Exemple de configuration d'ASA/PIX avec OSPF

Contenu

Introduction

Ce document décrit comment configurer le Cisco ASA pour apprendre les routes par l'intermédiaire de l'Open Shortest Path First (OSPF), exécuter l'authentification, et la redistribution.

Reportez-vous à PIX/ASA 8.X : Configuration du protocole EIGRP sur le dispositif de sécurité adaptatif Cisco (ASA) pour plus d'informations sur la configuration du protocole EIGRP.

Remarque : le routage asymétrique n'est pas pris en charge dans ASA/PIX.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Cisco ASA/PIX doit exécuter la version 7.x ou ultérieure.
- OSPF n'est pas pris en charge en mode multicontexte ; il est pris en charge uniquement en mode unique.

Components Used

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

- Dispositif de sécurité adaptatif (ASA) de la gamme Cisco 5500 qui exécute les versions 8.0 et ultérieures du logiciel
- Logiciel Cisco Adaptive Security Device Manager (ASDM) version 6.0 et ultérieure

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. If your network is live, make sure that you understand the potential impact of any command.

Produits connexes

Les informations de ce document s'appliquent également au pare-feu PIX de la gamme Cisco 500 qui exécute les versions 8.0 et ultérieures du logiciel.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Le protocole OSPF utilise un algorithme d'état des liaisons afin de créer et de calculer le chemin le plus court vers toutes les destinations connues. Chaque routeur d'une zone OSPF contient une base de données d'état des liaisons identique, qui est une liste de chacune des interfaces utilisables du routeur et des voisins accessibles.

Les avantages du protocole OSPF par rapport au protocole RIP sont les suivants :

- Les mises à jour de la base de données d'état des liaisons OSPF sont envoyées moins fréquemment que les mises à jour RIP et la base de données d'état des liaisons est mise à jour instantanément plutôt que progressivement lorsque les informations obsolètes sont arrivées à expiration.
- Les décisions de routage sont basées sur le coût, qui indique la surcharge requise pour envoyer des paquets sur une interface donnée. L'appliance de sécurité calcule le coût d'une interface en fonction de la bande passante de liaison plutôt que du nombre de sauts vers la destination. Le coût peut être configuré pour spécifier les chemins préférés.

L'inconvénient des algorithmes de chemin le plus court est qu'ils nécessitent beaucoup de cycles de processeur et de mémoire.

L'appliance de sécurité peut exécuter deux processus du protocole OSPF simultanément, sur différents ensembles d'interfaces. Vous pouvez exécuter deux processus si vous avez des interfaces qui utilisent les mêmes adresses IP (NAT permet à ces interfaces de coexister, mais

OSPF ne permet pas le chevauchement des adresses). Vous pouvez également exécuter un processus à l'intérieur et un autre à l'extérieur, et redistribuer un sous-ensemble de routes entre les deux processus. De même, vous devrez peut-être séparer les adresses privées des adresses publiques.

Vous pouvez redistribuer des routes dans un processus de routage OSPF à partir d'un autre processus de routage OSPF, d'un processus de routage RIP ou de routes statiques et connectées configurées sur des interfaces compatibles OSPF.

L'appliance de sécurité prend en charge les fonctions OSPF suivantes :

- Prise en charge des routes intra-zone, interzone et externes (Type I et Type II).
- Prise en charge d'une liaison virtuelle.
- Inondation de LSA OSPF.
- Authentification aux paquets OSPF (authentification par mot de passe et MD5).
- Prise en charge de la configuration de l'appliance de sécurité en tant que routeur désigné ou routeur de sauvegarde désigné. Le dispositif de sécurité peut également être configuré en tant qu'ABR. Cependant, la possibilité de configurer l'appliance de sécurité en tant qu'ASBR est limitée aux informations par défaut uniquement (par exemple, l'injection d'une route par défaut).
- Prise en charge des zones de stub et des zones de non-stubby.
- Filtrage LSA de type 3 du routeur de périphérie de zone.

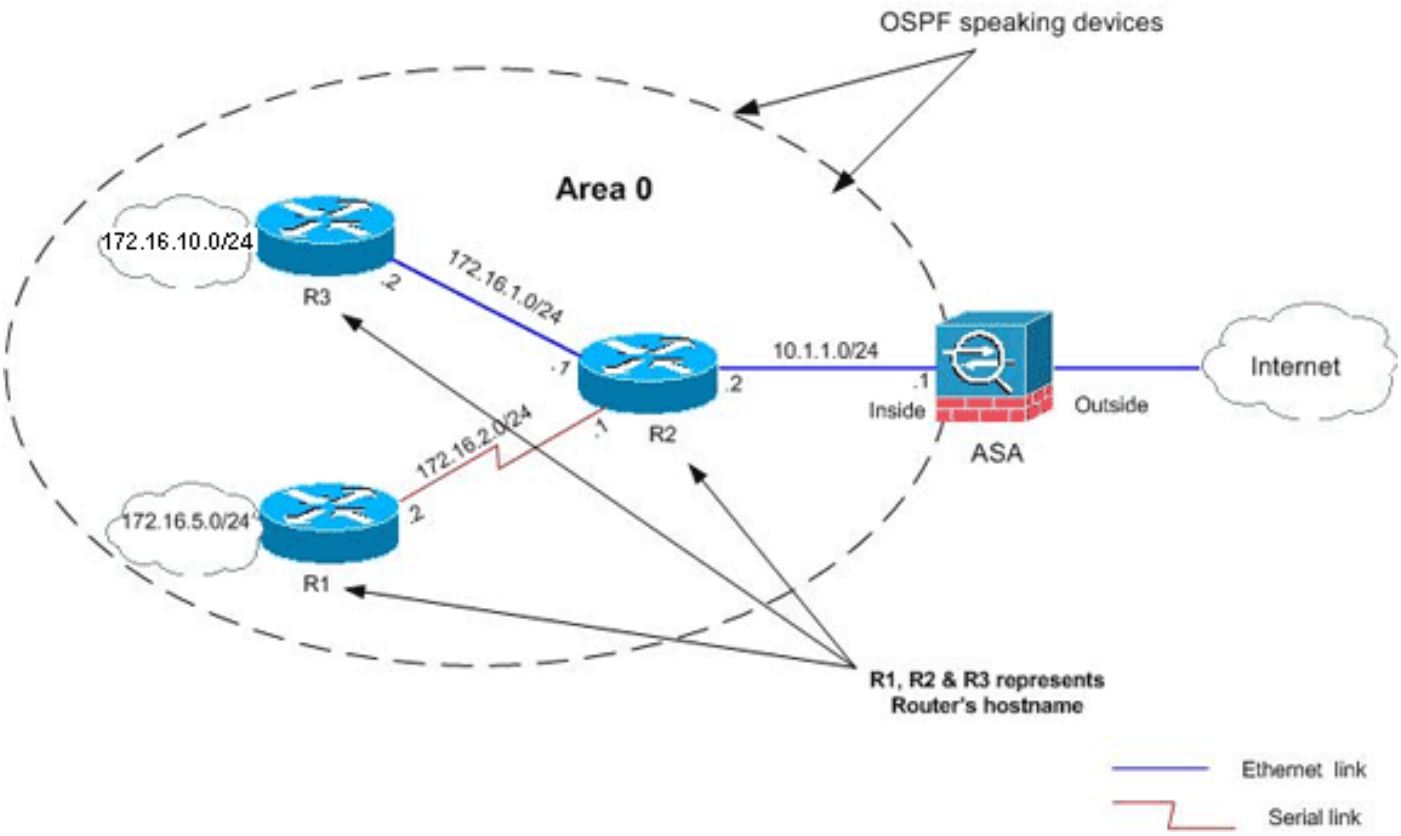
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) afin d'obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Dans cette topologie de réseau, l'adresse IP de l'interface interne Cisco ASA est 10.1.1.1/24. L'objectif est de configurer OSPF sur Cisco ASA afin d'apprendre les routes vers les réseaux internes (172.16.1.0/24, 172.16.2.0/24, 172.16.5.0/24 et 172.16.10.0/24) de manière dynamique via le routeur adjacent (R2). R2 apprend les routes vers les réseaux internes distants via les deux autres routeurs (R1 et R3).

Configurations

Ce document utilise les configurations suivantes :

