

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

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Présentation de Cisco IDS](#)

[Cisco IDS et WLC - Présentation de l'intégration](#)

[Arrêt IDS](#)

[Conception de l'architecture réseau](#)

[Configuration du capteur Cisco IDS](#)

[Configurer le WLC](#)

[Exemple de configuration du capteur Cisco IDS](#)

[Configurer un ASA pour IDS](#)

[Configurer AIP-SSM pour l'inspection du trafic](#)

[Configurer un WLC pour interroger l'AIP-SSM pour les blocs de clients](#)

[Ajouter une signature de blocage à AIP-SSM](#)

[Blocage et événements de surveillance avec IDM](#)

[Contrôle de l'exclusion du client dans un contrôleur sans fil](#)

[Surveiller les événements dans WCS](#)

[Exemple de configuration de Cisco ASA](#)

[Exemple de configuration du capteur du système de prévention des intrusions Cisco](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

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 complète de la sécurité, à la périphérie sans fil, à la périphérie filaire, à la périphérie WAN et à travers le data center. Lorsqu'un client associé envoie du trafic malveillant via le réseau sans fil unifié de Cisco, un périphérique IDS câblé de Cisco détecte l'attaque et envoie des requêtes d'annulation aux contrôleurs de réseau local sans fil (WLC) de Cisco, qui dissocient ensuite le périphérique client.

Cisco IPS est une solution en ligne basée sur le réseau, conçue pour identifier, classer et arrêter

avec précision le trafic malveillant, y compris les vers, les logiciels espions/publicitaires, les virus réseau et les utilisations abusives des applications, avant qu'ils n'affectent la continuité de l'activité.

Grâce à l'utilisation du logiciel Cisco IPS Sensor version 5, la solution Cisco IPS associe des services de prévention en ligne à des technologies innovantes pour améliorer la précision. Il en résulte une confiance totale dans la protection fournie de votre solution IPS, sans crainte de perte de trafic légitime. La solution Cisco IPS offre également une protection complète de votre réseau grâce à sa capacité unique à collaborer avec d'autres ressources de sécurité réseau et offre une approche proactive de la protection de votre réseau.

La solution Cisco IPS aide les utilisateurs à arrêter davantage de menaces en toute confiance grâce à l'utilisation des fonctionnalités suivantes :

- **Technologies de prévention en ligne précises** : offre une confiance inégalée pour prendre des mesures préventives contre un plus large éventail de menaces sans risque de perte de trafic légitime. Ces technologies uniques offrent une analyse intelligente, automatisée et contextuelle de vos données et vous aident à tirer le meilleur parti de votre solution de prévention des intrusions.
- **Identification des menaces multivecteurs** - Protège votre réseau contre les violations de politiques, les exploitations de vulnérabilité et les activités anormales grâce à une inspection détaillée du trafic des couches 2 à 7.
- **Collaboration réseau unique** - Améliore l'évolutivité et la résilience grâce à la collaboration réseau, notamment des techniques efficaces de capture du trafic, des fonctionnalités d'équilibrage de charge et une visibilité sur le trafic chiffré.
- **Solutions de déploiement complètes** : fournit des solutions pour tous les environnements, des petites et moyennes entreprises (PME) aux filiales en passant par les grandes entreprises et les fournisseurs de services.
- **Puissants services de gestion, de corrélation d'événements et d'assistance** : offre une solution complète comprenant des services de configuration, de gestion, de corrélation de données et d'assistance avancée. En particulier, Cisco Security Monitoring, Analysis, and Response System (MARS) identifie, isole et recommande la suppression précise des éléments offensants, pour une solution de prévention des intrusions à l'échelle du réseau. De plus, le système de contrôle des incidents Cisco empêche les nouveaux vers et virus de se propager en permettant au réseau de s'adapter rapidement et de fournir une réponse distribuée.

Combinés, ces éléments constituent une solution complète de prévention en ligne et vous donnent la confiance nécessaire pour détecter et arrêter le trafic malveillant le plus étendu avant qu'il n'affecte la continuité de l'activité. L'initiative Cisco Self-Defending Network préconise une sécurité intégrée et intégrée pour les solutions réseau. Les systèmes WLAN actuels basés sur le protocole LWAPP (Lightweight Access Point Protocol) prennent uniquement en charge les fonctions IDS de base, car il s'agit essentiellement d'un système de couche 2 et sa puissance de traitement de ligne est limitée. Cisco publie le nouveau code en temps opportun pour inclure de nouvelles fonctionnalités améliorées dans les nouveaux codes. La version 4.0 présente les dernières fonctionnalités qui incluent l'intégration d'un système WLAN basé sur LWAPP à la gamme de produits Cisco IDS/IPS. Dans cette version, l'objectif est de permettre au système Cisco IDS/IPS de demander aux WLC de bloquer certains clients d'accès aux réseaux sans fil lorsqu'une attaque est détectée entre les couches 3 et 7 et implique le client en question.

[Conditions préalables](#)

Conditions requises

Assurez-vous de respecter les conditions minimales suivantes :

- Microprogramme WLC version 4.x et ultérieure
- Il est souhaitable de savoir comment configurer Cisco IPS et Cisco WLC.

