Guide d'intégration du contrôleur de réseau local sans fil et du système IPS

Contenu

Introduction

Le système de détection des intrusions Cisco Unified Intrusion Detection System (IDS)/système de prévention des intrusions (IPS) fait partie du réseau à capacité d'autodéfense Cisco et est la première solution de sécurité câblée et sans fil intégré de l'industrie. Cisco Unified IDS/IPS adopte une approche globale à la Sécurité — à la périphérie Sans fil, périphérie de câble, périphérie WAN, et par le centre de traitement des données. Quand un client associé envoie le trafic malveillant par le réseau sans fil unifié Cisco, un périphérique d'ID de câble par Cisco détecte l'attaque et l'envoie évitent des demandes aux contrôleurs LAN Sans fil de Cisco (WLCs), qui dissocient alors le périphérique de client.

Le Cisco IPS est un en ligne, solution réseaux, conçue exactement pour identifier, classifier, et

arrêter le trafic malveillant, y compris des vers, le logiciel espion/logiciel publicitaire, des virus de réseau, et l'abus d'application, avant qu'ils affectent la continuité d'affaires.

Avec l'utilisation de la version de logiciel 5 de capteur de Cisco IPS, la solution de Cisco IPS combine des services intégrés de prévention avec des technologies innovantes pour améliorer la précision. Le résultat est confiance totale en protection assurée de votre solution IPS, sans crainte du trafic légitime étant abandonné. La solution de Cisco IPS également offre la protection complète de votre réseau par sa faculté unique de collaborer avec d'autres ressources en sécurité des réseaux et fournit une approche proactive à la protection de votre réseau.

Les utilisateurs d'aides de solution de Cisco IPS lèvent plus de menaces avec une plus grande confiance par l'utilisation de ces caractéristiques :

- **Technologies intégrées précises de prévention** — Fournit la confiance inégalée pour prendre une mesure préventive contre un choix plus large de menaces sans risque de relâcher le trafic légitime. Ces seules Technologies offrent l'analyse intelligente, automatisée, contextuelle de vos données et aident à s'assurer que vous recevez les la plupart hors de votre solution de prévention des intrusions.
- **identification de menace de Multi-vecteur** — Protège votre réseau contre des violations de stratégie, des exploitations de vulnérabilité, et l'activité anormale par l'inspection détaillée du trafic dans des couches 2 à 7.
- **Seule Collaboration de réseau** — Améliore l'évolutivité et la résilience par la Collaboration de réseau, y compris des techniques de capture du trafic, des capacités d'Équilibrage de charge, et la visibilité efficaces dans le trafic chiffré.
- **Solutions complètes de déploiement** — Fournit des solutions pour tous les environnements, des petites et moyennes entreprises (PME) et des emplacements de succursale à de grandes installations d'entreprise et de fournisseur de services.
- **Gestion, corrélation d'événements, et services de support technique puissants** — active une solution complète, y compris la configuration, la Gestion, la corrélation de données, et les services de support technique avancés. En particulier la surveillance de sécurité Cisco, l'analyse, et le système de réponse (MARS) l'identifie, des isolats, et recommande la suppression de précision des éléments offensants, pour une solution large de prévention des intrusions de réseau. Et le Système de contrôle des incidents Cisco empêche le nouveau ver et les attaques de virus en permettant au réseau rapidement d'adapter et fournir une réponse distribuée.

Une fois combinés, ces éléments fournissent une solution intégrée complète de prévention et te donnent la confiance pour détecter et arrêter la plus large plage du trafic malveillant avant qu'elle affecte la continuité d'affaires. L'initiative de Cisco Self-Defending Network nécessite la Sécurité intégrée et intégrée pour des solutions réseau. Les systèmes basés sur en cours de Protocol de point d'accès léger (LWAPP) WLAN prend en charge seulement les caractéristiques de base d'ID étant donné que c'est essentiellement un système de la couche 2 et il a limité ligne-traiter l'alimentation. Cisco libère le nouveau code en temps utile pour inclure de nouvelles fonctions améliorées dans les nouveaux codes. La version 4.0 a les dernières caractéristiques qui incluent l'intégration d'un système basé sur LWAPP WLAN avec la gamme de produits de Cisco IDS/IPS. Dans cette release, le but est de permettre au système de Cisco IDS/IPS pour demander au WLCs pour bloquer certains clients de l'accès aux réseaux Sans fil quand une attaque est n'importe où de la couche détectée 3 à la couche 7 qui fait participer le client dans la considération.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences minimum :

- Version 4.x et ultérieures de micrologiciels WLC
- La connaissance sur la façon dont configurer le Cisco IPS et le Cisco WLC est desirable.

Composants utilisés

Cisco WLC

Ces contrôleurs sont inclus avec la version de logiciel 4.0 pour des modifications d'ID :

- Gamme Cisco 2000 WLC
- Gamme Cisco 2100 WLC
- WLC de la gamme Cisco 4400
- Wireless Services Module de Cisco (WiSM)
- La gamme de Cisco Catalyst 3750G a unifié le commutateur d'accès
- Module du contrôleur LAN sans fil (WLCM)

Points d'accès

- Cisco Aironet 1100 Points d'accès léger de gamme AG
- Cisco Aironet 1200 Points d'accès léger de gamme AG
- Point d'accès léger de Gamme Cisco Aironet 1300
- Point d'accès léger de Gamme Cisco Aironet 1000

Gestion

- Système de contrôle sans fil Cisco (WCS)
- Capteur de gamme Cisco 4200
- Gestion d'ID de Cisco - Gestionnaire de périphériques d'ID de Cisco (IDM)

Plateformes de Cisco Unified IDS/IPS

- Détecteurs de la gamme Cisco IPS 4200 avec logiciel 5.x de capteur de Cisco IPS ou plus tard.
- SSM10 et SSM20 pour le Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500 avec le logiciel 5.x de capteur de Cisco IPS
- Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500 avec le logiciel 5.x de capteur de Cisco IPS
- Module réseau d'ID de Cisco (NM-CIDS) avec le logiciel 5.x de capteur de Cisco IPS
- Module de Detection System d'intrusion de gamme Cisco Catalyst 6500 2 (IDSM-2) avec le logiciel 5.x de capteur de Cisco IPS

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.

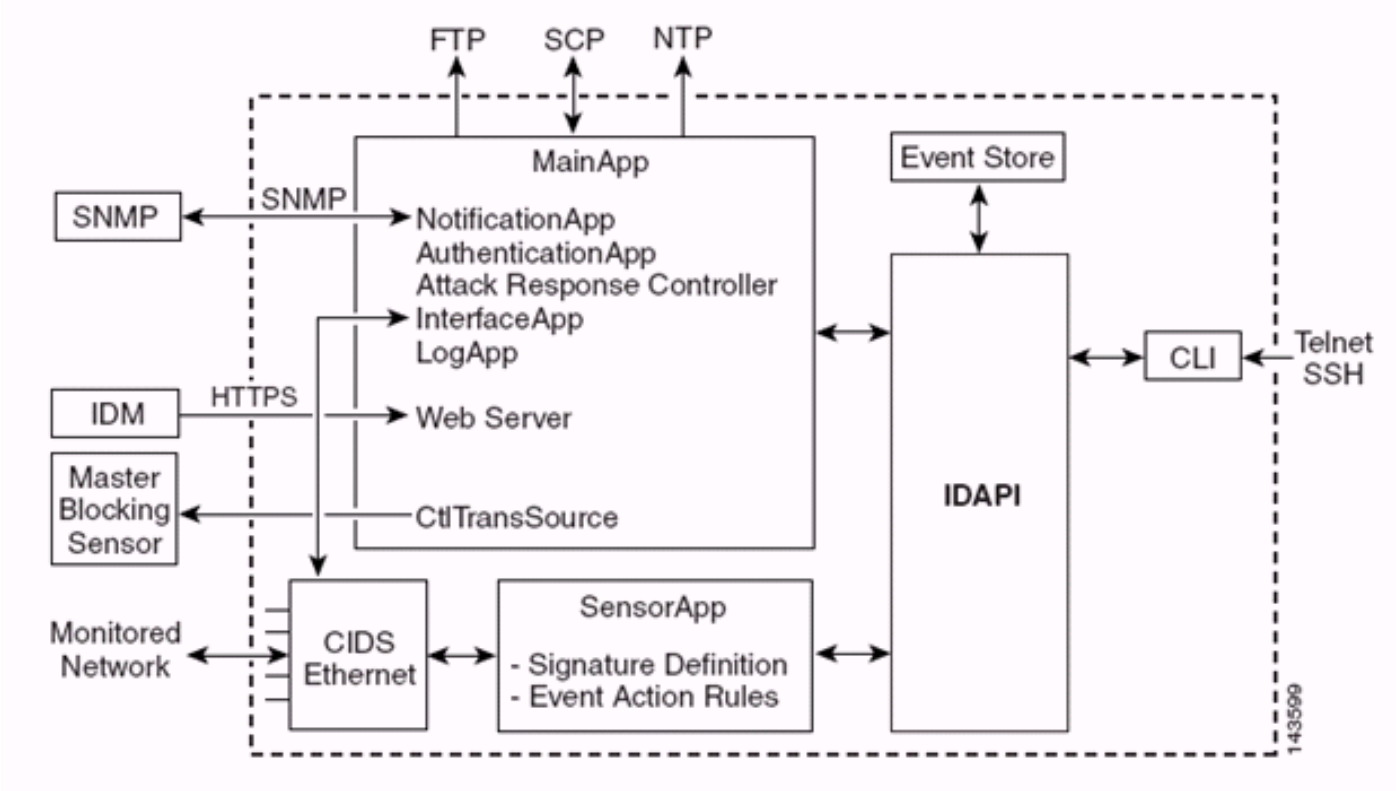
Conventions

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

Aperçu d'ID de Cisco

Les principaux composants des ID de Cisco (version 5.0) sont :

- **App de capteur** — Exécute la capture et l'analyse de paquet.
- **Gestion du stockage d'événement et module d'actions** — Fournit la mémoire des violations de stratégie.
- **La représentation, installent et démarrent le module** — Les chargements, initialise, et commence tout le logiciel système.
- **Interfaces utilisateur et module de support UI** — Fournit un CLI inclus et l'IDM.
- **SYSTÈME D'EXPLOITATION de capteur** — Système d'exploitation d'hôte (basé sur le Linux).



L'application de capteur (logiciel IPS) se compose :

- **App principal** — Initialise le système, commence et arrête d'autres applications, configure le SYSTÈME D'EXPLOITATION et est responsable des mises à jour. Il contient ces composants :**Contrôlez le serveur de transaction** — Permet aux capteurs pour envoyer les transactions de contrôle qui sont utilisées pour activer le maître de contrôleur de réponse d'attaque (autrefois connu sous le nom de contrôleur d'accès au réseau) bloquant la capacité de capteur.**Mémoire d'événement** — Une mémoire répertoriée utilisée pour enregistrer des événements IPS (erreurs, état et messages de système d'alerte) qui est accessible par le CLI, l'IDM, l'Adaptive Security Device Manager (ASDM), ou le Protocol d'échange de données distant (RDEP).
- **App d'interface** — Les traitements sautent et les configurations physiques et définissent les interfaces appareillées. Les configurations physiques se composent de la vitesse, du duplex, et des états administratifs.
- **App de log** — Écrit les messages de log de l'application au fichier journal et aux messages

d'erreur à la mémoire d'événement.
- **Contrôleur de réponse d'attaque (ARC) (autrefois connu sous le nom de contrôleur d'accès au réseau)** — parvient des périphériques réseau distants (Pare-feu, Routeurs, et Commutateurs) pour fournir bloquer des capacités quand un événement vigilant s'est produit. L'ARC crée et applique le Listes de contrôle d'accès (ACL) sur le périphérique commandé de réseau ou utilise la commande d'**évitement** (Pare-feu).
- **App de notification** — Envoie des déroutements SNMP une fois déclenché par une alerte, un état, et des erreurs. L'app de notification utilise un agent SNMP de domaine public ceci. Le SNMP GETs fournissent des informations au sujet des santés d'un capteur.**Serveur Web (serveur de HTTP RDEP2)** — Fournit une interface utilisateur d'utilisateur web. Il fournit également des moyens de communiquer avec d'autres périphériques IPS par RDEP2 utilisant plusieurs servlets pour fournir des services IPS.**App d'authentification** — Vérifie que des utilisateurs sont autorisés à exécuter des actions CLI, IDM, ASDM, ou RDEP.
- **App de capteur (engine d'analyse)** — Exécute la capture et l'analyse de paquet.
- **CLI** — L'interface qui est exécutée quand les utilisateurs ouvrent une session avec succès au capteur par le telnet ou le SSH. Tous les comptes créés par le CLI utilisent le CLI en tant que leur shell (à moins que le compte des services - on permet seulement un compte des services). Les commandes permises CLI dépendent du privilège de l'utilisateur.

Toutes les applications IPS communiquent les uns avec les autres par une interface de programmation commune (API) IDAPI appelé. Les applications distantes (les autres capteurs, applications d'administration, et logiciel tierce partie) communiquent avec des capteurs par RDEP2 et protocoles de l'échange d'événement de périphérique de sécurité (SDEE).

Il doit noter que le capteur a ces partitions de disque :

- **Partition d'application** — Contient la pleine image de système IPS.
- **Partition de maintenance** — Une image IPS de but spécifique a utilisé à la re-image la partition d'application de l'IDSM-2. Une re-image de la partition de maintenance a comme conséquence les paramètres de configuration perdus.
- **Partition de reprise** — Une image de but spécifique utilisée pour la reprise du capteur. L'initialisation dans la partition de reprise active des utilisateurs complètement à la re-image la partition d'application. Des paramètres réseau sont préservés, mais toutes autres configurations sont perdues.

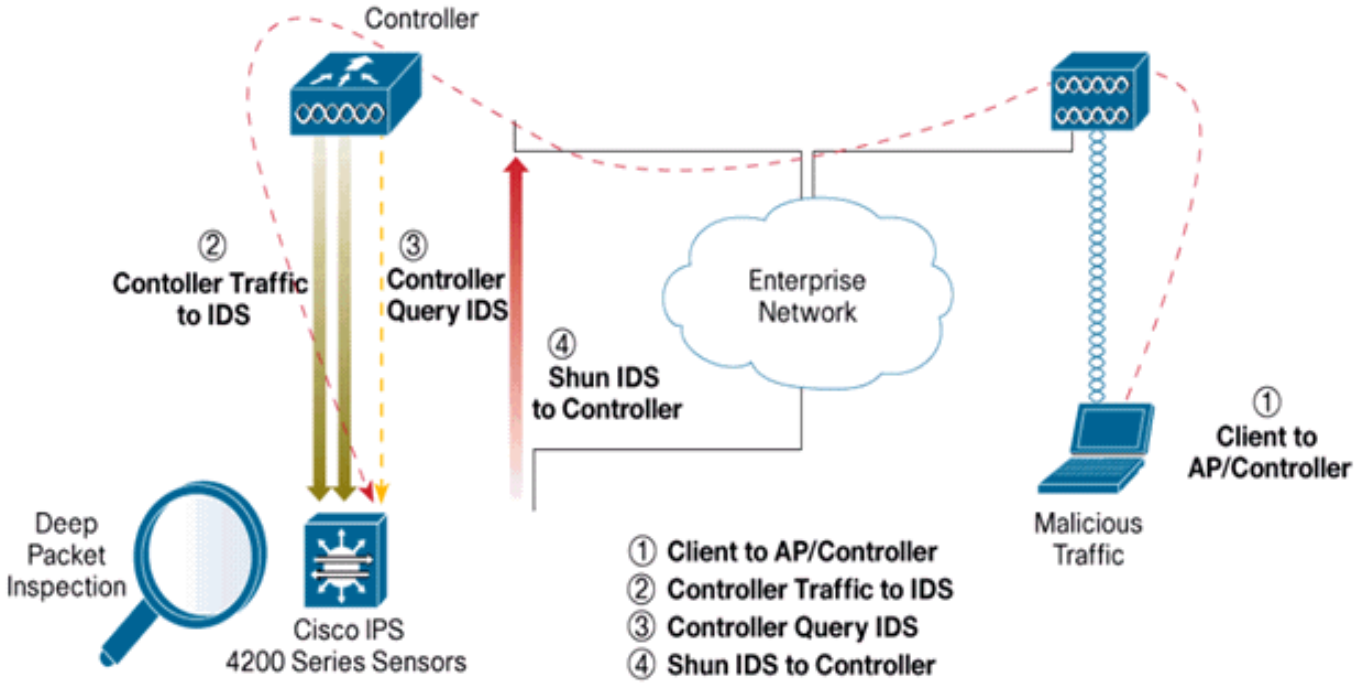
ID de Cisco et WLC – Aperçu d'intégration

La version 5.0 des ID de Cisco introduit la capacité de configurer refusent des actions quand des violations de stratégie (signatures) sont détectées. Basé sur la configuration utilisateur au système IDS/IPS, une demande d'évitement peut être envoyée à un Pare-feu, à un routeur, ou à un WLC afin de bloquer les paquets d'une adresse IP particulière.

Avec la version de logiciel 4.0 de réseau sans fil unifié Cisco pour les contrôleurs Sans fil de Cisco, une demande d'évitement doit être envoyée à un WLC afin de déclencher le client mettant sur la liste noire ou le comportement d'exclusion disponible sur un contrôleur. L'interface que le contrôleur l'utilise pour obtenir la demande d'évitement est l'interface de commandement et de contrôle sur les ID de Cisco.

- Le contrôleur permet jusqu'à cinq capteurs d'ID à configurer sur un contrôleur donné.
- Chaque capteur configuré d'ID est identifié par son adresse IP ou qualifications qualifiées de

nom et d'autorisation de réseau.
- Chaque capteur d'ID peut être configuré sur un contrôleur avec du seul débit de requête en quelques secondes.



ID évitant

Le contrôleur questionne le capteur au débit configuré de requête afin de récupérer tous les événements d'évitement. Donné évitent la demande est distribué dans tout le groupe de mobilité entier du contrôleur qui récupère la demande du capteur d'ID. Chacun évite la demande d'un client que l'adresse IP est en vigueur pour la valeur spécifiée de secondes de délai d'attente. Si la valeur du dépassement de durée indique un temps infini, alors l'événement d'évitement finit seulement si l'entrée d'évitement est retirée sur les ID. L'état évité de client est mis à jour sur chaque contrôleur au groupe de mobilité même si tout ou une partie des contrôleurs sont remis à l'état initial.

Note: La décision d'éviter un client est toujours prise par le capteur d'ID. Le contrôleur ne détecte pas des attaques de la couche 3. C'est un processus bien plus compliqué pour déterminer que le client lance une attaque malveillante à la couche 3. Le client est authentifié à la couche 2 qui est assez bonne pour que le contrôleur accorde l'accès de la couche 2.

Note: Par exemple, si un client obtient une adresse IP (évitée) offensante précédente assignée, il appartient au délai d'attente de capteur pour débloquer l'accès de la couche 2 pour ce nouveau client. Même si le contrôleur donne l'accès à la couche 2, le trafic de client pourrait être bloqué aux Routeurs dans la couche 3 de toute façon, parce que le capteur informe également des Routeurs de l'événement d'évitement.

Supposez qu'un client a l'adresse IP R. Maintenant, quand le contrôleur vote les ID pour évitent des événements, les ID envoie la demande d'évitement au contrôleur avec l'adresse IP A comme adresse IP de cible. Maintenant, le noir de contrôleur répertorie ce client R. Sur le contrôleur, les clients sont des handicapés basés sur une adresse MAC.

Maintenant, supposez que le client change son adresse IP d'A au B. Pendant le prochain balayage, le contrôleur obtient une liste de clients évités basés sur l'adresse IP. Cette fois de

nouveau, l'adresse IP A est toujours dans la liste évitée. Mais puisque le client a changé son adresse IP d'A à B (qui n'est pas dans la liste d'adresses IP évitée), ce client avec une nouvelle adresse IP de B est libéré une fois que le délai d'attente des clients énumérés noirs est atteint sur le contrôleur. Maintenant, les débuts de contrôleur pour permettre à ce client avec nouveau l'adresse IP de B (mais de l'adresse MAC de client reste le même).

Par conséquent, bien qu'un client reste handicapé pour la durée du temps d'exclusion de contrôleur et re-soit exclu si elle re-saisit son adresse précédente DHCP, ce client n'est plus désactivé si l'adresse IP du client qui est les modifications évitées. Par exemple, si le client se connecte au le même réseau et le délai d'attente de bail DHCP n'est pas expiré.

Connexion de support de contrôleurs seulement aux ID pour le client évitant les demandes qui utilisent le port de gestion sur le contrôleur. Le contrôleur se connecte aux ID pour l'inspection de paquet par l'intermédiaire des interfaces VLAN applicables qui portent le trafic de client sans fil.

