Exemple de configuration d'ASA/PIX avec RIP

Contenu

Introduction

Ce document explique comment configurer Cisco ASA afin d'apprendre les routes via le protocole RIP (Routing Information Protocol), 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 : Cette configuration de document est basée sur RIP version 2.

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.
- RIP 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 RIP est un protocole de routage à vecteur de distance qui utilise le nombre de sauts comme métrique de sélection de chemin. Lorsque le protocole RIP est activé sur une interface, l’interface échange des diffusions RIP avec les périphériques voisins afin d’apprendre dynamiquement des routes et de les annoncer.

Le dispositif de sécurité prend en charge les versions 1 et 2 du protocole RIP. RIP version 1 n’envoie pas le masque de sous-réseau avec la mise à jour de routage. RIP version 2 envoie le masque de sous-réseau avec la mise à jour de routage et prend en charge les masques de sous-réseau de longueur variable. En outre, RIP version 2 prend en charge l’authentification des voisins lors de l’échange de mises à jour de routage. Cette authentification garantit que l'appliance de sécurité reçoit des informations de routage fiables d'une source fiable.

Limites:

1. Le dispositif de sécurité ne peut pas transmettre les mises à jour RIP entre les interfaces.
2. RIP Version 1 ne prend pas en charge les masques de sous-réseau de longueur variable (VLSM).
3. Le nombre maximal de sauts du protocole RIP est de 15. Une route dont le nombre de sauts est supérieur à 15 est considérée comme inaccessible.

4. La convergence RIP est relativement lente par rapport aux autres protocoles de routage.
5. Vous ne pouvez activer qu'un seul processus RIP sur l'appliance de sécurité.

Remarque : ces informations s'appliquent uniquement au protocole RIP version 2 :

1. Si vous utilisez l'authentification de voisin, la clé d'authentification et l'ID de clé doivent être identiques sur tous les périphériques voisins qui fournissent des mises à jour RIP version 2 à l'interface.
2. Avec RIP version 2, le dispositif de sécurité transmet et reçoit les mises à jour de route par défaut avec l'utilisation de l'adresse de multidiffusion 224.0.0.9. En mode passif, il reçoit les mises à jour de route à cette adresse.
3. Lorsque le protocole RIP version 2 est configuré sur une interface, l'adresse de multidiffusion 224.0.0.9 est enregistrée sur cette interface. Lorsqu'une configuration RIP version 2 est supprimée d'une interface, cette adresse de multidiffusion n'est pas enregistrée.

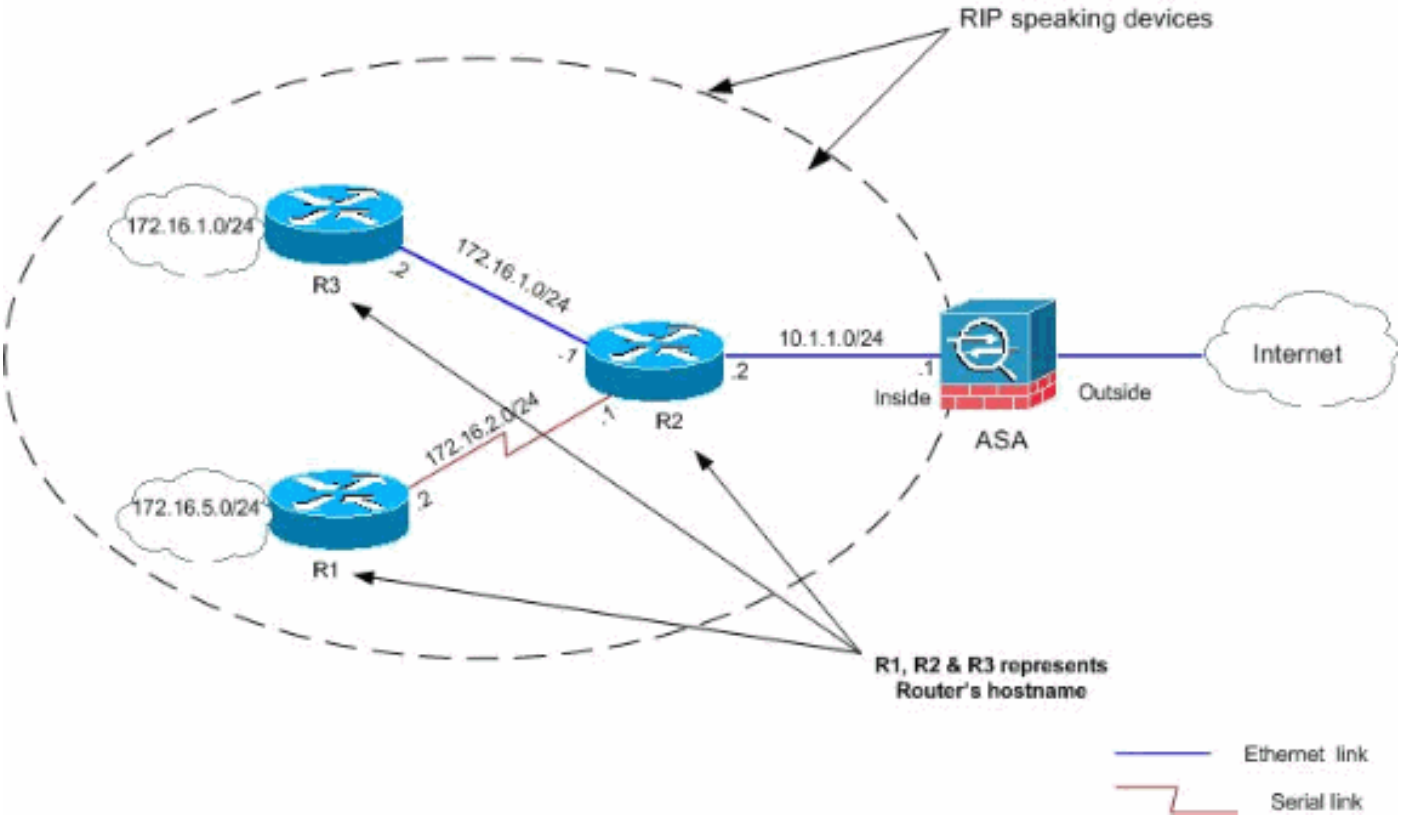
Configuration

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 :



Configurations

Ce document utilise les configurations suivantes :

