

Configurer un VPN site à site basé sur la route et sensible au VRF sur FTD géré par FDM

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configuration du FTD](#)

[Configuration de l'ASA](#)

[Vérifier](#)

[Dépannage](#)

[Référence](#)

Introduction

Ce document décrit comment configurer un VPN de site à site basé sur route compatible VRF sur FTD géré par FDM.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base du VPN
- Compréhension de base du routage et du transfert virtuels (VRF)
- Expérience avec FDM

Composants utilisés

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

- Cisco FTDv version 7.4.2
- Cisco FDM version 7.4.2
- Cisco ASAv version 9.20.3

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.

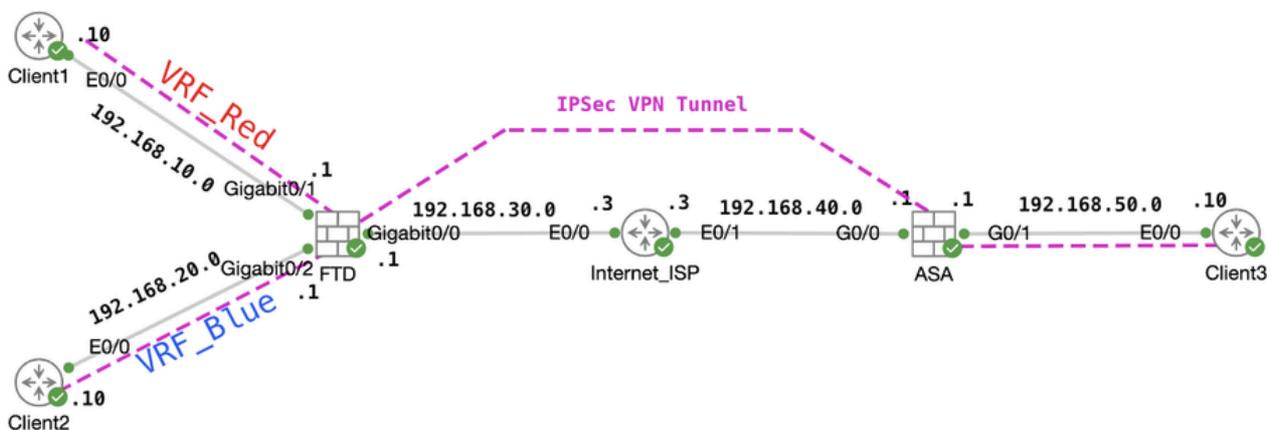
Informations générales

Virtual Routing and Forwarding (VRF) sur Firepower Device Manager (FDM) vous permet de créer plusieurs instances de routage isolées sur un seul périphérique Firepower Threat Defense (FTD). Chaque instance VRF fonctionne comme un routeur virtuel distinct avec sa propre table de routage, ce qui permet une séparation logique du trafic réseau et offre des fonctionnalités de sécurité et de gestion du trafic améliorées.

Ce document explique comment configurer un VPN IPsec compatible VRF avec VTI. Le réseau VRF rouge et le réseau VRF bleu sont derrière le FTD. Le Client1 dans le réseau VRF Rouge et le Client2 dans le réseau VRF Bleu communiqueraient avec le Client 3 derrière l'ASA via le tunnel VPN IPsec.

Configurer

Diagramme du réseau

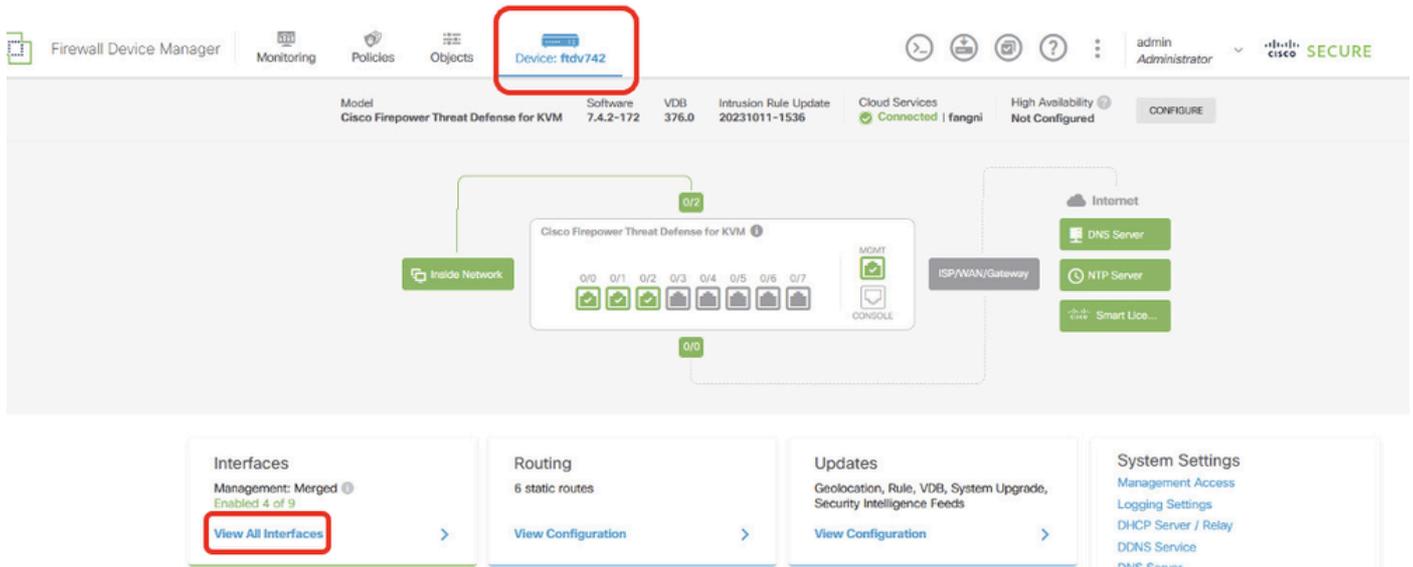


Topologie

Configuration du FTD

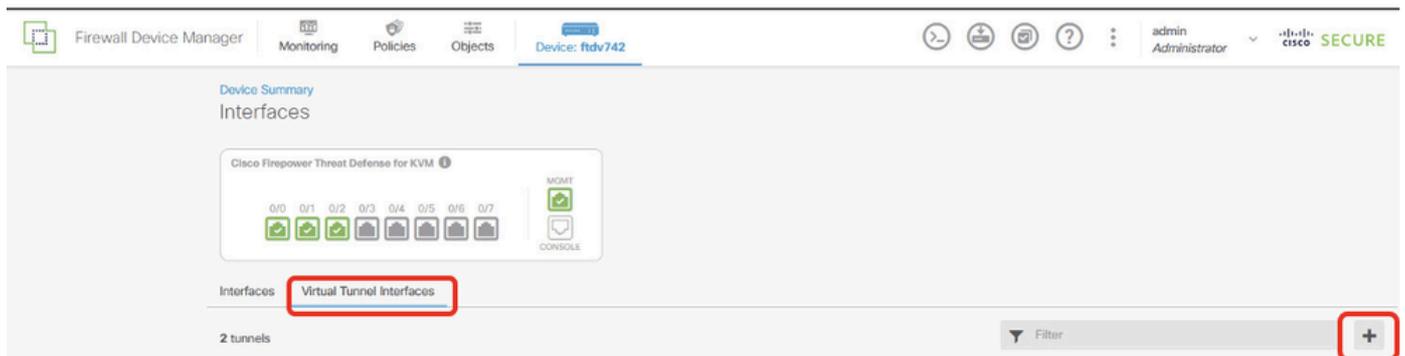
Étape 1. Il est essentiel de s'assurer que la configuration préliminaire de l'interconnectivité IP entre les noeuds a été dûment effectuée. Le Client1 et le Client2 utilisent l'adresse IP interne FTD comme passerelle. Le Client3 utilise l'adresse IP interne ASA comme passerelle.

