Configurer BGP sur un VPN basé sur la route sur FTD géré par FDM

Table des matières

Introduction

Ce document décrit la configuration de BGP sur un VPN site à site basé sur route sur FTDv géré par FirePower Device Manager (FDM).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base du VPN
- Configurations BGP sur FTDv
- Expérience avec FDM

Composants utilisés

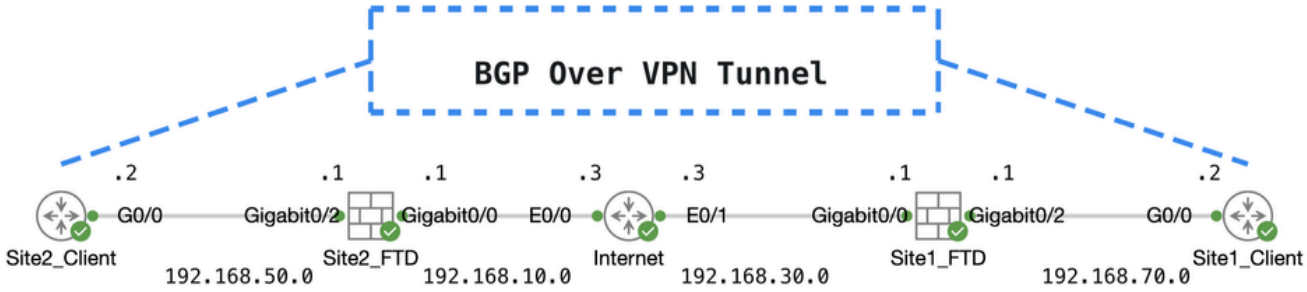
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco FTDv version 7.4.2
- Cisco FDM version 7.4.2

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

Diagramme du réseau



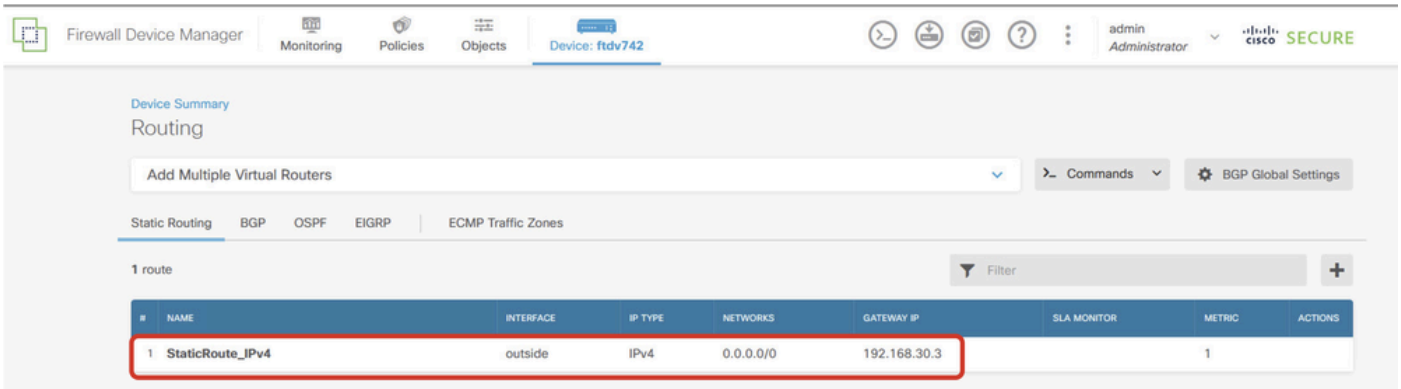
Topo

Configurations sur VPN

Étape 1. Assurez-vous que l'interconnectivité IP entre les noeuds est prête et stable. La licence Smart sur FDM est enregistrée avec le compte Smart.

Étape 2. La passerelle du client Site1 est configurée avec l'adresse IP interne du FTD Site1 (192.168.70.1). La passerelle du client Site2 est configurée avec l'adresse IP interne de Site2 FTD (192.168.50.1). Assurez-vous également que la route par défaut sur les deux FTD est configurée correctement après l'initialisation de FDM.

Connectez-vous à l'interface utilisateur graphique de chaque FDM. Accédez àDevice > Routing. Cliquez surView Configuration. Cliquez sur l'**Static Routing**onglet afin de vérifier la route statique par défaut.



Passerelle_FTD_Site1

Passerelle_FTD_Site2

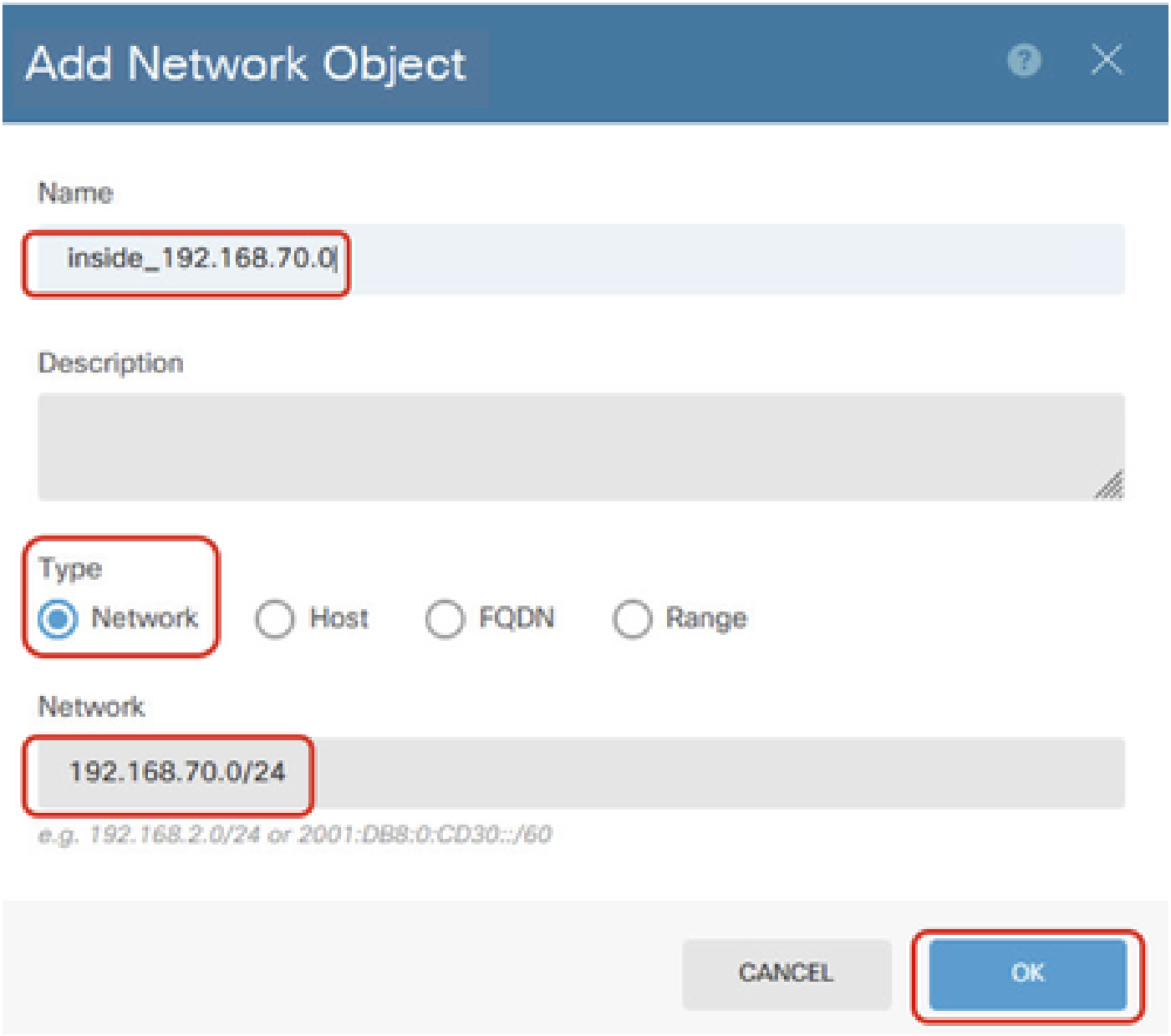
Étape 3. Configurez un VPN site à site basé sur la route. Dans cet exemple, commencez par configurer le FTD Site1.

Étape 3.1. Connectez-vous à l'interface utilisateur graphique FDM du FTD Site1. Créez un nouvel objet réseau pour le réseau interne du FTD Site1. Accédez à **Objects** > **Networks**, puis cliquez sur le bouton +.

Créer_Objet_Réseau

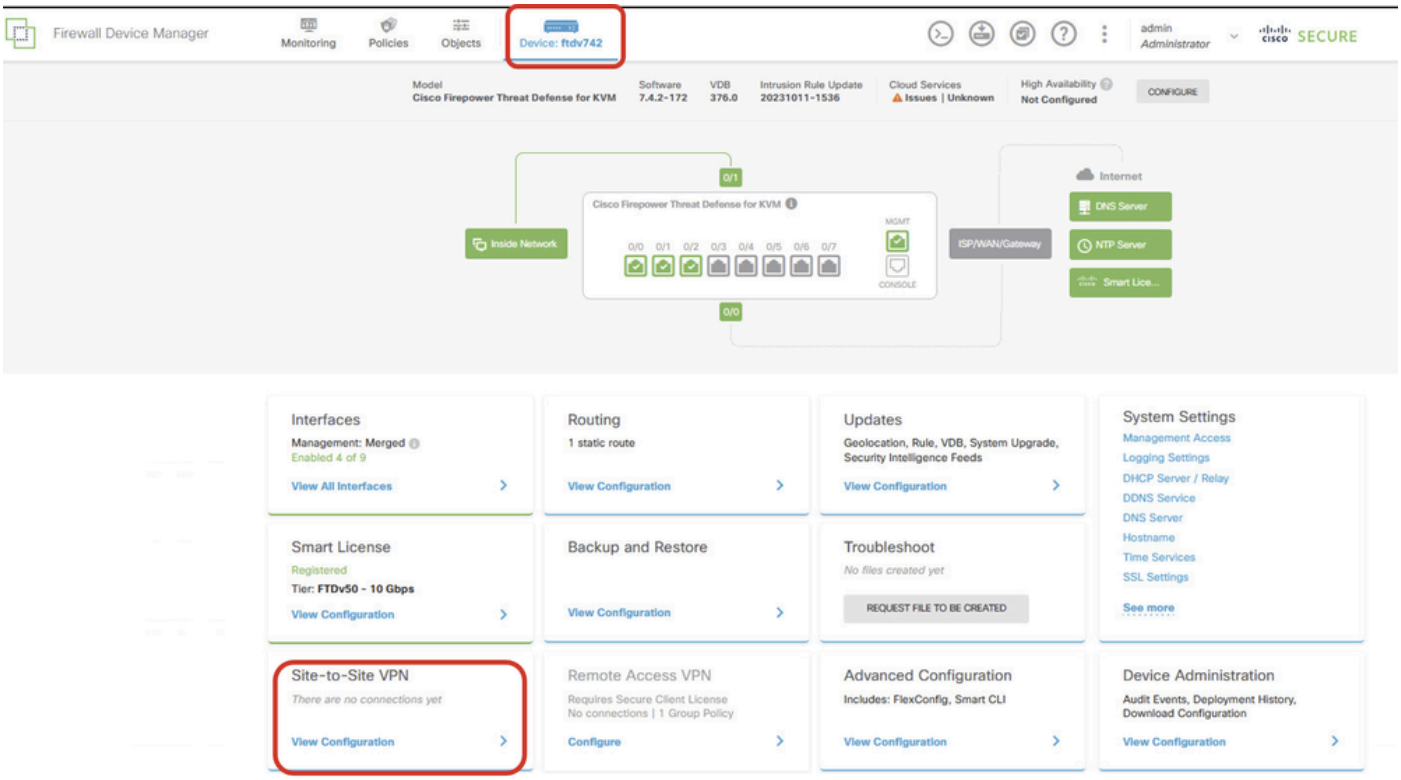
Étape 3.2. Fournir les informations nécessaires. Cliquez sur leOK bouton.

- Nom : inside_192.168.70.0
- Type : Réseau
- Réseau : 192.168.70.0/24



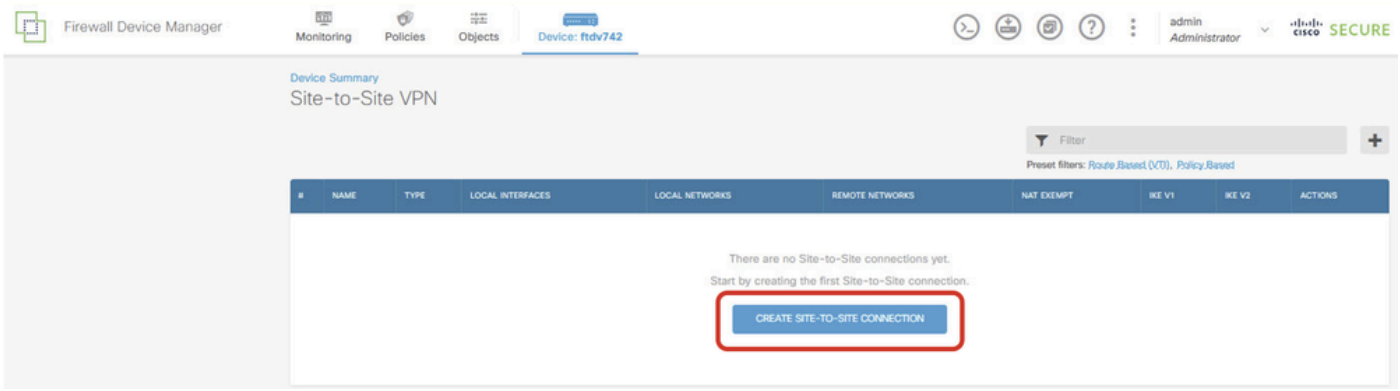
Site1_Réseau_Interne

Étape 3.3. Accédez à **Device > Site-to-Site VPN** . Cliquez sur **View Configuration** .



