ASA/PIX 7.x : Exemple de configuration de liens ISP redondants ou de sauvegarde

Contenu

Introduction

Un problème avec les routes statiques est qu'aucun mécanisme inhérent n'existe pour déterminer si la route en activée ou désactivée. 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 fonction de suivi de route statique est utilisée pour suivre la disponibilité d'une route statique et, si la route échoue, supprimez-la de la table de routage et remplacez-la par une route de secours.

Ce document fournit un exemple de la façon d'utiliser la fonction de suivi de route statique sur le dispositif de sécurité de la gamme PIX 500 ou le dispositif de sécurité adaptatif dédié de la gamme Cisco ASA 5500 afin de permettre au périphérique d'utiliser des connexions Internet redondantes ou de secours. Dans cet exemple, le suivi des routes statiques permet au dispositif de sécurité d'utiliser une connexion peu coûteuse à un fournisseur de services Internet secondaire

(ISP) au cas où la ligne louée primaire deviendrait indisponible.

Afin de réaliser cette redondance, le dispositif de Sécurité associe une route statique à une cible de surveillance que vous définissez. L'opération SLA (Service level agreement, contrat de niveau de service) surveille la cible avec des demandes d'écho ICMP (Internet Control Message Protocol) périodiques. Si aucune réponse d'écho n'est reçue, l'objet est considéré comme inactif, et la route associée est retirée de la table de routage. Une route de secours précédemment configurée est utilisée au lieu de la route qui est retirée. Tandis que la route de secours est en service, l'opération de surveillance SLA continue à essayer 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.

Note: La configuration décrite dans ce document ne peut pas être utilisée pour l'équilibrage de charge ou le partage de charge car ils ne sont pas pris en charge sur ASA/PIX. Utilisez cette configuration à des fins de redondance ou de secours seulement. Le trafic sortant utilise l'ISP primaire et puis l'ISP secondaire, si le primaire échoue. La panne de l'ISP primaire entraîne une interruption provisoire du trafic.

Conditions préalables

Conditions requises

Choisissez une cible de surveillance qui peut répondre aux demandes d'écho ICMP. La cible peut être n'importe quel objet du réseau que vous choisissez, mais une cible qui est étroitement attachée à votre connexion ISP est recommandée. Quelques cibles de surveillance possibles incluent :

- L'adresse de la passerelle ISP
- Une autre adresse gérée par l'ISP
- Un serveur sur un autre réseau, comme un serveur AAA, avec lequel le dispositif de sécurité 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 le dispositif de sécurité est complètement opérationnel et configuré pour permettre à Cisco ASDM d'apporter des modifications de configuration.

Note: Pour des informations sur la façon de permettre à l'ASDM de configurer le périphérique, référez-vous à Permettre l'accès HTTPS pour l'ASDM.

Composants utilisés

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

- Cisco PIX Security Appliance 515E avec la version 7.2(1) ou ultérieure du logiciel
- Cisco Adaptive Security Device Manager 5.2(1) ou versions ultérieures

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

Vous pouvez également utiliser cette configuration avec les Dispositifs de sécurité dédiés de la gamme Cisco ASA 5500 version 7.2(1).

Note: La commande **backup interface** est requise pour configurer la quatrième interface sur ASA 5505. Référez-vous à la commande backup interface pour plus d'informations.

Conventions

Pour plus d'informations sur les conventions des documents, reportez-vous au document Conventions relatives aux conseils techniques Cisco.

Informations générales

Dans cet exemple, le dispositif de sécurité gère deux connexions à l'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 d'abonné numérique (DSL) à vitesse réduite qui est accessible via un modem DSL fourni par l'ISP secondaire.

Note: L'équilibrage de charge ne se produit pas dans cet exemple.

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 à l'ISP primaire s'arrête, le dispositif de sécurité change la table de routage pour diriger le trafic vers la connexion DSL. Le suivi des routes statiques est utilisé pour réaliser cette redondance.

Le dispositif de sécurité est configuré avec une route statique qui dirige tout le trafic Internet vers l'ISP primaire. Toutes les 10 secondes, le processus de surveillance SLA vérifie que la passerelle de l'ISP primaire 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 situés derrière le dispositif de sécurité. Comme décrit dans ce document, cette configuration peut ne pas convenir à l'accès entrant vers les ressources situées derrière le dispositif de sécurité. Des qualifications de mise en réseau avancées sont requises pour réaliser des connexions entrantes transparentes. Ces qualifications ne sont pas couvertes dans ce document.

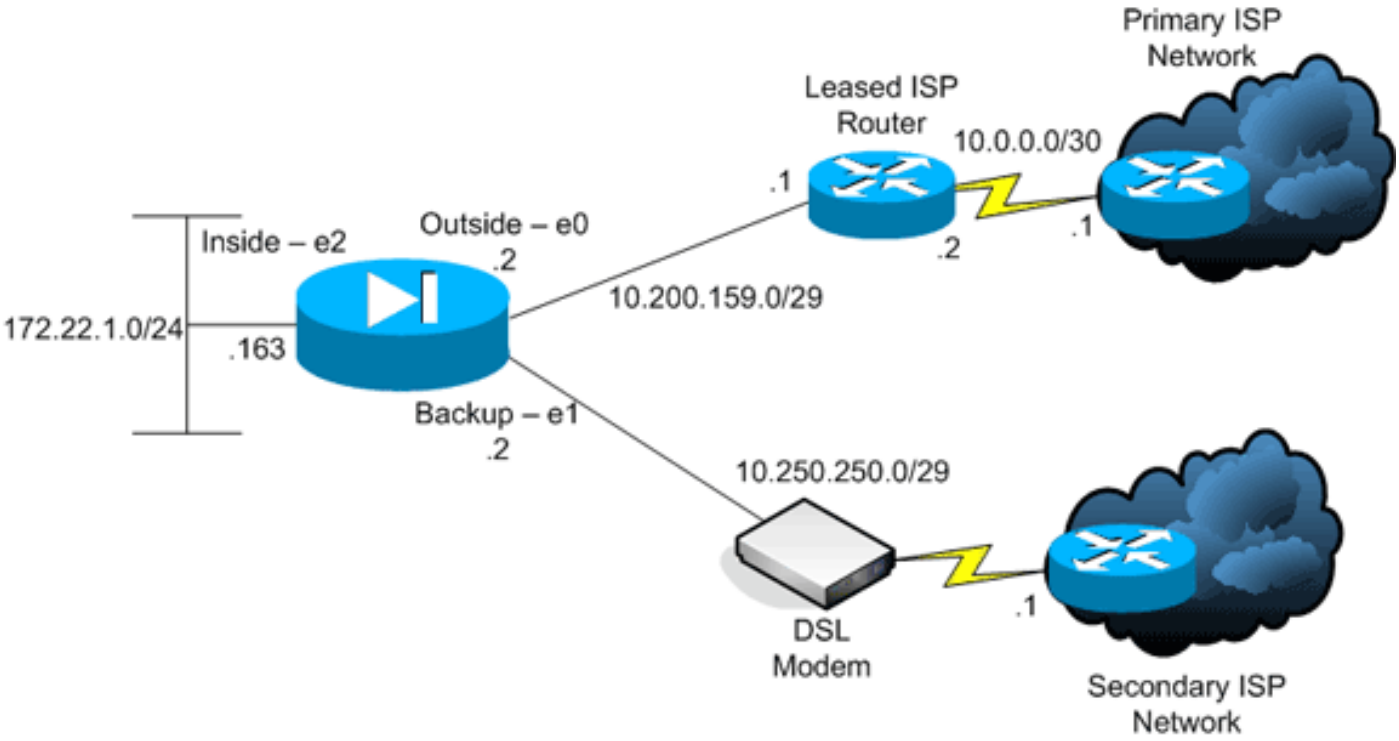
Configurez

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

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

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise les configurations suivantes :