Étape 2. Créer une interface de tunnel virtuelle. Connectez-vous à l'interface utilisateur graphique FDM de FTD. Accédez à Device > Interfaces. Cliquez sur View All Interfaces .



FTD_View_Interfaces

Étape 2.1. Cliquez sur l'onglet Virtual Tunnel Interfaces. Cliquez sur le bouton +.



FTD_Create_VTI

Étape 2.2. Fournir les informations nécessaires. Cliquez sur le bouton OK.

- Name : demovti
- ID de tunnel : 1
- Source du tunnel : externe (GigabitEthernet0/0)
- Adresse IP et masque de sous-réseau : 169.254.10.1/24
- État : cliquez sur le curseur jusqu'à la position Activé

Name
demovti

Status

Most features work with named interfaces only, although some require unnamed interfaces.

Description

Tunnel ID ⓘ
1

0 - 10413

Tunnel Source ⓘ
outside (GigabitEthernet0/0)

IP Address and Subnet Mask

169.254.10.1 / 24

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

CANCEL

OK

FTD_Create_VTI_Details

Étape 3. Accédez à Device > Site-to-Site VPN . Cliquez sur le bouton View Configuration.

Firewall Device Manager

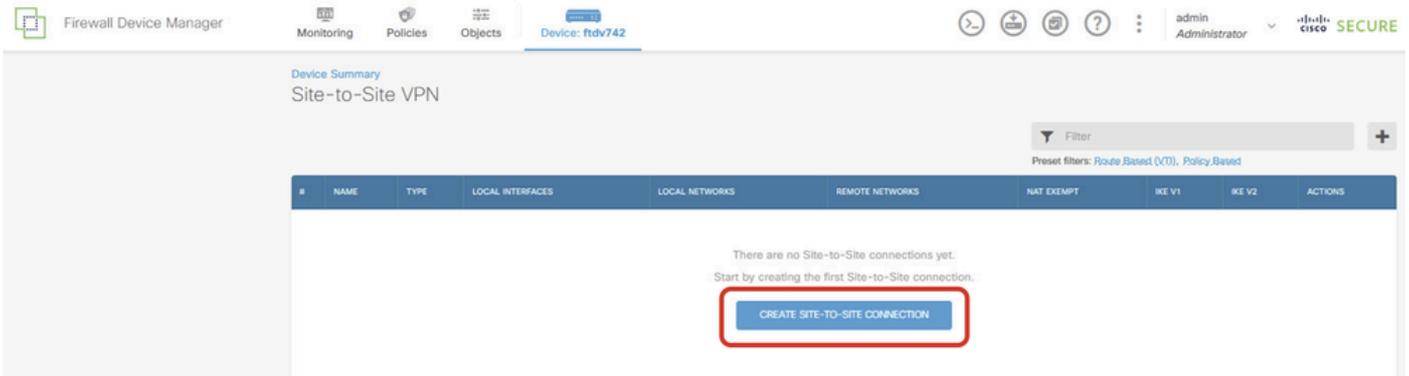
Monitoring Policies Objects **Device: ftdv742**

Model: Cisco Firepower Threat Defense for KVM | Software: 7.4.2-172 | VDB: 376.0 | Intrusion Rule Update: 20231011-1536 | Cloud Services: Issues | Unknown | High Availability: Not Configured

Inside Network | Cisco Firepower Threat Defense for KVM | ISP/WAN Gateway | Internet (DNS Server, NTP Server, Smart Lic...)

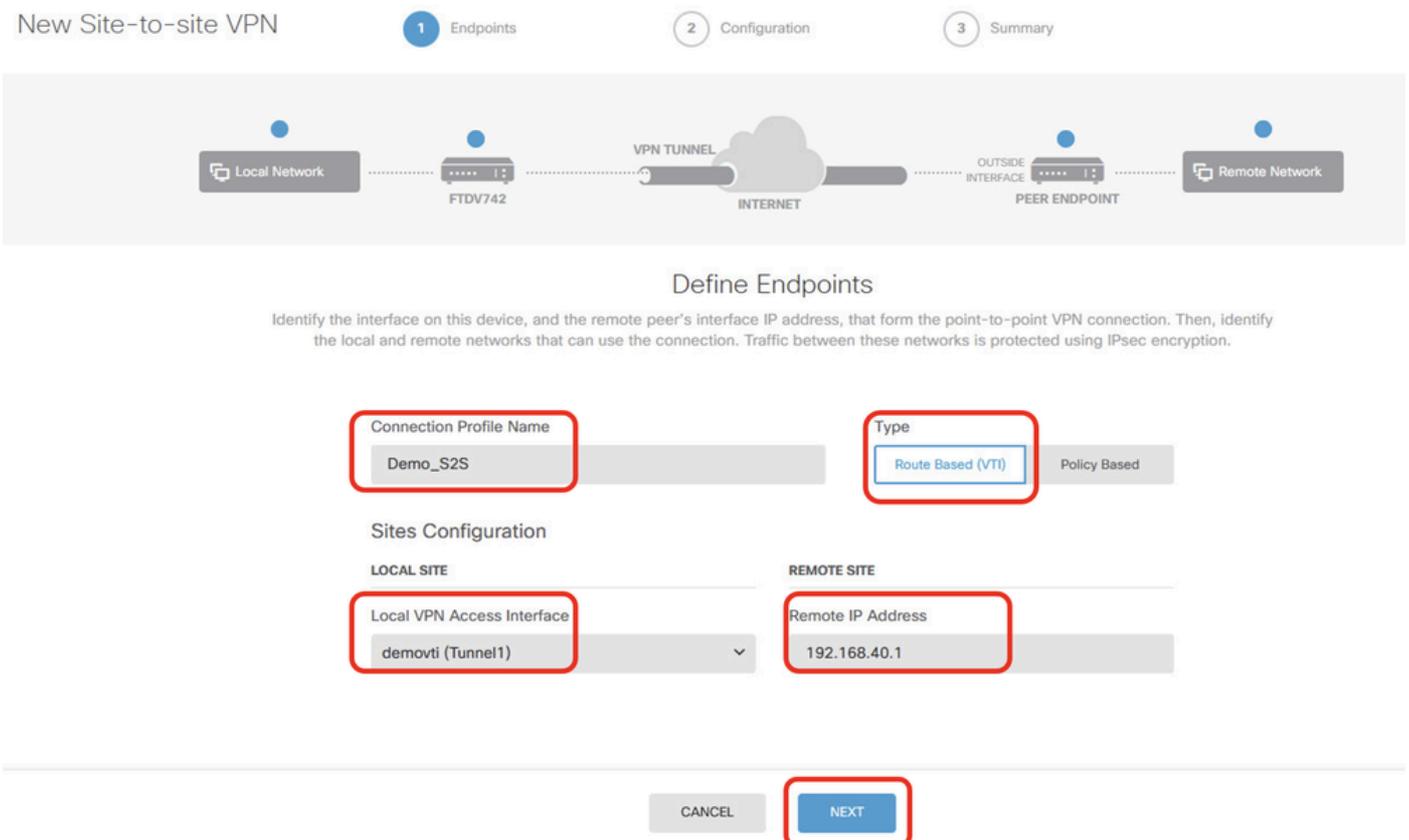
Interfaces Management: Merged ⓘ Enabled 4 of 9 View All Interfaces	Routing 1 static route View Configuration	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	System Settings Management Access Logging Settings DHCP Server / Relay DDNS Service DNS Server Hostname Time Services SSL Settings See more
Smart License Registered Tier: FTDv50 - 10 Gbps View Configuration	Backup and Restore View Configuration	Troubleshoot No files created yet REQUEST FILE TO BE CREATED	
Site-to-Site VPN There are no connections yet View Configuration	Remote Access VPN Requires Secure Client License No connections 1 Group Policy Configure	Advanced Configuration Includes: FlexConfig, Smart CLI View Configuration	Device Administration Audit Events, Deployment History, Download Configuration View Configuration