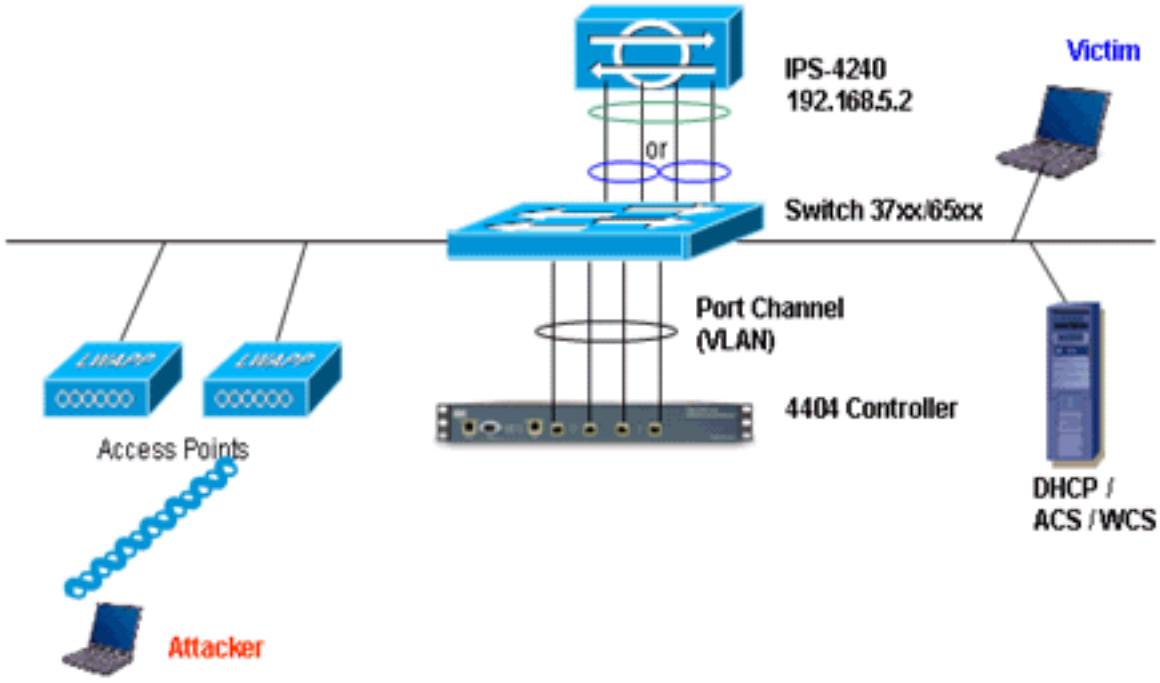
Sur le contrôleur, la page de clients de débronchement affiche chaque client qui a été désactivé par l'intermédiaire d'une demande de capteur d'ID. **La commande show** CLI affiche également une liste de clients mis sur la liste noire.

Sur le WCS, les clients exclus sont affichés sous l'onglet de sous-titre de Sécurité.

Voici les étapes à suivre afin de se terminer l'intégration des capteurs et des Cisco WLC de Cisco IPS.

1. Installez et connectez l'appliance d'ID sur le même commutateur où le contrôleur sans-fil réside.
2. Reflétez (ENVERGURE) les ports WLC qui portent le trafic de client sans fil à l'appliance d'ID.
3. L'appliance d'ID reçoit une copie de chaque paquet et examine le trafic à la couche 3 à 7.
4. L'appliance d'ID offre un fichier de signatures téléchargeable, qui peut également être personnalisé.
5. Les ID que l'appliance génère l'alarme avec une action d'événement de évitent quand une signature d'attaque est détectée.
6. Le WLC vote les ID pour des alarmes.
7. Quand une alarme avec l'adresse IP d'un client sans fil, qui est associé au WLC, est détectée, elle met le client dans la liste d'exclusion.
8. On annonce un déroutement est généré par le WLC et le WCS.
9. L'utilisateur est retiré de la liste d'exclusion après la période indiquée.

Conception de Network Architecture



Le Cisco WLC est connecté aux interfaces de gigabit sur le Catalyst 6500. Créez un Port canalisé pour les interfaces de gigabit et activez l'agrégation de liaisons (LAG) sur le WLC.

```
(Cisco Controller) >show interface summary

Interface Name                    Port  Vlan Id   IP Address       Type     Ap Mgr
--------------------------------  ----  --------  ---------------  -------  ------
ap-manager                        LAG   untagged  10.10.99.3       Static   Yes
management                        LAG   untagged  10.10.99.2       Static   No
service-port                      N/A   N/A       192.168.1.1      Static   No
virtual                           N/A   N/A       1.1.1.1          Static   No
vlan101                           LAG   101       10.10.101.5      Dynamic  No
```

Le contrôleur est connecté pour relier le gigabit 5/1 et le gigabit 5/2 sur le Catalyst 6500.

```
cat6506#show run interface gigabit 5/1
Building configuration...

Current configuration : 183 bytes
!
interface GigabitEthernet5/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 99
 switchport mode trunk
 no ip address
 channel-group 99 mode on
end

cat6506#show run interface gigabit 5/2
Building configuration...

Current configuration : 183 bytes
!
interface GigabitEthernet5/2
 switchport
```

```
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 99
 switchport mode trunk
 no ip address
 channel-group 99 mode on
end

cat6506#show run interface port-channel 99
Building configuration...

Current configuration : 153 bytes
!
interface Port-channel99
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 99
 switchport mode trunk
 no ip address
end
```

Les interfaces de détection du capteur IPS peuvent fonctionner individuellement en **mode promiscueux** ou vous pouvez les appareiller pour créer les interfaces intégrées pour le **mode de détection intégré**.

En mode promiscueux, les paquets ne traversent pas le capteur. Le capteur analyse une copie du trafic surveillé plutôt que le paquet expédié par effectif. L'avantage du fonctionnement en mode promiscueux est que le capteur n'affecte pas l'écoulement de paquet avec le trafic expédié.

Note: Le diagramme d'architecture est juste une installation d'exemple de WLC et d'IPS d'architecture intégrée. L'exemple de configuration affiché ici explique les ID sentant l'interface agissant en mode promiscueux. Le diagramme d'architecture affiche les interfaces de détection étant appareillées ensemble pour agir en mode intégré de paires. Référez-vous au mode intégré pour plus d'informations sur le mode interface intégré.

Dans cette configuration, on le suppose que l'interface de détection agit en mode promiscueux. L'interface de surveillance du capteur d'ID de Cisco est connectée à l'interface 5/3 de gigabit sur le Catalyst 6500. Créez une session de surveillance sur le Catalyst 6500 où l'interface de canal de port est la source des paquets et la destination est l'interface de gigabit où l'interface de surveillance du capteur de Cisco IPS est connectée. Ceci réplique tous les d'entrée et trafic en sortie des interfaces de câble par contrôleur vers les ID pour l'inspection de la couche 3 à la couche 7.

```
cat6506#show run | inc monitor
monitor session 5 source interface Po99
monitor session 5 destination interface Gi5/3

cat6506#show monitor session 5
Session 5
---------
Type                   : Local Session
Source Ports           :
    Both               : Po99
Destination Ports      : Gi5/3
cat6506#
```

Configurez le capteur d'ID de Cisco

La configuration initiale du capteur d'ID de Cisco est faite du port de console ou en connectant un

moniteur et un clavier au capteur.

1. Procédure de connexion à l'appliance :Connectez un port de console au capteur.Connectez un moniteur et un clavier au capteur.
2. Tapez votre nom d'utilisateur et mot de passe à l'invite d'ouverture de connexion.**Note**: Le nom d'utilisateur et mot de passe par défaut sont deux Cisco. Vous êtes incité aux changer la première fois vous procédure de connexion à l'appliance. Vous devez d'abord entrer le mot de passe Unix, qui est Cisco. Alors vous devez entrer le nouveau mot de passe deux fois.

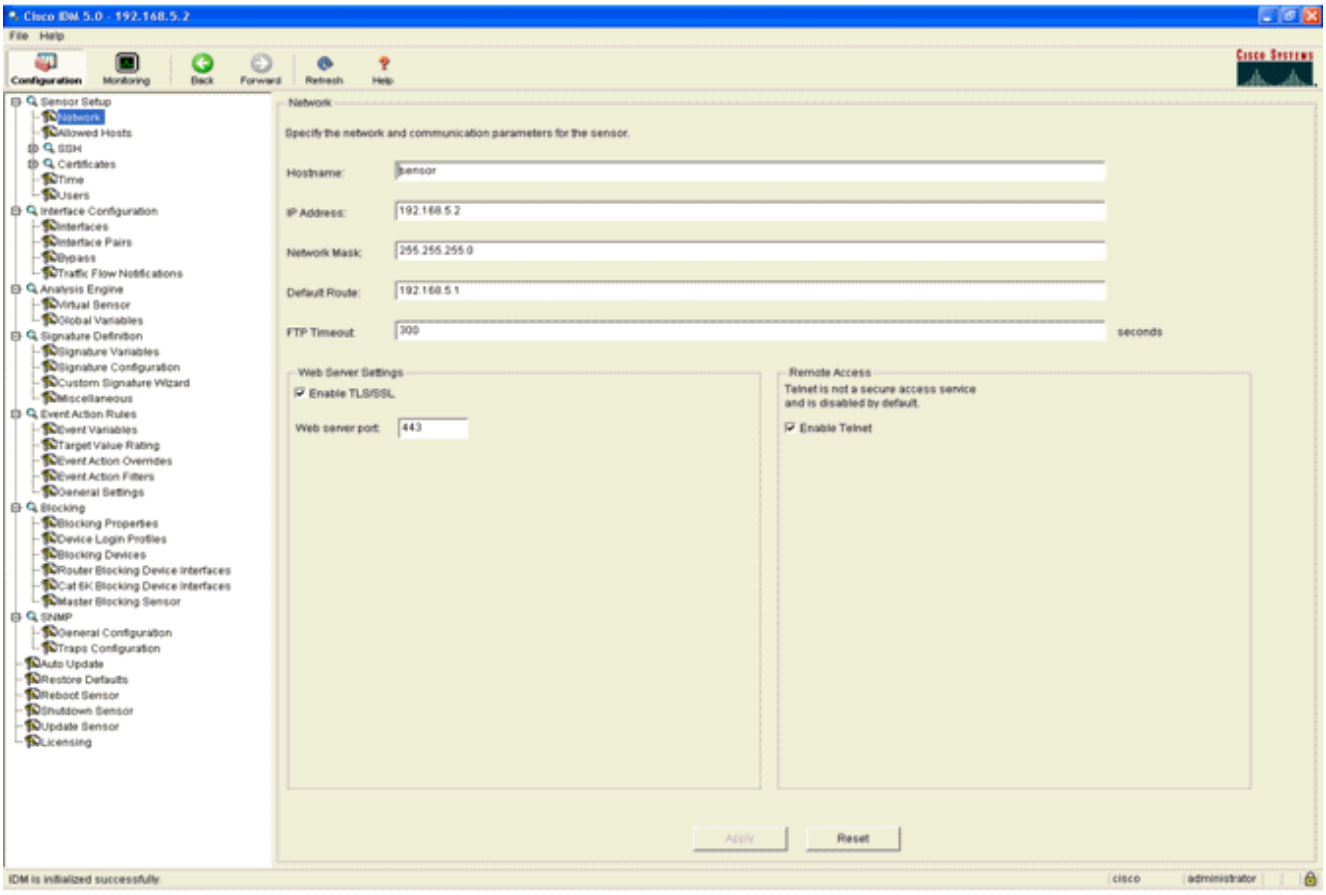
```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to
United States and local country laws governing import, export,
transfer and use. Delivery of Cisco cryptographic products does
not imply third-party authority to import, export, distribute or
use encryption. importers, exporters, distributors and users are
responsible for compliance with U.S. and local country laws.
By using this product you agree to comply with applicable laws
and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may
be found at:

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending
email to export@cisco.com.
***LICENSE NOTICE***
There is no license key installed on the system.
Please go to https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet (registered
customers only) to obtain a new license or install a license.
```

3. Configurez l'adresse IP, le masque de sous-réseau et la liste d'accès sur le capteur.**Note**: C'est l'interface de commandement et de contrôle sur les ID utilisés pour communiquer avec le contrôleur. Cette adresse devrait être routable à l'interface de gestion de contrôleur. Les interfaces de détection n'exigent pas l'adressage. La liste d'accès devrait inclure l'adresse d'interface de gestion de contrôleurs, aussi bien que des adresses permises pour la Gestion des ID.

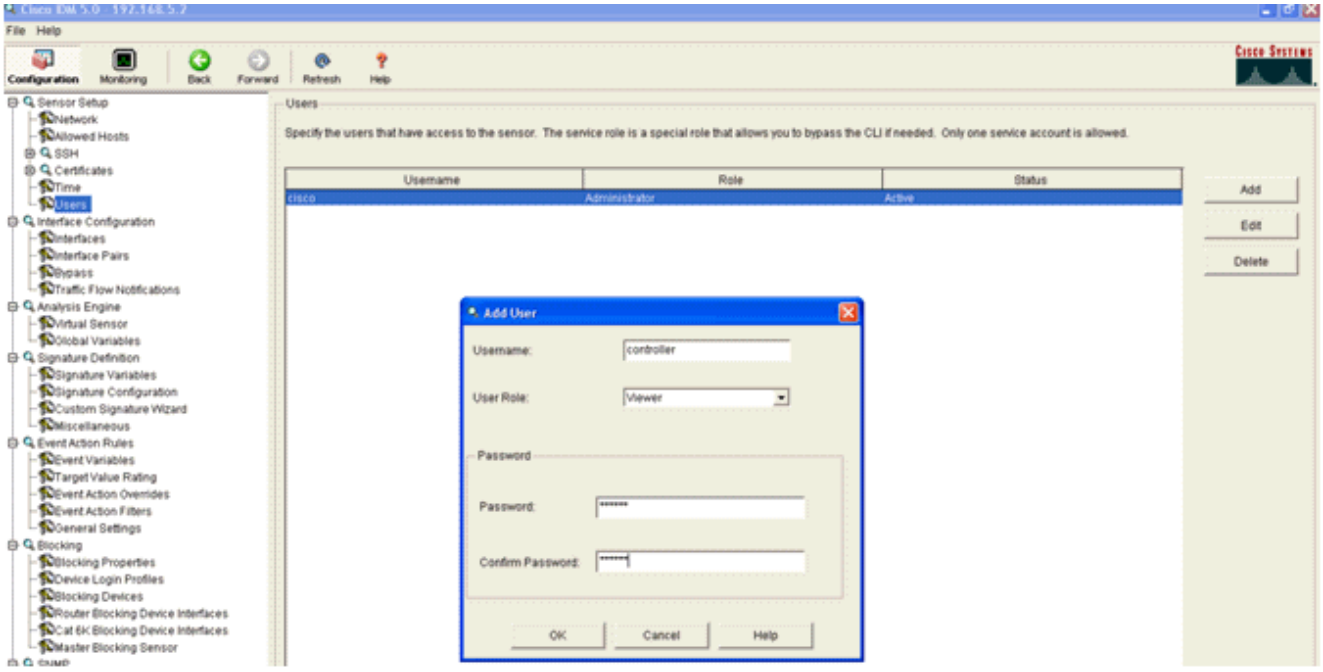
```
sensor#configure terminal
sensor(config)#service host
sensor(config-hos)#network-settings
sensor(config-hos-net)#host-ip 192.168.5.2/24,192.168.5.1
sensor(config-hos-net)#access-list 10.0.0.0/8
sensor(config-hos-net)#access-list 40.0.0.0/8
sensor(config-hos-net)#telnet-option enabled
sensor(config-hos-net)#exit
sensor(config-hos)#exit
Apply Changes:?[yes]: yes
sensor(config)#exit
sensor#
sensor#ping 192.168.5.1
PING 192.168.5.1 (192.168.5.1): 56 data bytes
64 bytes from 192.168.5.1: icmp_seq=0 ttl=255 time=0.3 ms
64 bytes from 192.168.5.1: icmp_seq=1 ttl=255 time=0.9 ms
64 bytes from 192.168.5.1: icmp_seq=2 ttl=255 time=0.3 ms
64 bytes from 192.168.5.1: icmp_seq=3 ttl=255 time=1.0 ms
--- 192.168.5.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
```

```
round-trip min/avg/max = 0.3/0.6/1.0 ms
sensor#
```

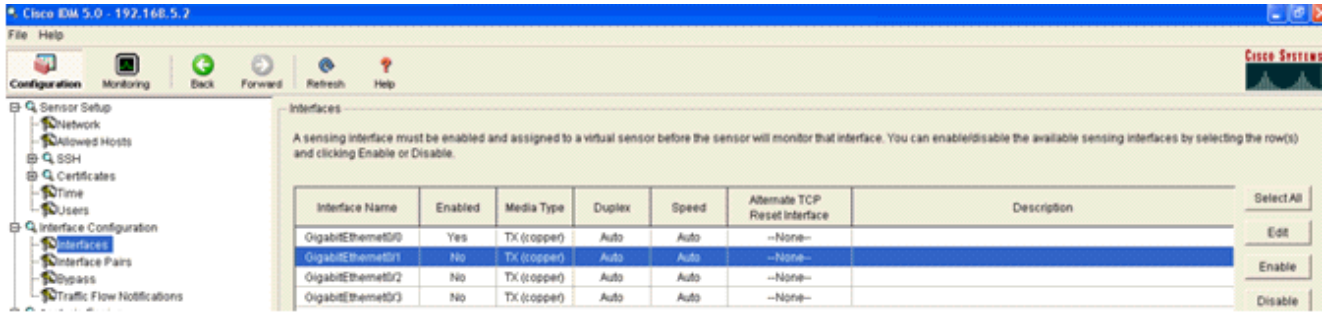
4. Vous pouvez maintenant configurer le capteur IPS du GUI. Indiquez le navigateur l'adresse IP de Gestion du capteur. Affichages de cette image un échantillon où le capteur est configuré avec 192.168.5.2.



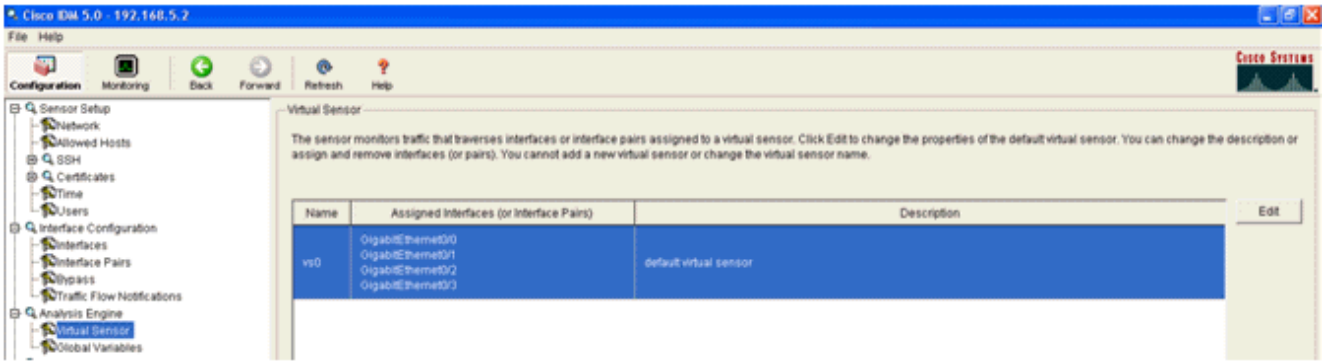
5. Ajoutez un utilisateur que le WLC l'utilise pour accéder aux événements de capteur IPS.



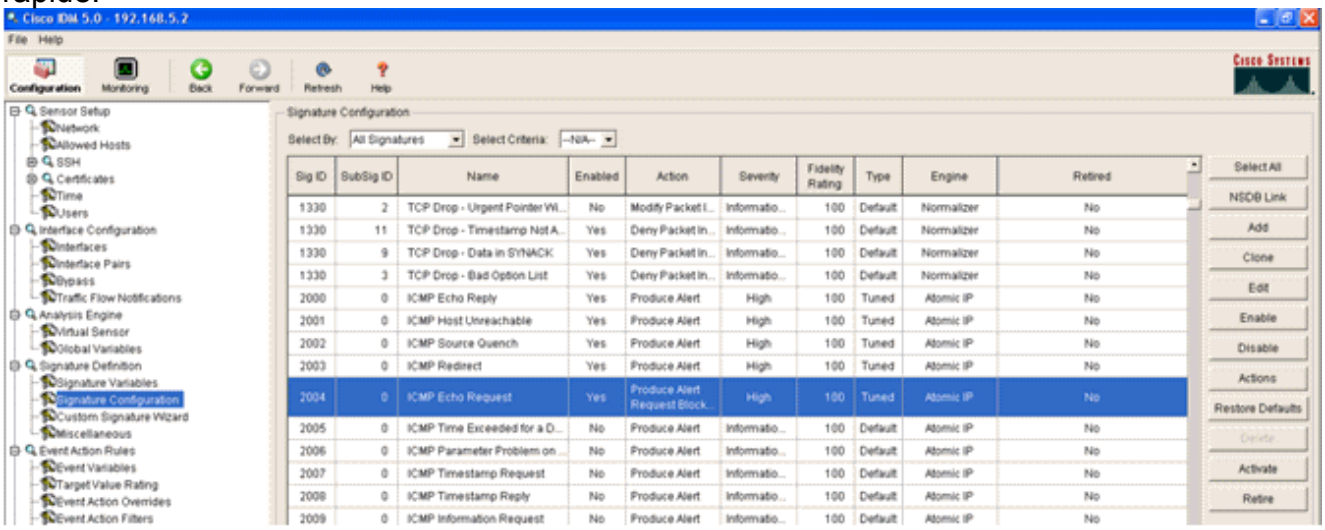
6. Activez les interfaces de surveillance.



