ASA : Exemple de configuration pour l'acheminement de trafic réseau entre l'ASA et l'AIP SSM

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Configurez
Diagramme du réseau
Configurations initiales
Examinez tout le trafic avec l'AIP SSM en mode intégré ou promiscueux
Examinez tout le trafic avec l'AIP SSM utilisant l'ASDM
Examinez le trafic spécifique avec l'AIP SSM
Excluez le trafic réseau spécifique de la lecture d'AIP SSM
Vérifiez
Dépannez
Problèmes avec le Basculement
Messages d'erreur
Prise en charge de Syslog
Réinitialisation d'AIP SSM
Alerte par courrier électronique d'AIP SSM
Informations connexes

Introduction

Ce document fournit un exemple de configuration sur la façon d'envoyer le trafic réseau qui traverse les dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500 au module d'Advanced Inspection and Prevention Security Services Module (AIP SSM) (IPS). Des exemples de configuration sont équipés d'interface de ligne de commande (CLI).

Référez-vous à l'ASA : Envoyez le trafic réseau de l'ASA à l'exemple de configuration CSC-SSM afin d'envoyer le trafic réseau de l'appliance de sécurité adaptatif de la gamme Cisco ASA 5500 (ASA) au Content Security and Control Security Services Module (CSC-SSM).

Référez-vous à assigner les capteurs virtuels à un contexte de sécurité (AIP SSM seulement) pour plus d'informations sur la façon envoyer le trafic réseau qui traverse l'appliance de sécurité adaptatif de la gamme Cisco ASA 5500 (ASA) dans le mode de contexte multiple à l'Advanced Inspection and Prevention Security Services Module (AIP SSM) (IPS) module.

Note: Le trafic réseau qui traverse l'ASA inclut les utilisateurs internes qui accèdent à l'Internet ou les internautes qui accèdent à des ressources protégées par ASA dans un réseau de la zone démilitarisée (DMZ) ou de l'intérieur. Le trafic réseau envoyé à et de l'ASA n'est pas envoyé au module IPS pour l'inspection. Un exemple du trafic non envoyé au module IPS inclut le PING (ICMP) les interfaces ou Telnetting ASA à l'ASA.

Note: Le cadre de stratégie modulaire utilisé par l'ASA afin de classifier le trafic pour l'inspection ne prend en charge pas l'IPv6. Ainsi si vous détournez le trafic d'IPv6 à l'AIP SSM par l'ASA, il n'est pas pris en charge.

Note: Pour plus d'informations sur la configuration initiale de l'AIP SSM, référez-vous à la configuration initiale du capteur d'AIP SSM.

Conditions préalables

Conditions requises

Ce document suppose que le public a une compréhension de base de la façon configurer la version de logiciel 8.x de Cisco ASA et la version de logiciel 6.x IPS.

- Les composants nécessaires de configuration pour ASA 8.x incluent des interfaces, des Listes d'accès, le Traduction d'adresses de réseau (NAT), et le routage.
- Les composants nécessaires de configuration pour l'AIP SSM (logiciel 6.x IPS) incluent la configuration réseau, permise des hôtes, la configuration d'interface, des définitions de signature, et des règles d'action d'événement.

Composants utilisés

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

- ASA 5510 avec la version de logiciel 8.0.2
- AIP-SSM-10 avec la version de logiciel 6.1.2 IPS

Note: Cet exemple de configuration est compatible avec n'importe quel Pare-feu de gamme de Cisco ASA 5500 avec OS 7.x et plus tard et le module d'AIP SSM avec IPS 5.x et plus tard.

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez

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

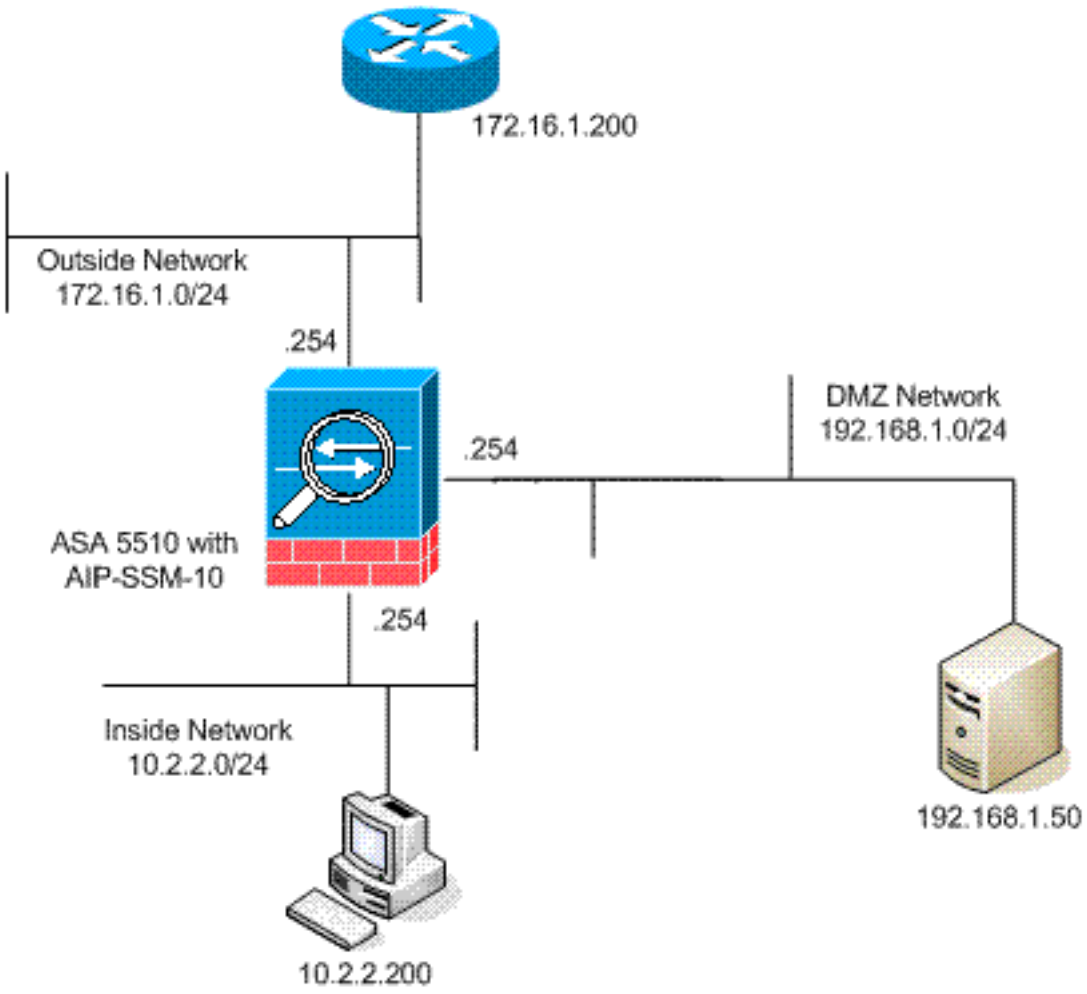
document.

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

Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisés dans un environnement de laboratoire.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations initiales

Ce document utilise les configurations suivantes. Le début ASA et d'AIP SSM avec une configuration par défaut mais ont les modifications spécifiques apportées afin de tester. Des ajouts sont notés dans la configuration.