Étape 3.1. Commencez à créer un nouveau VPN site à site. Cliquez sur le bouton CREATE SITE-TO-SITE CONNECTION. Ou cliquez sur le bouton +.

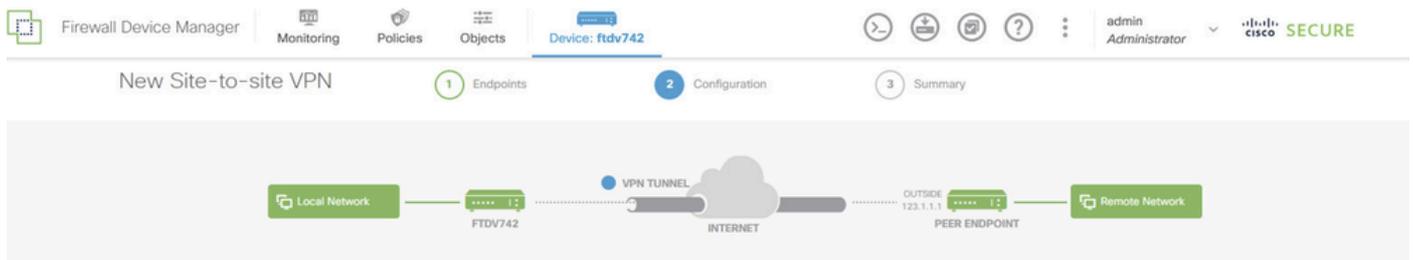


Étape 3.2. Fournir les informations nécessaires. Cliquez sur le bouton NEXT.

- Nom du profil de connexion : Démo_S2S
- type : Basé sur la route (VTI)
- Local VPN Access Interface : demovti (créé à l'étape 2)
- Adresse IP distante : 192.168.40.1 (il s'agit de l'adresse IP externe ASA homologue)



Étape 3.3. Accédez à IKE Policy. Cliquez sur le bouton EDIT.



Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

IKE Policy

1 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 VERSION 1

IKE Policy

Globally applied

IPSec Proposal

None selected 

FTD_Edit_IKE_Policy

Étape 3.4. Pour la stratégie IKE, vous pouvez utiliser des paramètres prédéfinis ou en créer un nouveau en cliquant sur **Créer une nouvelle stratégie IKE** .

Dans cet exemple, basculez un nom de stratégie IKE existant AES-SHA-SHA . Cliquez sur le bouton OK pour enregistrer.

Filter

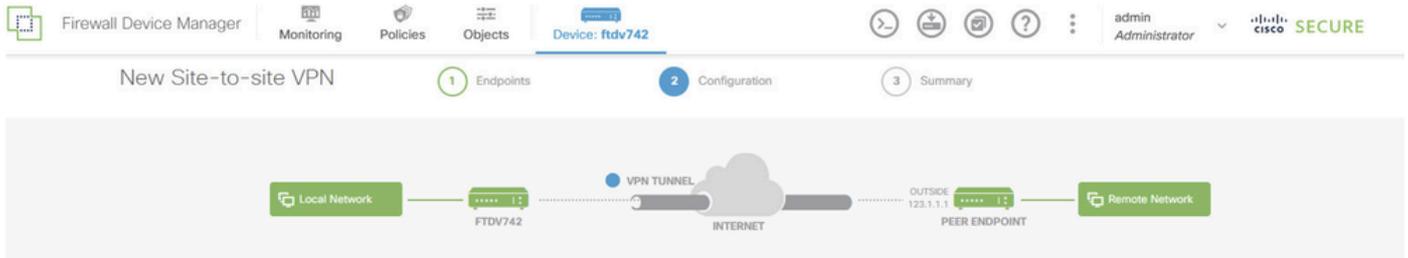
<input type="checkbox"/>	AES-GCM-NULL-SHA	i
<input checked="" type="checkbox"/>	AES-SHA-SHA	i
<input type="checkbox"/>	DES-SHA-SHA	i

Create New IKE Policy

OK

FTD_Enable_IKE_Policy

Étape 3.5. Accédez à la proposition IPSec. Cliquez sur le bouton EDIT.



Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

IKE Policy

1 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 VERSION 1

IKE Policy

Globally applied

IPSec Proposal

None selected 1

FTD_Edit_IPSec_Proposal

Étape 3.6. Pour les propositions IPSec, vous pouvez utiliser des propositions prédéfinies ou en créer une nouvelle en cliquant sur Créer une nouvelle proposition IPSec .

Dans cet exemple, basculez un nom de proposition IPSec existant AES-SHA . Cliquez OK pour l'enregistrer.

Select IPsec Proposals



Filter

SET DEFAULT

 AES-GCM *In Default Set* 



AES-SHA



DES-SHA-1



[Create new IPsec Proposal](#)

CANCEL

OK

FTD_Enable_IPsec_Proposal

Étape 3.7. Faites défiler la page vers le bas et configurez la clé pré-partagée. Cliquez sur NEXT .

Notez cette clé pré-partagée et configurez-la sur ASA ultérieurement.