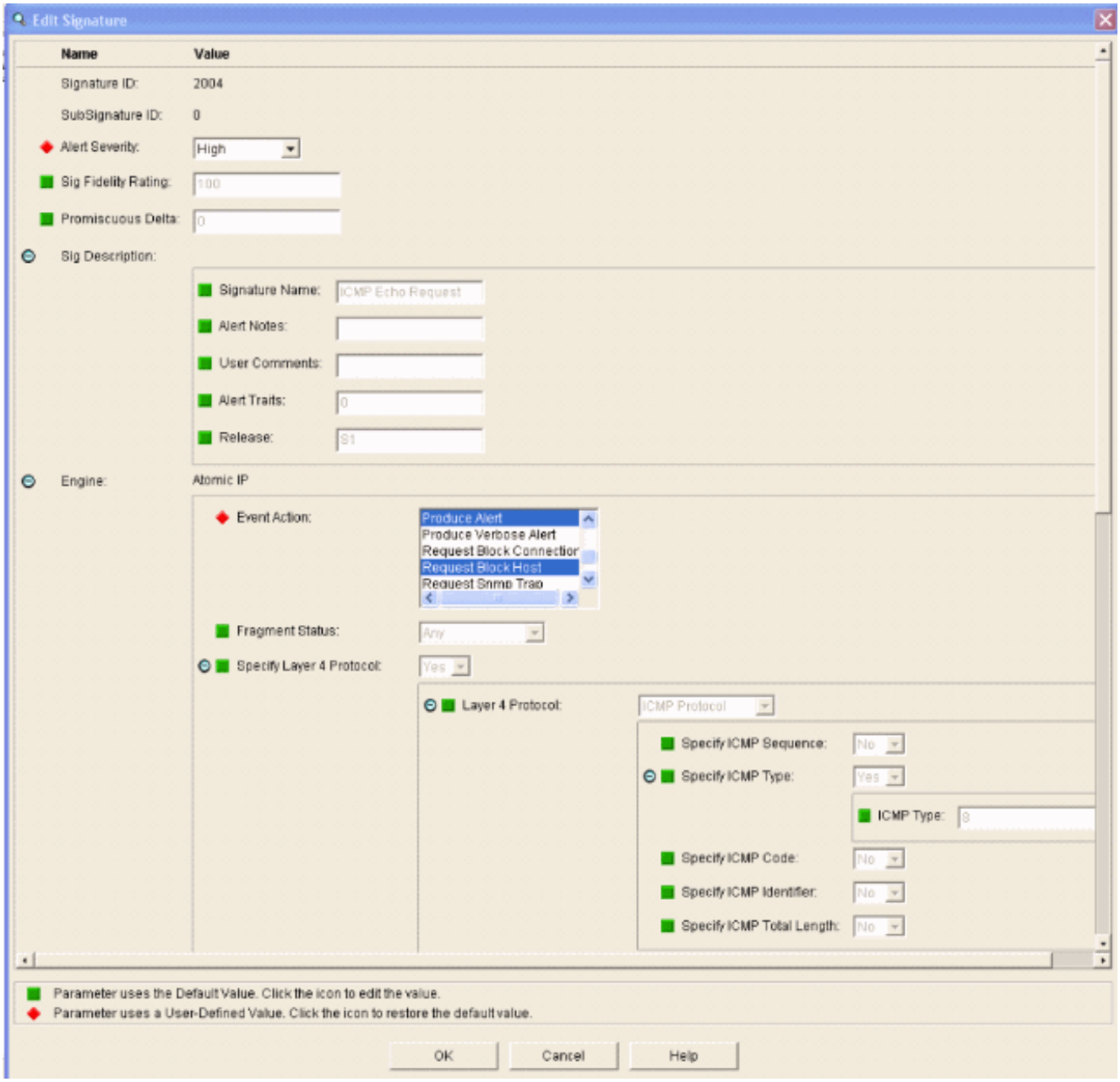
Les interfaces de surveillance doivent être ajoutées à l'engine d'analyse, car cette fenêtre affiche
:



7. Sélectionnez la signature 2004 (requête d'écho d'ICMP) afin d'exécuter une vérification de configuration
rapide.



La signature devrait être activée, positionnement vigilant de sévérité à la **haute** et positionnement d'action d'événement **produire l'alerte** et l'**hôte de bloc de demande** pour que cette étape de vérification soit
terminée.

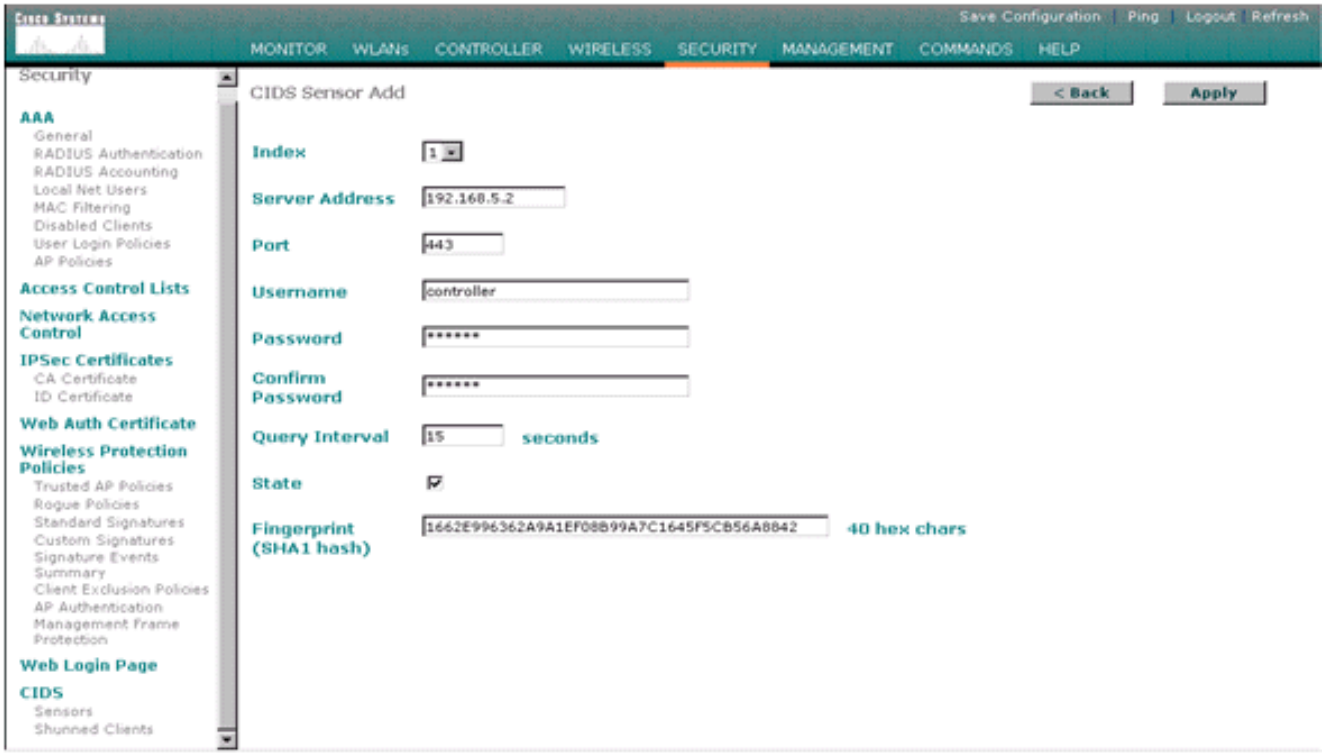


Configurez le WLC

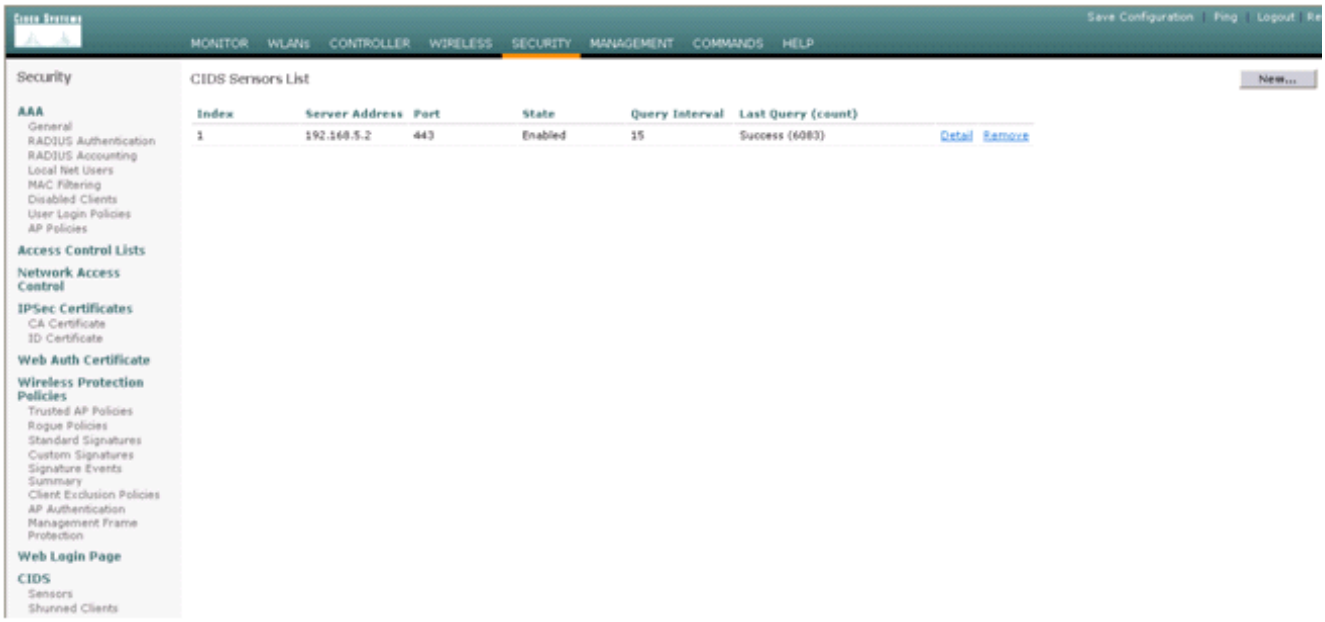
Terminez-vous ces étapes afin de configurer le WLC :

1. Une fois que l'appliance IPS est configurée et prépare pour être ajoutée dans le contrôleur, choisissez la **Sécurité > le CIDS > les capteurs > nouveau**.
2. Ajoutez l'adresse IP, nombre de port TCP, nom d'utilisateur et mot de passe que vous avez précédemment créé.Afin d'obtenir l'empreinte digital du capteur IPS, exécuter cette commande dans le capteur IPS et ajouter l'empreinte digital SHA1 sur le WLC (sans deux points). Ceci est utilisé pour sécuriser les contrôleur-à-ID votant la transmission.

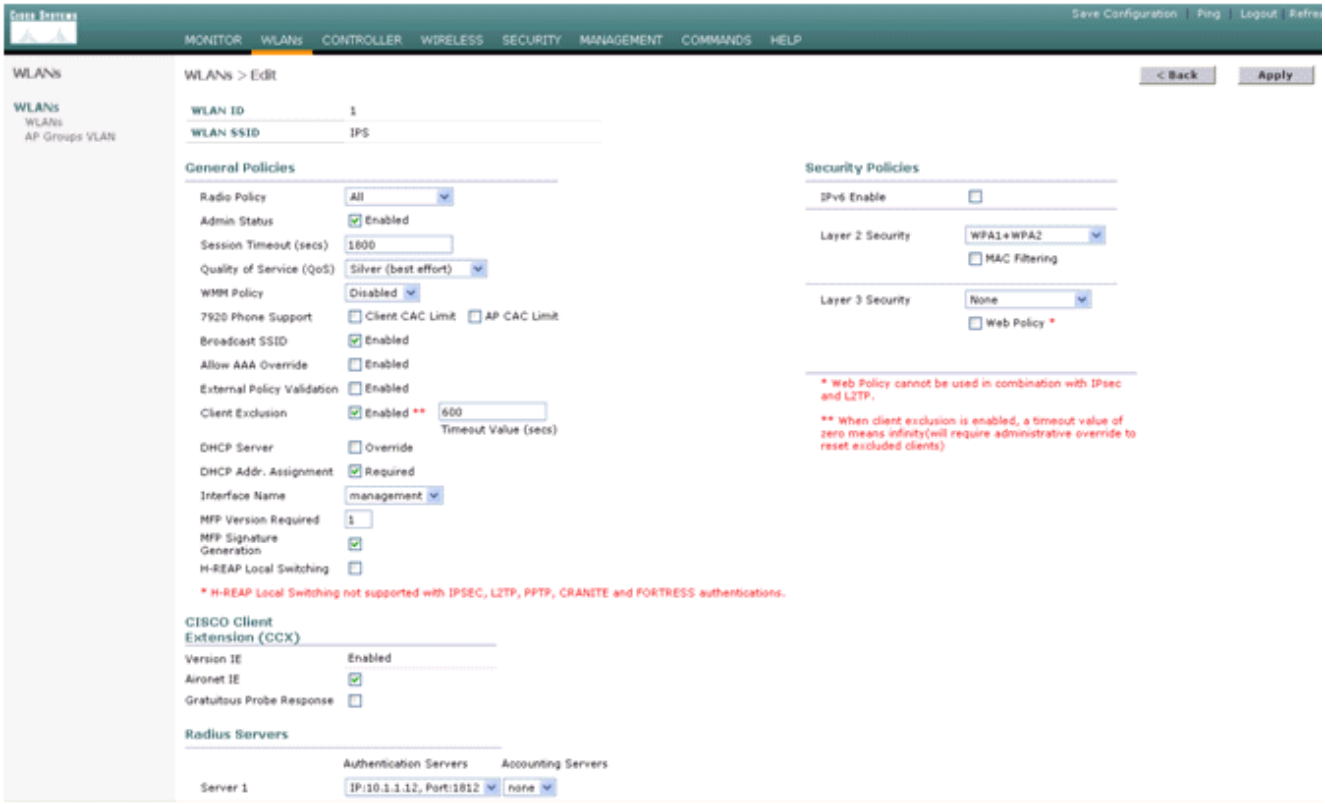
```
sensor#show tls fingerprint
MD5: 1A:C4:FE:84:15:78:B7:17:48:74:97:EE:7E:E4:2F:19
SHA1: 16:62:E9:96:36:2A:9A:1E:F0:8B:99:A7:C1:64:5F:5C:B5:6A:88:42
```



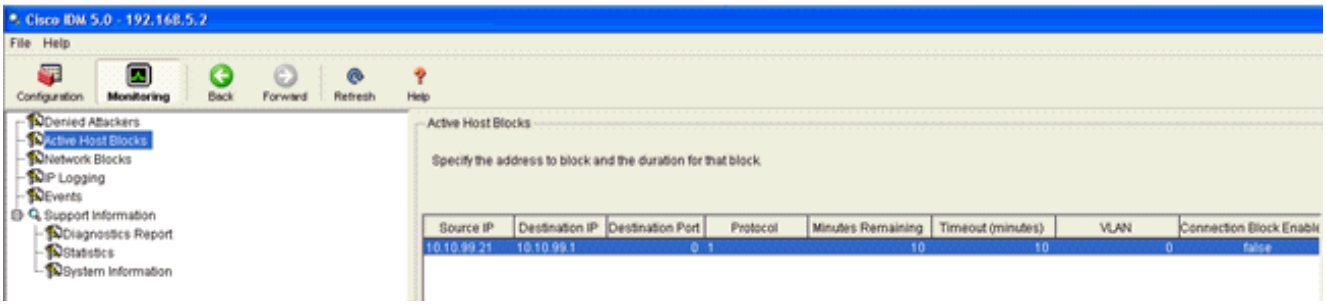
3. Vérifiez le statut de la connexion entre le capteur IPS et le WLC.



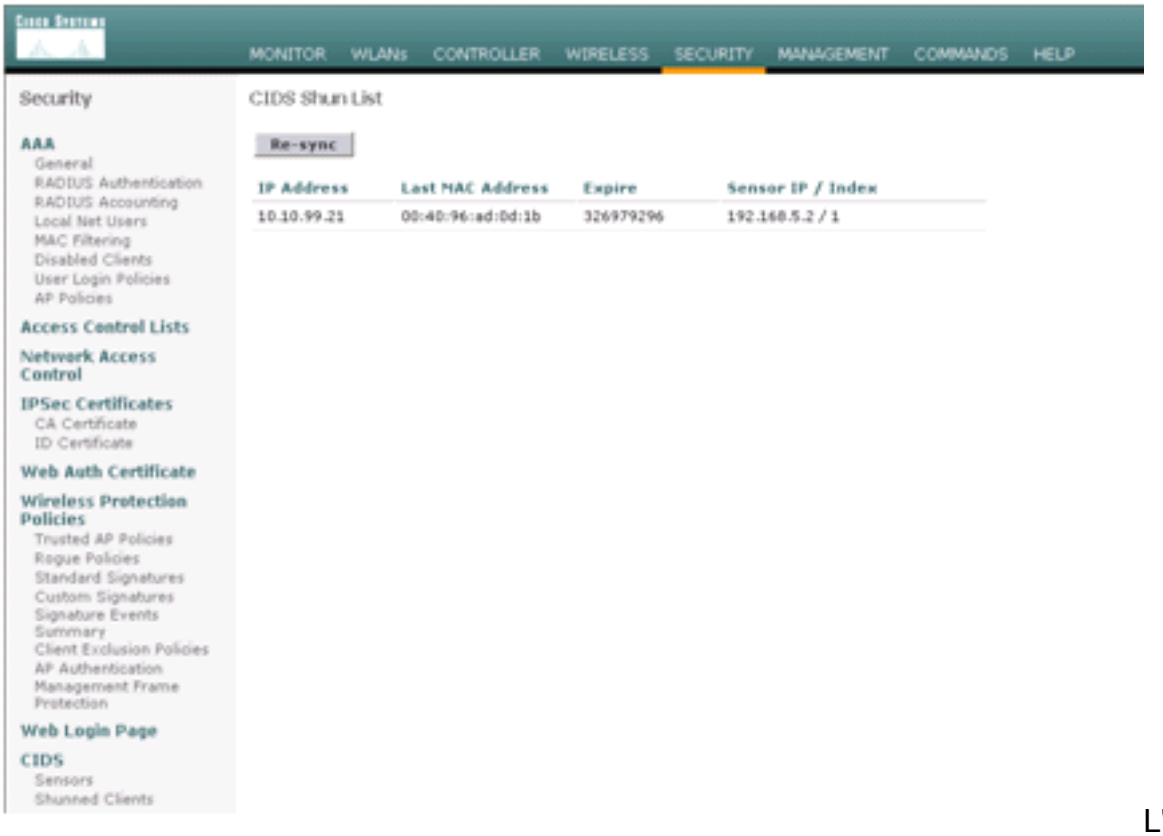
4. Une fois que vous établissez la Connectivité avec le capteur de Cisco IPS, assurez-vous que la configuration WLAN est correcte et cela vous activez l'**exclusion de client**.La valeur du dépassement de durée par défaut d'exclusion de client est de 60 secondes. Notez également qu'indépendamment du temporisateur d'exclusion de client, l'exclusion de client persiste tant que le bloc de client appelé par les ID demeure actif. Le temps par défaut de bloc dans les ID est de 30 minutes.



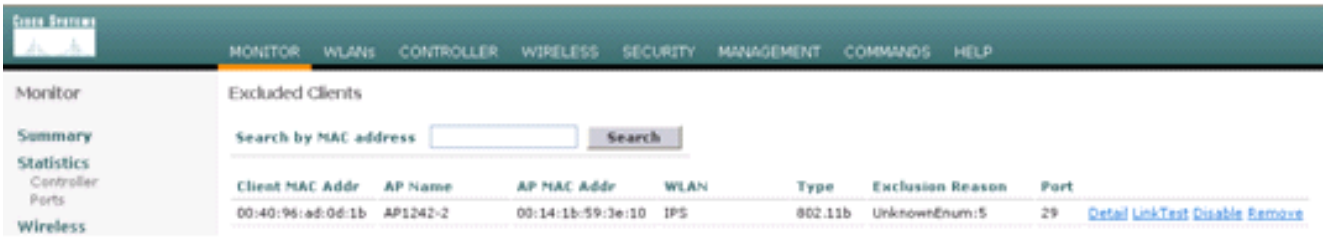
5. Vous pouvez déclencher un événement dans le système de Cisco IPS l'un ou l'autre quand vous faites un balayage NMAP à certains périphériques dans le réseau ou quand vous faites un ping à quelques hôtes surveillés par le capteur de Cisco IPS. Une fois qu'une alarme est déclenchée dans le Cisco IPS, allez à la **surveillance et aux blocs actifs d'hôte** afin de vérifier les détails au sujet de
l'hôte.



