Exemple de configuration du protocole EIGRP ASA 9.x

Contenu

Introduction

Ce document décrit comment configurer le dispositif de sécurité adaptatif Cisco (ASA) afin d'apprendre les routes via le protocole EIGRP (Enhanced Interior Gateway Routing Protocol), qui est pris en charge dans le logiciel ASA version 9.x et ultérieures, et effectuer l'authentification.

Conditions préalables

Conditions requises

Cisco exige que vous remplissiez ces conditions avant de tenter cette configuration :

- Cisco ASA doit exécuter la version 9.x ou ultérieure.
- EIGRP doit être en mode de contexte unique, car il n'est pas pris en charge en mode de contexte multiple.

Components Used

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

- Logiciel Cisco ASA version 9.2.1
- Cisco Adaptive Security Device Manager (ASDM) version 7.2.1
- Routeur Cisco IOS® qui exécute la version 12.4

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.

Informations générales

Directives et limitations

- Une instance EIGRP est prise en charge en mode unique et par contexte en mode multimode.
- Deux threads sont créés par contexte par instance EIGRP en mode multimode et peuvent être affichés avec le processus show.
- La récapitulation automatique est désactivée par défaut.
- Une relation de voisinage n'est pas établie entre les unités de cluster en mode d'interface individuelle.
- Les informations par défaut de [<acl>] sont utilisées afin de filtrer le bit extérieur dans les routes candidates entrantes par défaut.
- Default-information out [<acl>] est utilisé afin de filtrer le bit Exterior dans les routes candidates sortantes par défaut.

EIGRP et basculement

Le code Cisco ASA version 8.4.4.1 et ultérieure synchronise les routes dynamiques de l'unité ACTIVE à l'unité STANDBY. En outre, la suppression des routes est également synchronisée avec l'unité STANDBY. Cependant, l'état des contiguïtés homologues n'est pas synchronisé ; seul le périphérique ACTIVE gère l'état du voisin et participe activement au routage dynamique. Reportez-vous à la FAQ ASA : Que se passe-t-il après le basculement si les routes dynamiques sont synchronisées ? pour plus d'informations.

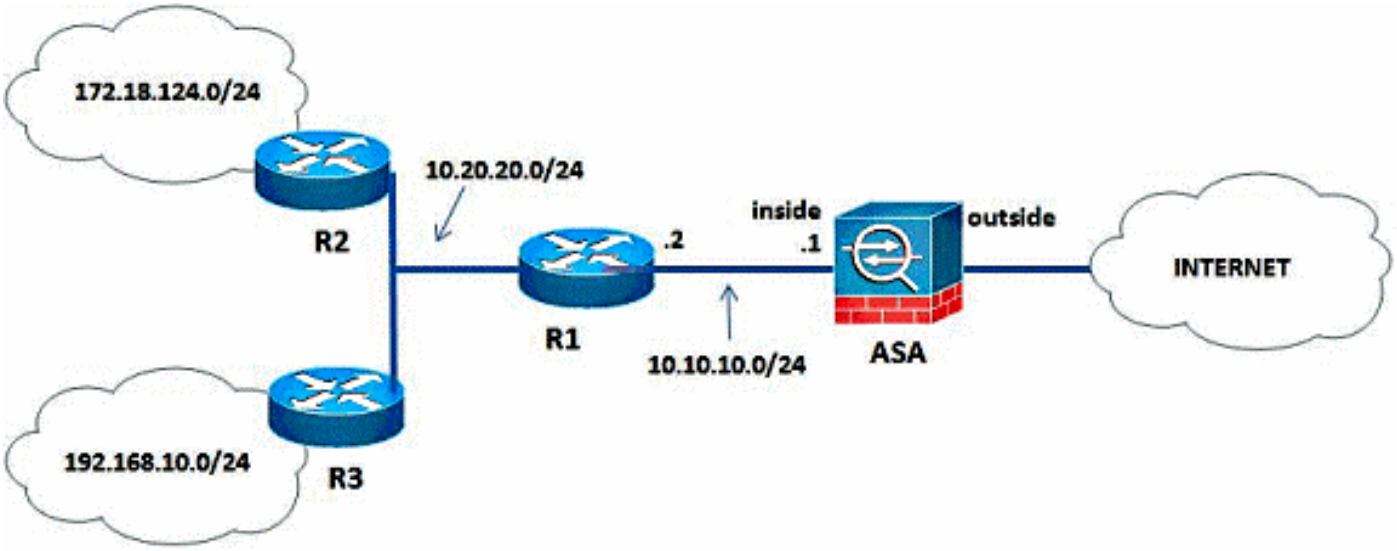
Configuration

Cette section décrit comment configurer les fonctionnalités couvertes dans ce document.

Note: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Dans la topologie de réseau illustrée, l'adresse IP de l'interface interne Cisco ASA est 10.10.10.1/24. L'objectif est de configurer EIGRP sur Cisco ASA afin d'apprendre les routes vers les réseaux internes (10.20.20.0/24, 172.18.124.0/24 et 192.168.10.0/24) de manière dynamique via le routeur adjacent (R1). R1 apprend les routes vers les réseaux internes distants via les deux autres routeurs (R2 et R3).

