Configurer l'ASA pour les liaisons ISP redondantes ou de secours

Contenu

Introduction

Ce document décrit comment configurer le dispositif de sécurité adaptatif (ASA) de la gamme Cisco ASA 5500 pour l'utilisation de la fonctionnalité de suivi de route statique afin de permettre au périphérique d'utiliser des connexions Internet redondantes ou de sauvegarde.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

- Gamme Cisco ASA 5555-X qui exécute le logiciel version 9.x ou ultérieure
- Cisco ASDM version 7.x ou 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

Vous pouvez également utiliser cette configuration avec la gamme Cisco ASA 5500 version 9.1(5).

> **Note**: La commande **backup interface** est requise pour configurer la quatrième interface sur la gamme ASA 5505. Pour plus d'informations, reportez-vous à la section backup interface du *Guide de référence des commandes de Cisco Security Appliance, version 7.2*.

Informations générales

Cette section présente la fonctionnalité de suivi de route statique décrite dans ce document, ainsi que quelques recommandations importantes avant de commencer.

Présentation de la fonctionnalité de suivi de route statique

L'un des problèmes liés à l'utilisation de routes statiques est qu'il n'existe aucun mécanisme inhérent permettant de déterminer si la route est active ou inactive. La route reste dans la table de routage même si le saut de passerelle suivant devient indisponible. Les routes statiques sont retirées de la table de routage seulement si l'interface associée sur le dispositif de sécurité devient inactive. Afin de résoudre ce problème, une fonctionnalité de suivi de route statique est utilisée afin de suivre la disponibilité d'une route statique. La fonctionnalité supprime la route statique de la table de routage et la remplace par une route de secours en cas de défaillance.

Le suivi de route statique permet à l'ASA d'utiliser une connexion peu coûteuse à un FAI secondaire en cas d'indisponibilité de la ligne louée principale. Afin d'atteindre cette redondance, l'ASA associe une route statique à une cible de surveillance que vous définissez. L'opération SLA (Service Level Agreement) surveille la cible avec des requêtes d'écho ICMP périodiques. Si aucune réponse d'écho n'est reçue, l'objet est considéré comme désactivé et la route associée est supprimée de la table de routage. Une route de secours précédemment configurée est utilisée au lieu de la route qui est retirée. Pendant que la route de secours est utilisée, l'opération de surveillance SLA poursuit ses tentatives d'atteindre la cible de surveillance. Une fois que la cible est de nouveau disponible, la première route est substituée dans la table de routage, et la route de secours est retirée.

Dans l'exemple utilisé dans ce document, l'ASA gère deux connexions à Internet. La première connexion est une ligne louée à grande vitesse qui est accessible via un routeur fourni par l'ISP primaire. La deuxième connexion est une ligne DSL (Digital Subscriber Line) à plus faible débit accessible via un modem DSL fourni par le FAI secondaire.

> **Note**: La configuration décrite dans ce document ne peut pas être utilisée pour l'équilibrage de charge ou le partage de charge, car elle n'est pas prise en charge sur l'ASA. Utilisez cette configuration à des fins de redondance ou de secours seulement. Le trafic sortant utilise le FAI principal, puis le FAI secondaire en cas de défaillance du routeur principal. La panne de l'ISP primaire entraîne une interruption provisoire du trafic.

La connexion DSL est inactive tant que la ligne louée est en activité et que la passerelle de l'ISP primaire est accessible. Cependant, si la connexion au FAI principal est interrompue, l'ASA modifie la table de routage afin de diriger le trafic vers la connexion DSL. Le suivi de route statique est utilisé afin d'atteindre cette redondance.

L'ASA est configuré avec une route statique qui dirige tout le trafic Internet vers le FAI principal. Toutes les dix secondes, le processus de surveillance SLA vérifie que la passerelle principale du FAI est accessible. Si le processus de surveillance SLA détermine que la passerelle de l'ISP primaire n'est pas accessible, la route statique qui dirige le trafic vers cette interface est retirée de la table de routage. Afin de substituer cette route statique, une route statique alternative qui dirige le trafic vers l'ISP secondaire est installée. Cette route statique alternative dirige le trafic vers l'ISP secondaire via le modem DSL jusqu'à ce que la liaison avec l'ISP primaire soit accessible.

Cette configuration fournit un moyen relativement peu coûteux de s'assurer que l'accès Internet sortant reste disponible pour les utilisateurs derrière l'ASA. Comme décrit dans ce document, cette configuration peut ne pas convenir pour l'accès entrant aux ressources derrière l'ASA. Des compétences avancées en matière de réseau sont nécessaires pour établir des connexions entrantes transparentes. Ces qualifications ne sont pas couvertes dans ce document.

Recommandations importantes

Avant de tenter la configuration décrite dans ce document, vous devez choisir une cible de surveillance capable de répondre aux requêtes d'écho ICMP (Internet Control Message Protocol). La cible peut être n'importe quel objet réseau que vous choisissez, mais une cible étroitement liée à votre connexion de fournisseur d'accès à Internet (FAI) est recommandée. Voici quelques cibles de surveillance possibles :

- L'adresse de la passerelle ISP
- Une autre adresse gérée par l'ISP
- Un serveur sur un autre réseau, tel qu'un serveur AAA (Authentication, Authorization, and Accounting) avec lequel l'ASA doit communiquer
- Un objet de réseau persistant sur un autre réseau (un ordinateur de bureau ou portable que vous pouvez arrêter la nuit n'est pas un bon choix)

Ce document suppose que l'ASA est entièrement opérationnel et configuré afin de permettre à Cisco Adaptive Security Device Manager (ASDM) d'apporter des modifications de configuration.

Astuce : Pour plus d'informations sur la façon d'autoriser l'ASDM à configurer le périphérique, référez-vous à la section Configuration de l'accès HTTPS pour l'ASDM du *manuel CLI 1 : Guide de configuration de l'interface de ligne de commande des opérations générales de la gamme Cisco ASA, 9.1*.