Components Used

WLC Cisco

Ces contrôleurs sont inclus avec la version logicielle 4.0 pour les modifications IDS :

- WLC Cisco, série 2000
- WLC de la gamme Cisco 2100
- WLC de la gamme Cisco 4400
- Module de services sans fil Cisco (WiSM)
- Commutateur d'accès unifié Cisco Catalyst 3750G
- Module de contrôleur LAN sans fil Cisco (WLCM)

Points d'accès

- Points d'accès légers de la gamme Cisco Aironet 1100 AG
- Points d'accès légers de la gamme Cisco Aironet 1200 AG
- Points d'accès légers de la gamme Cisco Aironet 1300
- Points d'accès légers de la gamme Cisco Aironet 1000

Gestion

- Cisco Wireless Control System (WCS)
- Capteur de la gamme Cisco 4200
- Cisco IDS Management - Cisco IDS Device Manager (IDM)

Plates-formes Cisco Unified IDS/IPS

- Capteurs de la gamme Cisco IPS 4200 avec logiciel Cisco IPS Sensor 5.x ou version ultérieure.
- SSM10 et SSM20 pour les appareils de sécurité adaptatifs de la gamme Cisco ASA 5500 avec le logiciel Cisco IPS Sensor 5.x
- Appareils de sécurité adaptatifs de la gamme Cisco ASA 5500 avec logiciel Cisco IPS Sensor 5.x
- Module de réseau Cisco IDS (NM-CIDS) avec logiciel Cisco IPS Sensor 5.x
- Module IDSM-2 (Intrusion Detection System Module 2) de la gamme Cisco Catalyst 6500 avec logiciel Cisco IPS Sensor 5.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

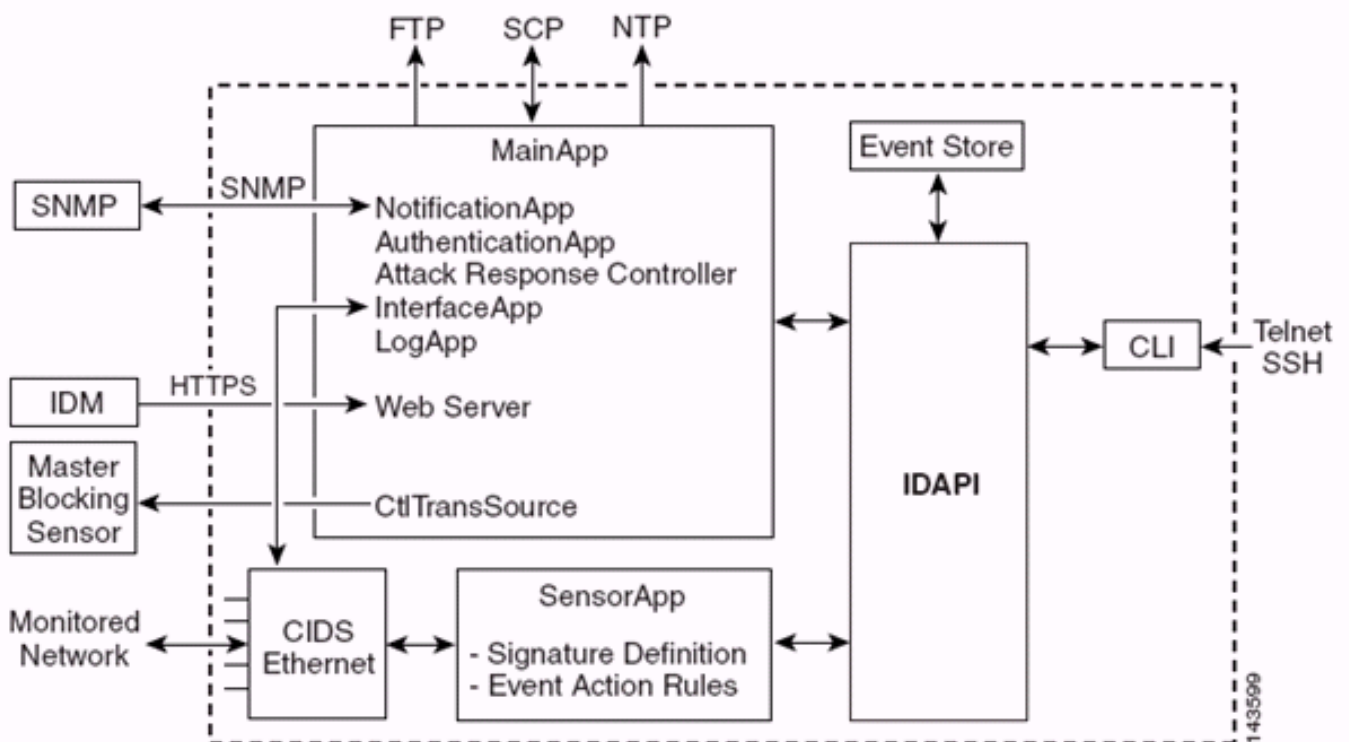
Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à

Présentation de Cisco IDS

Les principaux composants de Cisco IDS (version 5.0) sont les suivants :

- **Application de capteur** : effectue la capture et l'analyse des paquets.
- **Event Storage Management and Actions Module** - Permet le stockage des violations de stratégie.
- **Module d'imagerie, d'installation et de démarrage** : charge, initialise et démarre tous les logiciels système.
- **User Interfaces and UI Support Module** : fournit une interface de ligne de commande intégrée et l'IDM.
- **Sensor OS** : système d'exploitation hôte (basé sur Linux).



L'application de détection (logiciel IPS) se compose des éléments suivants :

- **Application principale** : initialise le système, démarre et arrête d'autres applications, configure le système d'exploitation et est responsable des mises à niveau. Il contient les composants suivants : **Control Transaction Server** : permet aux capteurs d'envoyer des transactions de contrôle utilisées pour activer la fonctionnalité de capteur de blocage principal du contrôleur de réponse aux attaques (anciennement appelé contrôleur d'accès au réseau). **Event Store** - Magasin indexé utilisé pour stocker les événements IPS (erreurs, messages d'état et d'alerte) accessibles via l'interface de ligne de commande, IDM, Adaptive Security Device Manager (ASDM) ou le protocole RDEP (Remote Data Exchange Protocol).
- **Application d'interface** : gère les paramètres physiques et de contournement et définit les interfaces associées. Les paramètres physiques comprennent les états de vitesse, de duplex et d'administration.
- **Log App** : écrit les messages de journal de l'application dans le fichier journal et les messages

d'erreur dans le magasin d'événements.

