Exemple de configuration d'ASA/PIX avec RIP

Contenu

Introduction

Ce document explique comment configurer Cisco ASA afin d'apprendre des artères par le Protocole RIP (Routing Information Protocol), exécute l'authentification, et la redistribution.

Référez-vous à PIX/ASA 8.X : Configurer l'EIGRP sur l'appliance de sécurité adaptable Cisco (ASA) pour plus d'informations sur la configuration EIGRP.

Remarque: Cette configuration de document est basée sur le 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 ultérieures.
- Le RIP n'est pas pris en charge en mode de multi-contexte ; il est pris en charge seulement dans le mode unique.

Composants utilisés

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

- Sécurité adaptative Appliance(ASA) de gamme Cisco 5500 qui exécute la version de logiciel 8.0 et plus tard.
- Version de logiciel adaptative 6.0 de Manager(ASDM) de périphérique de sécurité de Cisco et plus tard.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

Les informations dans ce document s'appliquent également au Pare-feu de la gamme Cisco 500 PIX qui exécute la version de logiciel 8.0 et plus tard.

Conventions

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

Informations générales

Le RIP est un protocole de routage de vecteur de distance qui utilise le compte de saut comme mesure pour la sélection de chemin. Quand le RIP est activé sur une interface, le RIP d'échanges d'interface annonce avec des périphériques voisins afin d'apprendre dynamiquement environ et annoncer des artères.

La version RIP 1 de la version RIP 1 et de la version RIP 2. de support d'appareils de Sécurité n'envoie pas le subnet mask avec la mise à jour de routage. Le RIP version 2 envoie le subnet mask avec la mise à jour de routage et prend en charge les masques de longueur variable de sous-réseau. Supplémentaire, le RIP version 2 prend en charge l'authentification voisine en conduisant des mises à jour sont permutés. Cette authentification s'assure que les dispositifs de sécurité reçoivent les informations de routage fiables d'une source sûre.

Limites :

1. Les dispositifs de sécurité ne peuvent pas passer des mises à jour de RIP entre les interfaces.
2. Le RIP Version 1 ne prend en charge pas les masques de longueur variable de sous-réseau

(VLSM).
3. Le RIP a un nombre maximum de sauts de 15. Une artère avec un compte de saut plus grand que 15 est considérée inaccessible.
4. La convergence de RIP est relativement lente comparée à d'autres protocoles de routage.
5. Vous pouvez seulement activer un processus RIP simple sur les dispositifs de sécurité.

Remarque: Ces informations s'appliquent au RIP version 2 seulement :

1. Si vous utilisez l'authentification voisine, la clé et l'ID de clé d'authentification doivent être identique sur tous les périphériques voisins qui fournissent des mises à jour de RIP version 2 à l'interface.
2. Avec le RIP version 2, l'appliance de Sécurité transmet et reçoit des mises à jour de default route avec l'utilisation de l'adresse de multidiffusion 224.0.0.9. En mode passif, il reçoit des mises à jour de route à cette adresse.
3. Quand le RIP version 2 est configuré sur une interface, l'adresse de multidiffusion 224.0.0.9 est enregistrée sur cette interface. Quand une configuration de RIP version 2 est retirée d'une interface, cette adresse de multidiffusion est non inscrite.

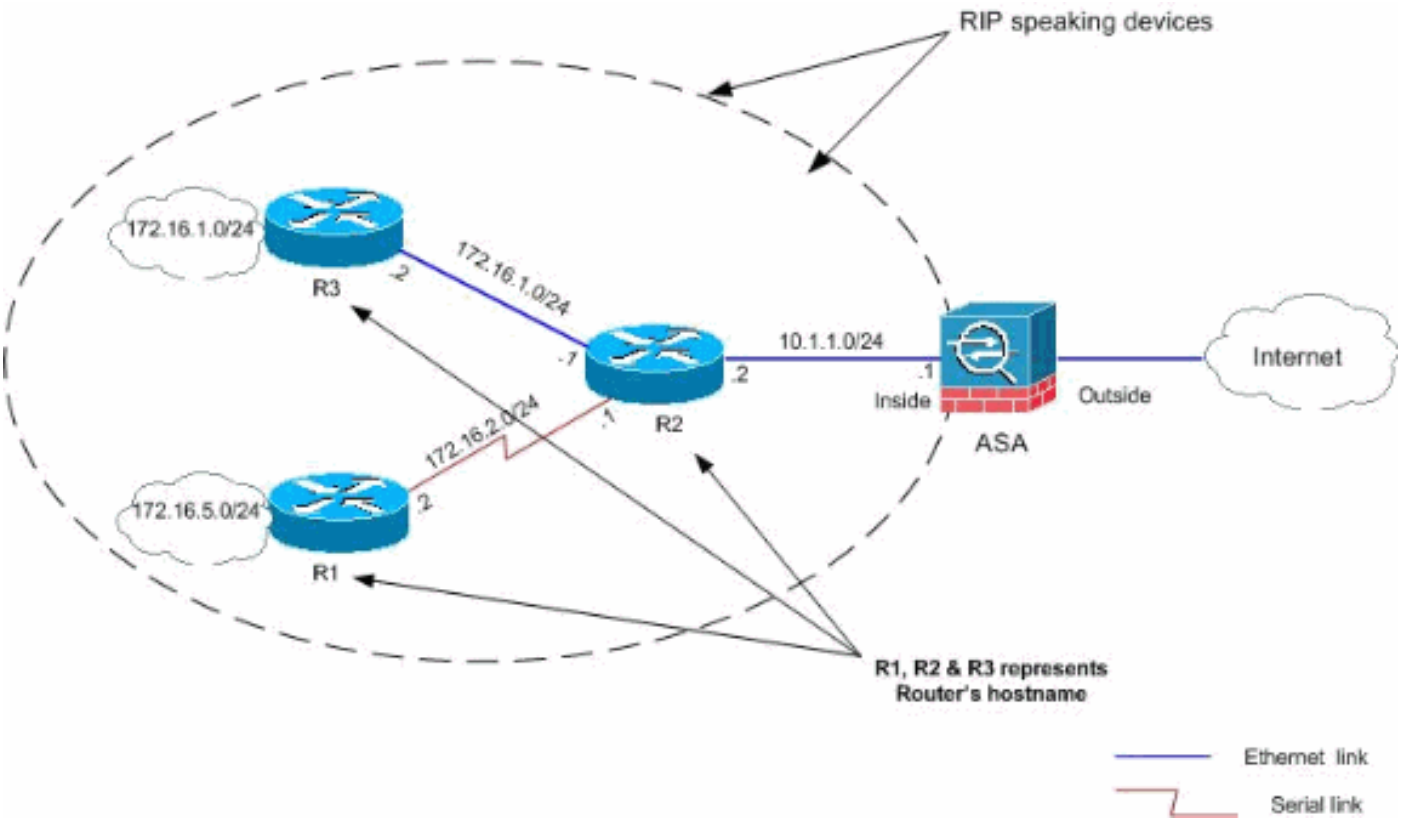
Configurez

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

Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour 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 :