Configuration

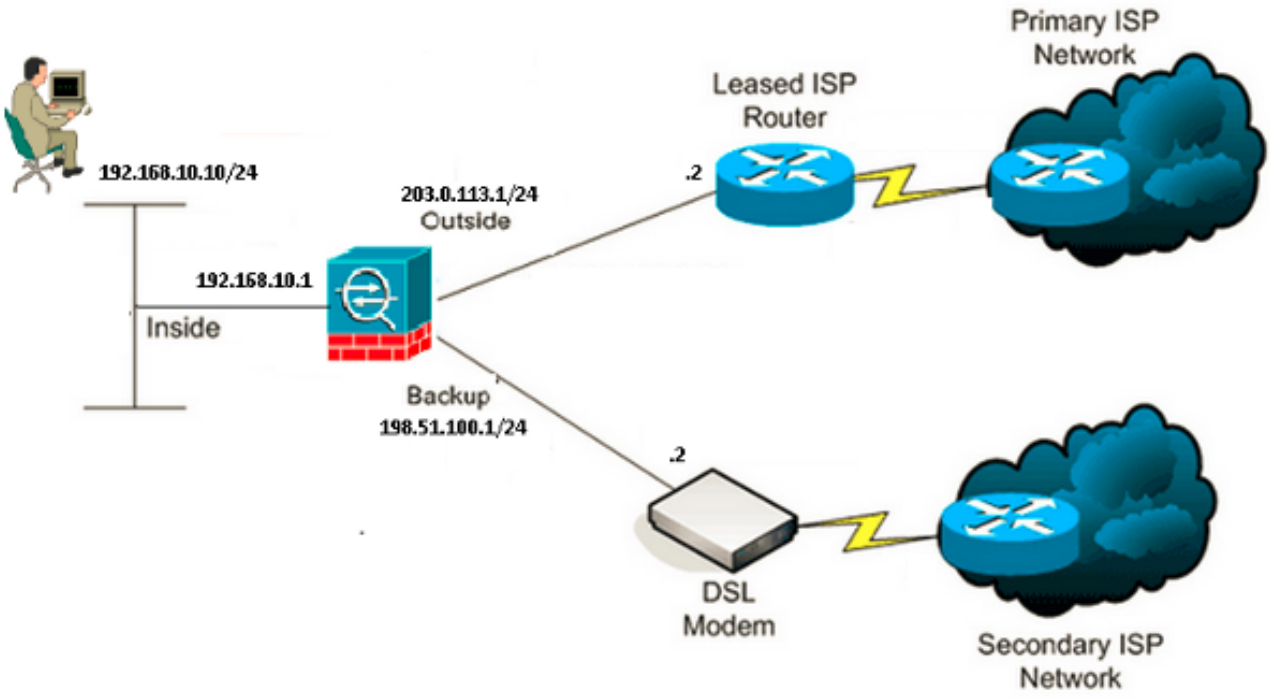
Utilisez les informations décrites dans cette section afin de configurer l'ASA pour l'utilisation de la fonctionnalité de suivi de route statique.

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

Note: Les adresses IP utilisées dans cette configuration ne sont pas routables légalement sur Internet. Il s'agit d'adresses RFC 1918, utilisées dans un environnement de travaux pratiques.

Diagramme du réseau

L'exemple fourni dans cette section utilise cette configuration réseau :



Configuration CLI

Utilisez ces informations afin de configurer l'ASA via la CLI :

```
ASA# show running-config

ASA Version 9.1(5)
!
hostname ASA
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 203.0.113.1 255.255.255.0
!
interface GigabitEthernet0/2
 nameif backup
 security-level 0
 ip address 198.51.100.1 255.255.255.0

!--- The interface attached to the Secondary ISP.
!--- "backup" was chosen here, but any name can be assigned.

!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 no nameif
 no security-level
 no ip address
!
boot system disk0:/asa915-smp-k8.bin
ftp mode passive
clock timezone IND 5 30
object network Inside_Network
 subnet 192.168.10.0 255.255.255.0
object network inside_network
 subnet 192.168.10.0 255.255.255.0
pager lines 24
logging enable
mtu inside 1500
mtu outside 1500
mtu backup 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
```

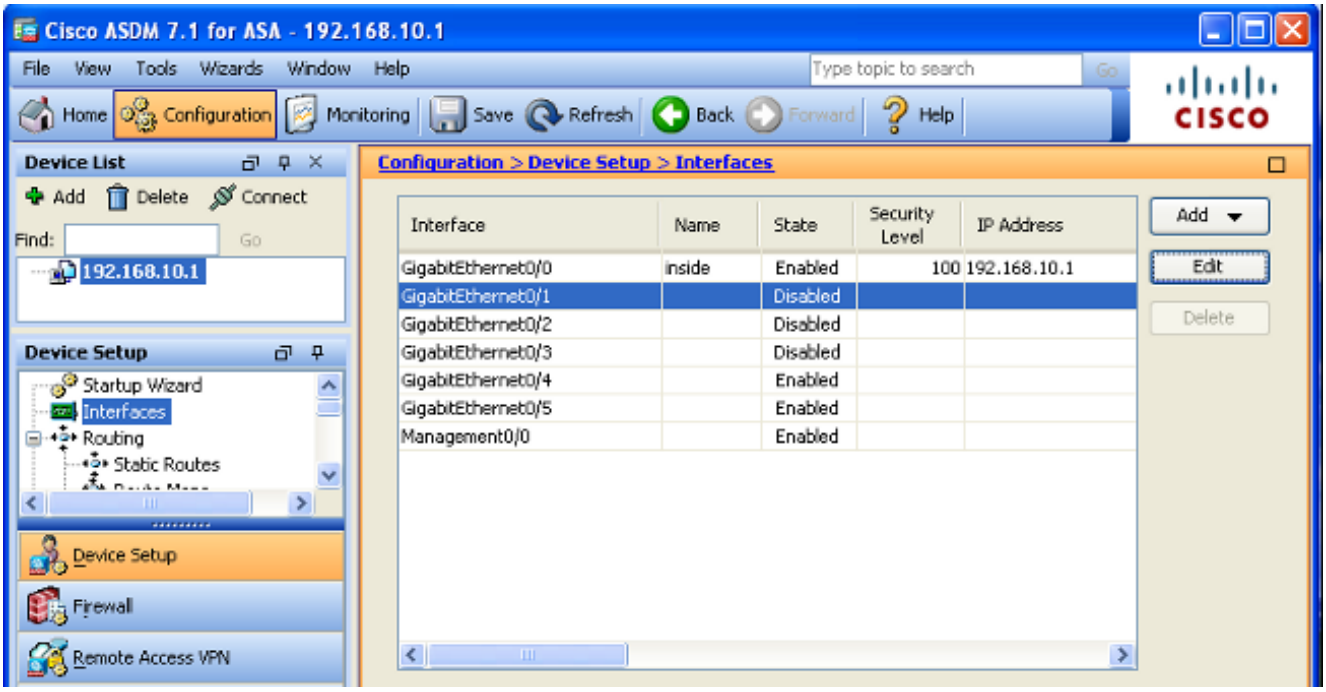
```
no arp permit-nonconnected
!
object network Inside_Network
 nat (inside,outside) dynamic interface
object network inside_network
 nat (inside,backup) dynamic interface

!--- NAT Configuration for Outside and Backup

route outside 0.0.0.0 0.0.0.0 203.0.113.2 1 track 1

!--- Enter this command in order to track a static route.
!--- This is the static route to be installed in the routing
!--- table while the tracked object is reachable.  The value after
!--- the keyword "track" is a tracking ID you specify.

route backup 0.0.0.0 0.0.0.0 198.51.100.2 254

!--- Define the backup route to use when the tracked object is unavailable.
!--- The administrative distance of the backup route must be greater than
!--- the administrative distance of the tracked route.
!--- If the primary gateway is unreachable, that route is removed
!--- and the backup route is installed in the routing table
!--- instead of the tracked route.

timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00

sla monitor 123
 type echo protocol ipIcmpEcho 4.2.2.2 interface outside
 num-packets 3
 frequency 10

!--- Configure a new monitoring process with the ID 123.  Specify the
!--- monitoring protocol and the target network object whose availability the tracking
!--- process monitors.  Specify the number of packets to be sent with each poll.
!--- Specify the rate at which the monitor process repeats (in seconds).

sla monitor schedule 123 life forever start-time now

!--- Schedule the monitoring process.  In this case the lifetime
!--- of the process is specified to be forever.  The process is scheduled to begin
!--- at the time this command is entered.  As configured, this command allows the
!--- monitoring configuration specified above to determine how often the testing
!--- occurs.  However, you can schedule this monitoring process to begin in the
!--- future and to only occur at specified times.

crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
!
track 1 rtr 123 reachability

!--- Associate a tracked static route with the SLA monitoring process.
!--- The track ID corresponds to the track ID given to the static route to monitor:
!--- route outside 0.0.0.0 0.0.0.0 10.0.0.2 1 track 1
!--- "rtr" = Response Time Reporter entry.  123 is the ID of the SLA process
!--- defined above.
```

```
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
priority-queue inside
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum client auto
 message-length maximum 512
policy-map global_policy
 class inspection_default
 inspect dns preset_dns_map
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect rsh
 inspect rtsp
 inspect esmtp
 inspect sqlnet
 inspect skinny
 inspect sunrpc
 inspect xdmcp
 inspect sip
 inspect netbios
 inspect tftp
 inspect ip-options
 inspect icmp
!
service-policy global_policy global
```