Les clients évités les répertorient dans le contrôleur est maintenant remplis avec l'IP et l'adresse MAC de

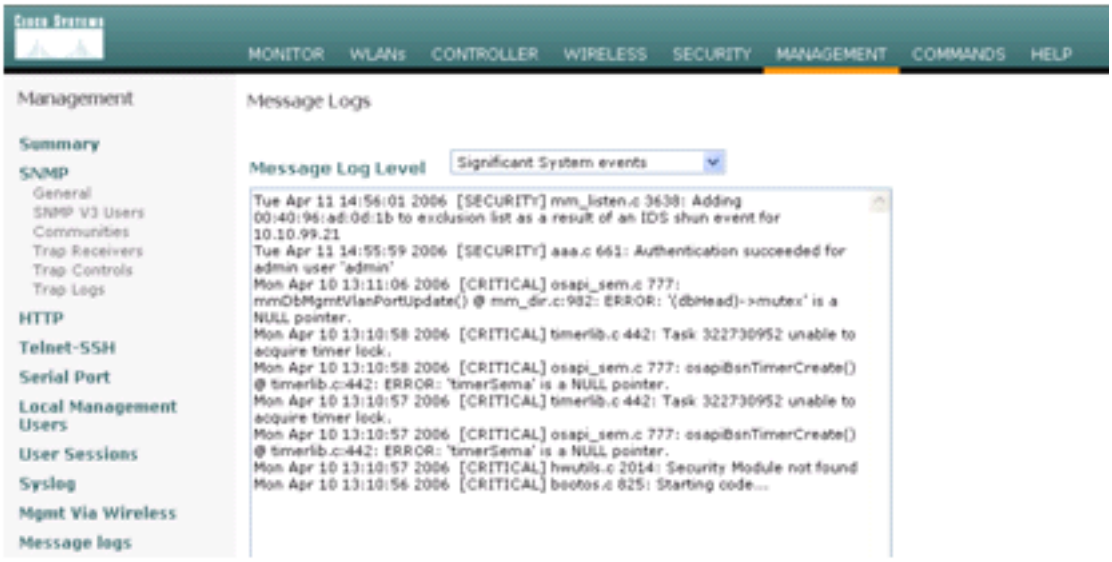


l'hôte. L'utilisateur est ajouté à la liste d'exclusion de client.

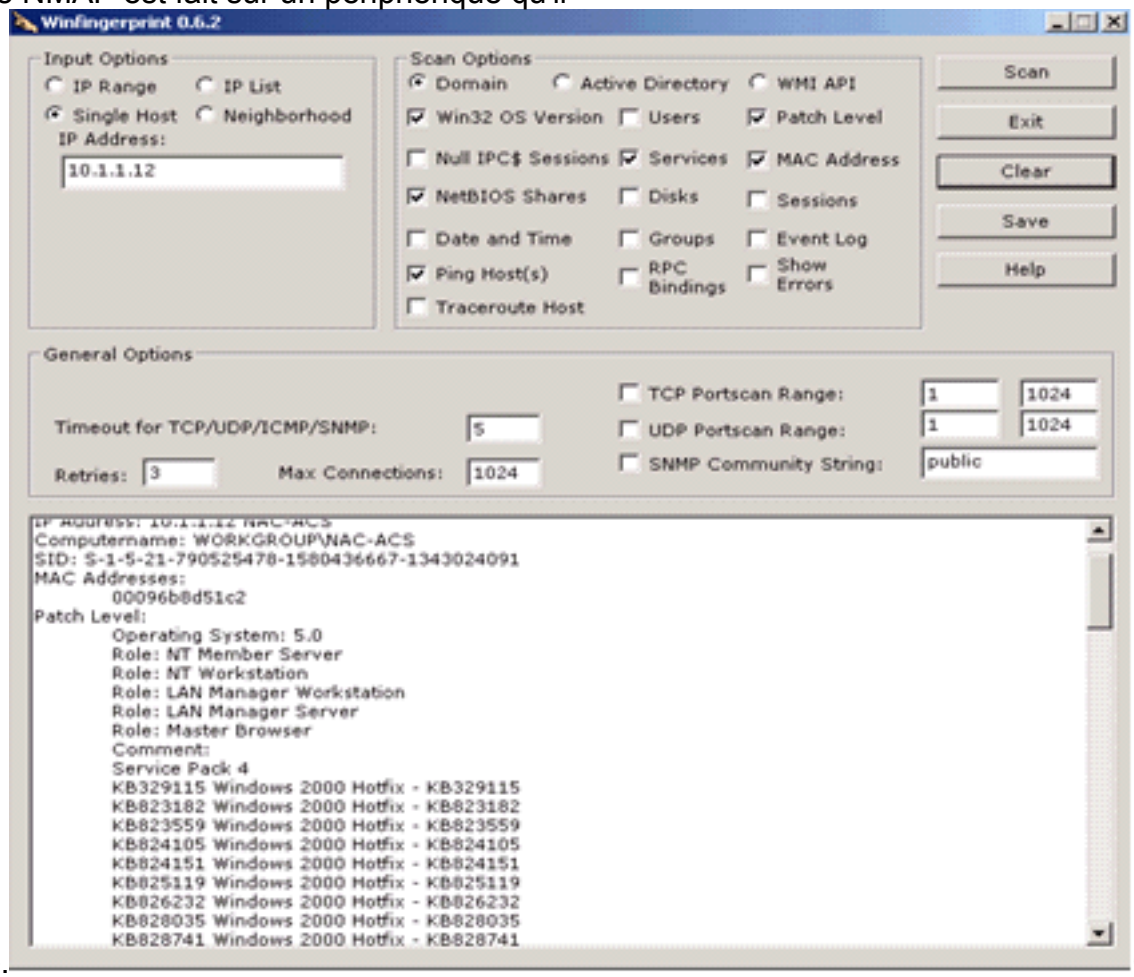


Un log de déroutement est généré comme un client est ajouté à la liste d'évitement.

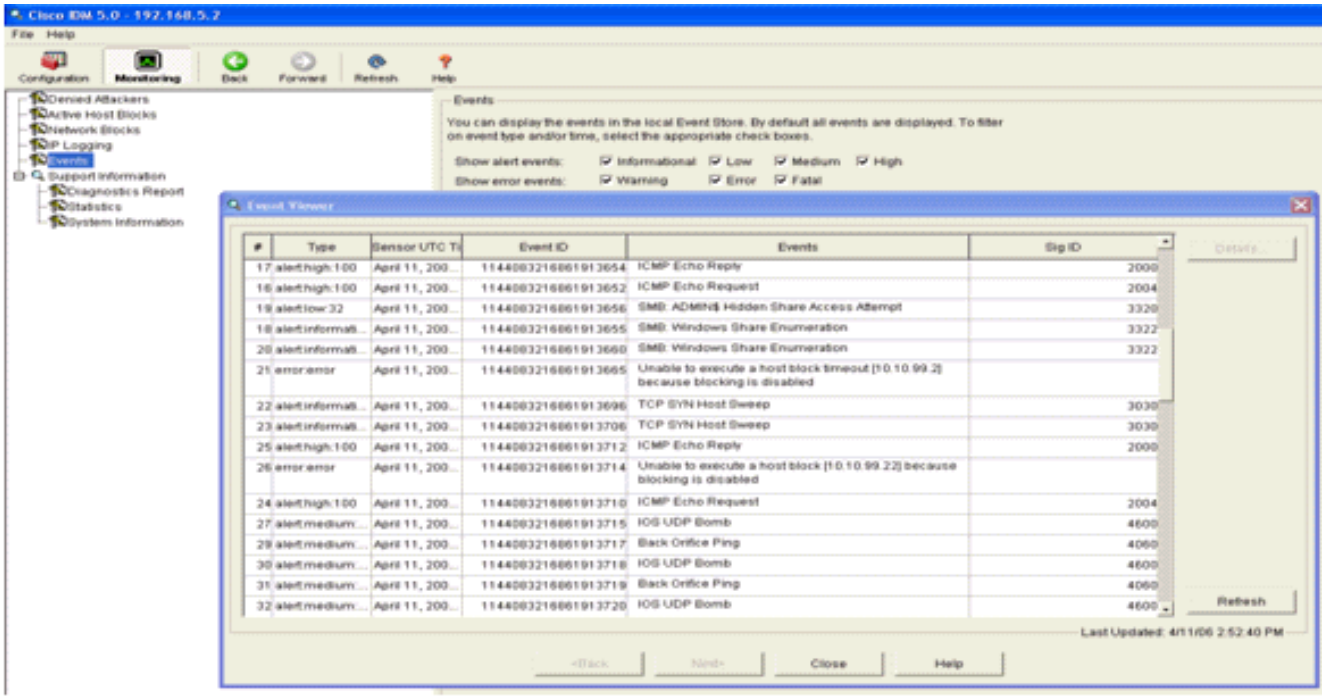
Un journal des messages est également généré pour



l'événement. Quelques événements supplémentaires sont générés dans le capteur de Cisco IPS quand un balayage NMAP est fait sur un périphérique qu'il



surveille. Cette fenêtre affiche des événements générés dans le capteur de Cisco IPS.



Configuration d'échantillon de capteur d'ID de Cisco

C'est la sortie du script d'installation de l'installation :

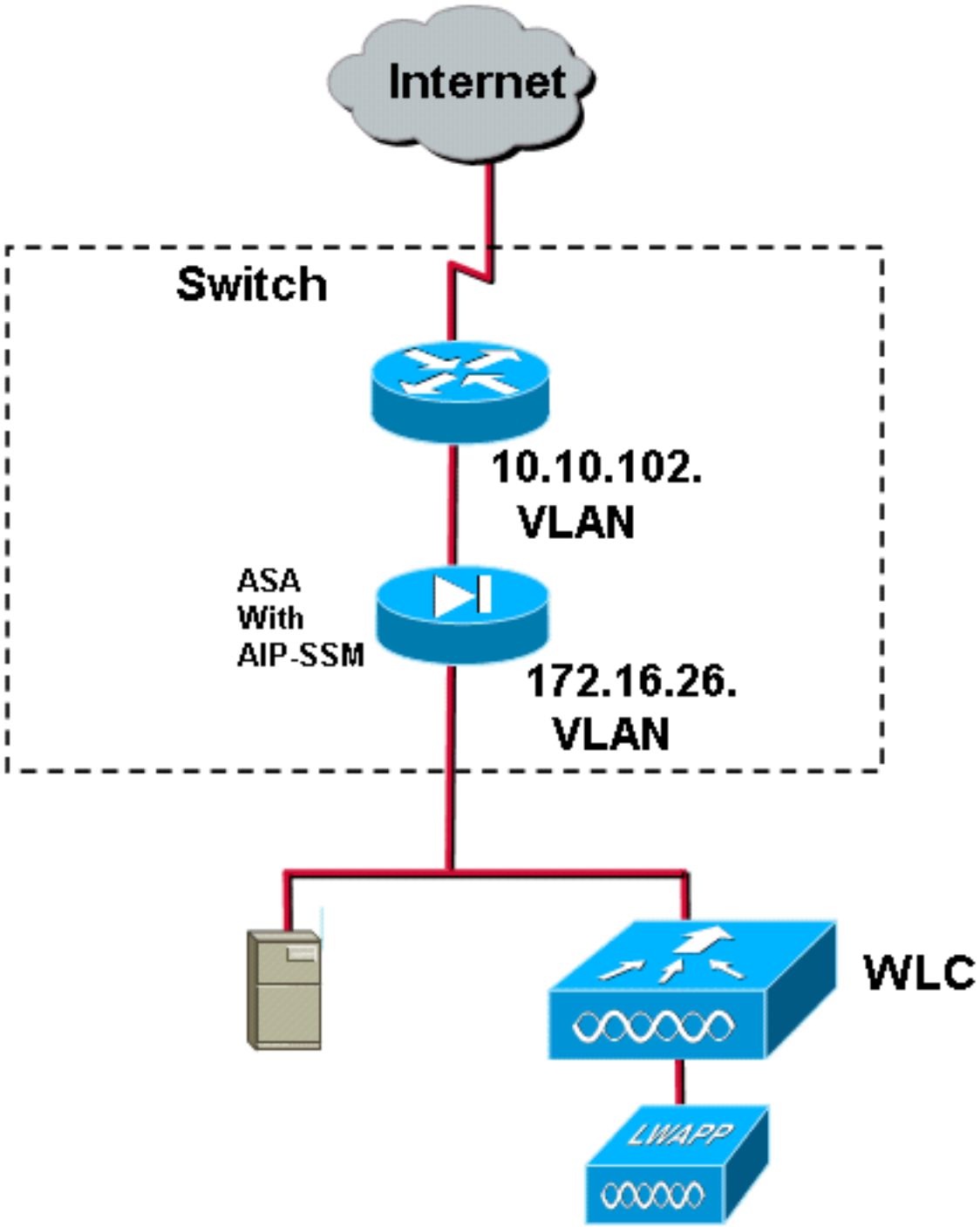
```
sensor#show config
! ------------------------------
! Version 5.0(2)
! Current configuration last modified Mon Apr 03 15:32:07 2006
! ------------------------------
service host
network-settings
host-ip 192.168.5.2/25,192.168.5.1
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list 40.0.0.0/8
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 2000 0
alert-severity high
status
enabled true
exit
exit
signatures 2001 0
alert-severity high
status
enabled true
exit
```

```
exit
signatures 2002 0
alert-severity high
status
enabled true
exit
exit
signatures 2003 0
alert-severity high
status
enabled true
exit
exit
signatures 2004 0
alert-severity high
engine atomic-ip
event-action produce-alert|request-block-host
exit
status
enabled true
exit
exit
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service authentication
exit
! ------------------------------
service web-server
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service analysis-engine
virtual-sensor vs0
description default virtual sensor
physical-interface GigabitEthernet0/0
exit
exit
! ------------------------------
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
exit
! ------------------------------
service trusted-certificates
exit
sensor#
```

Configurez une ASA pour des ID

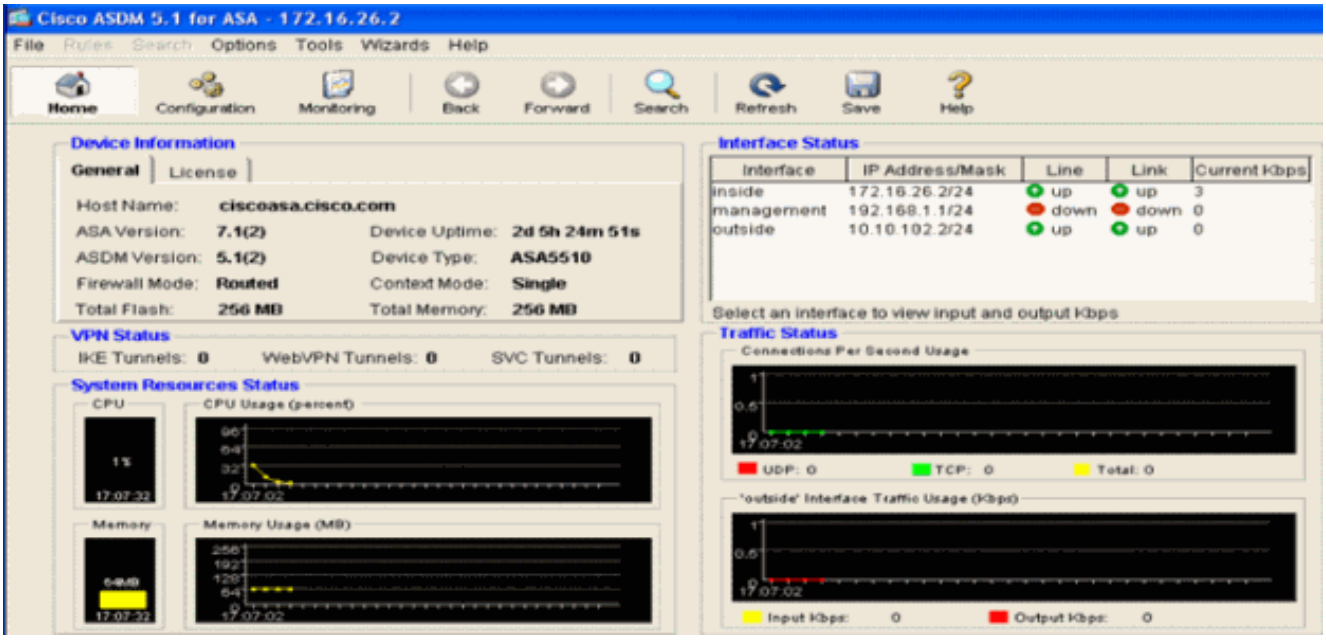
Àla différence d'un capteur traditionnel de détection d'intrusion, une ASA doit toujours être dans le chemin de données. En d'autres termes, au lieu de répartir le trafic d'un port de commutateur plus

d'à un port passif de reniflement sur le capteur, l'ASA doit recevoir des données sur une interface, la traite intérieurement, et lui expédie alors un autre port. Pour des ID, employez le cadre de stratégie modulaire (MPF) afin de copier le trafic que l'ASA reçoit plus d'à l'Advanced Inspection and Prevention Security Services Module interne (AIP SSM) pour l'inspection.

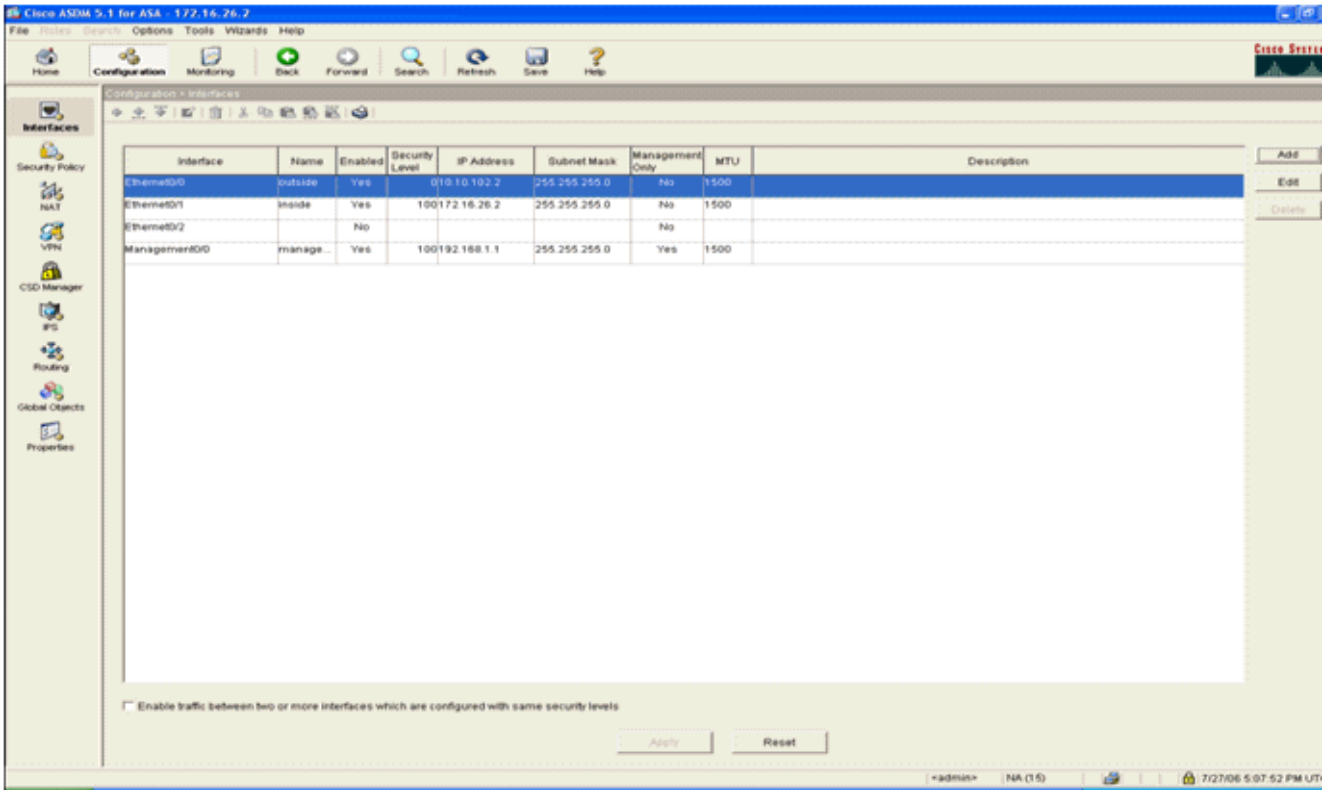


Dans cet exemple, l'ASA utilisée est déjà installée et les passages trafiquent. Ces étapes expliquent comment créer une stratégie qui envoie des données à l'AIP SSM.