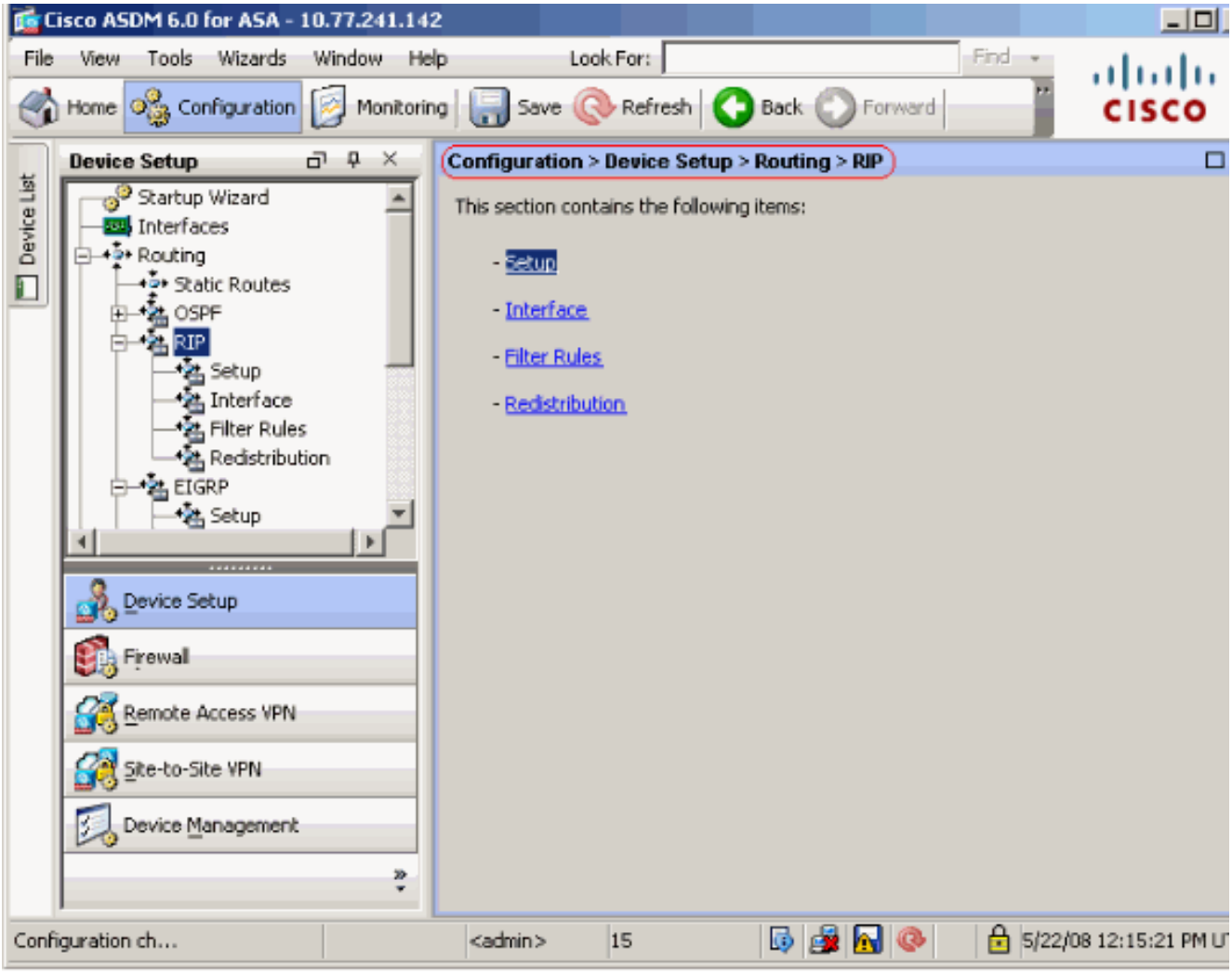
- Configuration ASDM
- Configurez l'authentification de RIP
- Configuration de Cisco ASA CLI
- Configuration CLI du routeur Cisco IOS (R2)
- Configuration CLI du routeur Cisco IOS (R1)
- Configuration CLI du routeur Cisco IOS (R3)

Configuration ASDM

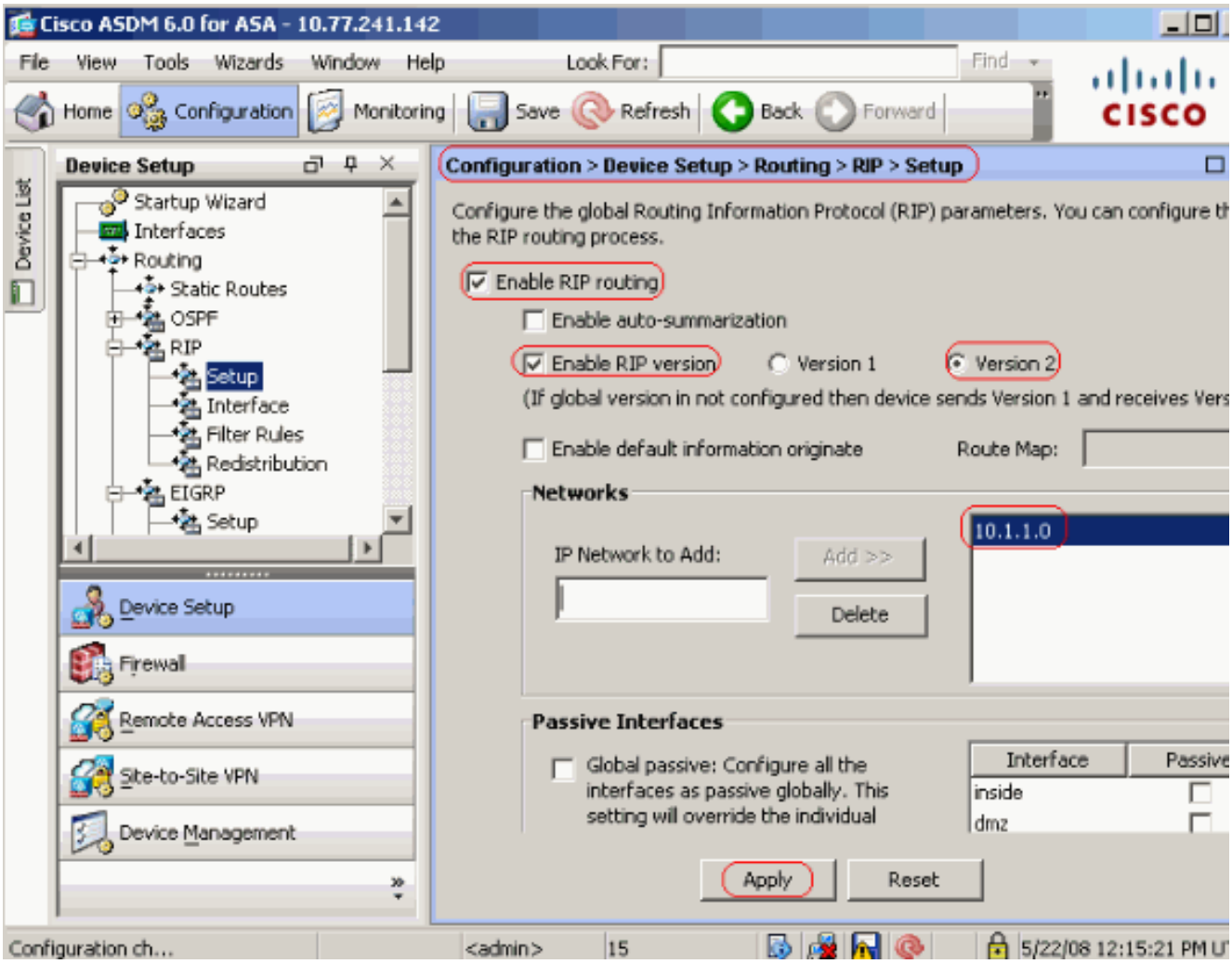
Adaptive Security Device Manager (ASDM) est une application navigateur utilisée afin de configurer et surveiller le logiciel sur des dispositifs de sécurité. L'ASDM est chargé des dispositifs de sécurité, et puis utilisé pour configurer, surveiller, et gérer le périphérique. Vous pouvez également utiliser le lanceur ASDM (Windows® seulement) afin de lancer l'application ASDM plus rapide que l'applet Java. Cette section décrit les informations que vous devez configurer les caractéristiques décrites dans ce document avec l'ASDM.