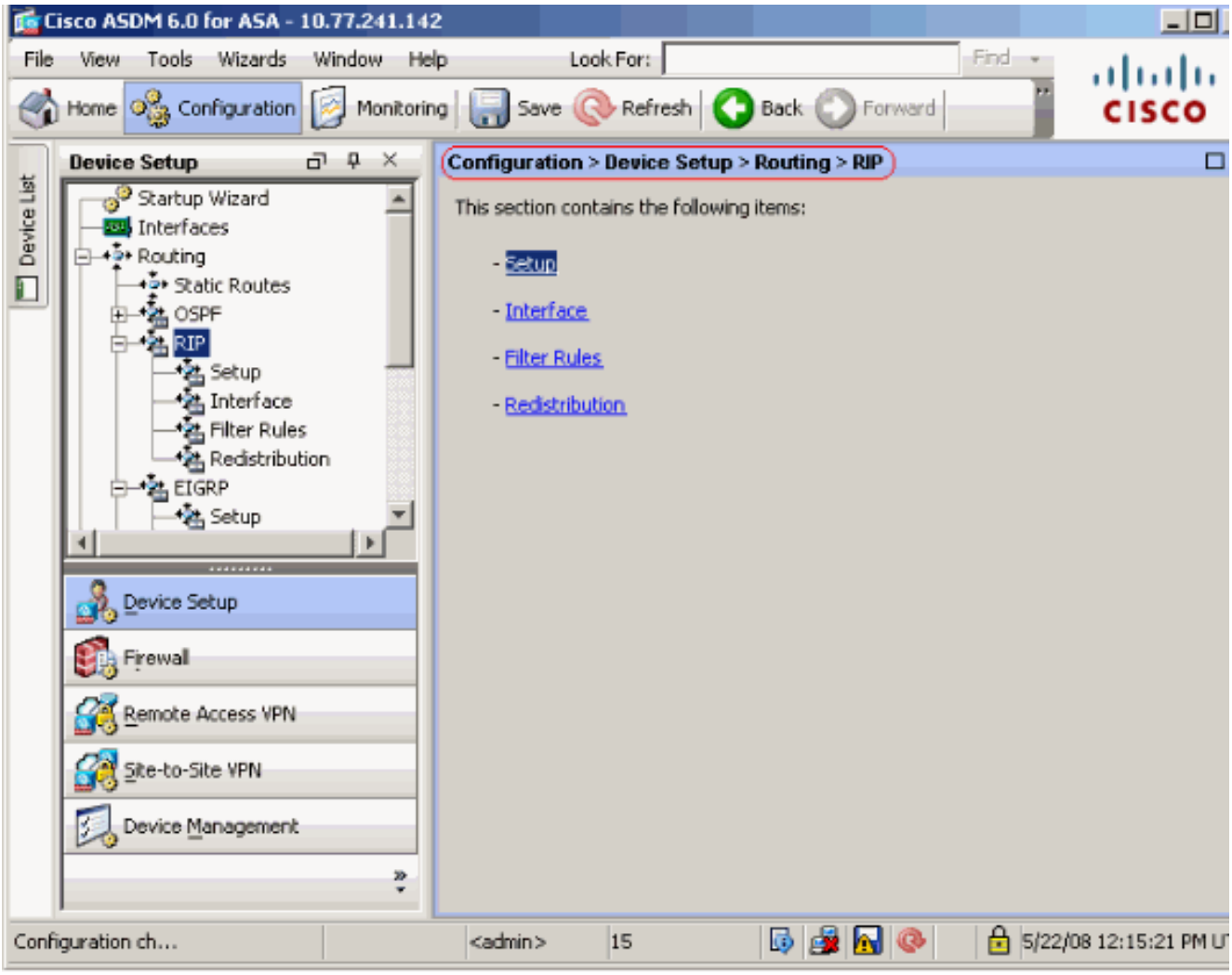
- Configuration ASDM
- Configuration de l'authentification RIP
- Configuration CLI de Cisco ASA
- Configuration CLI du routeur Cisco IOS (R2)
- Configuration CLI du routeur Cisco IOS (R1)
- Configuration CLI du routeur Cisco IOS (R3)

Configuration ASDM

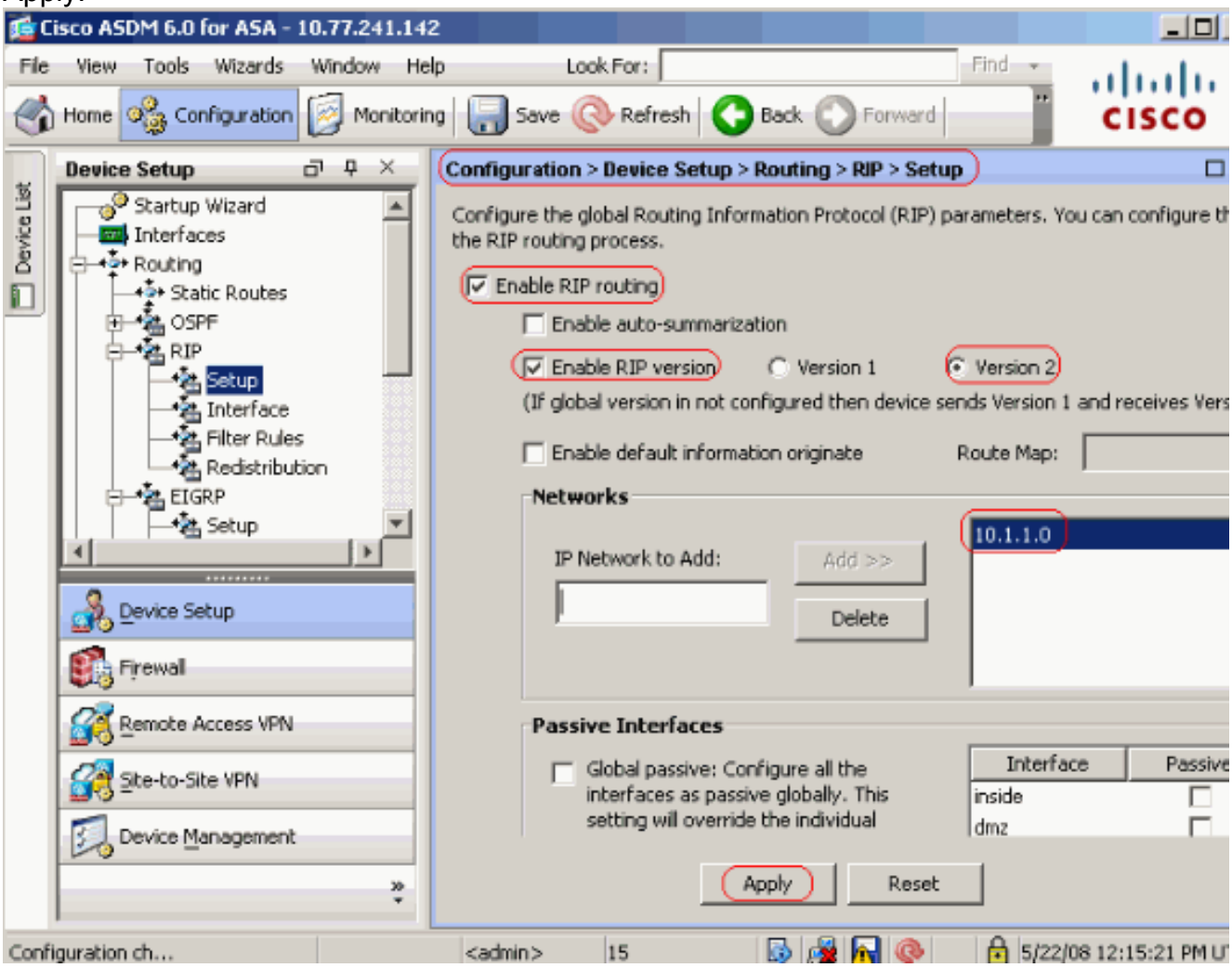
Adaptive Security Device Manager (ASDM) est une application basée sur navigateur utilisée pour configurer et surveiller le logiciel sur les appliances de sécurité. L'ASDM est chargé à partir de l'appliance de sécurité, puis utilisé pour configurer, surveiller et gérer le périphérique. Vous pouvez également 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 RIP dans Cisco ASA :

1. Connectez-vous à Cisco ASA avec ASDM.
2. Choisissez **Configuration > Device Setup > Routing > RIP** dans l'interface ASDM, comme indiqué dans la capture d'écran.



3. Choisissez **Configuration > Device Setup > Routing > RIP > Setup** afin d'activer le routage RIP comme indiqué.Activez la case à cocher **Activer le routage RIP**.Activez la case à cocher **Activer la version RIP** avec le bouton radio **Version 2**.Sous l'onglet **Réseaux**, ajoutez le réseau **10.1.1.0**.Cliquez sur
Apply.