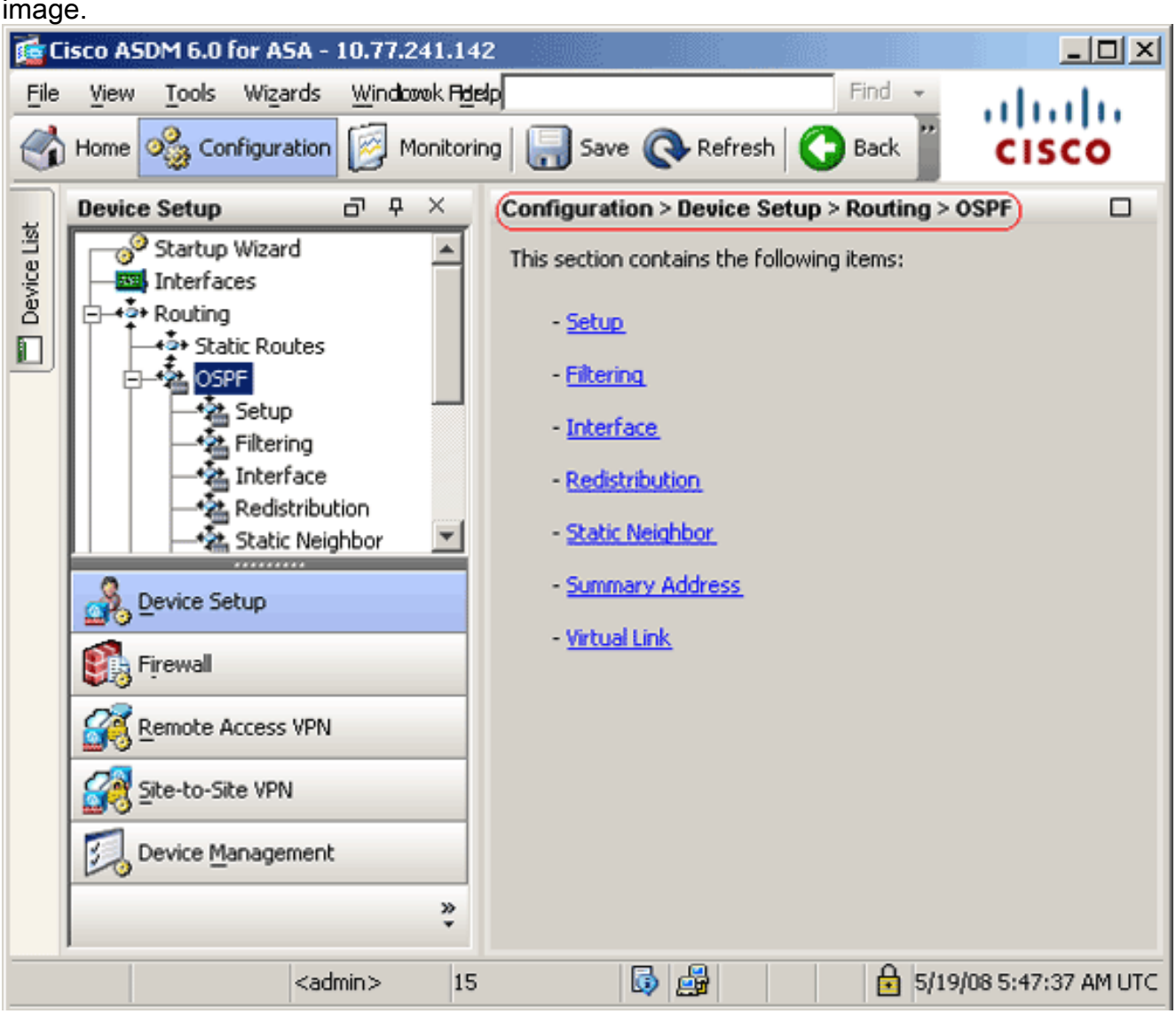
- Configuration ASDM
- Configuration de l'authentification OSPF
- Configuration CLI de Cisco ASA
- Configuration CLI du routeur Cisco IOS (R2)
- Configuration CLI du routeur Cisco IOS (R1)
- Configuration CLI du routeur Cisco IOS (R3)
- Redistribuer dans OSPF avec ASA

Configuration ASDM

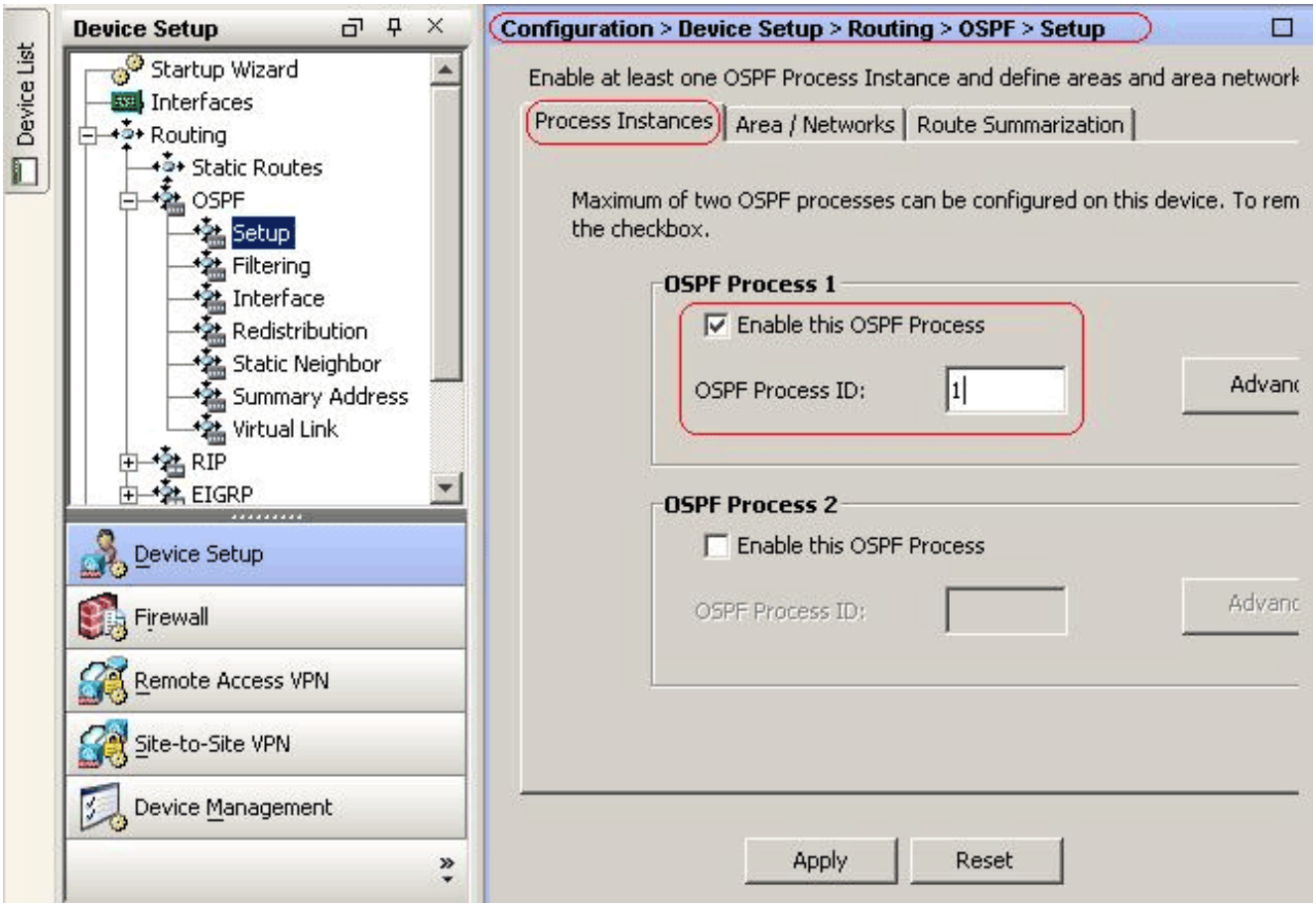
Adaptive Security Device Manager (ASDM) est une application basée sur navigateur utilisée pour configurer et surveiller le logiciel sur les appliances de sécurité. L'ASDM est chargé à partir de l'appliance de sécurité, puis utilisé pour configurer, surveiller et gérer le périphérique. Vous pouvez également utiliser le lanceur ASDM (Windows uniquement) afin de lancer l'application ASDM plus rapidement que l'applet Java. Cette section décrit les informations dont vous avez besoin pour configurer les fonctionnalités décrites dans ce document avec ASDM.

Complétez ces étapes afin de configurer OSPF dans Cisco ASA :

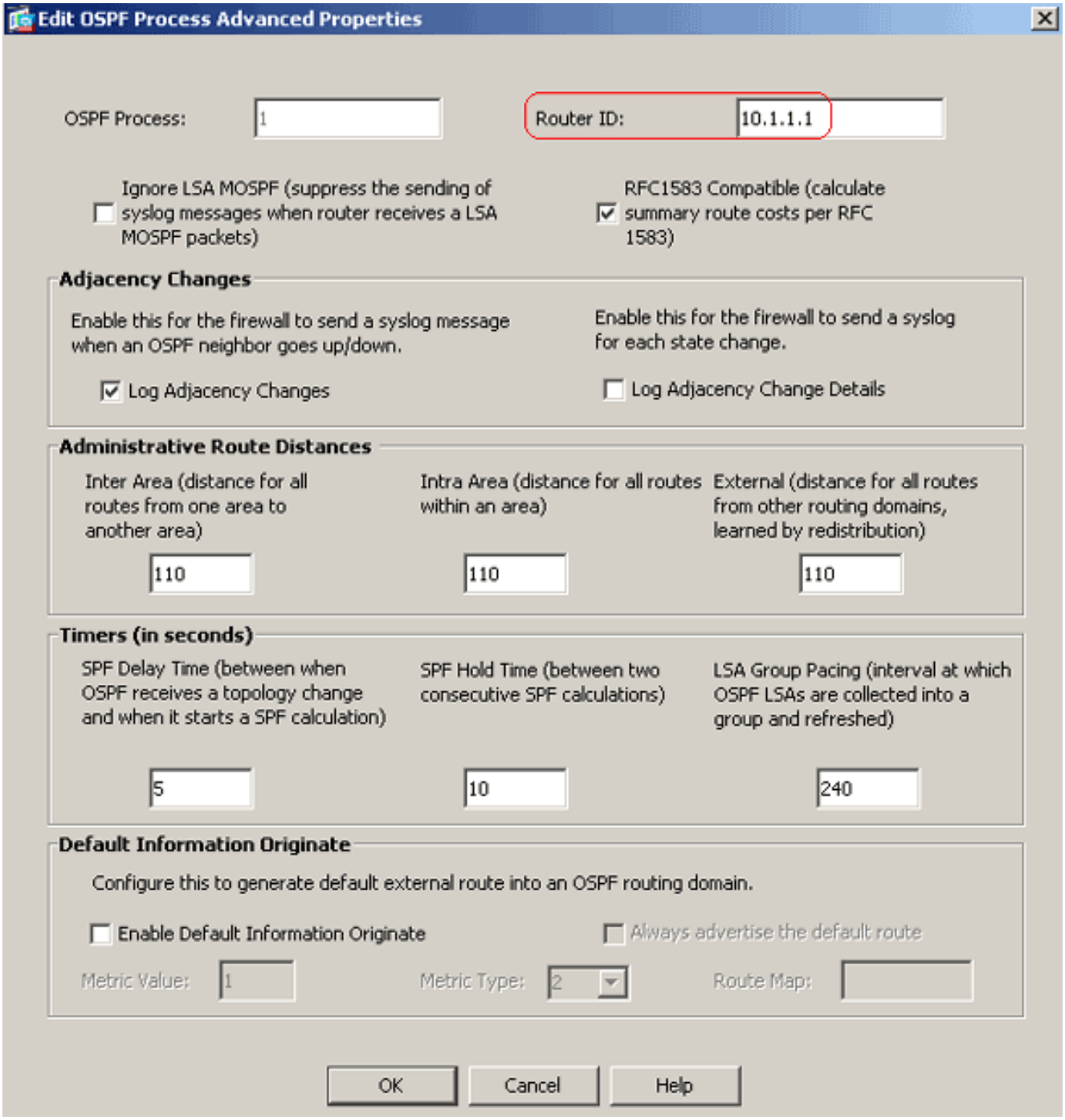
1. Connectez-vous à Cisco ASA avec ASDM.
2. Accédez à la zone **Configuration > Device Setup > Routing > OSPF** de l'interface ASDM, comme illustré dans cette
image.