Terminez-vous ces étapes afin de configurer le RIP à Cisco ASA :

1. Procédure de connexion à Cisco ASA avec l'ASDM.
2. Choisissez la **configuration > l'installation de périphérique > le routage > le RIP** dans l'interface ASDM, suivant les indications du tir d'écran.



3. Choisissez la **configuration > l'installation de périphérique > le routage > le RIP > installé** afin d'activer le routage de RIP comme affiché.Choisissez le **routage de RIP d'enable de** case.Choisissez la **version RIP d'enable de** case avec la **version 2 de** case d'option.Sous des **réseaux** tabulez, ajoutez le réseau **10.1.1.0**.Cliquez sur **Apply**.



ChampsRoutage de RIP d'enable — Cochez cette commande d'inb de case pour activer le routage de RIP sur les dispositifs de sécurité. Quand vous activez le RIP, il est activé sur toutes les interfaces. Si vous cochez cette case, ceci active également les autres champs sur ce volet. Décochez cette case afin de désactiver le routage de RIP sur les dispositifs de sécurité.Récapitulation automatique d'enable — Effacez cette case afin de désactiver le résumé du routage automatique. Cochez cette case afin de réactiver le résumé du routage automatique. Le RIP Version 1 utilise toujours la récapitulation automatique. Vous ne pouvez pas désactiver la récapitulation automatique pour le RIP Version 1. Si vous utilisez le RIP version 2, vous pouvez arrêter la récapitulation automatique si vous décochez cette case. Désactivez la récapitulation automatique si vous devez exécuter le routage entre les sous-réseaux déconnectés. Quand la récapitulation automatique est désactivée, des sous-réseaux sont annoncés.Version RIP d'enable — Cochez cette case afin de spécifier la version du RIP utilisée par les dispositifs de sécurité. Si cette case est effacée, alors l'appliance de Sécurité envoie des mises à jour de RIP Version 1 et reçoit des mises à jour de RIP Version 1 et de version 2. Cette configuration peut être par interface ignoré dans le volet d'interface.Version 1 — Spécifie que l'appliance de Sécurité seulement envoie et reçoit des mises à jour de RIP Version 1. Toutes les mises à jour de version 2 reçues sont abandonnées.Version 2 — Spécifie que l'appliance de Sécurité seulement envoie et reçoit des mises à jour de RIP version 2. Toutes les mises à jour de version 1 reçues sont abandonnées.Les informations par défaut d'enable commencent — Cochez cette case afin de générer un default route dans le processus de routage de RIP. Vous pouvez configurer un mappage de route qui doit être satisfait avant que le default route puisse être généré.Route-map — Écrivez le nom du mappage de route afin de s'appliquer. Le processus de routage génère le default route si le mappage de route est satisfait.Réseau IP à ajouter — Définit un

réseau pour le processus de routage de RIP. Le network number spécifié ne doit contenir aucune information de sous-réseau. Il n'y a aucune limite au nombre de réseau que vous pouvez ajouter à la configuration de dispositifs de sécurité. Des mises à jour de routage de RIP est envoyées et reçues seulement par des interfaces sur les réseaux spécifiés. En outre, si le réseau d'une interface n'est pas spécifié, l'interface n'est annoncée dans aucune mise à jour de RIP.Ajoutez — Cliquez sur ce bouton afin d'ajouter le réseau spécifié à la liste de réseaux.Effacement — Cliquez sur ce bouton afin de retirer le réseau sélectionné de la liste de réseauxConfigurez les interfaces en tant que passif globalement — Cochez cette case pour placer toutes les interfaces sur les dispositifs de sécurité au mode passif de RIP. Les dispositifs de sécurité écoutent des émissions de routage de RIP sur toutes les interfaces et les utilisations que les informations pour remplir tables de routage mais n'annoncent pas des mises à jour de routage. Employez la table passive d'interfaces afin de placer les interfaces spécifiques au RIP passif.Table passive d'interfaces — Répertorie les interfaces configurées sur les dispositifs de sécurité. Cochez la case dans la colonne passive pour ces interfaces que vous voulez actionner en mode passif. Les autres interfaces envoient et reçoivent toujours des émissions de RIP.

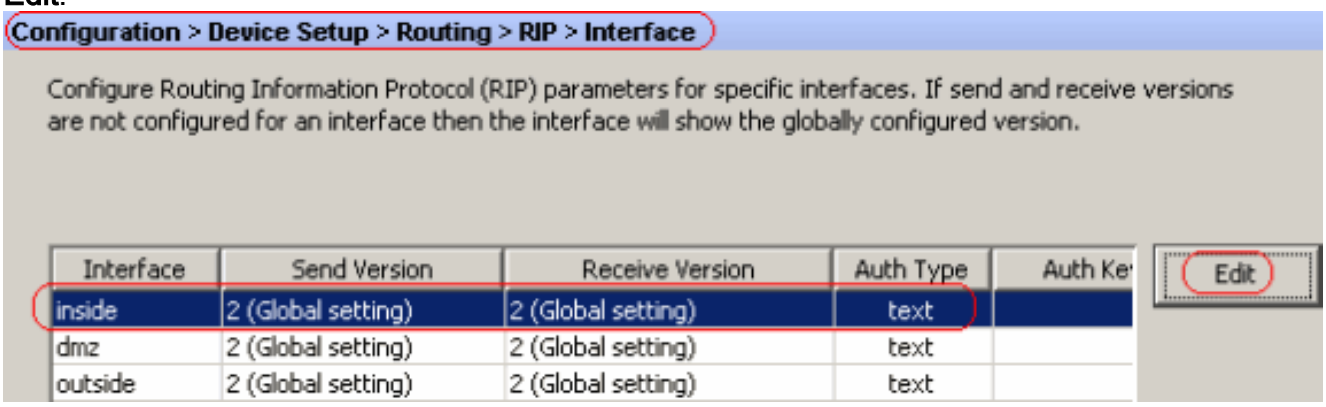
Configurez l'authentification de RIP

Cisco ASA prend en charge l'authentification de MD5 des mises à jour de routage du protocole de routage de RIP v2. Le condensé introduit par MD5 dans chaque paquet RIP empêche l'introduction des messages non autorisés ou faux de routage des sources inapprouvées. L'ajout de l'authentification à vos messages RIP s'assure que vos Routeurs et Cisco ASA reçoivent seulement des messages de routage d'autres périphériques de routage qui sont configurés avec la même clé pré-partagée. Sans cette authentification configurée, si vous introduit un autre périphérique de routage avec les informations différentes ou contraires d'artère en fonction au réseau, les tables de routage sur vos Routeurs ou Cisco ASA peuvent devenir corrompues, et une attaque par déni de service peut s'ensuivre. Quand vous ajoutez l'authentification aux messages RIP envoyés entre vos périphériques de routage, qui inclut l'ASA, elle empêche l'ajout utile ou accidentel d'un autre routeur au réseau et à n'importe quel problème.