ChampsEnable RIP Routing : cochez cette case afin d'activer le routage RIP sur l'appliance de sécurité. Lorsque vous activez le protocole RIP, il est activé sur toutes les interfaces. Si vous cochez cette case, les autres champs de ce volet sont également activés. Désactivez cette case à cocher afin de désactiver le routage RIP sur l'appliance de sécurité.Enable Auto-summary : désactivez cette case à cocher afin de désactiver la récapitulation de route automatique. Cochez cette case afin de réactiver la récapitulation automatique de route. RIP version 1 utilise toujours la récapitulation automatique. Vous ne pouvez pas désactiver la récapitulation automatique pour RIP Version 1. Si vous utilisez RIP Version 2, vous pouvez désactiver la récapitulation automatique si vous décochez cette case. Désactivez la récapitulation automatique si vous devez effectuer le routage entre les sous-réseaux déconnectés. Lorsque la récapitulation automatique est désactivée, les sous-réseaux sont annoncés.Enable RIP version : cochez cette case afin de spécifier la version du protocole RIP utilisée par l'appliance de sécurité. Si cette case est décochée, l'appliance de sécurité envoie les mises à jour RIP version 1 et accepte les mises à jour RIP version 1 et version 2. Ce paramètre peut être remplacé par interface dans le volet Interface.Version 1 : indique que l'appliance de sécurité envoie et reçoit uniquement les mises à jour RIP Version 1. Toutes les mises à jour de la version 2 reçues sont supprimées.Version 2 : indique que l'appliance de sécurité envoie et reçoit uniquement les mises à jour RIP Version 2. Toutes les mises à

jour de la version 1 reçues sont supprimées.Enable default information originate : cochez cette case afin de générer une route par défaut dans le processus de routage RIP. Vous pouvez configurer une carte de route qui doit être satisfaite avant que la route par défaut puisse être générée.Route-map : saisissez le nom de la route map afin de l'appliquer. Le processus de routage génère la route par défaut si le mappage de route est satisfait.IP Network to Add : définit un réseau pour le processus de routage RIP. Le numéro de réseau spécifié ne doit contenir aucune information de sous-réseau. Il n'y a aucune limite au nombre de réseaux que vous pouvez ajouter à la configuration de l'appliance de sécurité. Les mises à jour de routage RIP sont envoyées et reçues uniquement via des interfaces sur les réseaux spécifiés. En outre, si le réseau d'une interface n'est pas spécifié, l'interface n'est pas annoncée dans les mises à jour RIP.Add : cliquez sur ce bouton afin d'ajouter le réseau spécifié à la liste des réseaux.Supprimer : cliquez sur ce bouton afin de supprimer le réseau sélectionné de la liste des réseaux.Configurer globalement les interfaces comme passives : cochez cette case pour définir toutes les interfaces du dispositif de sécurité en mode RIP passif. Le dispositif de sécurité écoute les diffusions de routage RIP sur toutes les interfaces et utilise ces informations pour remplir les tables de routage mais ne diffuse pas les mises à jour de routage. Utilisez la table Passive Interfaces afin de définir des interfaces spécifiques sur RIP passif.Table Passive Interfaces : répertorie les interfaces configurées sur l'appliance de sécurité. Cochez la case de la colonne Passive pour les interfaces que vous souhaitez utiliser en mode passif. Les autres interfaces envoient et reçoivent toujours des diffusions RIP.

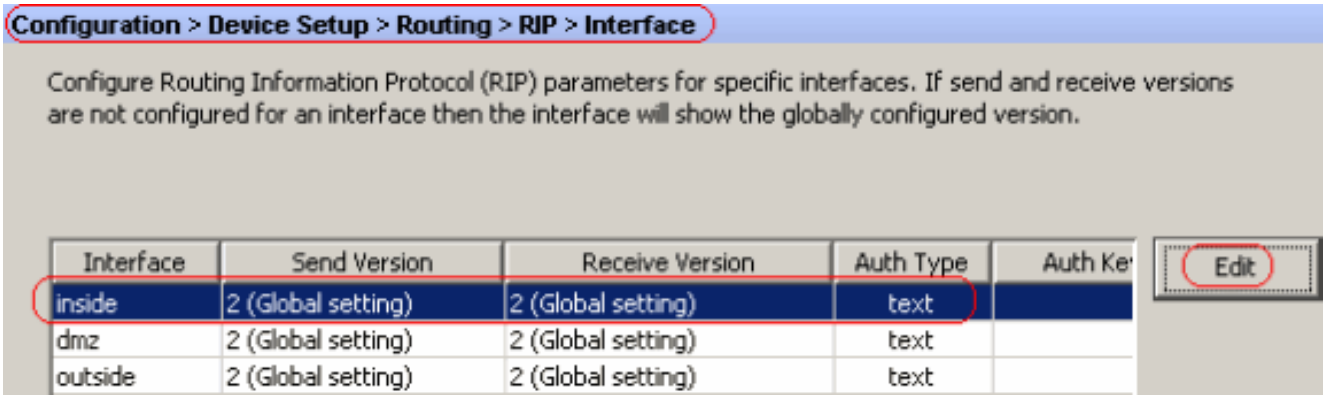
Configuration de l'authentification RIP

Cisco ASA prend en charge l'authentification MD5 des mises à jour de routage à partir du protocole de routage RIP v2. Le résumé à clé MD5 de chaque paquet RIP empêche l'introduction de messages de routage non autorisés ou faux provenant de sources non approuvées. L'ajout de l'authentification à vos messages RIP 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 vous introduisez 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 RIP 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.

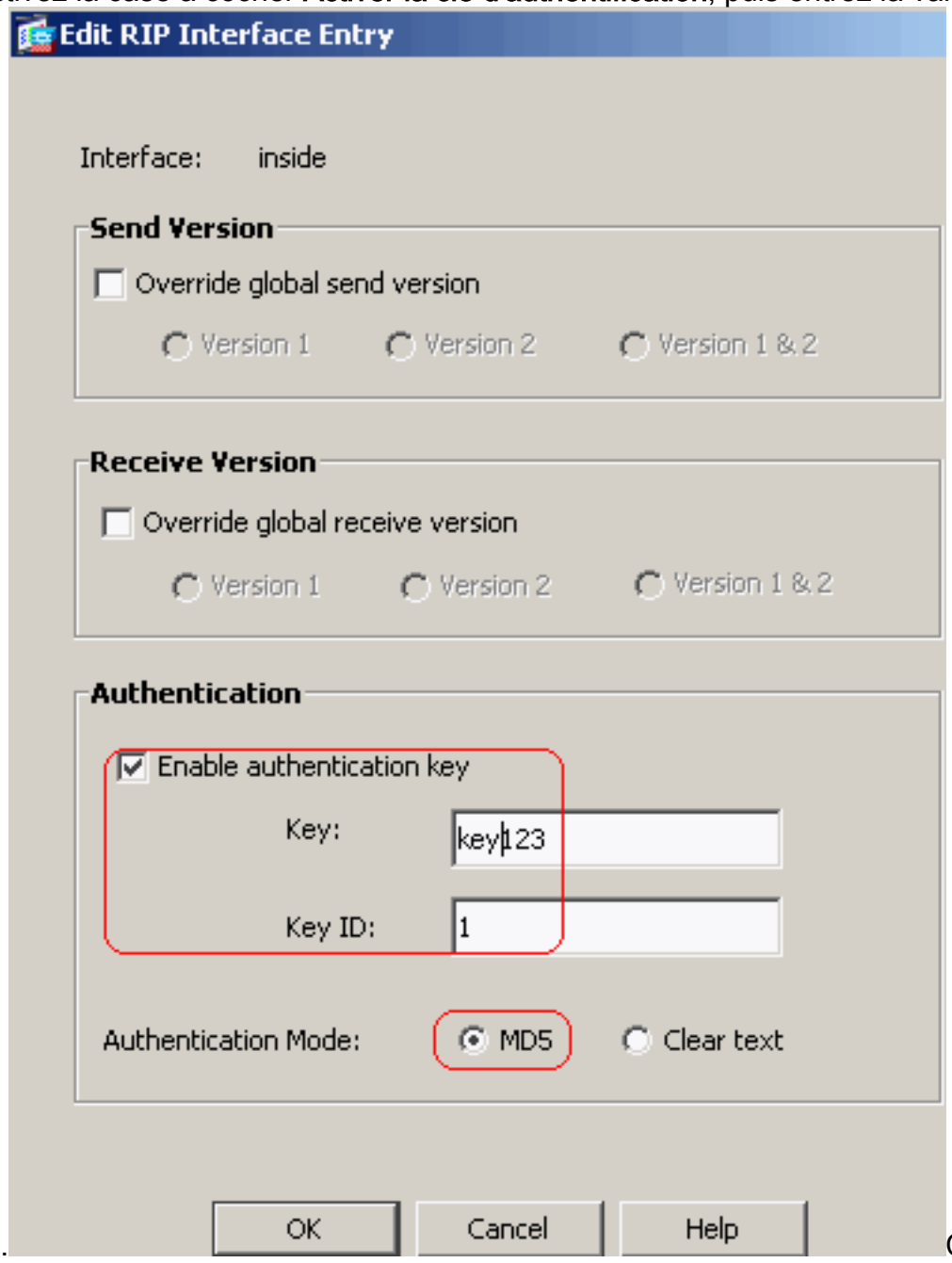
L'authentification de la route RIP est configurée par interface. Tous les voisins RIP sur les interfaces configurées pour l'authentification des messages RIP doivent être configurés avec le même mode et la même clé d'authentification.