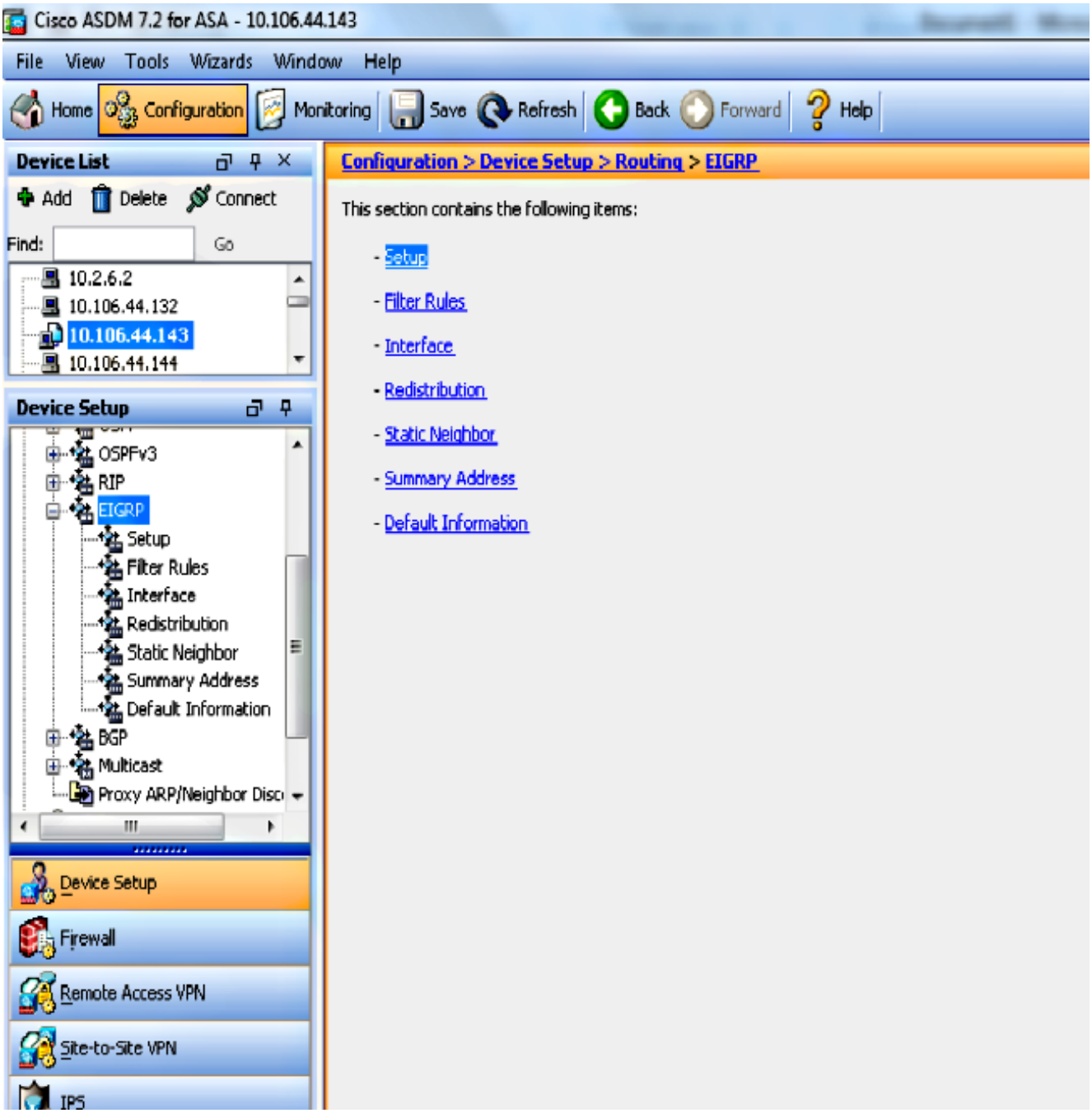
Configuration ASDM

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 du dispositif de sécurité, puis utilisé pour configurer, surveiller et gérer le périphérique. Vous pouvez également utiliser le lanceur ASDM 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.

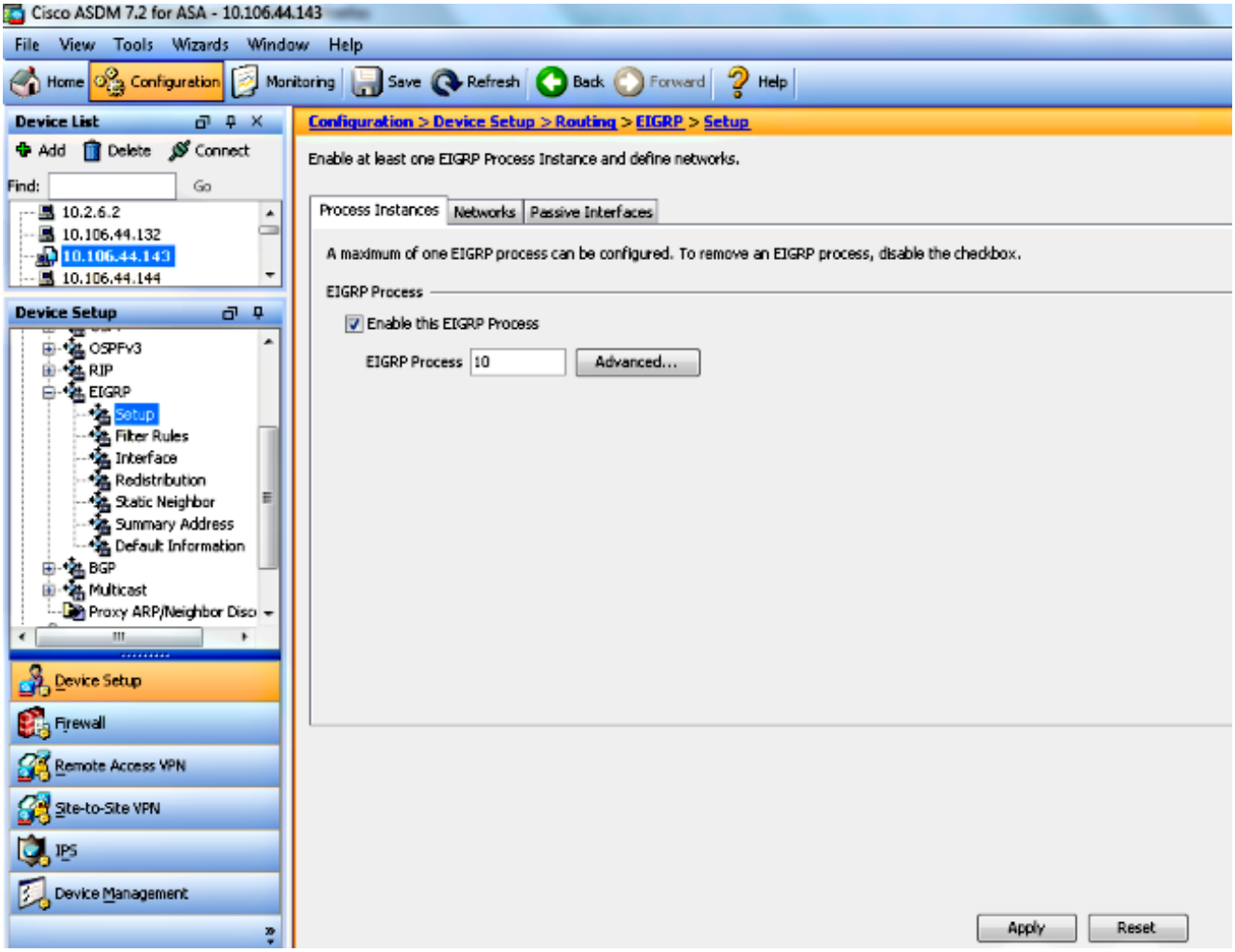
Complétez ces étapes afin de configurer le protocole EIGRP dans Cisco ASA.