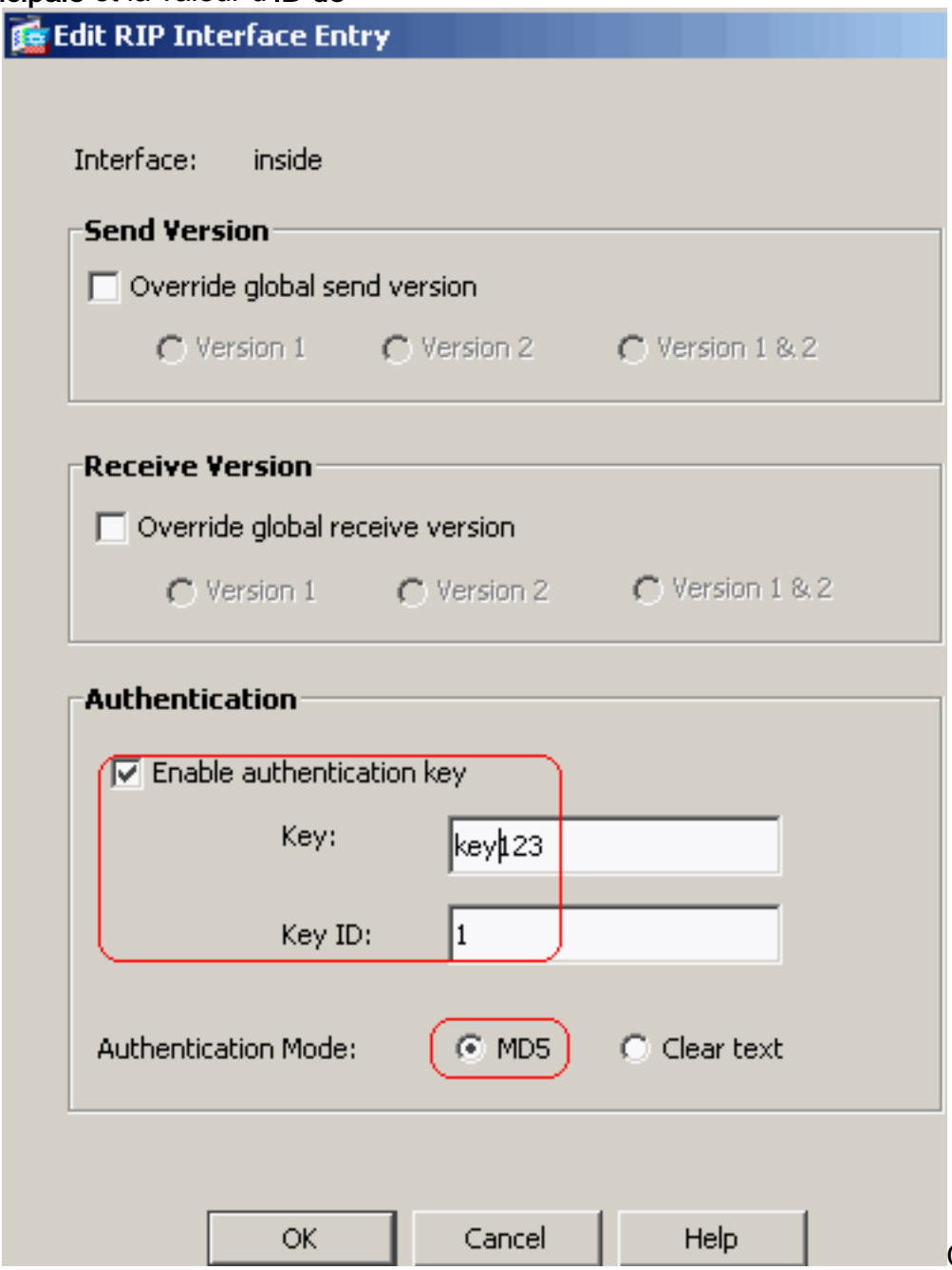
L'authentification de route RIP est par interface configuré. Tous les voisins RIP sur des interfaces configurées pour l'authentification de message RIP doivent être configurés avec la mêmes authentication mode et clé.

Terminez-vous ces étapes afin d'activer l'authentification de MD5 de RIP sur Cisco ASA.

1. Sur l'ASDM, choisissez la **configuration > l'installation de périphérique > le routage > le RIP > l'interface** et choisissez l'interface interne avec la souris. Cliquez sur **Edit**.



2. Choisissez la case à cocher de **clé d'authentification d'enable** et puis écrivez la valeur **principale** et la valeur d'**ID de**



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

Configuration de Cisco ASA CLI

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 <removed> key_id 1** ! *!--- 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

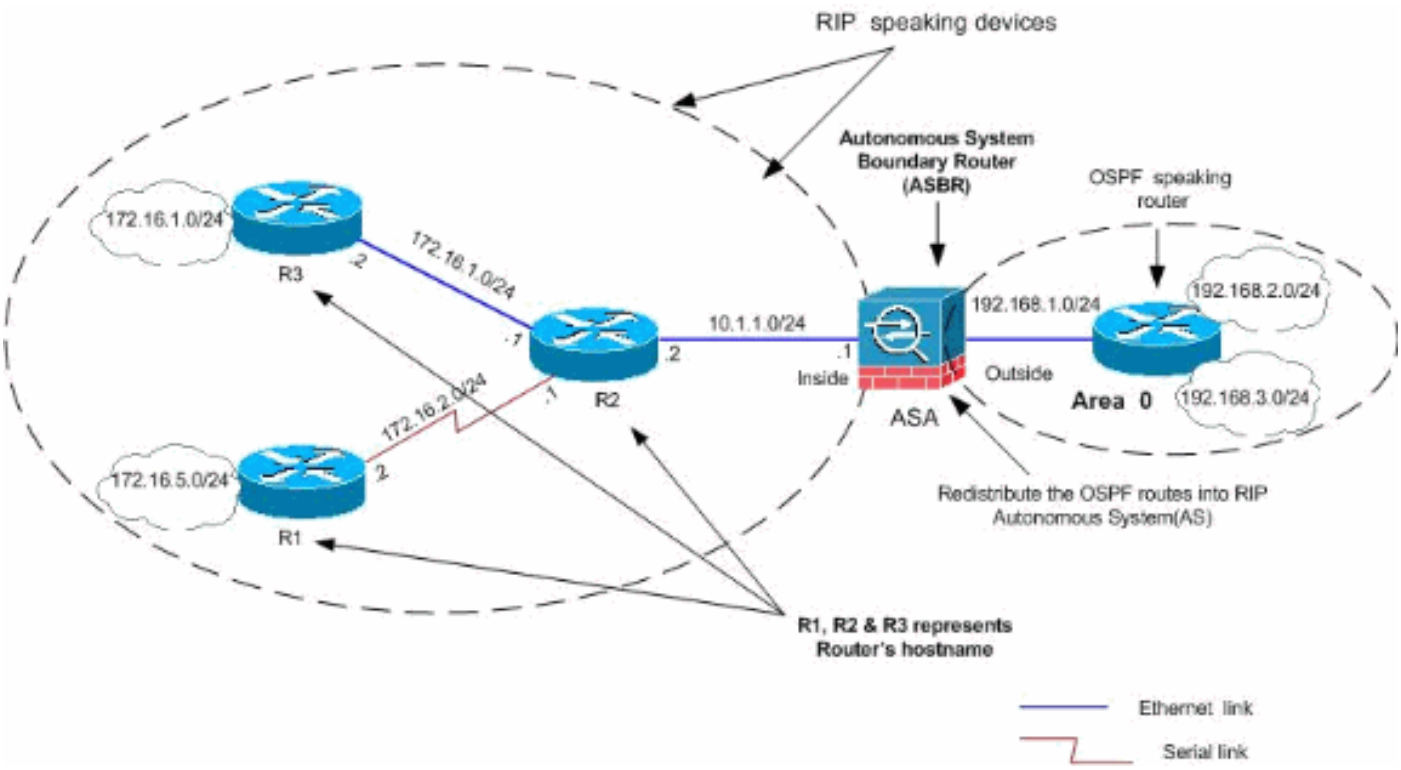
Configuration CLI du routeur Cisco IOS (R3)

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

Redistribuez dans le RIP avec l'ASA

Vous pouvez redistribuer des artères de l'OSPF, de l'EIGRP, de la charge statique, et des processus de routage connectés dans le processus de routage de RIP.

