2 sa`.

```
> show crypto ikev2 sa
```

IKEv2 SAs:

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

```
Tunnel-id Local Remote
3821043 172.16.100.10/500 192.168.200.10/500
    Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
    Life/Active Time: 86400/1150 sec
Child sa: local selector 10.10.116.0/0 - 10.10.116.255/65535
          remote selector 10.10.110.0/0 - 10.10.110.255/65535
          ESP spi in/out: 0x7398dcbd/0x2303b0c0
```

## Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

### Problèmes de connectivité initiaux

Lorsque vous créez un VPN, deux parties négocient le tunnel. Par conséquent, il est préférable d'obtenir les deux côtés de la conversation lorsque vous dépannez tout type de défaillance de tunnel. Un guide détaillé sur la façon de déboguer les tunnels IKEv2 peut être trouvé ici :

[Comment déboguer les VPN IKEv2](#)

La cause la plus fréquente des pannes de tunnel est un problème de connectivité. La meilleure façon de déterminer ceci est de prendre des captures de paquets sur le périphérique.

Utilisez cette commande pour effectuer des captures de paquets sur le périphérique :

Capture capout interface outside match ip host 172.16.100.10 host 192.168.200.10

Une fois la capture en place, essayez d'envoyer le trafic sur le VPN et vérifiez le trafic bidirectionnel dans la capture de paquets.

Examinez la capture de paquets avec la commande show cap capout.

```
firepower# show cap capout
```

```
4 packets captured
```

```
1: 01:21:06.763983      172.16.100.10.500 > 192.168.200.10.500:  udp 574
2: 01:21:06.769415      192.168.200.10.500 > 172.16.100.10.500:  udp 619
3: 01:21:06.770666      172.16.100.10.500 > 192.168.200.10.500:  udp 288
4: 01:21:06.773748      192.168.200.10.500 > 172.16.100.10.500:  udp 256
```

## Problèmes spécifiques au trafic

Les problèmes de trafic courants rencontrés par les utilisateurs sont les suivants :

- Problèmes de routage derrière le FTD : le réseau interne ne peut pas router les paquets vers les adresses IP et les clients VPN attribués.
- Listes de contrôle d'accès bloquant le trafic.
- La traduction d'adresses de réseau (NAT) n'est pas contournée pour le trafic VPN.

## Informations connexes

Pour plus d'informations sur les VPN de site à site sur le FTD géré par FDM, vous pouvez trouver le guide de configuration complet [ici](#).

- [Guide de configuration FTD géré par FDM](#).

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.