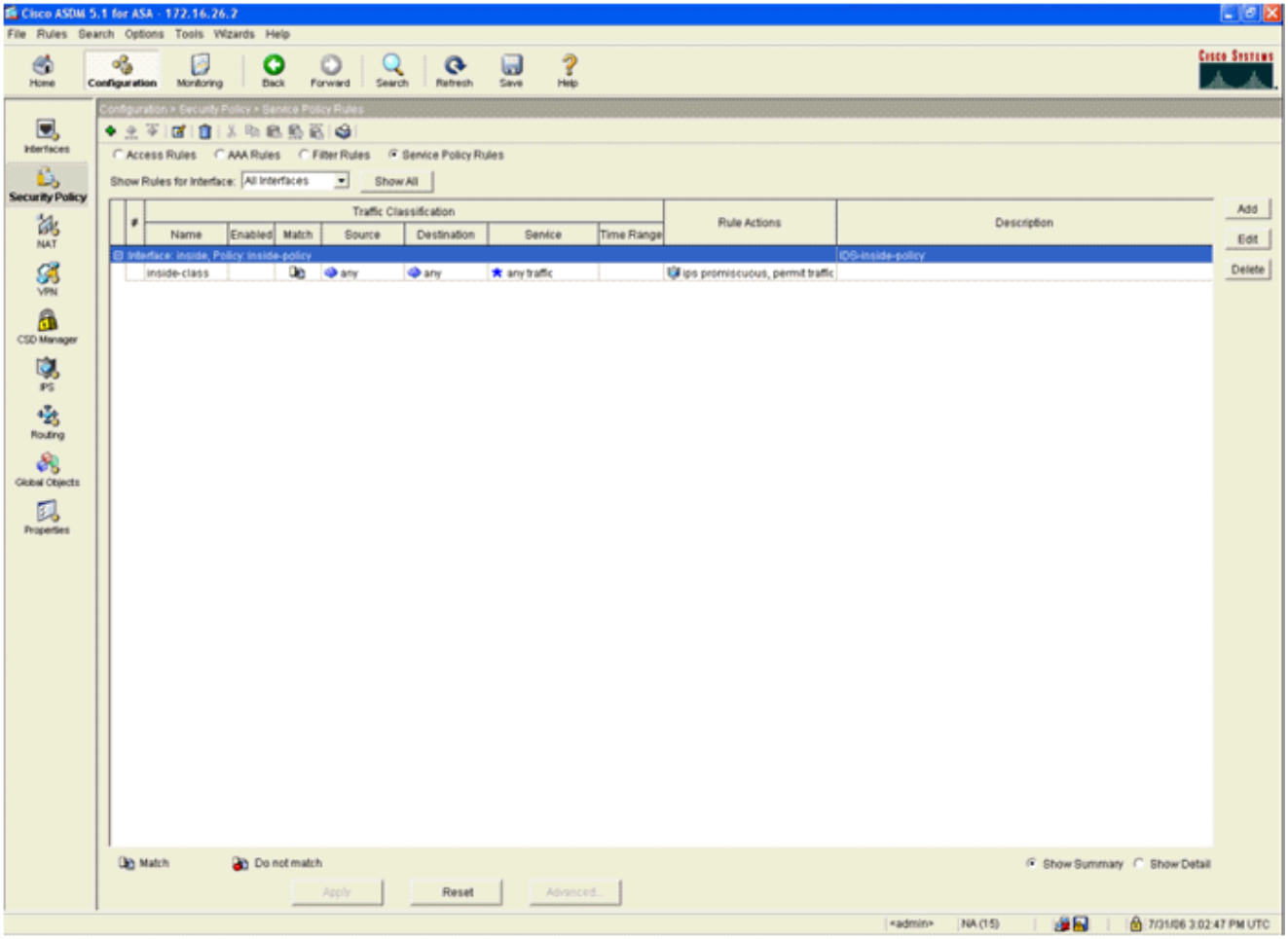
1. Connectez-vous dans l'ASA utilisant l'ASDM. Sur la procédure de connexion réussie, la fenêtre de circuit principal ASA
   apparaît.



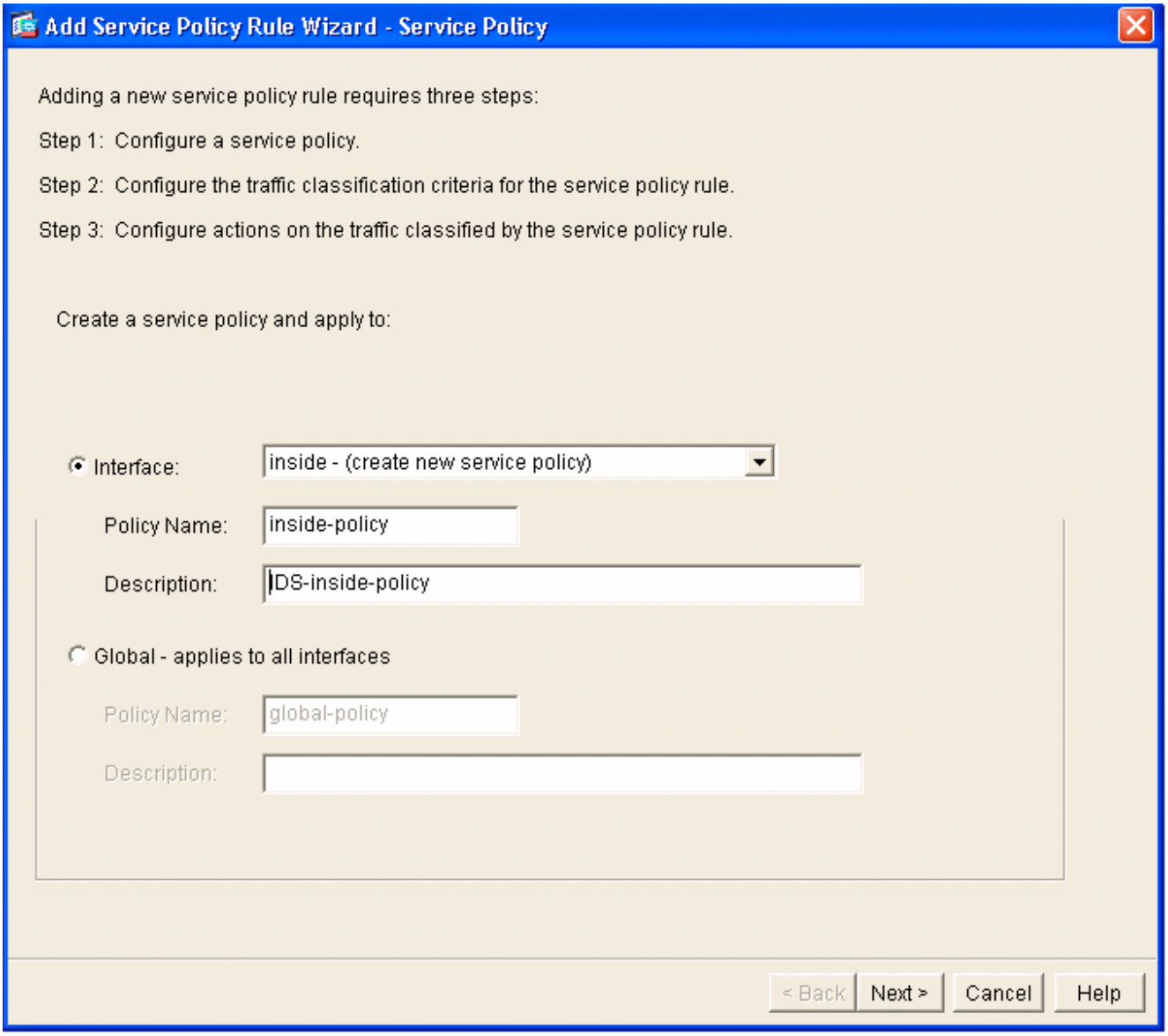
2. **Configuration de** clic en haut de la page. La fenêtre commute à une vue des interfaces ASA.



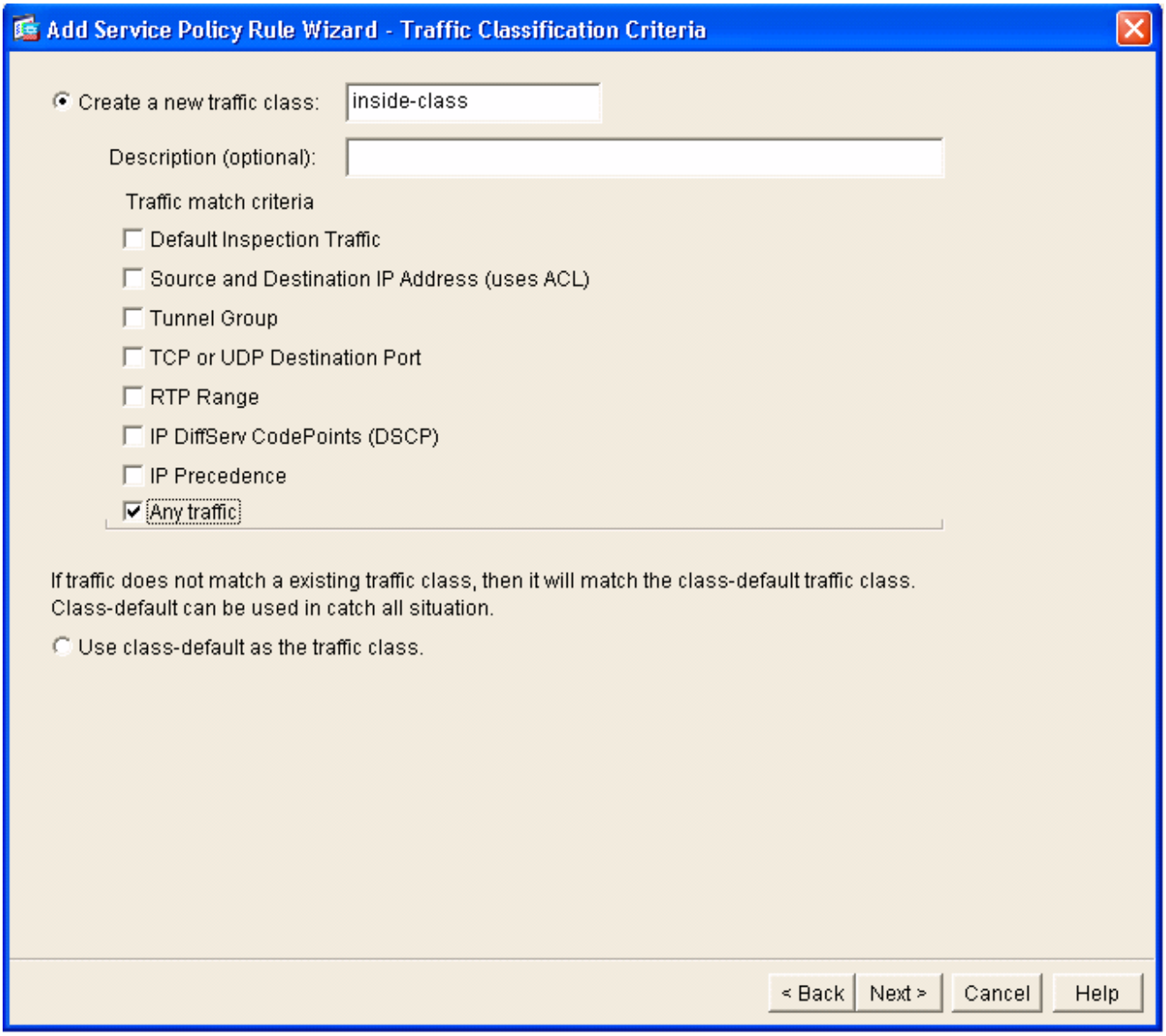
3. Cliquez sur Security la **stratégie du** côté gauche de la fenêtre. Sur la fenêtre résultante, choisissez l'onglet de **règles de stratégie de service**.



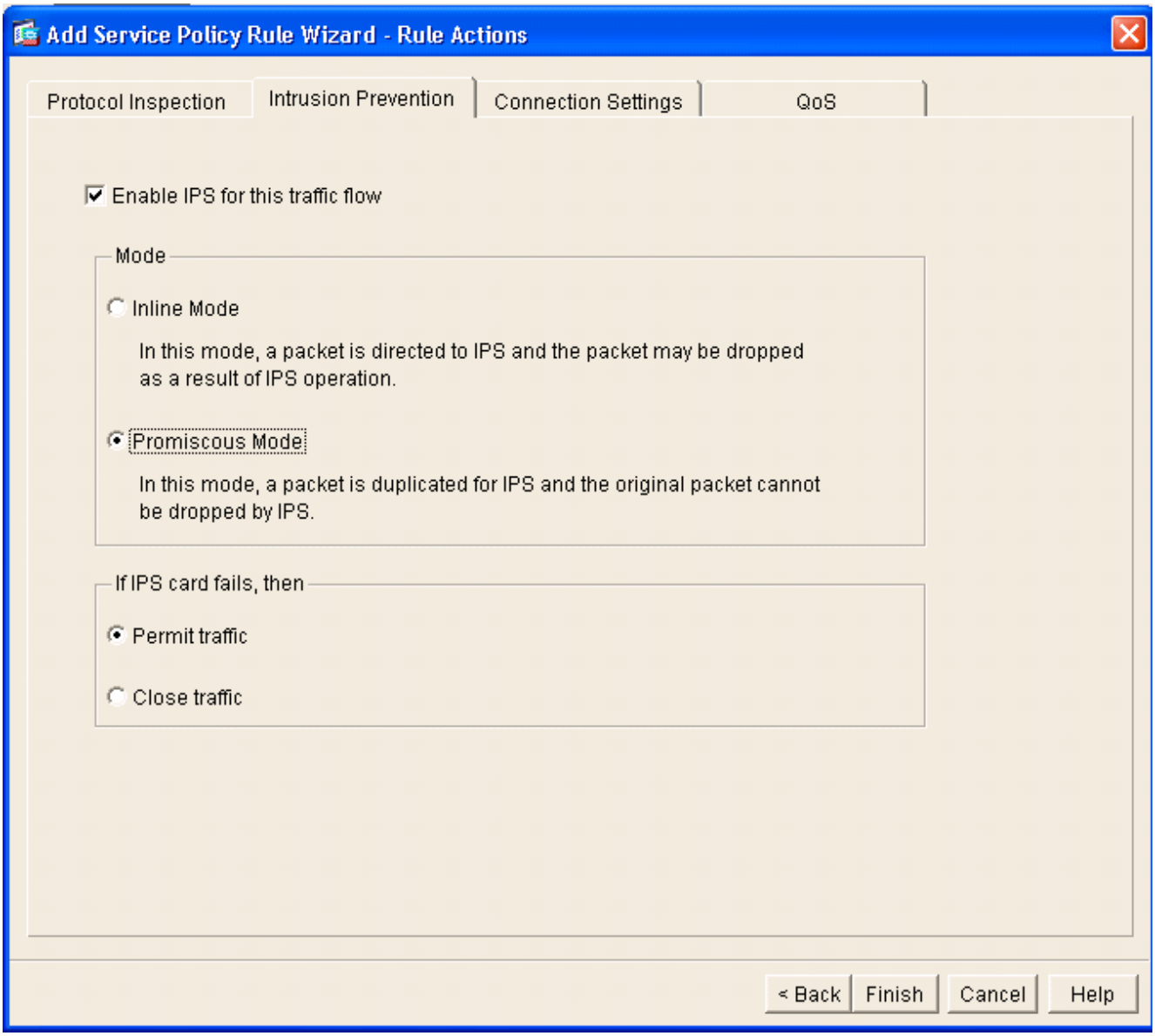
4. Cliquez sur Add afin de créer une nouvelle stratégie. Les lancements d'assistant de règle de stratégie de service d'ajouter dans une nouvelle fenêtre.Cliquez sur l'**interface** et puis choisissez l'interface appropriée de la liste déroulante afin de créer une nouvelle stratégie qui est liée à une des interfaces qui passe le trafic.Donnez à la stratégie un nom et une description de ce que la stratégie fait utilisant les deux zones de texte.Cliquez sur Next afin de se déplacer à l'étape
suivante.



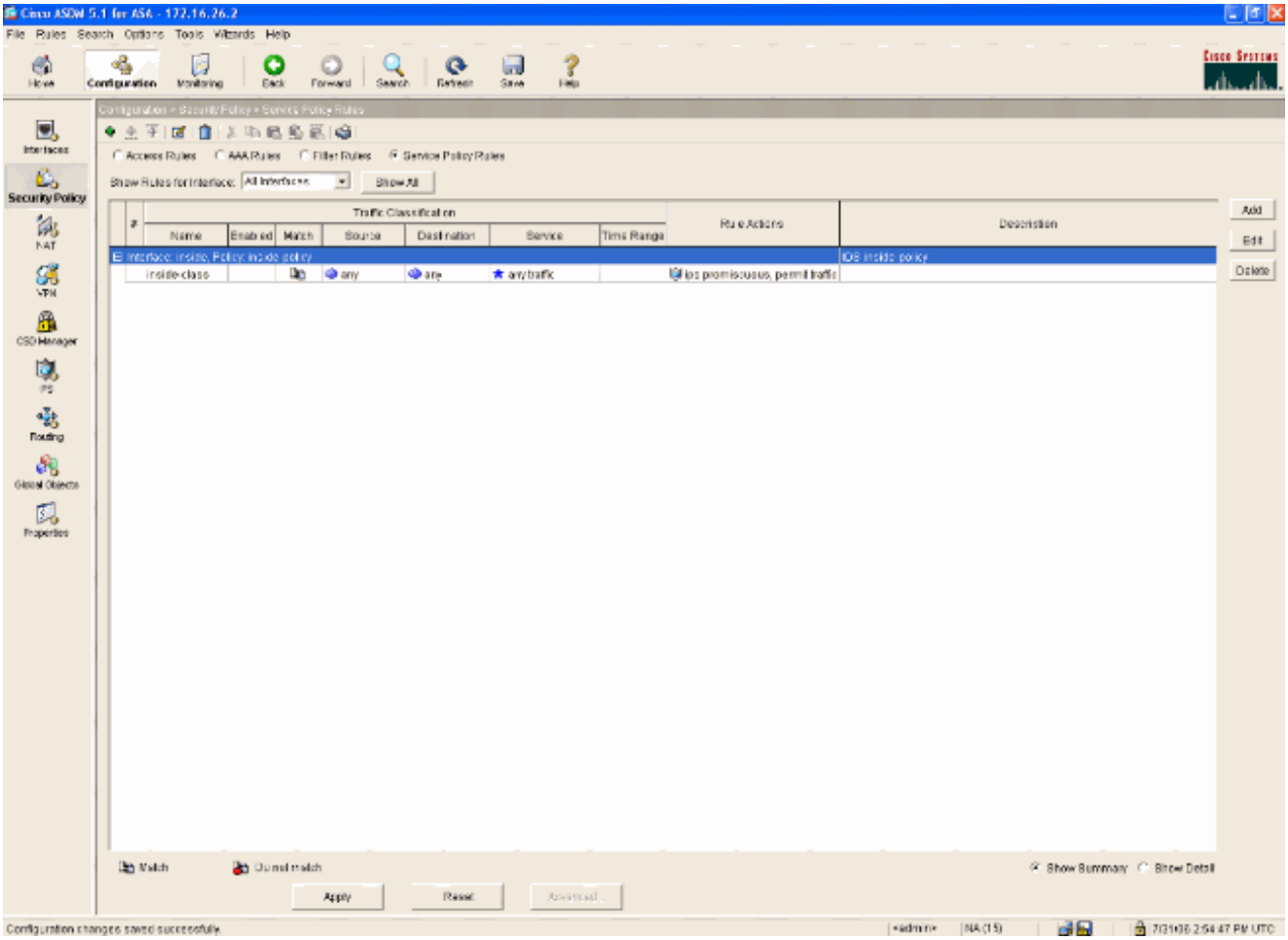
5. Établissez une nouvelle classe du trafic pour s'appliquer à la stratégie.Il est raisonnable d'établir les classes spécifiques afin d'examiner les types de données spécifiques, mais dans cet exemple, n'importe quel trafic est sélectionné pour la simplicité. Cliquez sur Next afin de poursuivre.



6. Terminez-vous ces étapesdemandez à l'ASA pour diriger le trafic plus de vers son AIP SSM.Vérifiez l'**enable IPS pour cette circulation** afin d'activer la détection d'intrusion.Placez le mode à **promiscueux** de sorte qu'une copie du trafic soit envoyée au module hors bande au lieu de placer l'en ligne de module avec du flux de données.**Le trafic d'autorisation de** clic afin de s'assurer que l'ASA commute à un état échec-ouvert au cas où l'AIP SSM échouerait.Cliquez sur Finish afin de commettre la modification.