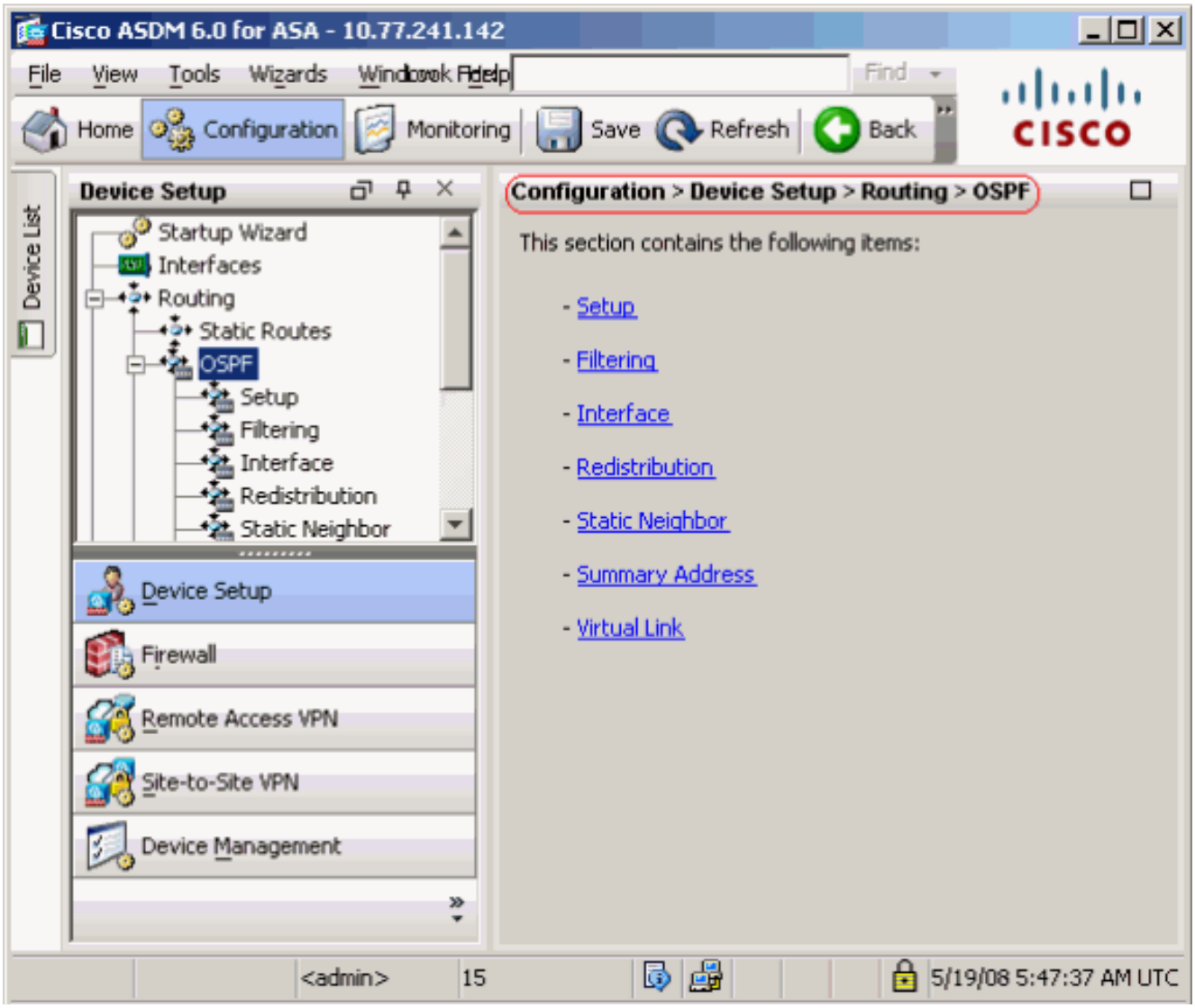
Dans cet exemple, la redistribution des artères OSPF dans le RIP avec le schéma de réseau est affichée :



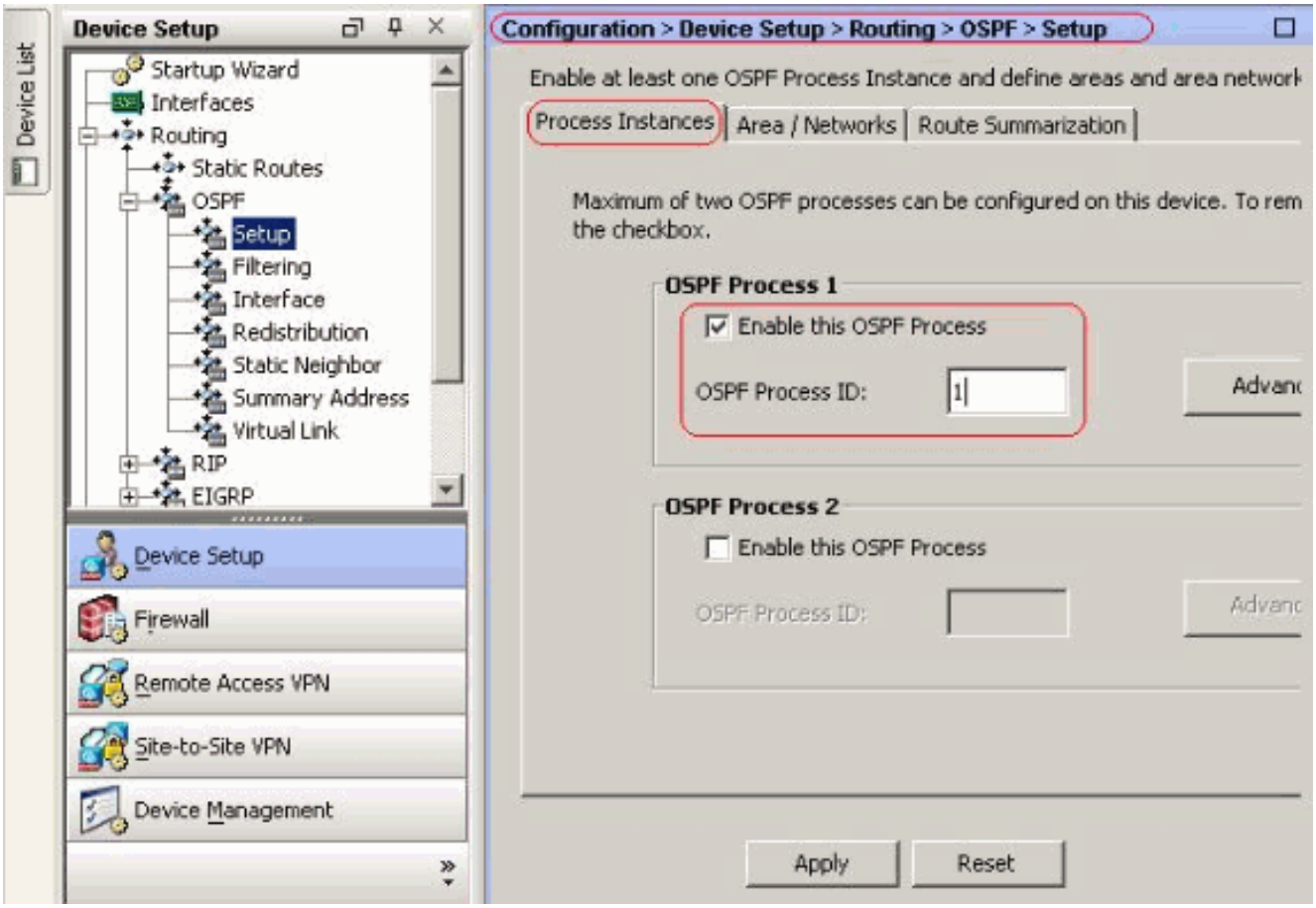
Configuration ASDM

Procédez comme suit :