- **Contrôleur de réponse aux attaques (ARC) (anciennement appelé contrôleur d'accès réseau)** : gère les périphériques réseau distants (pare-feu, routeurs et commutateurs) afin de fournir des fonctionnalités de blocage lorsqu'un événement d'alerte s'est produit. ARC crée et applique des listes de contrôle d'accès (ACL) sur le périphérique réseau contrôlé ou utilise la commande **shun** (pare-feu).
- **Notification App** : envoie des interruptions SNMP lorsqu'elles sont déclenchées par des événements d'alerte, d'état et d'erreur. L'application de notification utilise un agent SNMP de domaine public à cette fin. Les GET SNMP fournissent des informations sur l'état d'un capteur.
- **Serveur Web (serveur HTTP RDEP2)** : fournit une interface utilisateur Web. Il fournit également un moyen de communiquer avec d'autres périphériques IPS via RDEP2 en utilisant plusieurs servlets pour fournir des services IPS.
- **Authentication App** : vérifie que les utilisateurs sont autorisés à exécuter des actions CLI, IDM, ASDM ou RDEP.
- **Application de capteur (Analysis Engine)** : effectue la capture et l'analyse des paquets.
- **CLI** : interface exécutée lorsque les utilisateurs se connectent correctement au capteur via Telnet ou SSH. Tous les comptes créés via l'interface de ligne de commande utilisent l'interface de ligne de commande comme interpréteur de commandes (à l'exception du compte de service - un seul compte de service est autorisé). Les commandes CLI autorisées dépendent des privilèges de l'utilisateur.

Toutes les applications IPS communiquent entre elles via une API (Application Program Interface) commune appelée IDAPI. Les applications distantes (autres capteurs, applications de gestion et logiciels tiers) communiquent avec les capteurs via les protocoles RDEP2 et SDEE (Security Device Event Exchange).

Notez que le capteur possède les partitions de disque suivantes :

- **Application Partition** : contient l'image système IPS complète.
- **Partition de maintenance** : image IPS spéciale utilisée pour refaire l'image de la partition d'application de l'IDSM-2. Une nouvelle image de la partition de maintenance entraîne la perte des paramètres de configuration.
- **partition de récupération** : image spéciale utilisée pour la récupération du capteur. L'amorçage dans la partition de récupération permet aux utilisateurs de refaire complètement l'image de la partition d'application. Les paramètres réseau sont préservés, mais toutes les autres configurations sont perdues.

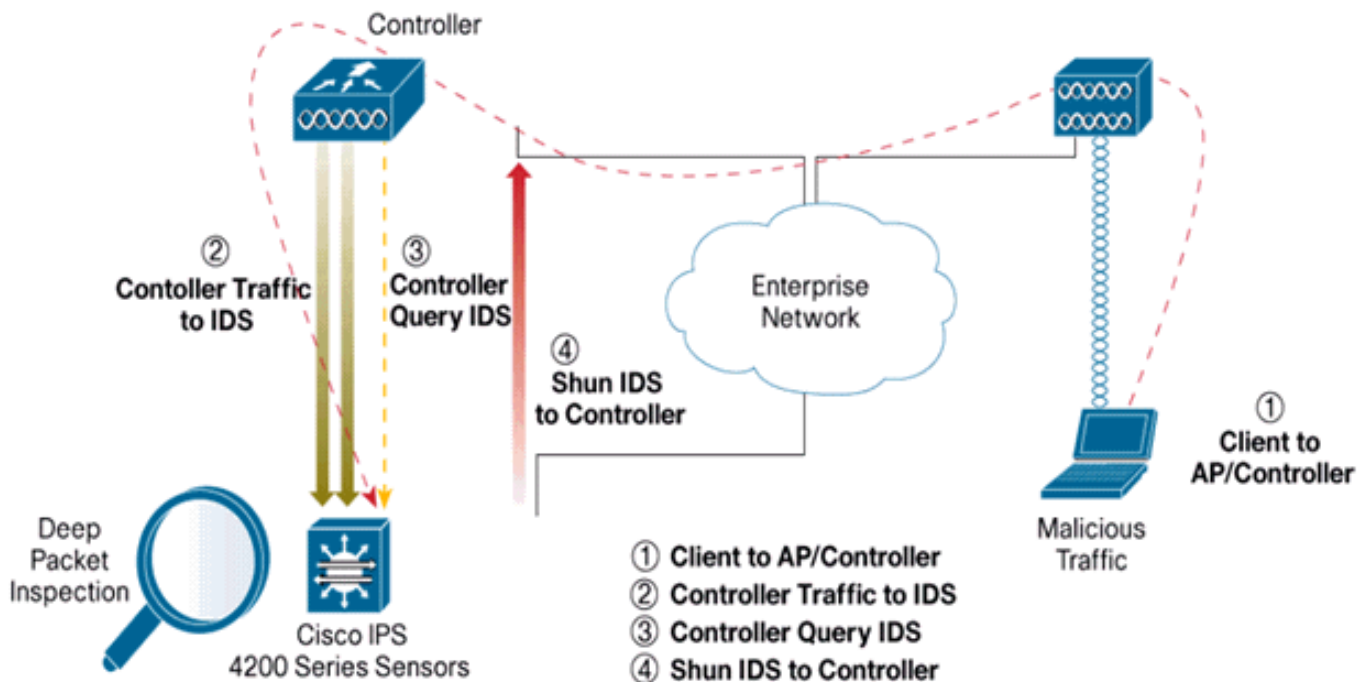
Cisco IDS et WLC - Présentation de l'intégration

La version 5.0 de Cisco IDS introduit la possibilité de configurer des actions de refus lorsque des violations de stratégie (signatures) sont détectées. En fonction de la configuration utilisateur au niveau du système IDS/IPS, une requête d'arrêt peut être envoyée à un pare-feu, un routeur ou un WLC afin de bloquer les paquets d'une adresse IP particulière.