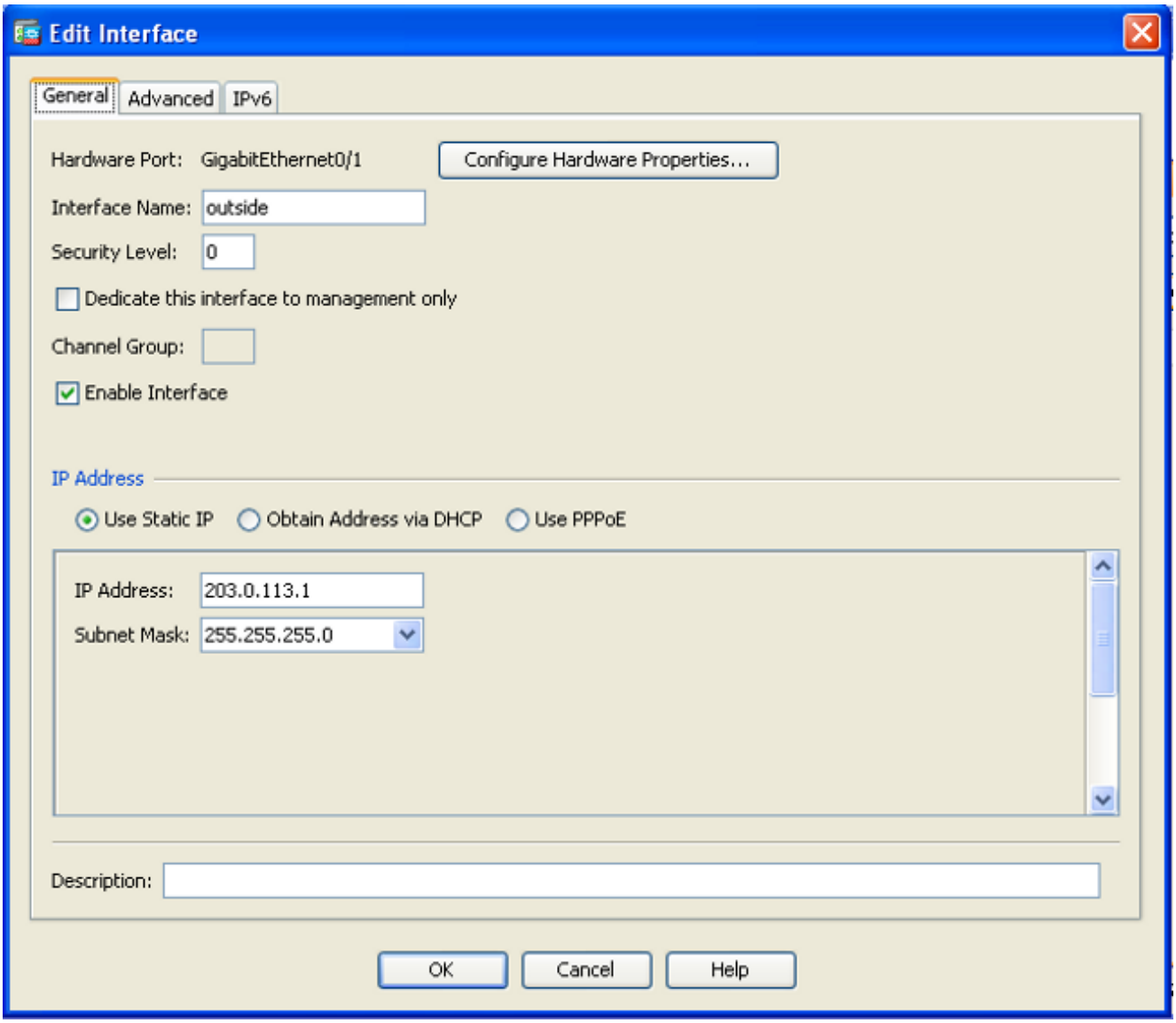
Configuration ASDM

Complétez ces étapes afin de configurer la prise en charge de FAI redondant ou de sauvegarde avec l'application ASDM :