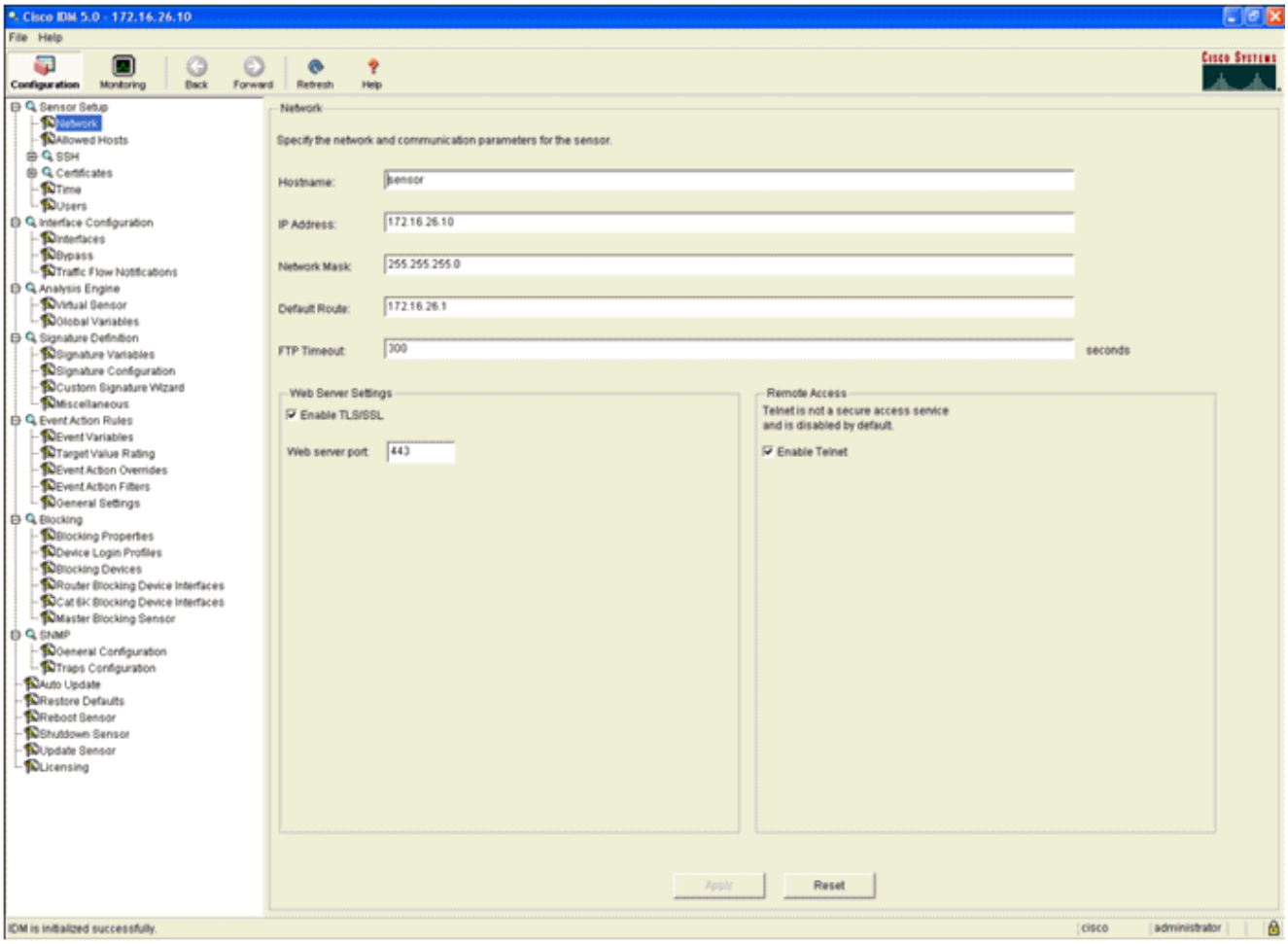
7. L'ASA est maintenant configurée pour envoyer le trafic au module IPS. **Sauvegarde de** clic sur la ligne du haut afin d'écrire les modifications à l'ASA.



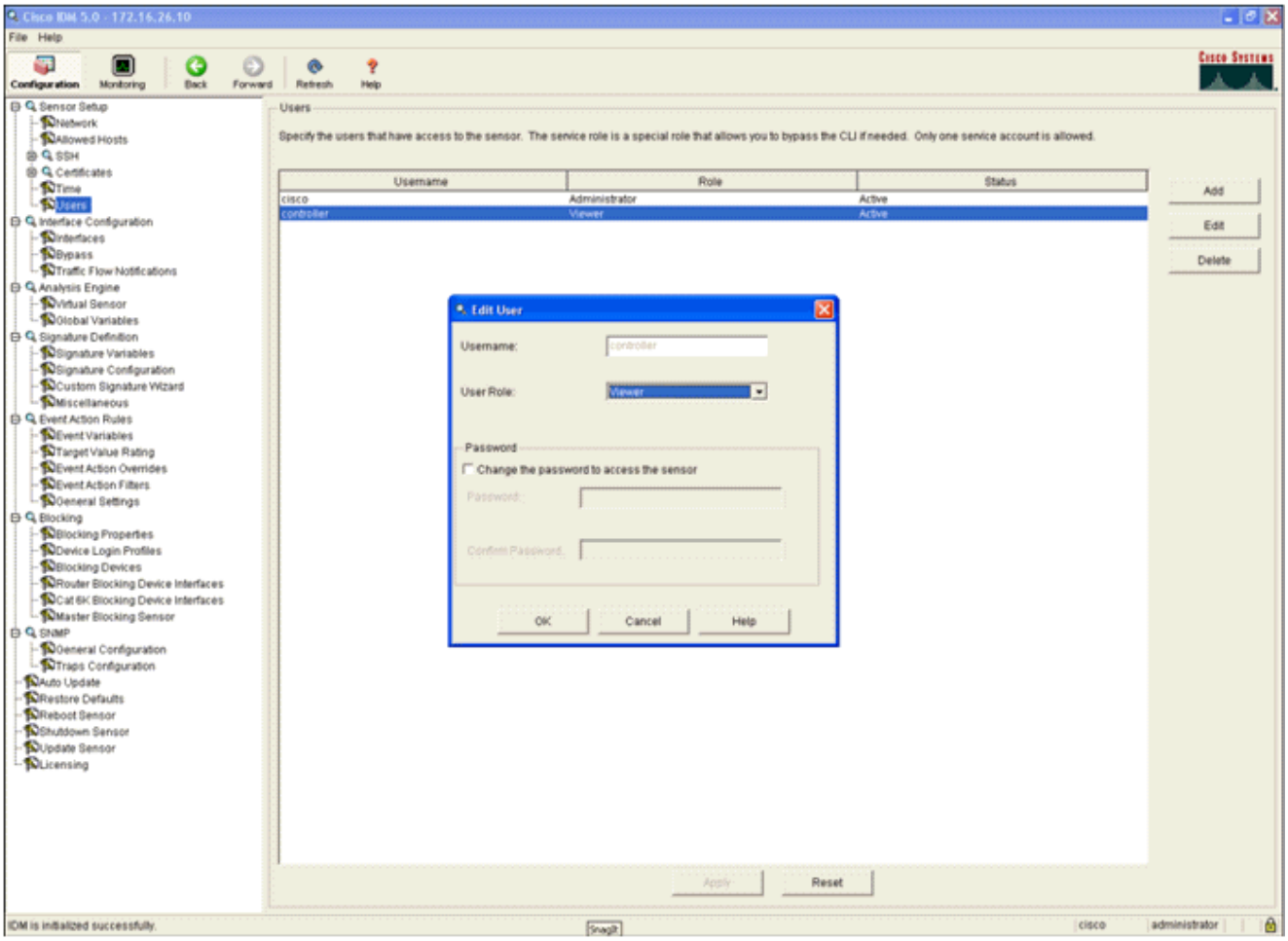
Configurez l'AIP SSM pour l'inspection du trafic

Tandis que l'ASA envoie des données au module IPS, associez l'interface d'AIP SSM à son engine virtuelle de capteur.

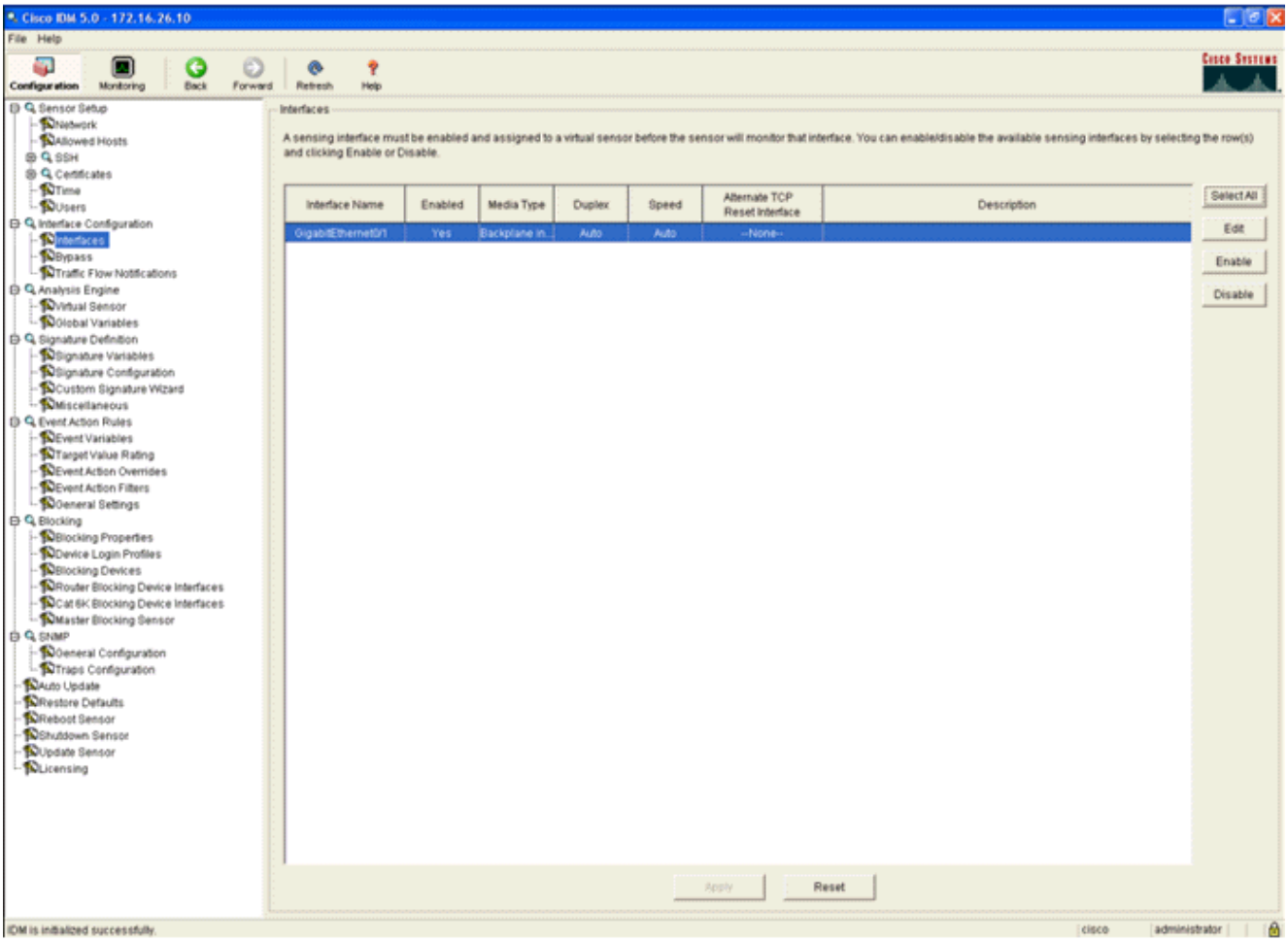
1. Procédure de connexion à l'AIP SSM utilisant IDM.



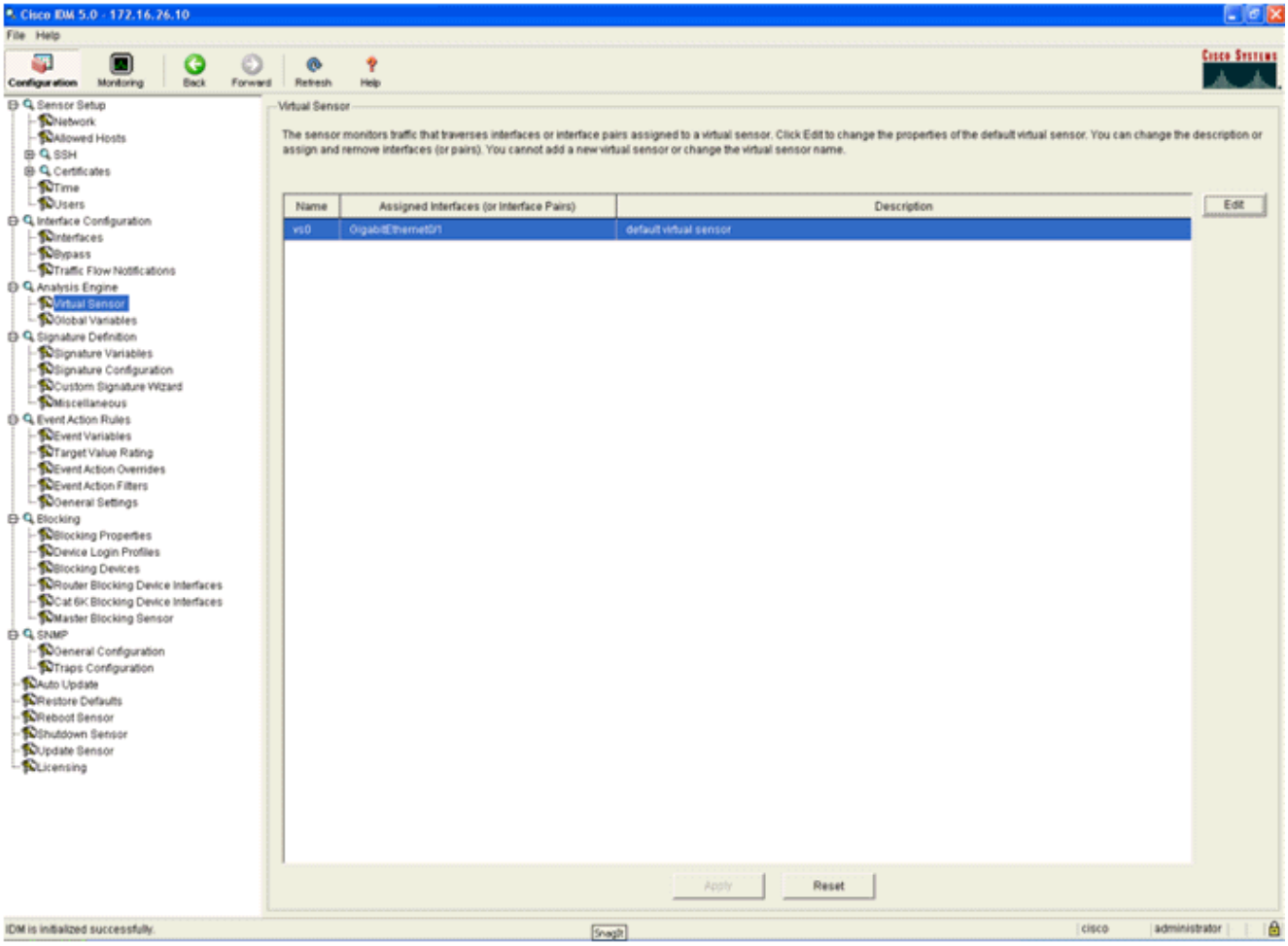
2. Ajoutez un utilisateur avec au moins des privilèges de visualiseur.



3. Activez l'interface.



4. Vérifiez la configuration virtuelle de capteur.

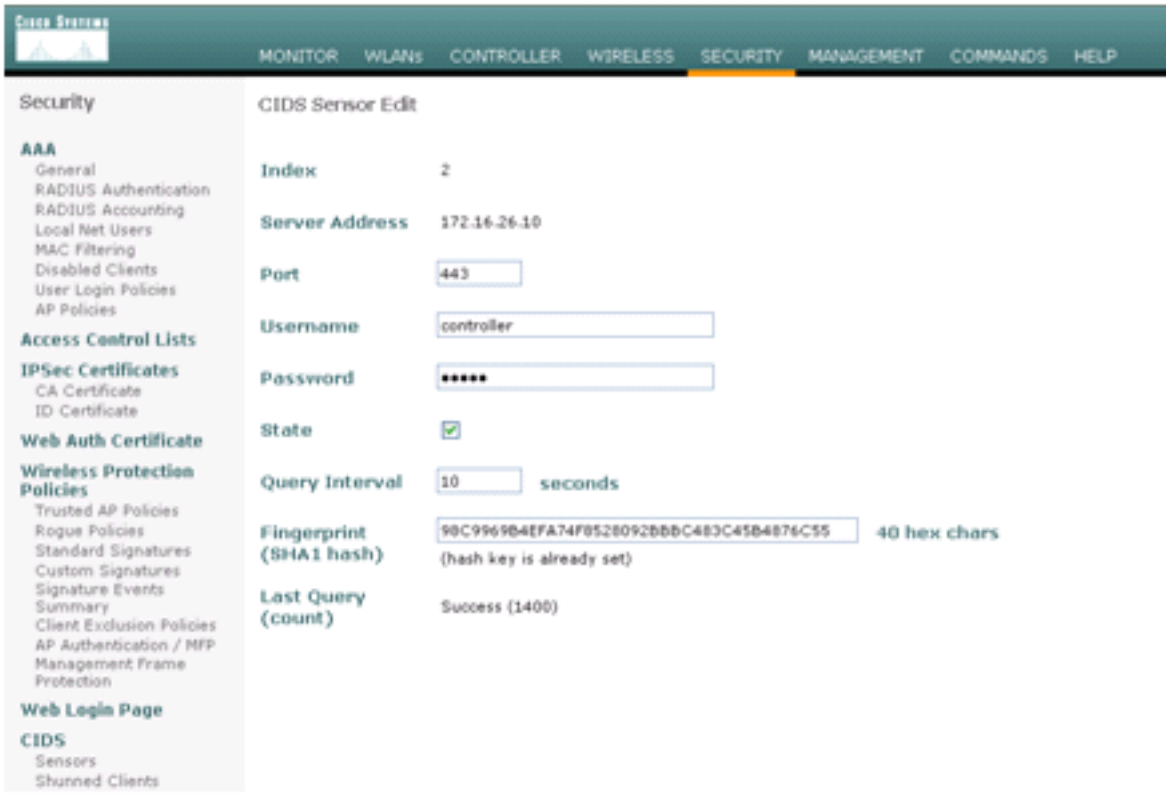


Configurez un WLC pour voter l'AIP SSM pour des blocs de client

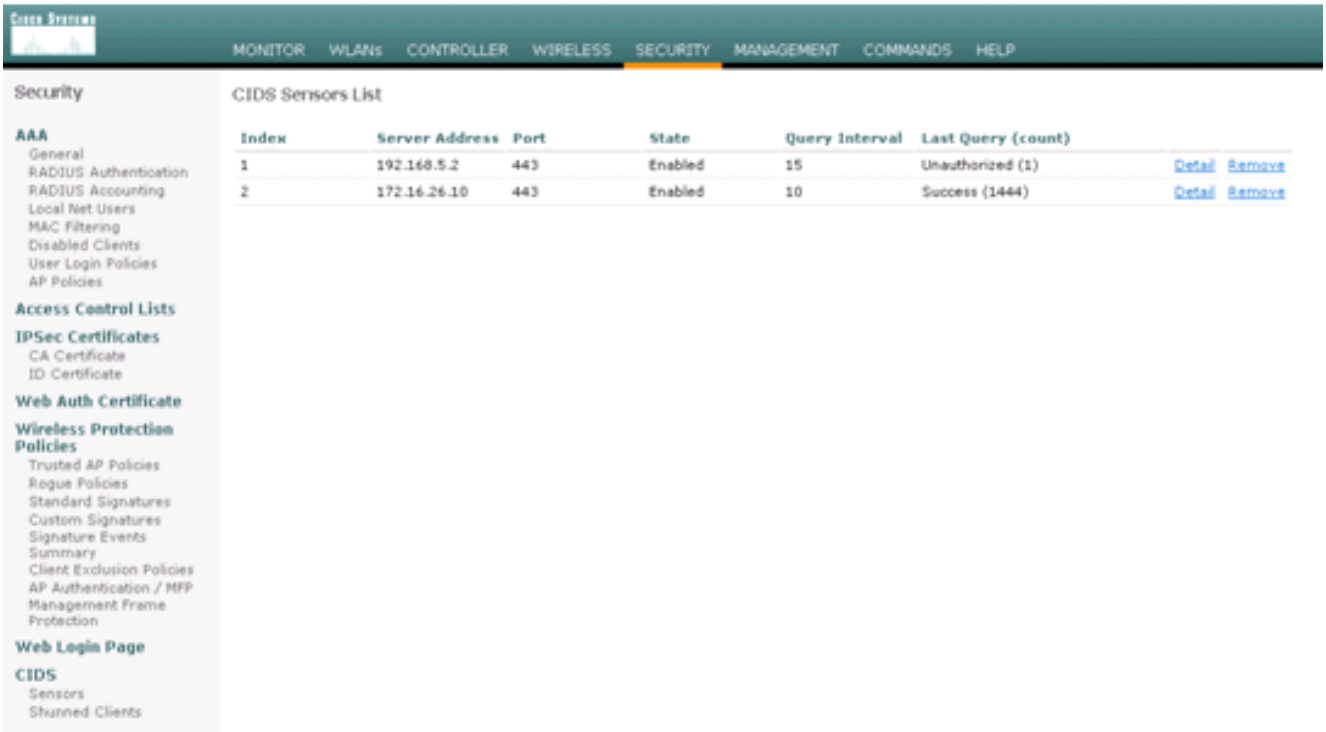
Terminez-vous ces étapes une fois que le capteur est configuré et les préparez pour être ajoutées dans le contrôleur :