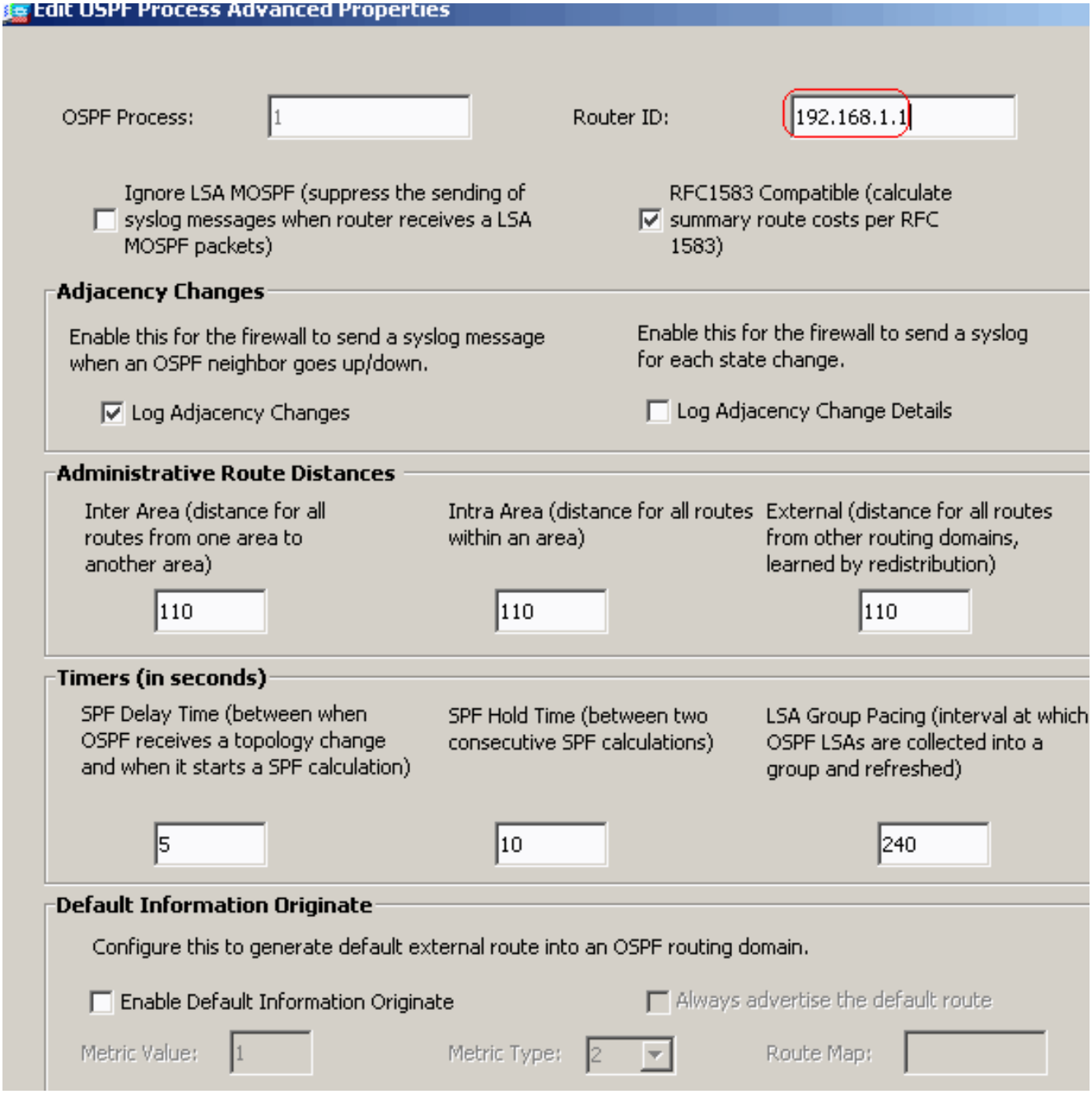
1. **Configuration OSPF**Choisissez la **configuration > l'installation de périphérique > le routage > l'OSPF** dans l'interface ASDM, suivant les indications du tir d'écran.



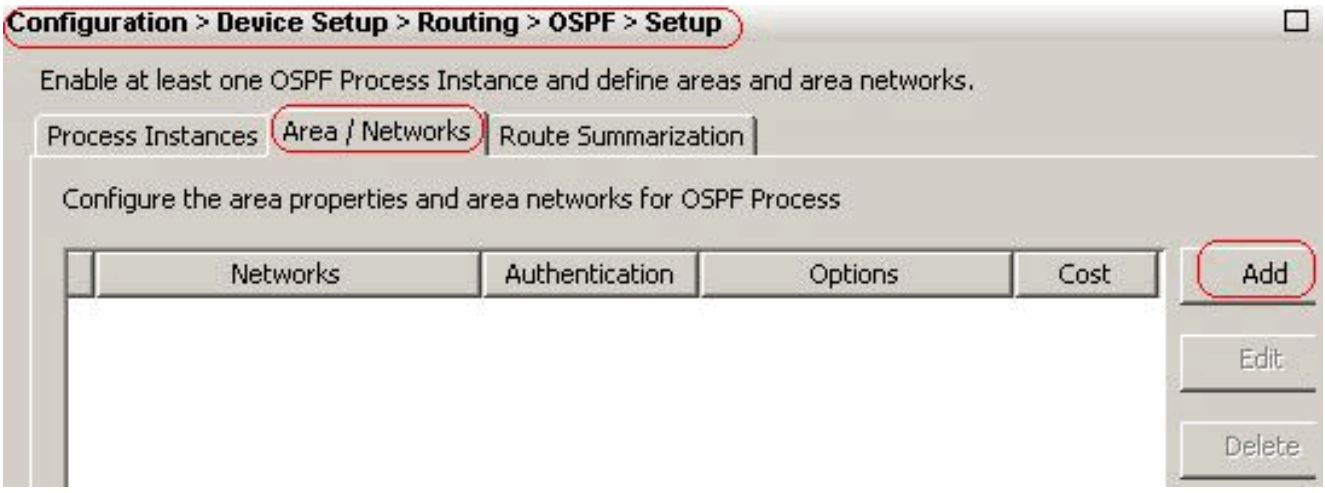
Activez le processus de routage OSPF sur l'onglet d'**exemples d'installation > de processus**, suivant les indications du tir d'écran. Dans cet exemple, le processus d'ID OSPF est **1.**



Le clic **a avancé** sur l'onglet d'**exemples d'installation > de processus** afin de configurer des paramètres de processus avancés facultatifs de routage OSPF. Vous pouvez éditer des configurations de processus-particularité, telles que l'ID de routeur, des modifications de contiguïté, des distances administratives d'artère, des temporisateurs, et les informations par défaut lancent des
configurations.