Avec le logiciel Cisco Unified Wireless Network Version 4.0 pour les contrôleurs sans fil Cisco, une demande de désactivation doit être envoyée à un WLC afin de déclencher la liste noire ou le comportement d'exclusion du client disponible sur un contrôleur. L'interface que le contrôleur utilise pour obtenir la requête shun est l'interface de commande et de contrôle sur le système Cisco IDS.

- Le contrôleur permet de configurer jusqu'à cinq capteurs IDS sur un contrôleur donné.

- Chaque capteur IDS configuré est identifié par son adresse IP ou son nom de réseau qualifié et ses informations d'autorisation.
- Chaque capteur IDS peut être configuré sur un contrôleur avec un taux de requête unique en secondes.



Arrêt IDS

Le contrôleur interroge le capteur à la vitesse de requête configurée afin de récupérer tous les événements shun. Une requête shun donnée est distribuée dans tout le groupe de mobilité du contrôleur qui récupère la requête du capteur IDS. Chaque requête de suppression d'une adresse IP client est en vigueur pour la valeur de délai d'attente spécifiée en secondes. Si la valeur de délai d'attente indique une heure infinie, l'événement shun ne se termine que si l'entrée shun est supprimée sur le système IDS. L'état du client ignoré est maintenu sur chaque contrôleur du groupe de mobilité, même si tous les contrôleurs ou l'un d'entre eux sont réinitialisés.

Remarque : La décision de ne pas utiliser un client est toujours prise par le capteur IDS. Le contrôleur ne détecte pas les attaques de couche 3. Il est beaucoup plus compliqué de déterminer que le client lance une attaque malveillante au niveau de la couche 3. Le client est authentifié au niveau de la couche 2, ce qui est suffisant pour que le contrôleur accorde l'accès à la couche 2.

Remarque : Par exemple, si un client reçoit une adresse IP (ignorée) offensante précédente, il est possible de débloquer l'accès de couche 2 pour ce nouveau client jusqu'au délai d'expiration du capteur. Même si le contrôleur donne accès à la couche 2, le trafic client peut être bloqué sur les routeurs de la couche 3 de toute façon, car le capteur informe également les routeurs de l'événement shun.

Supposez qu'un client a l'adresse IP A. Maintenant, lorsque le contrôleur interroge le système IDS pour les événements de shun, le système IDS envoie la requête de shun au contrôleur avec l'adresse IP A comme adresse IP cible. Maintenant, le contrôleur noir répertorie ce client A. Sur le contrôleur, les clients sont désactivés en fonction d'une adresse MAC.

Maintenant, supposez que le client change son adresse IP de A à B. Au cours du prochain

sondage, le contrôleur obtient une liste de clients ignorés en fonction de l'adresse IP. Cette fois encore, l'adresse IP A figure toujours dans la liste des adresses ignorées. Mais comme le client a changé son adresse IP de A à B (qui ne figure pas dans la liste des adresses IP ignorées), ce client avec une nouvelle adresse IP de B est libéré une fois que le délai d'expiration des clients noirs répertoriés est atteint sur le contrôleur. Maintenant, le contrôleur commence à autoriser ce client avec une nouvelle adresse IP de B (mais l'adresse MAC du client reste la même).

Par conséquent, bien qu'un client reste désactivé pour la durée du délai d'exclusion du contrôleur et soit réexclu s'il acquiert de nouveau son adresse DHCP précédente, ce client n'est plus désactivé si l'adresse IP du client ignoré change. Par exemple, si le client se connecte au même réseau et que le délai de bail DHCP n'est pas expiré.

Les contrôleurs prennent uniquement en charge la connexion au système IDS pour les demandes de mise en garde de clients qui utilisent le port de gestion sur le contrôleur. Le contrôleur se connecte à l'IDS pour l'inspection des paquets via les interfaces VLAN applicables qui transportent le trafic client sans fil.

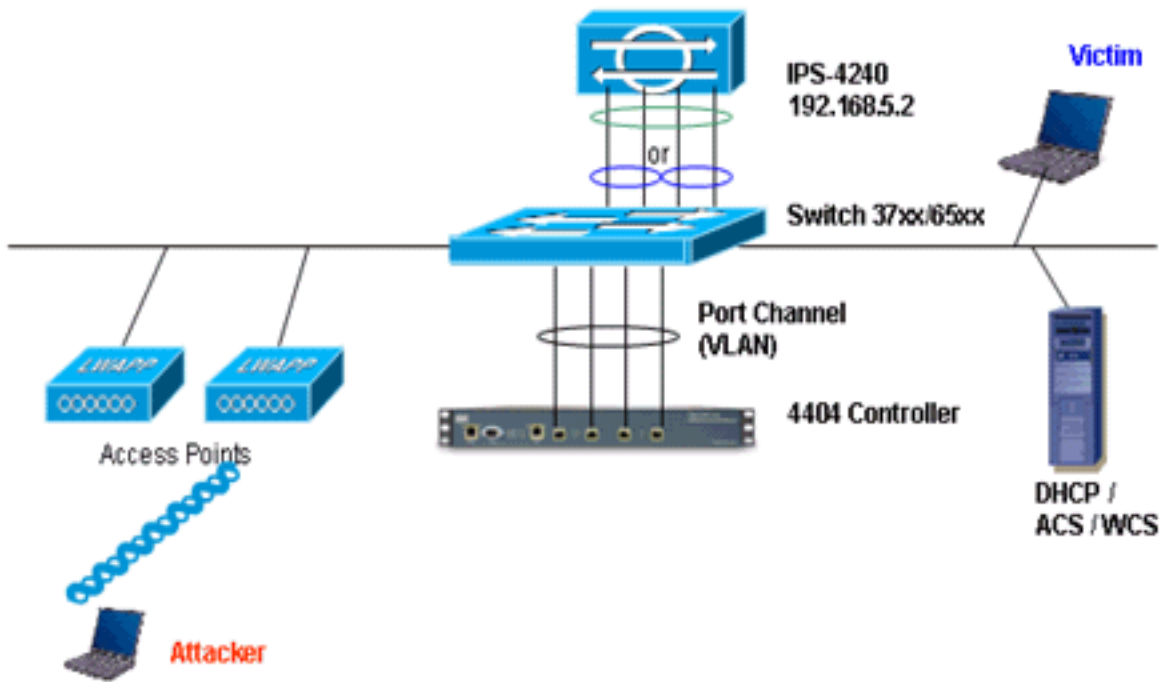
Sur le contrôleur, la page Désactiver les clients affiche chaque client qui a été désactivé via une demande de capteur IDS. La commande CLI **show** affiche également une liste de clients inscrits sur une liste noire.

