Configurez l'ASA pour les liens redondants ou de sauvegarde ISP

Contenu

Introduction

Ce document décrit comment configurer l'appliance de sécurité adaptatif de la gamme Cisco ASA 5500 (ASA) pour l'usage de la caractéristique de suivi des routes statiques afin de permettre au périphérique d'utiliser les connexions Internet redondantes ou de sauvegarde.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Gamme 5555-X de Cisco ASA qui exécute la version de logiciel 9.x ou plus tard
- Version 7.x ou ultérieures de Cisco ASDM

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 la version 9.1(5) de gamme de Cisco ASA 5500.

> Remarque: **La commande backup interface** est exigée afin de configurer la quatrième interface sur la gamme ASA 5505. Référez-vous à la section d'Interface de sauvegarde de la *référence de commandes d'appareils de sécurité Cisco,* pour en savoir plus de *version 7.2*.

Informations générales

Cette section fournit un aperçu de la caractéristique de suivi des routes statiques qui est décrite dans ce document, aussi bien que quelques importantes recommandations avant que vous commenciez.

Vue d'ensemble des fonctionnalités de suivi des routes statiques

Un problème avec l'utilisation des artères statiques est qu'aucun mécanisme inhérent n'existe qui peut déterminer si l'artère est en haut ou en bas. 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 caractéristique de suivi des routes statiques est utilisée afin de dépister la Disponibilité d'une artère statique. La caractéristique retire l'artère statique de la table de routage et la remplace par une route de secours lors de la panne.

Le suivi des routes statiques permet à l'ASA pour utiliser une connexion peu coûteuse à un ISP secondaire au cas où la ligne louée primaire deviendrait indisponible. Afin de réaliser cette Redondance, l'ASA associe une artère statique avec une cible de surveillance que vous définissez. L'exécution d'accord de niveau de service (SLA) surveille la cible avec des requêtes d'écho périodiques d'ICMP. Si une réponse d'écho n'est pas reçue, alors l'objet est considéré vers le bas, et l'artère 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'exécution de moniteur de SLA continue 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 qui est utilisé dans ce document, l'ASA met à jour 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 d'abonné numérique plus à vitesse réduite (DSL) qui est accédée à par un modem DSL fourni par l'ISP secondaire.

> Remarque: La configuration qui est décrite dans ce document ne peut pas être utilisée pour l'Équilibrage de charge ou le chargement partageant, 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 l'ISP primaire, et puis l'ISP secondaire si le primaire échoue. 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 à l'ISP primaire descend, l'ASA change la table de routage afin de se diriger le trafic à la connexion DSL. Le suivi des routes statiques est utilisé afin de réaliser cette Redondance.

L'ASA est configurée avec une artère statique qui dirige tout les trafic Internet vers l'ISP primaire. Toutes les dix secondes, les contrôles de processus de surveillance de SLA afin de confirmer que la passerelle primaire ISP 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 relativement une méthode économique de s'assurer que l'accès Internet sortant demeure disponible aux utilisateurs derrière l'ASA. Comme décrit dans ce document, cette installation ne pourrait pas convenir à l'accès entrant aux ressources derrière l'ASA. Des compétences de mise en réseau avancées sont exigées afin de réaliser les connexions entrantes sans couture. Ces qualifications ne sont pas couvertes dans ce document.

Importantes recommandations

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

- L'adresse de la passerelle ISP
- Une autre adresse gérée par l'ISP
- Un serveur sur un autre réseau, tel qu'un serveur d'Authentification, autorisation et comptabilité (AAA) 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 complètement opérationnelle et configurée afin de permettre au Cisco Adaptive Security Device Manager (ASDM) pour apporter des modifications de configuration.

> **Conseil** : Pour des informations sur la façon permettre à l'ASDM pour configurer le périphérique, référez-vous au HTTPS configurant Access pour la section ASDM de l'*ouvrage 1 CLI : Guide de configuration général CLI d'exécutions de gamme de Cisco ASA, 9.1*.

Configurez

Utilisez les informations qui sont décrites dans cette section afin de configurer l'ASA pour l'usage de la caractéristique de suivi des routes statiques.

> Remarque: Utilisez le Command Lookup Tool (clients enregistrés seulement) afin d'obtenir plus d'informations sur les commandes qui sont utilisées dans cette section.

> Remarque: Les adresses IP qui sont utilisées dans cette configuration ne sont pas légalement routable sur l'Internet. Ils sont les adresses RFC 1918, qui sont utilisées dans un environnement de travaux pratiques.