Complétez ces étapes afin d'activer l'authentification RIP MD5 sur Cisco ASA.

1. Sur ASDM, choisissez **Configuration > Device Setup > Routing > RIP > Interface** et choisissez l'interface interne avec la souris. Cliquez sur **Edit**.



2. Activez la case à cocher **Activer la clé d'authentification**, puis entrez la valeur **Key** et **Key ID**. 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 !--- RIP authentication is
configured on the inside interface. rip authentication
mode md5
 rip authentication key




!

!--- Output Suppressed !--- Outside interface
configuration interface Ethernet0/2 nameif outside
security-level 0 ip address 192.168.1.2 255.255.255.0 !-
-- RIP Configuration router rip
 network 10.0.0.0
 version 2

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

Configuration CLI du routeur Cisco IOS (R2)

Routeur Cisco IOS (R2)

```
interface Ethernet0
 ip address 10.1.1.2 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain 1

!
router rip
 version 2
 network 10.0.0.0
 network 172.16.0.0
 no auto-summary
```

Configuration CLI du routeur Cisco IOS (R1)

Routeur Cisco IOS (R1)

```
router rip
 version 2
 network 172.16.0.0
 no auto-summary
```

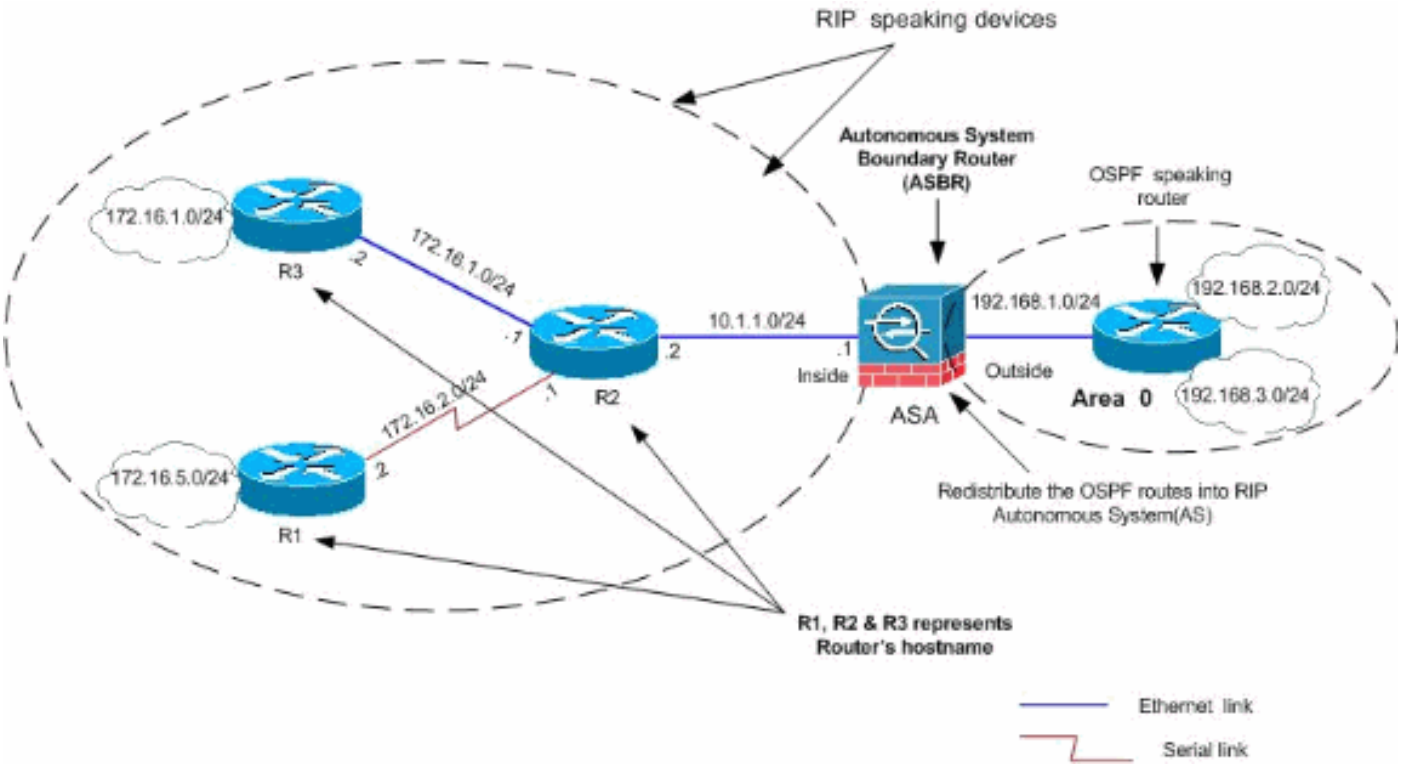
Configuration CLI du routeur Cisco IOS (R3)

Routeur Cisco IOS (R3)
router rip version 2 network 172.16.0.0 no auto-summary

Redistribuer dans RIP avec ASA

Vous pouvez redistribuer les routes des processus de routage OSPF, EIGRP, statique et connecté dans le processus de routage RIP.