1. Dans l'application ASDM, cliquez sur **Configuration**, puis sur **Interfaces**.



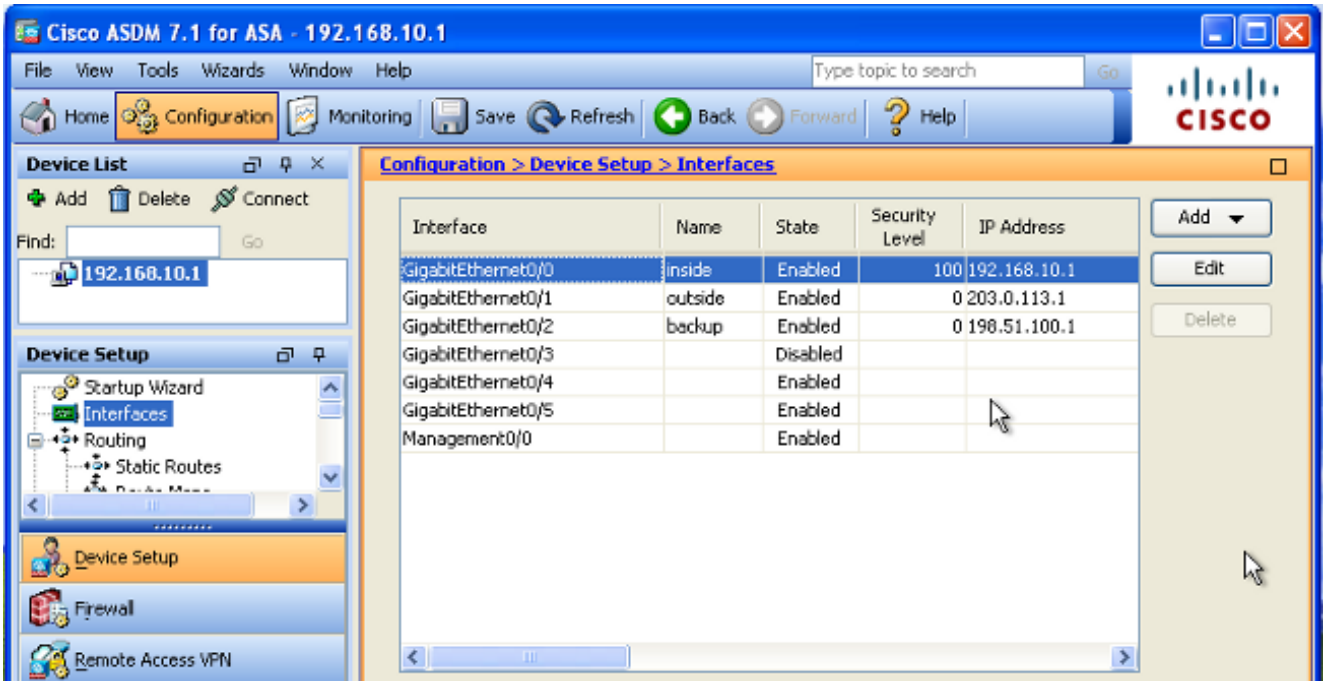
2. Sélectionnez **GigabitEthernet0/1** dans la liste Interfaces, puis cliquez sur **Modifier**. Cette boîte de dialogue apparaît:



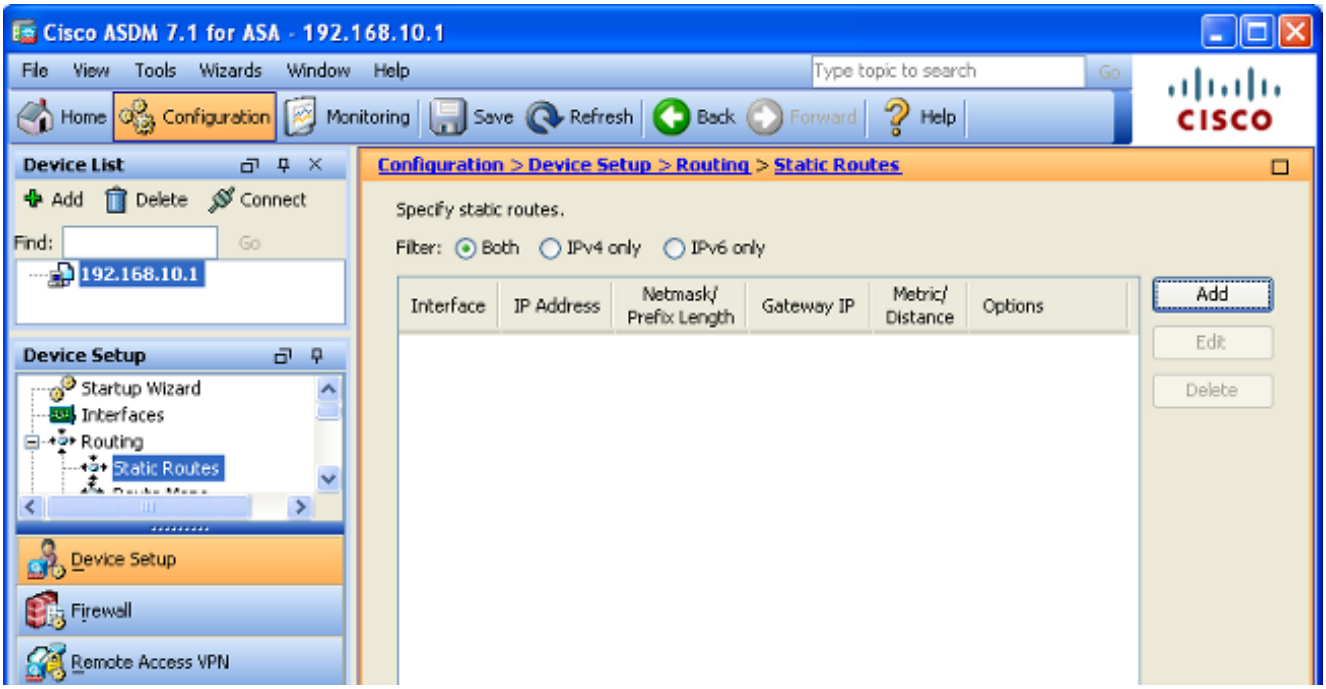
3. Cochez la case Activer l'interface et entrez les valeurs appropriées dans les champs *Nom de l'interface*, *Niveau de sécurité*, *Adresse IP* et *Masque de sous-réseau*.