Sur le WCS, les clients exclus sont affichés sous le sous-onglet Sécurité.

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

1. Installez et connectez l'appareil IDS sur le même commutateur que celui où réside le contrôleur sans fil.
2. Mettre en miroir (SPAN) les ports WLC qui transportent le trafic du client sans fil vers l'appareil IDS.
3. L'appareil IDS reçoit une copie de chaque paquet et inspecte le trafic des couches 3 à 7.
4. L'appareil IDS offre un fichier de signature téléchargeable, qui peut également être personnalisé.
5. L'appareil IDS génère l'alarme avec une action d'évitement d'événement lorsqu'une signature d'attaque est détectée.
6. Le WLC interroge l'IDS pour les alarmes.
7. Lorsqu'une alarme avec l'adresse IP d'un client sans fil, associé au WLC, est détectée, elle place le client dans la liste d'exclusion.
8. Un déroutement est généré par le WLC et WCS est averti.
9. L'utilisateur est supprimé de la liste d'exclusion après la période spécifiée.

[Conception de l'architecture réseau](#)



Le contrôleur de réseau local sans fil Cisco est connecté aux interfaces gigabit du Catalyst 6500. Créez un port-canal pour les interfaces 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 aux interfaces gigabit 5/1 et 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 Promiscuité** ou vous pouvez les jumeler pour créer des interfaces en ligne pour le **mode Inline Sensing**.

En mode Promiscuité, les paquets ne transitent pas par le capteur. Le capteur analyse une copie du trafic surveillé plutôt que le paquet transféré réel. L'avantage d'un fonctionnement en mode Promiscuité est que le capteur n'affecte pas le flux de paquets avec le trafic transféré.

Remarque : Le [diagramme d'architecture](#) n'est qu'un exemple de configuration de l'architecture intégrée WLC et IPS. L'exemple de configuration présenté ici explique l'interface de détection IDS agissant en mode Promiscuité. Le [diagramme d'architecture](#) montre les interfaces de détection en cours d'association pour agir en mode Paire en ligne. Référez-vous à [Mode en ligne](#) pour plus d'informations sur le mode Interface en ligne.

Dans cette configuration, on suppose que l'interface de détection agit en mode Promiscuité. L'interface de surveillance du Cisco IDS Sensor est connectée à l'interface Gigabit 5/3 du Catalyst 6500. Créez une session de surveillance sur le Catalyst 6500 où l'interface port-channel est la source des paquets et la destination est l'interface gigabit où l'interface de surveillance du capteur IPS Cisco est connectée. Ceci répliquera tout le trafic d'entrée et de sortie des interfaces filaires du contrôleur vers le système IDS pour l'inspection des couches 3 à 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#
```

[Configuration du capteur Cisco IDS](#)

La configuration initiale du Cisco IDS Sensor est effectuée à partir du port de console ou en

connectant un moniteur et un clavier au capteur.

1. Connectez-vous 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 votre mot de passe à l'invite de connexion.**Remarque** : le nom d'utilisateur et le mot de passe par défaut sont tous deux cisco. Vous êtes invité à les modifier la première fois que vous vous connectez à l'appliance. Vous devez d'abord saisir le mot de passe UNIX, cisco. Ensuite, vous devez saisir 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.**Remarque** : Il s'agit de l'interface de commande et de contrôle sur le système IDS utilisé pour communiquer avec le contrôleur. Cette adresse doit être routable vers l'interface de gestion du contrôleur. Les interfaces de détection ne nécessitent pas d'adressage. La liste d'accès doit inclure l'adresse de l'interface de gestion du ou des contrôleurs, ainsi que les adresses autorisées pour la gestion du système IDS.