3. Activez le processus de routage OSPF dans l'onglet **Setup > Process Instances**, comme illustré dans cette image. Dans cet exemple, le processus d'ID OSPF est **1**.



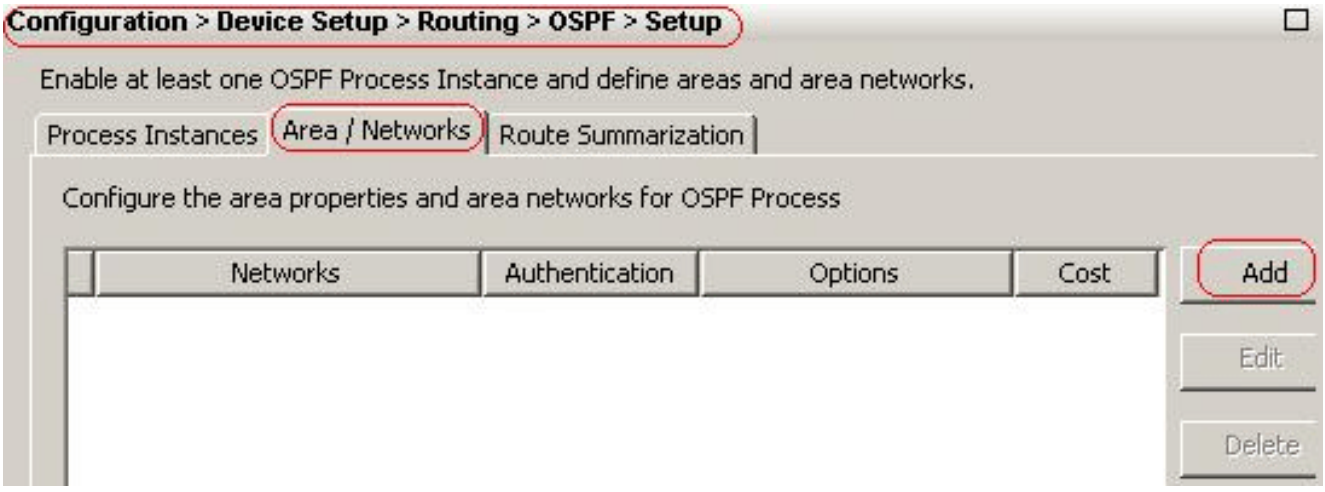
4. Vous pouvez cliquer sur **Avancé** dans l'onglet **Configuration > Instances de processus** afin de configurer des paramètres de processus de routage OSPF avancés facultatifs. Vous pouvez modifier des paramètres spécifiques au processus, tels que l'ID de routeur, les modifications de contiguïté, les distances de route administrative, les minuteurs et les paramètres d'origine des informations par
défaut.



Cette liste décrit chaque champ :Processus OSPF : affiche le processus OSPF que vous configurez. Vous ne pouvez pas modifier cette valeur.Router ID : afin d'utiliser un ID de routeur fixe, saisissez un ID de routeur au format d'adresse IP dans le champ Router ID. Si vous laissez cette valeur vide, l'adresse IP de niveau le plus élevé sur l'appliance de sécurité est utilisée comme ID de routeur.Dans cet exemple, l'ID de routeur est configuré de manière statique avec l'adresse IP de l'interface interne (10.1.1.1).Ignore LSA MOSPF : cochez cette case afin de supprimer l'envoi de messages du journal système lorsque l'appliance de sécurité reçoit des paquets LSA de type 6 (MOSPF). Ce paramètre est désactivé par défaut.Compatible RFC 1583 : cochez cette case afin de calculer les coûts de route récapitulatifs par RFC 1583. Désactivez cette case à cocher afin de calculer les coûts de route récapitulative par RFC 2328. Afin de minimiser les risques de boucles de routage, tous les périphériques OSPF dans un domaine de routage OSPF doivent avoir une compatibilité RFC définie de manière identique. Ce paramètre est sélectionné par défaut.Modifications de contiguïté : contient des paramètres qui définissent les modifications de contiguïté qui provoquent l'envoi de messages du journal système.Log Adjacency Changes : cochez cette

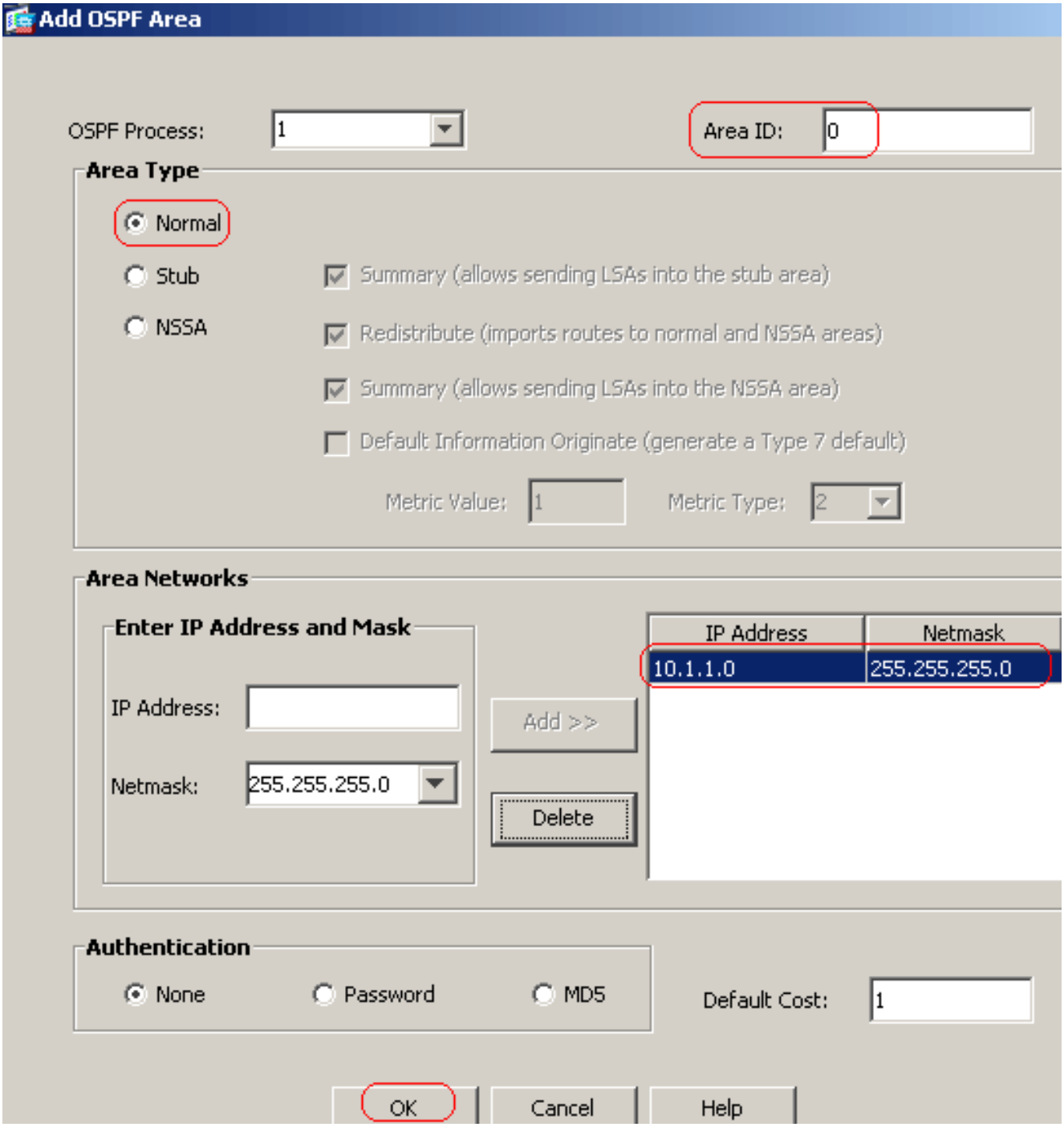
case afin que l'appliance de sécurité envoie un message de journal système chaque fois qu'un voisin OSPF s'active ou s'arrête. Ce paramètre est sélectionné par défaut.Log Adjacency Changes Detail : cochez cette case afin que l'appliance de sécurité envoie un message de journal système chaque fois qu'un changement d'état se produit, et pas seulement lorsqu'un voisin s'active ou s'arrête. Ce paramètre est désactivé par défaut.Administrative Route Distances : contient les paramètres des distances administratives des routes en fonction du type de route.Inter Area : définit la distance administrative de toutes les routes d'une zone à une autre. Les valeurs valides sont comprises entre 1 et 255. La valeur par défaut est 100.Intra Area : définit la distance administrative de toutes les routes d'une zone. Les valeurs valides sont comprises entre 1 et 255. La valeur par défaut est 100.External : définit la distance administrative de toutes les routes des autres domaines de routage qui sont apprises par le biais de la redistribution. Les valeurs valides sont comprises entre 1 et 255. La valeur par défaut est 100.Timers : contient les paramètres utilisés pour configurer le rythme LSA et les temporisateurs de calcul SPF.SPF Delay Time : indique le délai entre le moment où OSPF reçoit une modification de topologie et le début du calcul SPF. Les valeurs valides sont comprises entre 0 et 65535. La valeur par défaut est 5.SPF Hold Time : spécifie le temps d'attente entre les calculs SPF consécutifs.Les valeurs valides sont comprises entre 1 et 65534. La valeur par défaut est 10.LSA Group Pacing : spécifie l'intervalle auquel les LSA sont collectées dans un groupe et actualisées, récapitulées ou vieillies. Les valeurs valides sont comprises entre 10 et 1 800. La valeur par défaut est 240.Default Information Originate : contient les paramètres utilisés par un ASBR pour générer une route externe par défaut dans un domaine de routage OSPF.Enable Default Information Originate : cochez cette case afin d'activer la génération de la route par défaut dans le domaine de routage OSPF.Always advertise the default route : cochez cette case afin d'annoncer toujours la route par défaut. Cette option est désactivée par défaut.Metric Value : spécifie la métrique OSPF par défaut. Les valeurs valides sont comprises entre 0 et 16777214. La valeur par défaut est 1.Metric Type : spécifie le type de liaison externe associé à la route par défaut annoncée dans le domaine de routage OSPF. Les valeurs valides sont 1 ou 2, indiquant une route externe de type 1 ou 2. La valeur par défaut est 2.Route Map : (*Facultatif*) Nom de la route map à appliquer. Le processus de routage génère la route par défaut si le mappage de route est satisfait.