- Interface de ligne de commande (CLI)
- Adaptive Security Device Manager (ASDM)

Note: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Configuration CLI

PIX

```
pix# show running-config
: Saved
:
PIX Version 7.2(1)
!
hostname pix
domain-name default.domain.invalid
enable password 9jNfZuG3TC5tCVH0 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.200.159.2 255.255.255.248
!
interface Ethernet1
```

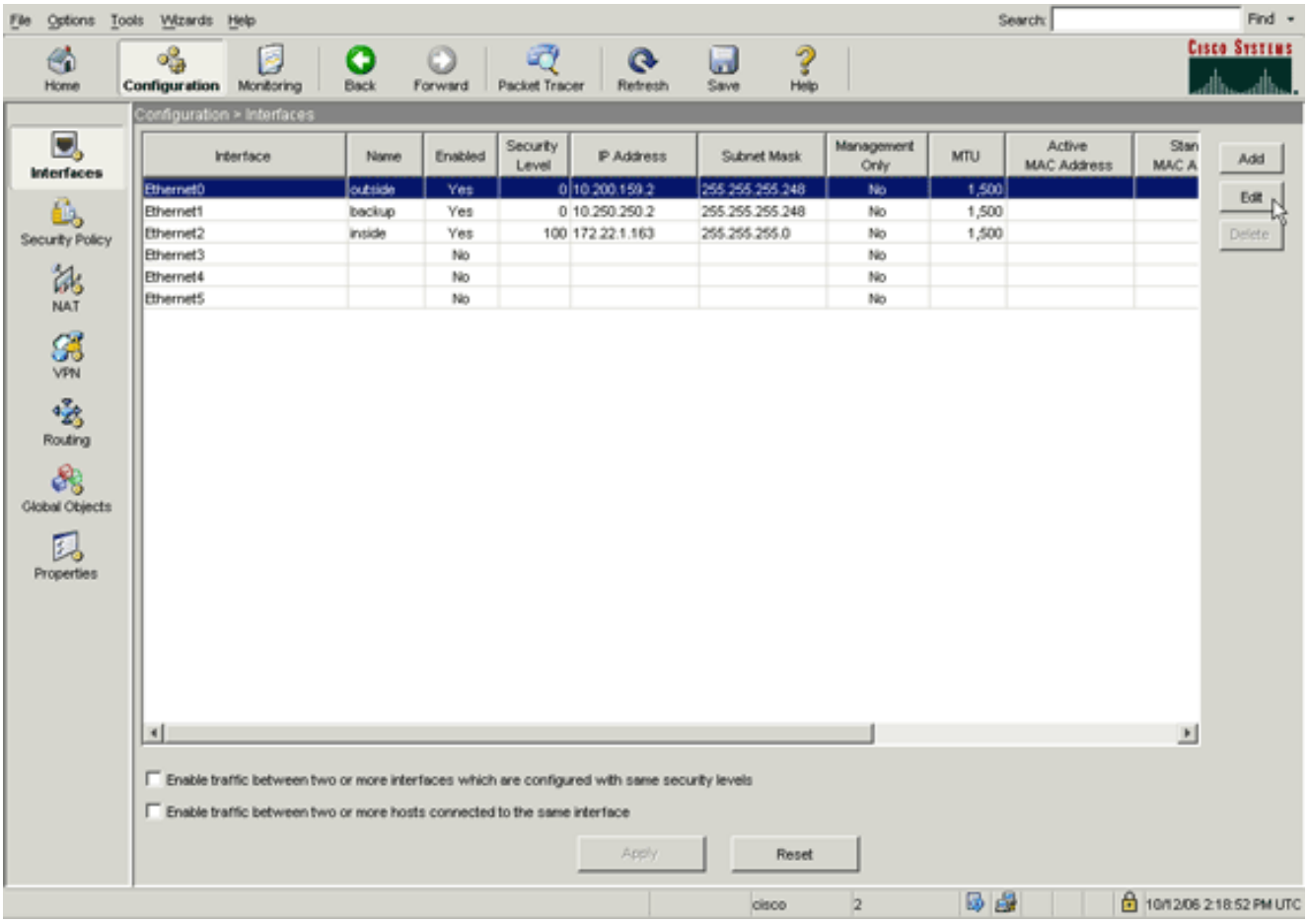
```
 nameif backup
!--- The interface attached to the Secondary ISP. !---
"backup" was chosen here, but any name can be assigned.
security-level 0 ip address 10.250.250.2 255.255.255.248
! interface Ethernet2 nameif inside security-level 100
ip address 172.22.1.163 255.255.255.0 ! interface
Ethernet3 shutdown no nameif no security-level no ip
address ! interface Ethernet4 shutdown no nameif no
security-level no ip address ! interface Ethernet5
shutdown no nameif no security-level no ip address !
passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive dns
server-group DefaultDNS domain-name
default.domain.invalid pager lines 24 logging enable
logging buffered debugging mtu outside 1500 mtu backup
1500 mtu inside 1500 no failover asdm image
flash:/asdm521.bin no asdm history enable arp timeout
14400 global (outside) 1 interface
global (backup) 1 interface
nat (inside) 1 172.16.1.0 255.255.255.0
!--- NAT Configuration for Outside and Backup route
outside 0.0.0.0 0.0.0.0 10.200.159.1 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
10.250.250.1 254
!--- 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 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 uauth 0:05:00 absolute
username cisco password ffIRPGpDSOJh9YLq encrypted http
server enable http 172.22.1.0 255.255.255.0 inside no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart sla monitor 123
 type echo protocol ipIcmpEcho 10.0.0.1 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. !
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 timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  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 netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:a4a0e9be4593ad43bc17a1cc25e32dc2
: end
```