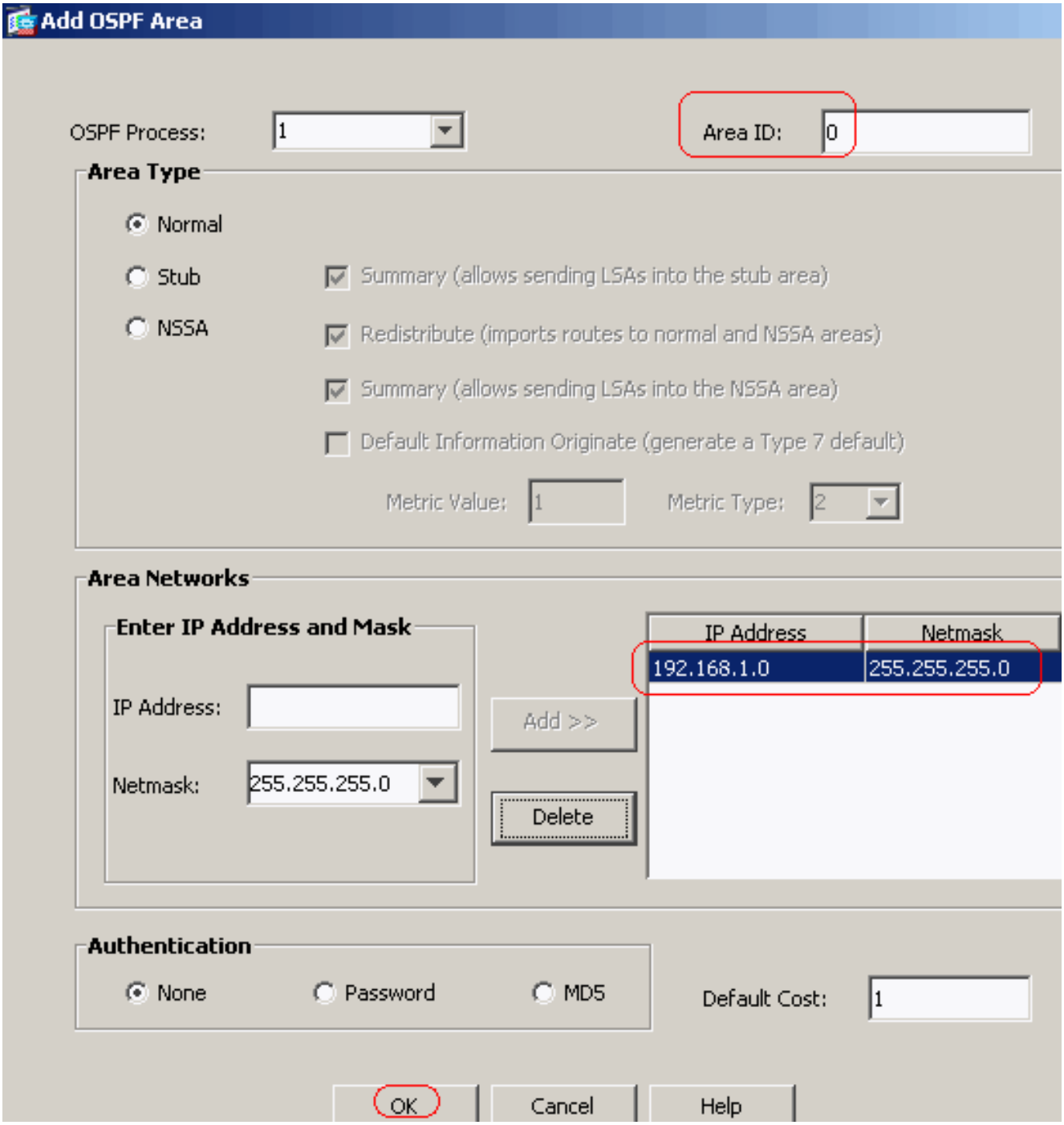


Cliquez sur **OK**.Après que vous vous terminiez les étapes précédentes, définissez les réseaux et les interfaces qui participent au routage OSPF sur l'**installation > la zone/réseaux** tableau cliquent sur Add suivant les indications de ce tir d'écran.

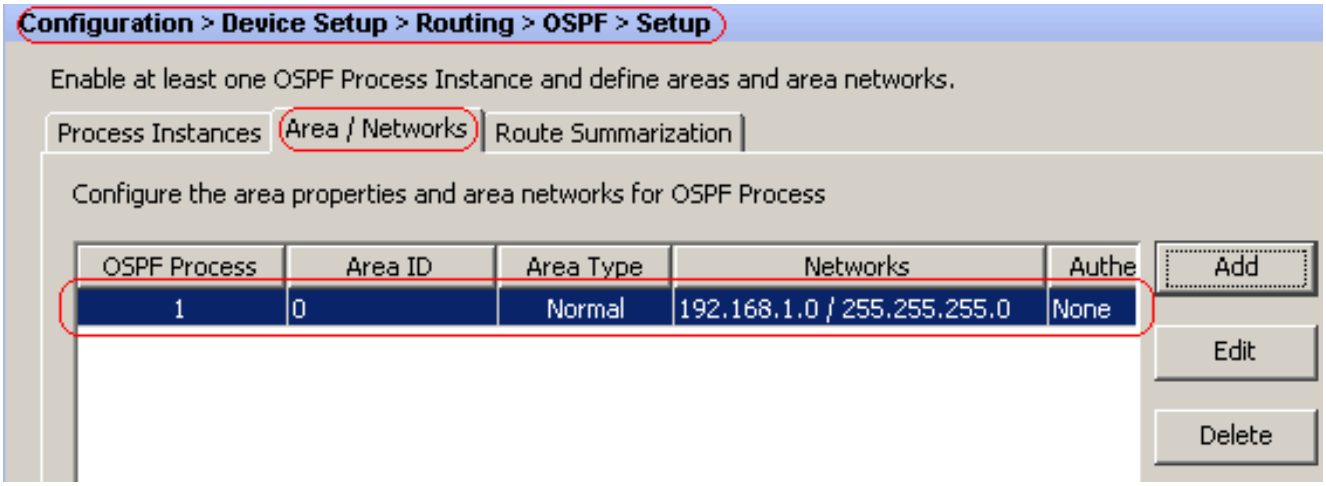


Cet écran apparaît. Dans cet exemple, le seul réseau que nous ajoutons est le réseau

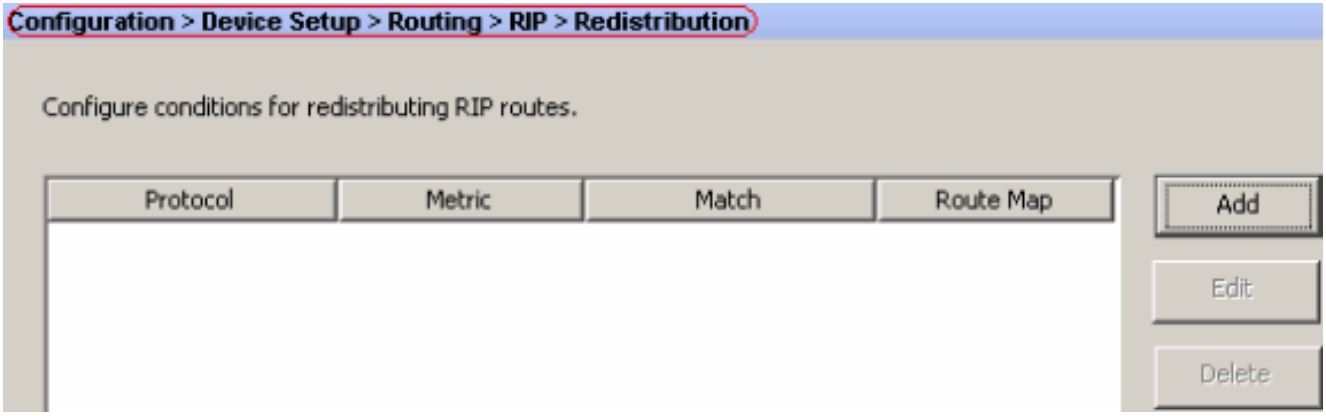
extérieur (192.168.1.0/24) puisque l'OSPF est activé seulement sur l'interface extérieure.**Remarque:** Se connecte par interface seulement à une adresse IP qui font partie des réseaux définis participent au processus de routage
OSPF.