1. Connectez-vous à Cisco ASA avec l'ASDM.

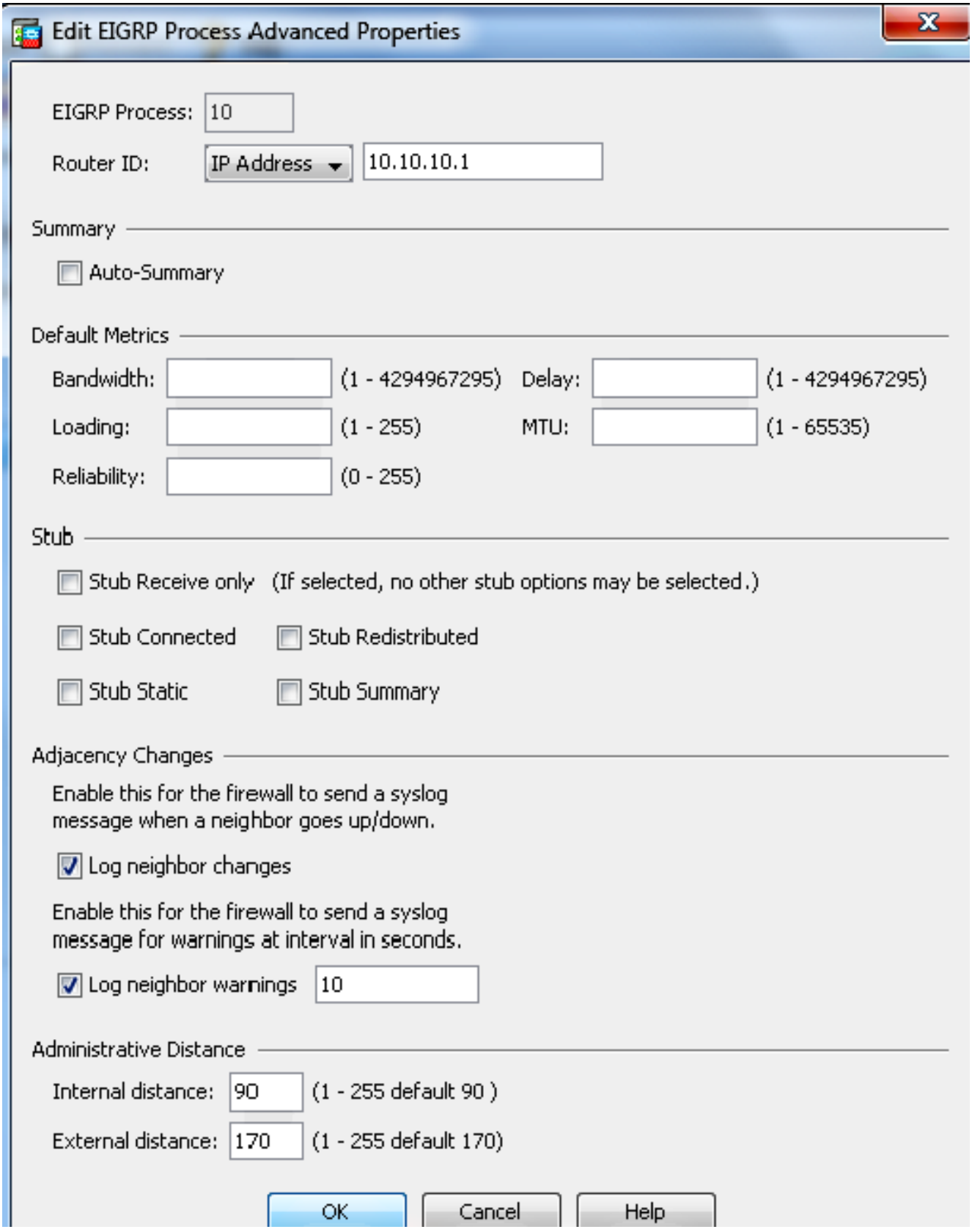
2. Accédez à la zone **Configuration > Device Setup > Routing > EIGRP** de l'interface ASDM, comme indiqué dans cette capture d'écran.



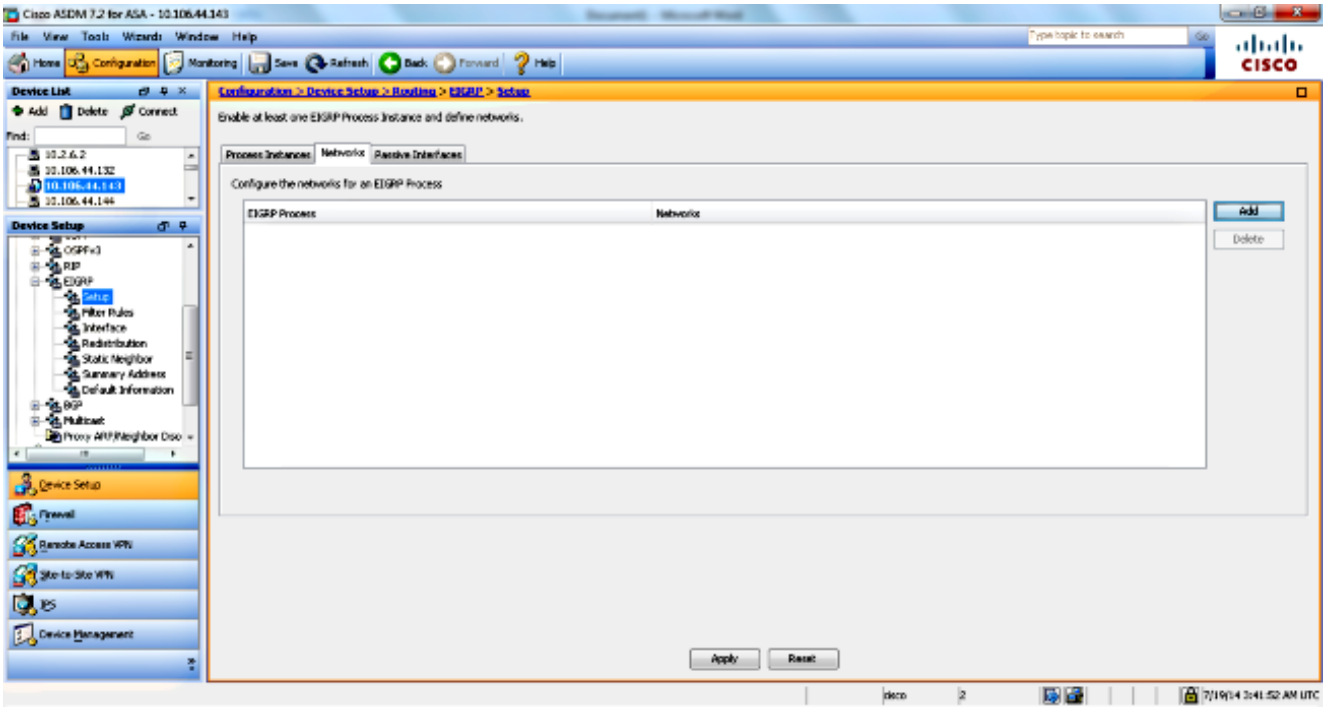
3. Activez le processus de routage EIGRP sous l'onglet **Setup > Process Instances**, comme indiqué dans cette capture d'écran. Dans cet exemple, le processus EIGRP est **10**.



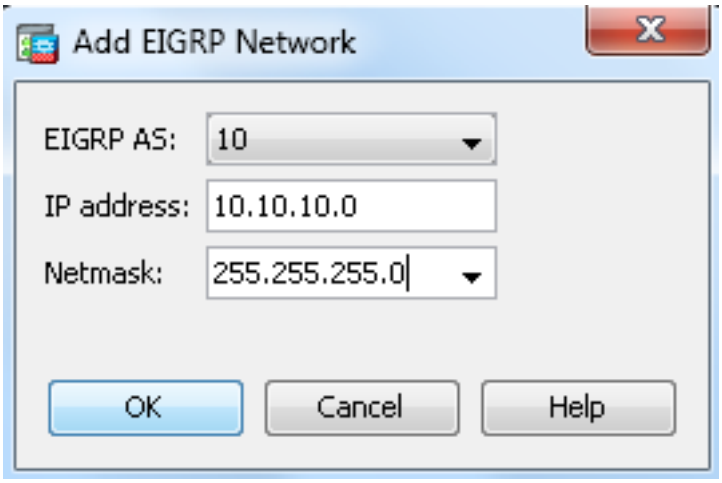
4. Vous pouvez configurer des paramètres de processus de routage EIGRP avancés en option. Cliquez sur **Avancé** dans l'onglet **Configuration > Instances de processus**. Vous pouvez configurer le processus de routage EIGRP en tant que processus de routage d'extrémité, désactiver la récapitulation automatique de route, définir les métriques par défaut pour les routes redistribuées, modifier les distances administratives pour les routes EIGRP internes et externes, configurer un ID de routeur statique et activer ou désactiver la journalisation des modifications de contiguïté. Dans cet exemple, l'ID de routeur EIGRP est configuré de manière statique avec l'adresse IP de l'interface interne (10.10.10.1). En outre, **Auto-Summary** est également désactivé. Toutes les autres options sont configurées avec leurs valeurs par défaut.