1. Choisissez la **Sécurité > le CIDS > les capteurs > nouveau** dans le WLC.
2. Ajoutez l'adresse IP, nombre de port TCP, nom d'utilisateur et mot de passe que vous avez créé dans la section précédente.
3. Afin d'obtenir l'empreinte digital du capteur, exécuter cette commande dans le capteur et ajouter l'empreinte digital SHA1 sur le WLC (sans deux points). Ceci est utilisé pour sécuriser les contrôleur-à-ID votant la transmission.

```
sensor#show tls fingerprint
MD5: 07:7F:E7:91:00:46:7F:BF:11:E2:63:68:E5:74:31:0E
SHA1: 98:C9:96:9B:4E:FA:74:F8:52:80:92:BB:BC:48:3C:45:B4:87:6C:55
```



4. Vérifiez le statut de la connexion entre l'AIP SSM et le WLC.

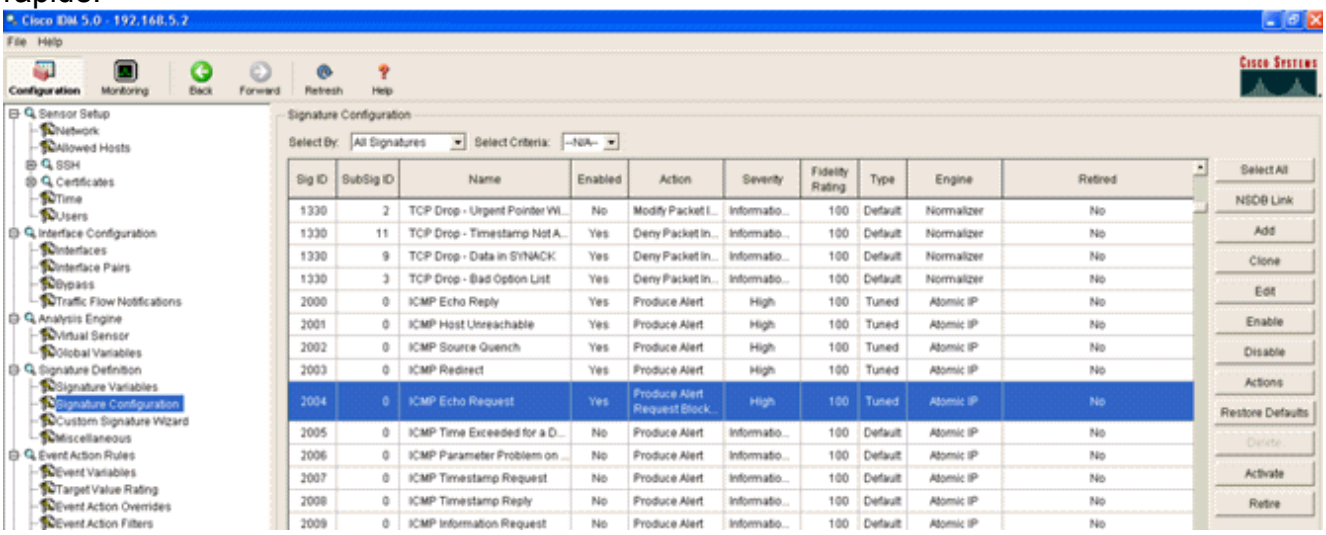


Ajoutez une signature de blocage à l'AIP SSM

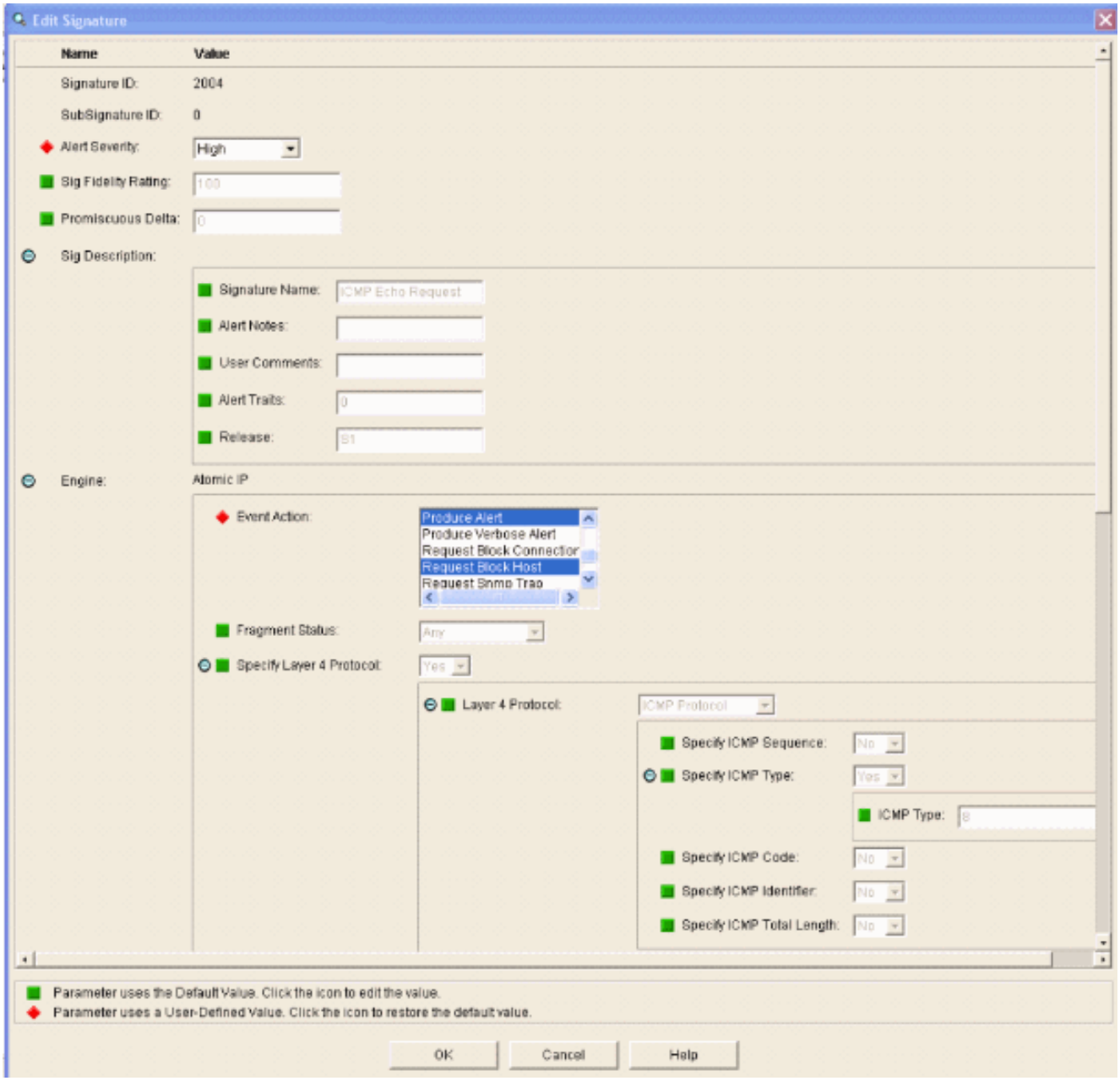
Ajoutez une signature d'inspection pour bloquer le trafic. Bien qu'il y ait beaucoup de signatures qui peuvent réaliser le travail basé sur les outils disponibles, cet exemple crée une signature qui bloque des paquets de ping.

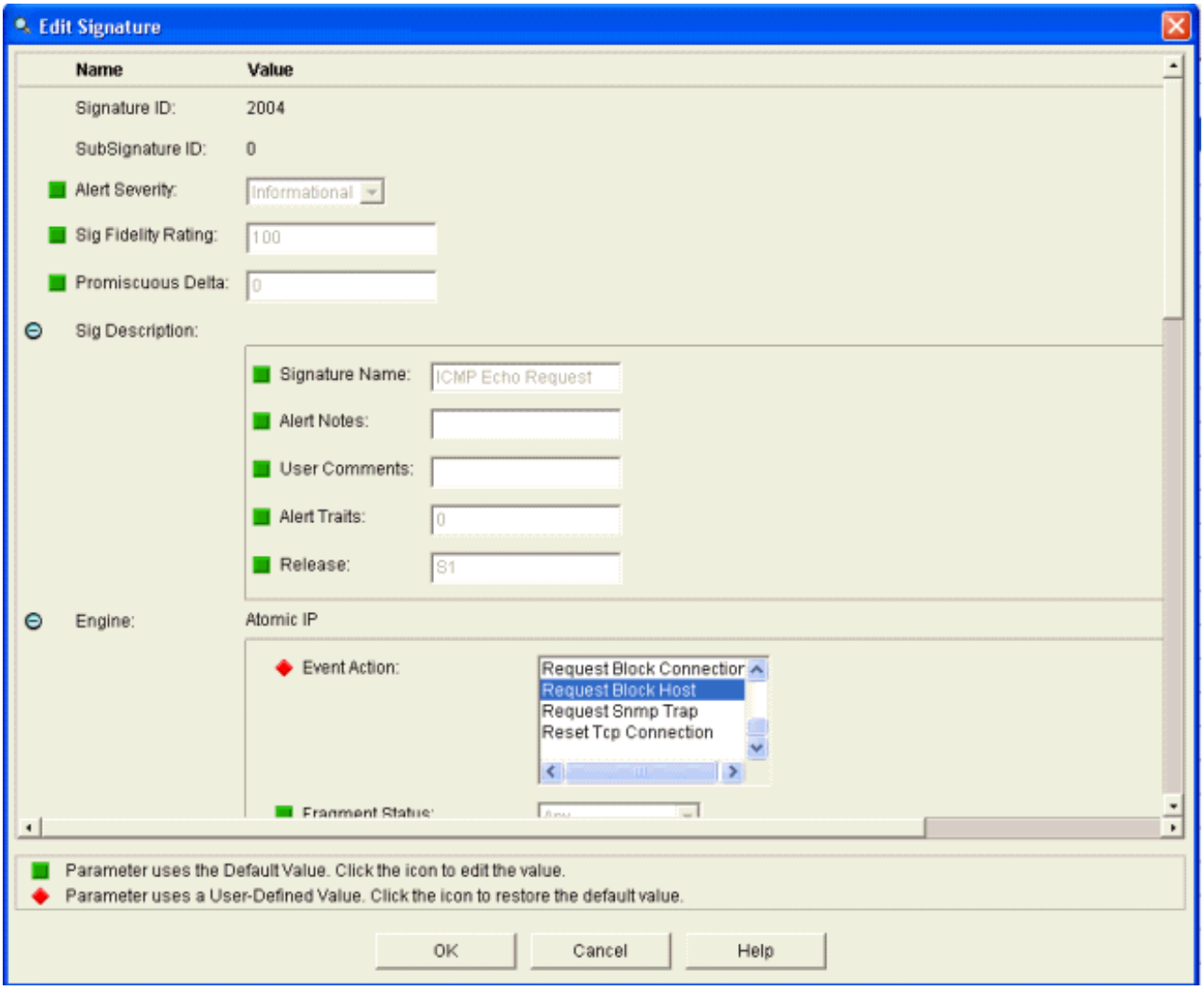
1. Sélectionnez la **signature 2004 (requête d'écho d'ICMP)** afin d'exécuter une vérification de configuration

rapide.



2. Activez la signature, placez la sévérité vigilante à la **haute** et placez l'action d'événement **de produire l'alerte** et l'**hôte de bloc de demande** afin de se terminer cette étape de vérification. Notez que l'action d'hôte de bloc de demande est la clé à signaler le WLC pour créer des exceptions de
client.


Edit Signature
Name
Value
Signature ID:
2004
SubSignature ID:
0
Alert Severity:
High
Sig Fidelity Rating:
100
Promiscuous Delta:
0
Sig Description:
Signature Name:
ICMP Echo Request
Alert Notes:
User Comments:
Alert Traits:
0
Release:
S1
Engine:
Atomic IP
Event Action:
Produce Alert
Produce Verbose Alert
Request Block Connection
Request Block Host
Request Snmp Trap
Fragment Status:
Any
Specify Layer 4 Protocol:
Yes
Layer 4 Protocol:
ICMP Protocol
Specify ICMP Sequence:
No
Specify ICMP Type:
Yes
ICMP Type:
8
Specify ICMP Code:
No
Specify ICMP Identifier:
No
Specify ICMP Total Length:
No
Parameter uses the Default Value. Click the icon to edit the value.
Parameter uses a User-Defined Value. Click the icon to restore the default value.
OK
Cancel
Help

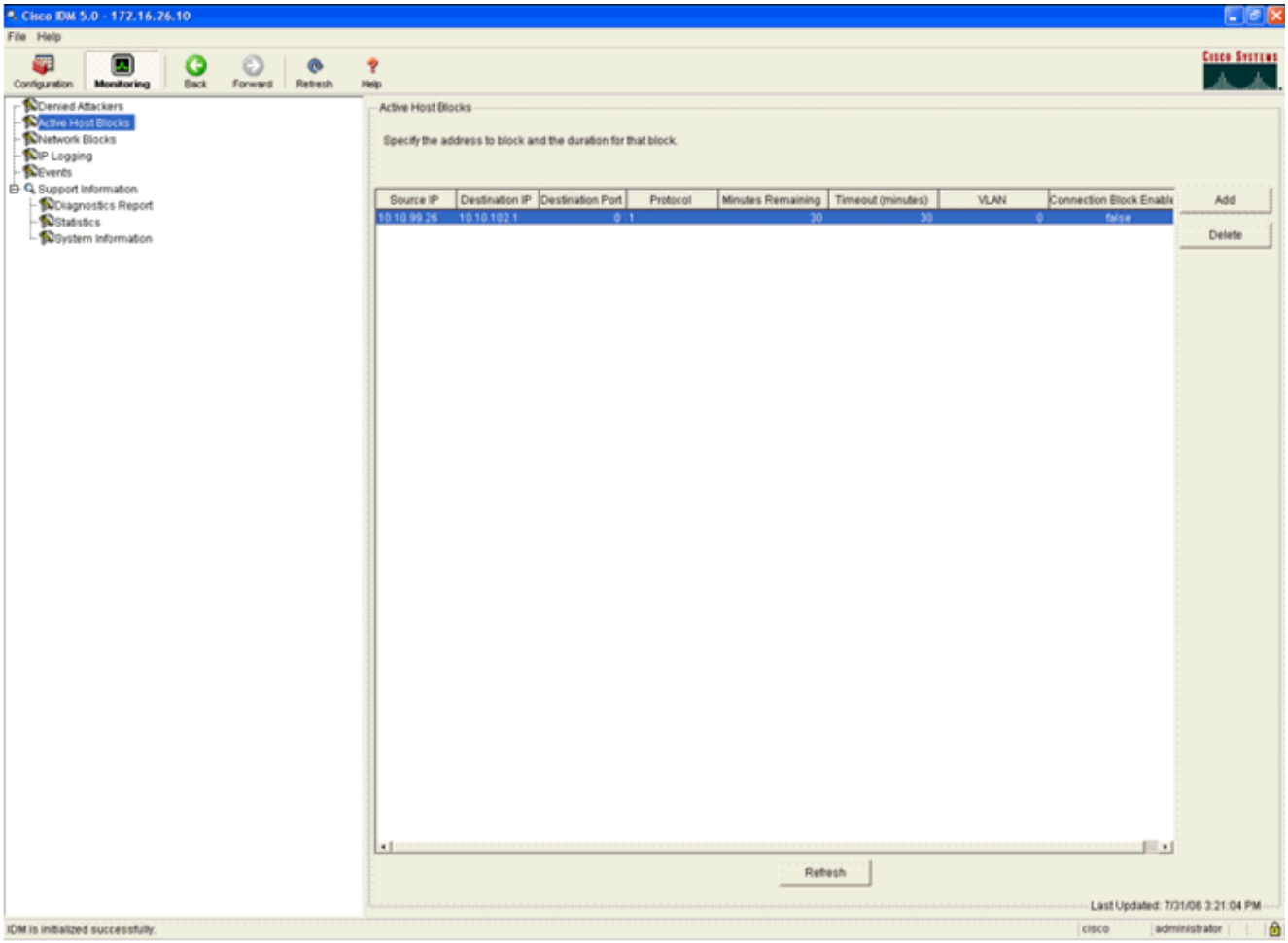


3. Cliquez sur OK afin de sauvegarder la signature.
4. Vérifiez que la signature est en activité et qu'elle est placée pour exécuter une action de blocage.
5. Cliquez sur Apply afin de commettre la signature au module.

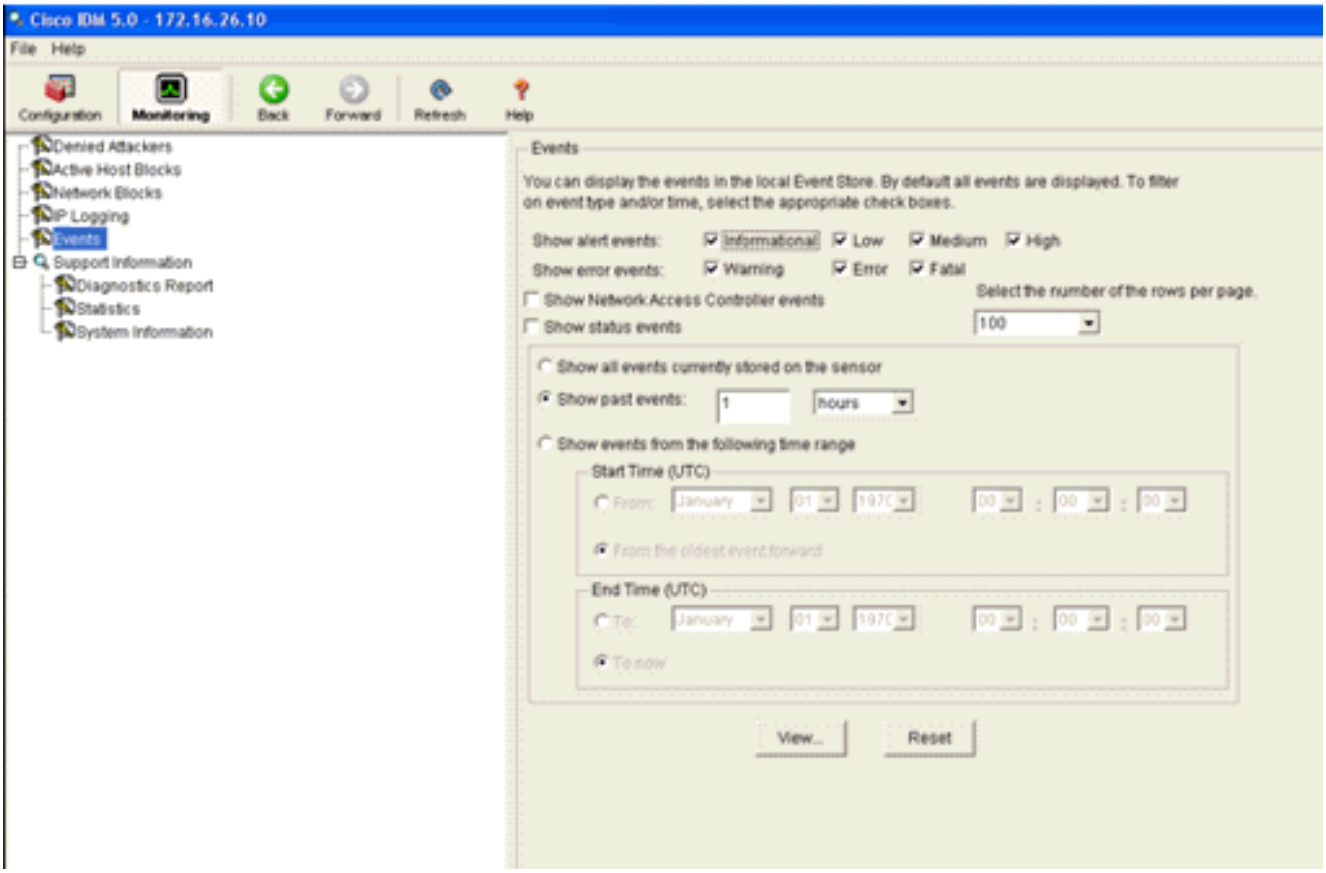
Surveillez le blocage et les événements avec IDM

Procédez comme suit :