- ASA 5510
- AIP SSM (IPS)

ASA 5510

```
ciscoasa#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ciscoasa
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
!--- IP addressing is added to the default
configuration. interface Ethernet0/0 nameif outside
security-level 0 ip address 172.16.1.254 255.255.255.0 !
interface Ethernet0/1 nameif inside security-level 100
ip address 10.2.2.254 255.255.255.0 ! interface
Ethernet0/2 nameif dmz security-level 50 ip address
192.168.1.254 255.255.255.0 ! interface Management0/0
nameif management security-level 0 ip address
172.22.1.160 255.255.255.0 management-only ! passwd
9jNfZuG3TC5tCVH0 encrypted ftp mode passive !--- Access
lists are added in order to allow test !--- traffic
(ICMP and Telnet). access-list acl_outside_in extended
permit icmp any host 172.16.1.50 access-list
acl_inside_in extended permit ip 10.2.2.0 255.255.255.0
any access-list acl_dmz_in extended permit icmp
192.168.1.0 255.255.255.0 any pager lines 24 !---
Logging is enabled. logging enable logging buffered
debugging mtu outside 1500 mtu inside 1500 mtu dmz 1500
mtu management 1500 asdm image disk0:/asdm-613.bin no
asdm history enable arp timeout 14400 !--- Translation
rules are added. global (outside) 1 172.16.1.100 global
(dmz) 1 192.168.1.100 nat (inside) 1 10.2.2.0
255.255.255.0 static (dmz,outside) 172.16.1.50
192.168.1.50 netmask 255.255.255.255 static (inside,dmz)
10.2.2.200 10.2.2.200 netmask 255.255.255.255 !---
Access lists are applied to the interfaces. access-group
acl_outside_in in interface outside access-group
acl_inside_in in interface inside access-group
acl_dmz_in in interface dmz 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 http
server enable http 0.0.0.0 0.0.0.0 dmz no snmp-server
location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart 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 !---
Out-of-the-box default configuration includes !---
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 !--- Out-of-the-box default
configuration includes !--- the service-policy
global_policy applied globally. prompt hostname context
. : end
```

AIP SSM (IPS)

```
AIP-SSM#show configuration
! ------------------------------
! Version 6.1(2)
! Current configuration last modified Mon Mar 23
21:46:47 2009
! ------------------------------
service interface
exit
! ------------------------------
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/1
exit
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
!--- The variables are defined. variables DMZ address
192.168.1.0-192.168.1.255 variables IN address 10.2.2.0-
10.2.2.255 exit ! ------------------------------ service
host network-settings !--- The management IP address is
set. host-ip 172.22.1.169/24,172.22.1.1 host-name AIP-
SSM telnet-option disabled access-list x.x.0.0/16 !---
The access list IP address is removed from the
configuration !--- because the specific IP address is
not relevant to this document. exit time-zone-settings
offset -360 standard-time-zone-name GMT-06:00 exit
summertime-option recurring offset 60 summertime-zone-
name UTC start-summertime month april week-of-month
first day-of-week sunday time-of-day 02:00:00 exit end-
summertime month october week-of-month last day-of-week
sunday time-of-day 02:00:00 exit exit exit ! ----------
------------------- service logger exit ! -------------
--------------- service network-access exit ! ---------
--------------------- service notification exit ! ------
------------------------ service signature-definition
sig0 !--- The signature is modified from the default
setting for testing purposes. signatures 2000 0 alert-
severity high engine atomic-ip event-action produce-
alert|produce-verbose-alert exit alert-frequency
summary-mode fire-all summary-key AxBx exit exit status
enabled true exit exit !--- The signature is modified
from the default setting for testing purposes.
signatures 2004 0 alert-severity high engine atomic-ip
event-action produce-alert|produce-verbose-alert exit
alert-frequency summary-mode fire-all summary-key AxBx
exit exit status enabled true exit exit !--- The custom
signature is added for testing purposes. signatures
60000 0 alert-severity high sig-fidelity-rating 75 sig-
description sig-name Telnet Command Authorization
Failure sig-string-info Command authorization failed
sig-comment signature triggers string command
authorization failed exit engine atomic-ip specify-l4-
protocol yes l4-protocol tcp no tcp-flags no tcp-mask
exit specify-payload-inspection yes regex-string Command
authorization failed exit exit exit exit exit ! --------
---------------------- service ssh-known-hosts exit ! --
---------------------------- service trusted-
certificates exit ! ------------------------------
service web-server enable-tls true exit AIP-SSM#
```

Note: Si vous êtes accès incapable le module d'AIP SSM avec des https, alors terminez-vous ces étapes :

- Configurez une adresse IP de Gestion pour le module. Et vous pouvez configurer la `liste d'accès au réseau`, dans laquelle vous spécifiez les réseaux IPs/IP qui sont permis pour se connecter à l'IP de Gestion.
- Assurez-vous que vous avez connecté l'interface Ethernet externe du module AIP. L'accès de Gestion au module AIP est possible par cette interface seulement.

Référez-vous à initialiser le pour en savoir plus d'AIP SSM.

Examinez tout le trafic avec l'AIP SSM en mode intégré ou promiscueux

Les administrateurs réseau et les seniors management de société indiquent souvent que tout doit être surveillé. Cette configuration répond à l'exigence de surveiller tout. En plus de surveiller tout, deux décisions doivent être prises au sujet de la façon dont l'ASA et l'AIP SSM interactifs.

- Le module d'AIP SSM à fonctionner ou déployer est-il en mode promiscueux ou intégré ?Le mode promiscueux signifie qu'une copie des données est envoyée à l'AIP SSM tandis que l'ASA en avant les données d'origine en fonction à la destination. L'AIP SSM en mode promiscueux peut être considéré un système de détection d'intrusions (ID). En ce mode, le paquet de déclencheur (le paquet qui entraîne l'alarme) peut encore atteindre la destination. L'évitement peut avoir lieu et arrêter les paquets supplémentaires d'atteindre la destination, toutefois le paquet de déclencheur n'est pas arrêté.Le mode intégré signifie que l'ASA en avant les données à l'AIP SSM pour l'inspection. Si les données passent l'inspection d'AIP SSM, les données reviennent à l'ASA afin de continuer à être traité et envoyé à la destination. L'AIP SSM en mode intégré peut être considéré un Système de prévention d'intrusion (IPS). À la différence du mode promiscueux, le mode intégré (IPS) peut réellement arrêter le paquet de déclencheur d'atteindre la destination.
- Au cas où l'ASA ne pourrait pas communiquer avec l'AIP SSM, comment le traitement ASA à-être-examiné devrait-il trafiquer ? Les exemples des exemples quand l'ASA ne peut pas communiquer avec l'AIP SSM incluent des recharges d'AIP SSM ou si le module échoue et a besoin de remplacement. Dans ce cas l'ASA peut échec-ouvert ou échec-fermé.Échec-ouvert permet à l'ASA pour continuer à passer le trafic à-être-examiné à la destination définitive si l'AIP SSM ne peut pas être atteint.les blocs Échec-fermés à-être-examinés trafiquent quand l'ASA ne peut pas communiquer avec l'AIP SSM.**Note**: Le trafic à-être-examiné est défini avec l'utilisation d'une liste d'accès. Dans cet exemple de sortie, la liste d'accès permet tout le trafic IP de n'importe quelle source à n'importe quelle destination. Par conséquent, le trafic à-être-examiné peut être quelque chose qui traverse l'ASA.