Firewall Device Manager | Monitoring | Policies | Objects | Device: ftdv742 | admin Administrator | Cisco Security

FTDV742 | INTERNET | PEER ENDPOINT

Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

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 VERSION 1

IKE Policy
Globally applied

IPSec Proposal
Custom set selected

Authentication Type
 Pre-shared Manual Key Certificate

Local Pre-shared Key

Remote Peer Pre-shared Key

FTD_Configure_Pre_Shared_Key

Étape 3.8. Révision de la configuration VPN Si vous devez modifier quelque chose, cliquez sur le bouton BACK. Si tout va bien, cliquez sur le bouton FINISH.

Demo_S2S Connection Profile

Peer endpoint needs to be configured according to specified below configuration.

VPN Access Interface demovti (169.254.10.1) ↔ **Peer IP Address** 192.168.40.1

IKE V2

IKE Policy aes,aes-192,aes-256-sha512,sha384,sha,sha256-sha512,sha384,sha,sha256-21,20,16,15,14

IPSec Proposal aes,aes-192,aes-256-sha-512,sha-384,sha-256,sha-1

Authentication Type Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

Lifetime Duration 28800 seconds

Lifetime Size 4608000 kilobytes

ADDITIONAL OPTIONS

Information is copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

Diffie-Hellman: Null (not selected)

Group:

BACK **FINISH**

FTD_Review_VPN_Configuration

Étape 3.9. Créer une règle de contrôle d'accès pour permettre au trafic de traverser le FTD. Dans cet exemple, autoriser tout pour la démonstration. Veuillez modifier votre politique en fonction de vos besoins réels.

Firewall Device Manager | Monitoring | Policies | Objects | Device: ftdv742 | admin Administrator | CISCO SECURE

Security Policies

SSL Decryption → Identity → Security Intelligence → NAT → Access Control → Intrusion

1 rule

#	NAME	ACTION	SOURCE			DESTINATION			APPLICATIONS	URLS	USERS	ACTIONS
			ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS				
1	Demo_allow	Allow	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY		

Default Action: Access Control **Block**

FTD_ACP_Example

Étape 3.10. (Facultatif) Configurez la règle d'exemption NAT pour le trafic client sur FTD si une

NAT dynamique est configurée pour que le client accède à Internet. Dans cet exemple, il n'est pas nécessaire de configurer une règle d'exemption NAT, car aucune NAT dynamique n'est configurée sur FTD.

Étape 3.11. Déployez les modifications de configuration.



FTD_Deployment_Changes

Étape 4 : configuration des routeurs virtuels

Étape 4.1. Créer des objets réseau pour la route statique. Accédez à Objets > Réseaux, cliquez sur + bouton.



FTD_Create_NetObjects

Étape 4.2. Fournissez les informations nécessaires sur chaque objet réseau. Cliquez sur le bouton OK.

- Name : local_blue_192.168.20.0
- type : Réseau
- Réseau: 192.168.20.0/24

Add Network Object



Name

local_blue_192.168.20.0

Description

Type



Network



Host

Network

192.168.20.0/24

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

FTD_VRF_Blue_Network

- Name : local_red_192.168.10.0
- type : Réseau
- Réseau: 192.168.10.0/24

Add Network Object



Name

local_red_192.168.10.0

Description

Type



Network



Host

Network

192.168.10.0/24

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

FTD_VRF_Red_Network

- Name : remote_192.168.50.0
- type : Réseau
- Réseau: 192.168.50.0/24

Add Network Object



Name

remote_192.168.50.0

Description

Type



Network



Host



FQDN



Range

Network

192.168.50.0/24

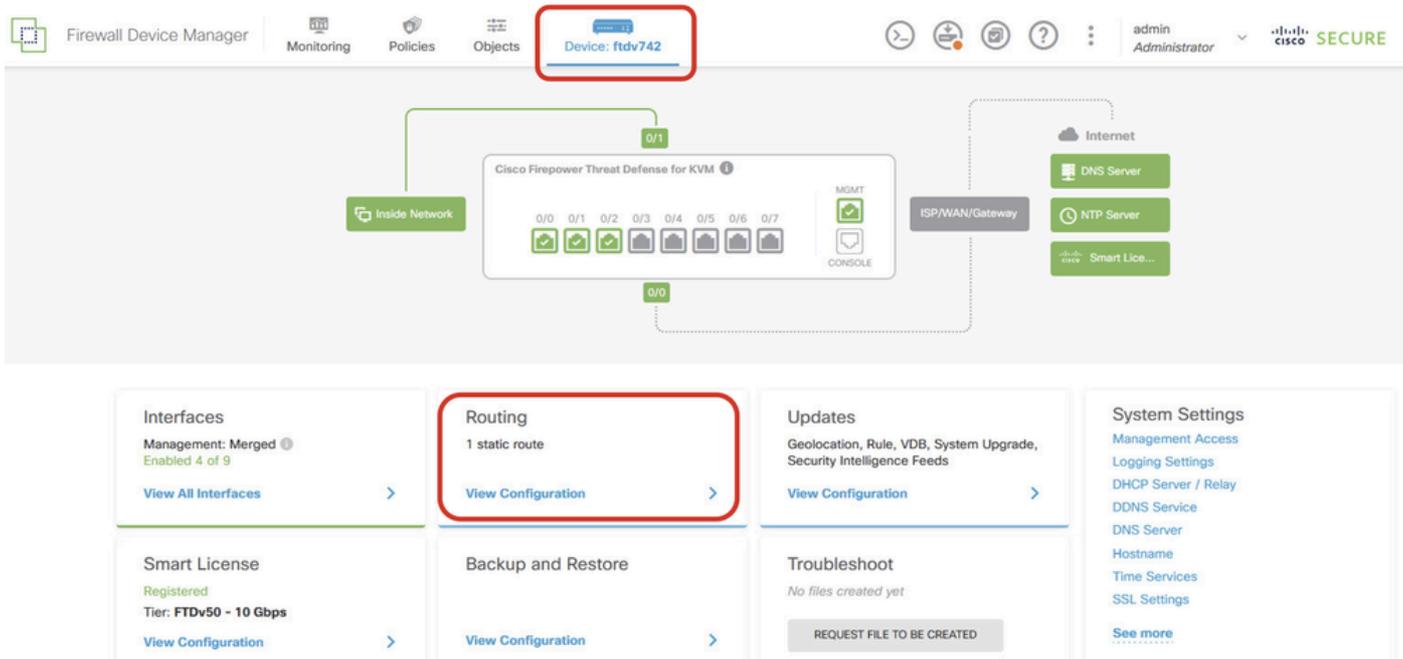
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