5. Après avoir effectué les étapes précédentes, définissez les réseaux et les interfaces qui participent au routage OSPF dans l'onglet **Setup > Area/Networks**, puis cliquez sur **Add** comme indiqué dans cette image :



La boîte de dialogue Add OSPF Area

s'affiche.

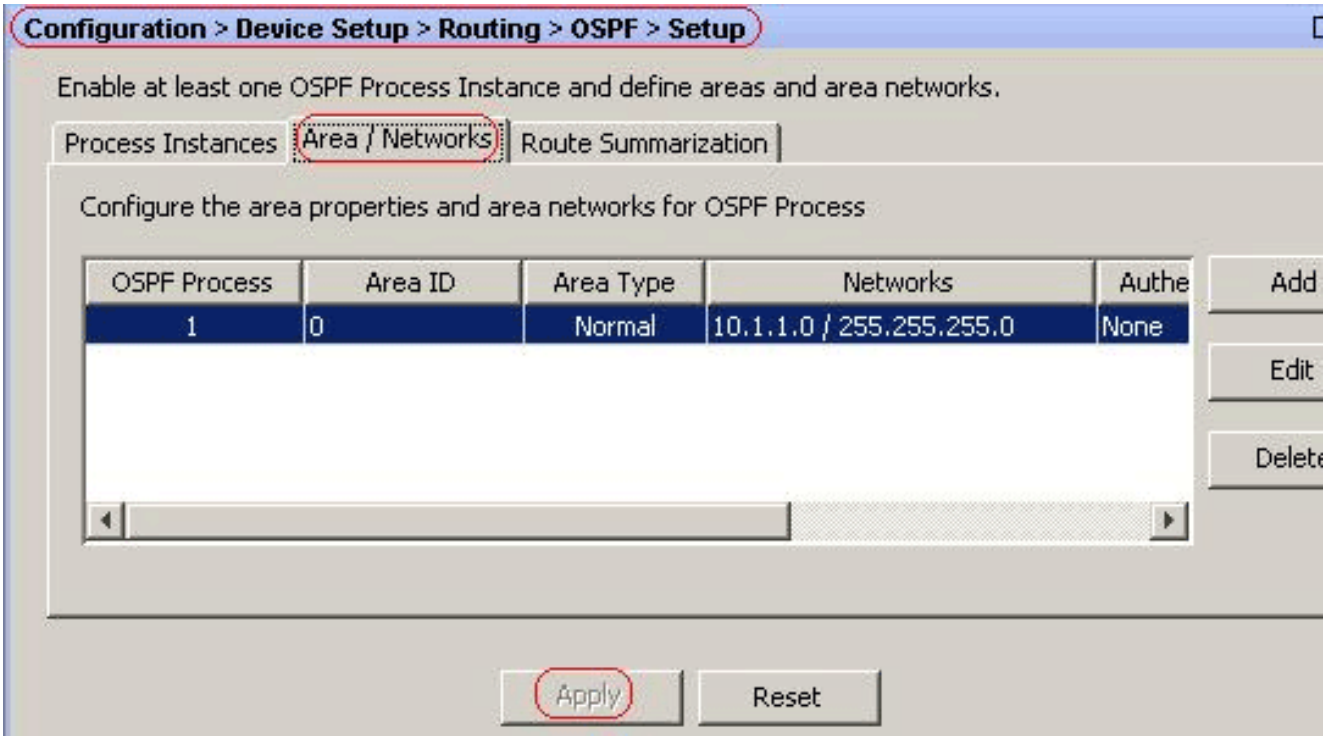


Dans cet exemple, le seul réseau qui est ajouté est le réseau interne (10.1.1.0/24), car OSPF est activé uniquement sur l'interface interne.**Remarque :** Seules les interfaces avec une adresse IP qui font partie des réseaux définis participent au processus de routage OSPF.

6. Click OK.Cette liste décrit chaque champ :Processus OSPF : lorsque vous ajoutez une nouvelle zone, choisissez l'ID du processus OSPF . Si un seul processus OSPF est activé sur l'appliance de sécurité, ce processus est sélectionné par défaut. Lorsque vous modifiez une zone existante, vous ne pouvez pas modifier l'ID de processus OSPF.ID de zone : lorsque vous ajoutez une nouvelle zone, saisissez l'ID de zone. Vous pouvez spécifier l'ID de zone sous la forme d'un nombre décimal ou d'une adresse IP. Les valeurs décimales valides vont de 0 à 4294967295. Vous ne pouvez pas modifier l'ID de zone lorsque vous modifiez une zone existante.Dans cet exemple, l'ID de zone est **0**.Area Type : contient les paramètres du type de zone en cours de configuration.Normal : sélectionnez cette option afin de faire de la zone une zone OSPF standard. Cette option est sélectionnée par défaut lorsque vous créez une zone pour la première fois.Stub : sélectionnez cette option afin de faire de la zone

une zone de stub. Les zones de stub n'ont pas de routeurs ou de zones au-delà. Les zones de stub empêchent les LSA externes AS (LSA de type 5) d'être inondées dans la zone de stub. Lorsque vous créez une zone de stub, vous pouvez décocher la case Résumé afin d'empêcher l'inondation des LSA récapitulatives (de type 3 et 4) dans la zone.Résumé : lorsque la zone définie est une zone de stub, décochez cette case afin d'empêcher l'envoi de LSA dans la zone de stub. Cette case à cocher est activée par défaut pour les zones de stub.NSSA : sélectionnez cette option afin de faire de la zone une zone non-si-stubby. Les NSSA acceptent les LSA de type 7. Lorsque vous créez une NSSA, vous pouvez décocher la case Résumé afin d'empêcher l'inondation des LSA récapitulatives dans la zone. En outre, vous pouvez décocher la case Redistribuer et activer l'origine des informations par défaut afin de désactiver la redistribution de route.Redistribute : décochez cette case afin d'empêcher l'importation de routes dans la NSSA. Cette case à cocher est activée par défaut.Résumé : lorsque la zone à définir est une NSSA, décochez cette case afin d'empêcher l'envoi de LSA dans la zone de stub. Cette case à cocher est activée par défaut pour les NSSA.Default Information Originate : cochez cette case afin de générer une valeur par défaut de type 7 dans la NSSA. Cette case est décochée par défaut.Metric Value : saisissez une valeur afin de spécifier la valeur de métrique OSPF pour la route par défaut. Les valeurs valides sont comprises entre 0 et 16777214. La valeur par défaut est 1.Metric Type : sélectionnez une valeur afin de spécifier le type de métrique OSPF pour la route par défaut. Les choix possibles sont 1 (type 1) ou 2 (type 2). La valeur par défaut est 2.Area Networks : contient les paramètres qui définissent une zone OSPF.Enter IP Address and Mask : contient les paramètres utilisés pour définir les réseaux de la zone.IP Address : saisissez l'adresse IP du réseau ou de l'hôte à ajouter à la zone. Utilisez 0.0.0.0 avec un masque de réseau de 0.0.0.0 pour créer la zone par défaut. Vous pouvez utiliser 0.0.0.0 dans une seule zone.Netmask : sélectionnez le masque de réseau pour l'adresse IP ou l'hôte à ajouter à la zone. Si vous ajoutez un hôte, sélectionnez le masque 255.255.255.255.Dans cet exemple, **10.1.1.0/24** est le réseau à configurer.Add : ajoute le réseau défini dans la zone Enter IP Address and Mask. Le réseau ajouté apparaît dans le tableau Réseaux de zone.Supprimer : supprime le réseau sélectionné du tableau Réseaux de zone.Area Networks : affiche les réseaux définis pour la zone.IP Address : affiche l'adresse IP du réseau.Netmask : affiche le masque de réseau du réseau.Authentication : contient les paramètres d'authentification de zone OSPF.None : sélectionnez cette option afin de désactiver l'authentification de zone OSPF. Voici la configuration par défaut .Password : sélectionnez cette option afin d'utiliser un mot de passe en texte clair pour l'authentification de zone. Cette option n'est pas recommandée lorsque la sécurité pose problème.MD5 : sélectionnez cette option afin d'utiliser l'authentification MD5.Coût par défaut : spécifiez un coût par défaut pour la zone. Les valeurs valides sont comprises entre 0 et 65535. La valeur par défaut est 1.

