Exemple de configuration ASA 9.x EIGRP

Contenu

Introduction

Ce document décrit comment configurer l'appliance de sécurité adaptable Cisco (ASA) afin d'apprendre des artères par le Protocole EIGPR (Enhanced Interior Gateway Routing Protocol), qui est prise en charge dans la version de logiciel 9.x ASA et plus tard, et exécuter l'authentification.

Conditions préalables

Exigences

Cisco exige que vous remplissez ces conditions avant que vous tentiez cette configuration :

- Cisco ASA doit exécuter la version 9.x ou ultérieures.
- L'EIGRP doit être en mode de contexte unique, parce qu'il n'est pas pris en charge en mode de multi-contexte.

Composants utilisés

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

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

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.

Informations générales

Instructions et limites

- Un exemple EIGRP est pris en charge dans le mode unique et par contexte dans à plusieurs modes de fonctionnement.
- Deux thread sont créés par contexte par exemple EIGRP dans à plusieurs modes de fonctionnement et peuvent être visualisés avec le processus d'exposition.
- Le résumé automatique est désactivé par défaut.
- Des relations voisines ne sont pas établies entre les unités de batterie dans le mode d'interface individuelle.
- Le default-information dedans [<acl>] est utilisé afin de filtrer le bit extérieur dans des default route entrants de candidat.
- Le default-information [<acl>] est utilisé afin de filtrer le bit extérieur dans des default route sortants de candidat.

EIGRP et Basculement

La version 8.4.4.1 de code de Cisco ASA et synchronise plus tard les artères dynamiques à partir de l'unité D'ACTIVE à l'équipement de réserve. En outre, la suppression des artères est également synchronisée à l'équipement de réserve. Cependant, l'état de contiguïtés de pair n'est pas synchronisé ; seulement le périphérique ACTIF met à jour l'état de voisinage et participe activement au routage dynamique. Référez-vous à la Foire aux questions ASA : Que se produit après Basculement si des artères dynamiques sont synchronisées ? pour plus d'informations.

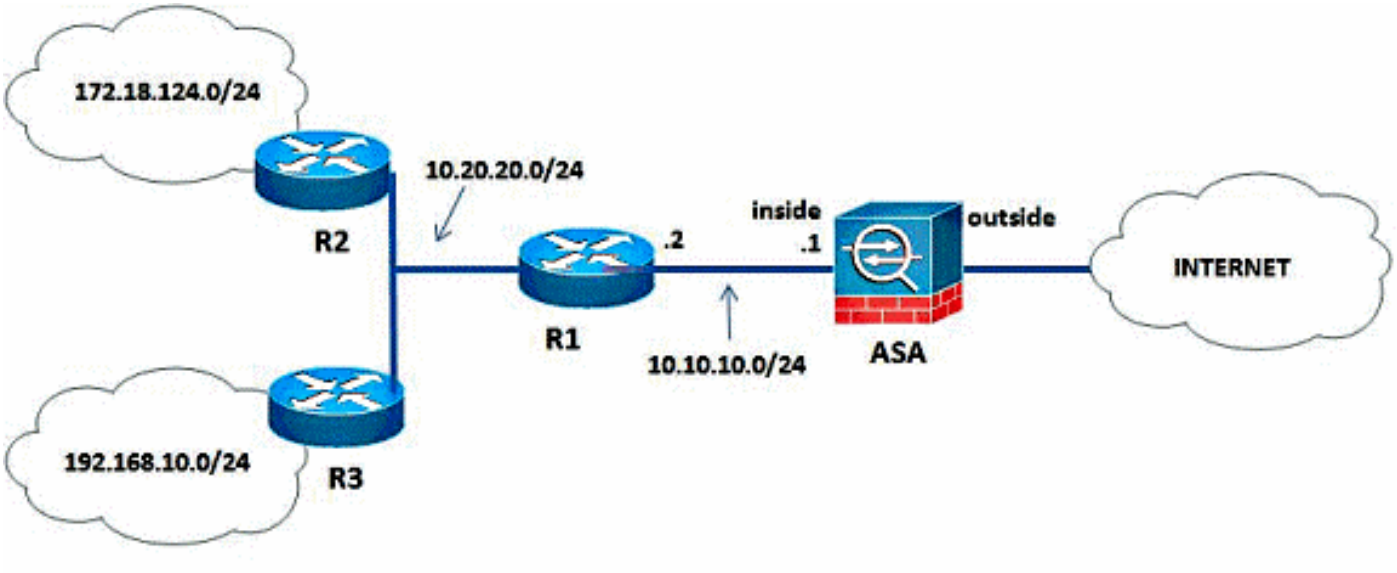
Configurer

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

Note: 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 :



En topologie du réseau qui est illustrée, l'adresse IP d'interface interne de Cisco ASA est 10.10.10.1/24. Le but est de configurer l'EIGRP sur Cisco ASA afin d'apprendre des artères aux réseaux internes (10.20.20.0/24, 172.18.124.0/24, et 192.168.10.0/24) dynamiquement par le routeur contigu (R1). R1 apprend les artères aux réseaux internes distants par les deux autres Routeurs (R2 et R3).