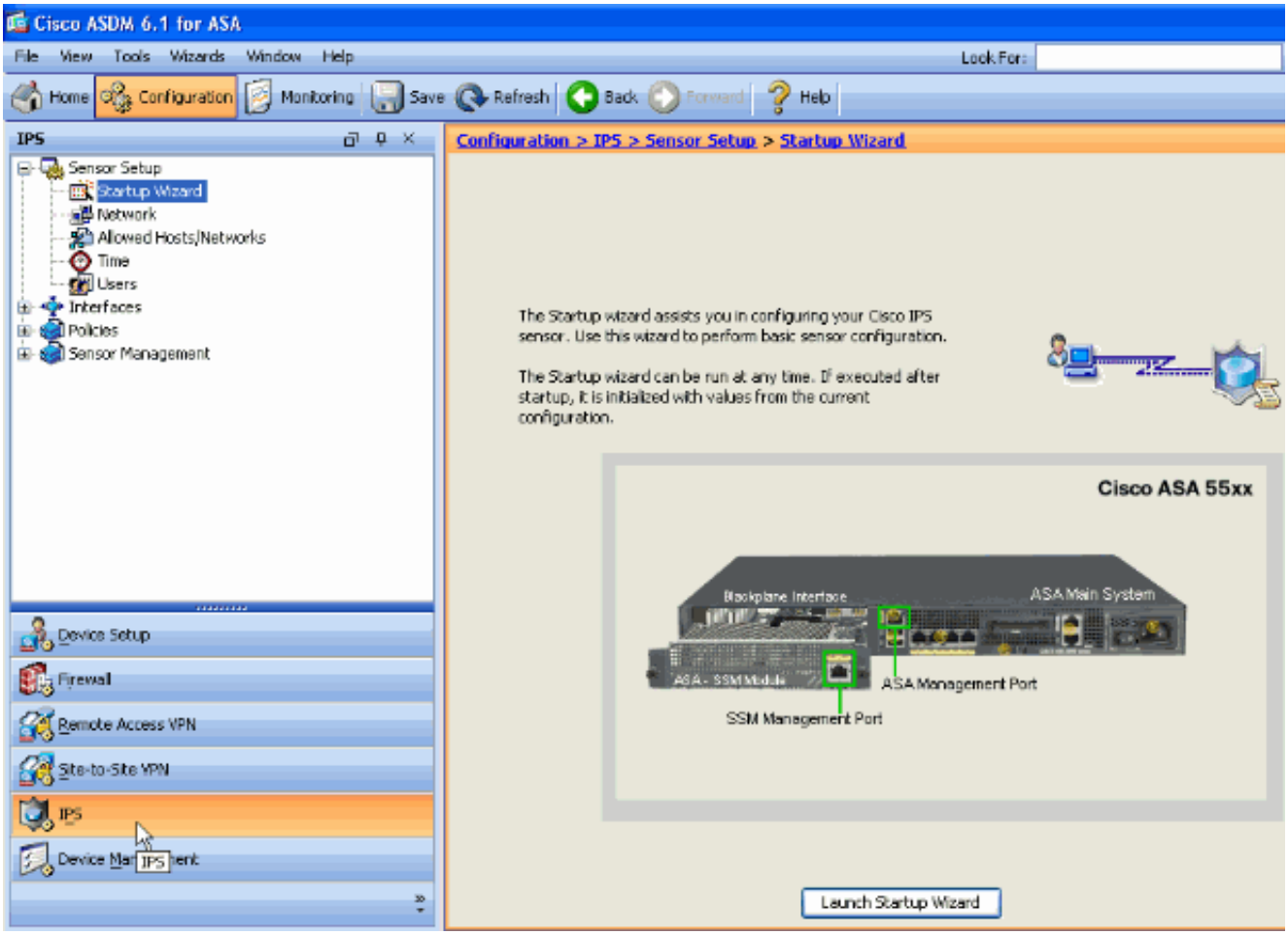
```
ciscoasa(config)#access-list traffic_for_ips permit ip any any
ciscoasa(config)#class-map ips_class_map
ciscoasa(config-cmap)#match access-list traffic_for_ips
!--- The match any command can be used in place of !--- the match access-list [access-list name]
command. !--- In this example, access-list traffic_for_ips permits !--- all traffic. The match
any command also !--- permits all traffic. You can use either configuration. !--- When you
define an access-list, it can ease troubleshooting.

ciscoasa(config)#policy-map global_policy
!--- Note that policy-map global_policy is a part of the !--- default configuration. In
addition, policy-map global_policy !--- is applied globally with the service-policy command.
```

```
ciscoasa(config-pmap)#class ips_class_map
ciscoasa(config-pmap-c)#ips inline fail-open
!--- Two decisions need to be made. !--- First, does the AIP-SSM function !--- in inline or
promiscuous mode? !--- Second, does the ASA fail-open or fail-closed? ciscoasa(config-pmap-
c)#ips promiscous fail-open
!--- If AIP-SSM is in promiscous mode, issue !--- the no ips promiscous fail-open command !---
in order to negate the command and then use !--- the ips inline fail-open command.
```

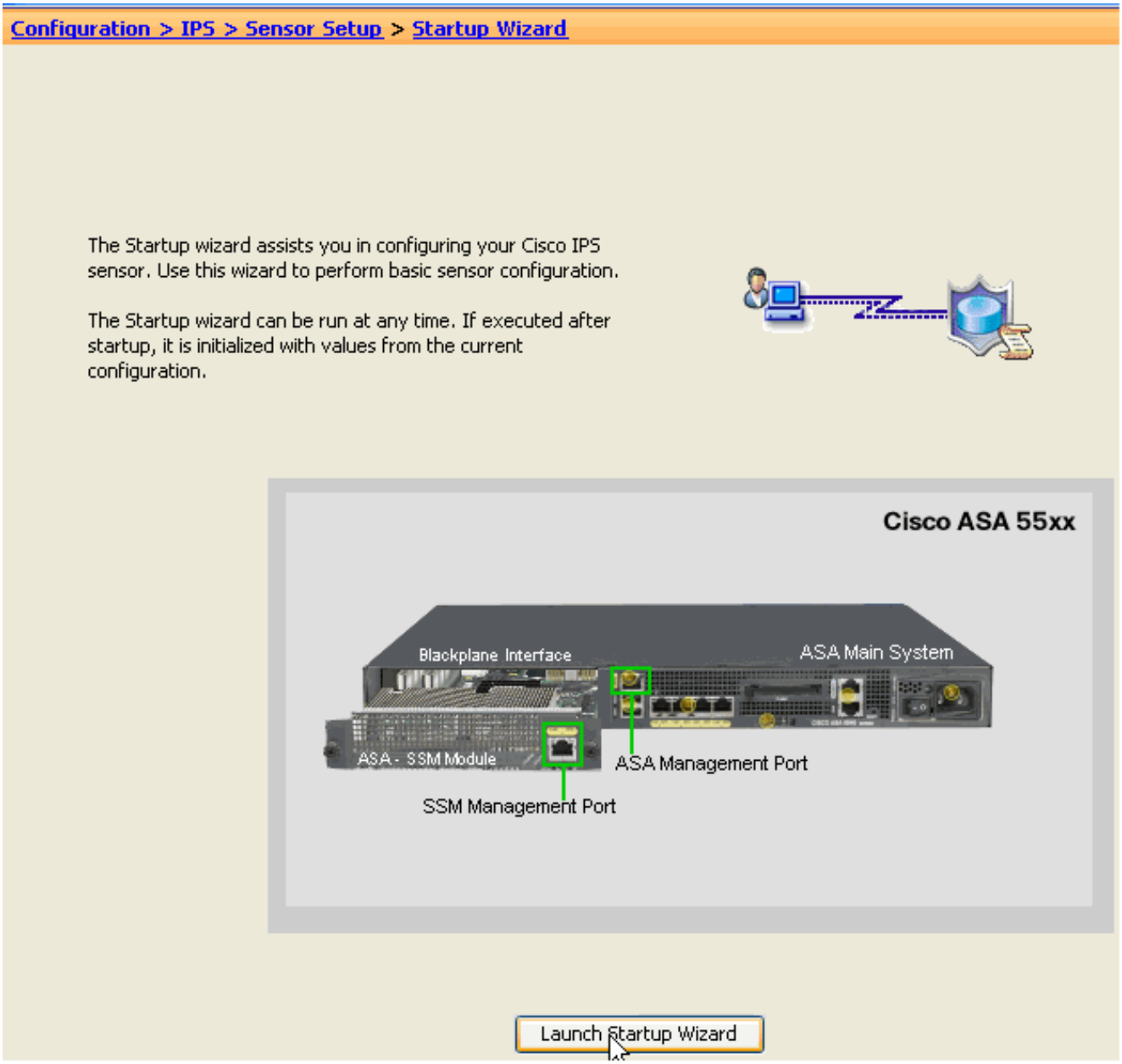
Examinez tout le trafic avec l'AIP SSM utilisant l'ASDM

Terminez-vous ces étapes afin d'examiner tout le trafic avec l'AIP SSM qui utilise l'ASDM :.