Cliquez sur **OK**.Cliquez sur
Apply.

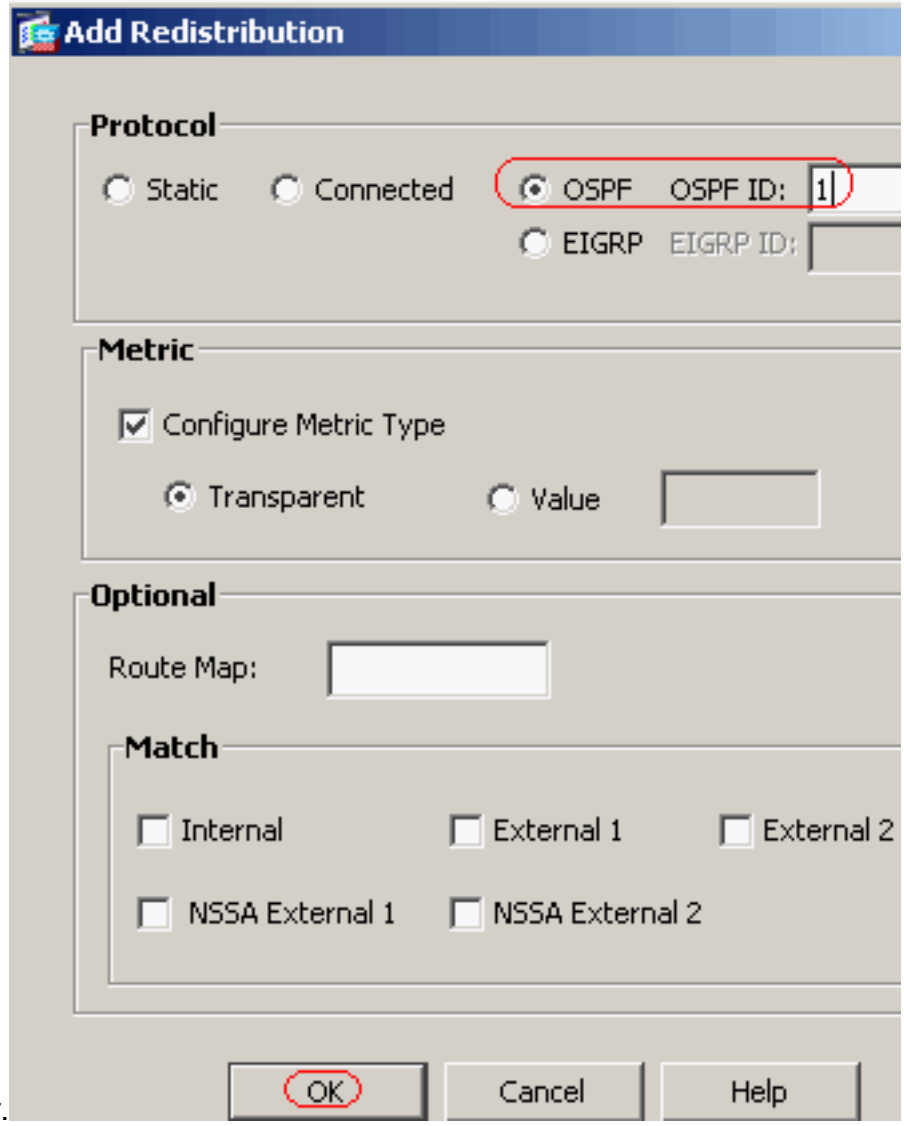


2. Choisissez la **configuration > l'installation de périphérique > le routage > le RIP > la redistribution > ajoutent** afin de redistribuer des artères OSPF dans le RIP.



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

Apply.



Configuration équivalente CLI

La configuration CLI de l'ASA pour redistribuent l'OSPF dans le 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 Cisco IOS voisin Router(R2) après avoir redistribué des artères OSPF dans le RIP AS.

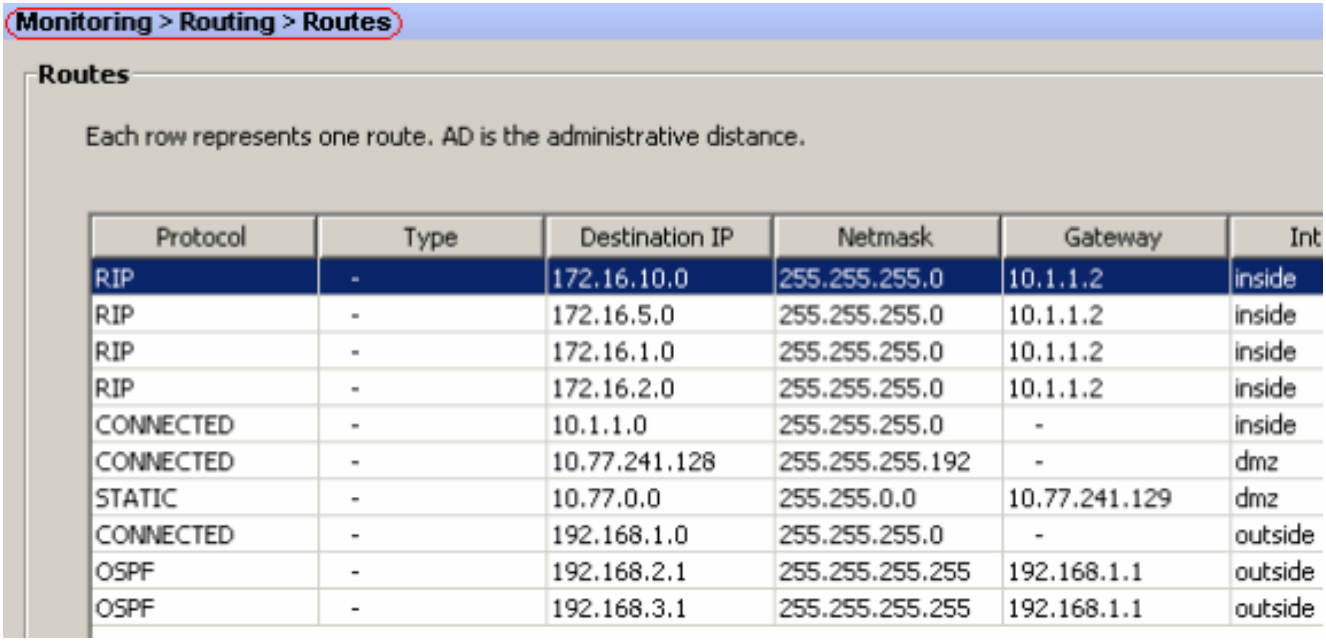
R2#**show ip route** Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, su - IS-IS 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
```

Vérifiez

Terminez-vous ces étapes afin de vérifier votre configuration :

1. Vous pouvez vérifier la table de routage si vous naviguez vers la **surveillance > routage > artères**. Dans ce tir d'écran, vous pouvez voir que les 172.16.1.0/24, 172.16.2.0/24, 172.16.5.0/24 et 172.16.10.0/24 réseaux sont appris par R2 (10.1.1.2) avec le 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. Du CLI, vous pouvez employer la commande de **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#
```

Dépannez

Cette section inclut des informations sur les commandes de débogage qui peuvent être utiles pour dépanner des 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: Référez-vous aux informations importantes sur les commandes de débogage avant

d'utiliser les commandes de **débogage**.

- **mettez au point les événements de déchirure** — Active l'élimination des imperfections des événements de 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