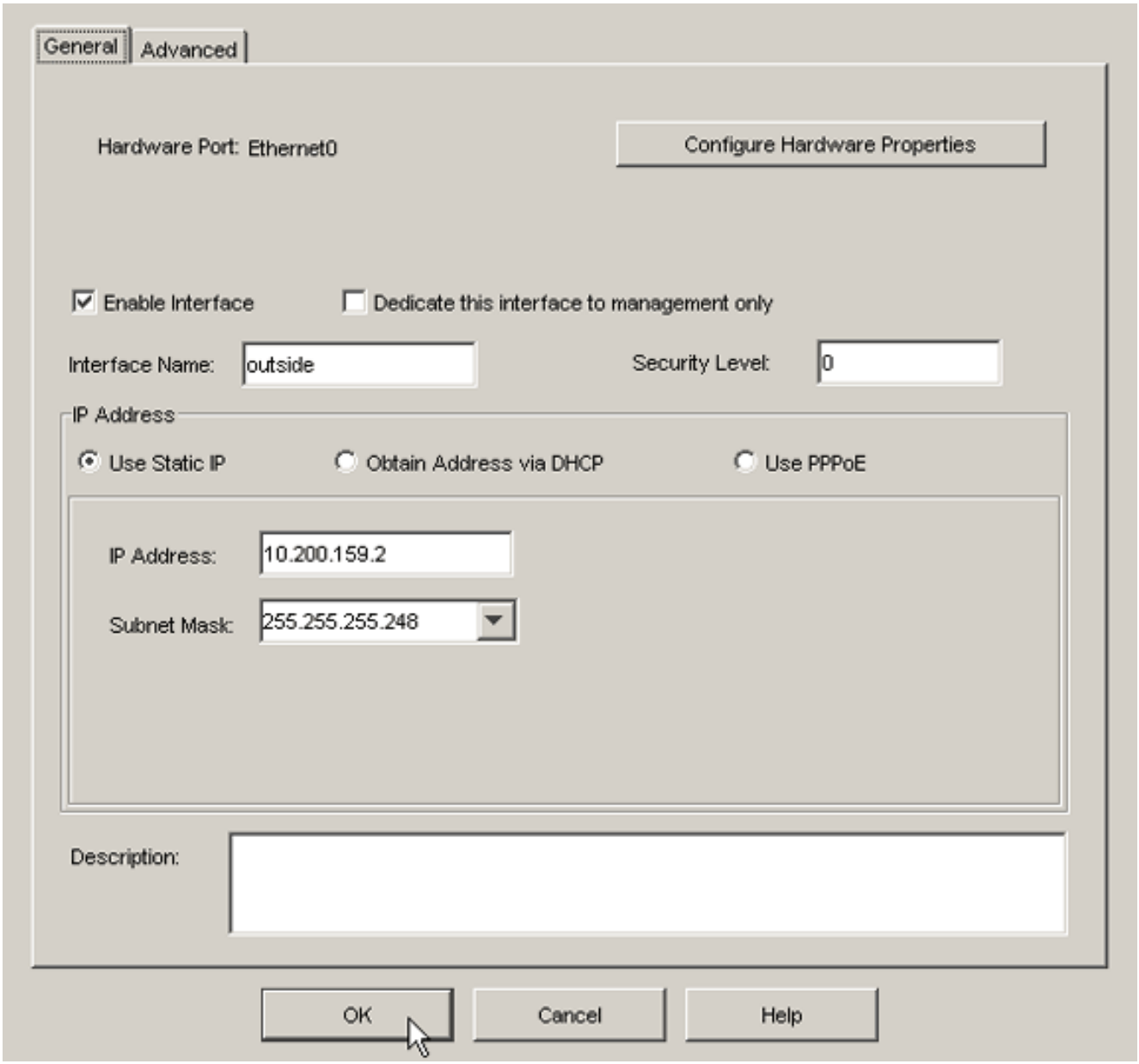
Configuration ASDM

Afin de configurer la prise en charge d'ISP redondante ou de secours avec l'application ASDM, complétez ces étapes :

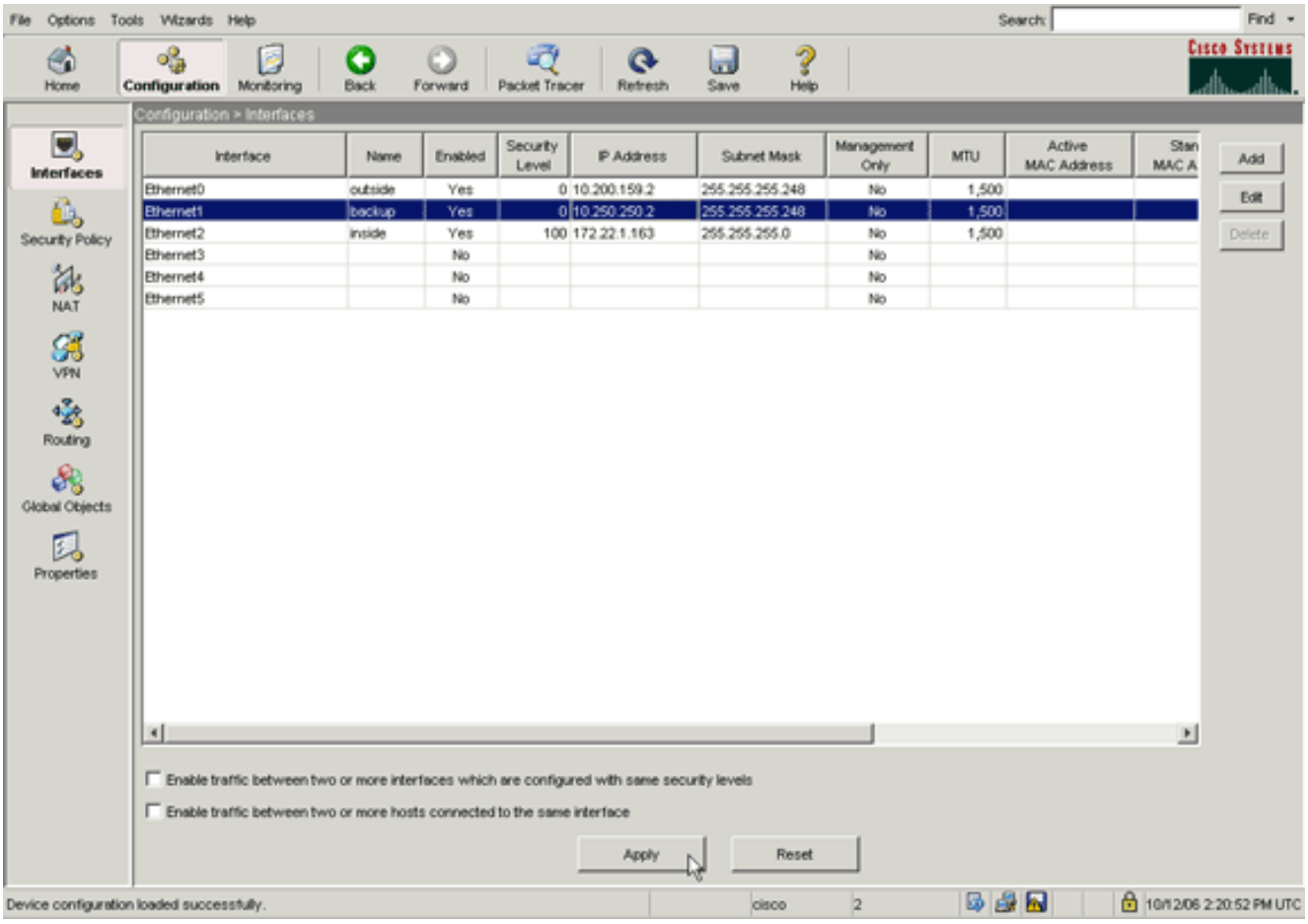
1. Dans l'application ASDM, cliquez sur **Configuration**, puis sur **Interfaces**.