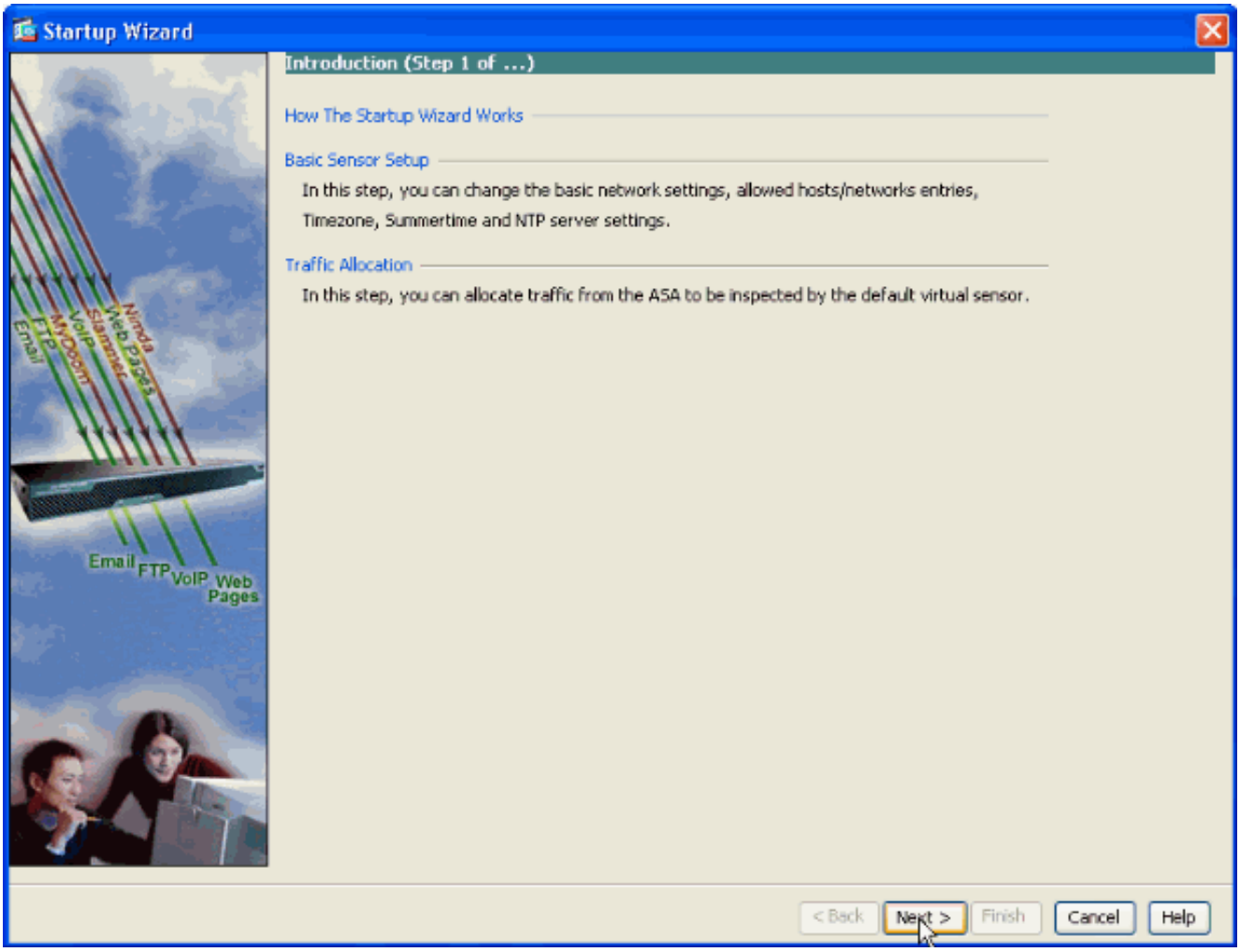
1. Choisissez la **configuration > l'IPS > le capteur installé > assistant de startup** en page d'accueil ASDM pour commencer la configuration, comme affiché :



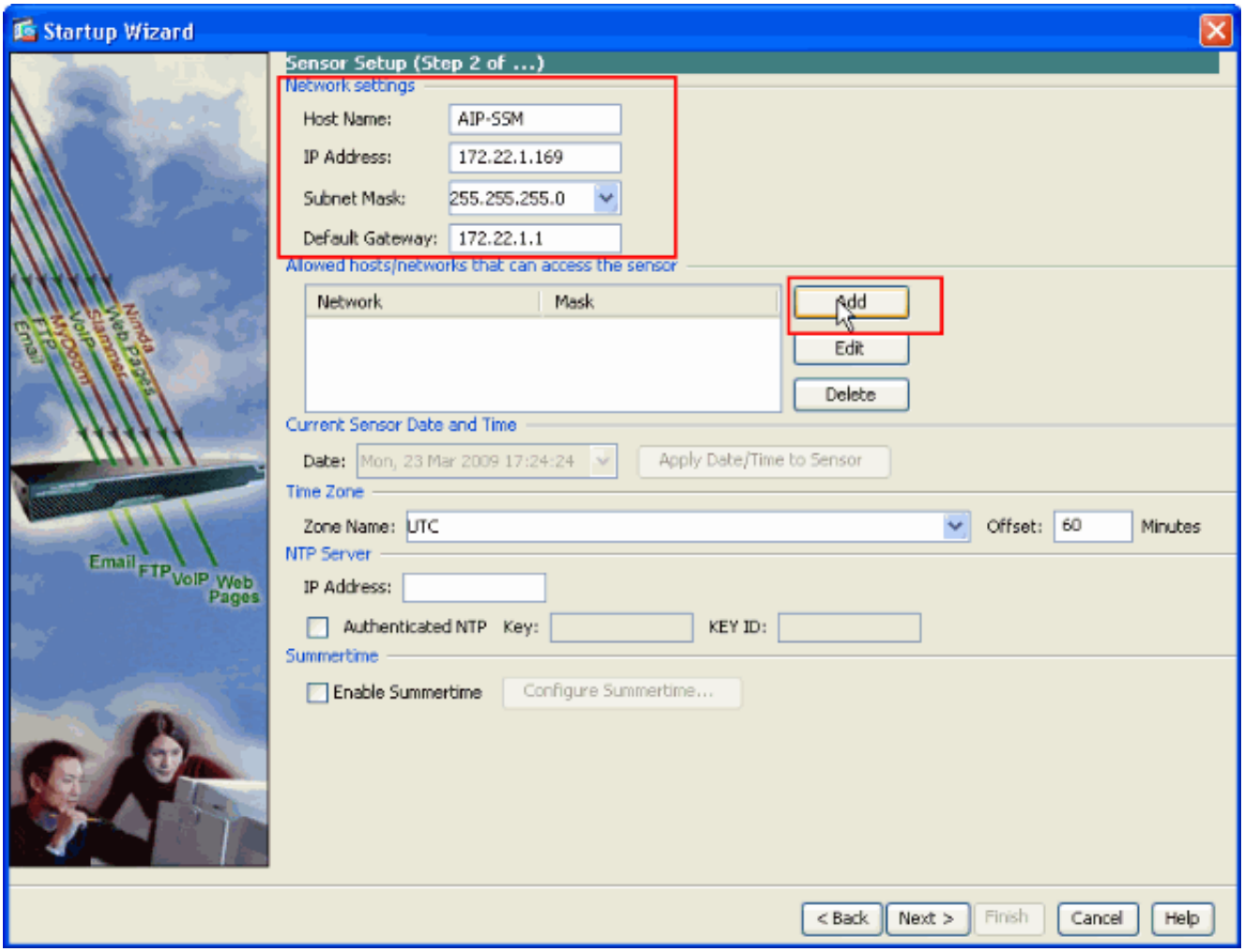
2. **Assistant de startup de lancement de** clic.