7. Cliquez sur
   Apply.



8. Vous pouvez éventuellement définir des filtres de routage dans le volet Règles de filtre. Le filtrage de route permet de contrôler davantage les routes autorisées à être envoyées ou reçues dans les mises à jour OSPF.
9. Vous pouvez éventuellement configurer la redistribution de route. Cisco ASA peut redistribuer les routes découvertes par RIP et EIGRP dans le processus de routage OSPF. Vous pouvez également redistribuer les routes statiques et connectées dans le processus de routage OSPF. Définissez la redistribution de route dans le volet Redistribution.
10. Les paquets Hello OSPF sont envoyés en tant que paquets de multidiffusion. Si un voisin OSPF est situé sur un réseau non diffusé, vous devez définir manuellement ce voisin. Lorsque vous définissez manuellement un voisin OSPF, des paquets Hello sont envoyés à ce voisin en tant que messages de monodiffusion. Afin de définir des voisins OSPF statiques, accédez au volet Voisin statique.
11. Les routes apprises à partir d'autres protocoles de routage peuvent être résumées. La métrique utilisée pour annoncer le résumé est la plus petite métrique de toutes les routes plus spécifiques. Les routes récapitulatives permettent de réduire la taille de la table de routage.L'utilisation de routes récapitulatives pour OSPF entraîne un ASBR OSPF à annoncer une route externe en tant qu'agrégat pour toutes les routes redistribuées qui sont couvertes par l'adresse. Seules les routes d'autres protocoles de routage qui sont redistribuées dans OSPF peuvent être résumées.
12. Dans le volet Liaison virtuelle, vous pouvez ajouter une zone à un réseau OSPF et il n'est pas possible de connecter directement la zone à la zone de backbone ; vous devez créer un lien virtuel. Une liaison virtuelle connecte deux périphériques OSPF qui ont une zone commune, appelée zone de transit. Un des périphériques OSPF doit être connecté à la zone de backbone.

Configuration de l'authentification OSPF

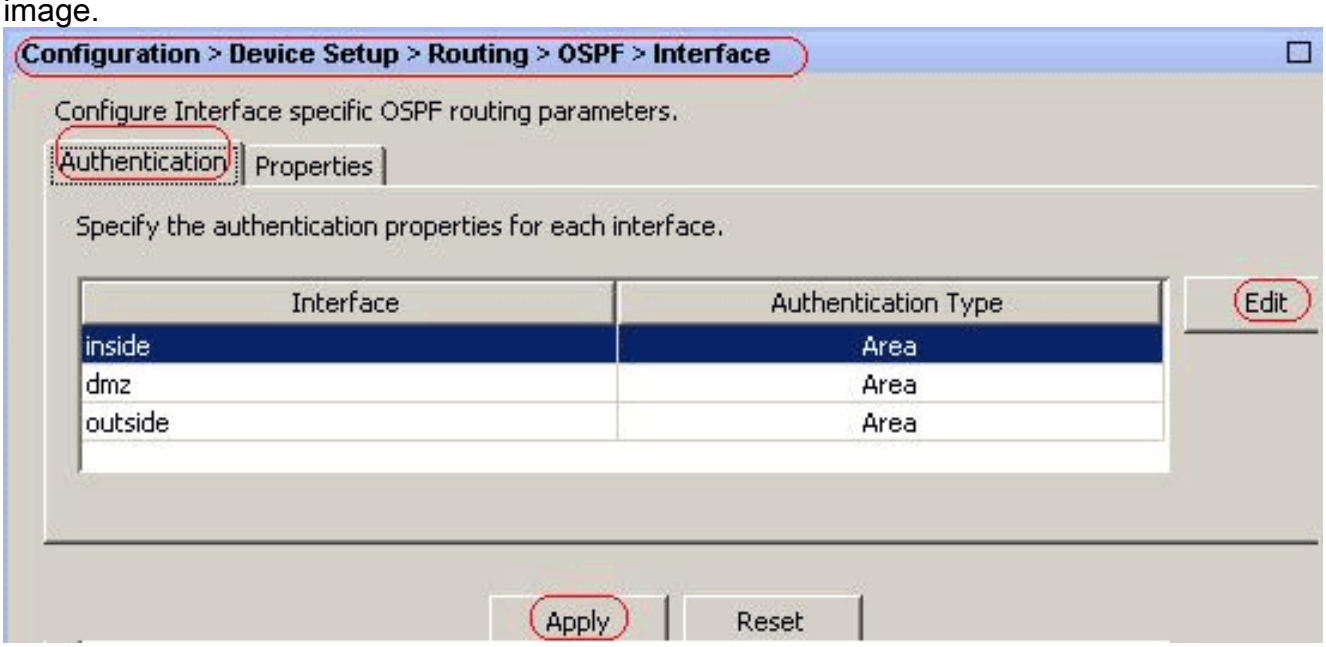
Cisco ASA prend en charge l'authentification MD5 des mises à jour de routage à partir du protocole de routage OSPF. Le résumé à clé MD5 de chaque paquet OSPF empêche l'introduction de messages de routage non autorisés ou faux provenant de sources non approuvées. L'ajout de l'authentification à vos messages OSPF garantit que vos routeurs et Cisco

ASA acceptent uniquement les messages de routage provenant d'autres périphériques de routage configurés avec la même clé pré-partagée. Sans cette authentification configurée, si quelqu'un introduit un autre périphérique de routage avec des informations de route différentes ou contraires sur le réseau, les tables de routage de vos routeurs ou de Cisco ASA peuvent devenir corrompues et une attaque par déni de service peut s'ensuivre. Lorsque vous ajoutez l'authentification aux messages EIGRP envoyés entre vos périphériques de routage (qui inclut l'ASA), cela empêche l'ajout intentionnel ou accidentel d'un autre routeur au réseau et tout problème.

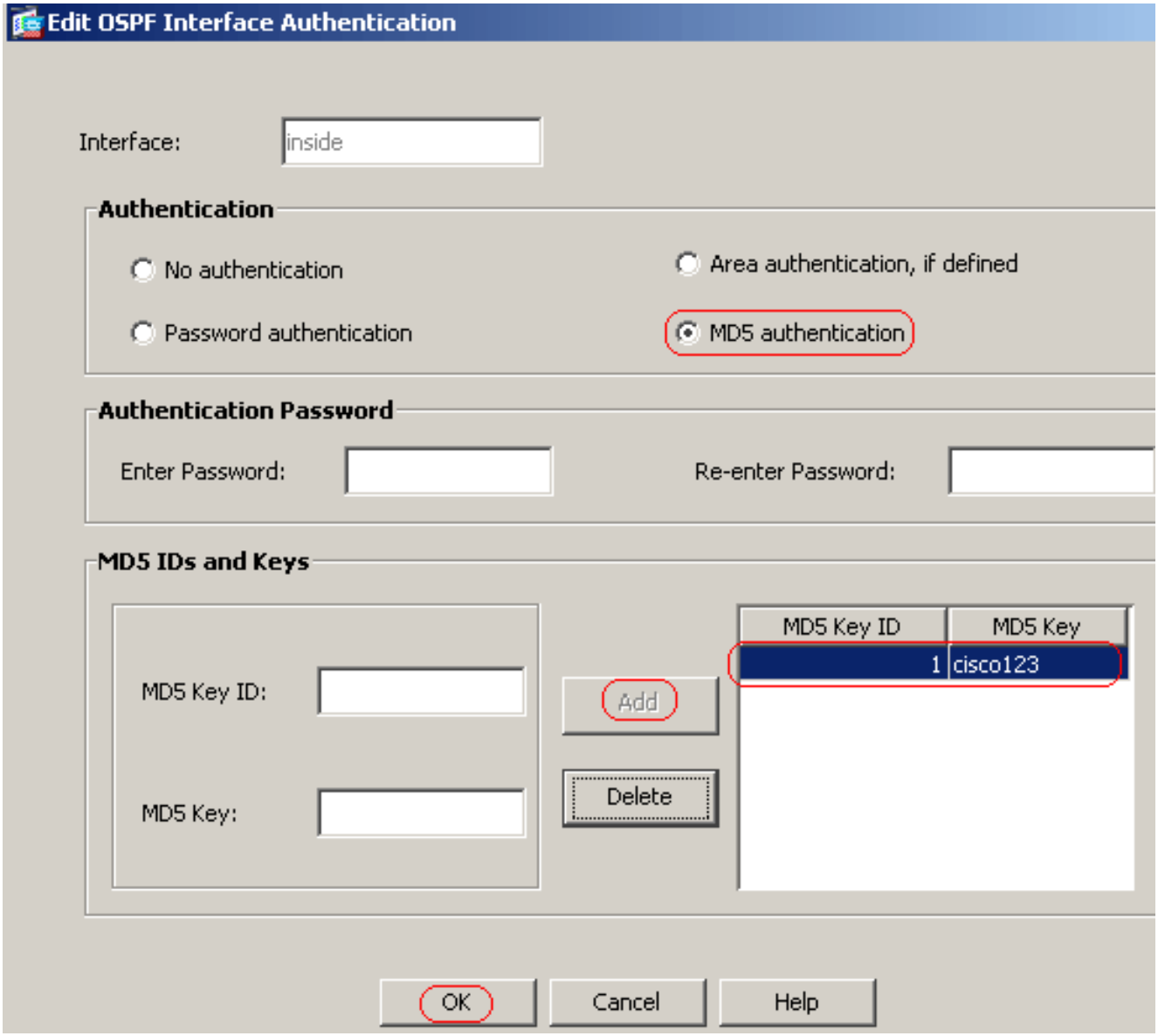
L'authentification de route OSPF est configurée par interface. Tous les voisins OSPF sur les interfaces configurées pour l'authentification des messages OSPF doivent être configurés avec le même mode et la même clé d'authentification pour les contiguïtés à établir.