Afficher le VPN de site à site

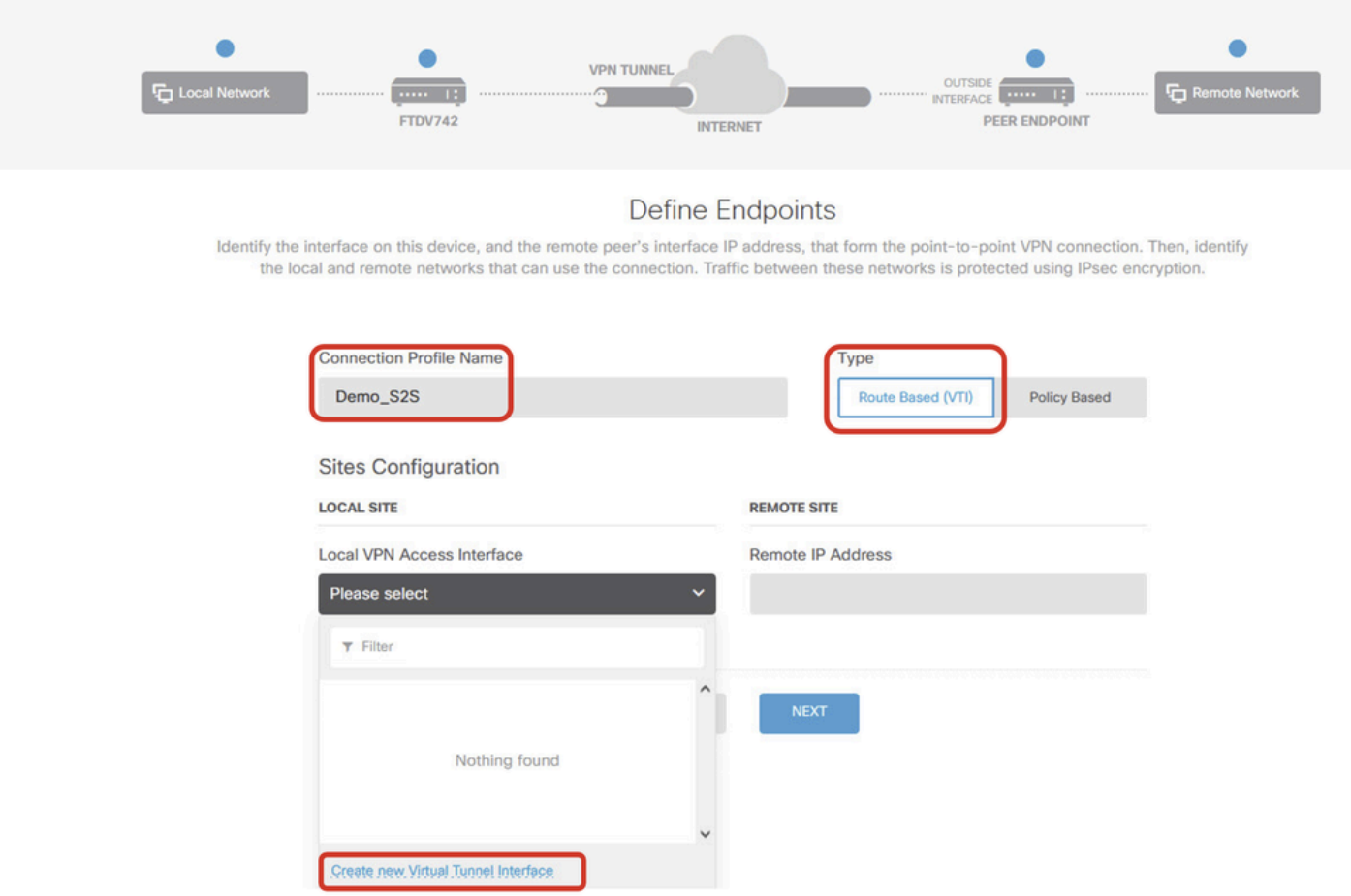
Étape 3.4. Commencez à créer un nouveau VPN de site à site. Cliquez sur **CREATE SITE-TO-SITE CONNECTION** .



Connexion_Créer_Site-à-Site

Étape 3.5. Fournissez les informations nécessaires.

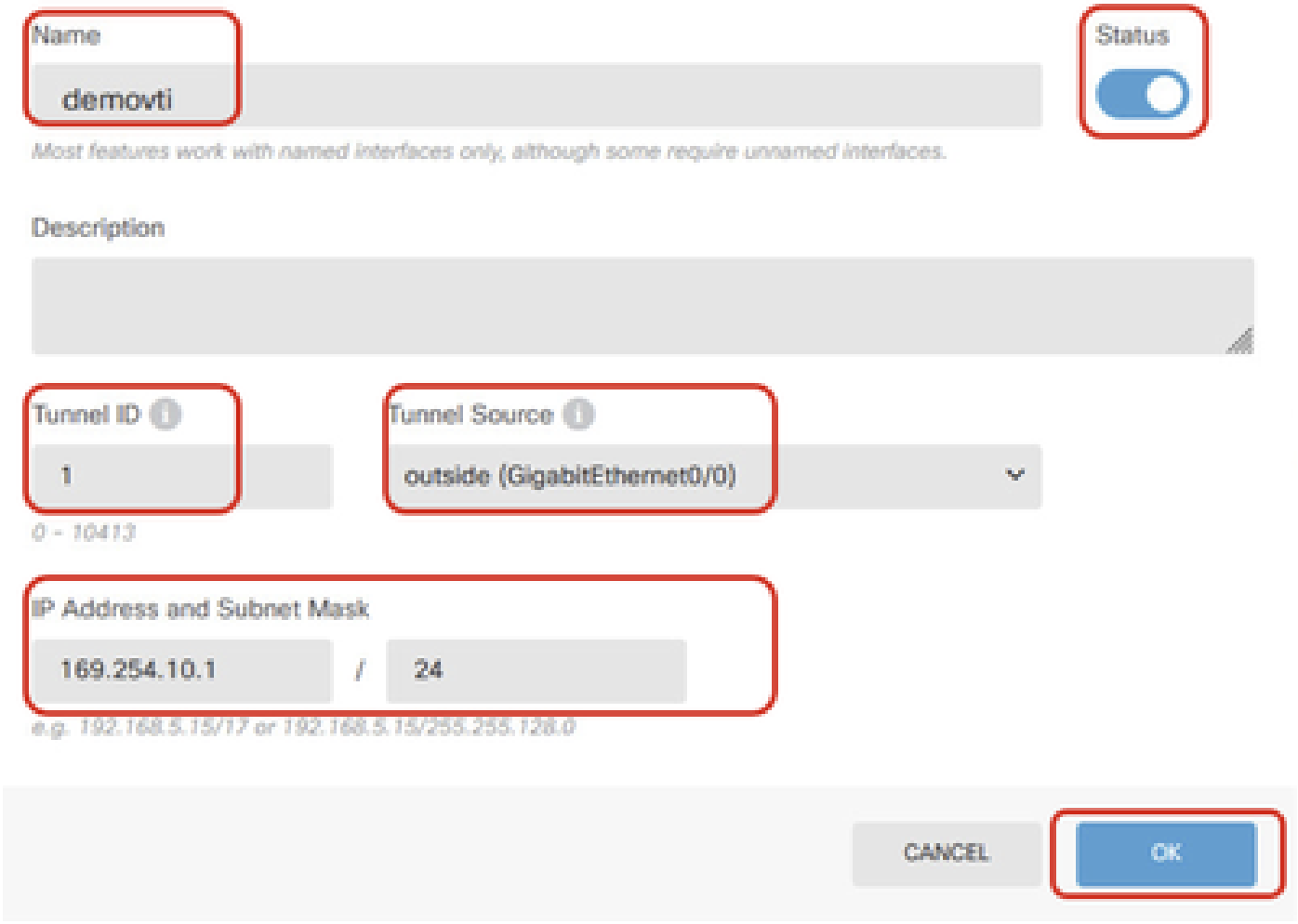
- Nom du profil de connexion : Demo_S2S
- Type : basé sur la route (VTI)
- Local VPN Access Interface : cliquez sur la liste déroulante, puis cliquez sur **Create new Virtual Tunnel Interface** .



Assistant_Create_VTI_in_VPN

Étape 3.6. Fournissez les informations nécessaires pour créer une nouvelle interface VTI. Cliquez sur le bouton OK.

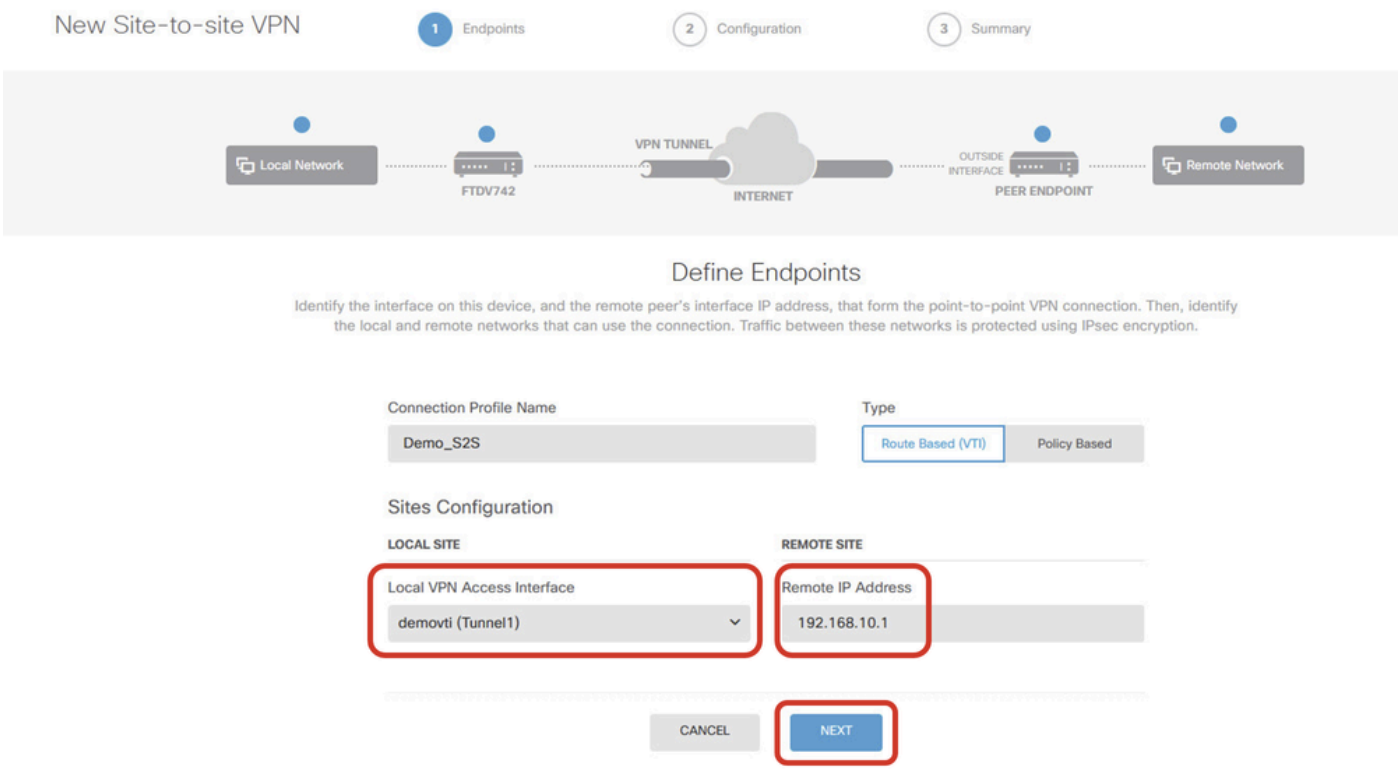
- Nom : demovti
- ID de tunnel : 1
- Source du tunnel : externe (GigabitEthernet0/0)
- Adresse IP et masque de sous-réseau : 169.254.10.1/24
- État : cliquez sur le curseur pour passer à la position Activé



Create_VTI_Details

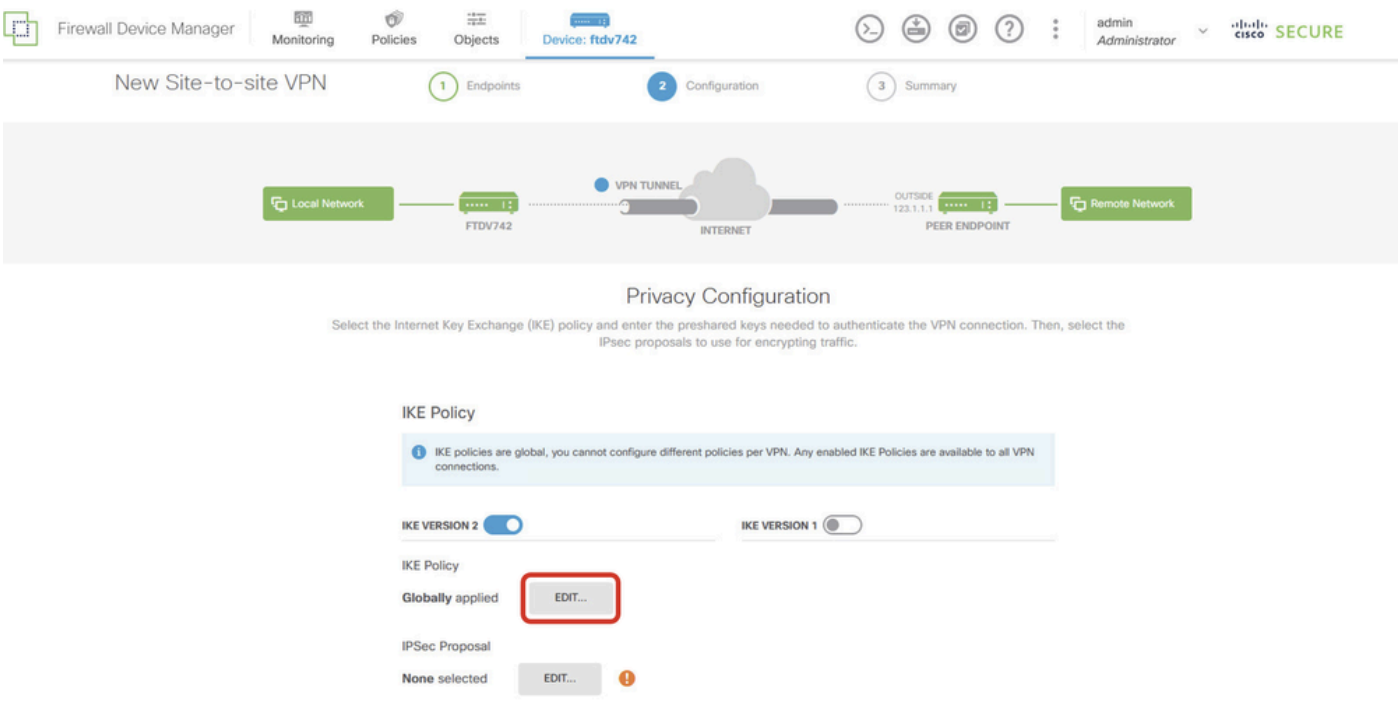
Étape 3.7. Continuez à fournir les informations nécessaires. Cliquez sur le bouton NEXT.

- Local VPN Access Interface : demovti (créé à l'étape 3.6.)
- Adresse IP distante : 192.168.10.1



Étape1 de l'assistant VPN_Endpoints_Wizard

Étape 3.8. Accédez à IKE Policy. Cliquez sur le bouton Edit.



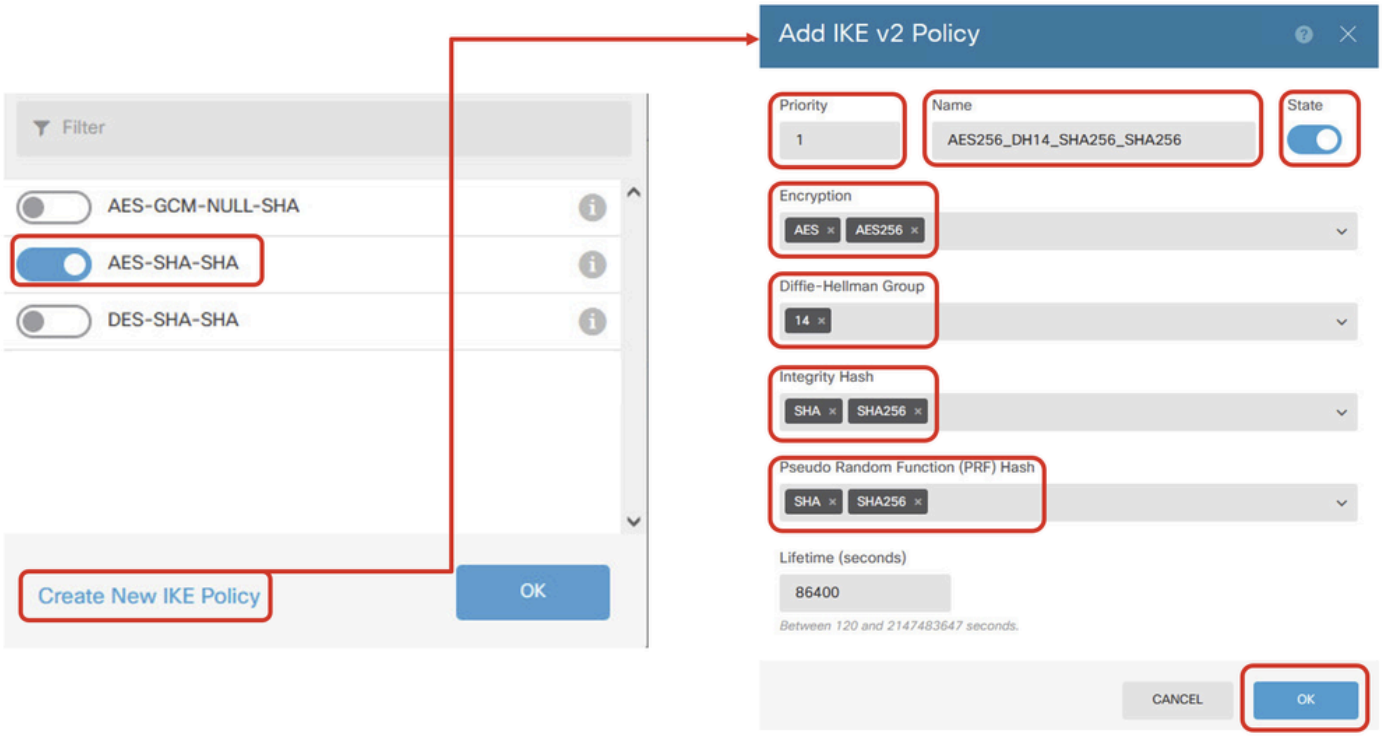
Modifier_politique_IKE

Étape 3.9. Pour la stratégie IKE, vous pouvez en utiliser une prédéfinie ou en créer une nouvelle en cliquant sur Create New IKE Policy.