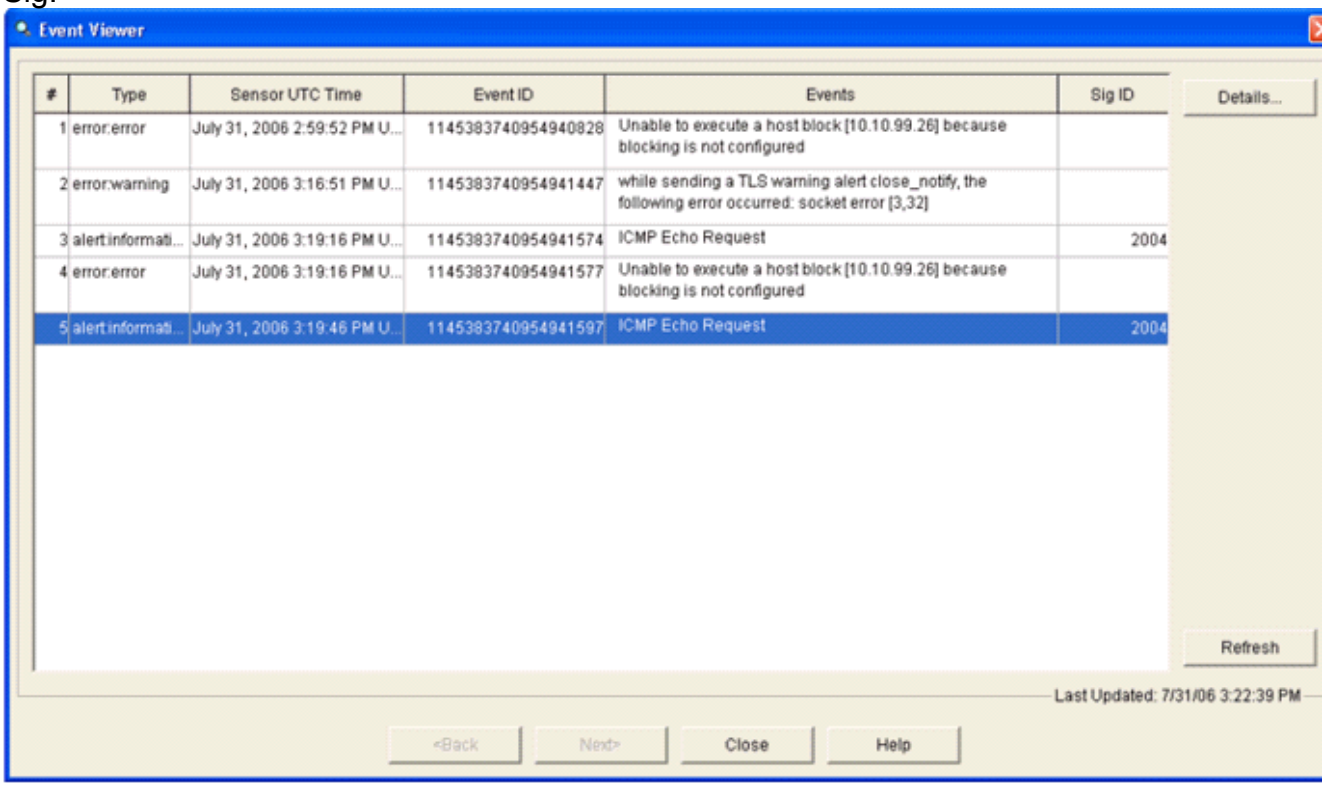
1. Quand la signature se déclenche avec succès, il y a deux endroits dans IDM pour noter ceci.La première méthode prouve aux blocs actifs que l'AIP SSM a installé. **Surveillance de** clic le long de la ligne du haut d'actions. Dans la liste d'éléments qui apparaît du côté gauche, l'**hôte actif** choisi **bloque**. Toutes les fois que les déclencheurs de signature de ping, l'hôte actif bloque la fenêtre affiche l'adresse IP du contrevenant, l'adresse du périphérique sous l'attaque, et le temps qui demeure pour ce qui est en vigueur le bloc. Le temps de blocage par défaut est de 30 minutes et est réglable. Cependant, changeant cette valeur n'est pas discuté dans ce document. Consultez la documentation relative à la configuration ASA selon les besoins pour les informations sur la façon dont changer ce paramètre. Retirez le bloc immédiatement, sélectionnez-le de la liste et puis cliquez sur Delete.



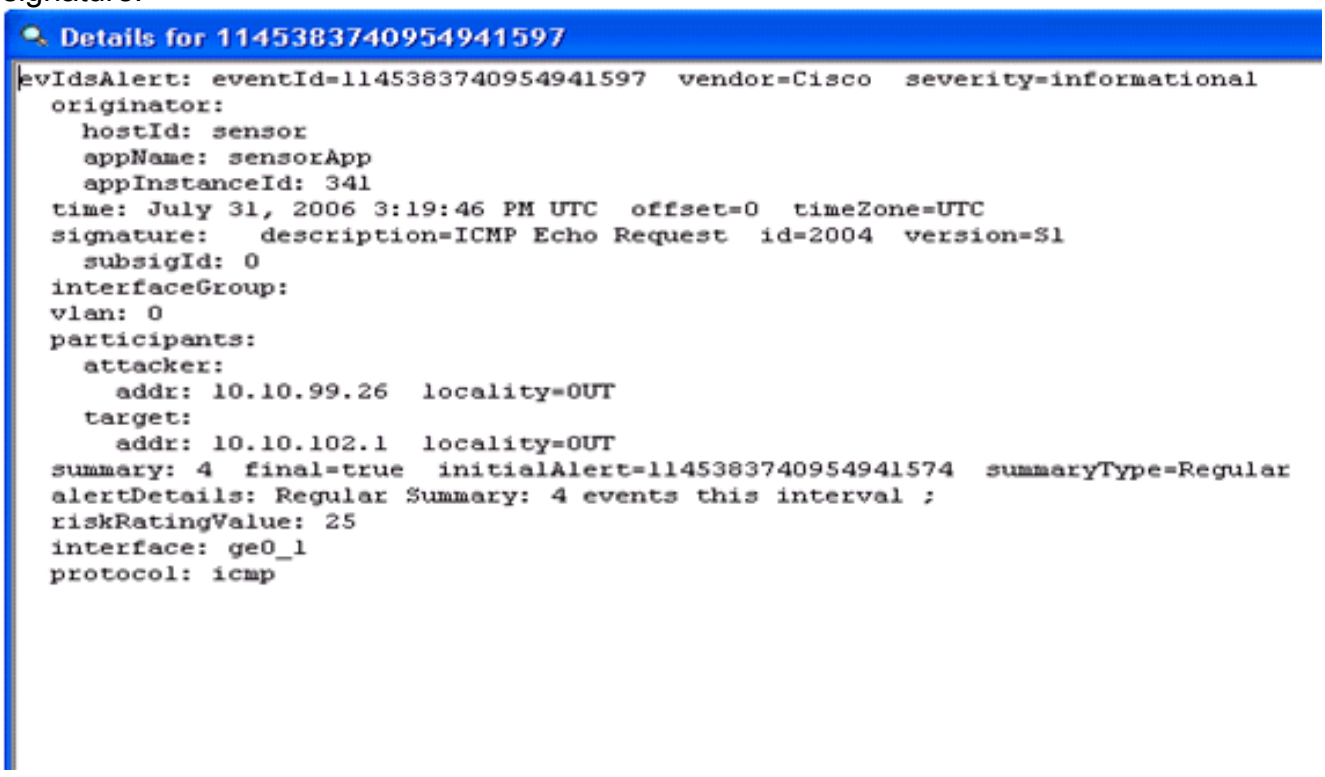
La deuxième méthode pour visualiser les signatures déclenchées utilise la mémoire tampon d'événement d'AIP SSM. De la page de surveillance IDM, les **événements** choisis dans les éléments les répertorient du côté gauche. L'utilitaire de recherche d'événements apparaît. Placez les critères de recherche et la **vue** appropriés de clic....



2. Le visualisateur d'événements apparaît alors avec une liste d'événements qui apparient les critères donnés. Parcourez la liste et trouvez la signature de requête d'écho d'ICMP modifiée dans les étapes de configuration précédente.Regardez dans la colonne d'événements pour le nom de la signature, ou bien recherchez le numéro d'identification de la signature sous la colonne d'ID de
Sig.

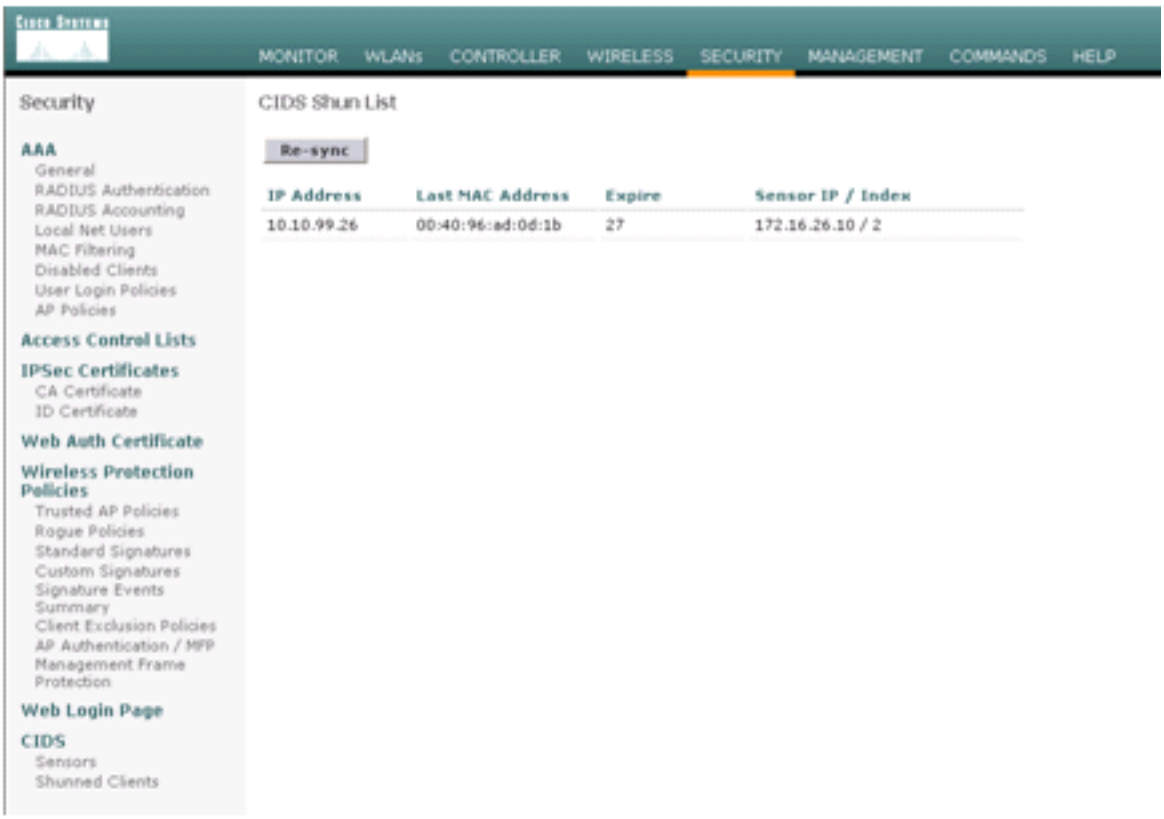


3. Après que vous localisiez la signature, double-cliquer l'entrée afin d'ouvrir une nouvelle fenêtre. La nouvelle fenêtre contient les informations détaillées sur l'événement qui a déclenché la
signature.

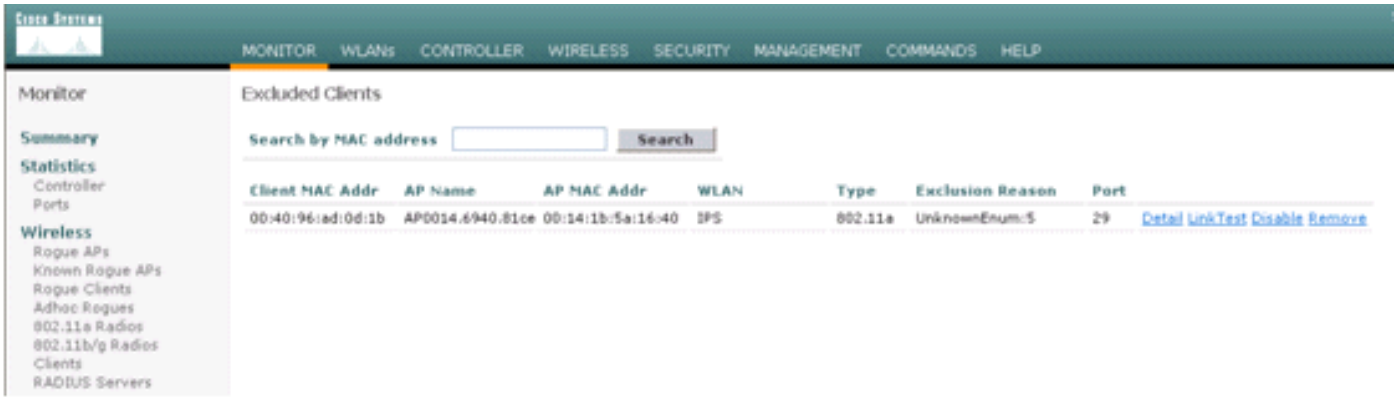


Surveillez l'exclusion de client dans un contrôleur sans-fil

Les clients évités les répertorient dans le contrôleur est remplis en ce moment du temps avec l'IP et l'adresse MAC de l'hôte.



L'utilisateur est ajouté à la liste d'exclusion de client.

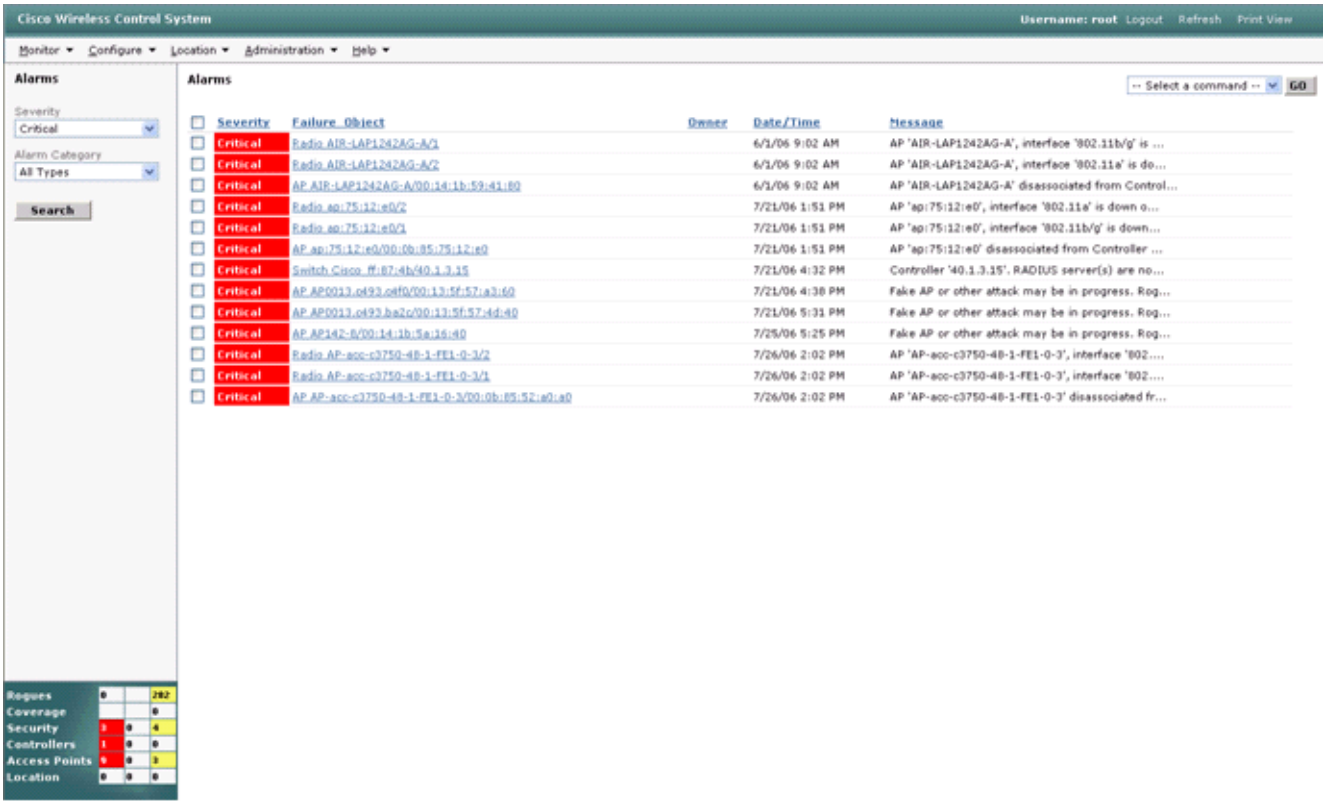


Surveillez les événements dans WCS

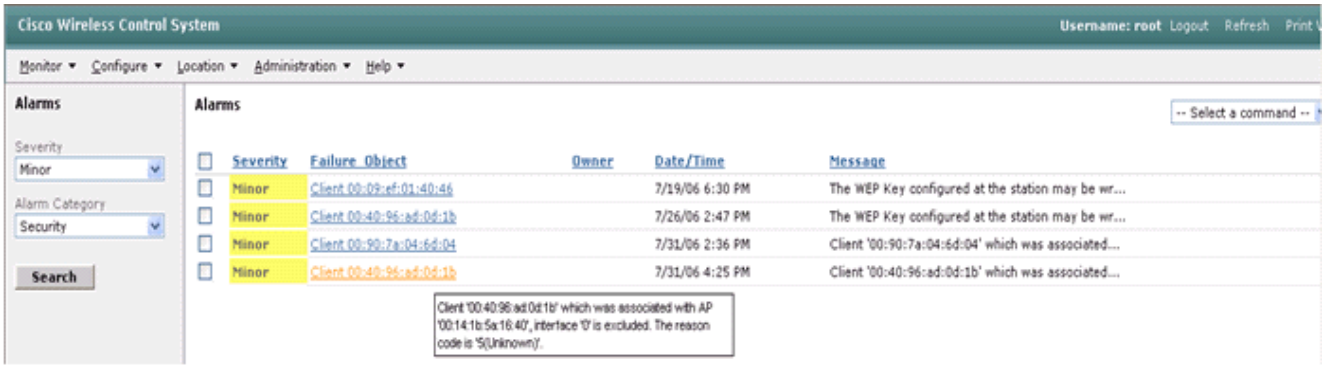
Événements de Sécurité qui déclenchent un bloc dans la cause d'AIP SSM le contrôleur pour ajouter l'adresse du contrevenant à la liste d'exclusion de client. Un événement est également généré dans WCS.

1. Utilisez le **moniteur > les alarmes** de service du menu principal WCS afin de visualiser l'événement d'exclusion. WCS affiche au commencement toutes les alarmes encombrées et présente également une fonction la recherchant du côté gauche de la fenêtre.

2. Modifiez les critères de recherche pour trouver le bloc de client. Sous la sévérité, choisissez le **mineur**, et placez également la catégorie d'alarme à la **Sécurité**.
3. **Recherche de**
   clic.



4. La fenêtre d'alarme répertorie alors seulement des alarmes de Sécurité avec la sévérité mineure. Dirigez la souris à l'événement qui a déclenché le bloc dans l'AIP SSM.En particulier, WCS affiche l'adresse MAC de la station client qui a entraîné l'alarme. Par le pointage à l'adresse appropriée, popups WCS une petite fenêtre avec les détails de l'événement. Cliquez sur le lien afin de visualiser ces mêmes détails sur une autre fenêtre.



Configuration d'échantillon de Cisco ASA

```
ciscoasa#show run
: Saved
:
ASA Version 7.1(2)
!
hostname ciscoasa
domain-name cisco.com
enable password 2KFQnbNIdI.2KYOU encrypted
```

```
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 10.10.102.2 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.26.2 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
pager lines 24
logging asdm informational
mtu inside 1500
mtu management 1500
mtu outside 1500
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
nat-control
global (outside) 102 interface
nat (inside) 102 172.16.26.0 255.255.255.0
nat (inside) 102 0.0.0.0 0.0.0.0
route inside 0.0.0.0 0.0.0.0 172.16.26.1 1
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
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 10.1.1.12 255.255.255.255 inside
http 0.0.0.0 0.0.0.0 inside
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 50
dhcpd enable management
!
class-map inside-class
 match any
```

```
!
!
policy-map inside-policy
 description IDS-inside-policy
 class inside-class
  ips promiscuous fail-open
!
service-policy inside-policy interface inside
Cryptochecksum:699d110f988e006f6c5c907473939b29
: end
ciscoasa#
```

Configuration d'échantillon de capteur de Système de protection contre les intrusions Cisco

```
sensor#show config
! ------------------------------
! Version 5.0(2)
! Current configuration last modified Tue Jul 25 12:15:19 2006
! ------------------------------
service host
network-settings
host-ip 172.16.26.10/24,172.16.26.1
telnet-option enabled
access-list 10.0.0.0/8
access-list 40.0.0.0/8
exit
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 2004 0
engine atomic-ip
event-action produce-alert|request-block-host
exit
status
enabled true
exit
exit
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service authentication
exit
! ------------------------------
service web-server
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service analysis-engine
```

```
virtual-sensor vs0
description default virtual sensor
physical-interface GigabitEthernet0/1
exit
exit
! ------------------------------
service interface
exit
! ------------------------------
service trusted-certificates
exit
sensor#
```

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Installant et utilisant le gestionnaire de périphériques 5.1 de Système de protection contre les intrusions Cisco
- Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500 - Guides de configuration
- Configurant le capteur de Système de protection contre les intrusions Cisco utilisant l'interface de ligne de commande 5.0 - configurer des interfaces
- Guide de configuration 4.0 WLC
- Soutien technique Sans fil
- Contrôleur de réseau local sans fil (WLC) - Forum Aux Questions
- Exemple de configuration de base d'un contrôleur LAN sans fil et d'un point d'accès léger
- Configurer des solutions de sécurité
- Support et documentation techniques - Cisco Systems