4. Cliquez sur **OK pour fermer la boîte de dialogue.**

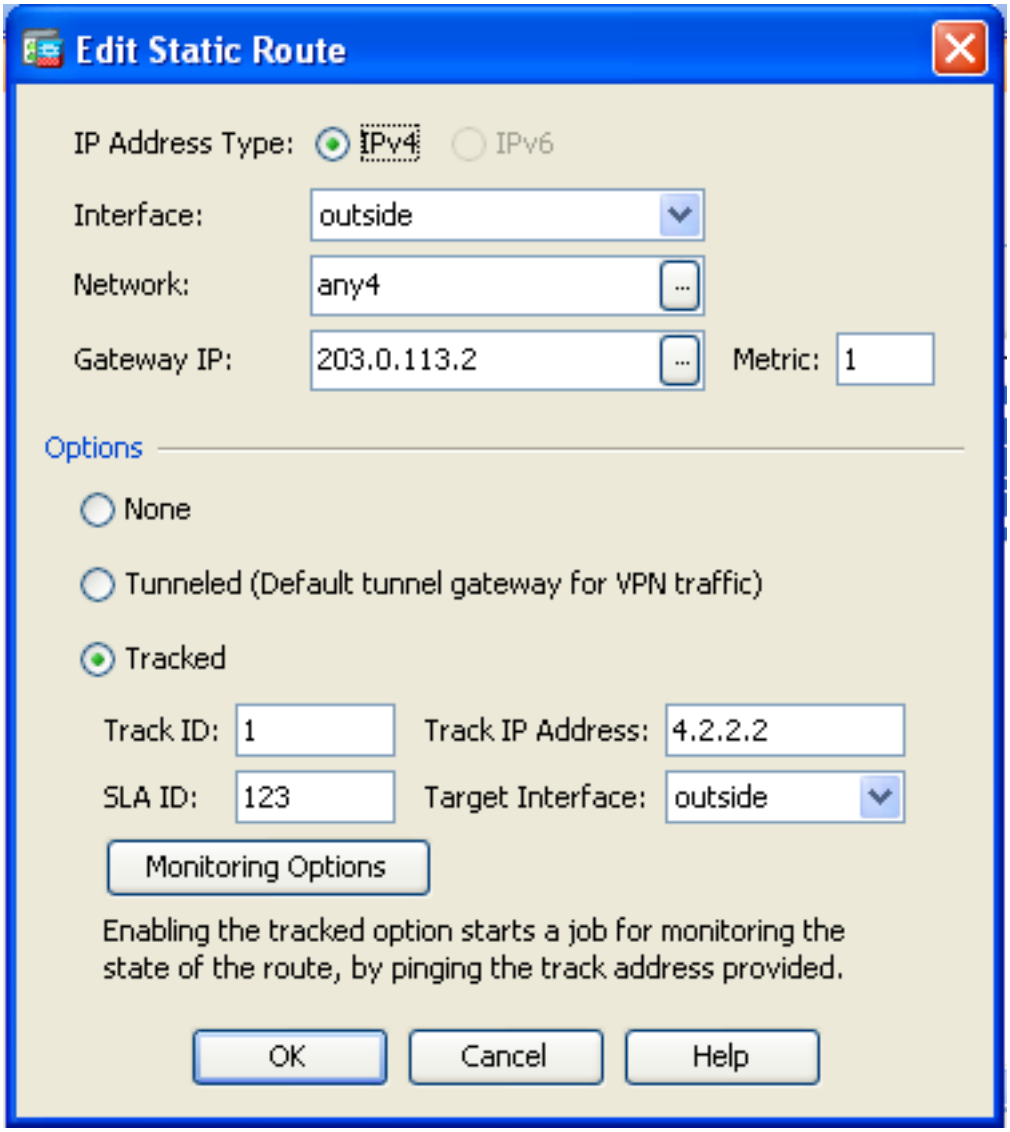
5. Configurez les autres interfaces selon les besoins, puis cliquez sur **Apply** afin de mettre à jour la configuration ASA :



6. Sélectionnez **Routage** et cliquez sur **Routes statiques** situées sur le côté gauche de l'application ASDM :



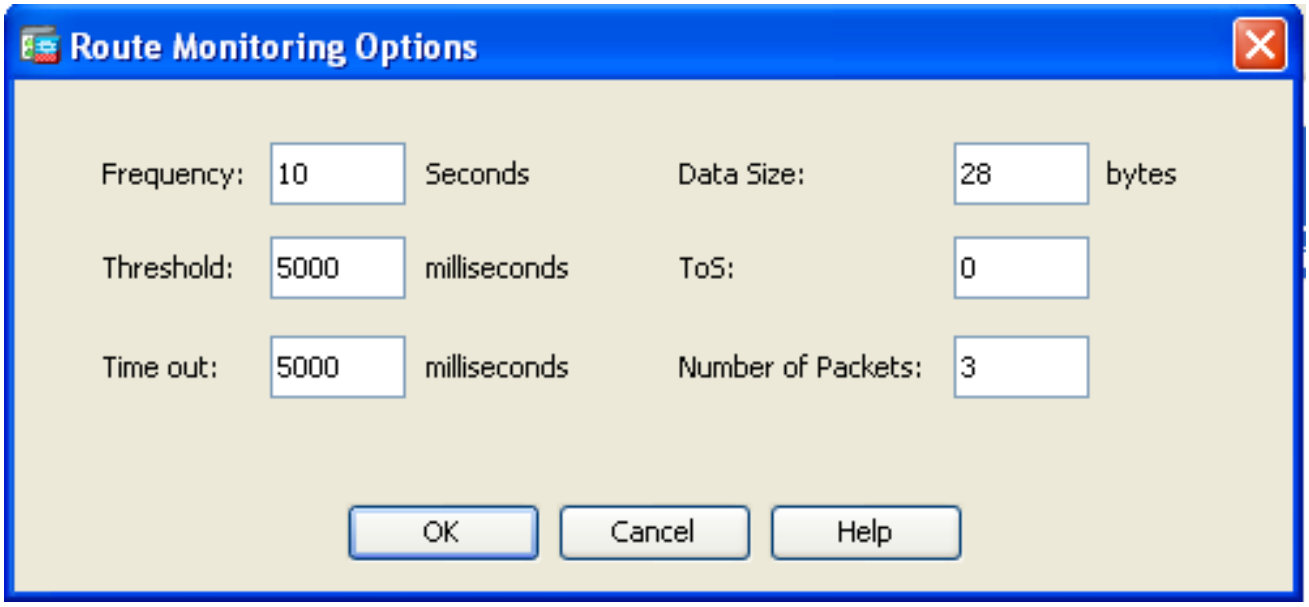
7. Cliquez sur **Add afin d'ajouter les nouvelles routes statiques.** Cette boîte de dialogue apparaît:



8. Dans la liste déroulante Interface Name, choisissez l'interface sur laquelle réside la route, et configurez la route par défaut pour atteindre la passerelle. Dans cet exemple, **203.0.113.2** est la passerelle principale du FAI et **4.2.2.2** est l'objet à surveiller avec des échos ICMP.

9. Dans la zone Options, cliquez sur la case d'option **Suivi** et entrez les valeurs appropriées dans les champs *ID de suivi*, *ID de contrat de niveau de service* et *Adresse IP de suivi*.