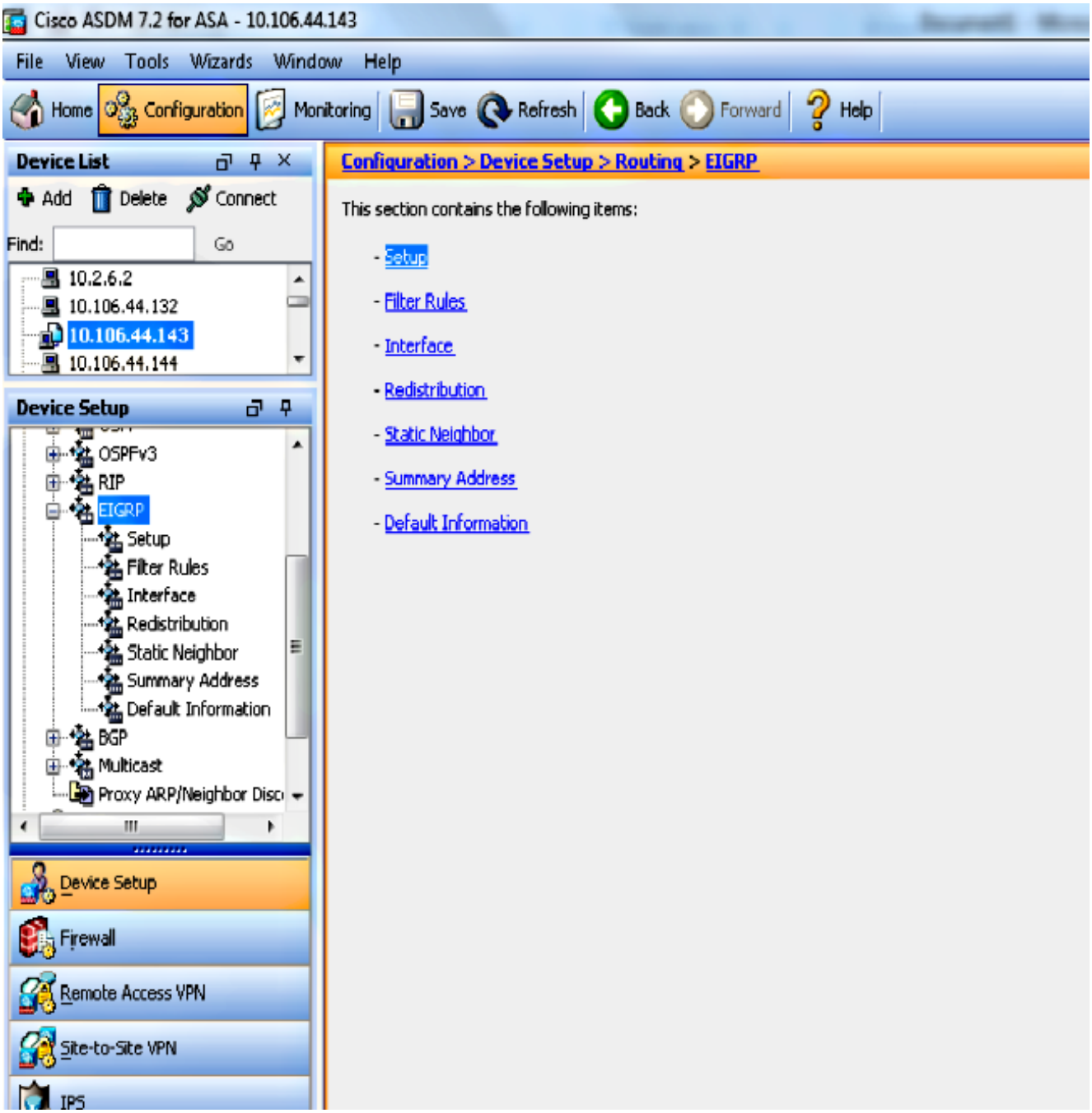
Configuration ASDM

L'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 afin de configurer, surveiller, et gérer le périphérique. Vous pouvez également utiliser le lanceur ASDM afin de lancer l'application ASDM plus rapide que l'applet Java. Cette section décrit les informations que vous devez afin de configurer les caractéristiques décrites dans ce document avec l'ASDM.

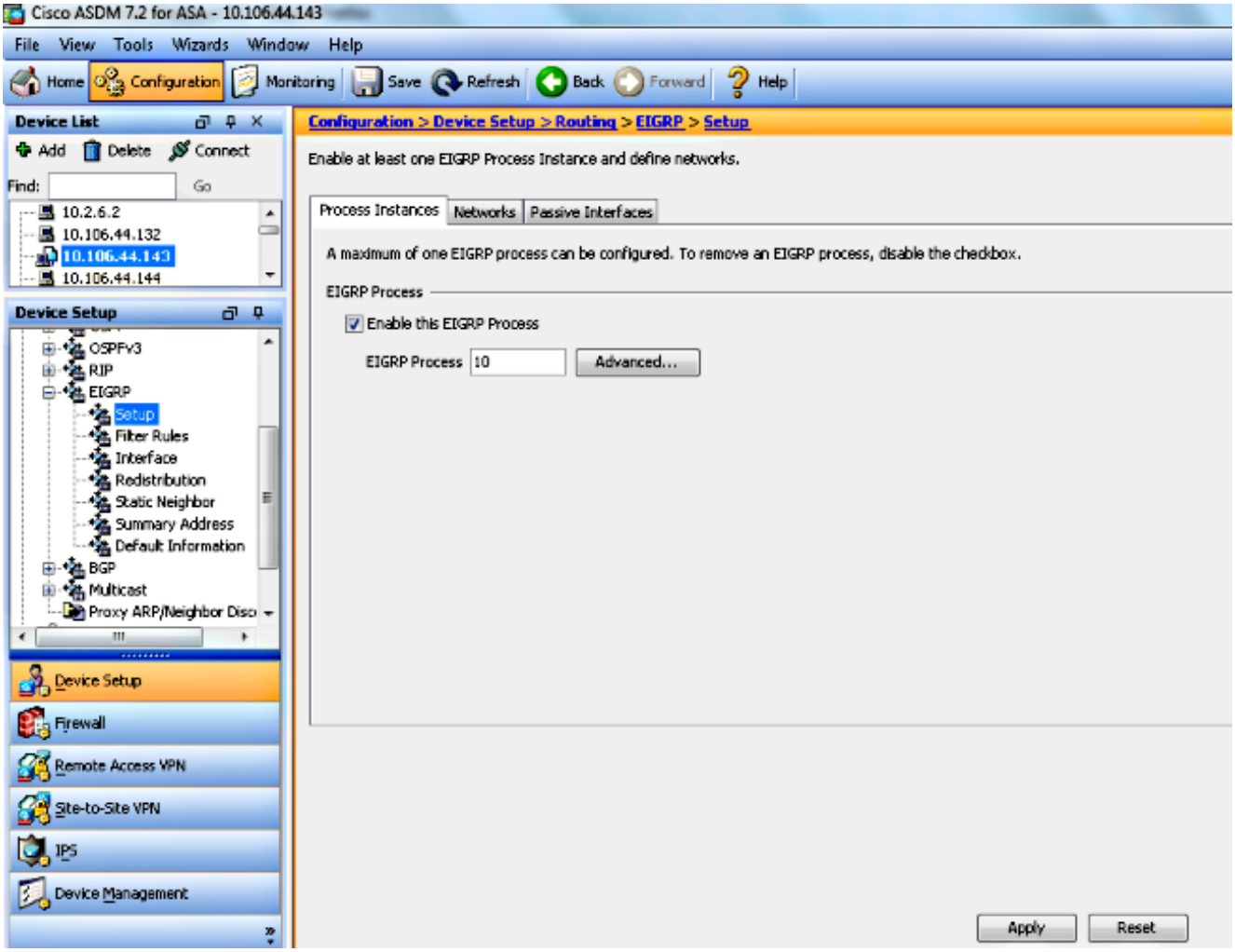
Terminez-vous ces étapes afin de configurer l'EIGRP à Cisco ASA.