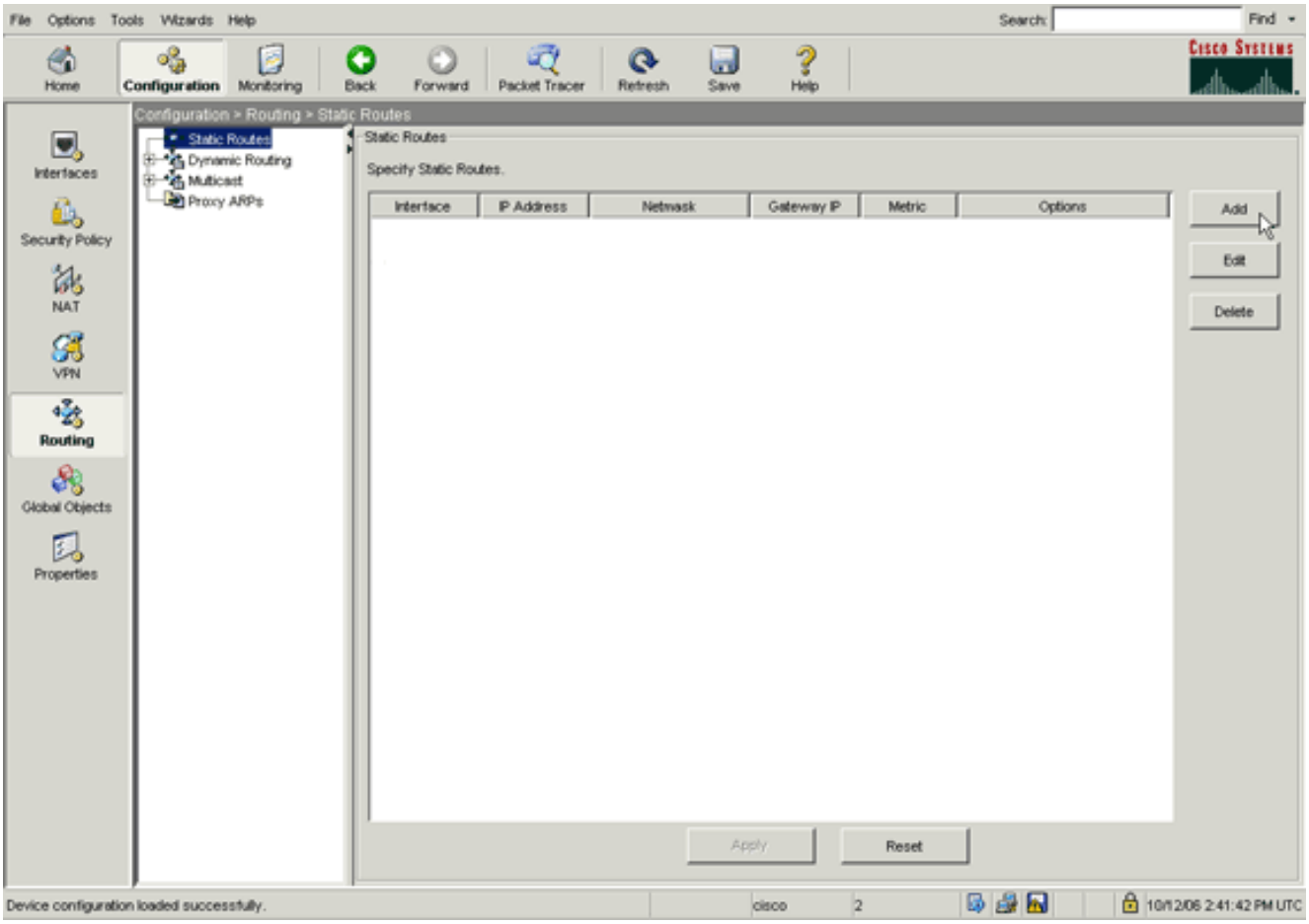
2. Dans la liste Interfaces, sélectionnez **Ethernet0**, puis cliquez sur **Edit**.Cette boîte de dialogue apparaît.



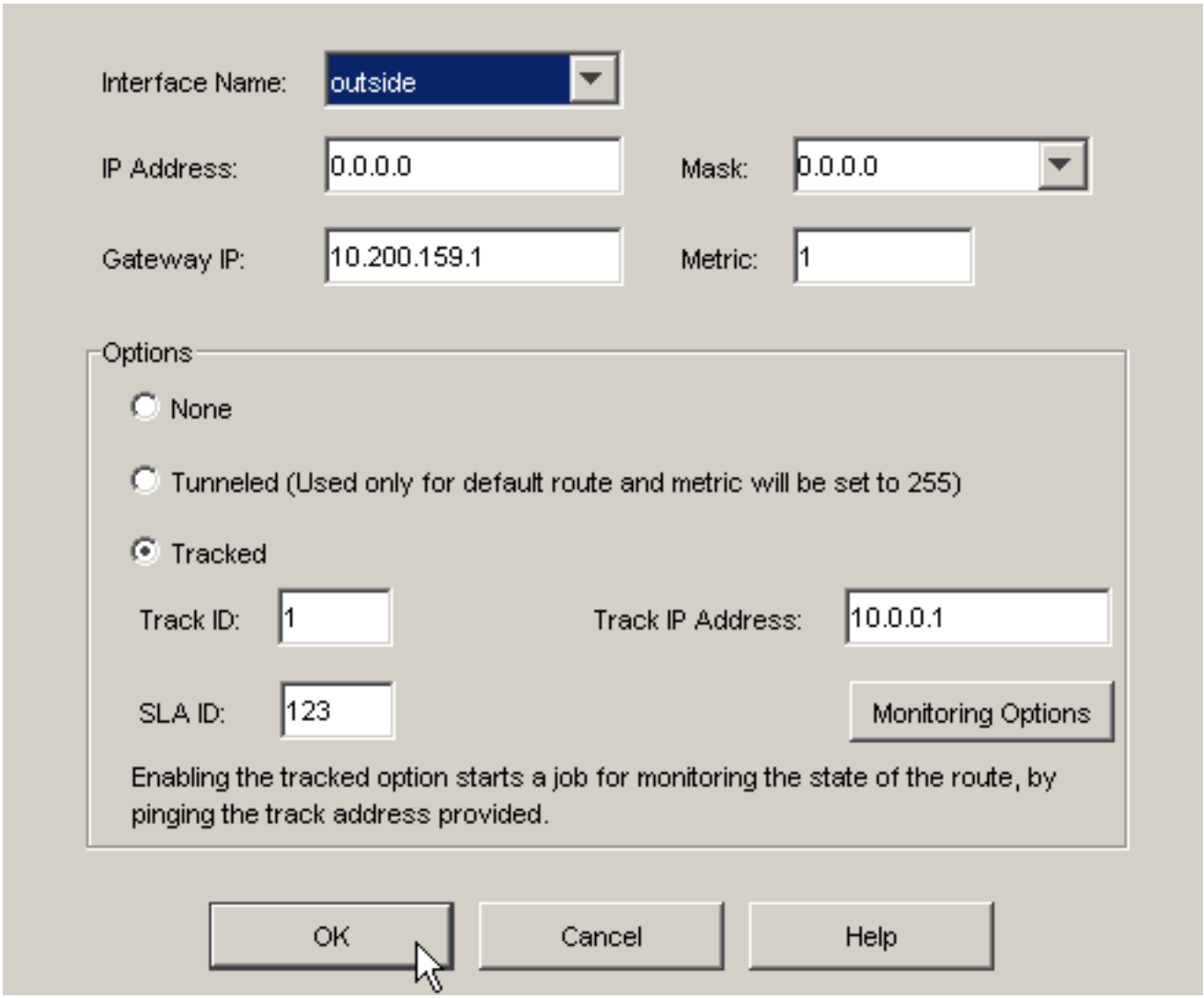
3. Activez la case à cocher **Enable Interface** , et entrez des valeurs dans les zones Interface Name, Security Level, IP Address et Subnet Mask.
4. Cliquez sur **OK** pour fermer la boîte de dialogue.
5. Configurez d'autres interfaces si nécessaire, et cliquez sur **Apply** pour mettre à jour la configuration du dispositif de
sécurité.