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



6. Cet écran apparaît. Dans cet exemple, le seul réseau que vous ajoutez est le réseau interne (10.10.10.0/24) puisque le protocole EIGRP est activé uniquement sur l'interface interne.



Seules les interfaces avec une adresse IP qui fait partie des réseaux définis participent au processus de routage EIGRP. Si vous avez une interface que vous ne voulez pas participer au routage EIGRP mais qui est connectée à un réseau que vous voulez annoncer, configurez une entrée réseau dans l'onglet **Setup > Networks** qui couvre le réseau auquel l'interface est connectée, puis configurez cette interface en tant qu'interface passive afin que l'interface ne puisse pas envoyer ou recevoir de mises à jour EIGRP.

Note: Les interfaces configurées comme passives n'envoient ni ne reçoivent de mises à jour EIGRP.

7. 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 EIGRP.

8. Vous pouvez éventuellement configurer la redistribution de route. Cisco ASA peut

redistribuer les routes découvertes par le protocole RIP (Routing Information Protocol) et OSPF (Open Shortest Path First) dans le processus de routage EIGRP. Vous pouvez également redistribuer des routes statiques et connectées dans le processus de routage EIGRP. Vous n'avez pas besoin de redistribuer les routes statiques ou connectées si elles se trouvent dans la plage d'un réseau configuré dans l'onglet **Setup > Networks**. Définissez la redistribution de route dans le volet Redistribution.

9. Les paquets Hello EIGRP sont envoyés en tant que paquets de multidiffusion. Si un voisin EIGRP est situé sur un réseau non diffusé, vous devez définir manuellement ce voisin. Lorsque vous définissez manuellement un voisin EIGRP, des paquets Hello sont envoyés à ce voisin en tant que messages de monodiffusion. Afin de définir des voisins EIGRP statiques, accédez au volet **Voisin statique**.

10. Par défaut, les routes par défaut sont envoyées et acceptées. Afin de restreindre ou de désactiver l'envoi et la réception des informations de route par défaut, ouvrez le volet **Configuration > Device Setup > Routing > EIGRP > Default Information**. Le volet Informations par défaut affiche un tableau de règles pour contrôler l'envoi et la réception des informations de route par défaut dans les mises à jour EIGRP.

    Note: Vous pouvez avoir une règle "*in »* et une règle "*out*" pour chaque processus de routage EIGRP. (Un seul processus est actuellement pris en charge.)

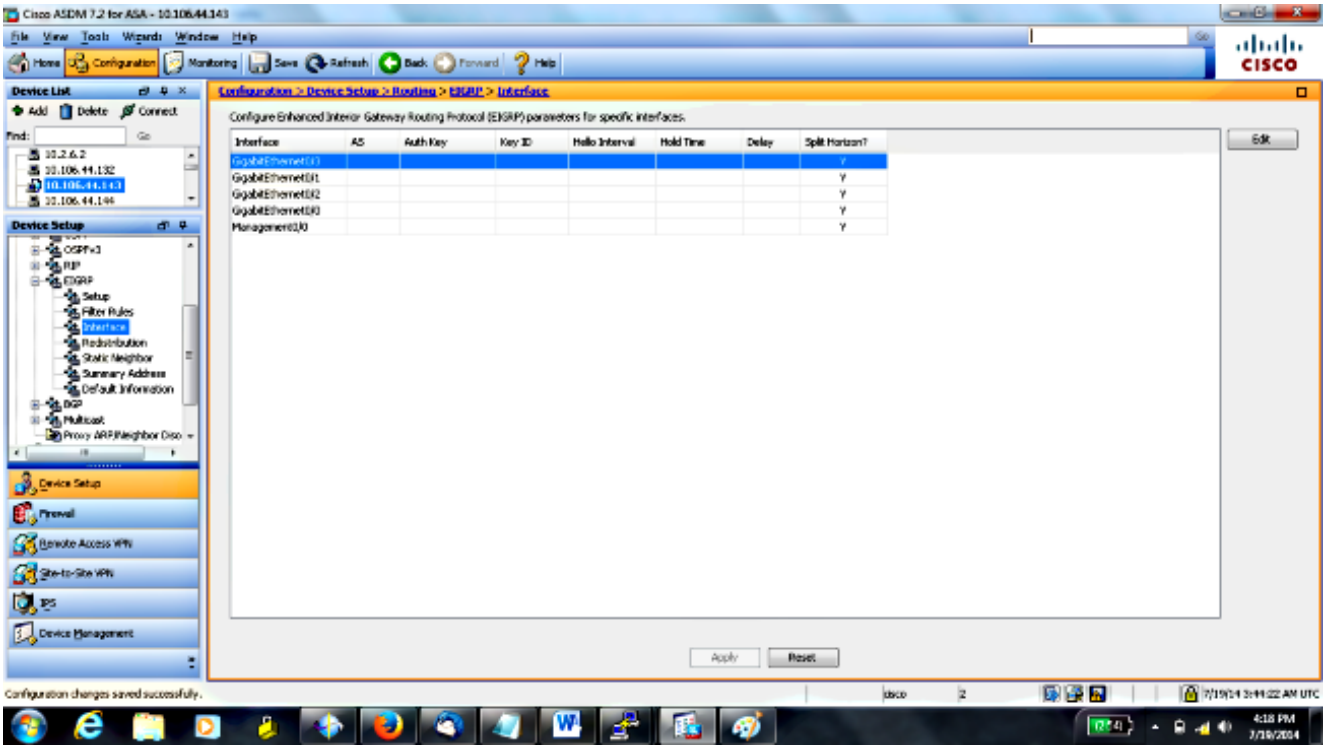
Configuration de l'authentification EIGRP

Cisco ASA prend en charge l'authentification MD5 des mises à jour de routage à partir du protocole de routage EIGRP. Le résumé à clé MD5 de chaque paquet EIGRP empêche l'introduction de messages de routage non autorisés ou faux provenant de sources non approuvées. L'ajout de l'authentification à vos messages EIGRP 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), elle empêche les ajouts non autorisés de routeurs EIGRP dans votre topologie de routage.