Complétez ces étapes afin d'activer l'authentification MD5 OSPF sur Cisco ASA :

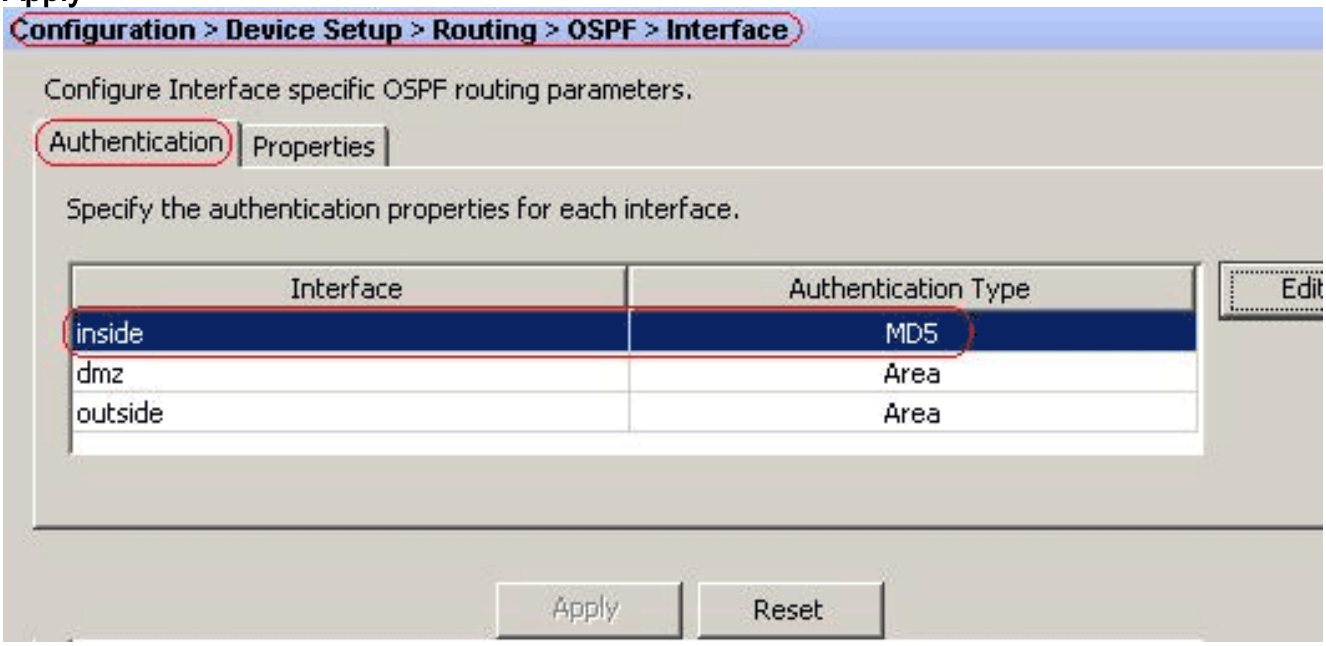
1. Sur ASDM, accédez à **Configuration > Device Setup > Routing > OSPF > Interface**, puis cliquez sur **Authentication** tab comme illustré dans cette image.



   Dans ce cas, OSPF est activé sur l'interface interne.
2. Choisissez l'interface **interne**, puis cliquez sur **Modifier**.
3. Sous Authentification, sélectionnez **Authentification MD5**, puis ajoutez ici plus d'informations sur les paramètres d'authentification.Dans ce cas, la clé prépartagée est **cisco123** et l'ID de clé est
   1.



4. Cliquez sur **OK**, puis sur **Apply**.



Configuration CLI de Cisco ASA

Cisco ASA

```
ciscoasa#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names

!--- Inside interface configuration interface
Ethernet0/1 nameif inside security-level 100 ip address
10.1.1.1 255.255.255.0 ospf cost 10 !--- OSPF
authentication is configured on the inside interface
ospf message-digest-key 1 md5 <removed> ospf
authentication message-digest ! !--- Outside interface
configuration interface Ethernet0/2 nameif outside
security-level 0 ip address 192.168.1.2 255.255.255.0
ospf cost 10 ! !--- Output Suppressed icmp unreachable
rate-limit 1 burst-size 1 asdm image disk0:/asdm-602.bin
no asdm history enable arp timeout 14400 ! !--- OSPF
Configuration router ospf 1
 network 10.1.1.0 255.255.255.0 area 0
 log-adj-changes
!

!--- This is the static default gateway configuration in
order to reach Internet route outside 0.0.0.0 0.0.0.0
192.168.1.1 1 ciscoasa#
```

Configuration CLI du routeur Cisco IOS (R2)

Routeur Cisco IOS (R2)

```
!--- Interface that connects to the Cisco ASA. !---
Notice the OSPF authentication parameters interface
Ethernet0
 ip address 10.1.1.2 255.255.255.0
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 cisco123

!--- Output Suppressed !--- OSPF Configuration router
ospf 1
 log-adjacency-changes
 network 10.1.1.0 0.0.0.255 area 0
 network 172.16.1.0 0.0.0.255 area 0
 network 172.16.2.0 0.0.0.255 area 0
```

Configuration CLI du routeur Cisco IOS (R1)

Routeur Cisco IOS (R1)

```
!--- Output Suppressed !--- OSPF Configuration router
ospf 1
 log-adjacency-changes
```

```
 network 172.16.5.0 0.0.0.255 area 0
 network 172.16.2.0 0.0.0.255 area 0
```

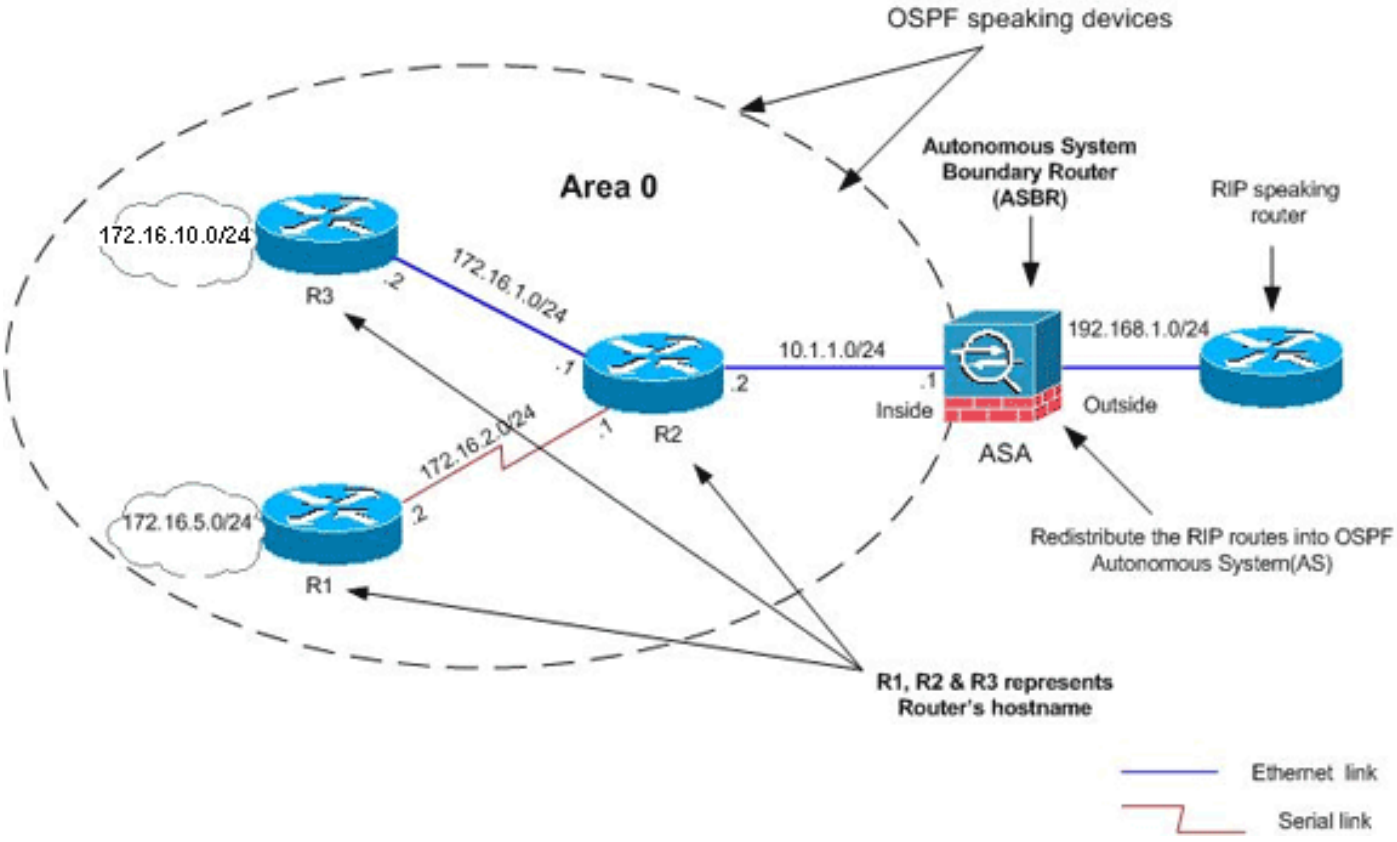
Configuration CLI du routeur Cisco IOS (R3)

Routeur Cisco IOS (R3)
`!--- Output Suppressed !--- OSPF Configuration` **router ospf 1** **log-adjacency-changes** **network 172.16.1.0 0.0.0.255 area 0** **network 172.16.10.0 0.0.0.255 area 0**