FTD_Réseau_Distant

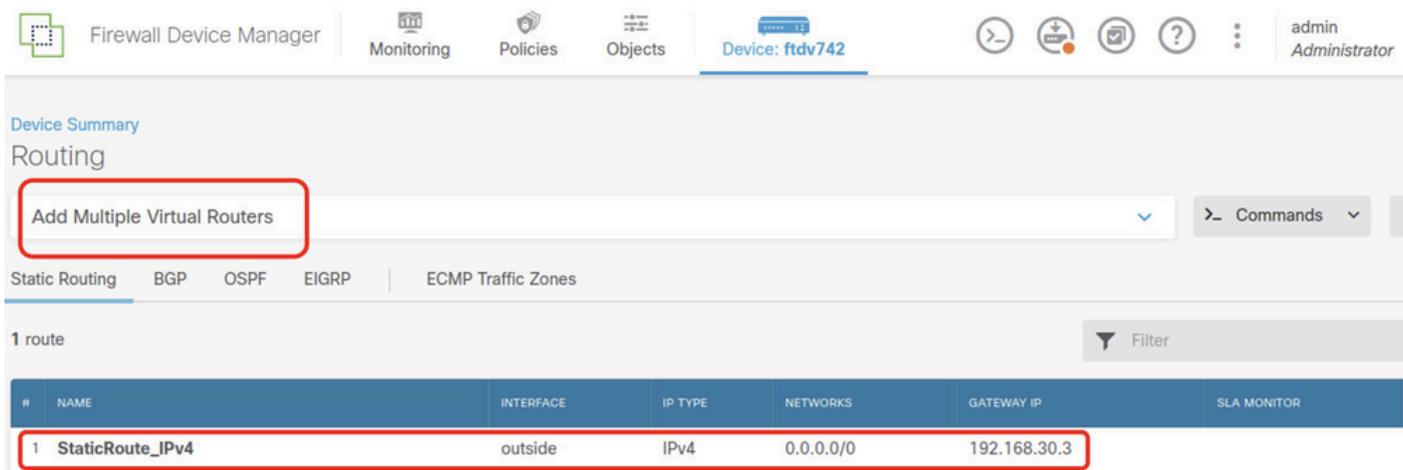
Étape 4.3. Création du premier routeur virtuel Accédez à Device > Routing . Cliquez sur Afficher la configuration .



FTD_View_Routing_Configuration

Étape 4.4. Cliquez sur Add Multiple Virtual Routers .

Remarque : une route statique via l'interface externe a déjà été configurée lors de l'initialisation de FDM. Si vous ne l'avez pas, configurez-le manuellement.



FTD_Add_First_Virtual_Router1

Étape 4.5. Cliquez sur CREATE FIRST CUSTOM VIRTUAL ROUTER .

Firewall Device Manager | Monitoring | Policies | Objects | Device: ftdv742 | admin Administrator

Device Summary

Routing

Virtual Route Forwarding (Virtual Routing) Description

You can create multiple virtual routing and forwarding instances, called virtual routers, to maintain separate routing tables for groups of interfaces. Because each virtual router has its own routing table, you can provide clean separation in the traffic flowing through the device.

Thus, you can provide support to two or more distinct customers over a common set of networking equipment. You can also use virtual routers to provide more separation for elements of your own network, for example, by isolating a development network from your general-purpose corporate network.

How Multiple Virtual Routers Work

Multiple Virtual Router mode is enabled automatically if there is at least one custom Virtual Router.

Diagram description: A central 'THREAT DEFENSE' module is connected to three 'VIRTUAL ROUTER' instances (A, B, N). Each virtual router is connected to two customer networks (e.g., CUSTOMER A NETWORK 1 and 2). A red box highlights the 'CREATE FIRST CUSTOM VIRTUAL ROUTER' button at the bottom.

Commands

FTD_Add_First_Virtual_Router2

Étape 4.6. Fourniture des informations nécessaires sur le premier routeur virtuel Cliquez sur le bouton OK. Après la première création du routeur virtuel, un nom de vrf Global s'afficherait automatiquement.

- Name : vrf_rouge
- Interfaces: inside_red (GigabitEthernet0/1)

Firewall Device Manager | admin Administrator

Device Summary

Routing

Add Virtual Router

Name: vrf_red

Description:

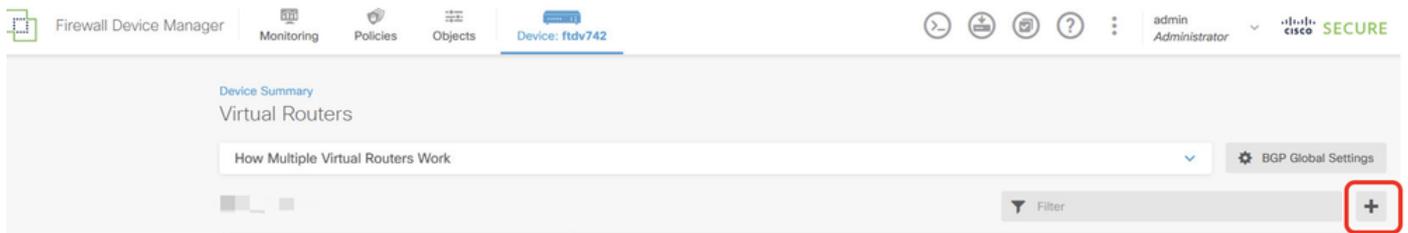
Interfaces: inside_red (GigabitEthernet0/1)

CANCEL OK

CREATE FIRST CUSTOM VIRTUAL ROUTER

FTD_Add_First_Virtual_Router3

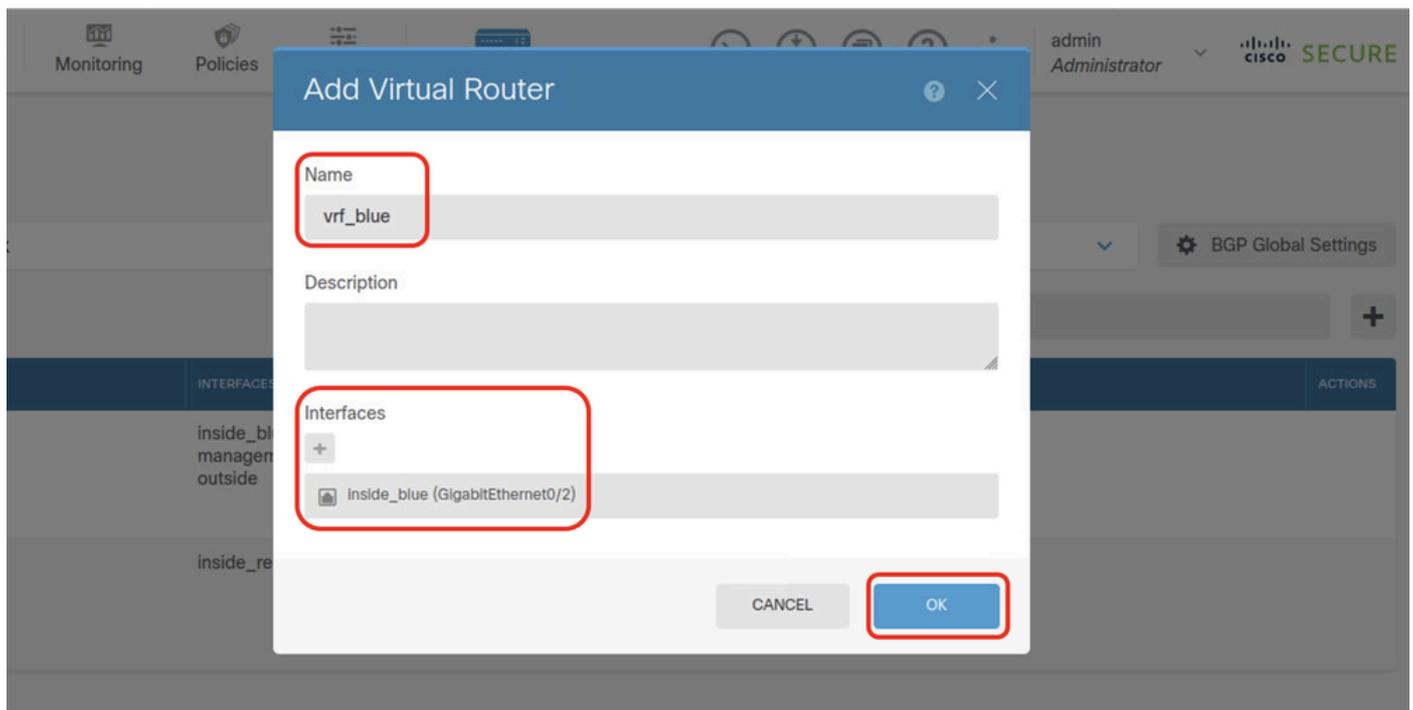
Étape 4.7. Créer un deuxième routeur virtuel. Accédez à Device > Routing . Cliquez sur Afficher la configuration . Cliquez sur le bouton +.