1. Procédure de connexion à Cisco ASA avec l'ASDM.

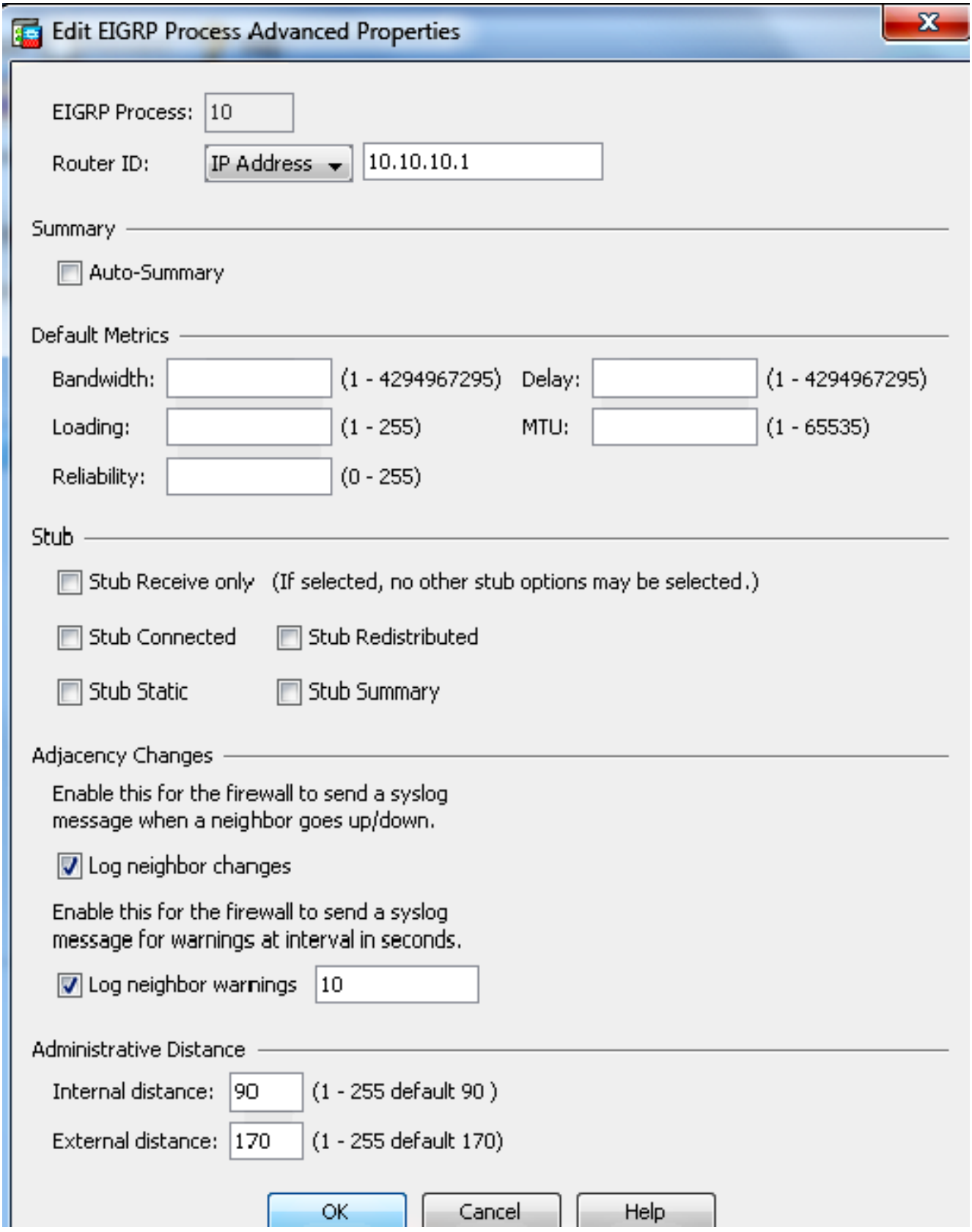
2. Naviguez vers la **configuration > l'installation de périphérique > le routage > la** zone **EIGRP de l'**interface ASDM, suivant les indications de ce tir d'écran.