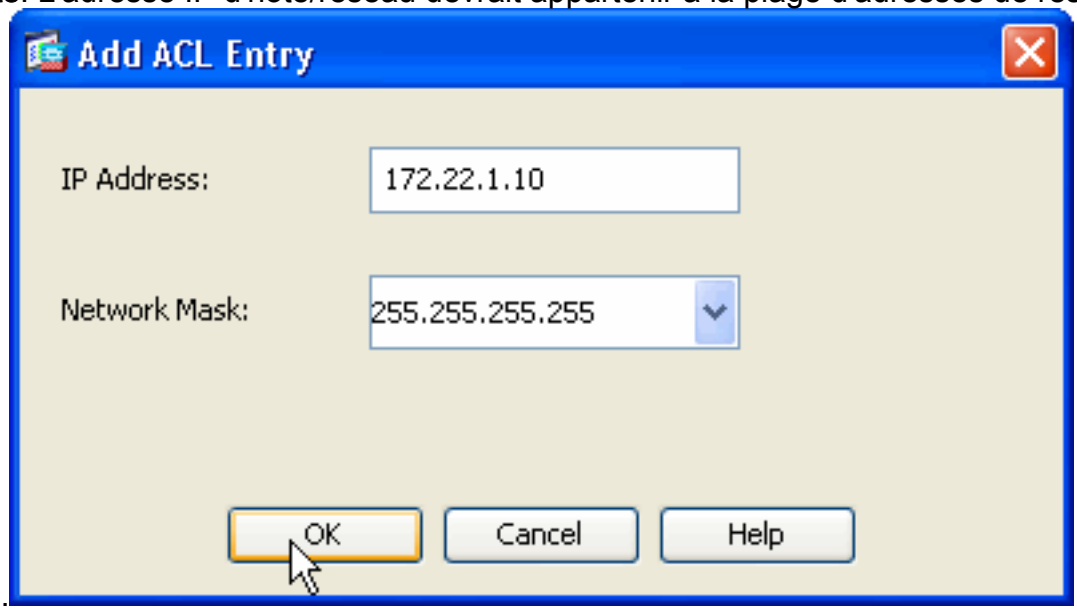
3. Cliquez sur Next dans la nouvelle fenêtre qui monte après que vous lanciez l'assistant de démarrage.



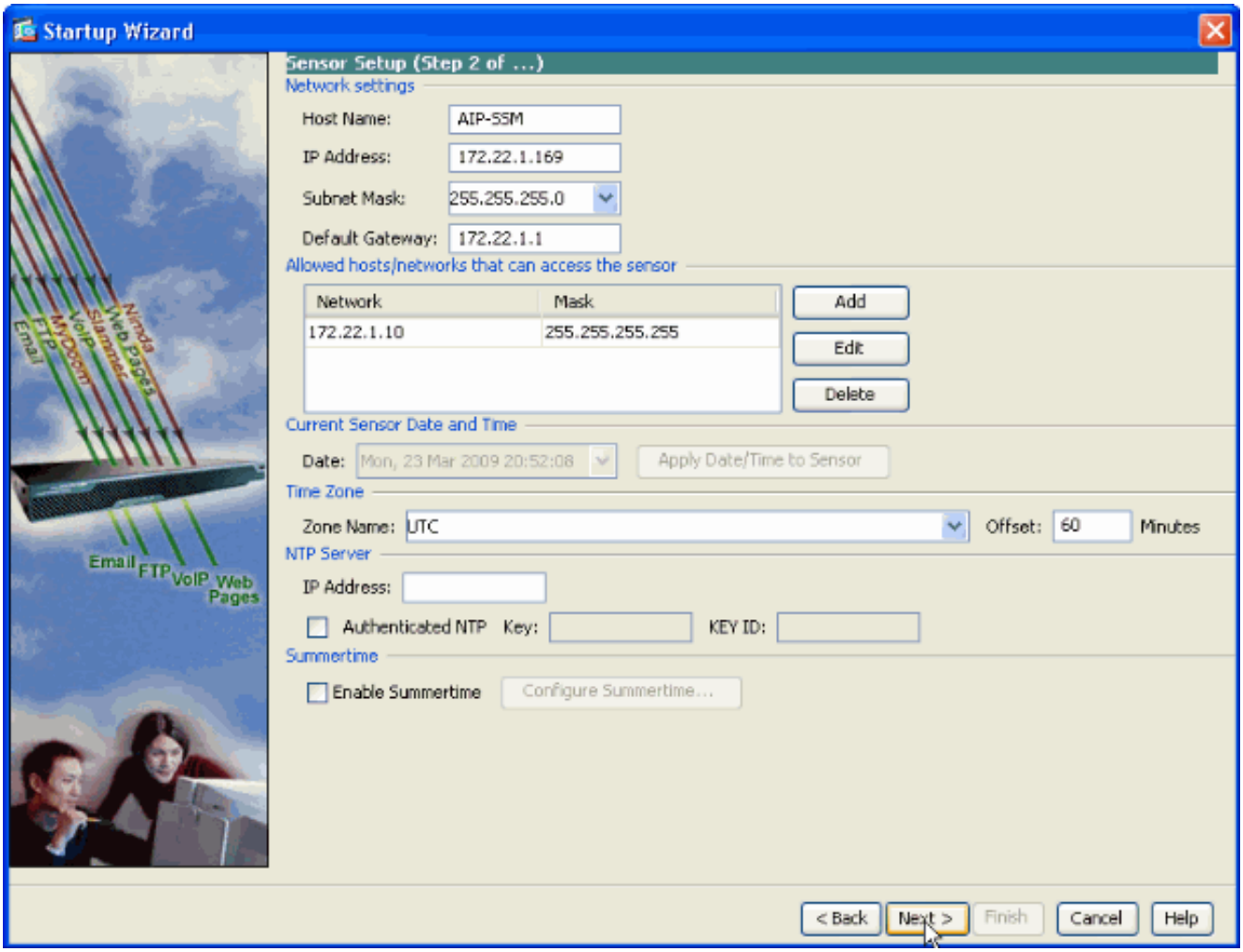
4. Dans la nouvelle fenêtre, fournissez le nom d'hôte, l'adresse IP, le masque de sous-réseau et l'adresse de passerelle par défaut pour le module d'AIP SSM dans l'espace prévu respectif sous la section de paramètres réseau. Cliquez sur Add alors afin d'ajouter les Listes d'accès pour permettre tout le trafic avec l'AIP
SSM.



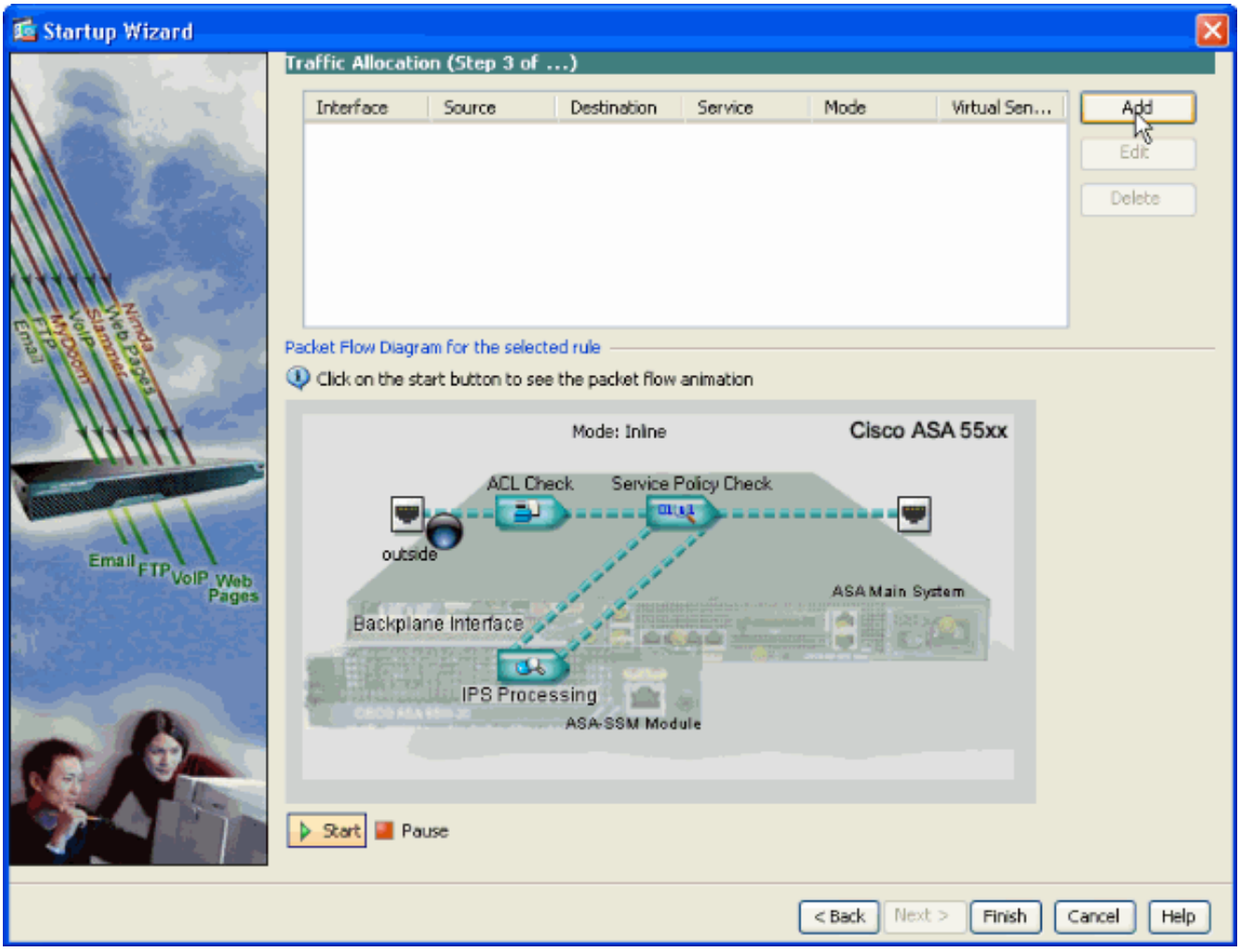
5. Dans la fenêtre de **rubrique de liste ACL d'ajouter** fournissez l'**adresse IP** et les détails de **masque de réseau des** hôtes/des réseaux à laisser accéder au capteur. Cliquez sur **OK**.**Note**: L'adresse IP d'hôte/réseau devrait appartenir à la plage d'adresses de réseau de gestion.