FTD_Add_Second_Virtual_Router

Étape 4.8. Fourniture des informations nécessaires sur le deuxième routeur virtuel Cliquez sur le bouton OK

- Name : vrf_bleu
- Interfaces: inside_blue (GigabitEthernet0/2)



FTD_Add_Second_Virtual_Router2

Étape 5 : création d'une fuite de route de vrf_bleu vers Global. Cette route permet aux points d'extrémité du réseau 192.168.20.0/24 d'établir des connexions qui traverseraient le tunnel VPN site à site. Dans cet exemple, le point d'extrémité distant protège le réseau 192.168.50.0/24.

Accédez à Device > Routing . Cliquez sur Afficher la configuration. cliquez sur l'icône Afficher dans la cellule Action du routeur virtuel vrf_bleu.

Device Summary
Virtual Routers

How Multiple Virtual Routers Work

3 virtual routers

#	NAME	INTERFACES	SHOW/TROUBLESHOOT	ACTIONS
1	Global	management outside	Routes Ipv6 routes BGP OSPF	
2	vrf_blue	inside_blue	Routes Ipv6 routes BGP OSPF	View
3	vrf_red	inside_red	Routes Ipv6 routes BGP OSPF	

FTD_View_VRF_Blue

Étape 5.1. Cliquez sur l'onglet Static Routing. Cliquez sur le bouton +.

Device Summary / Virtual Routers
vrf_blue

How Multiple Virtual Routers Work

Virtual Router Properties | **Static Routing** | BGP | OSPF | ECMP Traffic Zones

Filter +

FTD_Create_Static_Route_VRF_Blue

Étape 5.2. Fournir les informations nécessaires Cliquez sur le bouton OK.

- Name : Bleu_vers_ASA
- Interface: demovti (Tunnel1)
- Réseaux : remote_192.168.50.0
- Passerelle : laissez cet élément vide.

Name
Blue_to_ASA

Description

Interface
demovti (Tunnel1) Belongs to current Router
N/A

Protocol
 IPv4 IPv6

Networks
+
remote_192.168.50.0

Gateway
Please select a gateway Metric
1

SLA Monitor *Applicable only for IPv4 Protocol type*
Please select an SLA Monitor

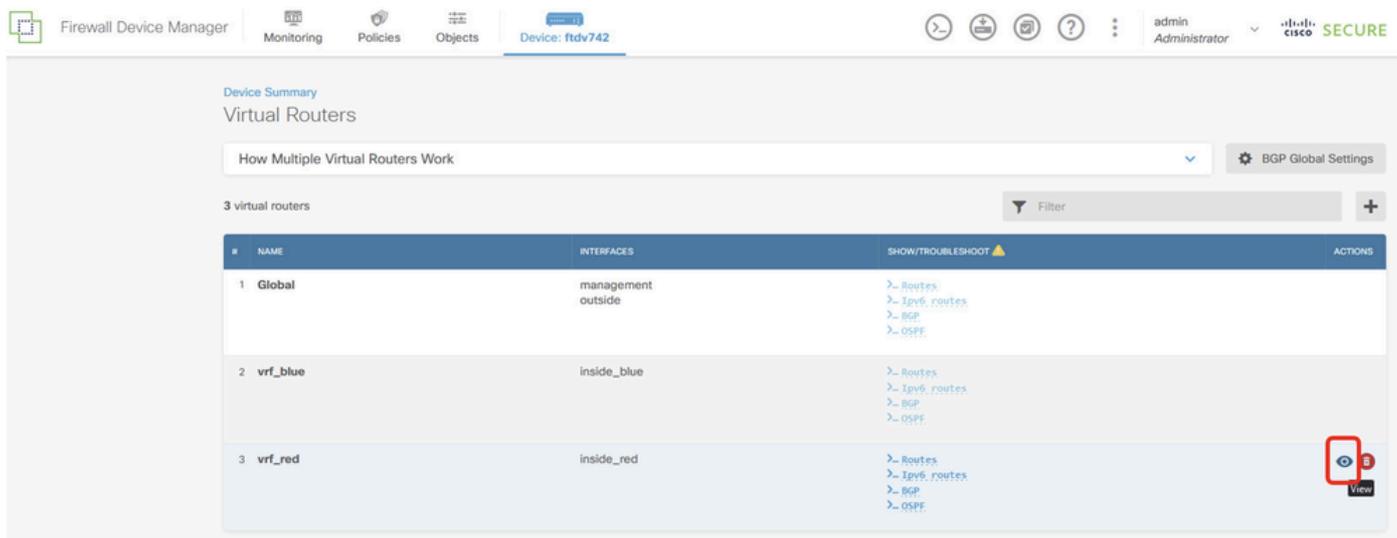
CANCEL OK

FTD_Create_Static_Route_VRF_Blue_Details

Étape 6. Création d'une fuite de route de vrf_red vers Global. Cette route permet aux points d'extrémité du réseau 192.168.10.0/24 d'établir des connexions qui traverseraient le tunnel VPN

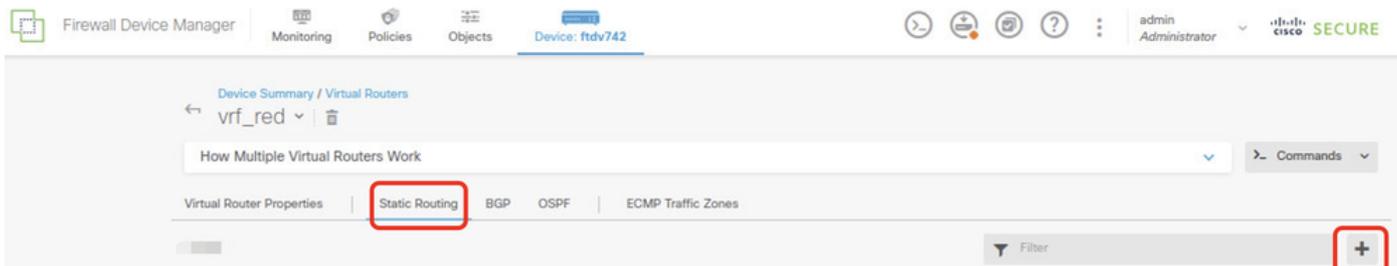
site à site. Dans cet exemple, le point d'extrémité distant protège le réseau 192.168.50.0/24.