Redistribuer dans OSPF avec ASA

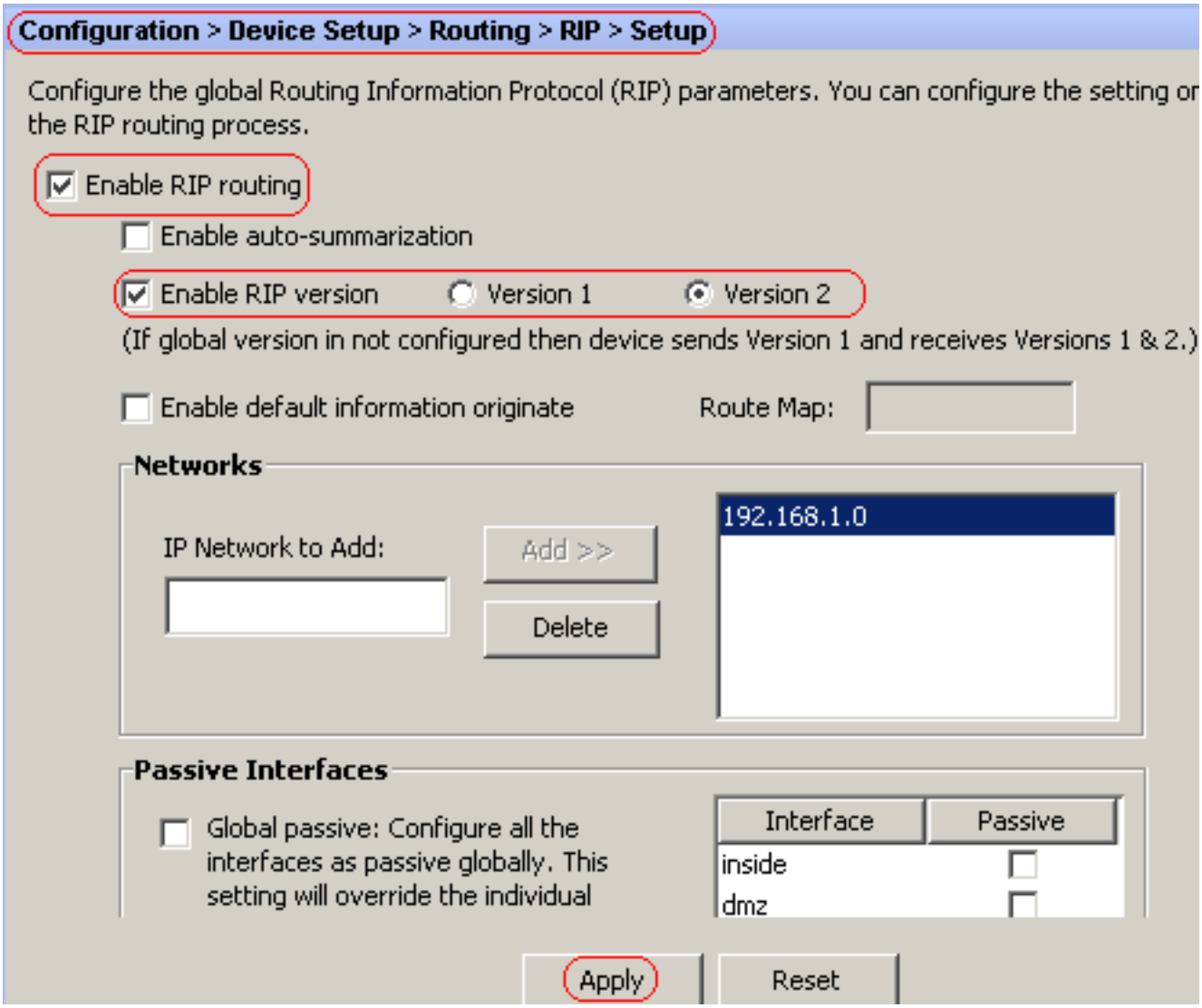
Comme mentionné précédemment, vous pouvez redistribuer des routes dans un processus de routage OSPF à partir d'un autre processus de routage OSPF, d'un processus de routage RIP ou à partir de routes statiques et connectées configurées sur des interfaces compatibles OSPF.

Dans cet exemple, redistribuez les routes RIP dans OSPF avec le schéma de réseau comme indiqué :

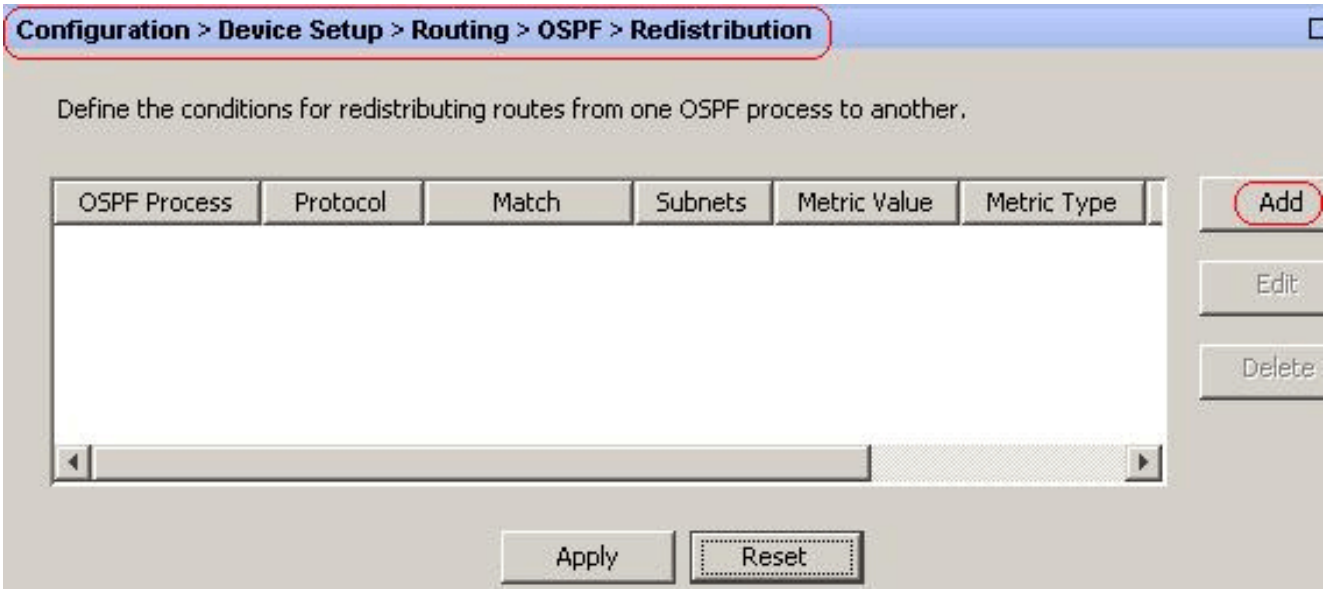


Configuration ASDM

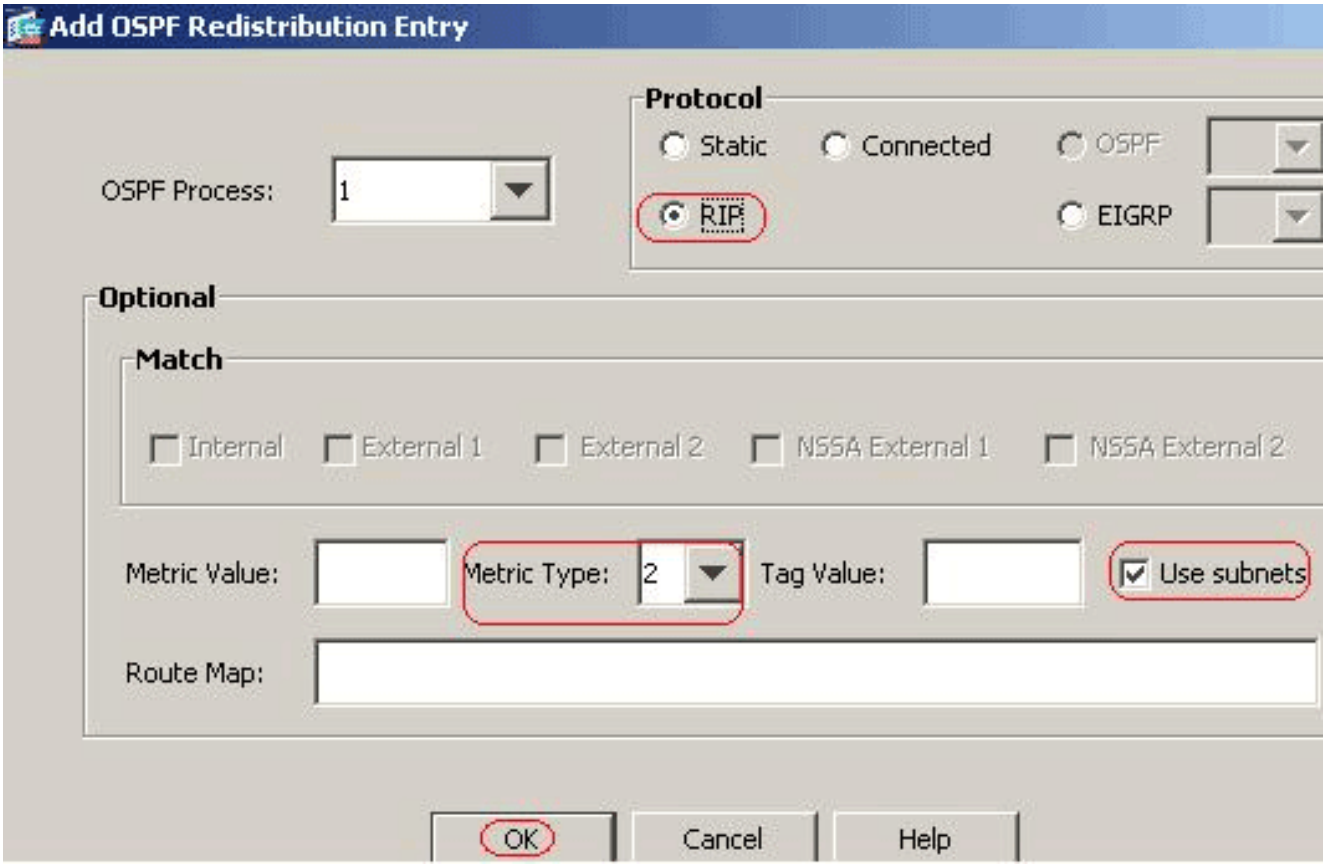
1. Choisissez **Configuration > Device Setup > Routing > RIP > Setup** afin d'activer RIP, et ajoutez le réseau 192.168.1.0 comme indiqué dans cette image.



2. Cliquez sur Apply.
3. Choisissez **Configuration > Device Setup > Routing > OSPF > Redistribution > Add** afin de redistribuer les routes RIP dans
OSPF.



4. Cliquez sur **OK**, puis sur
Apply.



Configuration CLI équivalente

Configuration CLI d'ASA pour la redistribution RIP dans OSPF AS
router ospf 1 network 10.1.1.0 255.255.255.0 area 0 log-adj-changes **redistribute rip subnets** router rip network 192.168.1.0

Vous pouvez voir la table de routage du routeur IOS voisin(R2) après avoir redistribué les routes RIP dans le système autonome OSPF.