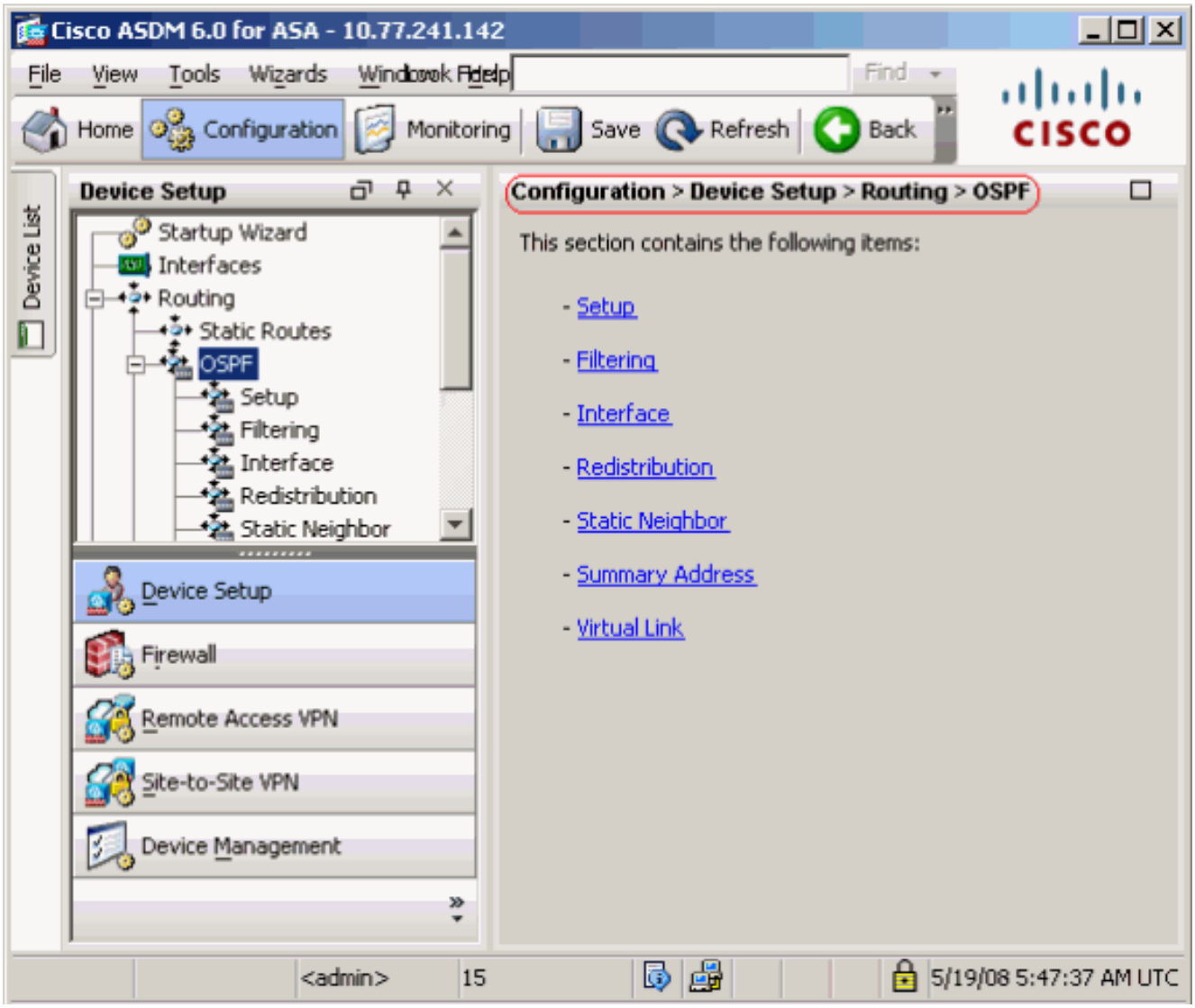
Dans cet exemple, la redistribution des routes OSPF dans RIP avec le schéma de réseau est présentée comme suit :



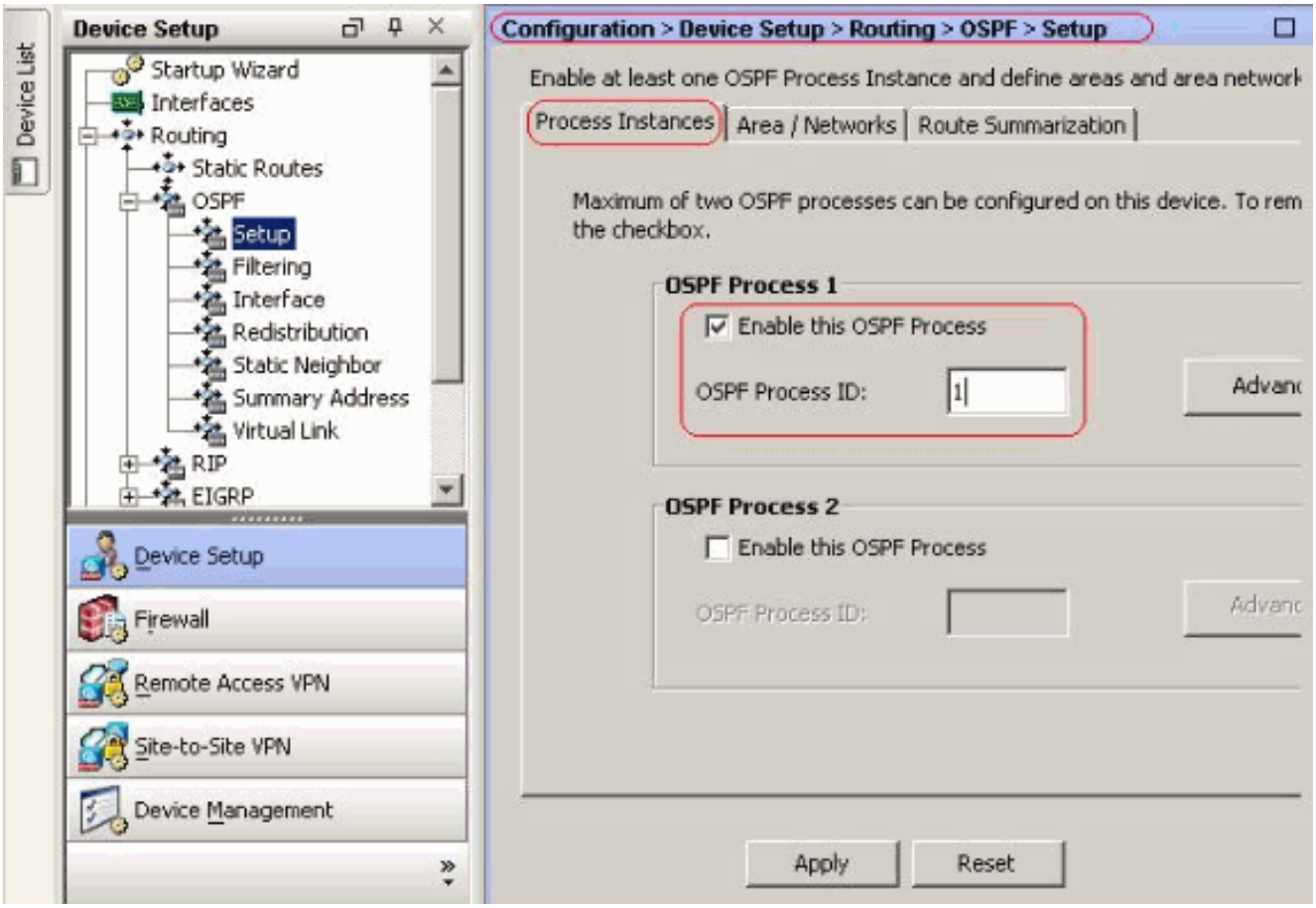
Configuration ASDM

Procédez comme suit :