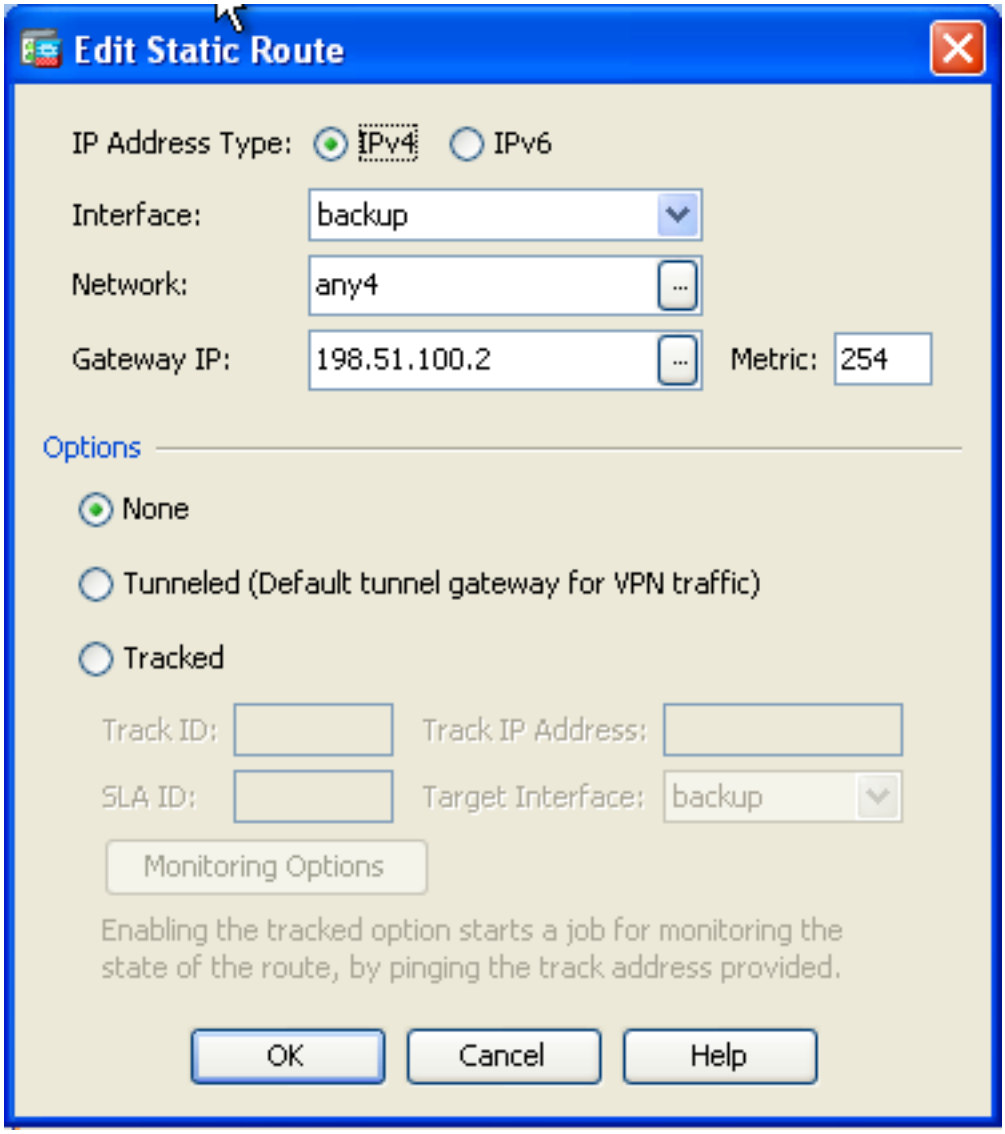
10. Cliquez sur **Monitoring Options**. Cette boîte de dialogue apparaît:



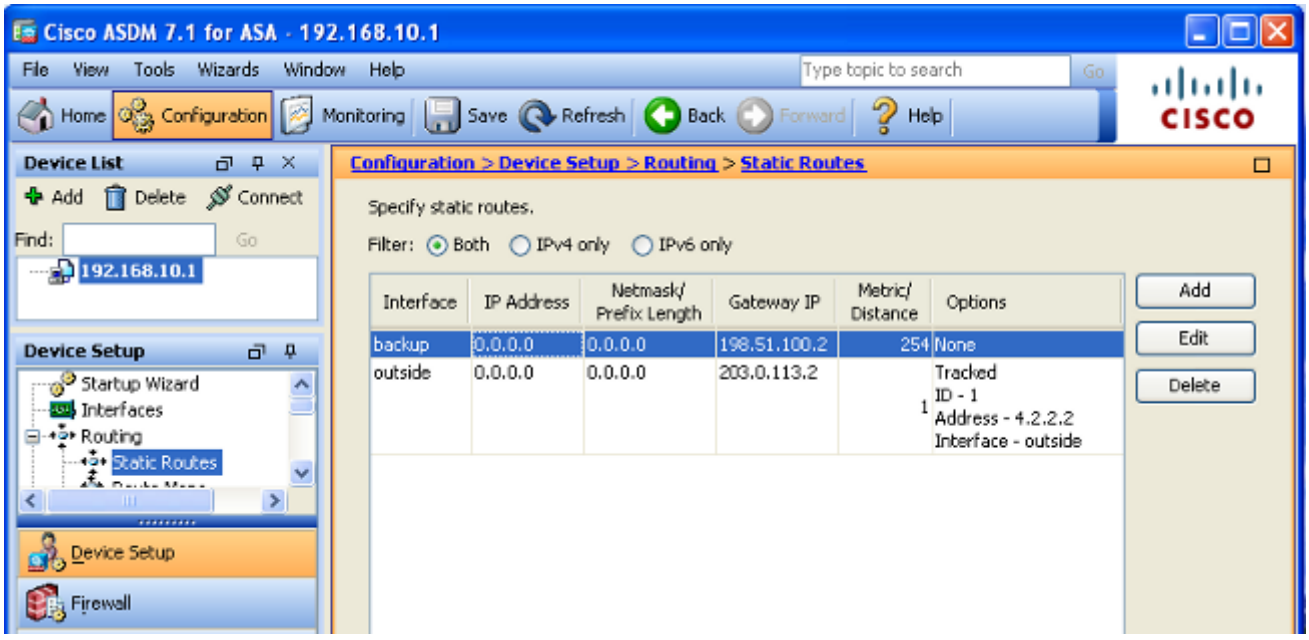
11. Entrez les valeurs appropriées pour la fréquence et les autres options de surveillance, puis cliquez sur **OK**.

12. Ajoutez une autre route statique pour l'ISP secondaire afin de fournir une route pour accéder à l'Internet. Afin d'en faire une route secondaire, configurez cette route avec une mesure plus élevée, telle que 254. Si la route primaire (ISP primaire) échoue, cette route est retirée de la table de routage. Cette route secondaire (ISP secondaire) est installée dans la table de routage PIX (Private Internet Exchange) à la place.

13. Cliquez sur **OK** afin de fermer la boîte de dialogue :



Les configurations apparaissent dans la liste Interface:



14. Sélectionnez la configuration de routage, puis cliquez sur **Apply** afin de mettre à jour la configuration ASA.

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Confirmer que la configuration est terminée

> **Note**: L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Utilisez ces commandes **show** afin de vérifier que votre configuration est terminée :

- **show running-config sla monitor** - Le résultat de cette commande affiche les commandes SLA dans la configuration.

```
ASA# show running-config sla monitor
sla monitor 123
 type echo protocol ipIcmpEcho 4.2.2.2 interface outside
 num-packets 3
 frequency 10
sla monitor schedule 123 life forever start-time now
```

- **show sla monitor configuration** - Le résultat de cette commande affiche les paramètres de configuration actuels de l'opération.

```
ASA# show sla monitor configuration 123
IP SLA Monitor, Infrastructure Engine-II.
Entry number: 123
Owner:
Tag:
Type of operation to perform: echo
Target address: 4.2.2.2
Interface: outside
Number of packets: 3
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data&colon; No
Operation frequency (seconds): 10
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

- **show sla monitor Operational-state** - Le résultat de cette commande affiche les statistiques opérationnelles de l'opération SLA.

  Avant que l'ISP primaire n'échoue, l'état opérationnel est le suivant :

```
ASA# show sla monitor operational-state 123
Entry number: 123
Modification time: 13:30:40.672 IND Sun Jan 4 2015
Number of Octets Used by this Entry: 2056
```

```
Number of operations attempted: 46
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 13:38:10.672 IND Sun Jan 4 2015
Latest operation return code: OK
RTT Values:
RTTAvg: 1       RTTMin: 1       RTTMax: 1
NumOfRTT: 3     RTTSum: 3       RTTSum2: 3
```

Une fois que le FAI principal échoue (et que le protocole ICMP fait écho au délai d'attente), il s'agit de l'état opérationnel :

```
ASA# show sla monitor operational-state
Entry number: 123
Modification time: 13:30:40.671 IND Sun Jan 4 2015
Number of Octets Used by this Entry: 2056
Number of operations attempted: 57
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 13:40:00.672 IND Sun Jan 4 2015
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

Confirmer que la route de sauvegarde est installée (méthode CLI)

Entrez la commande **show route** afin de confirmer que la route de sauvegarde est installée.