Diagramme du réseau

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

Configuration CLI

Employez ces informations afin de configurer l'ASA par l'intermédiaire du 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

Terminez-vous ces étapes afin de configurer le support redondant ou de sauvegarde ISP avec l'application ASDM :

1. Dans l'application ASDM, la **configuration de** clic, et cliquent sur alors des **interfaces**.

2. **GigabitEthernet0/1** choisis des interfaces les répertorient, et puis cliquent sur Edit. Cette boîte de dialogue apparaît :

3. Cochez la case d'**interface d'enable**, et écrivez les valeurs appropriées dans les domaines de *nom d'interface*, de *niveau de Sécurité*, d'*adresse IP*, et de *masque de sous-réseau*.

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

5. Configurez les autres interfaces comme nécessaire, et puis cliquez sur Apply afin de mettre à jour la configuration ASA :

6. **Artères** choisies de **charge statique de routage** et de clic situées du 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 primaire ISP et **4.2.2.2** est l'objet à surveiller avec des échos d'ICMP.

9. Dans la région d'options, cliquez sur la case d'option **dépistée** et écrivez les valeurs appropriées dans l'*ID de piste*, l'*ID de SLA*, et les domaines d'*adresse IP de piste*.

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

11. Écrivez les valeurs appropriées pour la fréquence et d'autres options de surveillance, et 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 artère secondaire (ISP secondaire) est installée dans la table de routage du Private Internet Exchange (PIX) 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, et puis cliquez sur Apply afin de mettre à jour la configuration ASA.

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Confirmez que la configuration est complète

> Remarque: L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Employez ces **commandes show** afin de vérifier que votre configuration est complète :

- **moniteur de sla de show running-config** – La sortie de cette commande affiche les commandes de 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
```

- **affichez la configuration de moniteur de sla** – La sortie de cette commande affiche les configurations de configuration en cours de l'exécution.

```
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:
```

- **affichez l'opérationnel-état de moniteur de sla** – La sortie de cette commande affiche les statistiques opérationnelles de l'exécution de 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
```

  Après que l'ISP primaire échoue (et la minuterie d'échos d'ICMP), c'est 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
```

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

Sélectionnez la commande de **show route** afin de confirmer que la route de secours est installée.

Avant que l'ISP primaire échoue, la table de routage ressemble à ceci :

```
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 que l'ISP primaire échoue, l'artère statique est retirée, et la route de secours est installée, la table de routage ressemble à ceci :

```
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
```

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

Afin de confirmer que la route de secours est installée par l'intermédiaire de l'ASDM, naviguez vers la **surveillance > routage**, et puis choisissez les **artères de l'**arborescence de routage.

Avant que l'ISP primaire échoue, la table de routage ressemble à cela affichée dans la prochaine image. Notez que le **default route** indique **203.0.113.2** par l'interface **extérieure** :

Après que l'ISP primaire échoue, l'artère est retirée et la route de secours est installée. **Le default route** indique maintenant **198.51.100.2** par l'**Interface de sauvegarde** :

Dépannez

Cette section fournit quelques commandes de débogage utiles et décrit comment dépanner une question où l'artère dépistée est retirée inutilement.

Commandes de débogage

Vous pouvez employer ces commandes de débogage afin de dépanner vos questions de configuration :

- **mettez au point le suivi de moniteur de sla** – La sortie de cette commande affiche le déroulement de l'exécution d'écho.

  Si l'objet dépisté (passerelle primaire ISP) est en hausse et les échos d'ICMP réussissent, la sortie ressemble 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 dépisté (passerelle primaire ISP) est en baisse et les échos d'ICMP échouent, la sortie ressemble 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
```

- **mettez au point l'erreur de moniteur de sla** – La sortie de cette commande affiche toutes les erreurs que le processus de surveillance de SLA rencontre.

  Si l'objet dépisté (passerelle primaire ISP) est en hausse et l'ICMP réussit, la sortie ressemble 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 dépisté (passerelle primaire ISP) est en baisse et l'artère dépistée est retiré, la sortie ressemble 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 qui est plus loin partie que la passerelle ISP, un autre lien le long de cette artère pourrait échouer ou un autre périphérique pourrait s'y mêler. Cette configuration pourrait faire conclure que la connexion à l'ISP primaire a manqué et faire le moniteur de SLA basculer inutilement l'ASA au lien secondaire ISP.

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 d'ICMP qui sont envoyés par l'échouer d'opération de contrôle, l'artère dépistée primaire est retirés, quoique le lien primaire ISP soit encore en activité.

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 s'assure que si les échos d'ICMP qui sont envoyés par l'échouer d'opération de contrôle, le lien ISP est presque sûrement vers le bas.

Informations connexes

- Pare-feu de la deuxième génération de gamme 5500-X de Cisco ASA
- Support et documentation techniques - Cisco Systems