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

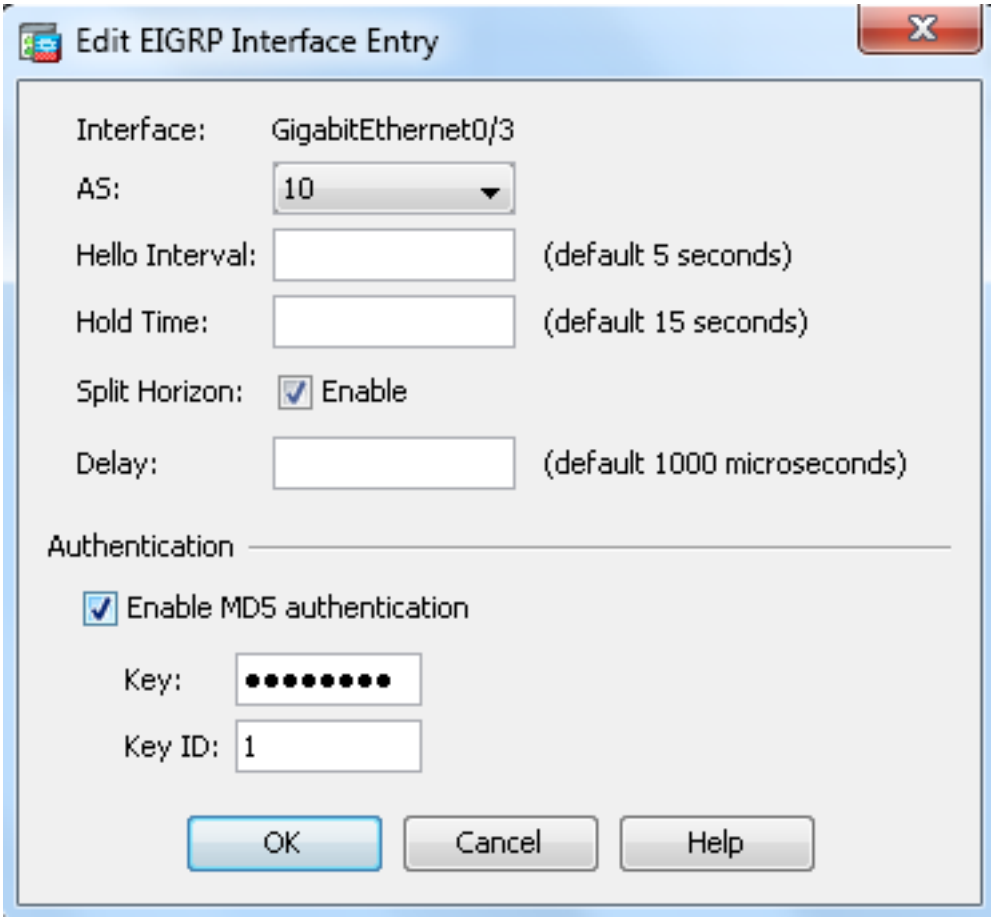
Complétez ces étapes afin d'activer l'authentification MD5 EIGRP sur Cisco ASA.

1. Sur l'ASDM, accédez à **Configuration > Device Setup > Routing > EIGRP > Interface** comme indiqué.



2. Dans ce cas, le protocole EIGRP est activé sur l'interface interne (GigabitEthernet 0/1). Choisissez l'interface **GigabitEthernet 0/1** et cliquez sur **Modifier**.

3. Sous Authentication, sélectionnez **Enable MD5 authentication**. 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**.



Filtrage de route EIGRP

Avec le protocole EIGRP, vous pouvez contrôler les mises à jour de routage envoyées et reçues. Dans cet exemple, vous allez bloquer les mises à jour de routage sur l'ASA pour le préfixe réseau 192.168.10.0/24, qui se trouve derrière R1. Pour le filtrage de route, vous pouvez uniquement utiliser la **liste de contrôle d'accès STANDARD**.

```
access-list eigrp standard deny 192.168.10.0 255.255.255.0
access-list eigrp standard permit any

router eigrp 10
distribute-list eigrp in
```

Vérification

```
ASA(config)# show access-list eigrp
access-list eigrp; 2 elements; name hash: 0xd43d3adc
access-list eigrp line 1 standard deny 192.168.10.0 255.255.255.0 (hitcnt=3) 0xeb48ecd0
access-list eigrp line 2 standard permit any4 (hitcnt=12) 0x883fe5ac
```

Configurations

Configuration CLI de Cisco ASA

Il s'agit de la configuration CLI de Cisco ASA.

```
!outside interface configuration

interface GigabitEthernet0/0
description outside interface connected to the Internet
nameif outside
security-level 0
ip address 198.51.100.120 255.255.255.0
!

!inside interface configuration

interface GigabitEthernet0/1
description interface connected to the internal network
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
!

!EIGRP authentication is configured on the inside interface

authentication key eigrp 10 cisco123 key-id 1
authentication mode eigrp 10 md5
!

!management interface configuration

interface Management0/0
```

```
nameif management
security-level 99
ip address 10.10.20.1 255.255.255.0 management-only
!
!

!EIGRP Configuration - the CLI configuration is very similar to the
!Cisco IOS router EIGRP configuration.

router eigrp 10
no auto-summary
eigrp router-id 10.10.10.1
network 10.10.10.0 255.255.255.0
!

!This is the static default gateway configuration

route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```

Configuration CLI du routeur Cisco IOS (R1)

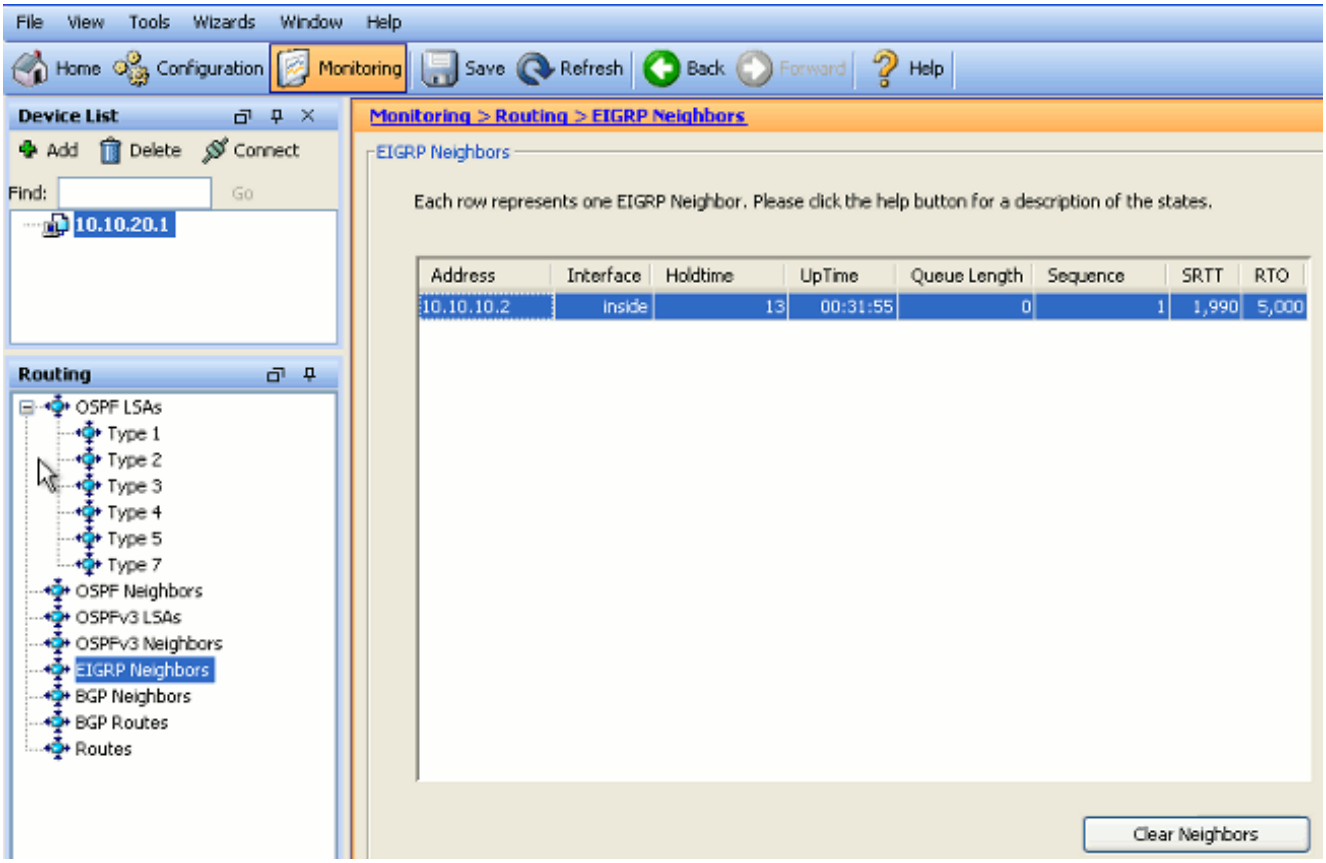
Il s’agit de la configuration CLI de R1 (routeur interne).