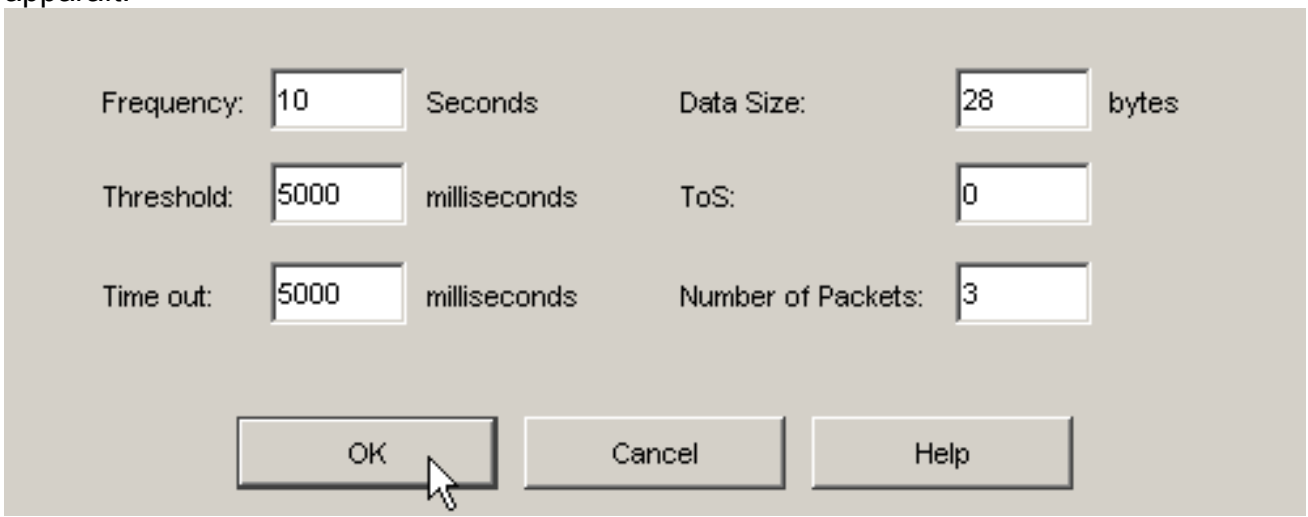
6. Cliquez sur **Routing** à gauche de l'application ASDM.



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



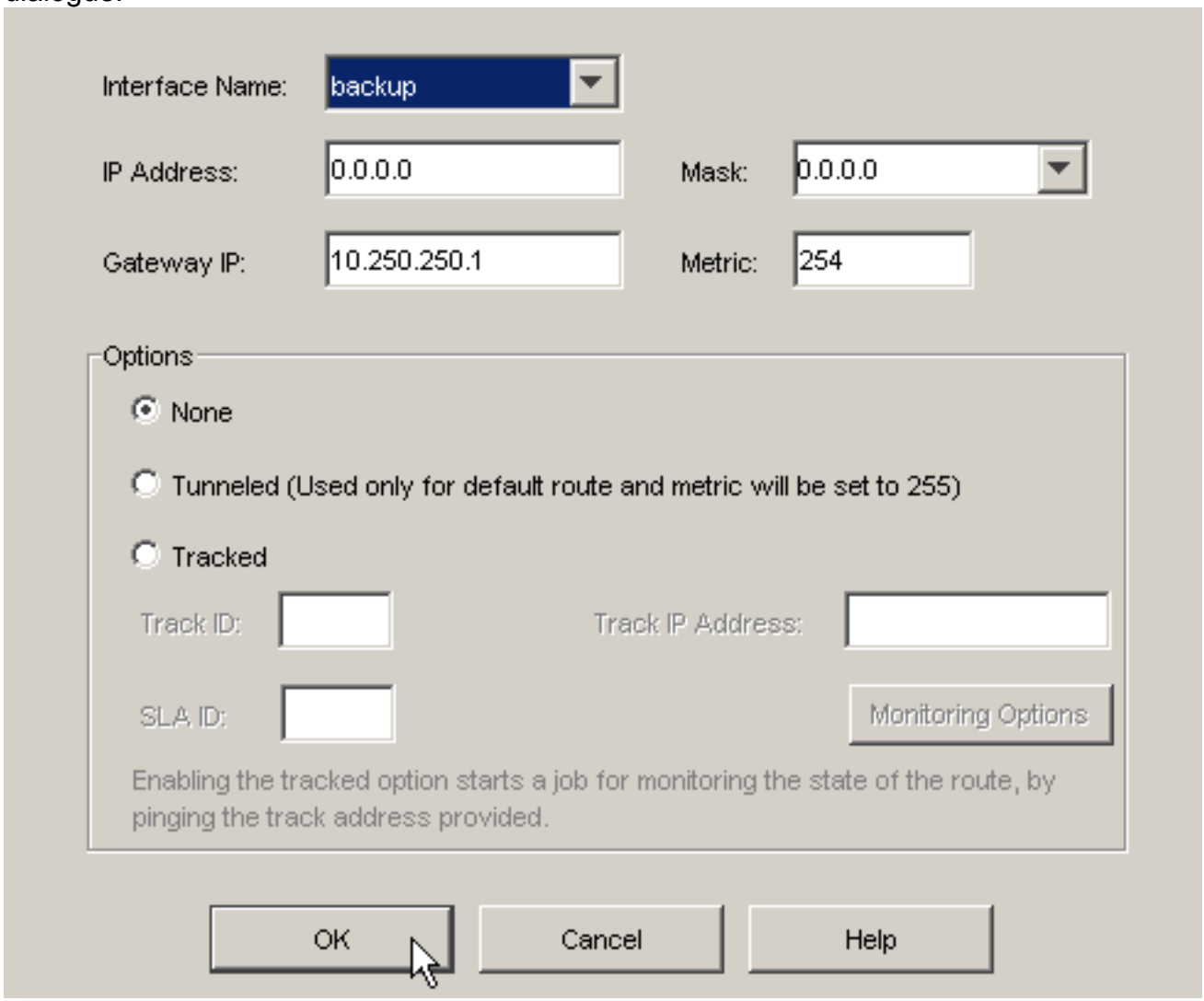
8. Dans la liste déroulante Interface Name, choisissez l'interface sur laquelle réside la route, et configurez la route par défaut pour atteindre la passerelle. Dans cet exemple, 10.0.0.1 est la passerelle de l'ISP primaire, ainsi que l'objet à surveiller avec des échos ICMP.
9. Dans la zone Options, cliquez sur la case d'option **Tracked**, et entrez des valeurs dans les zones Track ID, SLA ID et Track IP Address.
10. Cliquez sur **Monitoring Options**.Cette boîte de dialogue apparaît.