```
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
```

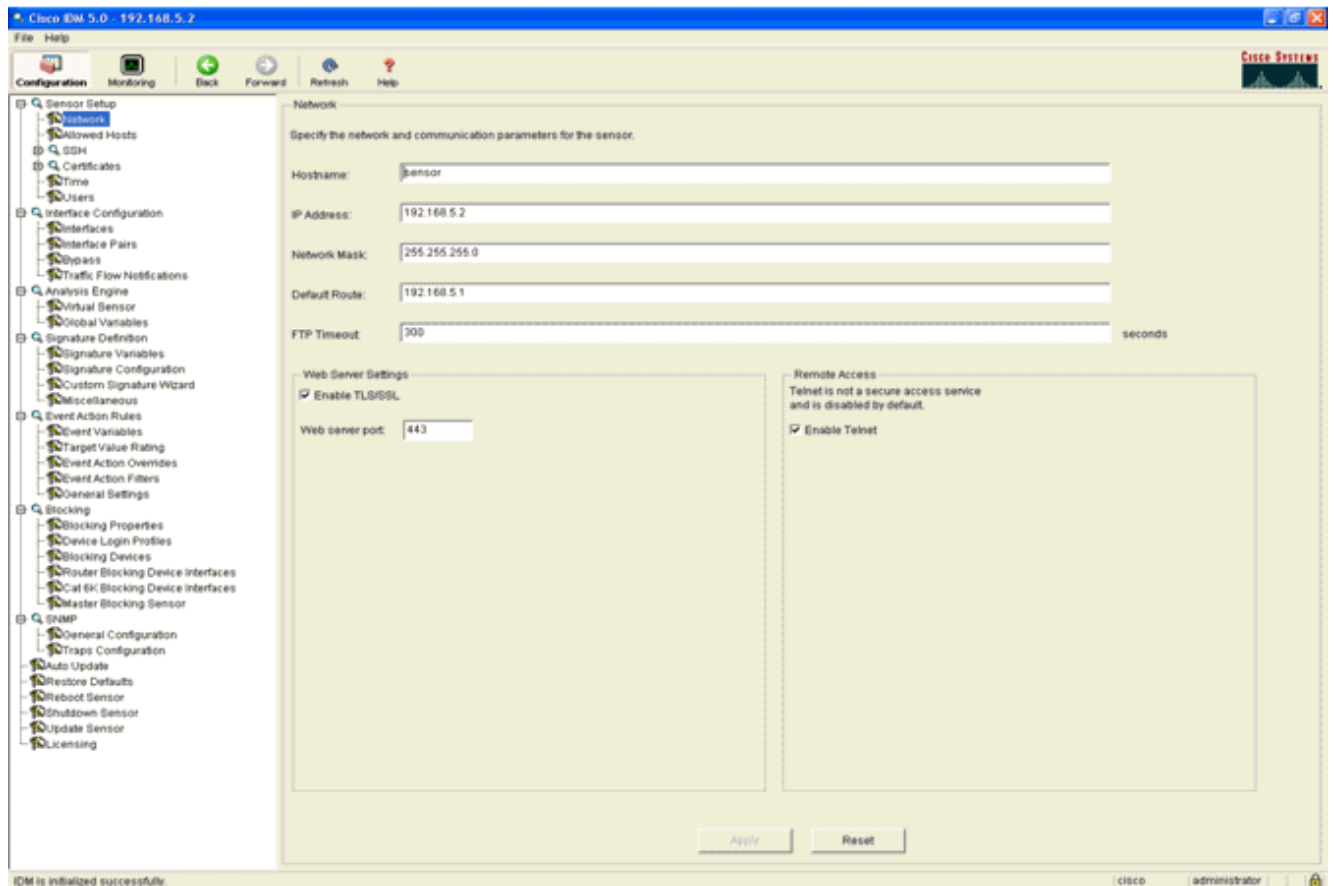
```
--- 192.168.5.1 ping statistics ---
```