```
!!Interface that connects to the Cisco ASA. Notice the EIGRP authentication
paramenters.


interface FastEthernet0/0
ip address 10.10.10.2 255.255.255.0
ip authentication mode eigrp 10 md5
ip authentication key-chain eigrp 10 MYCHAIN
!
!

! EIGRP Configuration

router eigrp 10
network 10.10.10.0 0.0.0.255
network 10.20.20.0 0.0.0.255
network 172.18.124.0 0.0.0.255
network 192.168.10.0
no auto-summary
```

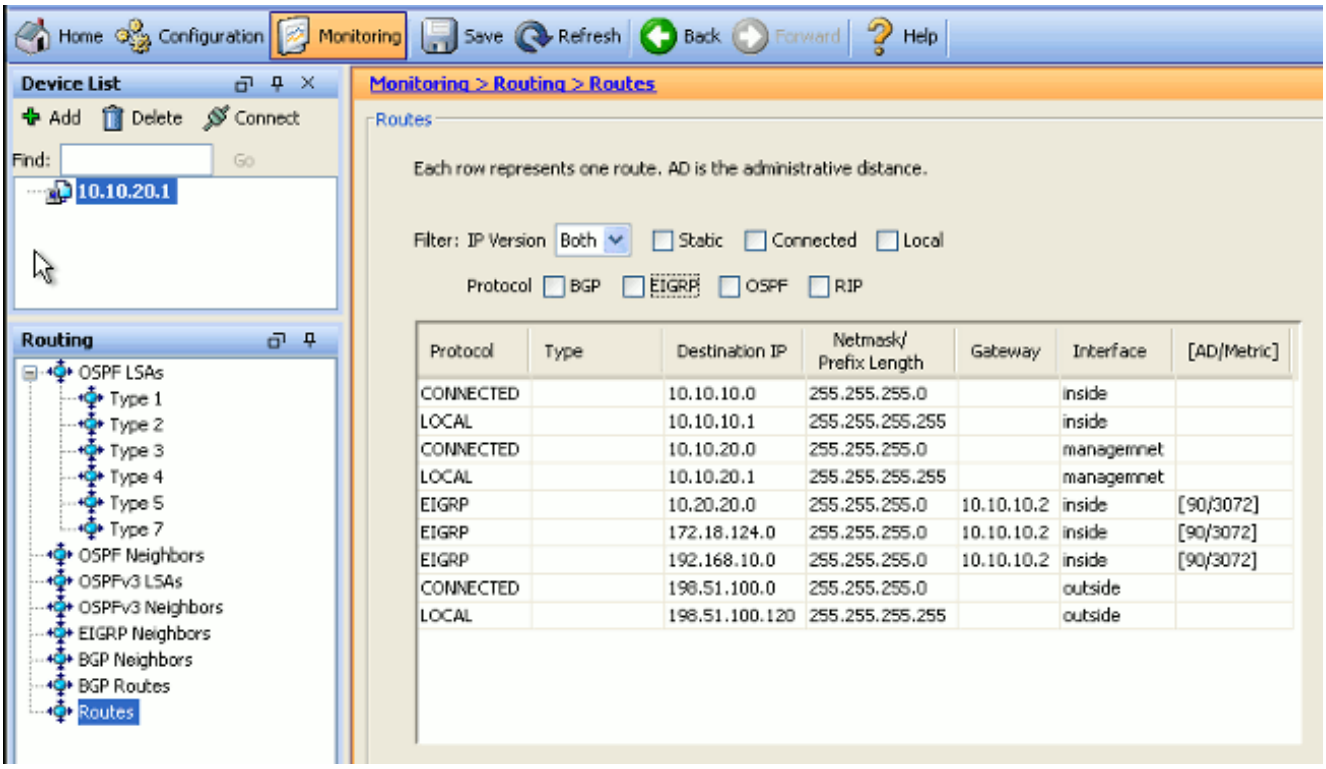
Vérification

Complétez ces étapes afin de vérifier votre configuration.

1. Sur l'ASDM, vous pouvez accéder à **Monitoring > Routing > EIGRP Neighbor** afin de voir chacun des voisins EIGRP. Cette capture d'écran montre le routeur interne (R1) en tant que voisin actif. Vous pouvez également voir l'interface où réside ce voisin, la durée de conservation et la durée de fonctionnement de la relation de voisinage (UpTime).



2. En outre, 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 **192.168.10.0/24, 172.18.124.0/24** et **10.20.20.0/24** sont appris via R1 (**10.10.10.2**).



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 100.10.10.2 to network 0.0.0.0
C 198.51.100.0 255.255.255.0 is directly connected, outside
D 192.168.10.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 172.18.124.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
C 127.0.0.0 255.255.0.0 is directly connected, cplane
D 10.20.20.0 255.255.255.0 [90/28672] via 10.10.10.2, 0:32:29, inside
C 10.10.10.0 255.255.255.0 is directly connected, inside
C 10.10.20.0 255.255.255.0 is directly connected, management
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

Avec ASA version 9.2.1 et ultérieure, vous pouvez utiliser la commande **show route eigrp** afin d'afficher uniquement les routes EIGRP.

```
ciscoasa(config)# show route eigrp

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

Gateway of last resort is not set

D 192.168.10.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 172.18.124.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 10.20.20.0 255.255.255.0 [90/28672] via 10.10.10.2, 0:32:29, inside
```

3. Vous pouvez également utiliser la commande **show eigrp topology** afin d'obtenir des informations sur les réseaux appris et la topologie EIGRP.

```
    ciscoasa# show eigrp topology
EIGRP-IPv4 Topology Table for AS(10)/ID(10.10.10.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status
P 10.20.20.0 255.255.255.0, 1 successors, FD is 28672
via 10.10.10.2 (28672/28416), GigabitEthernet0/1
P 10.10.10.0 255.255.255.0, 1 successors, FD is 2816
via Connected, GigabitEthernet0/1
P 192.168.10.0 255.255.255.0, 1 successors, FD is 131072
via 10.10.10.2 (131072/130816), GigabitEthernet0/1
P 172.18.124.0 255.255.255.0, 1 successors, FD is 131072
via 10.10.10.2 (131072/130816), GigabitEthernet0/1
```

4. La commande **show eigrp 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 de l'ASDM à l'étape 1.