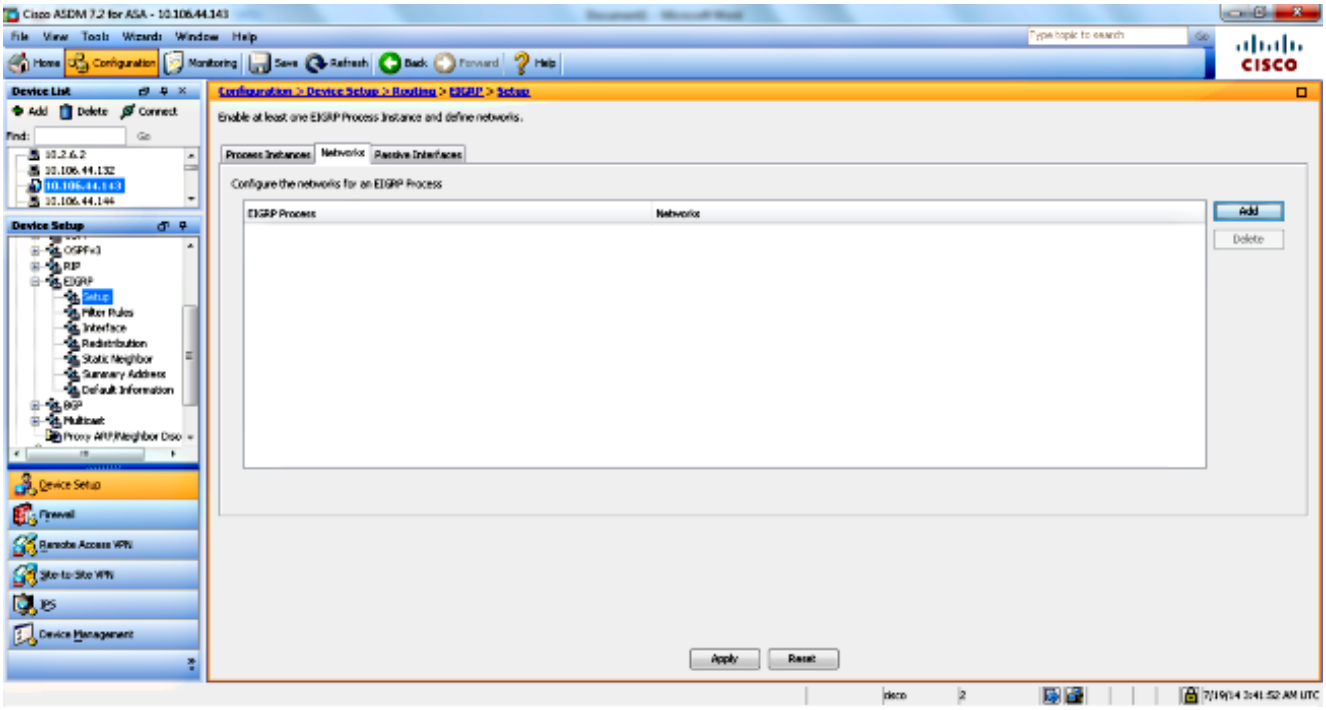
3. Activez le processus de routage EIGRP sur l'onglet d'**exemples d'installation > de processus**, suivant les indications de ce tir d'écran. Dans cet exemple, le processus EIGRP est **10.**



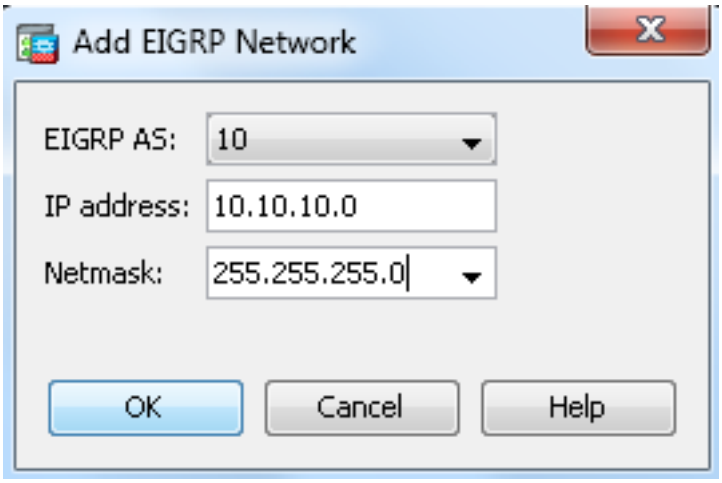
4. Vous pouvez configurer des paramètres de processus avancés facultatifs de routage EIGRP. Cliquez sur **avancé** sur l'onglet d'**exemples d'installation > de processus**. Vous pouvez configurer le processus de routage EIGRP pendant qu'un processus de routage de stub, désactivent le résumé du routage automatique, définissent les mesures par défaut pour les artères redistribuées, changent les distances administratives pour interne et des routes EIGRP externes, configurez un ID de routeur statique, et activez ou désactivez se connecter des modifications de contiguïté. Dans cet exemple, l'ID de routeur EIGRP est statiquement configuré avec l'adresse IP de l'interface interne (10.10.10.1). Supplémentaire, le **résumé automatique** est également désactivé. Toutes autres options sont configurées avec leurs valeurs par défaut.



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



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



Se connecte par interface seulement à une adresse IP que les chutes dans les réseaux définis participent au processus de routage EIGRP. Si vous avez une interface que vous ne voulez pas participer au routage EIGRP mais cela est relié à un réseau que vous voulez annoncé, configurez une entrée de réseau sur l'onglet d'**installation > de réseaux** qui couvre le réseau auquel l'interface est reliée, et configurer alors cette interface comme interface passive de sorte que l'interface ne puisse pas envoyer ou recevoir des mises à jour EIGRP.

Note: Les interfaces configurées comme passif n'envoient pas ou reçoivent des mises à jour EIGRP.

7. Vous pouvez sur option définir des filtres d'artère sur le volet de règles de filtrage. Le filtrage d'artère fournit plus de contrôle des artères qui sont permises pour être envoyées ou reçues dans les mises à jour EIGRP.

8. Vous pouvez sur option configurer la redistribution de routage. Cisco ASA peut redistribuer

des artères découvertes par Protocole RIP (Routing Information Protocol) et Protocole OSPF (Open Shortest Path First) dans le processus de routage EIGRP. Vous pouvez également redistribuer la charge statique et les routes connectées dans le processus de routage EIGRP. Vous n'avez pas besoin de redistribuer la charge statique ou les routes connectées si elles font partie de la marge d'un réseau configuré sur l'**installation > les réseaux** tableau définissent la redistribution de routage sur le volet de redistribution.

9. Des paquets HELLO EIGRP sont envoyés comme paquets de multidiffusion. Si un voisin EIGRP se trouve à travers un réseau de non-diffusion, vous devez manuellement définir ce voisin. Quand vous définissez manuellement un voisin EIGRP, bonjour des paquets sont envoyés à ce voisin comme messages d'unicast. Afin de définir les voisins statiques EIGRP, allez au volet **voisin statique**.