Accédez à Device > Routing . Cliquez sur Afficher la configuration. Cliquez sur l'icône Afficher dans la cellule Action du routeur virtuel vrf_red.



FTD_View_VRF_Red

Étape 6.1. Cliquez sur l'onglet Static Routing. Cliquez sur le bouton +.



FTD_Create_Static_Route_VRF_Red

Étape 6.2. Fournir les informations nécessaires Cliquez sur le bouton OK.

- Name : Rouge_vers_ASA
- Interface: demovti (Tunnel1)
- Réseaux : remote_192.168.50.0
- Passerelle : laissez cet élément vide.

vrf_red

Add Static Route



Name

Red_to_ASA

Description

Interface

demovti (Tunnel1)

Belongs to current Router

N/A

Protocol



IPv4



IPv6

Networks



remote_192.168.50.0

Gateway

Please select a gateway

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

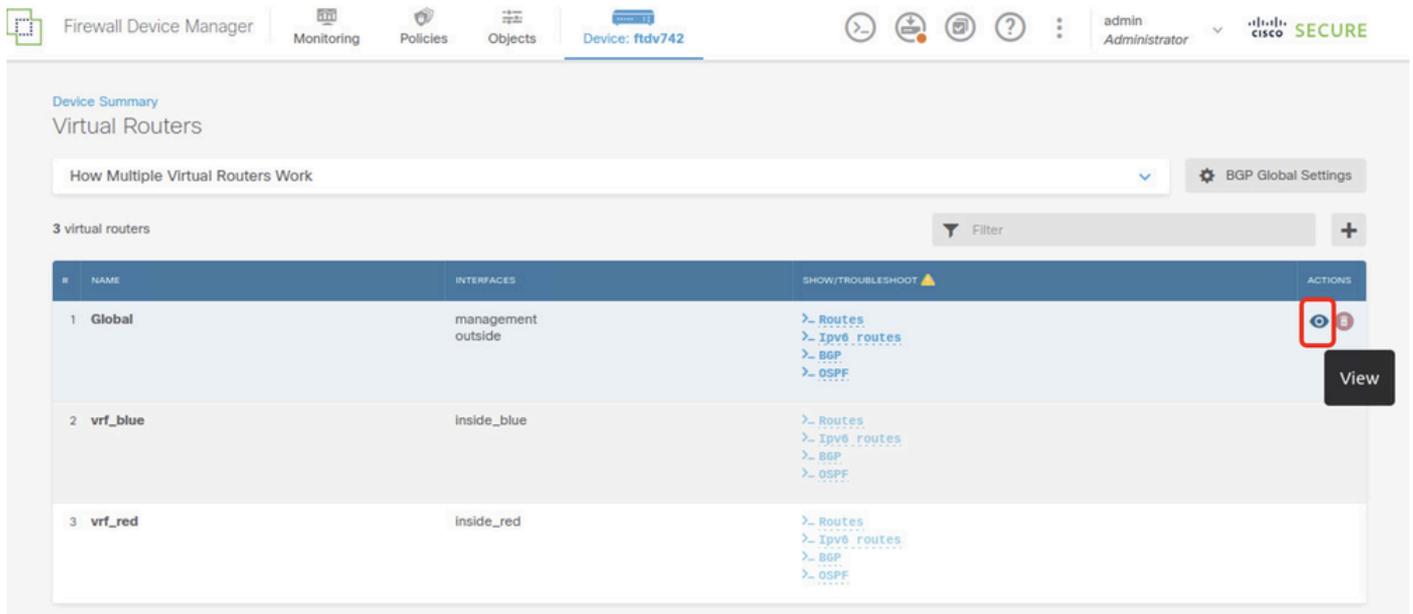
OK

FTD_Create_Static_Route_VRF_Red_Details

Étape 7 : création d'une fuite de route entre les routeurs globaux et virtuels Les routes permettent aux terminaux protégés par l'extrémité distante du VPN site à site d'accéder au réseau

192.168.10.0/24 dans le routeur virtuel vrf_red et au réseau 192.168.20.0/24 dans le routeur virtuel vrf_blue.

Accédez à Device > Routing . Cliquez sur View Configuration . Cliquez sur l'icône View dans la cellule Action du routeur virtuel global.



FTD_View_VRF_Global

Étape 7.1. Cliquez sur l'onglet Static Routing. Cliquez sur le bouton +.



FTD_Create_Static_Route_VRF_Global

Étape 7.2. Fournir les informations nécessaires Cliquez sur le bouton OK.

- Name : S2S_leak_blue
- Interface : inside_blue (GigabitEthernet0/2)
- Réseaux : local_blue_192.168.20.0
- Passerelle : laissez cet élément vide.

Global Add Static Route



Name

S25_leak_blue

Description



The selected interface belongs to a different virtual router. If you create this static route, the route will cross virtual router boundaries, with the risk that traffic from this virtual router will leak into another virtual router. Proceed with caution.

Interface

inside_blue (GigabitEthernet0/2)

Belongs to different Router

vt_blue

Protocol



IPv4



IPv6

Networks



local_blue_192.168.20.0

Gateway

Please select a gateway

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK

```
encryption aes-256 aes-192 aes
integrity sha512 sha384 sha256 sha
group 21 20 16 15 14
prf sha512 sha384 sha256 sha
lifetime seconds 86400
```

Étape 10. Créez une proposition IKEv2 ipsec qui définit les mêmes paramètres configurés sur le FTD.

<#root>

```
crypto ipsec ikev2 ipsec-proposal
```

AES-SHA

```
protocol esp encryption aes-256 aes-192 aes
protocol esp integrity sha-512 sha-384 sha-256 sha-1
```

Étape 11. Création d'un profil ipsec, référencement ipsec-proposition créée à l'étape 10.