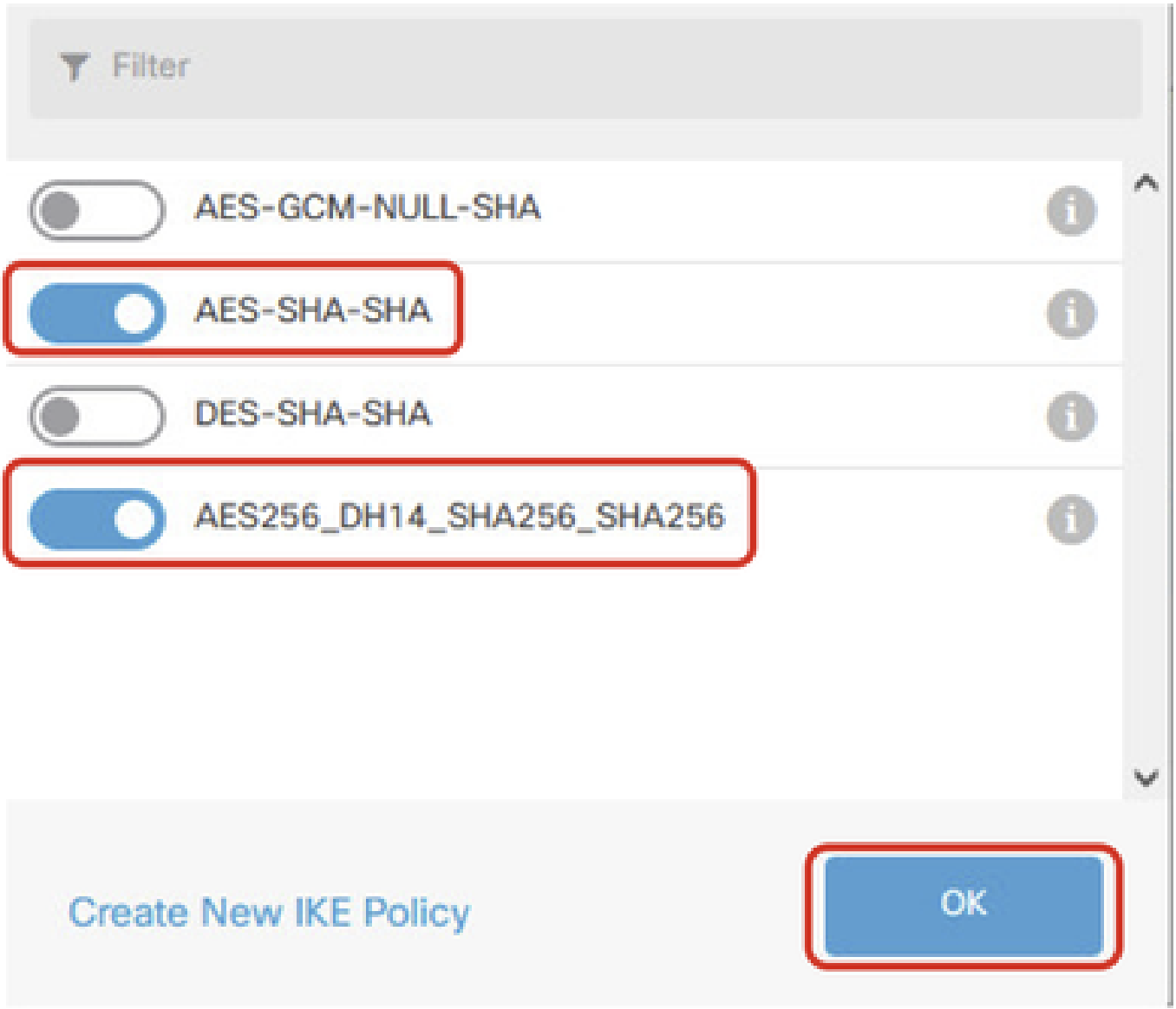
Dans cet exemple, basculez une stratégie IKE existante AES-SHA-SHA et créez-en une nouvelle

à des fins de démonstration. Cliquez sur le bouton OK afin d'enregistrer.

- Nom : AES256_DH14_SHA256_SHA256
- Cryptage : AES, AES256
- Groupe DH : 14
- Hachage d'intégrité : SHA, SHA256
- Hachage PRF : SHA, SHA256
- Durée de vie : 86400 (par défaut)

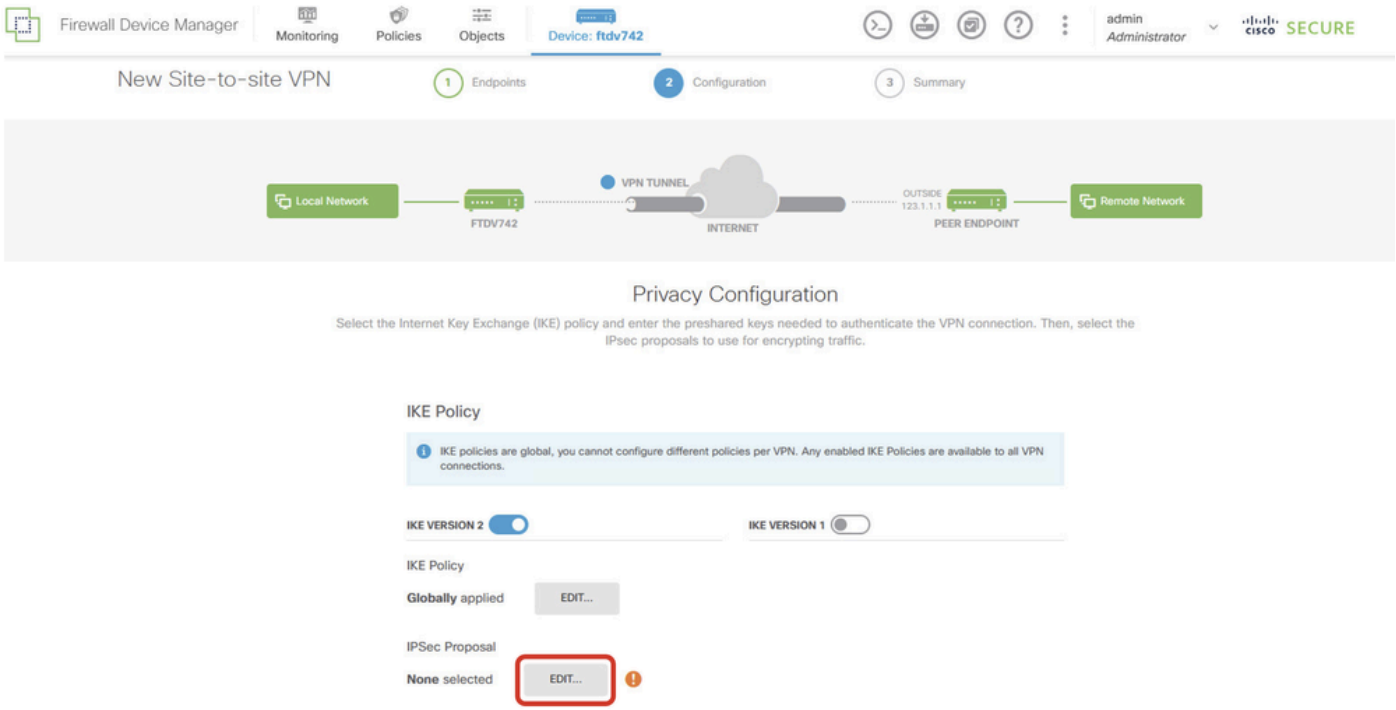


Add_New_IKE_Policy



Enable_New_IKE_Policy

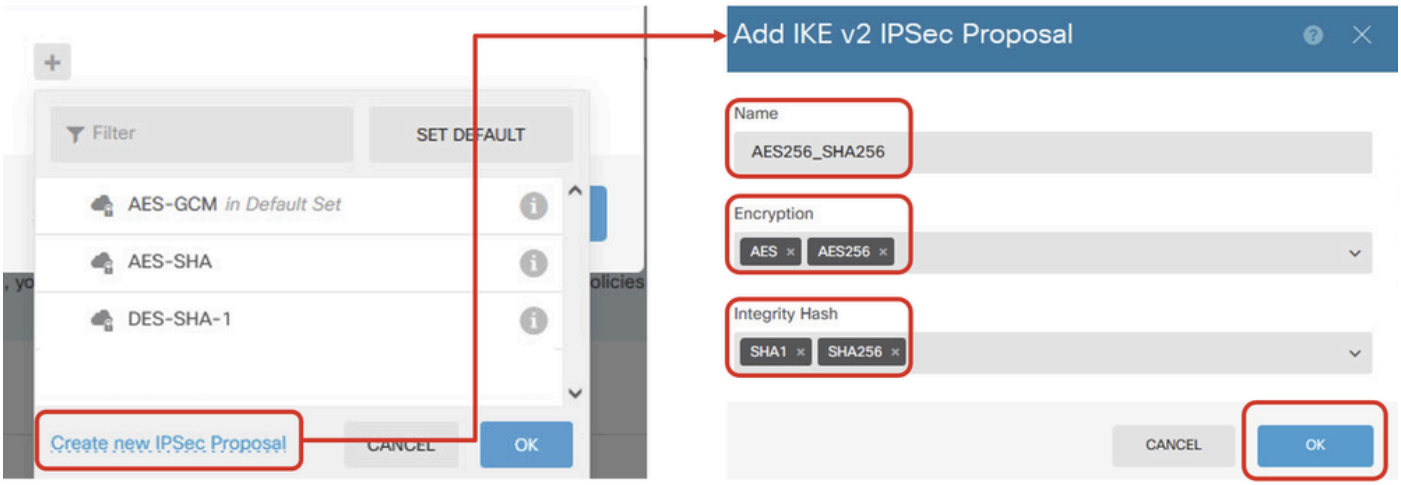
Étape 3.10. Accédez à la proposition IPSec. Cliquez sur le bouton Edit.



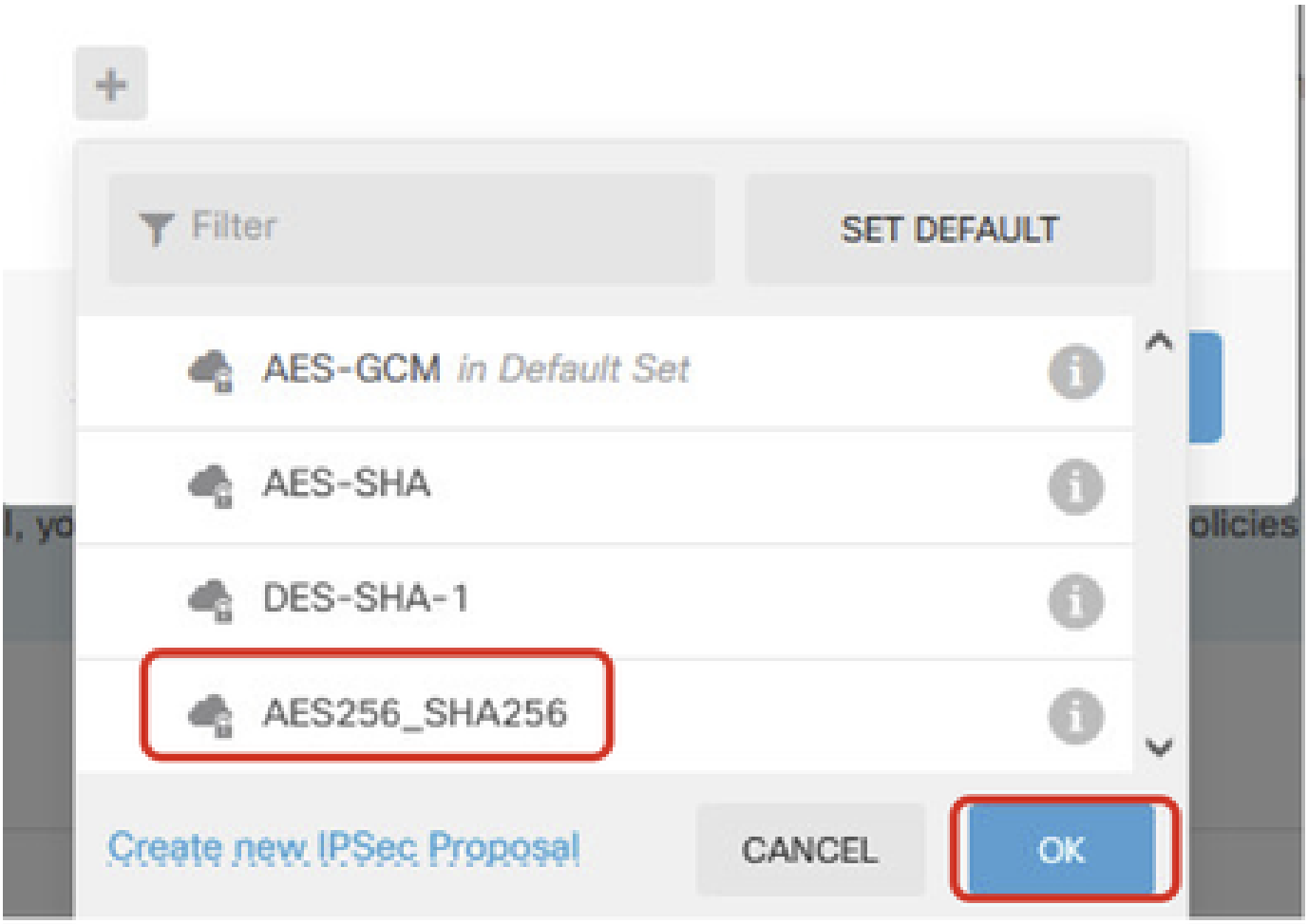
Modifier_Proposition_IKE

Étape 3.11. Pour la proposition IPSec, vous pouvez utiliser une proposition prédéfinie ou en créer une nouvelle en cliquant sur Create new IPSec Proposal. Dans cet exemple, créez-en un nouveau à des fins de démonstration. Fournissez les informations nécessaires. Cliquez sur le bouton OK afin d'enregistrer.