10. Par défaut, des default route sont envoyés et reçus. Afin de limiter ou désactiver l'envoi et la réception des informations de routage par défaut, ouvrez la **configuration > l'installation de périphérique > le routage > l'EIGRP > le** volet des **informations par défaut**. Le volet des informations par défaut affiche une table des règles de contrôler l'envoi et la réception des informations de routage par défaut dans les mises à jour EIGRP.

    Note: Vous pouvez faire ordonner un « *dans »* et on « » pour chaque processus de routage EIGRP. (Seulement un processus est actuellement pris en charge.)

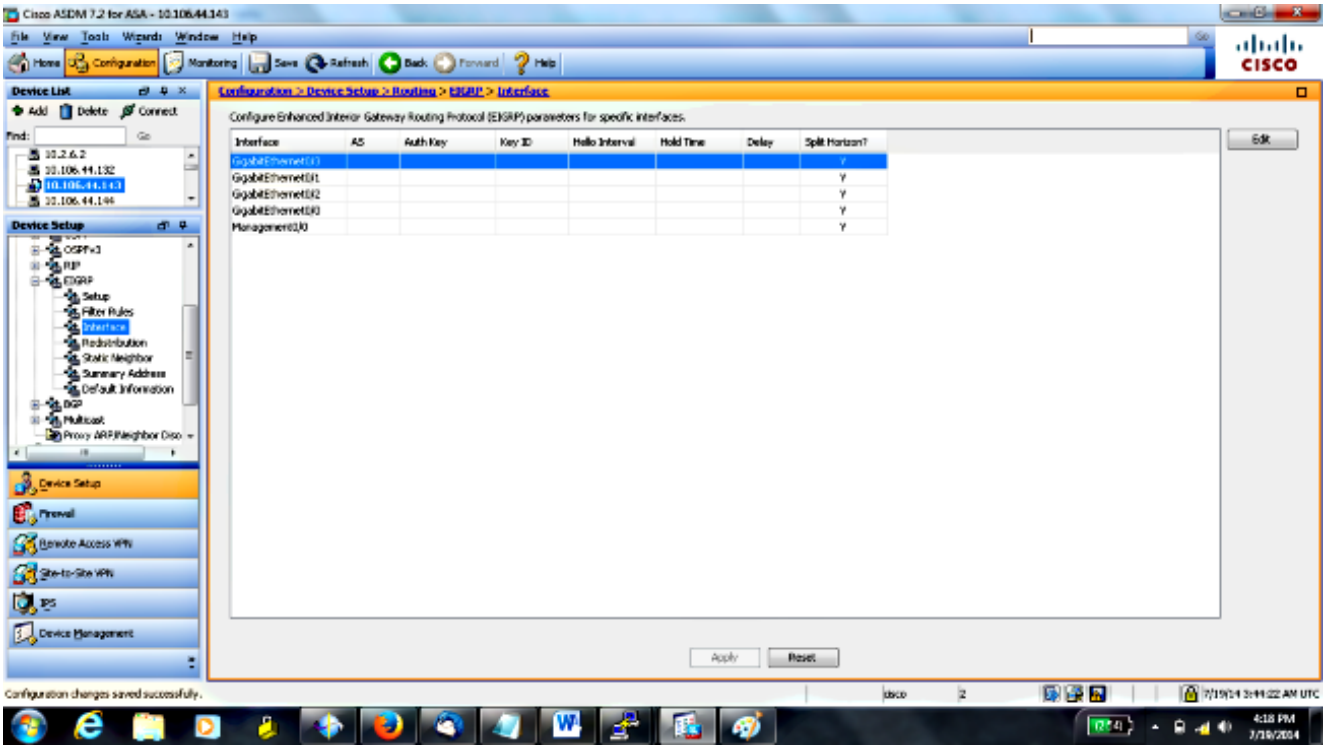
Configurez l'authentification EIGRP

Cisco ASA prend en charge l'authentification de MD5 des mises à jour de routage du protocole de routage EIGRP. Le condensé MD5-keyed dans chaque paquet EIGRP empêche l'introduction des messages non autorisés ou faux de routage des sources inapprouvées. L'ajout de l'authentification à vos messages EIGRP 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 quelqu'un 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 EIGRP envoyés entre vos périphériques de routage (qui inclut l'ASA), elle empêche les ajouts non autorisés des Routeurs EIGRP dans votre topologie de routage.

L'authentification d'artère EIGRP est par interface configuré. Tous les voisins EIGRP sur des interfaces configurées pour l'authentification de message EIGRP doivent être configurés avec la mêmes authentication mode et clé pour que des contiguïtés soient établies.

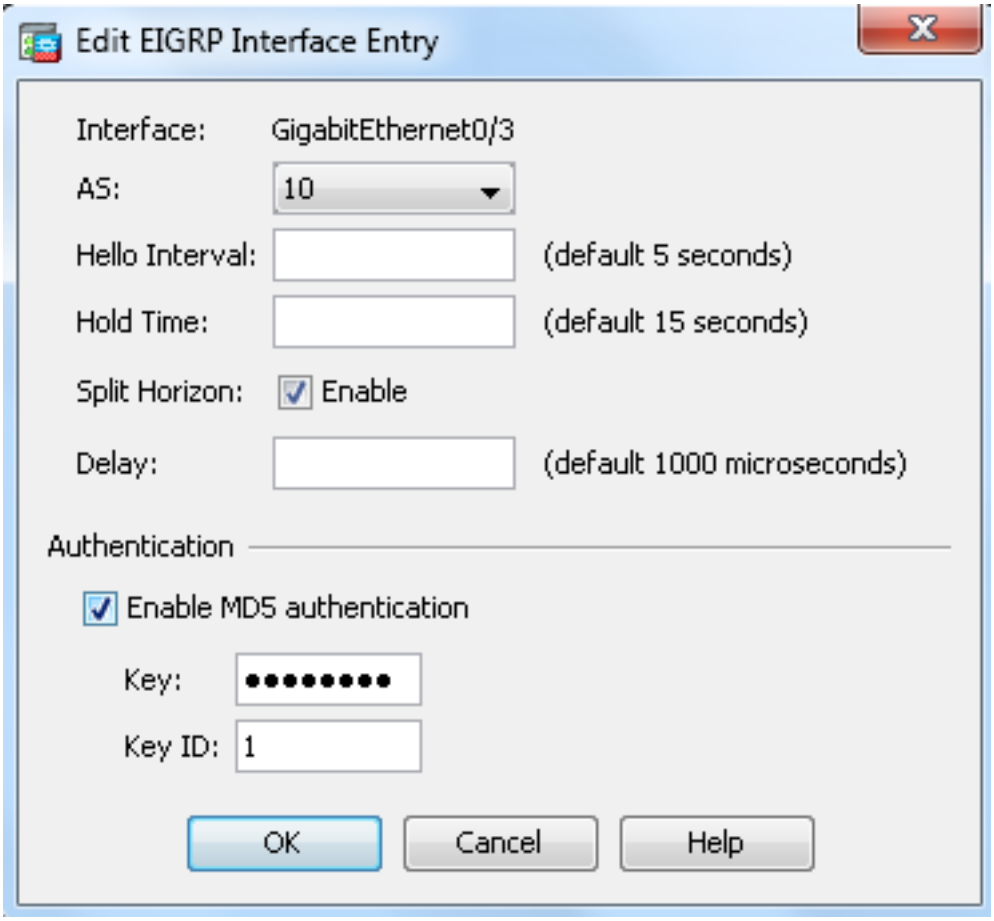
Terminez-vous ces étapes afin d'activer l'authentification MD5 EIGRP sur Cisco ASA.