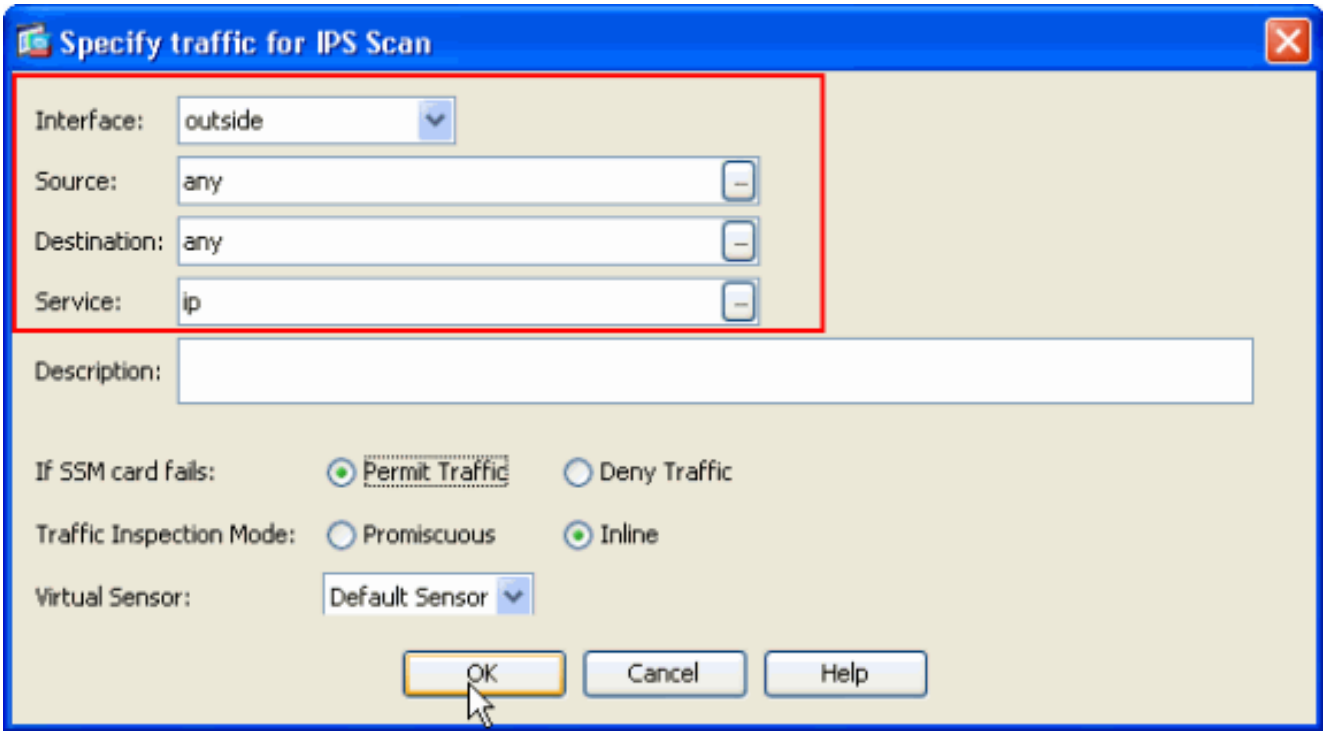
6. Cliquez sur Next après que vous fournissiez les détails dans les espaces respectifs fournis.