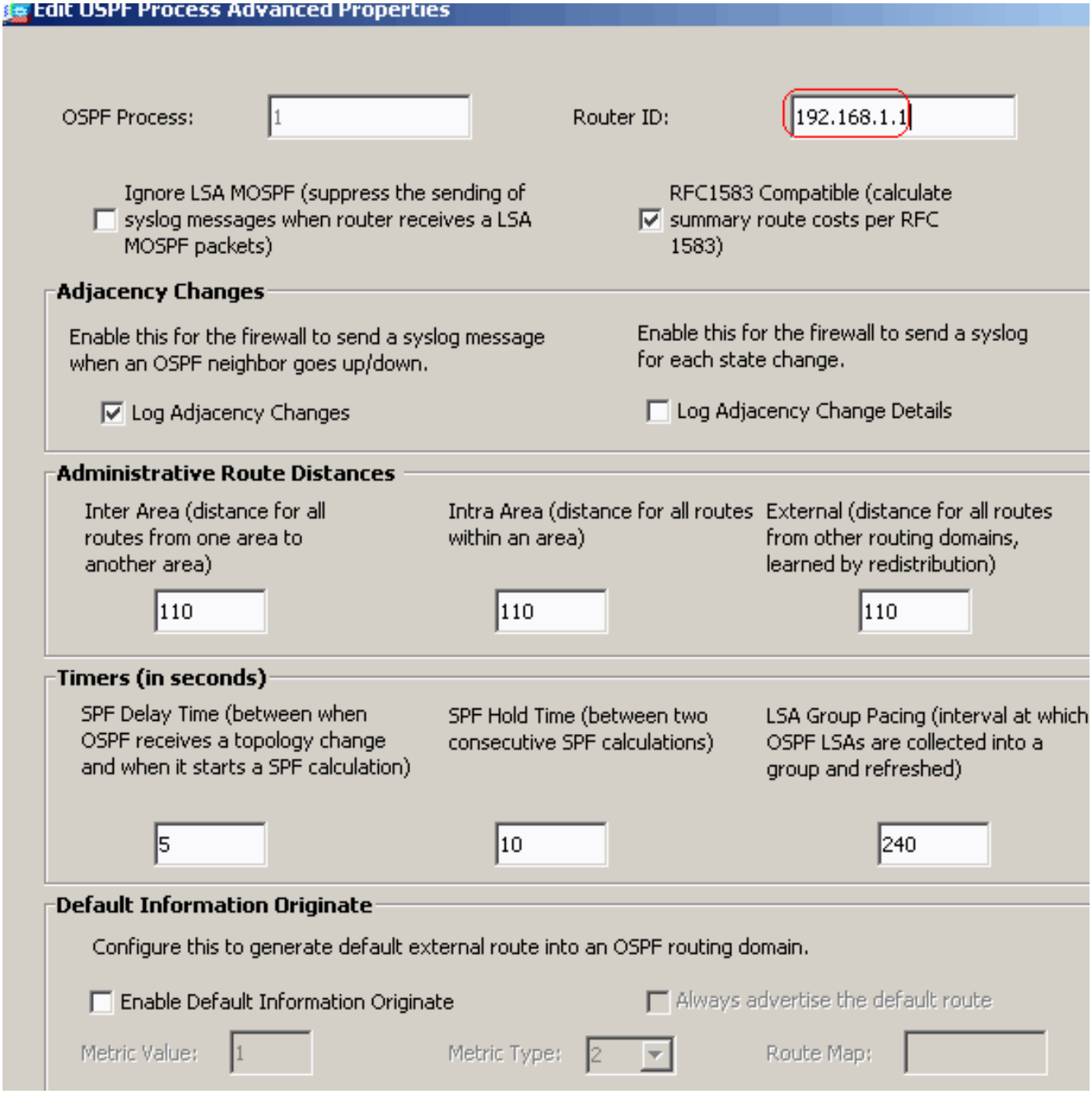
1. **Configuration OSPF**Choisissez **Configuration > Device Setup > Routing > OSPF** dans l'interface ASDM, comme indiqué dans la capture d'écran.



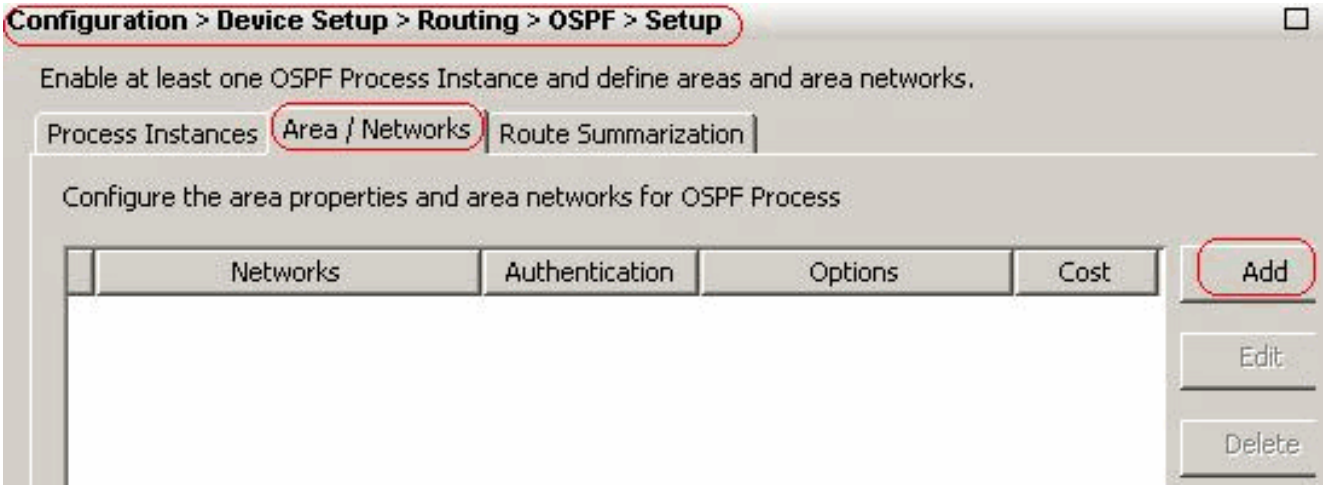
Activez le processus de routage OSPF dans l'onglet **Setup > Process Instances**, comme indiqué dans la capture d'écran. Dans cet exemple, le processus d'ID OSPF est **1**.



Cliquez sur **Advanced** dans l'onglet **Setup > Process Instances** afin de configurer les 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.

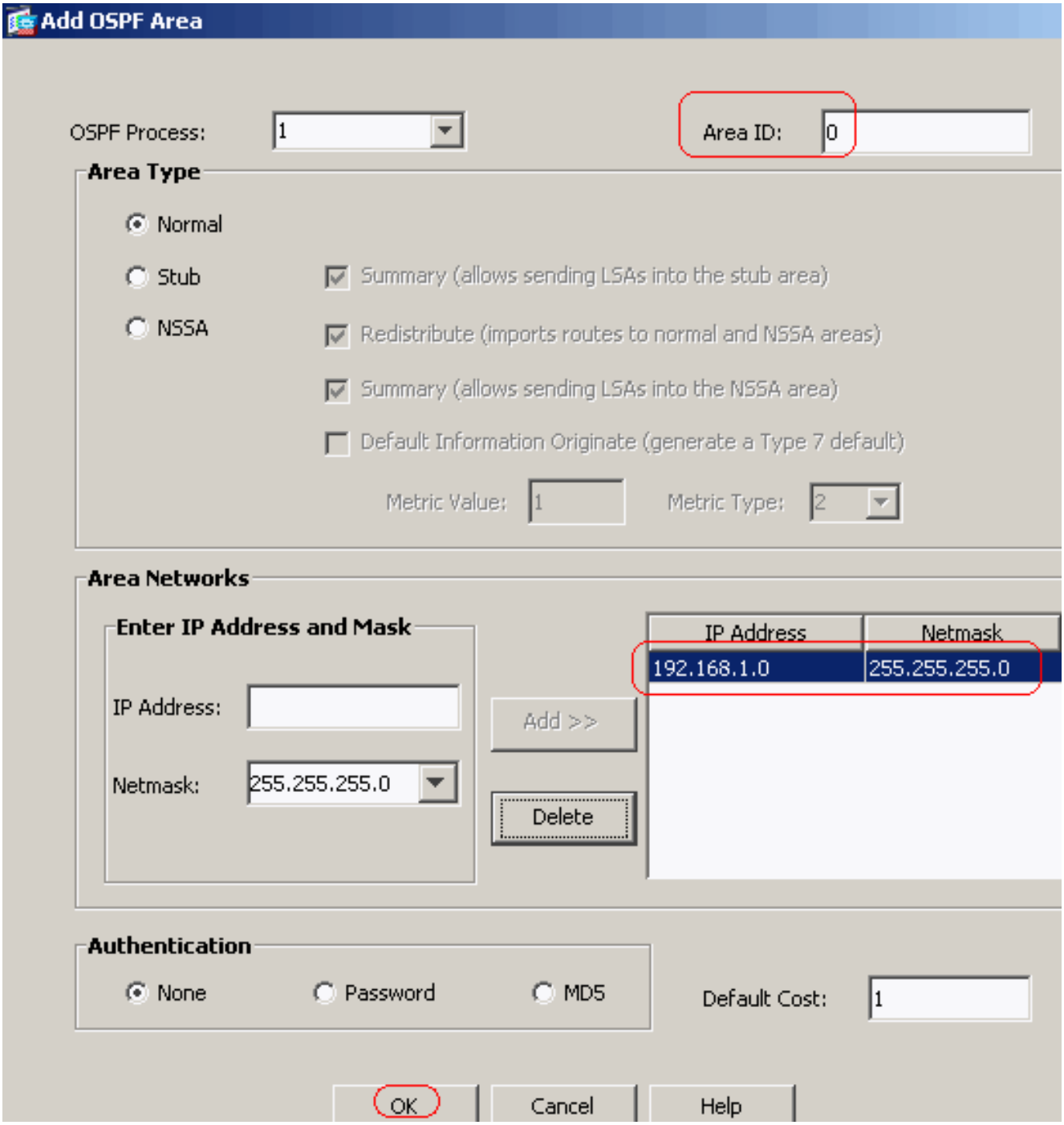


Click OK.Après avoir effectué les étapes précédentes, définissez les réseaux et les interfaces qui participent au routage OSPF dans l'onglet **Setup > Area/Networks**. Cliquez sur **Ajouter** comme indiqué dans cette capture d'écran.