1. Sur l'ASDM, naviguez vers la **configuration > l'installation de périphérique > le routage > l'EIGRP > l'interface** comme affichée.



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

3. Sous l'authentification, choisissez Enable l'**authentification de MD5**. Ajoutez plus d'informations sur les paramètres d'authentification ici. Dans ce cas, la clé pré-partagée est **cisco123**, et l'ID de clé est **1.**



Filtrage d'artère EIGRP

Avec l'EIGRP, vous pouvez contrôler les mises à jour de routage qui sont envoyées et reçues. Dans cet exemple, vous bloquerez des mises à jour de routage sur l'ASA pour le préfixe réseau 192.168.10.0/24, qui est derrière R1. Pour artère-filtrer, vous pouvez seulement utiliser l'**ACL 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
```

Vérifiez

```
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 de Cisco ASA CLI

C'est la configuration de Cisco ASA CLI.

```
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
```

Configuration CLI du routeur Cisco IOS (R1)

C'est la configuration CLI de R1 (routeur interne).

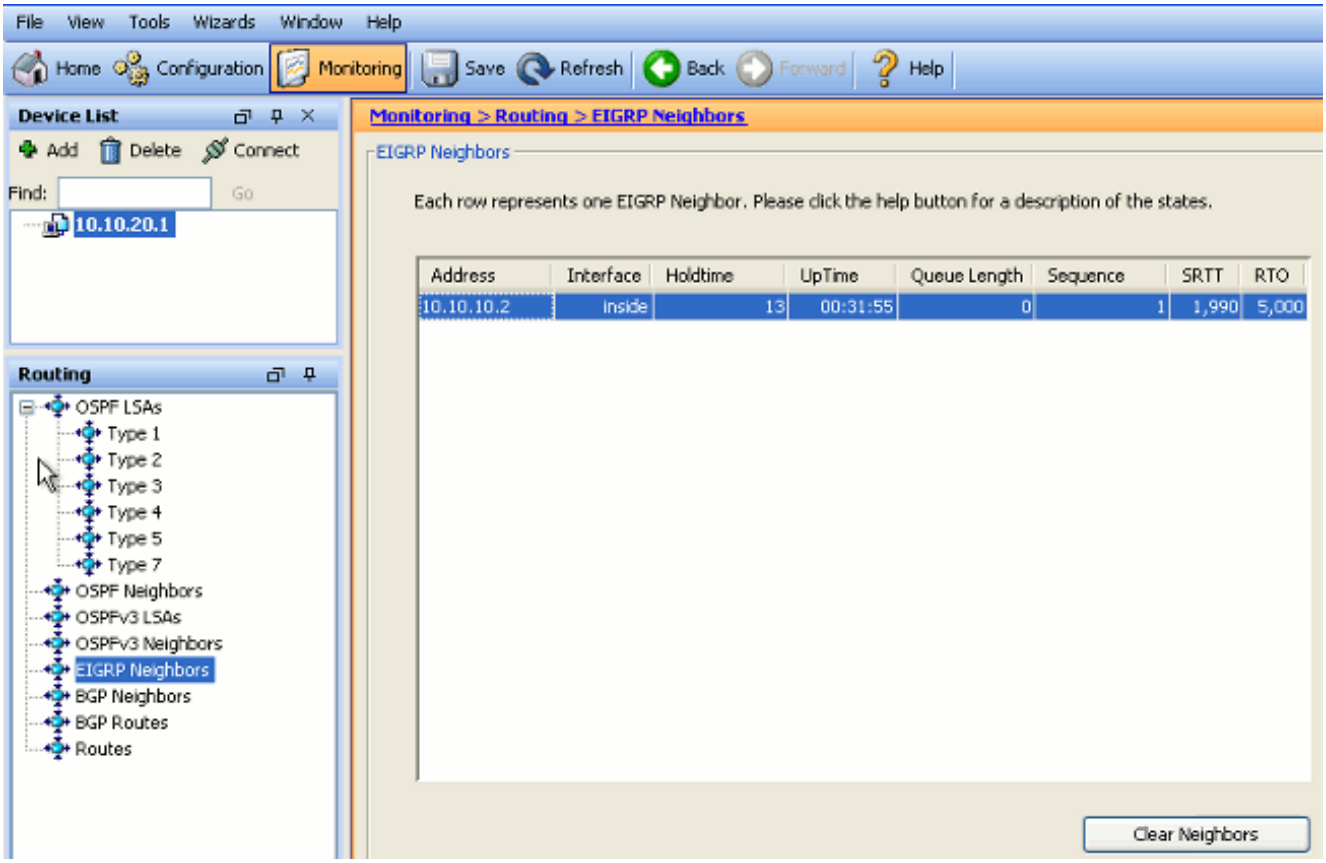
```
ASA(config)# show access-list eigrp
access-list eigrp; 2 elements; name hash: 0xd43d3adc
access-list eigrp line 1 standard deny 192.168.10.0 255.255.255.0 (hitcnt=3) 0xeb48ecd0
access-list eigrp line 2 standard permit any4 (hitcnt=12) 0x883fe5ac
```