7. Cliquez sur Add afin de configurer les détails d'allocation du trafic.

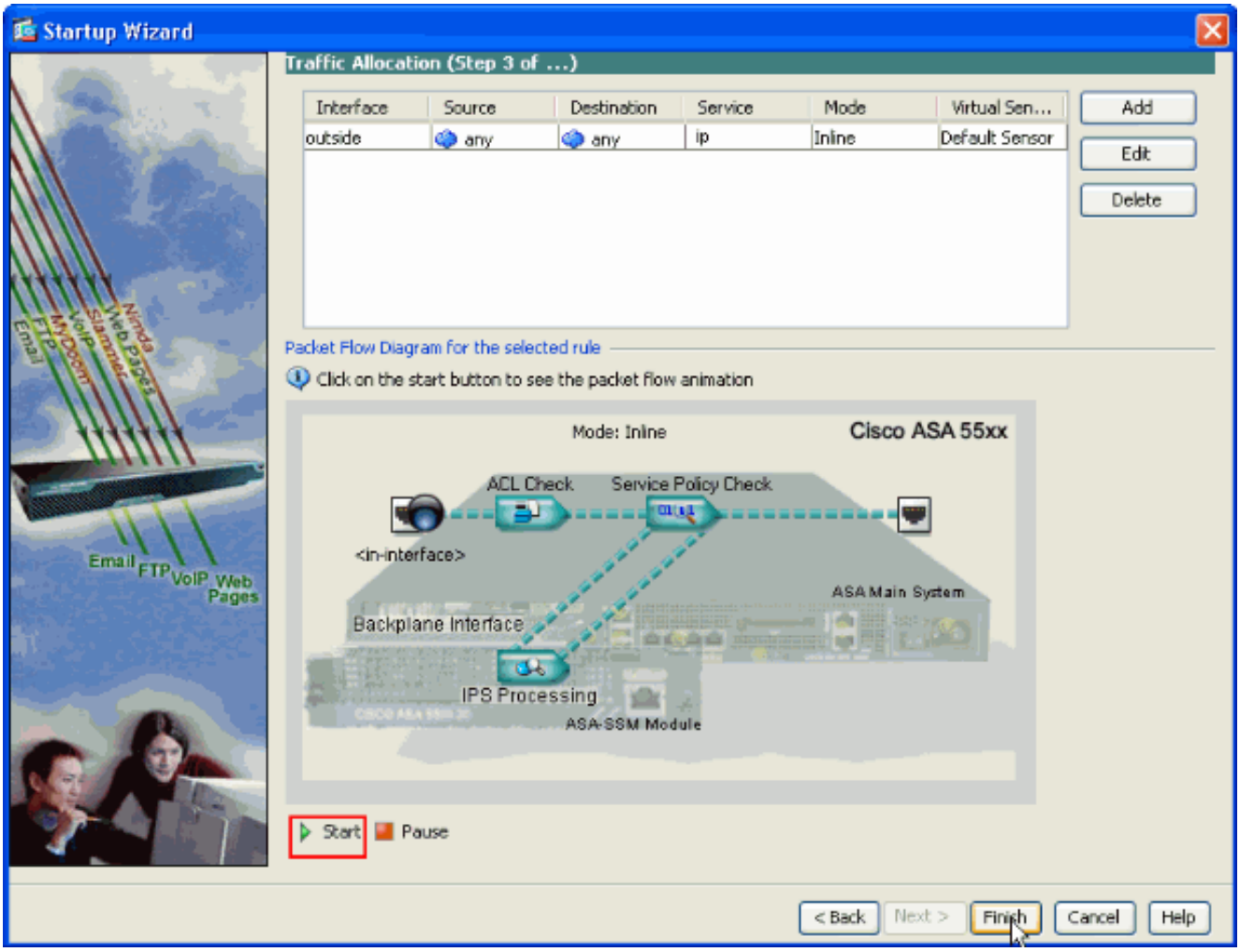


8. Fournissez la source et l'adresse réseau de destination et également le type de service, par exemple, IP est utilisée ici. Dans cet exemple, en est utilisé pour la source et la destination pendant que vous examinez tout le trafic avec l'AIP SSM. Cliquez ensuite sur **OK**.



9. Des règles configurées d'allocation du trafic sont affichées dans cette fenêtre et vous pouvez ajouter autant de règles pendant que nécessaire si vous remplissez la même procédure comme expliqué dans les étapes 7 et 8. Cliquez sur Finish alors et ceci remplit la procédure

de configuration ASDM.**Note**: Vous pouvez visualiser l'animation d'écoulement de paquet si vous cliquez sur en fonction le
début.



Examinez le trafic spécifique avec l'AIP SSM

Au cas où l'administrateur réseau voudrait avoir le moniteur d'AIP SSM comme sous-ensemble de tout le trafic, l'ASA a deux variables indépendantes qui peuvent être modifiées. D'abord, la liste d'accès peut être écrite pour inclure ou exclure le trafic nécessaire. En plus de la modification des Listes d'accès, une service-**stratégie** peut être appliquée à une interface ou globalement afin de changer le trafic examiné par l'AIP SSM.

Concernant le schéma de réseau dans ce document, l'administrateur réseau veut que l'AIP SSM examine *tout le* trafic entre le réseau et le réseau DMZ extérieurs.

```
ciscoasa#configure terminal
ciscoasa(config)#access-list traffic_for_ips deny ip 10.2.2.0 255.255.255.0 192.168.1.0
255.255.255.0
ciscoasa(config)#access-list traffic_for_ips permit ip any 192.168.1.0 255.255.255.0
ciscoasa(config)#access-list traffic_for_ips deny ip 192.168.1.0 255.255.255.0 10.2.2.0
255.255.255.0
ciscoasa(config)#access-list traffic_for_ips permit ip 192.168.1.0 255.255.255.0 any
ciscoasa(config)#class-map ips_class_map
ciscoasa(config-cmap)#match access-list traffic_for_ips
ciscoasa(config)#policy-map interface_policy
ciscoasa(config-pmap)#class ips_class_map
ciscoasa(config-pmap-c)#ips inline fail-open
```

```
ciscoasa(config)#service-policy interface_policy interface dmz
!--- The access-list denies traffic from the inside network to the DMZ network !--- and traffic
to the inside network from the DMZ network. !--- In addition, the service-policy command is
applied to the DMZ interface.
```

Ensuite, l'administrateur réseau veut que l'AIP SSM surveille le trafic *initié du* réseau intérieur au réseau extérieur. Le réseau intérieur au réseau DMZ n'est pas surveillé.

Note: Cette section particulière exige une compréhension intermédiaire de statefulness, de TCP, d'UDP, d'ICMP, de connexion, et de transmissions sans connexion.

```
ciscoasa#configure terminal
ciscoasa(config)#access-list traffic_for_ips deny ip 10.2.2.0 255.255.255.0 192.168.1.0
255.255.255.0
ciscoasa(config)#access-list traffic_for_ips permit ip 10.2.2.0 255.255.255.0 any
ciscoasa(config)#class-map ips_class_map
ciscoasa(config-cmap)#match access-list traffic_for_ips
ciscoasa(config)#policy-map interface_policy
ciscoasa(config-pmap)#class ips_class_map
ciscoasa(config-pmap-c)#ips inline fail-open
ciscoasa(config)#service-policy interface_policy interface inside
```

La liste d'accès refuse le trafic initié sur le réseau intérieur destiné pour le réseau DMZ. La deuxième ligne de liste d'accès permet ou envoie le trafic initié sur le réseau intérieur destiné pour le réseau extérieur à l'AIP SSM. En ce moment le statefulness de l'ASA entre dans le jeu. Par exemple, un utilisateur interne initie une connexion TCP (telnet) à un périphérique sur le réseau extérieur (routeur). L'utilisateur se connecte avec succès au routeur et aux logins. L'utilisateur émet alors une commande de routeur qui n'est pas autorisée. Le routeur répond avec l'`authorizaton de commande a manqué`. Le paquet de données qui contient l'`autorisation de commande a manqué` chaîne a une source du routeur extérieur et d'une destination de l'utilisateur intérieur. La source (dehors) et la destination (à l'intérieur) n'apparient pas les Listes d'accès précédemment définies dans ce document. L'ASA maintient des connexions d'avec état, pour cette raison, le paquet de données qui retourne (externe vers interne) est envoyé à l'AIP SSM pour l'inspection. La signature faite sur commande 60000 0, qui est configurée sur l'AIP SSM, alarme.

Note: Par défaut, l'ASA ne garde pas l'état pour le trafic d'ICMP. Dans la configuration d'échantillon précédente, l'utilisateur interne cingle (requête d'écho d'ICMP) le routeur extérieur. Le routeur répond avec la réponse d'écho d'ICMP. L'AIP SSM examine le paquet de demande d'écho mais pas le paquet de réponse d'écho. Si l'inspection d'ICMP est activée sur l'ASA, la requête d'écho et des paquets de réponse d'écho sont examinés par l'AIP SSM.

Excluez le trafic réseau spécifique de la lecture d'AIP SSM

L'exemple généralisé donné fournit une vue sur exempter le trafic spécifique à balayer par AIP SSM. Afin d'exécuter ceci, vous devez créer une liste d'accès qui contient la circulation qui doit être exclue de la lecture d'AIP SSM dans l'instruction de refus. Dans cet exemple, l'IPS est le nom de la liste d'accès qui définissent la circulation à balayer par AIP SSM. Le trafic entre le <source> et le <destination> sont exclus de la lecture ; tout autre trafic est examiné.

```
ciscoasa#configure terminal
ciscoasa(config)#access-list traffic_for_ips deny ip 10.2.2.0 255.255.255.0 192.168.1.0
255.255.255.0
```

```
ciscoasa(config)#access-list traffic_for_ips permit ip 10.2.2.0 255.255.255.0 any
ciscoasa(config)#class-map ips_class_map
ciscoasa(config-cmap)#match access-list traffic_for_ips
ciscoasa(config)#policy-map interface_policy
ciscoasa(config-pmap)#class ips_class_map
ciscoasa(config-pmap-c)#ips inline fail-open
ciscoasa(config)#service-policy interface_policy interface inside
```

Vérifiez

Vérifiez que des événements vigilants sont enregistrés dans l'AIP SSM.

Connectez-vous dans l'AIP SSM avec le compte utilisateur d'administrateur. La commande **vigilante d'événements d'exposition** génère cette sortie.

Note: La sortie varie basé sur les configurations, le type de trafic envoyé à l'AIP SSM, et la charge du réseau de signature.