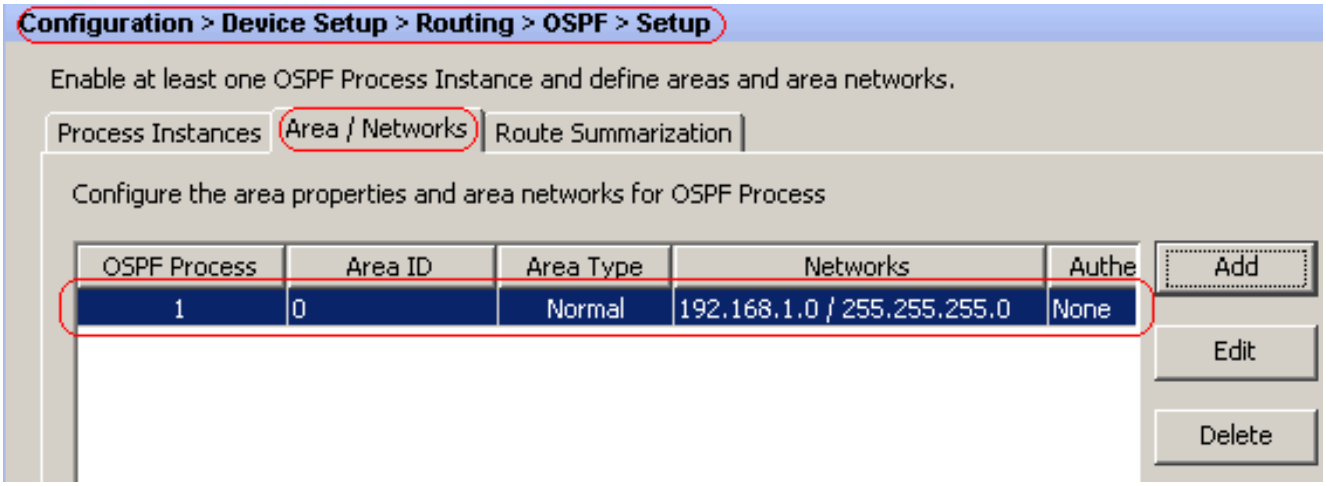


Cet écran apparaît. Dans cet exemple, le seul réseau que nous ajoutons est le réseau

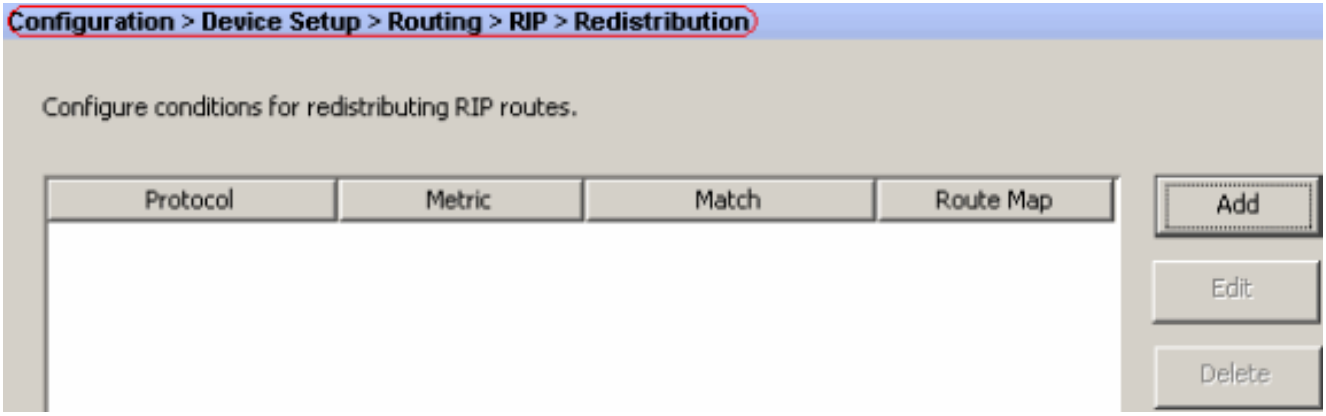
externe (192.168.1.0/24), car OSPF est activé uniquement sur l'interface externe.**Remarque :** Seules les interfaces avec une adresse IP qui font partie des réseaux définis participent au processus de routage
OSPF.



Click OK.Cliquez sur
Apply.

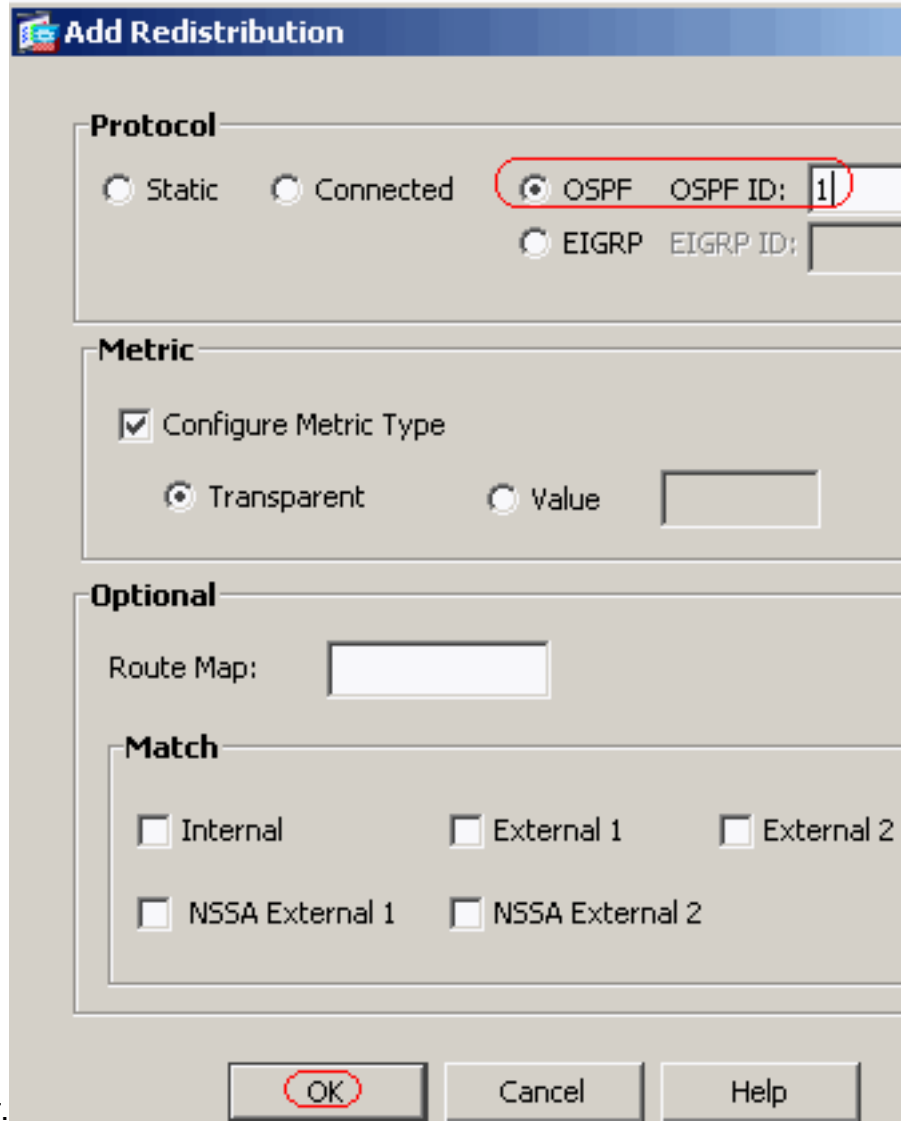


2. Choisissez **Configuration > Device Setup > Routing > RIP > Redistribution > Add** afin de redistribuer les routes OSPF dans
RIP.