- Nom : AES256_SHA256
- Cryptage : AES, AES256
- Hachage d'intégrité : SHA1, SHA256



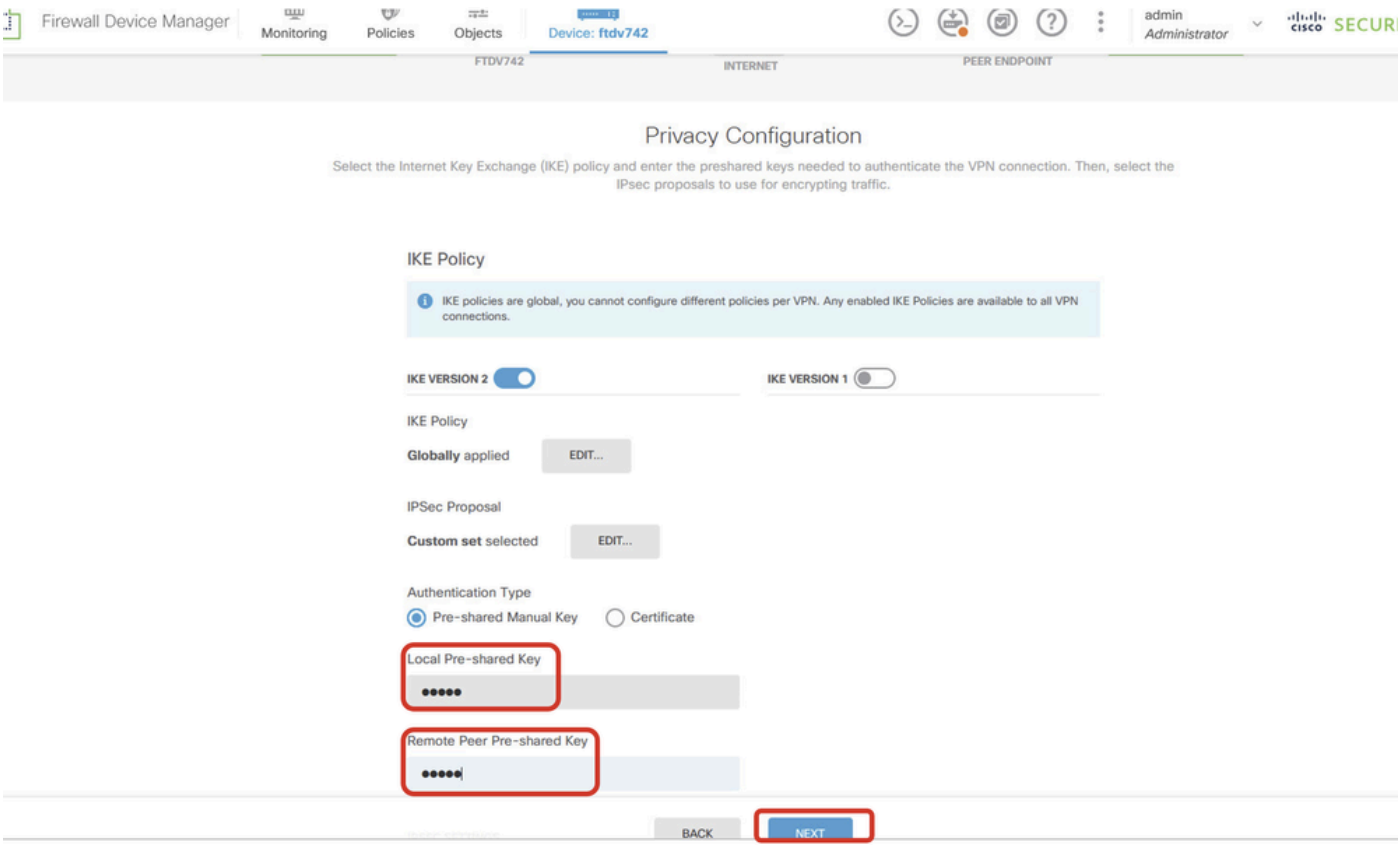
Ajouter_Nouvelle_Proposition_IPSec



Enable_New_IPSec_Proposal

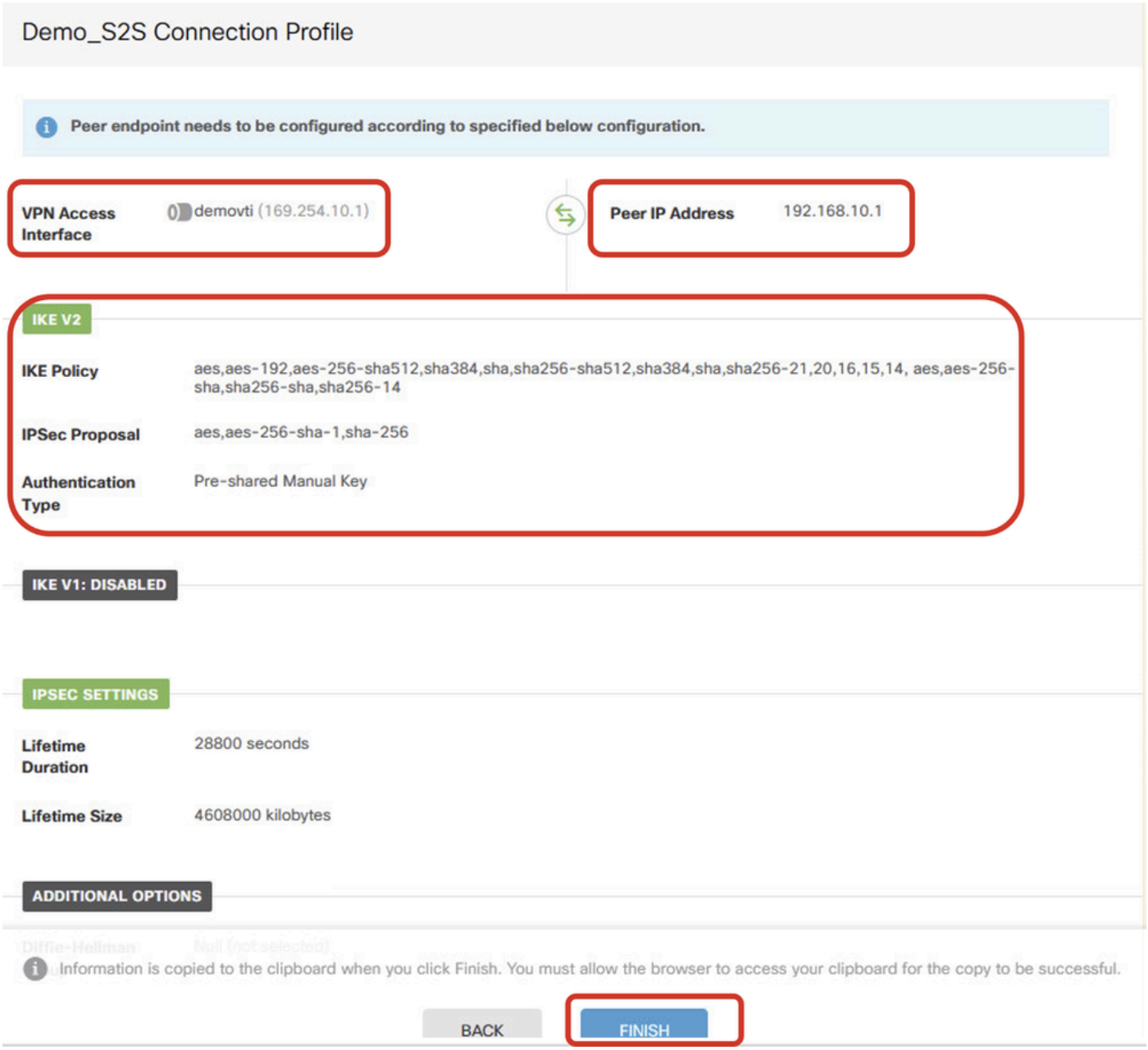
Étape 3.12. Configurez la clé pré-partagée. Cliquez sur le bouton NEXT.

Notez cette clé pré-partagée et configurez-la ultérieurement sur le FTD Site2.



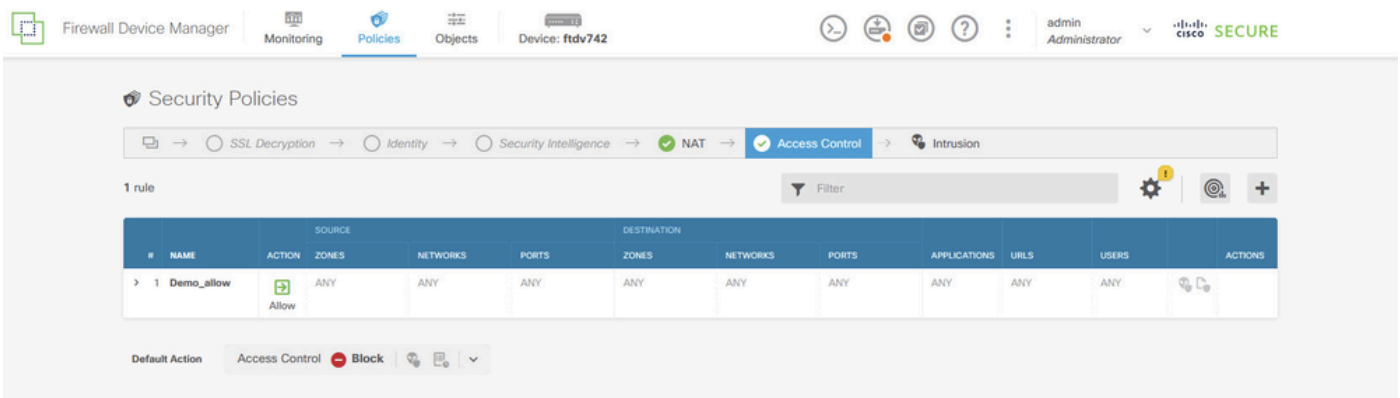
Configurer_Clé_Pré_Partagée

Étape 3.13. Examinez la configuration VPN. Si vous devez modifier quelque chose, cliquez sur le bouton BACK. Si tout va bien, cliquez sur le bouton FINISH.



Assistant_VPN_Terminé

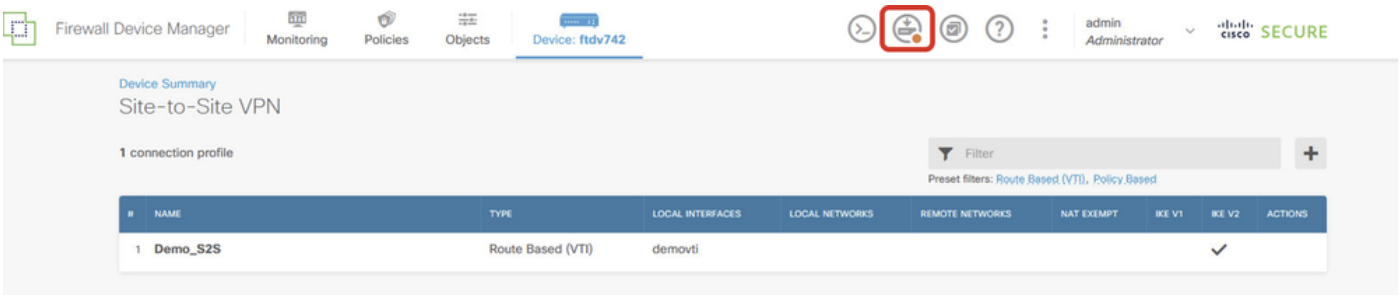
Étape 3.14. Créez une règle de contrôle d'accès afin d'autoriser le trafic à passer par le FTD. Dans cet exemple, autorisez tout pour les besoins de la démonstration. Modifiez votre stratégie en fonction de vos besoins réels.



Exemple de règle de contrôle d'accès

Étape 3.15. (Facultatif) Configurez la règle d’exemption NAT pour le trafic client sur FTD si la NAT dynamique est configurée pour le client afin d’accéder 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 chaque FTD.

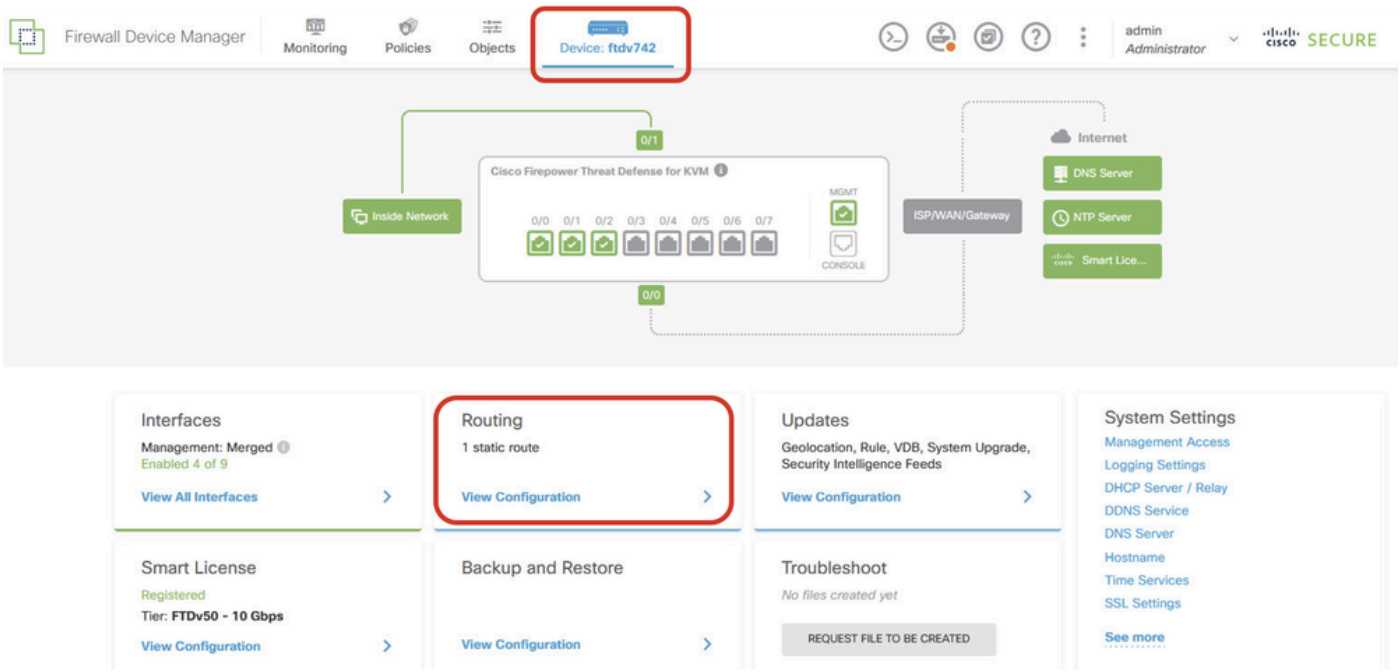
Étape 3.16. Déployez les modifications de configuration.