Avant que le FAI principal ne tombe en panne, la table de routage apparaît comme suit :

```
ASA# 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 203.0.113.2 to network 0.0.0.0

C    203.0.113.0 255.255.255.0 is directly connected, outside
C    192.168.10.0 255.255.255.0 is directly connected, inside
C    198.51.100.0 255.255.255.0 is directly connected, backup
S*   0.0.0.0 0.0.0.0 [1/0] via 203.0.113.2, outside
```

Après la défaillance du FAI principal, la route statique est supprimée et la route de secours est

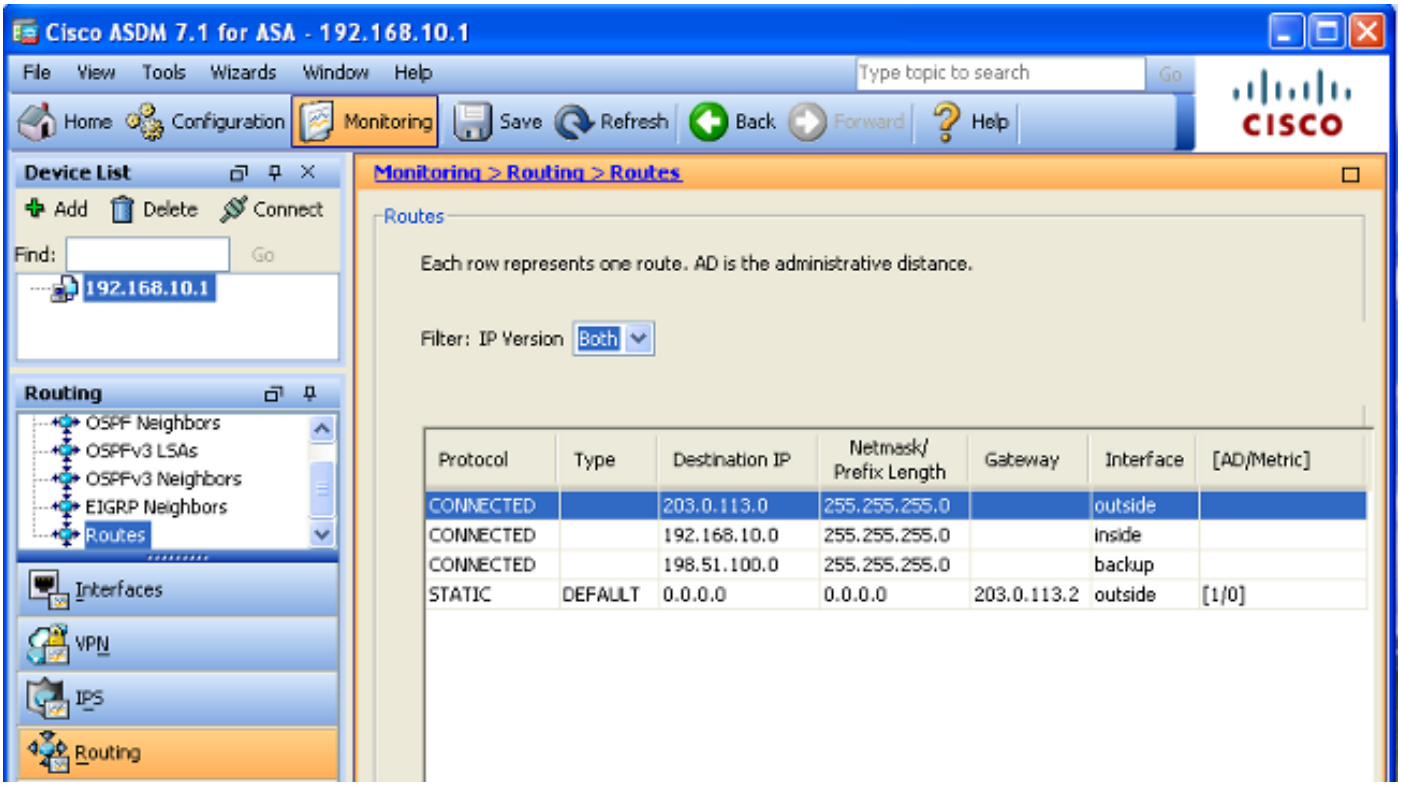
installée, la table de routage apparaît comme suit :

```
ASA# 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 198.51.100.2 to network 0.0.0.0

C     203.0.113.0 255.255.255.0 is directly connected, outside
C     192.168.10.0 255.255.255.0 is directly connected, inside
C     198.51.100.0 255.255.255.0 is directly connected, backup
S*    0.0.0.0 0.0.0.0 [254/0] via 198.51.100.2, backup
```