<#root>

```
crypto ipsec profile
```

demo_ipsec_profile

```
set ikev2 ipsec-proposal
```

AES-SHA

```
set security-association lifetime kilobytes 4608000
set security-association lifetime seconds 28800
```

Étape 12 : création d'une stratégie de groupe autorisant le protocole IKEv2

<#root>

```
group-policy
```

demo_gp_192.168.30.1

```
internal
group-policy demo_gp_192.168.30.1 attributes
vpn-tunnel-protocol ikev2
```

Étape 13. Créez un groupe de tunnels pour l'adresse IP externe FTD homologue, en faisant

référence à la stratégie de groupe créée à l'étape 12 et configuration de la même clé pré-partagée avec FTD (créée à l'étape 3.7).

```
<#root>
```

```
tunnel-group 192.168.30.1 type ipsec-l2l  
tunnel-group 192.168.30.1 general-attributes  
  default-group-policy
```

```
demo_gp_192.168.30.1
```

```
tunnel-group 192.168.30.1 ipsec-attributes  
  ikev2 remote-authentication pre-shared-key *****  
  ikev2 local-authentication pre-shared-key *****
```

Étape 14. Activez IKEv2 sur l'interface externe.

```
crypto ikev2 enable outside
```

Étape 15. Création d'un tunnel virtuel

```
<#root>
```

```
interface Tunnel1  
  nameif demovti_asa  
  ip address 169.254.10.2 255.255.255.0  
  tunnel source interface outside  
  tunnel destination 192.168.30.1  
  tunnel mode ipsec ipv4  
  tunnel protection ipsec profile
```

```
demo_ipsec_profile
```

Étape 16. Créer une route statique

```
route demovti_asa 192.168.10.0 255.255.255.0 169.254.10.1 1  
route demovti_asa 192.168.20.0 255.255.255.0 169.254.10.1 1  
route outside 0.0.0.0 0.0.0.0 192.168.40.3 1
```

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Étape 1. Accédez à l'interface de ligne de commande de FTD et d'ASA via la console ou SSH pour vérifier l'état VPN des phases 1 et 2 à l'aide des commandes show crypto ikev2 sa et show crypto ipsec sa .

DFT :

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
ftdv742#
ftdv742# show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
32157565 192.168.30.1/500 192.168.40.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/67986 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0x4cf55637/0xa493cc83
```

```
ftdv742# show crypto ipsec sa
interface: demovti
Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.30.1
```

```
Protected vrf (ivrf): Global
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 192.168.40.1
```

```
#pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
#pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 30, #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.: 192.168.30.1/500, remote crypto endpt.: 192.168.40.1/500
path mtu 1500, ipsec overhead 94(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: A493CC83
current inbound spi : 4CF55637
```

```
inbound esp sas:
spi: 0x4CF55637 (1291146807)
SA State: active
transform: esp-aes-256 esp-sha-512-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, VTI, }
slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (4055040/16867)
```

```
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
outbound esp sas:
spi: 0xA493CC83 (2761149571)
SA State: active
transform: esp-aes-256 esp-sha-512-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, VTI, }
slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (4285440/16867)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

ASA :

```
ASA9203# show crypto ikev2 sa
```

```
IKEv2 SAs:
```

```
Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local Remote
26025779 192.168.40.1/500 192.168.30.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/68112 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0xa493cc83/0x4cf55637
```

```
ASA9203#
```

```
ASA9203# show cry
```

```
ASA9203# show crypto ipsec sa
```

```
interface: demovti_asa
```

```
Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.40.1
```

```
Protected vrf (ivrf): Global
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 192.168.30.1
```

```
#pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
#pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 30, #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.: 192.168.40.1/500, remote crypto endpt.: 192.168.30.1/500
path mtu 1500, ipsec overhead 94(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 4CF55637
```

current inbound spi : A493CC83

inbound esp sas:

spi: 0xA493CC83 (2761149571)

SA State: active

transform: esp-aes-256 esp-sha-512-hmac no compression

in use settings ={L2L, Tunnel, IKEv2, VTI, }

slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1

sa timing: remaining key lifetime (kB/sec): (4101120/16804)

IV size: 16 bytes

replay detection support: Y

Anti replay bitmap:

0x00000000 0x00000001

outbound esp sas:

spi: 0x4CF55637 (1291146807)

SA State: active

transform: esp-aes-256 esp-sha-512-hmac no compression

in use settings ={L2L, Tunnel, IKEv2, VTI, }

slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1

sa timing: remaining key lifetime (kB/sec): (4055040/16804)

IV size: 16 bytes

replay detection support: Y

Anti replay bitmap:

0x00000000 0x00000001

Étape 2 : vérification de la route de VRF et de Global sur FTD

ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF

Gateway of last resort is 192.168.30.3 to network 0.0.0.0

```
S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.30.3, outside
C 169.254.10.0 255.255.255.0 is directly connected, demovti
L 169.254.10.1 255.255.255.255 is directly connected, demovti
SI 192.168.10.0 255.255.255.0 [1/0] is directly connected, inside_red
SI 192.168.20.0 255.255.255.0 [1/0] is directly connected, inside_blue
C 192.168.30.0 255.255.255.0 is directly connected, outside
L 192.168.30.1 255.255.255.255 is directly connected, outside
```

ftdv742# show route vrf vrf_blue

Routing Table: vrf_blue

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route

```
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set
```

```
C      192.168.20.0 255.255.255.0 is directly connected, inside_blue
L      192.168.20.1 255.255.255.255 is directly connected, inside_blue
SI     192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti
```

```
ftdv742# show route vrf vrf_red
```

```
Routing Table: vrf_red
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set
```

```
C      192.168.10.0 255.255.255.0 is directly connected, inside_red
L      192.168.10.1 255.255.255.255 is directly connected, inside_red
SI     192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti
```

Étape 3 : vérification du test ping

Avant d'envoyer une requête ping, vérifiez les compteurs de `show crypto ipsec sa | interface inc` | `encap|decap` sur FTD.

Dans cet exemple, Tunnel1 montre 30 paquets pour l'encapsulation et la décapsulation.

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
    #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
ftdv742#
```

Client1 a envoyé une requête ping à Client3.

```
Client1#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/299/620 ms
```

Client2 a envoyé une requête ping à Client3.

```
Client2#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 11/297/576 ms
```

Vérifiez les compteurs de `show crypto ipsec sa | interface inc :|encap|decap` sur FTD après l'exécution de la commande ping.

Dans cet exemple, Tunnel1 affiche 40 paquets pour l'encapsulation et la décapsulation après une requête ping réussie. En outre, les deux compteurs ont augmenté de 10 paquets, correspondant aux 10 requêtes d'écho ping, ce qui indique que le trafic ping a traversé le tunnel IPsec avec succès.

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 40, #pkts encrypt: 40, #pkts digest: 40
    #pkts decaps: 40, #pkts decrypt: 40, #pkts verify: 40
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Dépannage

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

Vous pouvez utiliser ces commandes debug pour dépanner la section VPN.

```
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug vti 255
```

Vous pouvez utiliser ces commandes debug pour dépanner la section route.

```
debug ip routing
```

Référence

[Guide de configuration de Cisco Secure Firewall Device Manager, version 7.4](#)

[Guide de configuration de l'interface de ligne de commande Cisco Secure Firewall ASA VPN, 9.20](#)

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.