Configuration_VPN_Déploiement

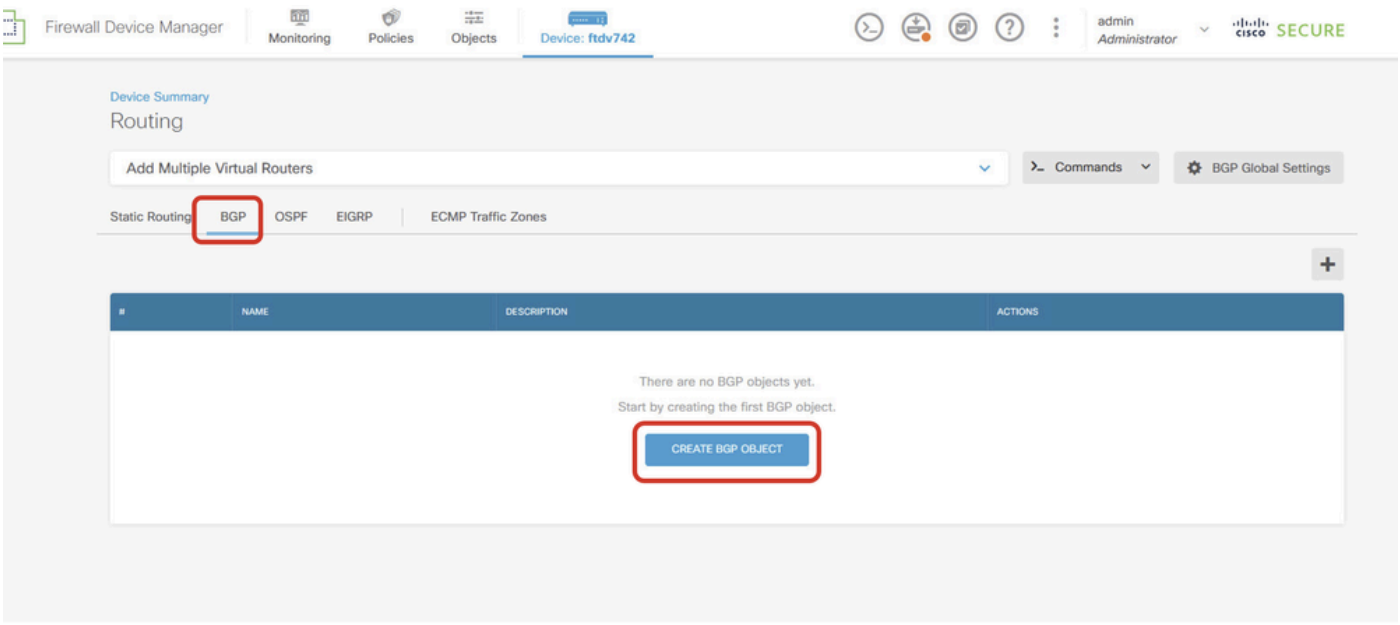
Configurations sur BGP

Étape 4. Accédez à Device > Routing. Cliquez sur Afficher la configuration.



Afficher_Configuration_Routage

Étape 5. Cliquez sur l'onglet BGP, puis sur CREATE BGP OBJECT.



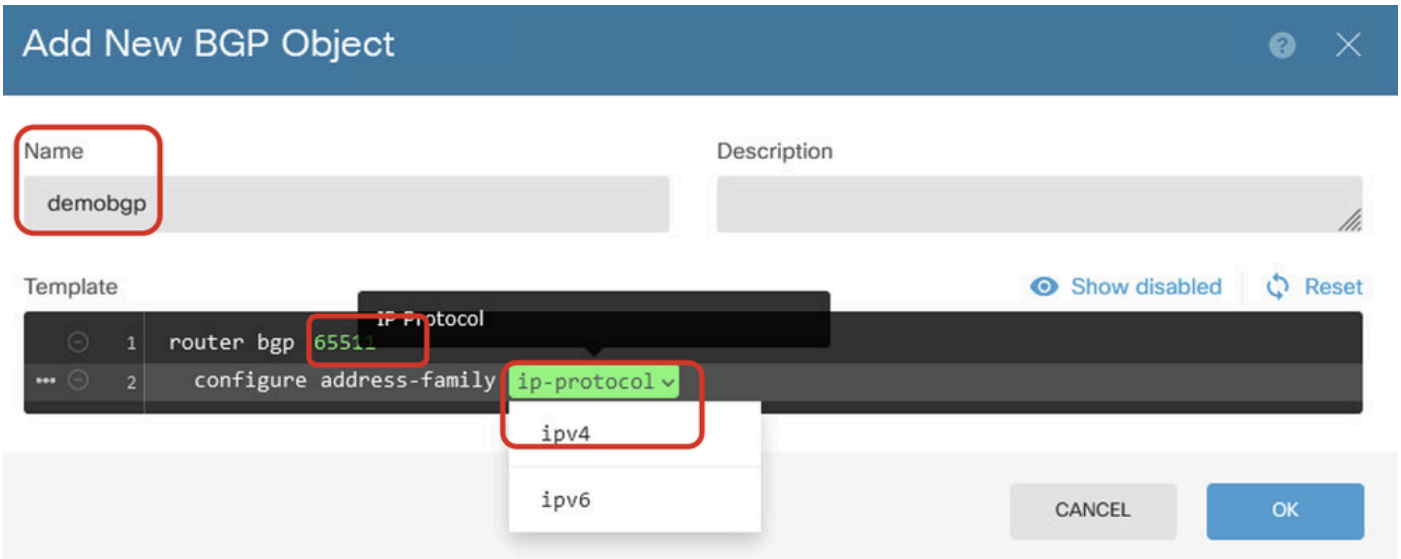
Create_BGP_Object

Étape 6. Fournissez le nom de l'objet. Accédez à Modèle et configurez. Cliquez sur le bouton OK pour enregistrer.

Nom : démobilisation

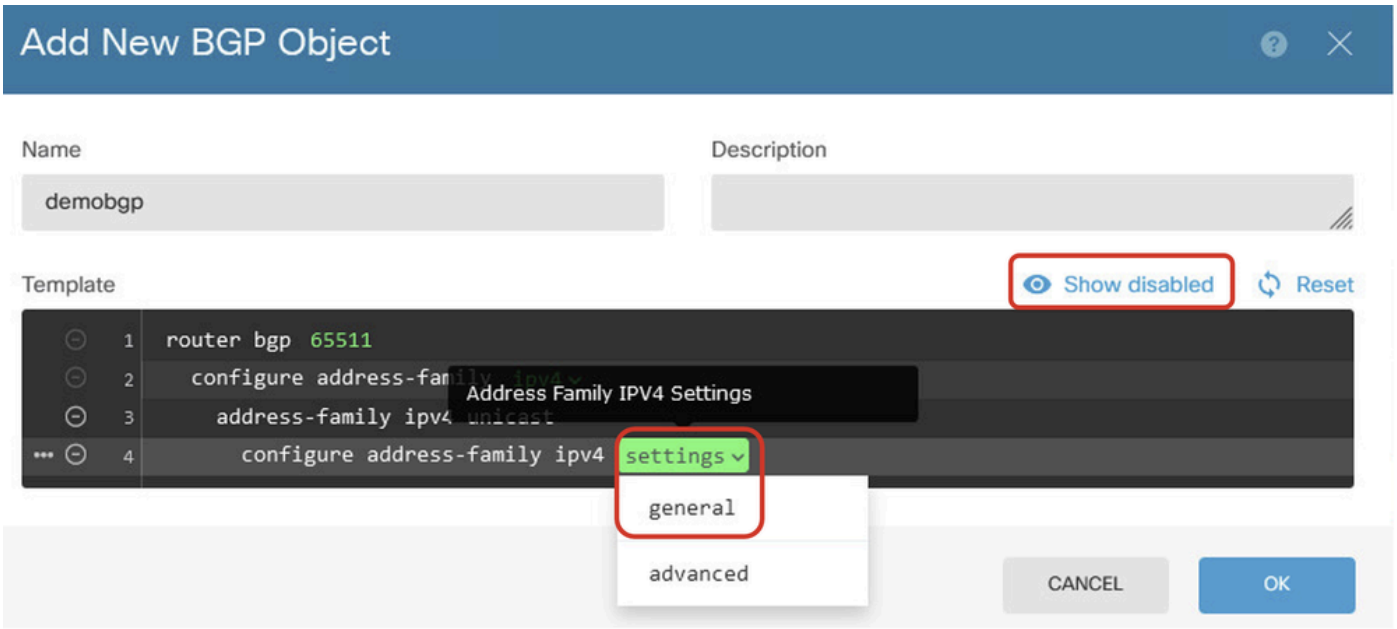
Ligne 1 : configurez le numéro de système autonome. Cliquez sur as-number. Numéro de système autonome local entré manuellement. Dans cet exemple, numéro de système autonome 65511 pour le site 1 FTD.

Ligne 2 : configurez le protocole IP. Cliquez sur ip-protocol. Sélectionnez ipv4.



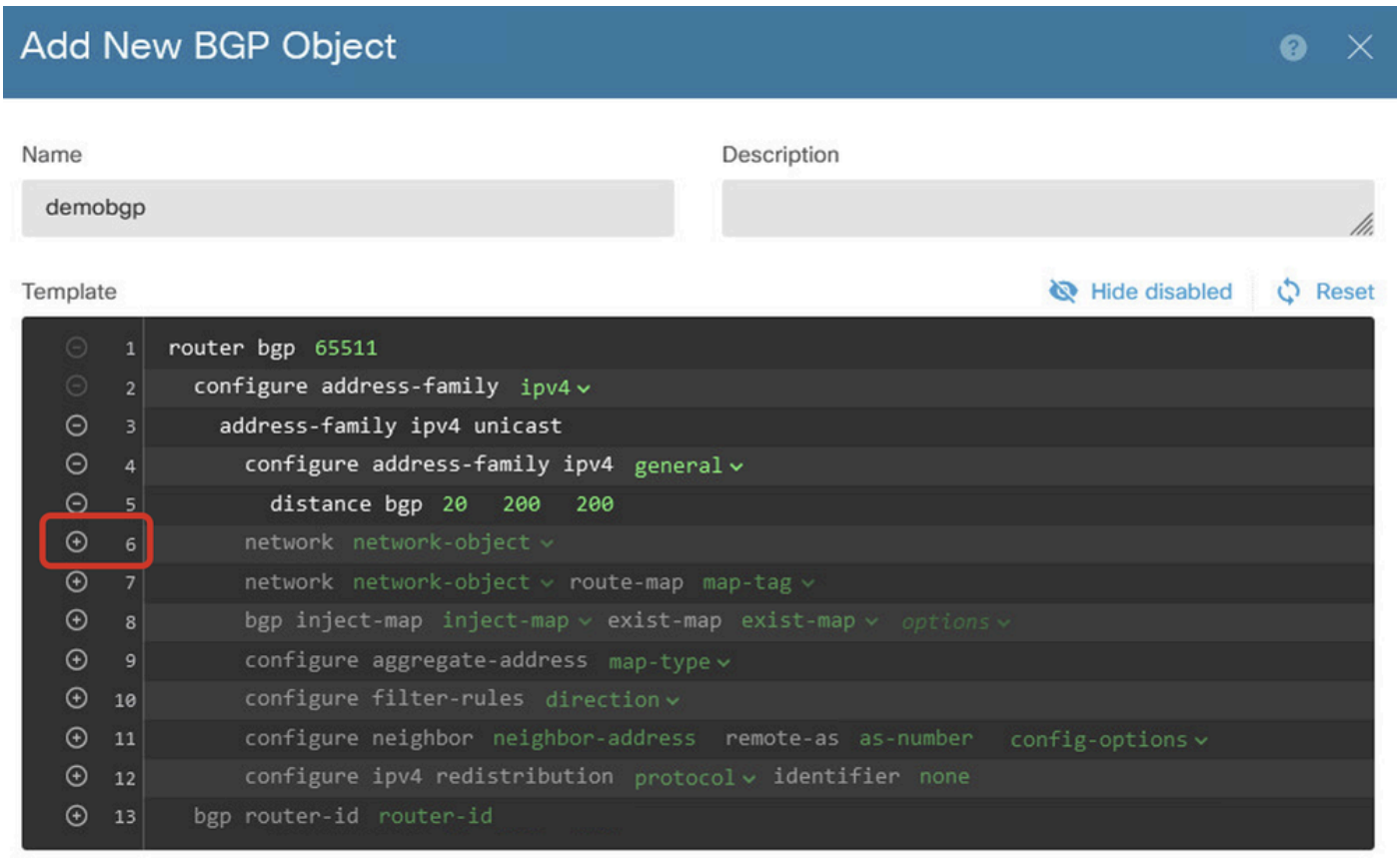
Create_BGP_Object_ASNumber_Protocol

Ligne 4 : Configurez d'autres paramètres. Cliquez sur settings, choisissez general, puis cliquez sur Show disabled.

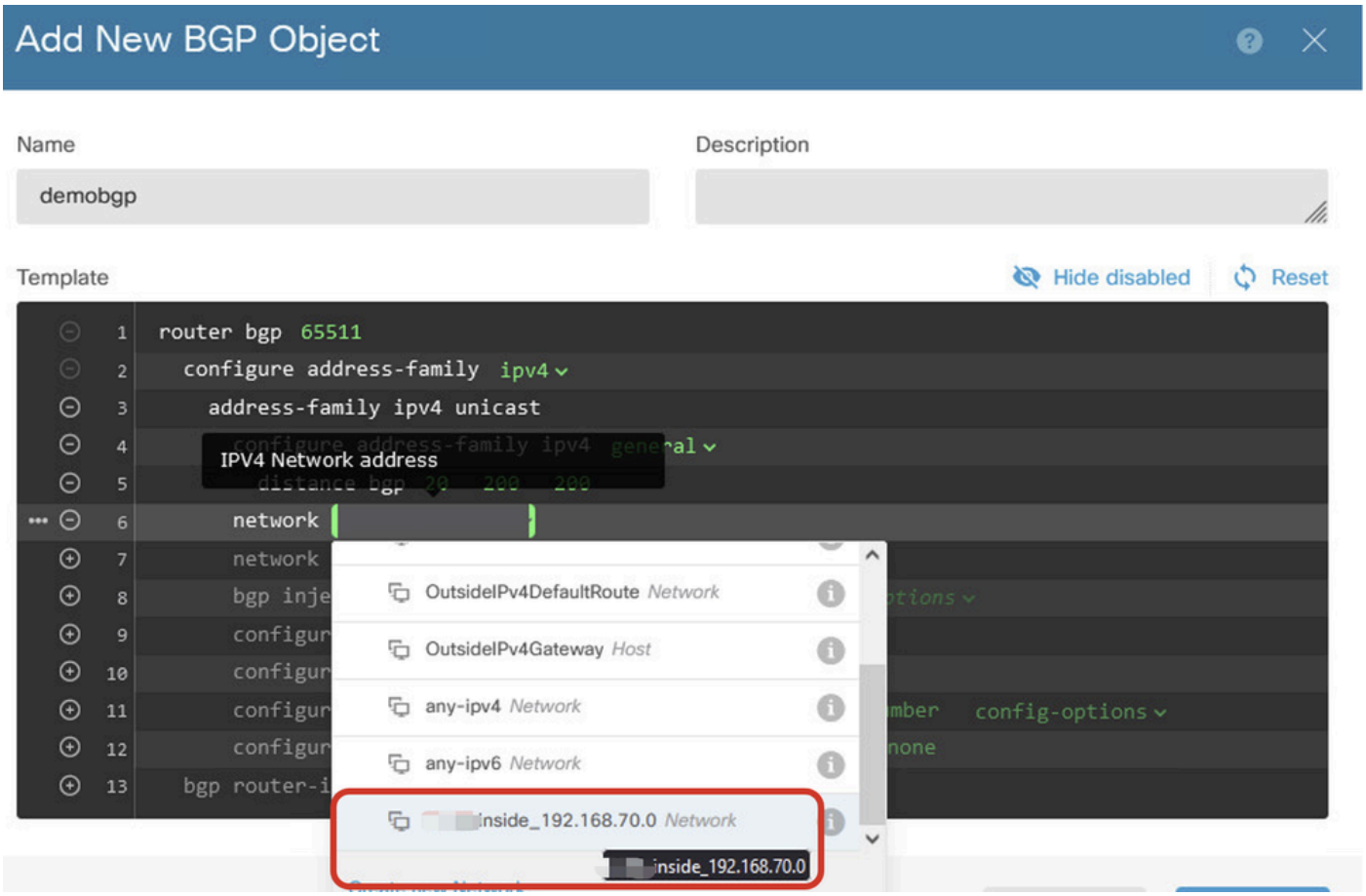


Create_BGP_Object_AddressSetting

Ligne 6 : Cliquez sur l'icône + afin d'activer la ligne pour configurer le réseau BGP. Cliquez sur network-object. Vous pouvez afficher les objets disponibles existants et en choisir un. Dans cet exemple, choisissez le nom d'objet inside_192.168.70.0 (créé à l'étape 3.2.).