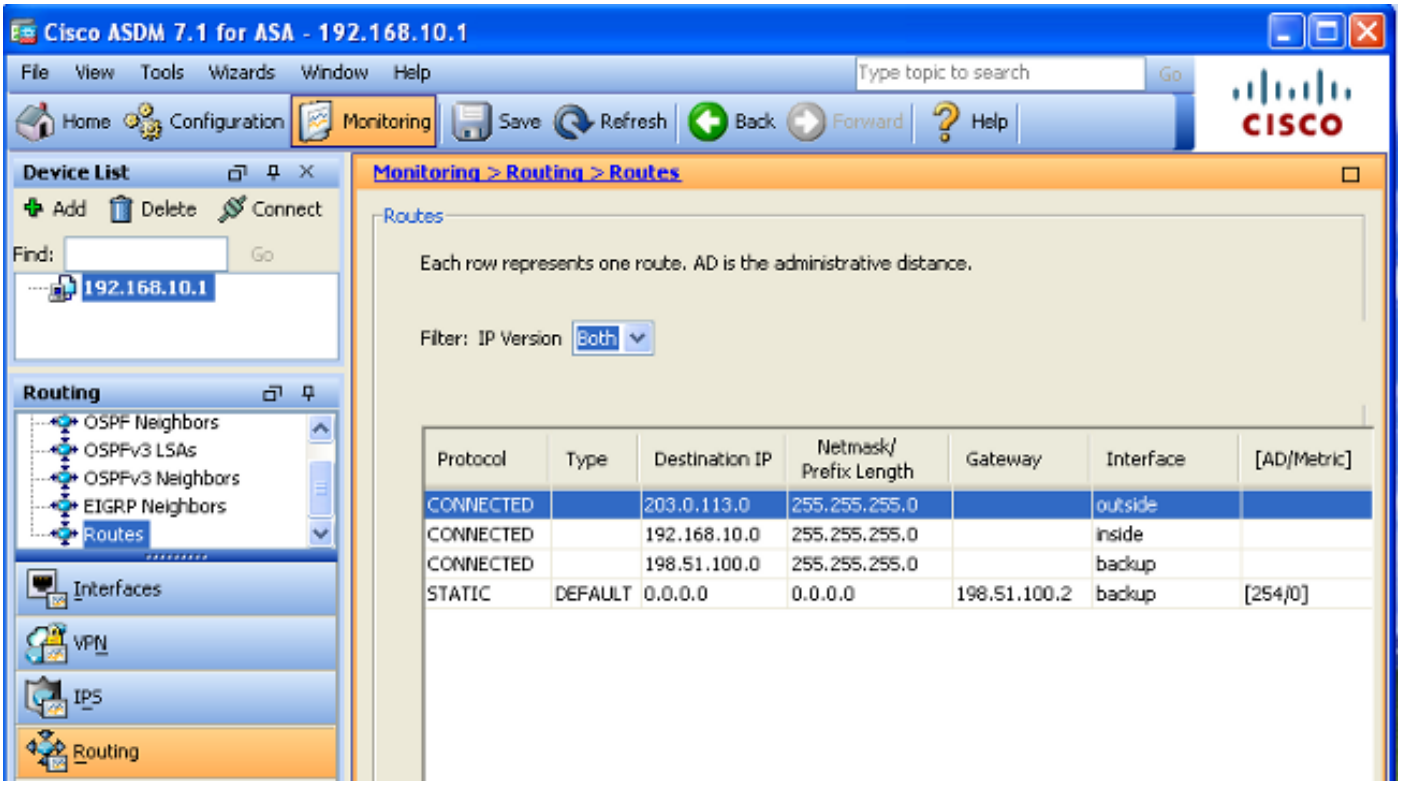
Confirmer que la route de sauvegarde est installée (méthode ASDM)

Afin de confirmer que la route de secours est installée via l'ASDM, accédez à **Monitoring > Routing**, puis choisissez **Routes** dans l'arborescence de routage.

Avant que le FAI principal ne tombe en panne, la table de routage apparaît comme celle illustrée dans l'image suivante. Notez que la route **DEFAULT** pointe vers **203.0.113.2** via l'interface **externe** :



Après la défaillance du FAI principal, la route est supprimée et la route de secours est installée. La route DEFAULT pointe maintenant vers 198.51.100.2 via l'interface de secours:



Dépannage

Cette section fournit quelques commandes de débogage utiles et décrit comment résoudre un problème où la route suivie est supprimée inutilement.

Commandes de débogage

Vous pouvez utiliser ces commandes de débogage afin de résoudre vos problèmes de configuration :

- **debug sla monitor trace** - Le résultat de cette commande affiche la progression de l'opération d'écho.

  Si l'objet suivi (passerelle principale du FAI) est actif et que les échos ICMP réussissent, le résultat semble similaire à ceci :

```
IP SLA Monitor(123) Scheduler: Starting an operation
IP SLA Monitor(123) echo operation: Sending an echo operation
IP SLA Monitor(123) echo operation: RTT=0 OK
IP SLA Monitor(123) echo operation: RTT=0 OK
IP SLA Monitor(123) echo operation: RTT=1 OK
IP SLA Monitor(123) Scheduler: Updating result
```

  Si l'objet suivi (passerelle principale du FAI) est arrêté et que les échos ICMP échouent, la sortie semble similaire à ceci :

```
IP SLA Monitor(123) Scheduler: Starting an operation
IP SLA Monitor(123) echo operation: Sending an echo operation
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) echo operation: Timeout
```

```
IP SLA Monitor(123) Scheduler: Updating result
```

- **debug sla monitor error** - Le résultat de cette commande affiche toutes les erreurs rencontrées par le processus de surveillance SLA.

  Si l'objet suivi (passerelle principale du FAI) est actif et que l'ICMP réussit, le résultat est similaire à ceci :

```
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:4.2.2.2
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/39878 laddr 203.0.113.1/39878
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/39878 laddr 203.0.113.1/39878
%ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:00
%ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:00
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:4.2.2.2
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/39879 laddr 203.0.113.1/39879
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/39879 laddr 203.0.113.1/39879
%ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:00
%ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:00
```

  Si l'objet suivi (passerelle principale du FAI) est arrêté et que la route suivie est supprimée, le résultat est similaire à ceci :

```
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:4.2.2.2
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/59003 laddr 203.0.113.1/59003
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/59004 laddr 203.0.113.1/59004
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/59005 laddr 203.0.113.1/59005
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/59003 laddr 203.0.113.1/59003
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/59004 laddr 203.0.113.1/59004
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/59005 laddr 203.0.113.1/59005
%ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:02
%ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:02
%ASA-6-622001: Removing tracked route 0.0.0.0 0.0.0.0 203.0.113.2,
distance 1, table Default-IP-Routing-Table, on interface outside

!--- 4.2.2.2 is unreachable, so the route to the Primary ISP is removed.
```

La route suivie est retirée inutilement

Si la route suivie est retirée inutilement, assurez-vous que votre cible de surveillance est toujours disponible pour recevoir des demandes d'écho. En outre, assurez-vous que l'état de votre cible de surveillance (c'est-à-dire, si la cible est ou non accessible) est étroitement lié à l'état de la connexion à l'ISP primaire.

Si vous choisissez une cible de surveillance plus éloignée que la passerelle du FAI, une autre liaison le long de cette route peut échouer ou un autre périphérique peut interférer. Cette configuration peut amener le moniteur SLA à conclure que la connexion au FAI principal a échoué et faire basculer inutilement l'ASA vers la liaison du FAI secondaire.

Par exemple, si vous choisissez un routeur de succursale comme cible de surveillance, la connexion de l'ISP à votre succursale peut échouer, ainsi que n'importe quelle autre liaison intermédiaire. Une fois que les échos ICMP envoyés par l'opération de surveillance échouent, la route suivie principale est supprimée, même si la liaison principale du FAI est toujours active.

Dans cet exemple, la passerelle de l'ISP primaire qui est utilisée comme cible de surveillance est gérée par l'ISP et se trouve de l'autre côté de la liaison ISP. Cette configuration garantit que si les échos ICMP envoyés par l'opération de surveillance échouent, la liaison ISP est presque certainement en panne.

Informations connexes

- Pare-feu de nouvelle génération Cisco ASA 5500-X
- Support et documentation techniques - Cisco Systems