```
ciscoasa# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq (sec) (ms)Cnt Num

0 10.10.10.2 Gi0/1 12 00:39:12 107 642 0 1
```

Flux des paquets

Voici le flux de paquets.

1. L'ASA apparaît sur la liaison et envoie un paquet Hello mCast via toutes ses interfaces configurées EIGRP.

2. R1 reçoit un paquet Hello et envoie un paquet Hello mCast.

13 5.572557	10.10.10.1	224.0.0.10	EIGRP	86 0x3b1a (15130)	Hello
14 5.573335	10.10.10.2	224.0.0.10	EIGRP	86 0x2321 (8993)	Hello
15 5.575212	10.10.10.1	10.10.10.2	EIGRP	54 0x0589 (1417)	Update
16 5.581712	10.10.10.2	10.10.10.1	EIGRP	54 0x19d9 (6617)	Update
17 5.585145	10.10.10.1	10.10.10.2	EIGRP	54 0x755e (30046)	Hello (Ack)
18 5.585373	10.10.10.1	10.10.10.2	EIGRP	96 0x1c93 (7315)	Update
19 5.591919	10.10.10.2	10.10.10.1	EIGRP	54 0x6695 (26261)	Hello (Ack)
20 5.591950	10.10.10.2	10.10.10.1	EIGRP	180 0x7925 (31013)	Update
21 5.595200	10.10.10.1	10.10.10.2	EIGRP	96 0x62e8 (25320)	Update
22 5.601913	10.10.10.2	10.10.10.1	EIGRP	54 0x08a7 (2215)	Hello (Ack)
23 5.601944	10.10.10.2	10.10.10.1	EIGRP	96 0x31c5 (12741)	Update

3. L'ASA reçoit le paquet Hello et envoie un paquet Update avec un bit initial défini, ce qui indique qu'il s'agit du processus d'initialisation.

4. R1 reçoit un paquet Update et envoie un paquet Update avec un jeu de bits initial, ce qui indique qu'il s'agit du processus d'initialisation.

```
⊞ Frame 15: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
⊞ Ethernet II, Src: Cisco_25:32:e2 (00:21:a0:25:32:e2), Dst: Cisco_1f:25:e3 (6c:41:6a:1f:25:e3)
⊞ Internet Protocol Version 4, Src: 10.10.10.1 (10.10.10.1), Dst: 10.10.10.2 (10.10.10.2)
⊟ Cisco EIGRP
    Version: 2
    Opcode: Update (1)
    Checksum: 0xfdc4 [correct]
  ⊟ Flags: 0x00000001, Init
      .... .... .... .... .... .... .... ...1 = Init: Set
      .... .... .... .... .... .... .... ..0. = Conditional Receive: Not set
      .... .... .... .... .... .... .... .0.. = Restart: Not set
      .... .... .... .... .... .... .... 0... = End Of Table: Not set
    Sequence: 47
    Acknowledge: 0
    Virtual Router ID: 0 (Address-Family)
    Autonomous System: 10
```

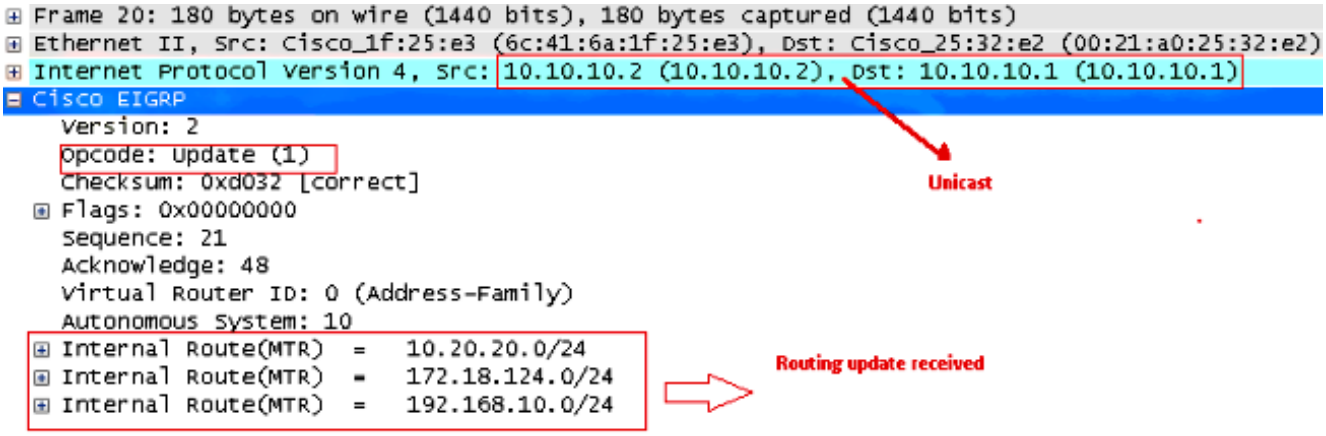
5. Une fois que l'ASA et R1 ont échangé des paquets Hello et que la contiguïté de voisinage est établie, l'ASA et R1 répondent tous deux avec un paquet ACK, ce qui indique que les

informations de mise à jour ont été reçues.

6. ASA envoie ses informations de routage à R1 dans un paquet Update.

7. R1 insère les informations de paquet Update dans sa table topologique. La table topologique inclut toutes les destinations annoncées par les voisins. Il est organisé de sorte que chaque destination soit répertoriée, ainsi que tous les voisins qui peuvent se rendre à la destination et leurs métriques associées.

8. R1 envoie ensuite un paquet Update à l'ASA.



9. Une fois qu'il a reçu le paquet Update, l'ASA envoie un paquet ACK à R1. Une fois que l'ASA et R1 ont reçu les paquets de mise à jour les uns des autres, ils sont prêts à choisir les routes successeur (meilleure) et successeur potentiel (de secours) dans la table topologique et à offrir les routes successeur à la table de routage.

Dépannage

Cette section contient des informations sur les commandes **debug** et **show** qui peuvent être utiles pour résoudre les problèmes EIGRP.

Dépannage des commandes

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

> **Note**: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage. Afin d'afficher les informations de débogage de la machine à état fini DUAL (Diffusing Update Algorithm), utilisez la commande **debug eigrp fsm** en mode d'exécution privilégié. Cette commande vous permet d'observer l'activité du successeur potentiel EIGRP et de déterminer si les mises à jour de route sont installées et supprimées par le processus de routage.

Il s'agit de la sortie de la commande **debug** dans l'appairage réussi avec R1. Vous pouvez voir chacune des différentes routes qui sont correctement installées sur le système.