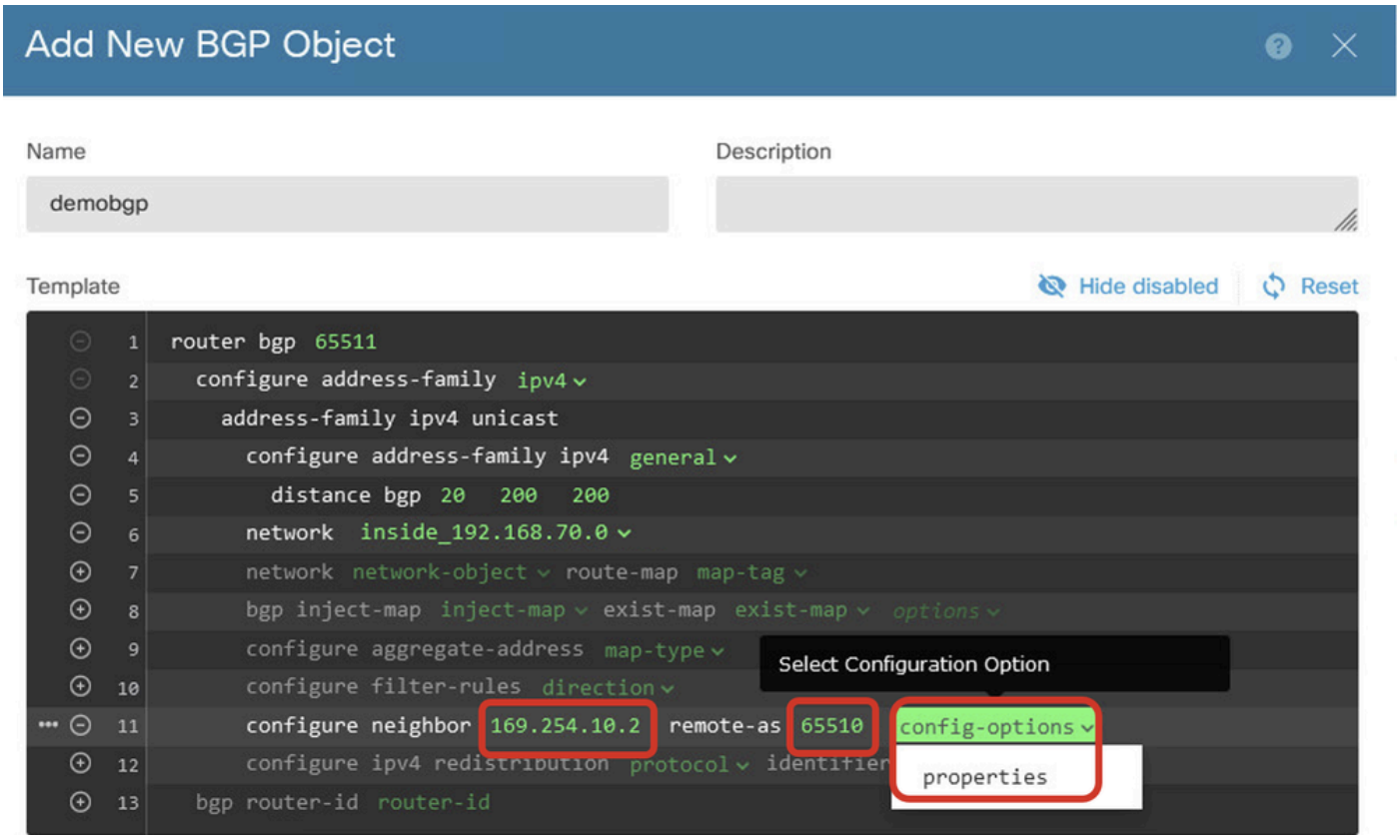


Create_BGP_Object_Add_Network



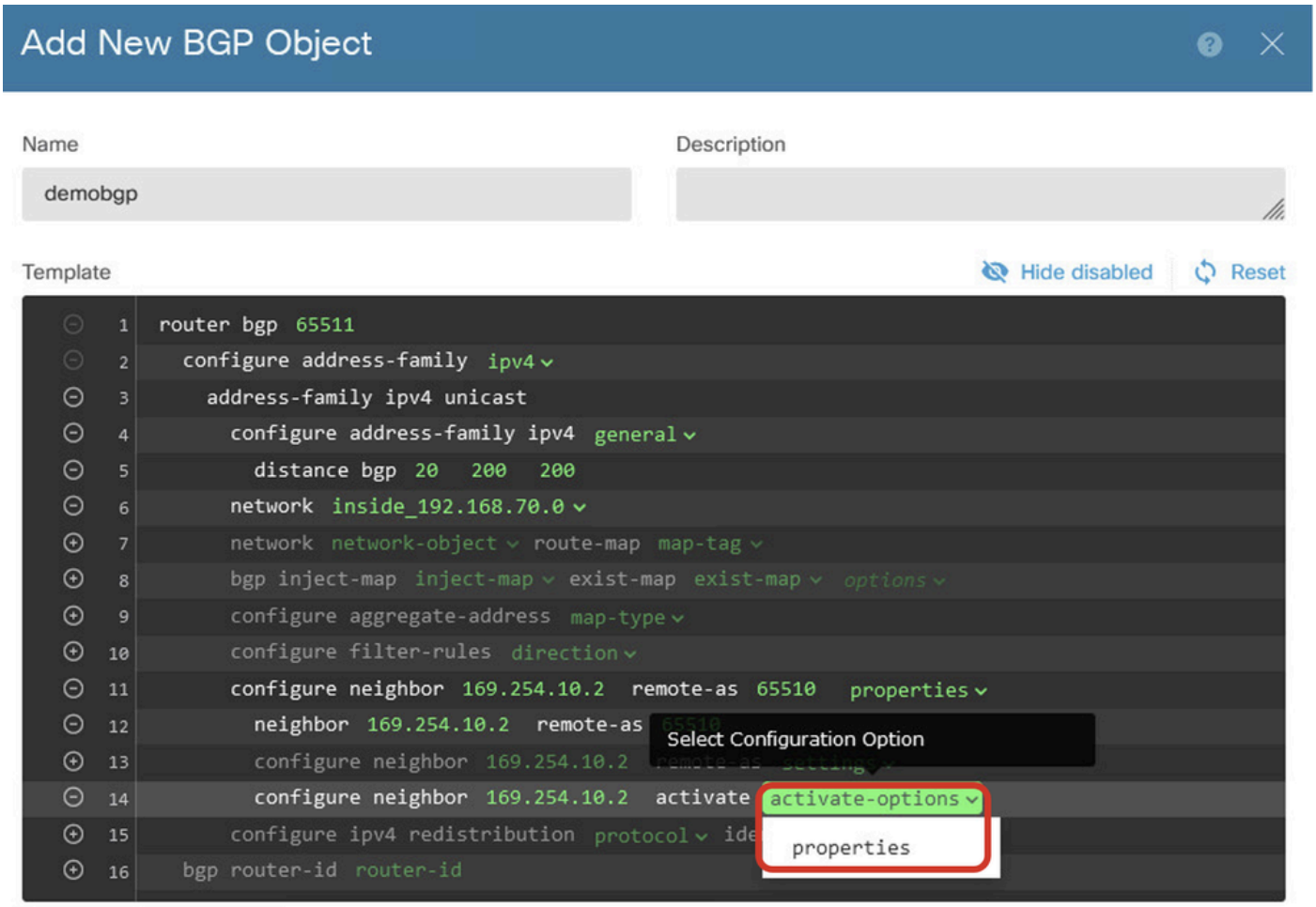
Create_BGP_Object_Add_Network2

Ligne 11 : Cliquez sur l'icône + afin d'activer la ligne pour configurer les informations relatives aux voisins BGP. Cliquez sur neighbor-address, et entrez manuellement l'adresse du voisin BGP homologue. Dans cet exemple, il s'agit de 169.254.10.2 (adresse IP VTI de Site2 FTD). Cliquez sur numéro-as, et entrez manuellement le numéro AS homologue. Dans cet exemple, 65510 est pour le site 2 FTD. Cliquez sur config-options et choisissez properties.



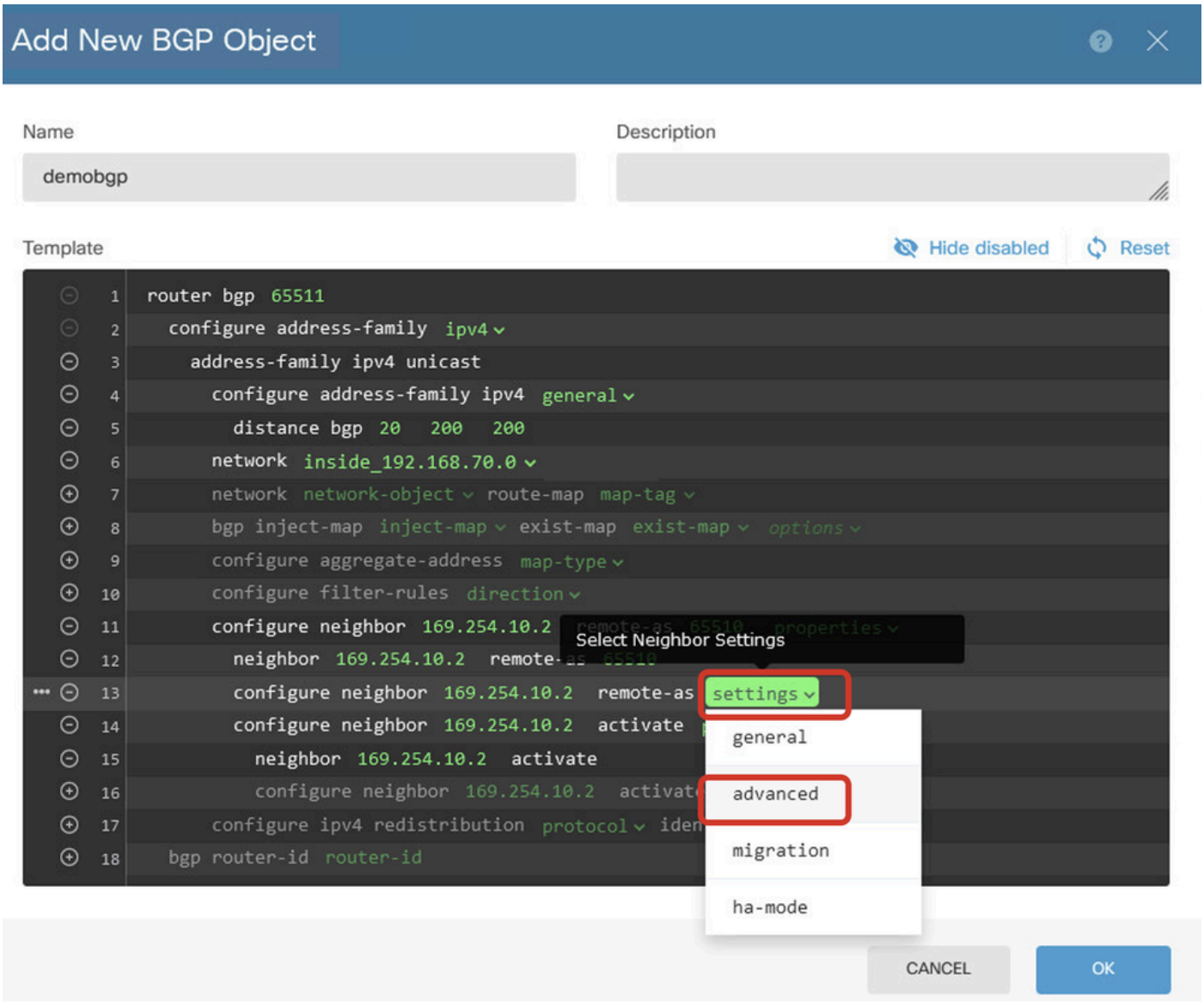
Create_BGP_Object_NeighborSetting

Ligne 14 : Cliquez sur l'icône + afin d'activer la ligne pour configurer certaines propriétés du voisin. Cliquez sur activate-options et choisissez properties.



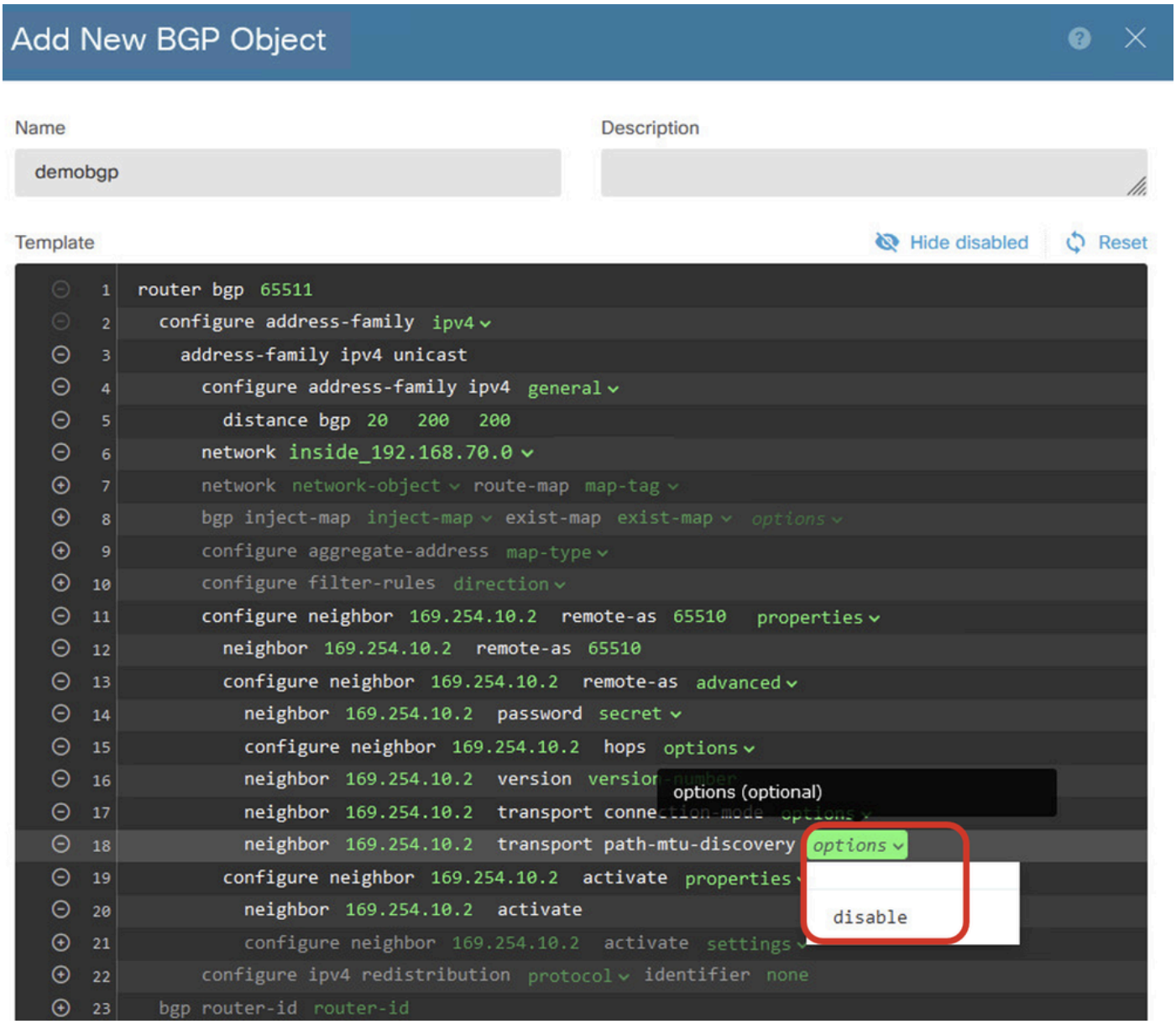
Create_BGP_Object_NeighborSetting_Properties

Ligne 13 : Cliquez sur l'icône + afin d'activer la ligne pour afficher les options avancées. Cliquez sur settings et choisissez advanced.