Vérifiez

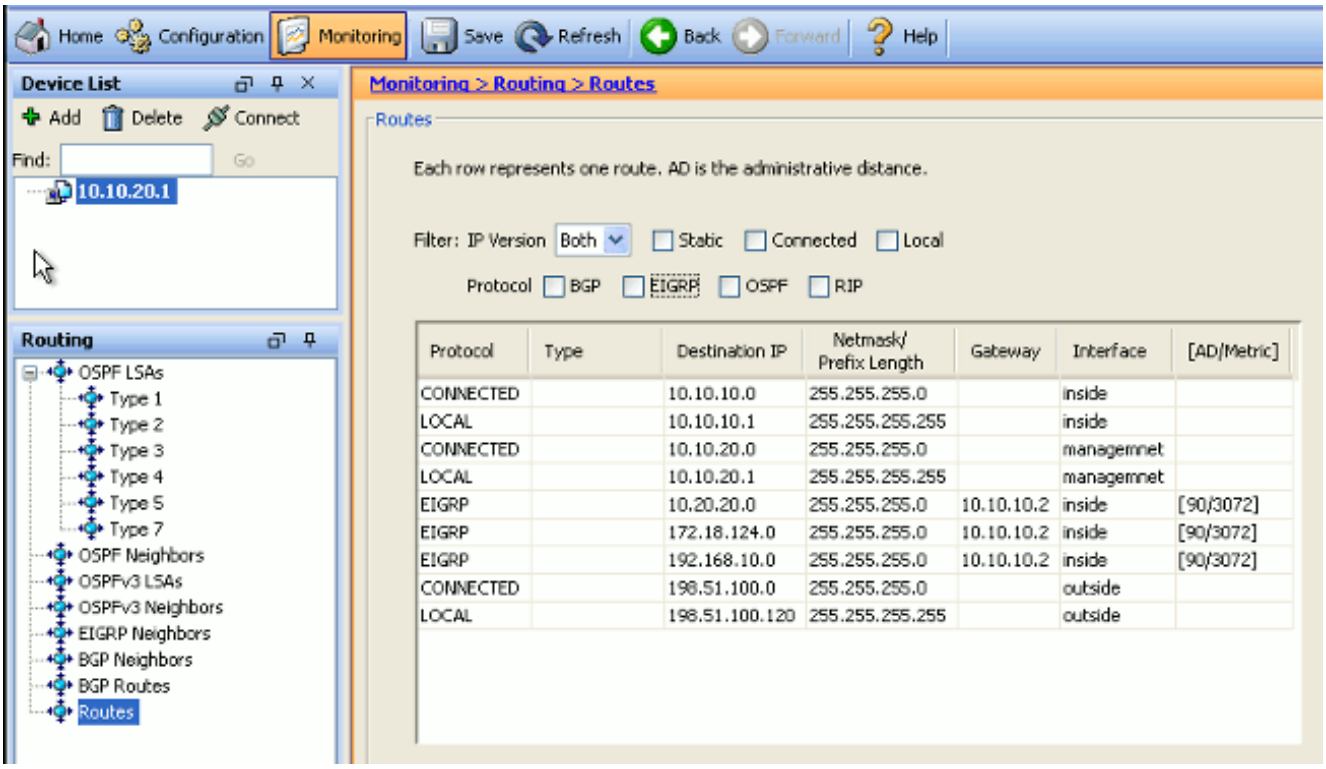
Terminez-vous ces étapes afin de vérifier votre configuration.

1. Sur l'ASDM, vous pouvez naviguer vers la **surveillance > routage > voisin EIGRP** afin de voir chacun des voisins EIGRP. Ce tir d'écran affiche le routeur interne (R1) en tant que voisin actif. Vous pouvez également voir l'interface où ce voisin réside, le holdtime, et en hausse

combien de temps les relations voisines ont été (disponibilité).



2. Supplémentaire, 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 **192.168.10.0/24, 172.18.124.0/24**, et **10.20.20.0/24** réseaux sont appris par R1 (**10.10.10.2**).



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 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 la version 9.2.1 et ultérieures ASA, vous pouvez employer la commande d'**eigrp de show route** afin d'afficher seulement des artères 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 employer la commande de **show eigrp topology** afin d'obtenir des informations sur les réseaux instruits 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. L'ordre de **show eigrp neighbors** est également utile afin de vérifier les voisins actifs et les informations correspondantes. Cet exemple affiche les mêmes informations que vous avez obtenues de l'ASDM dans 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 l'écoulement de paquet.

1. L'ASA monte sur le lien et envoie un paquet de mCast bonjour par toutes ses interfaces EIGRP-configurées.

2. R1 reçoit bonjour un paquet et envoie un paquet de mCast bonjour.

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 bonjour le paquet et envoie un paquet de mise à jour avec un premier positionnement de bit, qui indique que c'est le processus d'initialisation.

4. R1 reçoit un paquet de mise à jour et envoie un paquet de mise à jour avec un premier positionnement de bit, qui indique que c'est le processus d'initialisation.