```
EIGRP-IPv4(Default-IP-Routing-Table:10): Callback: route_adjust GigabitEthernet0/1
DUAL: dest(10.10.10.0 255.255.255.0) not active
DUAL: rcvupdate: 10.10.10.0 255.255.255.0 via Connected metric 2816/0 on topoid 0
DUAL: Find FS for dest 10.10.10.0 255.255.255.0. FD is 4294967295, RD is 4294967
295 on topoid 0 found
DUAL: RT installed 10.10.10.0 255.255.255.0 via 0.0.0.0
DUAL: Send update about 10.10.10.0 255.255.255.0. Reason: metric chg on topoid
0
DUAL: Send update about 10.10.10.0 255.255.255.0. Reason: new if on topoid 0
DUAL: dest(10.20.20.0 255.255.255.0) not active
DUAL: rcvupdate: 10.20.20.0 255.255.255.0 via 10.10.10.2 metric 28672/28416 on t
opoid 0
DUAL: Find FS for dest 10.20.20.0 255.255.255.0. FD is 4294967295, RD is 4294967
295 on topoid 0 found
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 10.20.20.0 ()
DUAL: RT installed 10.20.20.0 255.255.255.0 via 10.10.10.2
DUAL: Send update about 10.20.20.0 255.255.255.0. Reason: metric chg on topoid
0
DUAL: Send update about 10.20.20.0 255.255.255.0. Reason: new if on topoid 0
DUAL: dest(172.18.124.0 255.255.255.0) not active
DUAL: rcvupdate: 172.18.124.0 255.255.255.0 via 10.10.10.2 metric 131072/130816
on topoid 0
DUAL: Find FS for dest 172.18.124.0 255.255.255.0. FD is 4294967295, RD is 42949
67295 on topoid 0 found
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 172.18.124.0 ()
DUAL: RT installed 172.18.124.0 255.255.255.0 via 10.10.10.2
DUAL: Send update about 172.18.124.0 255.255.255.0. Reason: metric chg on topoi
d 0
DUAL: Send update about 172.18.124.0 255.255.255.0. Reason: new if on topoid 0
DUAL: dest(192.168.10.0 255.255.255.0) not active
DUAL: rcvupdate: 192.168.10.0 255.255.255.0 via 10.10.10.2 metric 131072/130816
on topoid 0
DUAL: Find FS for dest 192.168.10.0 255.255.255.0. FD is 4294967295, RD is 42949
67295 on topoid 0 found
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 192.168.10.0 ()
DUAL: RT installed 192.168.10.0 255.255.255.0 via 10.10.10.2
DUAL: Send update about 192.168.10.0 255.255.255.0. Reason: metric chg on topoi
d 0
DUAL: Send update about 192.168.10.0 255.255.255.0. Reason: new if on topoid 0
```

Vous pouvez également utiliser la commande **debug eigrp neighbor**. Ceci est le résultat de cette commande **debug** lorsque l'ASA Cisco a créé avec succès une nouvelle relation de voisinage avec R1.

```
ciscoasa# EIGRP-IPv4(Default-IP-Routing-Table:10): Callback: route_adjust Gigabi
tEthernet0/1
EIGRP: New peer 10.10.10.2
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 10.20.20.0 ()
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 172.18.124.0 ()
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 192.168.10.0 ()
```

Vous pouvez également utiliser les paquets debug EIGRP pour obtenir des informations détaillées sur l'échange de messages EIGRP entre Cisco ASA et ses homologues. Dans cet exemple, la clé d'authentification a été modifiée sur le routeur (R1) et le résultat du débogage vous montre que le problème est une non-correspondance d'authentification.

```
ciscoasa# EIGRP: Sending HELLO on GigabitEthernet0/1
AS 655362, Flags 0x0, Seq 0/0 interfaceQ 1/1 iidbQ un/rely 0/0
EIGRP: pkt key id = 1, authentication mismatch
EIGRP: GigabitEthernet0/1: ignored packet from 10.10.10.2, opcode = 5
```

```
(invalid authentication)
```

Le voisinage EIGRP descend avec Syslogs ASA-5-336010

ASA abandonne le voisinage EIGRP lorsque des modifications sont apportées à la liste de distribution EIGRP. Ce message Syslog est affiché.

```
EIGRP Nieghborship Resets with syslogs ASA-5-336010: EIGRP-IPv4: PDM(314 10:
Neighbor 10.15.0.30 (GigabitEthernet0/0) is down: route configuration changed
```

Avec cette configuration, chaque fois qu'une **nouvelle entrée de liste de contrôle d'accès est ajoutée** dans la liste de contrôle d'accès, le voisinage EIGRP **Eigrp-network-list** est réinitialisé.

```
router eigrp 10
distribute-list Eigrp-network-list in
network 10.10.10.0 255.0.0.0
passive-interface default
no passive-interface inside
redistribute static

access-list Eigrp-network-list standard permit any
```

Vous pouvez observer que la relation de voisinage est active avec le périphérique adjacent.

```
ciscoasa(config)# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.10.10.2 Gi0/3 10 00:01:22 1 5000 0 5

ciscoasa(config)# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.10.10.2 Gi0/3 13 00:01:29 1 5000 0 5
```

Vous pouvez maintenant ajouter **access-list Eigrp-network-list standard deny 172.18.24.0 255.255.255.0**.

```
%ASA-5-111010: User 'enable_15', running 'CLI' from IP 0.0.0.0, executed 'debug
eigrp fsm'
%ASA-7-111009: User 'enable_15' executed cmd: show access-list
%ASA-5-111008: User 'enable_15' executed the 'access-list Eigrp-network-list line
1 permit 172.18.24.0 255.255.255.0' command.
%ASA-5-111010: User 'enable_15', running 'CLI' from IP 0.0.0.0, executed 'access-list
Eigrp-network-list line 1 permit 172.18.24.0 255.255.255.0'
%ASA-7-111009: User 'enable_15' executed cmd: show eigrp neighbors
%ASA-5-336010: EIGRP-IPv4: PDM(599 10: Neighbor 10.10.10.2 (GigabitEthernet0/3) is
down: route configuration changed
%ASA-5-336010: EIGRP-IPv4: PDM(599 10: Neighbor 10.10.10.2 (GigabitEthernet0/3) is
up: new adjacency
```

Ces journaux sont visibles dans **debug eigrp fsm**.

```
IGRP2: linkdown: start - 10.10.10.2 via GigabitEthernet0/3
DUAL: Destination 10.10.10.0 255.255.255.0 for topoid 0
DUAL: linkdown: finish
```

Ce comportement est attendu dans toutes les nouvelles versions ASA de 8.4 et 8.6 à 9.1. Il en est de même pour les routeurs qui exécutent les trains de codes 12.4 à 15.1. Cependant, ce comportement n'est pas observé dans les versions 8.2 et antérieures du logiciel ASA, car les modifications apportées à une liste de contrôle d'accès ne réinitialisent pas les contiguïtés EIGRP.

Étant donné que le protocole EIGRP envoie la table topologique complète à un voisin lors de la première apparition du voisin, puis qu'il envoie uniquement les modifications, la configuration d'une liste de distribution avec le caractère événementiel du protocole EIGRP rendrait difficile l'application des modifications sans une réinitialisation complète de la relation de voisinage. Les routeurs doivent suivre chaque route envoyée et reçue d'un voisin afin de savoir quelle route a changé (c'est-à-dire, serait ou ne serait pas envoyée/acceptée) afin d'appliquer les modifications telles que dictées par la liste de distribution actuelle. Il est beaucoup plus facile de simplement démolir et rétablir la contiguïté entre voisins.

Lorsqu'une contiguïté est désactivée et rétablie, toutes les routes apprises entre des voisins particuliers sont simplement oubliées et la synchronisation complète entre les voisins est effectuée à nouveau - avec la nouvelle liste de distribution en place.

La plupart des techniques EIGRP que vous utilisez pour dépanner les routeurs Cisco IOS peuvent être appliquées sur Cisco ASA. Afin de dépanner EIGRP, utilisez le diagramme de flux principal de dépannage ; commencer à la case marquée **Main**.