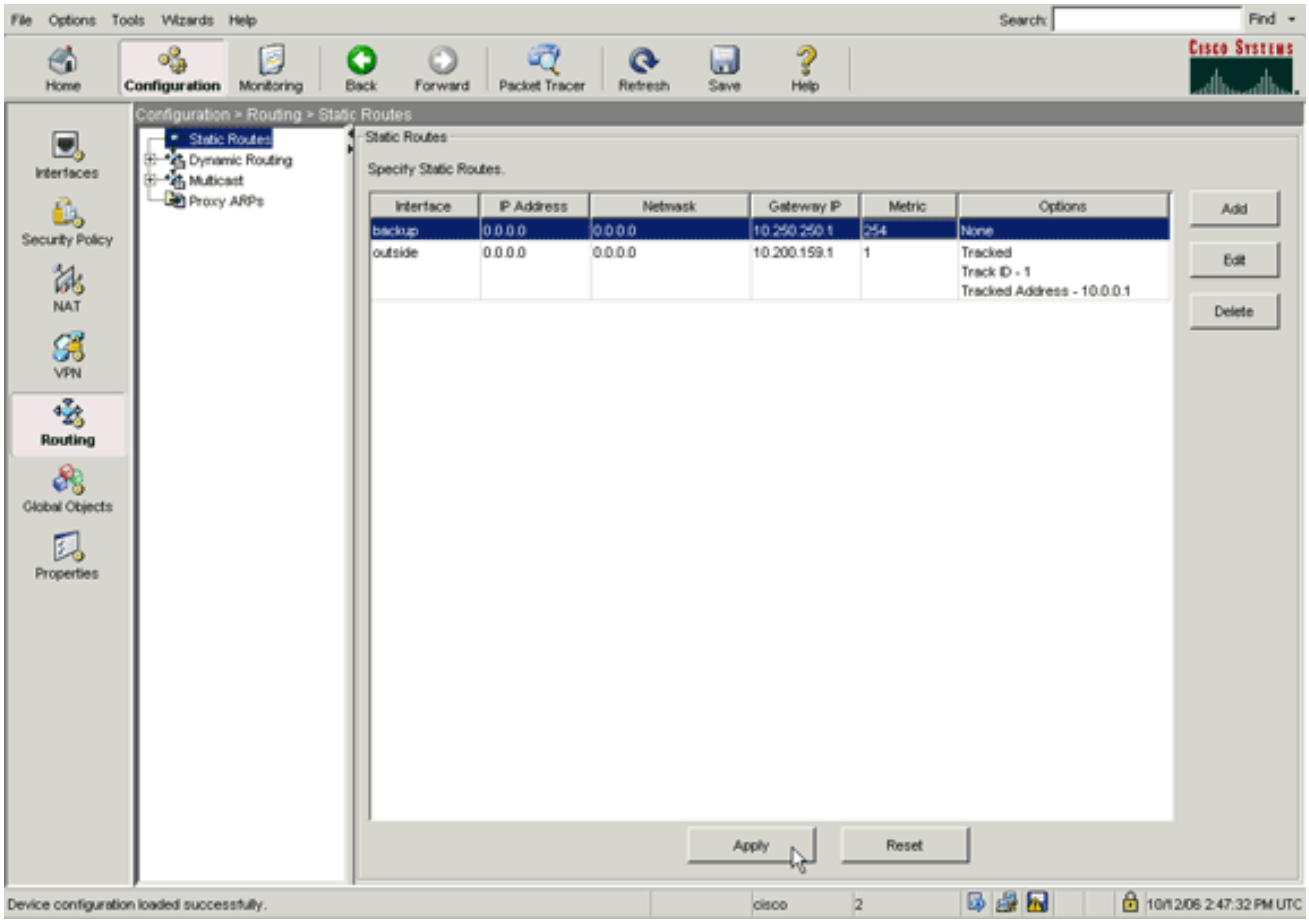
11. Entrez des valeurs pour la fréquence et d'autres options de surveillance, et cliquez sur **OK**.
12. Ajoutez une autre route statique pour l'ISP secondaire afin de fournir une route pour accéder à l'Internet.Afin d'en faire une route secondaire, configurez cette route avec une

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 à la place.

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



Les configurations apparaissent dans la liste Interface.



14. Sélectionnez la configuration de routage, et cliquez sur **Apply** pour mettre à jour la configuration du dispositif de sécurité.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Confirmez que la configuration est terminée

Utilisez ces commandes **show** pour vérifier que votre configuration est terminée.

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** .

- **show running-config sla monitor** — Affiche les commandes SLA dans configuration.

```
pix# show running-config sla monitor
sla monitor 123
 type echo protocol ipIcmpEcho 10.0.0.1 interface outside
 num-packets 3
 frequency 10
sla monitor schedule 123 life forever start-time now
```

- **show sla monitor configuration** - Affiche les paramètres de configuration actuels de l'opération.

```
pix# show sla monitor configuration 123
IP SLA Monitor, Infrastructure Engine-II.
Entry number: 123
Owner:
Tag:
Type of operation to perform: echo
```

```
Target address: 10.0.0.1
Interface: outside
Number of packets: 3
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: 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 configuration** - Affiche les statistiques opérationnelles de l'opération SLA.Avant que l'ISP primaire n'échoue, l'état opérationnel est le suivant :

```
pix# show sla monitor operational-state 123
Entry number: 123
Modification time: 13:59:37.824 UTC Thu Oct 12 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 367
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: 15:00:37.825 UTC Thu Oct 12 2006
Latest operation return code: OK
RTT Values:
RTTAvg: 1       RTTMin: 1       RTTMax: 1
NumOfRTT: 3     RTTSum: 3       RTTSum2: 3
```

Après que l'ISP primaire a échoué (et que les échos ICMP ont expiré), l'état opérationnel est le suivant :

```
pix# show sla monitor operational-state
Entry number: 123
Modification time: 13:59:37.825 UTC Thu Oct 12 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 385
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: 15:03:27.825 UTC Thu Oct 12 2006
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

Confirmez que la route de secours est installée (méthode CLI)

Utilisez la commande **show route** pour déterminer quand la route de secours est installée.