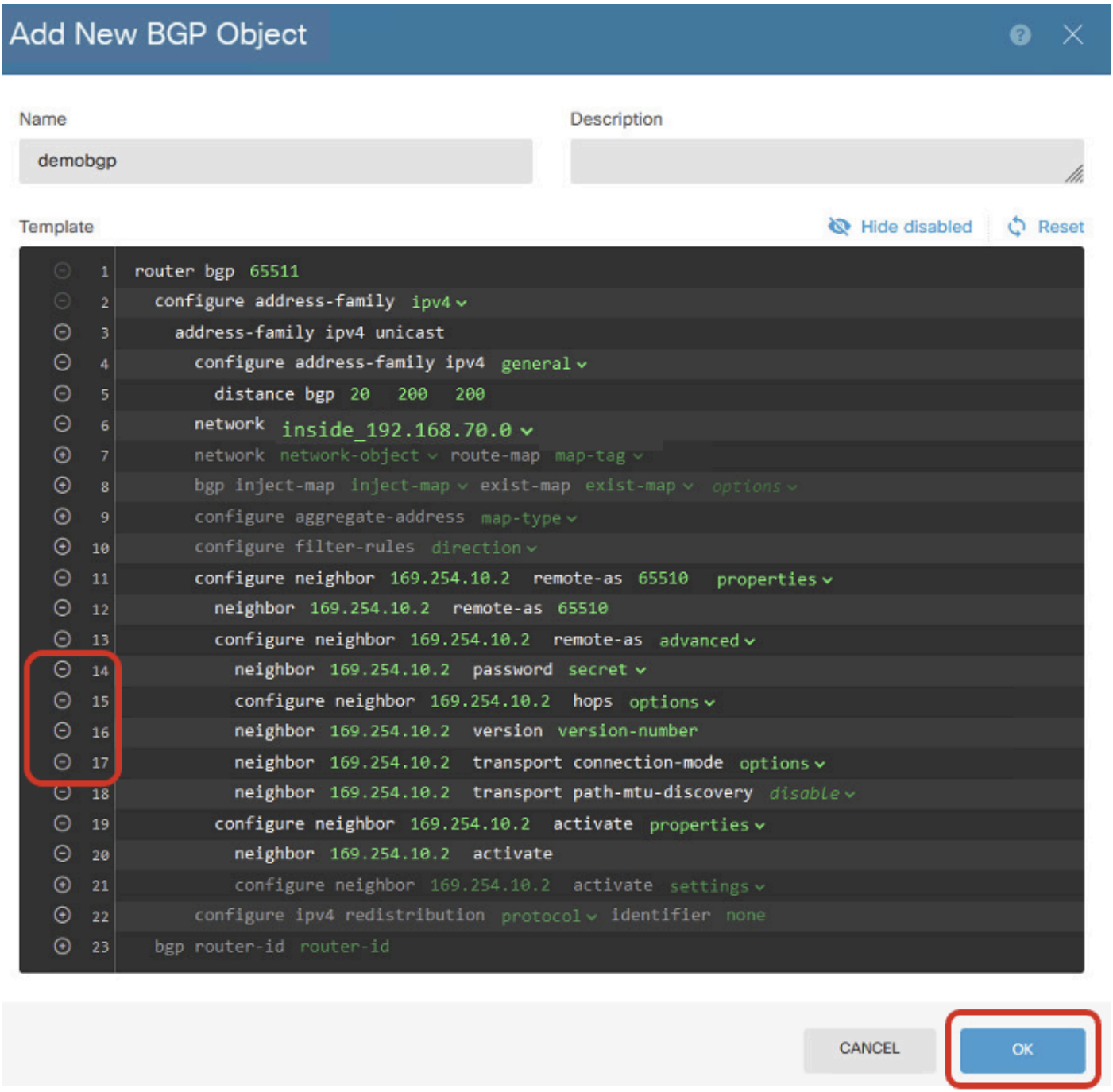
Create_BGP_Object_NeighborSetting_Properties_Advanced

Ligne 18 : Cliquez sur options et choisissez disable afin de désactiver la découverte de MTU de chemin.



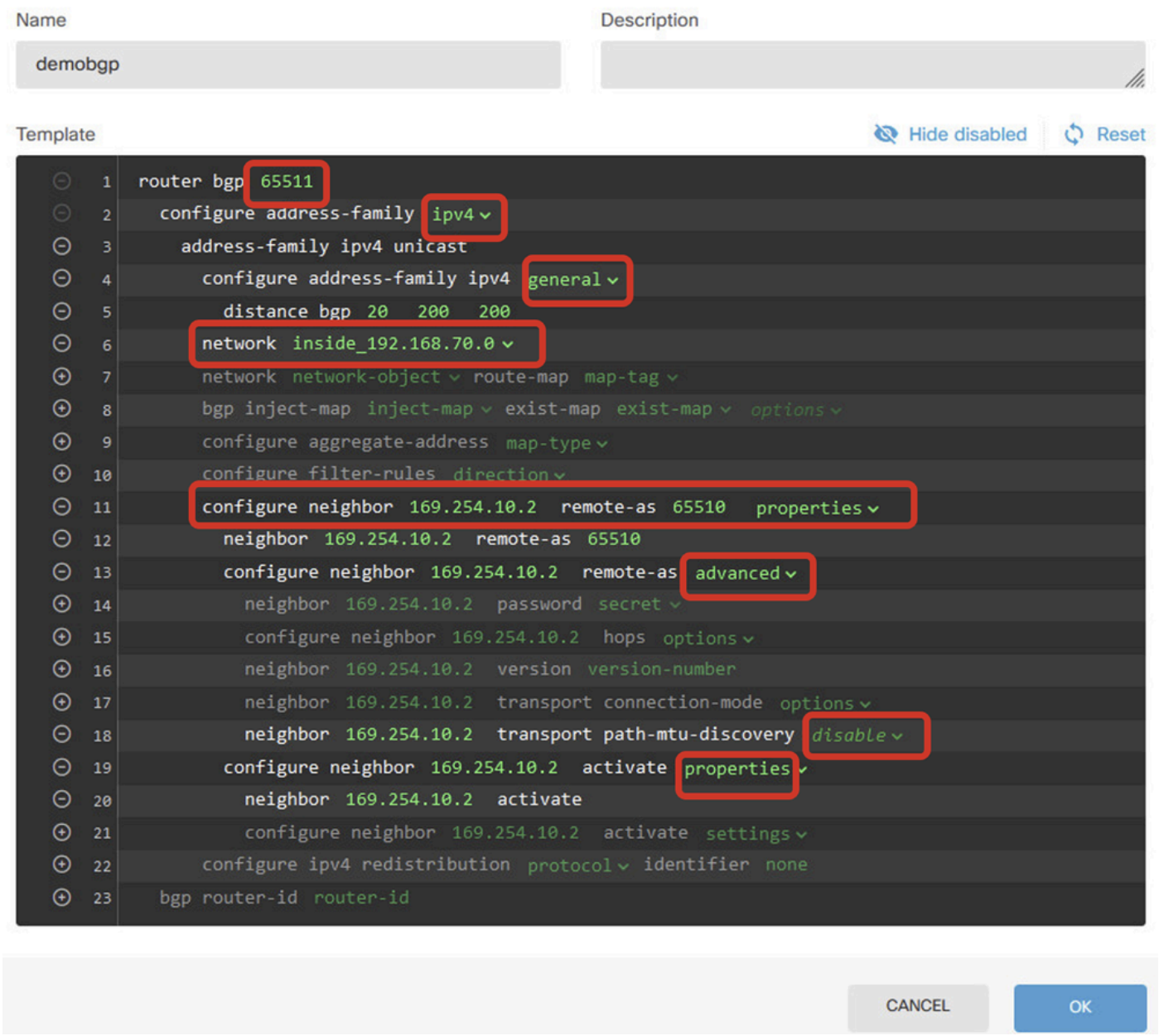
Create_BGP_Object_NeighborSetting_Properties_Advanced_PMD

Line 14, 15, 16, 17 : Cliquez sur le - bouton afin de désactiver les lignes. Cliquez ensuite sur le bouton OK pour enregistrer l'objet BGP.



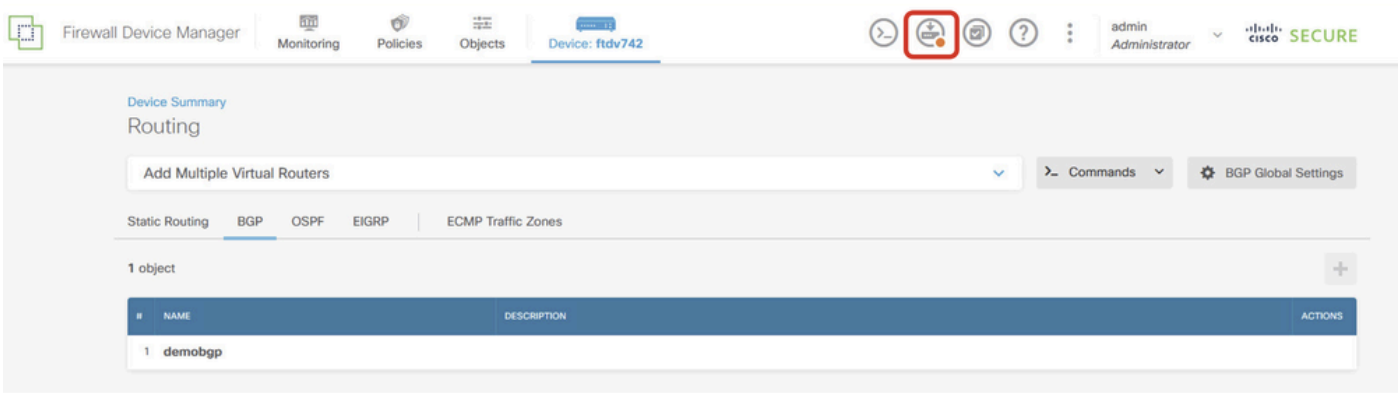
Create_BGP_Object_DisableLines

Ceci est une vue d'ensemble du paramètre BGP dans cet exemple. Vous pouvez configurer les autres paramètres BGP selon vos besoins réels.



Create_BGP_Object_Final_Overview

Étape 7. Déployez les modifications de configuration BGP.



Configuration_BGP_Déploiement

Étape 8. La configuration du FTD du site 1 est maintenant terminée.

Afin de configurer le VPN FTD et le BGP du Site2, répétez l'étape 3. à l'étape 7. avec les paramètres correspondants du FTD du Site2.

Vue d'ensemble de la configuration de Site1 FTD et Site2 FTD dans CLI.

Site1 FTD	Site2 FTD
NGFW version 7.4.2 interface GigabitEthernet0/0 nameif outside manuel de l'organisme de contrôle des transports aériens propagate sgt preserve-untag stratégie statique sgt désactivée approuvée niveau de sécurité 0 ip address 192.168.30.1 255.255.255.0 interface GigabitEthernet0/2 name if inside niveau de sécurité 0 ip address 192.168.70.1 255.255.255.0 interface Tunnel1 nameif demovti ip address 169.254.10.1 255.255.255.0 interface source du tunnel à l'extérieur tunnel destination 192.168.10.1 tunnel mode ipsec ipv4 tunnel protection ipsec profile ipsec_profile|e4084d322d réseau objet OutsideIPv4Gateway hôte 192.168.30.3 réseau objet inside_192.168.70.0 sous-réseau 192.168.70.0 255.255.255.0 access-group NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457 : POLITIQUE D'ACCÈS : NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457 : L5 RULE : Inside_Outside_Rule access-list NGFW_ONBOX_ACL groupe d'objets d'approbation avancée |acSvcg-268435457 ifc à l'intérieur de tout ifc en dehors de tout rule-id 268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id 268435458 : POLITIQUE D'ACCÈS : NGFW_Access_Policy	NGFW version 7.4.2 interface GigabitEthernet0/0 nameif outside manuel de l'organisme de contrôle des transports aériens propagate sgt preserve-untag stratégie statique sgt désactivée approuvée niveau de sécurité 0 ip address 192.168.10.1 255.255.255.0 interface GigabitEthernet0/2 name if inside niveau de sécurité 0 ip address 192.168.50.1 255.255.255.0 interface Tunnel1 nameif demovti25 ip address 169.254.10.2 255.255.255.0 interface source du tunnel à l'extérieur tunnel destination 192.168.30.1 tunnel mode ipsec ipv4 tunnel protection ipsec profile ipsec_profile|e4084d322d réseau objet OutsideIPv4Gateway hôte 192.168.10.3 réseau objet inside_192.168.50.0 sous-réseau 192.168.50.0 255.255.255.0 access-group NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457 : POLITIQUE D'ACCÈS : NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457 : L5 RULE : Inside_Outside_Rule access-list NGFW_ONBOX_ACL groupe d'objets d'approbation avancée |acSvcg-268435457 ifc à l'intérieur de tout ifc en dehors de tout rule-id 268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id 268435458 : POLITIQUE D'ACCÈS : NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458

```
access-list NGFW_ONBOX_ACL remark rule-id 268435458
: L5 RULE : Demo_allow
access-list NGFW_ONBOX_ACL advanced permit object-
group |acSvcg-268435458 any any rule-id 268435458
event-log both
access-list NGFW_ONBOX_ACL remark rule-id 1 :
POLITIQUE D'ACCÈS : NGFW_Access_Policy
access-list NGFW_ONBOX_ACL remark rule-id 1 : L5
RULE : DefaultActionRule
access-list NGFW_ONBOX_ACL advanced deny ip any any
rule-id 1

routeur bgp 65511
bgp log-neighbor-changes
bgp router-id vrf auto-assign
address-family ipv4 unicast
neighbor 169.254.10.2 remote-as 65510
neighbor 169.254.10.2 transport path-mtu-discovery disable
neighbor 169.254.10.2 activate
réseau 192.168.70.0
no auto-summary
aucune synchronisation
exit-address-family

route en dehors de 0.0.0.0 0.0.0.0 192.168.30.3 1

crypto ipsec ikev2 ipsec-proposition AES256_SHA256
protocole esp encryption aes-256 aes
protocole intégrité esp sha-256 sha-1

crypto ipsec profile ipsec_profile|e4084d322d
set ikev2 ipsec-proposition AES256_SHA256
set security-association lifetime kilo-octets 4608000
set security-association lifetime secondes 28800

crypto ipsec security-association pmtu-aging infinite

crypto ikev2 policy 1
cryptage aes-256 aes
intégrité sha256 sha
groupe 14
prf sha256 sha
durée de vie secondes 86400

crypto ikev2 policy 20
cryptage aes-256 aes-192 aes
intégrité sha512 sha384 sha256 sha
```

```
: L5 RULE : Demo_allow
access-list NGFW_ONBOX_ACL advanced permit object-
group |acSvcg-268435458 any any rule-id 268435458
event-log both
access-list NGFW_ONBOX_ACL remark rule-id 1 :
POLITIQUE D'ACCÈS : NGFW_Access_Policy
access-list NGFW_ONBOX_ACL remark rule-id 1 : L5
RULE : DefaultActionRule
access-list NGFW_ONBOX_ACL advanced deny ip any any
rule-id 1

routeur bgp 65510
bgp log-neighbor-changes
bgp router-id vrf auto-assign
address-family ipv4 unicast
neighbor 169.254.10.1 remote-as 65511
neighbor 169.254.10.1 transport path-mtu-discovery disable
neighbor 169.254.10.1 activate
réseau 192.168.50.0
no auto-summary
aucune synchronisation
exit-address-family

route en dehors de 0.0.0.0 0.0.0.0 192.168.10.3 1

crypto ipsec ikev2 ipsec-proposition AES256_SHA256
protocole esp encryption aes-256 aes
protocole intégrité esp sha-256 sha-1

crypto ipsec profile ipsec_profile|e4084d322d
set ikev2 ipsec-proposition AES256_SHA256
set security-association lifetime kilo-octets 4608000
set security-association lifetime secondes 28800

crypto ipsec security-association pmtu-aging infinite

crypto ikev2 policy 1
cryptage aes-256 aes
intégrité sha256 sha
groupe 14
prf sha256 sha
durée de vie secondes 86400

crypto ikev2 policy 20
cryptage aes-256 aes-192 aes
intégrité sha512 sha384 sha256 sha
groupe 21 20 16 15 14
```

groupe 21 20 16 15 14 prf sha512 sha384 sha256 sha durée de vie secondes 86400 crypto ikev2 enable outside politique du groupe |s2sGP|192.168.10.1 interne politique du groupe Attributs |s2sGP|192.168.10.1 vpn-tunnel-protocol ikev2 tunnel-group 192.168.10.1 type ipsec-l2l tunnel-group 192.168.10.1 attributs-généraux default-group-policy |s2sGP|192.168.10.1 tunnel-group 192.168.10.1 ipsec-attributes ikev2 remote-authentication pre-shared-key ***** ikev2 local-authentication pre-shared-key *****	prf sha512 sha384 sha256 sha durée de vie secondes 86400 crypto ikev2 enable outside politique du groupe |s2sGP|192.168.30.1 interne politique du groupe Attributs |s2sGP|192.168.30.1 vpn-tunnel-protocol ikev2 tunnel-group 192.168.30.1 type ipsec-l2l tunnel-group 192.168.30.1 attributs-généraux default-group-policy |s2sGP|192.168.30.1 tunnel-group 192.168.30.1 ipsec-attributes ikev2 remote-authentication pre-shared-key ***** ikev2 local-authentication pre-shared-key *****

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Étape 1. Accédez à la CLI de chaque FTD via la console ou SSH afin de vérifier l'état VPN des phases 1 et 2 à travers les commandes show crypto ikev2 sa et show crypto ipsec sa.