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.

```
show events alert

evIdsAlert: eventId=1156198930427770356 severity=high vendor=Cisco
  originator:
    hostId: AIP-SSM
    appName: sensorApp
    appInstanceId: 345
  time: 2009/03/23 22:52:57 2006/08/24 17:52:57 UTC
  signature: description=Telnet Command Authorization Failure id=60000 version=custom
    subsigId: 0
    sigDetails: Command authorization failed
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 172.16.1.200
      port: 23
    target:
      addr: locality=IN 10.2.2.200
      port: 33189
  riskRatingValue: 75
  interface: ge0_1
  protocol: tcp


evIdsAlert: eventId=1156205750427770078 severity=high vendor=Cisco
  originator:
    hostId: AIP-SSM
    appName: sensorApp
    appInstanceId: 345
  time: 2009/03/23 23:46:08 2009/03/23 18:46:08 UTC
  signature: description=ICMP Echo Request id=2004 version=S1
    subsigId: 0
  interfaceGroup:
  vlan: 0
  participants:
```

```
    attacker:
      addr: locality=OUT 172.16.1.200
    target:
      addr: locality=DMZ 192.168.1.50
  triggerPacket:
000000  00 16 C7 9F 74 8C 00 15  2B 95 F9 5E 08 00 45 00  ....t...+..^..E.
000010  00 3C 2A 57 00 00 FF 01  21 B7 AC 10 01 C8 C0 A8  .<*W....!.......
000020  01 32 08 00 F5 DA 11 24  00 00 00 01 02 03 04 05  .2.....$........
000030  06 07 08 09 0A 0B 0C 0D  0E 0F 10 11 12 13 14 15  ................
000040  16 17 18 19 1A 1B 1C 1D  1E 1F                    ..........
  riskRatingValue: 100
  interface: ge0_1
  protocol: icmp


evIdsAlert: eventId=1156205750427770079 severity=high vendor=Cisco
  originator:
    hostId: AIP-SSM
    appName: sensorApp
    appInstanceId: 345
  time: 2009/03/23 23:46:08 2009/03/23 18:46:08 UTC
  signature: description=ICMP Echo Reply id=2000 version=S1
    subsigId: 0
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=DMZ 192.168.1.50
    target:
      addr: locality=OUT 172.16.1.200
  triggerPacket:
000000  00 16 C7 9F 74 8E 00 03  E3 02 6A 21 08 00 45 00  ....t.....j!..E.
000010  00 3C 2A 57 00 00 FF 01  36 4F AC 10 01 32 AC 10  .<*W....6O...2..
000020  01 C8 00 00 FD DA 11 24  00 00 00 01 02 03 04 05  .......$........
000030  06 07 08 09 0A 0B 0C 0D  0E 0F 10 11 12 13 14 15  ................
000040  16 17 18 19 1A 1B 1C 1D  1E 1F                    ..........
  riskRatingValue: 100
  interface: ge0_1
  protocol: icmp
```

Dans les configurations d'échantillon, plusieurs signatures IPS sont accordées pour alarmer sur le trafic de test. La signature 2000 et 2004 sont modifiées. La signature faite sur commande 60000 est ajoutée. Dans un environnement de travaux pratiques ou un réseau où peu de données traversent l'ASA, il peut être nécessaire de modifier des signatures afin de déclencher des événements. Si l'ASA et l'AIP SSM sont déployés dans un environnement qui passe un grand nombre de trafic, les configurations par défaut de signature sont susceptibles de générer un événement.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

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.

Émettez ces **commandes show de l'**ASA.

- **show module** — Informations d'expositions sur le SSM sur l'ASA aussi bien que les informations système.

```
ciscoasa#show module
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5510 Adaptive Security Appliance         ASA5510            JMX0935K040
  1 ASA 5500 Series Security Services Module-10  ASA-SSM-10         JAB09440271

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 0012.d948.e912 to 0012.d948.e916  1.0          1.0(10)0     8.0(2)
  1 0013.c480.cc18 to 0013.c480.cc18  1.0          1.0(10)0     6.1(2)E3

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 IPS                            Up               6.1(2)E3

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
!--- Each of the areas highlighted indicate that !--- the ASA recognizes the AIP-SSM and the
AIP-SSM status is up.
```

- **affichez le passage**

```
ciscoasa#show run
!--- Output is suppressed. access-list traffic_for_ips extended permit ip any any ... class-
map ips_class_map match access-list traffic_for_ips ... policy-map global_policy ... class
ips_class_map ips inline fail-open ... service-policy global_policy global !--- Each of
these lines are needed !--- in order to send data to the AIP-SSM.
```

- **liste d'accès d'exposition** — Affiche les compteurs pour une liste d'accès.

```
ciscoasa#show access-list traffic_for_ips
access-list traffic_for_ips; 1 elements
access-list traffic_for_ips line 1 extended permit ip any any (hitcnt=2) 0x9bea7286
!--- Confirms the access-list displays a hit count greater than zero.
```

Avant que vous installiez et utilisiez l'AIP SSM, le trafic réseau traverse-il l'ASA comme prévue ? Sinon, il peut être nécessaire de dépanner les règles de stratégie de réseau et d'accès ASA.

Problèmes avec le Basculement

- Si vous avez deux ASA dans une configuration de basculement et que chacun contient un module AIP-SSM, vous devez répliquer manuellement la configuration des AIP-SSM. Seule la configuration du ASA est répliquée par le mécanisme de basculement. Le module AIP-SSM n'est pas inclus dans le basculement. Référez-vous à l'exemple de configuration de basculement actif/veille PIX/ASA 7.x pour plus d'informations sur des problèmes de Basculement.
- L'AIP SSM ne participe pas au basculement dynamique si le basculement dynamique est configuré sur les paires de Basculement ASA.

Messages d'erreur

Le module IPS (AIP SSM) produit des messages d'erreur comme affiché et ne se déclenchant pas des événements.


```
ciscoasa#show access-list traffic_for_ips
access-list traffic_for_ips; 1 elements
access-list traffic_for_ips line 1 extended permit ip any any (hitcnt=2) 0x9bea7286
!--- Confirms the access-list displays a hit count greater than zero.
```

La cause pour ce message d'erreur est que le capteur virtuel IPS n'a pas été assigné à l'interface du fond de panier de l'ASA. L'ASA est installée de la manière correcte afin d'envoyer le trafic au module de SSM, mais vous devez assigner le capteur virtuel à l'interface du fond de panier que l'ASA crée pour que le SSM balaye le trafic.

```
ciscoasa#show access-list traffic_for_ips
access-list traffic_for_ips; 1 elements
access-list traffic_for_ips line 1 extended permit ip any any (hitcnt=2) 0x9bea7286
!--- Confirms the access-list displays a hit count greater than zero.
```

Ces messages sont indicatifs de l'IP SE CONNECTANT l'activation, qui a à leur tour accaparé vers le haut de toutes les ressources système. Cisco recommande de désactiver l'IP SE CONNECTANT pendant qu'il devrait seulement être utilisé pour le dépannage/buts investigateurs seulement.

Note: `Le contournement intégré errWarning de données a commencé le` message d'erreur est comportement prévu pendant que le capteur redémarre momentanément l'engine d'analyse après la mise à jour de signature, qui est une partie nécessaire du processus de mise à jour de signature.

Prise en charge de Syslog

L'AIP SSM ne prend en charge pas le Syslog comme format vigilant.

La méthode par défaut pour recevoir les informations vigilantes de l'AIP SSM est par l'échange d'événement de périphérique de sécurité (SDEE). Une autre option est de configurer différentes signatures afin de générer un déroutement SNMP comme action de prendre quand elles sont déclenchées.

Réinitialisation d'AIP SSM

Le module d'AIP SSM ne répond pas correctement.

Si le module d'AIP SSM ne répond pas correctement, alors redémarrez le module d'AIP SSM sans redémarrer l'ASA. Employez la commande de recharge du module 1 de hw-module afin de redémarrer le module d'AIP SSM et ne redémarrez pas l'ASA.

Alerte par courrier électronique d'AIP SSM

L'AIP SSM peut-il envoyer des alertes par courrier électronique aux utilisateurs ?

Non, il n'est pas pris en charge.

Informations connexes

- Référence des commandes des dispositifs de sécurité Cisco, version 7.2
- Messages du journal système des dispositifs de sécurité Cisco, version 7.2
- Référence de commandes pour le Système de protection contre les intrusions Cisco 5.1
- Support et documentation techniques - Cisco Systems