- Avant que l'ISP primaire n'échoue, la table de routage est la suivante :

```
pix# 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 10.200.159.1 to network 0.0.0.0

S    64.101.0.0 255.255.0.0 [1/0] via 172.22.1.1, inside
C    172.22.1.0 255.255.255.0 is directly connected, inside
C    10.250.250.0 255.255.255.248 is directly connected, backup
C    10.200.159.0 255.255.255.248 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.200.159.1, outside
```

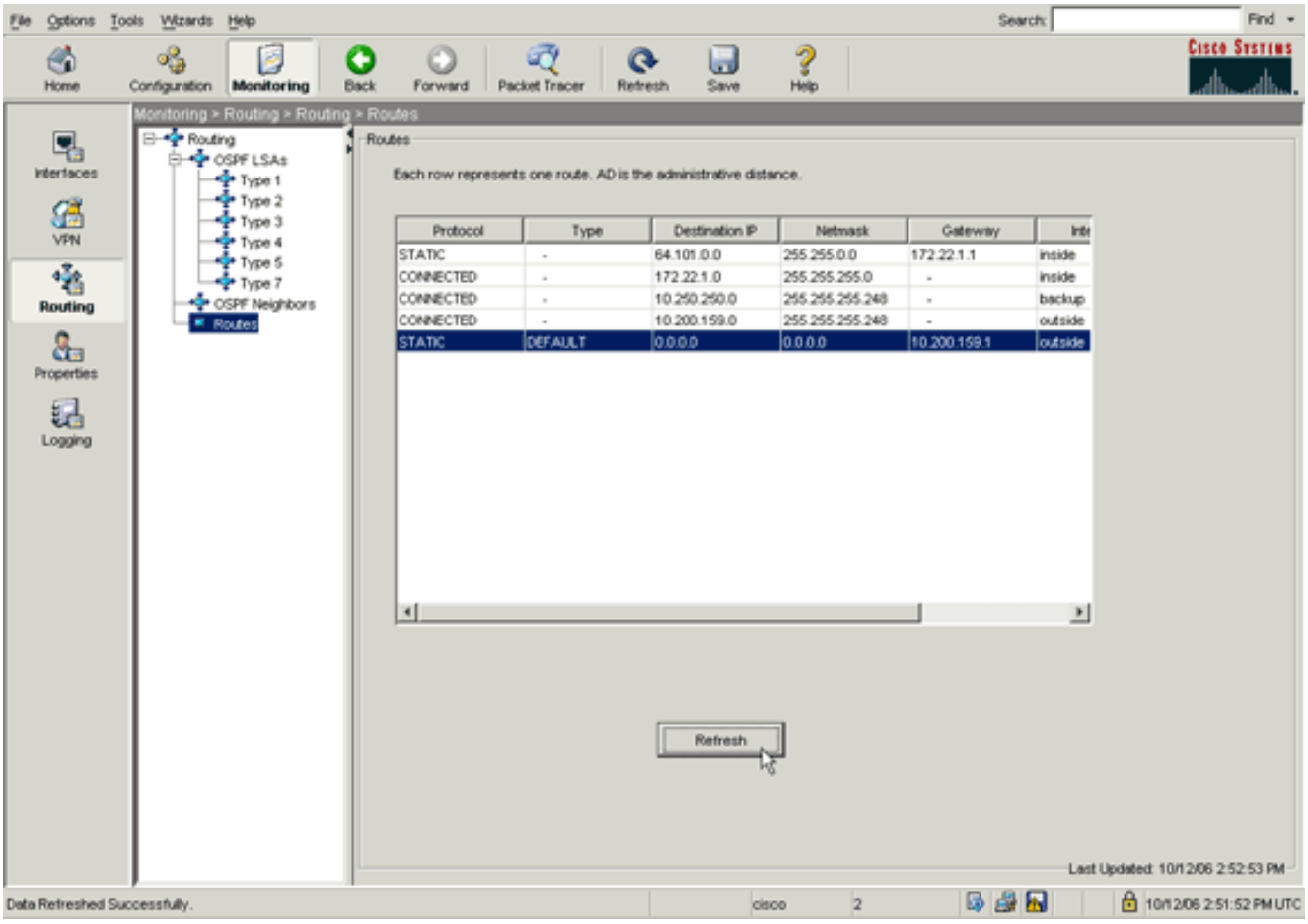
- Après que l'ISP primaire a échoué, que la route statique est retirée et que la route de secours est installée, la table de routage est la suivante :

```
pix(config)# 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 10.250.250.1 to network 0.0.0.0

S    64.101.0.0 255.255.0.0 [1/0] via 172.22.1.1, inside
C    172.22.1.0 255.255.255.0 is directly connected, inside
C    10.250.250.0 255.255.255.248 is directly connected, backup
C    10.200.159.0 255.255.255.248 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [254/0] via 10.250.250.1, backup
```