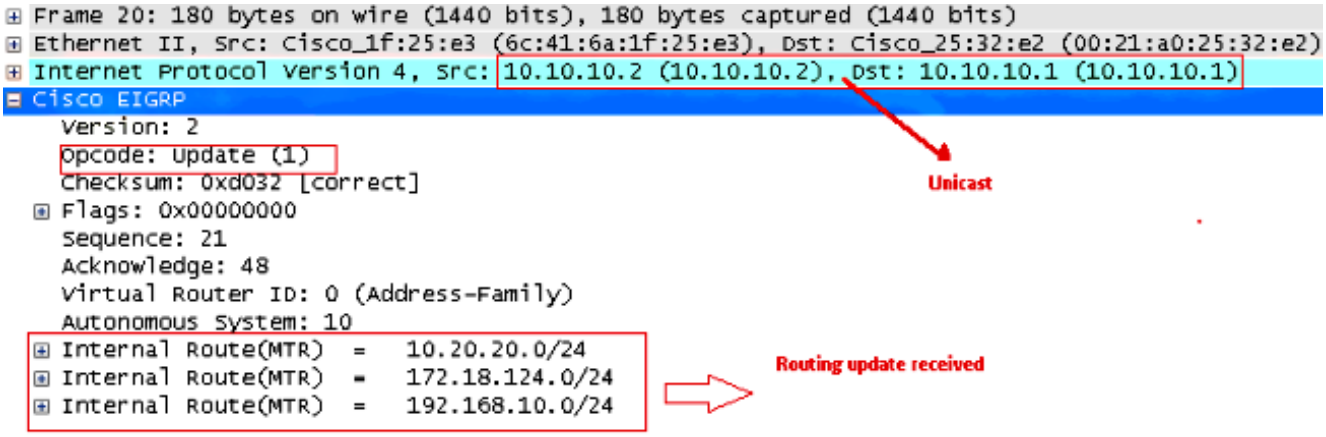
```
⊞ Frame 15: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
⊞ Ethernet II, Src: Cisco_25:32:e2 (00:21:a0:25:32:e2), Dst: Cisco_1f:25:e3 (6c:41:6a:1f:25:e3)
⊞ Internet Protocol Version 4, Src: 10.10.10.1 (10.10.10.1), Dst: 10.10.10.2 (10.10.10.2)
⊟ Cisco EIGRP
    Version: 2
    Opcode: 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. Après l'ASA et R1 ont permuté des hellos et la contiguïté de voisinage est établie, ASA et la réponse R1 avec un paquet ACK, qui indique que l'information de mise à jour a été reçue.

6. L'ASA envoie ses informations de routage à R1 dans un paquet de mise à jour.

7. R1 insère les informations de paquet de mise à jour dans sa table de topologie. La table de topologie inclut toutes les destinations annoncées par des voisins. Il est organisé de sorte que chaque destination soit répertoriée, avec tous les voisins qui peuvent voyager à la destination et à leurs mesures associées.

8. R1 envoie alors un paquet de mise à jour à l'ASA.



9. Une fois qu'il reçoit le paquet de mise à jour, l'ASA envoie un paquet ACK à R1. Après que l'ASA et les R1 reçoivent avec succès les paquets de mise à jour entre eux, elles sont prêtes ont choisi les artères de successeur (meilleur) et de successeur potentiel (sauvegarde) dans la table de topologie, et offrent les routes successeur à la table de routage.

Dépanner

Cette section inclut des informations sur **mettent au point** et les **commandes show** qui peuvent être utiles afin de dépanner des 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 mettez au point les informations la DOUBLE) machine à état défini de Diffusing Update Algorithm (, utilisent la commande de **debug eigrp fsm** dans le mode d'exécution privilégié. Cette commande vous permet d'observer l'activité de successeur potentiel EIGRP et de déterminer si des mises à jour de route sont installées et supprimées par le processus de routage.

C'est la sortie de la commande de **débogage** dans scruter réussi avec R1. Vous pouvez voir

chacune des routes différentes qui est avec succès installé sur le système.

```
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
```

Vous pouvez également utiliser l'ordre de **debug eigrp neighbor**. C'est la sortie de cette commande de **débogage** quand Cisco ASA a avec succès créé une nouvelle relation voisine 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 debugs eigrp packets pour les informations détaillées d'échange de message EIGRP entre Cisco ASA et ses pairs. Dans cet exemple, la clé d'authentification a été changée sur le routeur (R1), et la sortie de débogage te prouve que le problème est une non-concordance 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)
```

La proximité EIGRP est vers le bas assortie aux Syslog ASA-5-336010

L'ASA relâche la proximité EIGRP quand tous les changements de la liste de distribution EIGRP sont faits. Ce message de Syslog est vu.

```
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)
```

Avec cette configuration, toutes les fois qu'un **nouveau rubrique de liste ACL est ajouté** dans l'ACL, la proximité de l'Eigrp-réseau-**liste** EIGRP est remise à l'état initial.

```
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)
```

Vous pouvez observer que les relations voisines sont en hausse avec le périphérique contigu.

```
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
```

Maintenant vous pouvez ajouter la **norme d'Eigrp-réseau-liste de liste d'accès refusez 172.18.24.0 255.255.255.0**.

```
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
```

Ces logs peuvent être vus dans le **debug eigrp fsm**.

```
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
```

C'est comportement prévu dans toutes les nouvelles versions ASA de 8.4 et 8.6 à 9.1. Le même a été observé dans des Routeurs qui exécutent les 12.4 à 15.1 séries de code. Cependant, on n'observe pas ce comportement dans des versions de logiciel de la version 8.2 et antérieures ASA ASA parce que les modifications apportées à un ACL ne remettent pas à l'état initial les contiguïtés EIGRP.

Puisque l'EIGRP envoie la pleine table de topologie à un voisin quand le voisin monte d'abord, et puis il envoie seulement les modifications, configurer une liste de distribution avec la nature entraînée par les événements de l'EIGRP le rendrait difficile pour que les modifications s'appliquent sans pleine remise des relations voisines. Les Routeurs devraient maintenir chaque artère envoyée à et reçue d'un voisin afin de connaître quelle artère a changé (c'est-à-dire, ou ne serait pas envoyé/a été reçu) afin d'appliquer les modifications comme dicté par le courant distribuez la liste. Il est beaucoup plus facile de démolir simplement et rétablir la contiguïté entre les voisins.

Quand une contiguïté est démolie et rétablie, toutes les routes apprises entre les voisins particuliers sont simplement oubliées et la synchronisation entière entre les voisins est exécutée à nouveau - avec le nouveau distribuez la liste en place.

La plupart des techniques EIGRP que vous employez afin de dépanner des routeurs Cisco IOS peuvent être appliquées sur Cisco ASA. Afin de dépanner l'EIGRP, utilisez l'organigramme principal de dépannage ; début à la **canalisation** marquée de case.