```
4 packets transmitted, 4 packets received, 0% packet loss
```

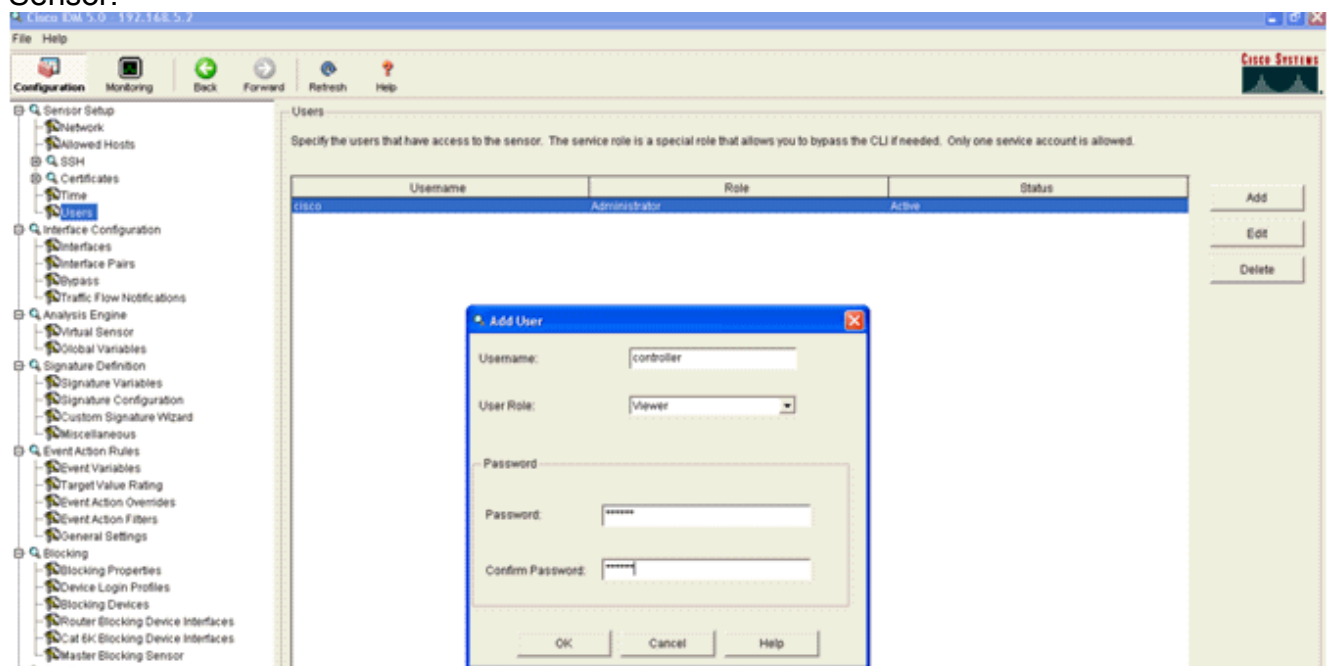
```
round-trip min/avg/max = 0.3/0.6/1.0 ms
```

sensor#

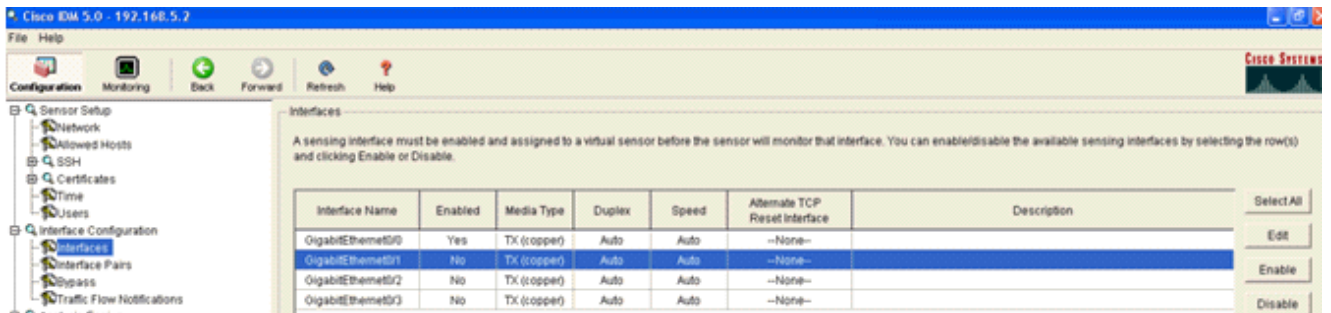
4. Vous pouvez maintenant configurer le capteur IPS à partir de l'interface utilisateur graphique. Pointez le navigateur vers l'adresse IP de gestion du capteur. Cette image affiche un exemple dans lequel le capteur est configuré avec 192.168.5.2.



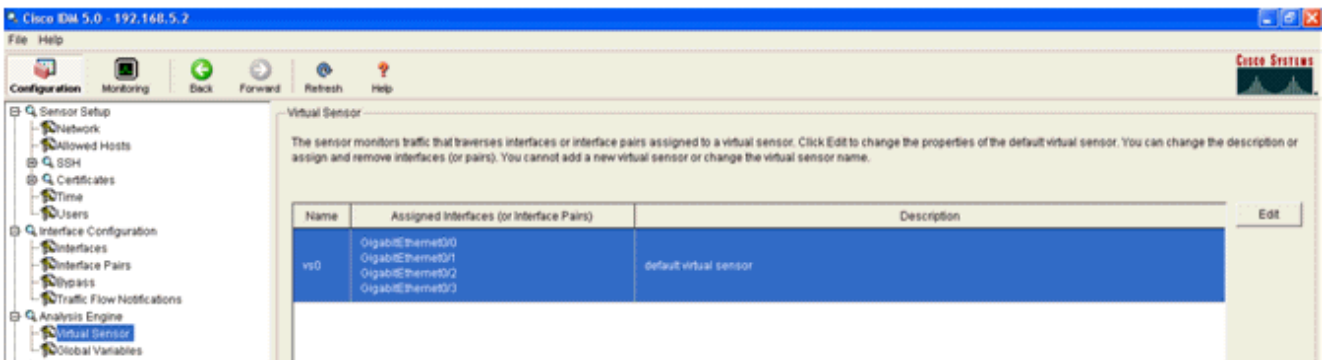
5. Ajoutez un utilisateur que le WLC utilise pour accéder aux événements IPS Sensor.



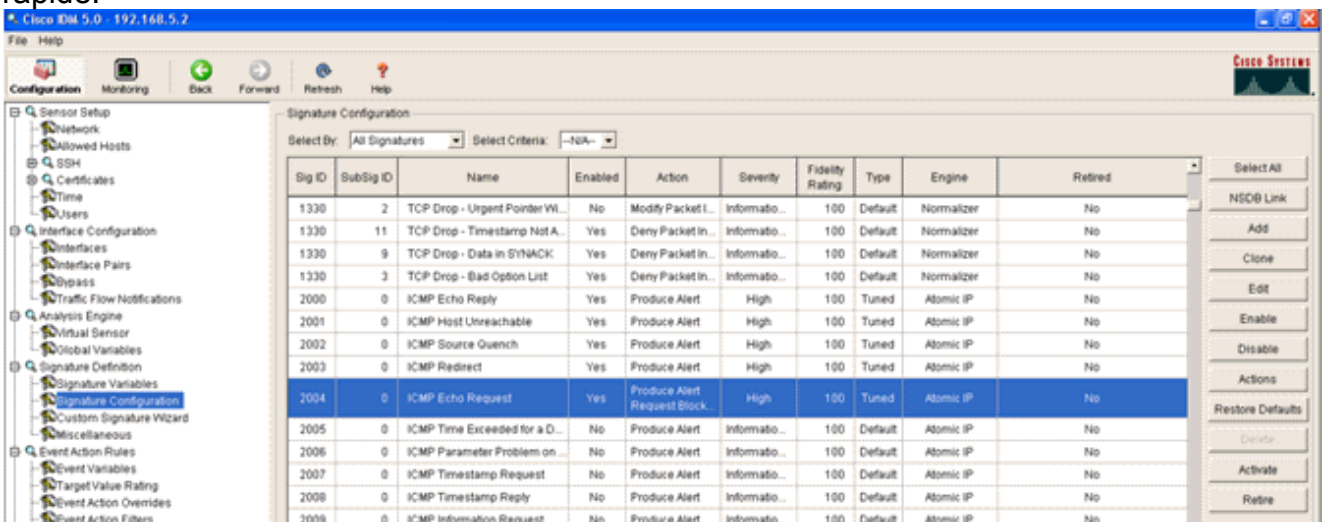
6. Activez les interfaces de surveillance.



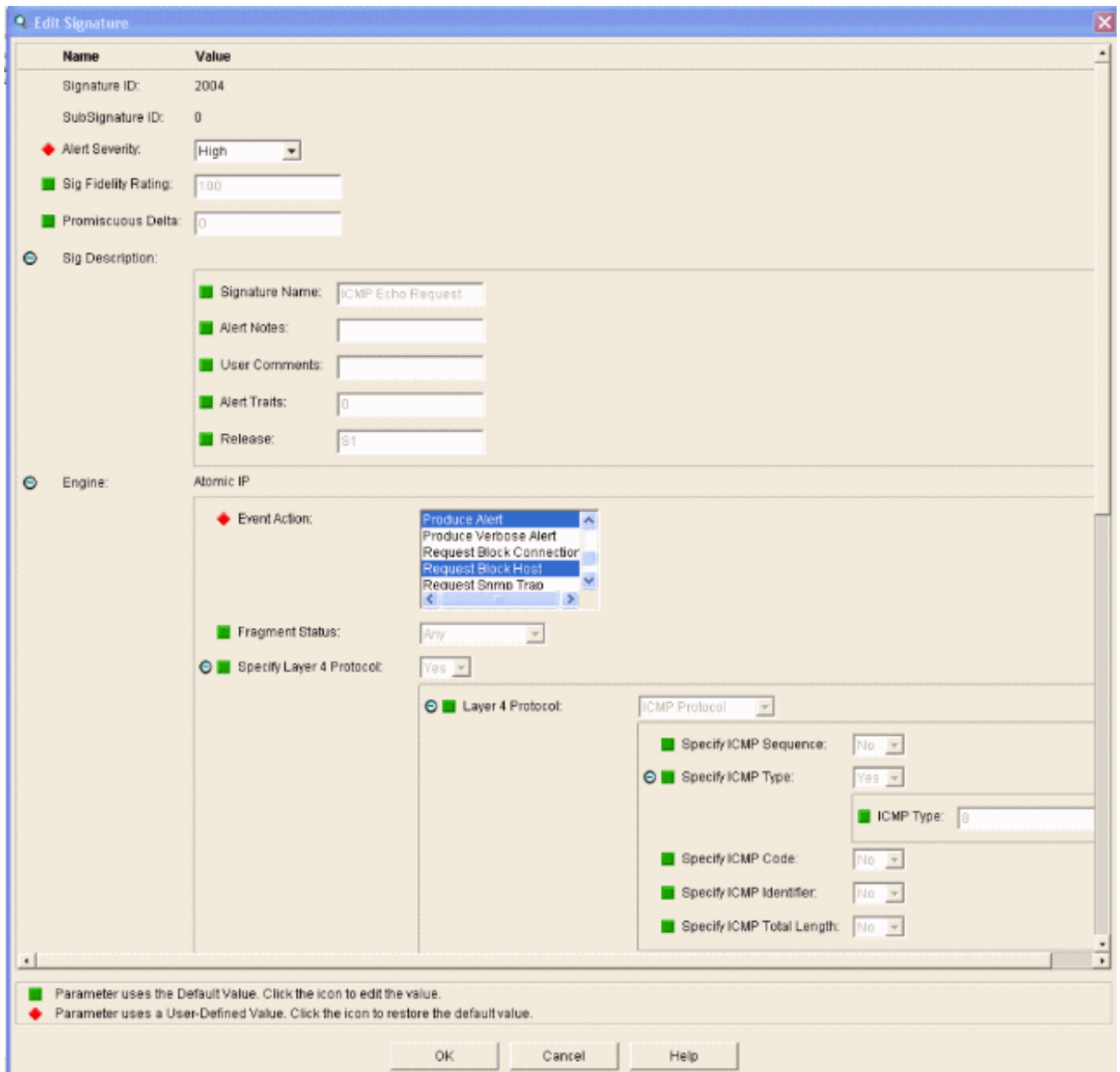
Les interfaces de surveillance doivent être ajoutées au moteur d'analyse, comme le montre cette fenêtre



7. Sélectionnez la signature 2004 (ICMP Echo Request) afin d'effectuer une vérification de configuration rapide.



La signature doit être activée, la gravité de l'alerte définie sur **Élevé** et l'action d'événement définie sur **Produire l'alerte** et l'hôte de bloc de demande pour que cette étape de vérification soit terminée.



Configurer le WLC

Complétez ces étapes afin de configurer le WLC :