Site1 FTD	Site2 FTD
ftdv742# show crypto ikev2 sa Associations de sécurité IKEv2 : ID de session:134, état:UP-ACTIVE, nombre d'IKE:1, nombre d'ENFANTS:1 Rôle d'état fvrf/ivrf local distant Tunnel-id 563984431 192.168.30.1/500 192.168.10.1/500 RÉPONDEUR GLOBAL/PRÊT POUR LE MONDE Encr : AES-CBC, taille de clé : 256, Hachage : SHA256, DH Grp : 14, Signe d'authentification : PSK, Vérification de l'authentification : PSK Durée de vie/Durée active : 86400/5145 s Sas enfant : sélecteur local 0.0.0.0/0 - 255.255.255.255/65535	ftdv742# show crypto ikev2 sa Associations de sécurité IKEv2 : ID de session:13, état:UP-ACTIVE, nombre d'IKE:1, nombre d'ENFANTS:1 Rôle d'état fvrf/ivrf local distant Tunnel-id 339797985 192.168.10.1/500 192.168.30.1/500 INITIATEUR PRÊT POUR LE MONDE/MONDIAL Encr : AES-CBC, taille de clé : 256, Hachage : SHA256, DH Grp : 14, Signe d'authentification : PSK, Vérification de l'authentification : PSK Durée de vie/Durée active : 86400/74099 sec Sas enfant : sélecteur local 0.0.0.0/0 - 255.255.255.255/65535 sélecteur distant 0.0.0.0/0 - 255.255.255.255/65535 Entrée/sortie spi ESP : 0xb7b5b38b/0xf0c4239d

sélecteur distant 0.0.0.0/0 - 255.255.255.255/65535 Entrée/sortie spi ESP : 0xf0c4239d/0xb7b5b38b	
ftdv742# show crypto ipsec sa interface : demovti Étiquette de crypto-carte : __vti-crypto-map-Tunnel1-0-1, numéro de séquence : 65280, adresse locale : 192.168.30.1 VRF protégé (VRF) : Global identificateur local (addr/mask/port/port) : (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/port/port) : (0.0.0.0/0.0.0.0/0/0) current_peer : 192.168.10.1 #pkts encaps : 5720, #pkts encrypt : 5720, #pkts digest : 5720 #pkts decaps : 5717, #pkts decrypt : 5717, #pkts verify : 5717 #pkts compressé : 0, #pkts décompressé : 0 #pkts non compressé : 5720, #pkts échec comp : 0, #pkts échec dép : 0 #pre-frag réussites : 0, #pre-frag échecs : 0, #fragments créé : 0 #PMTUs envoyé : 0, #PMTUs rcvd : 0, #decapsulated frgs nécessitant un réassemblage : 0 #TFC rcvd : 0, #TFC envoyé : 0 #Valid Erreurs ICMP rcvd : 0, #Invalid Erreurs ICMP rcvd : 0 #send erreurs : 0, #recv erreurs : 0 terminal de chiffrement local : 192.168.30.1/500, terminal de chiffrement distant : 192.168.10.1/500 path mtu 1500, surcharge ipsec 78(44), media mtu 1500 Temps PMTU restant (s) : 0, stratégie DF : copy-df Validation des erreurs ICMP : désactivée, paquets TFC : désactivée spi sortant actuel : B7B5B38B	ftdv742# show crypto ipsec sa interface : demovti25 Étiquette de crypto-carte : __vti-crypto-map-Tunnel1-0-1, numéro de séquence : 65280, adresse locale : 192.168.10.1 VRF protégé (VRF) : Global identificateur local (addr/mask/port/port) : (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/port/port) : (0.0.0.0/0.0.0.0/0/0) current_peer : 192.168.30.1 #pkts encaps : 5721, #pkts encrypt : 5721, #pkts digest : 5721 #pkts decaps : 5721, #pkts decrypt : 5721, #pkts verify : 5721 #pkts compressé : 0, #pkts décompressé : 0 #pkts non compressé : 5721, #pkts échec comp : 0, #pkts échec dép : 0 #pre-frag réussites : 0, #pre-frag échecs : 0, #fragments créé : 0 #PMTUs envoyé : 0, #PMTUs rcvd : 0, #decapsulated frgs nécessitant un réassemblage : 0 #TFC rcvd : 0, #TFC envoyé : 0 #Valid Erreurs ICMP rcvd : 0, #Invalid Erreurs ICMP rcvd : 0 #send erreurs : 0, #recv erreurs : 0 terminal de chiffrement local : 192.168.10.1/500, terminal de chiffrement distant : 192.168.30.1/500 path mtu 1500, surcharge ipsec 78(44), media mtu 1500 Temps PMTU restant (s) : 0, stratégie DF : copy-df Validation des erreurs ICMP : désactivée, paquets TFC : désactivée spi sortants actuels : F0C4239D

spi entrant actuel : F0C4239D sas esp entrants : spi : 0xF0C4239D (4039386013) État SA : actif transformation : esp-aes-256 esp-sha-256-hmac pas de compression paramètres d'utilisation ={L2L, Tunnel, IKEv2, VTI, } slot : 0, conn_id : 266, crypto-map : __vti-crypto- map-Tunnel1-0-1 sa timing : durée de vie restante de la clé (kB/s) : (4285389/3722) Taille IV : 16 octets support de détection de relecture : Y Bitmap anti-relecture : 0xFFFFFFF 0xFFFFFFFF sas esp sortants : spi : 0xB7B5B38B (3082138507) État SA : actif transformation : esp-aes-256 esp-sha-256-hmac pas de compression paramètres d'utilisation ={L2L, Tunnel, IKEv2, VTI, } slot : 0, conn_id : 266, crypto-map : __vti-crypto- map-Tunnel1-0-1 sa timing : durée de vie restante de la clé (kB/s) : (4147149/3722) Taille IV : 16 octets support de détection de relecture : Y Bitmap anti-relecture : 0x00000000 0x00000001	spi entrant actuel : B7B5B38B sas esp entrants : spi : 0xB7B5B38B (3082138507) État SA : actif transformation : esp-aes-256 esp-sha-256-hmac pas de compression paramètres d'utilisation ={L2L, Tunnel, IKEv2, VTI, } slot : 0, conn_id : 160, crypto-map : __vti-crypto- map-Tunnel1-0-1 sa timing : durée de vie restante de la clé (kB/s) : (3962829/3626) Taille IV : 16 octets support de détection de relecture : Y Bitmap anti-relecture : 0xFFFFFFF 0xFFFFFFFF sas esp sortants : spi : 0xF0C4239D (4039386013) État SA : actif transformation : esp-aes-256 esp-sha-256-hmac pas de compression paramètres d'utilisation ={L2L, Tunnel, IKEv2, VTI, } slot : 0, conn_id : 160, crypto-map : __vti-crypto- map-Tunnel1-0-1 sa timing : durée de vie restante de la clé (kB/s) : (4101069/3626) Taille IV : 16 octets support de détection de relecture : Y Bitmap anti-relecture : 0x00000000 0x00000001

Étape 2. Accédez à la CLI de chaque FTD via la console ou SSH afin de vérifier l'état BGP en utilisant les commandes show bgp neighbors et show route bgp.

Site1 FTD	Site2 FTD
ftdv742# show bgp neighbors Le voisin BGP est 169.254.10.2, vrf single_vf, remote AS 65510, liaison externe BGP version 4, ID de routeur distant 192.168.50.1 État BGP = établi, jusqu'à 1d20h Dernière lecture 00:00:25, dernière écriture	ftdv742# show bgp neighbors Le voisin BGP est 169.254.10.1, vrf single_vf, remote AS 65511, liaison externe BGP version 4, ID de routeur distant 192.168.70.1 État BGP = établi, jusqu'à 1d20h Dernière lecture 00:00:11, dernière écriture

00:00:45, temps d'attente de 180 secondes, intervalle de test d'activité de 60 secondes Sessions voisines : 1 actif, n'est pas multisession (désactivé) Fonctionnalités de voisinage : Actualisation de la route : annoncée et reçue (nouvelle) Capacité ASN de quatre octets : annoncée et reçue Famille d'adresses IPv4 Unicast : annoncé et reçu Fonctionnalité multisession : Statistiques des messages : La profondeur InQ est 0 La profondeur OutQ est 0 Envoi reçu Ouvertures : 1 1 Notifications : 0 0 Mises à jour : 2 2 Keepalives : 2 423 2 427 Actualisation de la route : 0 0 Total : 2 426 2 430 La durée minimale par défaut entre les exécutions de publication est de 30 secondes Pour la famille d'adresses : monodiffusion IPv4 Session : 169.254.10.2 Table BGP version 3, voisin version 3/0 Taille de la file d'attente de sortie : 0 Index 1 1 membre du groupe de mise à jour Envoi reçu Exercice avec préfixe : ---- ---- Préfixes actuels : 1 1 (Consomme 80 octets) Total des préfixes : 1 1 Retrait implicite : 0 0 Retrait explicite : 0 0 Utilisé comme meilleur chemin : n/a 1 Utilisé comme chemin multiple : n/a 0 Sortant entrant Préfixes de stratégie locale refusés : -------- ------ - Meilleur chemin à partir de cet homologue : 1 n/a	00:00:52, temps d'attente de 180 secondes, intervalle de test d'activité de 60 secondes Sessions voisines : 1 actif, n'est pas multisession (désactivé) Fonctionnalités de voisinage : Actualisation de la route : annoncée et reçue (nouvelle) Capacité ASN de quatre octets : annoncée et reçue Famille d'adresses IPv4 Unicast : annoncé et reçu Fonctionnalité multisession : Statistiques des messages : La profondeur InQ est 0 La profondeur OutQ est 0 Envoi reçu Ouvertures : 1 1 Notifications : 0 0 Mises à jour : 2 2 Keepalives : 2 424 2 421 Actualisation de la route : 0 0 Total : 2 427 2 424 La durée minimale par défaut entre les exécutions de publication est de 30 secondes Pour la famille d'adresses : monodiffusion IPv4 Session : 169.254.10.1 Table BGP version 9, voisin version 9/0 Taille de la file d'attente de sortie : 0 Index 4 4 membre du groupe de mise à jour Envoi reçu Exercice avec préfixe : ---- ---- Préfixes actuels : 1 1 (Consomme 80 octets) Total des préfixes : 1 1 Retrait implicite : 0 0 Retrait explicite : 0 0 Utilisé comme meilleur chemin : n/a 1 Utilisé comme chemin multiple : n/a 0 Sortant entrant Préfixes de stratégie locale refusés : -------- ------ - Meilleur chemin à partir de cet homologue : 1 n/a

Total : 1 0 Nombre d'INRP dans la mise à jour envoyée : max 1, min 0 Le suivi d'adresse est activé, le RIB dispose d'une route vers 169.254.10.2 Connexions établies 1 ; abandonnées 0 Dernière réinitialisation jamais Transport(tcp) path-mtu-discovery est désactivé Graceful-Restart est désactivé	Total : 1 0 Nombre d'INRP dans la mise à jour envoyée : max 1, min 0 Le suivi d'adresse est activé, le RIB dispose d'une route vers 169.254.10.1 Connexions établies 4 ; abandonnées 3 Dernière réinitialisation 1d21h, due à l'affaissement de l'interface de la session 1 Transport(tcp) path-mtu-discovery est désactivé Graceful-Restart est désactivé
ftdv742# show route bgp Codes : L - local, C - connecté, S - statique, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP externe, O - OSPF, IA - OSPF inter-zone N1 - OSPF NSSA de type externe 1, N2 - OSPF NSSA de type externe 2 E1 - OSPF de type externe 1, E2 - OSPF de type externe 2, V - VPN i - IS-IS, su - Résumé IS-IS, L1 - IS-IS niveau 1, L2 - IS-IS niveau 2 ia - IS-IS inter-zone, * - candidat default, U - route statique par utilisateur o - ODR, P - route statique téléchargée périodiquement, + - route répliquée SI - InterVRF statique, BI - BGP InterVRF La passerelle de dernier recours est 192.168.30.3 vers le réseau 0.0.0.0 B 192.168.50.0 255.255.255.0 [20/0] via 169.254.10.2, 1d20h	ftdv742# show route bgp Codes : L - local, C - connecté, S - statique, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP externe, O - OSPF, IA - OSPF inter-zone N1 - OSPF NSSA de type externe 1, N2 - OSPF NSSA de type externe 2 E1 - OSPF de type externe 1, E2 - OSPF de type externe 2, V - VPN i - IS-IS, su - Résumé IS-IS, L1 - IS-IS niveau 1, L2 - IS-IS niveau 2 ia - IS-IS inter-zone, * - candidat default, U - route statique par utilisateur o - ODR, P - route statique téléchargée périodiquement, + - route répliquée SI - InterVRF statique, BI - BGP InterVRF La passerelle de dernier recours est 192.168.10.3 vers le réseau 0.0.0.0 B 192.168.70.0 255.255.255.0 [20/0] via 169.254.10.1, 1d20h

Étape 3. Le client Site1 et le client Site2 s’envoient des requêtes ping.

Client Site1 :

```
Site1_Client#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/56/90 ms
```

Client Site2 :

```
Site2_Client#ping 192.168.70.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.70.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/39/71 ms
```

Dépannage

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

Vous pouvez utiliser ces commandes debug afin de 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 afin de dépanner la section BGP.

```
ftdv742# debug ip bgp ?

A.B.C.D    BGP neighbor address
all All    address families
events     BGP events
import     BGP path import across topologies, VRFs or AFs in BGP Inbound information
ipv4       Address family
ipv6       Address family
keepalives BGP keepalives
out        BGP Outbound information
range      BGP dynamic range
rib-filter Next hop route watch filter events
updates    BGP updates
vpnv4      Address family
vpnv6      Address family
vrf        VRF scope
<cr>
```

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.