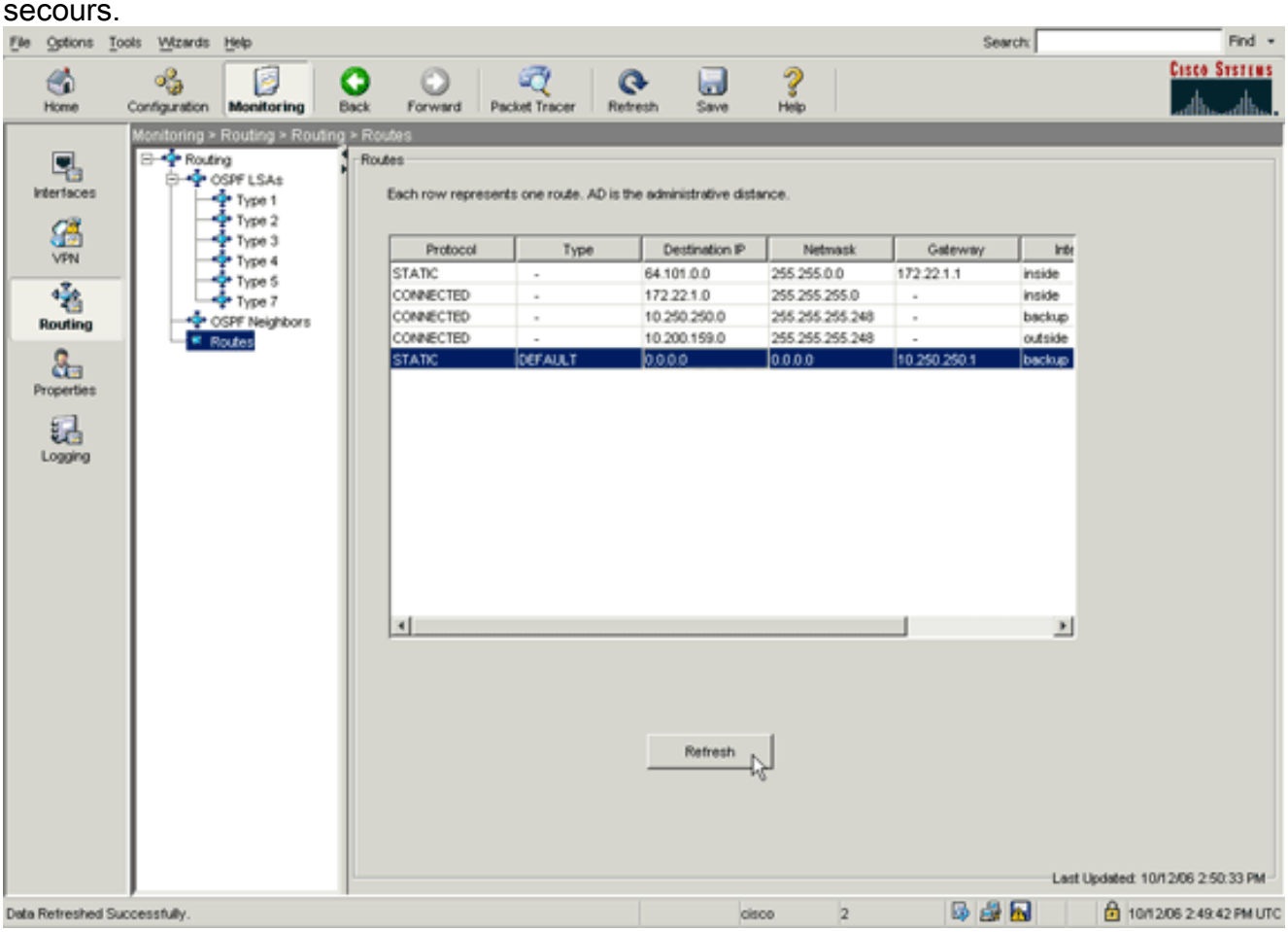
Confirmez que la route de secours est installée (méthode ASDM)

Afin de confirmer avec l'ASDM que la route de secours est installée, complétez ces étapes :

1. Cliquez sur **Monitoring**, puis sur **Routing**.
2. Dans l'arborescence Routing, choisissez **Routes**.Avant que l'ISP primaire n'échoue, la table de routage est la
   suivante :



La route DEFAULT pointe vers 10.0.0.2 via l'interface externe.Après que l'ISP primaire a échoué, la route est retirée, et la route de secours est installée. La route DEFAULT pointe maintenant vers 10.250.250.1 via l'interface de secours.



Dépannez

Commandes de débogage

- **debug sla monitor trace** - Affiche la progression de l'opération d'écho.L'objet suivi (passerelle de l'ISP primaire) est actif, et les échos ICMP réussissent.

```
pix(config)# 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 10.250.250.1 to network 0.0.0.0

S    64.101.0.0 255.255.0.0 [1/0] via 172.22.1.1, inside
C    172.22.1.0 255.255.255.0 is directly connected, inside
C    10.250.250.0 255.255.255.248 is directly connected, backup
C    10.200.159.0 255.255.255.248 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [254/0] via 10.250.250.1, backup
```

L'objet suivi (passerelle de l'ISP primaire) est inactif, et les échos ICMP échouent.

```
pix(config)# 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 10.250.250.1 to network 0.0.0.0

S    64.101.0.0 255.255.0.0 [1/0] via 172.22.1.1, inside
C    172.22.1.0 255.255.255.0 is directly connected, inside
C    10.250.250.0 255.255.255.248 is directly connected, backup
C    10.200.159.0 255.255.255.248 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [254/0] via 10.250.250.1, backup
```

- **debug sla monitor error** - Affiche les erreurs que le processus de surveillance SLA rencontre.L'objet suivi (passerelle de l'ISP primaire) est actif, et ICMP réussit.

```
pix(config)# 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 10.250.250.1 to network 0.0.0.0

S    64.101.0.0 255.255.0.0 [1/0] via 172.22.1.1, inside
C    172.22.1.0 255.255.255.0 is directly connected, inside
```

```
C    10.250.250.0 255.255.255.248 is directly connected, backup
C    10.200.159.0 255.255.255.248 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [254/0] via 10.250.250.1, backup
```

L'objet suivi (passerelle de l'ISP primaire) est inactif, et la route suivie est retirée.

```
%PIX-7-609001: Built local-host NP Identity Ifc:10.200.159.2
%PIX-7-609001: Built local-host outside:10.0.0.1
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6405 laddr 10.200.159.2/6405
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6406 laddr 10.200.159.2/6406
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6407 laddr 10.200.159.2/6407
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6405 laddr 10.200.159.2/6405
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6406 laddr 10.200.159.2/6406
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6407 laddr 10.200.159.2/6407
%PIX-7-609002: Teardown local-host NP Identity Ifc:10.200.159.2
               duration 0:00:02
%PIX-7-609002: Teardown local-host outside:10.0.0.1 duration 0:00:02
%PIX-6-622001: Removing tracked route 0.0.0.0 0.0.0.0 10.200.159.1,
               distance 1, table Default-IP-Routing-Table, on interface
               outside
!--- 10.0.0.1 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 qui est située au-delà de la passerelle de l'ISP, une autre liaison le long de cette route peut échouer ou un autre périphérique peut interférer. Cette configuration peut faire en sorte que le processus de surveillance SLA conclue que la connexion à l'ISP primaire a échoué et entraîner le basculement inutile du dispositif de sécurité sur la liaison ISP 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 qui sont envoyés par l'opération de surveillance ont échoué, la route suivie primaire est retirée, bien que la liaison ISP primaire soit 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 assure que si les échos ICMP qui sont envoyés par l'opération de surveillance échouent, il est presque certain que la liaison ISP est inactive.

Surveillance SLA sur ASA

Problème :

La surveillance SLA ne fonctionne pas après la mise à niveau de l'ASA vers la version 8.0.

Solution :

Le problème est probablement dû à la commande **IP Reverse Path** configurée dans l'**interface OUTSIDE**. Supprimez la commande dans ASA et essayez de vérifier la surveillance SLA.

Informations connexes

- Configuration du suivi des routes statiques
- Référence des commandes PIX/ASA 7.2
- Dispositifs de sécurité de la gamme Cisco ASA 5500
- Dispositifs de sécurité de la gamme Cisco PIX 500
- Support et documentation techniques - Cisco Systems