3. Cliquez sur **OK, puis sur**

Apply.



Configuration CLI équivalente

Configuration CLI d'ASA pour la redistribution OSPF dans RIP AS
router rip network 10.0.0.0 **redistribute ospf 1 metric transparent** version 2 ! router ospf 1 router-id 192.168.1.1 network 192.168.1.0 255.255.255.0 area 0 area 0 log-adj-changes

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

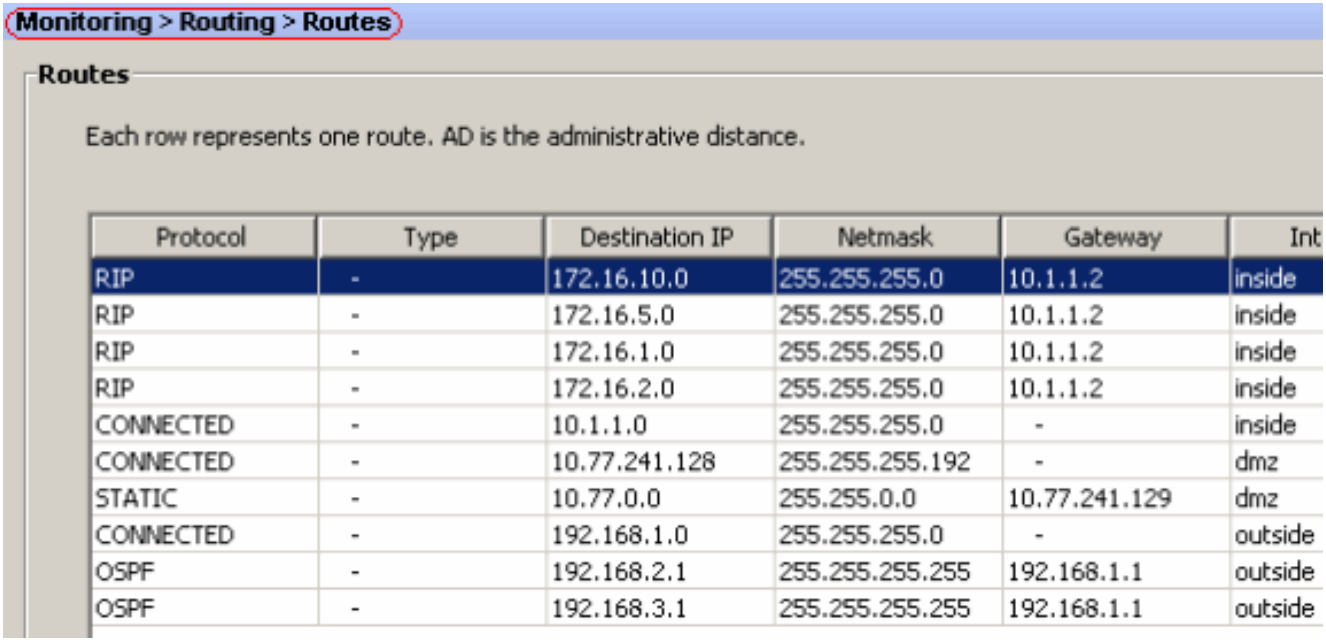
```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
        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

     172.16.0.0/24 is subnetted, 4 subnets
R       172.16.10.0 [120/1] via 172.16.1.2, 00:00:25, Ethernet1
R       172.16.5.0 [120/1] via 172.16.2.2, 00:00:20, Serial1
C       172.16.1.0 is directly connected, Ethernet1
C       172.16.2.0 is directly connected, Serial1
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Ethernet0
R       10.77.241.128/26 [120/1] via 10.1.1.1, 00:00:06, Ethernet0
R    192.168.1.0/24 [120/1] via 10.1.1.1, 00:00:05, Ethernet0
     192.168.2.0/32 is subnetted, 1 subnets
R       192.168.2.1 [120/12] via 10.1.1.1, 00:00:05, Ethernet0
     192.168.3.0/32 is subnetted, 1 subnets
R       192.168.3.1 [120/12] via 10.1.1.1, 00:00:05, Ethernet0
!--- Redistributed route advertised by Cisco ASA
```

Vérification

Complétez ces étapes afin de vérifier votre configuration :

1. Vous pouvez vérifier la table de routage si vous accédez à **Surveillance > Routage > Routes**. Dans cette capture d'écran, vous pouvez voir que 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) avec RIP.



Protocol	Type	Destination IP	Netmask	Gateway	Int
RIP	-	172.16.10.0	255.255.255.0	10.1.1.2	inside
RIP	-	172.16.5.0	255.255.255.0	10.1.1.2	inside
RIP	-	172.16.1.0	255.255.255.0	10.1.1.2	inside
RIP	-	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
OSPF	-	192.168.2.1	255.255.255.255	192.168.1.1	outside
OSPF	-	192.168.3.1	255.255.255.255	192.168.1.1	outside

2. 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 not set

R    172.16.10.0 255.255.255.0 [120/2] via 10.1.1.2, 0:00:10, inside
R    172.16.5.0 255.255.255.0 [120/2] via 10.1.1.2, 0:00:10, inside
R    172.16.1.0 255.255.255.0 [120/1] via 10.1.1.2, 0:00:10, inside
R    172.16.2.0 255.255.255.0 [120/1] via 10.1.1.2, 0:00:10, 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
O    192.168.2.1 255.255.255.255 [110/11] via 192.168.1.1, 0:34:46, outside
O    192.168.3.1 255.255.255.255 [110/11] via 192.168.1.1, 0:34:46, outside
ciscoasa#
```

Dépannage

Cette section contient des informations sur les commandes de débogage qui peuvent être utiles pour résoudre les problèmes OSPF.

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 rip events** : active le débogage des événements RIP

```
ciscoasa#debug rip events
rip_route_adjust for inside coming up
RIP: sending request on inside to 224.0.0.9
RIP: received v2 update from 10.1.1.2 on inside
     172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops
     172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops
RIP: Update contains 4 routes
RIP: received v2 update from 10.1.1.2 on inside
     172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops
     172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops
RIP: Update contains 4 routes
RIP: sending v2 flash update to 224.0.0.9 via dmz (10.77.241.142)
RIP: build flash update entries
        10.1.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
        172.16.1.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
        172.16.2.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
        172.16.5.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
        172.16.10.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
RIP: Update contains 5 routes
RIP: Update queued
RIP: sending v2 flash update to 224.0.0.9 via inside (10.1.1.1)
RIP: build flash update entries - suppressing null update
RIP: Update sent via dmz rip-len:112
RIP: sending v2 update to 224.0.0.9 via dmz (10.77.241.142)
RIP: build update entries
        10.1.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
```

```
        172.16.1.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
        172.16.2.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
        172.16.5.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
        172.16.10.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
        192.168.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
        192.168.2.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0
        192.168.3.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0
RIP: Update contains 8 routes
RIP: Update queued
RIP: sending v2 update to 224.0.0.9 via inside (10.1.1.1)
RIP: build update entries
        10.77.241.128 255.255.255.192 via 0.0.0.0, metric 1, tag 0
        192.168.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
        192.168.2.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0
        192.168.3.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0
RIP: Update contains 4 routes
RIP: Update queued
RIP: Update sent via dmz rip-len:172
RIP: Update sent via inside rip-len:92
RIP: received v2 update from 10.1.1.2 on inside
     172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops
     172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops
RIP: Update contains 4 routes
```

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