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       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

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O       172.16.10.1/32 [110/11] via 172.16.1.2, 01:17:29, Ethernet1
O       172.16.5.1/32 [110/65] via 172.16.2.2, 01:17:29, Serial1
C       172.16.1.0/24 is directly connected, Ethernet1
C       172.16.2.0/24 is directly connected, Serial1
     10.0.0.0/24 is subnetted, 1 subnets
```

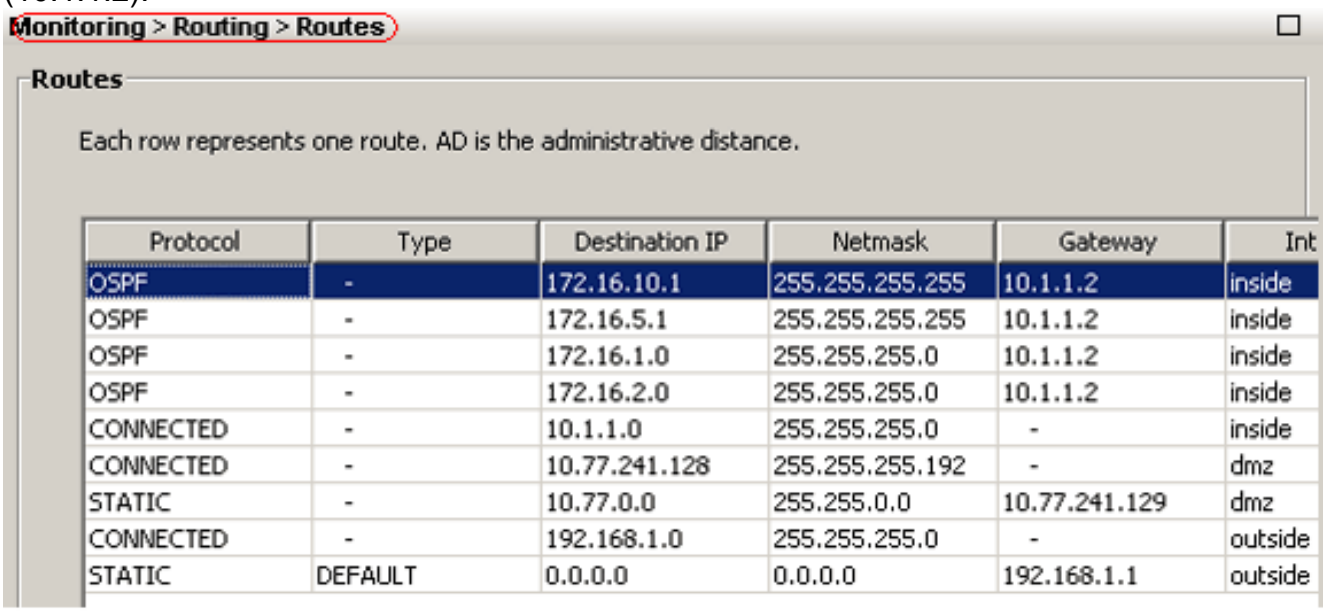
```
C       10.1.1.0 is directly connected, Ethernet0
O E2 192.168.1.0/24 [110/20] via 10.1.1.1, 01:17:29, Ethernet0
!--- Redistributed route adverstied by Cisco ASA
```

Vérification

Effectuez les étapes suivantes pour vérifier votre configuration :

1. Sur ASDM, vous pouvez accéder à **Monitoring > Routing > OSPF Neighbors** pour afficher chacun des voisins OSPF. Cette image montre le routeur interne (R2) en tant que voisin actif. Vous pouvez également voir l'interface où réside ce voisin, l'ID du routeur voisin, l'état et le temps
mort.

2. En outre, vous pouvez vérifier la table de routage si vous accédez à **Surveillance > Routage > Routes**. Dans cette image, les réseaux 172.16.1.0/24, 172.16.2.0/24, 172.16.5.0/24 et 172.16.10.0/24 sont appris via R2
(10.1.1.2).



Protocol	Type	Destination IP	Netmask	Gateway	Int
OSPF	-	172.16.10.1	255.255.255.255	10.1.1.2	inside
OSPF	-	172.16.5.1	255.255.255.255	10.1.1.2	inside
OSPF	-	172.16.1.0	255.255.255.0	10.1.1.2	inside
OSPF	-	172.16.2.0	255.255.255.0	10.1.1.2	inside
CONNECTED	-	10.1.1.0	255.255.255.0	-	inside
CONNECTED	-	10.77.241.128	255.255.255.192	-	dmz
STATIC	-	10.77.0.0	255.255.0.0	10.77.241.129	dmz
CONNECTED	-	192.168.1.0	255.255.255.0	-	outside
STATIC	DEFAULT	0.0.0.0	0.0.0.0	192.168.1.1	outside

3. Àpartir de l'interface de ligne de commande, vous pouvez utiliser la commande **show route** afin d'obtenir la même sortie.

```
ciscoasa#show route

Codes: C - connected, S - static, I - IGRP, 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, E - EGP
```

```
        i - IS-IS, 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

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

O    172.16.10.1 255.255.255.255 [110/21] via 10.1.1.2, 0:00:06, inside
O    172.16.5.1 255.255.255.255 [110/75] via 10.1.1.2, 0:00:06, inside
O    172.16.1.0 255.255.255.0 [110/20] via 10.1.1.2, 0:00:06, inside
O    172.16.2.0 255.255.255.0 [110/74] via 10.1.1.2, 0:00:06, inside
C    10.1.1.0 255.255.255.0 is directly connected, inside
C    10.77.241.128 255.255.255.192 is directly connected, dmz
S    10.77.0.0 255.255.0.0 [1/0] via 10.77.241.129, dmz
C    192.168.1.0 255.255.255.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 192.168.1.1, outside
```

4. Vous pouvez également utiliser la commande **show ospf database** afin d'obtenir des informations sur les réseaux appris et la topologie ospf.

```
ciscoasa#show ospf database


       OSPF Router with ID (192.168.1.2) (Process ID 1)


                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
172.16.1.2      172.16.1.2      123         0x80000039 0xfd1d 2
172.16.2.1      172.16.2.1      775         0x8000003c 0x9b42 4
172.16.5.1      172.16.5.1      308         0x80000038 0xb91b 3
192.168.1.2     192.168.1.2     1038        0x80000037 0x29d7 1

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.1.1        192.168.1.2     1038        0x80000034 0x72ee
172.16.1.1      172.16.2.1      282         0x80000036 0x9e68
```

5. La commande **show ospf neighbors** est également utile afin de vérifier les voisins actifs et les informations correspondantes. Cet exemple montre les mêmes informations que celles que vous avez obtenues d'ASDM à l'étape 1.

```
ciscoasa#show ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.2.1        1   FULL/BDR        0:00:36     10.1.1.2        inside
```

Dépannage

Cette section fournit des informations qui peuvent faciliter le dépannage des problèmes OSPF.

Configuration de voisinage statique pour un réseau point à point

Si vous avez configuré *le réseau OSPF point à point sans diffusion* sur l'ASA, vous devez définir des voisins OSPF statiques pour annoncer les routes OSPF sur un réseau point à point sans diffusion. Référez-vous à Définition de voisins OSPF statiques pour plus d'informations.

Dépannage des commandes

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug ospf events** - Active le débogage des événements OSPF.

```
ciscoasa(config)#debug ospf events
OSPF events debugging is on
ciscoasa(config)# int e0/1
ciscoasa(config-if)# no shu
ciscoasa(config-if)#
OSPF: Interface inside going Up
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: 2 Way Communication to 172.16.2.1 on inside, state 2WAY
OSPF: Backup seen Event before WAIT timer on inside
OSPF: DR/BDR election on inside
OSPF: Elect BDR 172.16.2.1
OSPF: Elect DR 172.16.2.1
       DR: 172.16.2.1 (Id)   BDR: 172.16.2.1 (Id)
OSPF: Send DBD to 172.16.2.1 on inside seq 0x1abd opt 0x2 flag 0x7 len 32
OSPF: Send with youngest Key 1
OSPF: End of hello processing
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x12f3 opt 0x42 flag 0x7 len 32  mtu
 1500 state EXSTART
OSPF: First DBD and we are not SLAVE
OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x1abd opt 0x42 flag 0x2 len 152  mt
u 1500 state EXSTART
OSPF: NBR Negotiation Done. We are the MASTER
OSPF: Send DBD to 172.16.2.1 on inside seq 0x1abe opt 0x2 flag 0x3 len 132
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Database request to 172.16.2.1
OSPF: sent LS REQ packet to 10.1.1.2, length 12
OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x1abe opt 0x42 flag 0x0 len 32  mtu
 1500 state EXCHANGE
OSPF: Send DBD to 172.16.2.1 on inside seq 0x1abf opt 0x2 flag 0x1 len 32
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x1abf opt 0x42 flag 0x0 len 32  mtu
 1500 state EXCHANGE
OSPF: Exchange Done with 172.16.2.1 on inside
OSPF: Synchronized with 172.16.2.1 on inside, state FULL
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: Neighbor change Event on interface inside
OSPF: DR/BDR election on inside
OSPF: Elect BDR 192.168.1.2
OSPF: Elect DR 172.16.2.1
OSPF: Elect BDR 192.168.1.2
OSPF: Elect DR 172.16.2.1
       DR: 172.16.2.1 (Id)   BDR: 192.168.1.2 (Id)
OSPF: End of hello processing
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
```

```
OSPF: End of hello processing
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
```

Remarque : Reportez-vous à la section debug ospf de la version 8.0 du Guide de référence des commandes de l'appliance de sécurité Cisco pour plus d'informations sur les différentes commandes utiles pour résoudre le problème.

Informations connexes

- Page de support pour appliances de sécurité adaptables de la gamme Cisco 5500
- Page de support Cisco 500 gamme PIX
- PIX/ASA 8.X : Configuration d'EIGRP sur le dispositif de sécurité adaptatif dédié (ASA) Cisco
- Support et documentation techniques - Cisco Systems