1. Une fois l'appareil IPS configuré et prêt à être ajouté au contrôleur, sélectionnez **Security > CIDS > Sensors > New**.
2. Ajoutez l'adresse IP, le numéro de port TCP, le nom d'utilisateur et le mot de passe que vous avez précédemment créés. Afin d'obtenir l'empreinte du capteur IPS, exécutez cette commande dans le capteur IPS et ajoutez l'empreinte SHA1 sur le WLC (sans les deux-points). Cette option permet de sécuriser la communication d'interrogation contrôleur/IDS.

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

The screenshot shows the 'CIDS Sensor Add' configuration page in the Cisco IPS GUI. The left sidebar contains a navigation menu with categories like AAA, Access Control Lists, Network Access Control, IPsec Certificates, Web Auth Certificate, Wireless Protection Policies, Web Login Page, and CIDS. The main content area is titled 'CIDS Sensor Add' and includes the following fields:

- Index:** 1
- Server Address:** 192.168.5.2
- Port:** 443
- Username:** controller
- Password:** [masked]
- Confirm Password:** [masked]
- Query Interval:** 15 seconds
- State:**
- Fingerprint (SHA1 hash):** 1662E996362A9A1EF08B99A7C1645F5CB56A8842 (40 hex chars)

Buttons for '< Back' and 'Apply' are located at the top right of the configuration area.

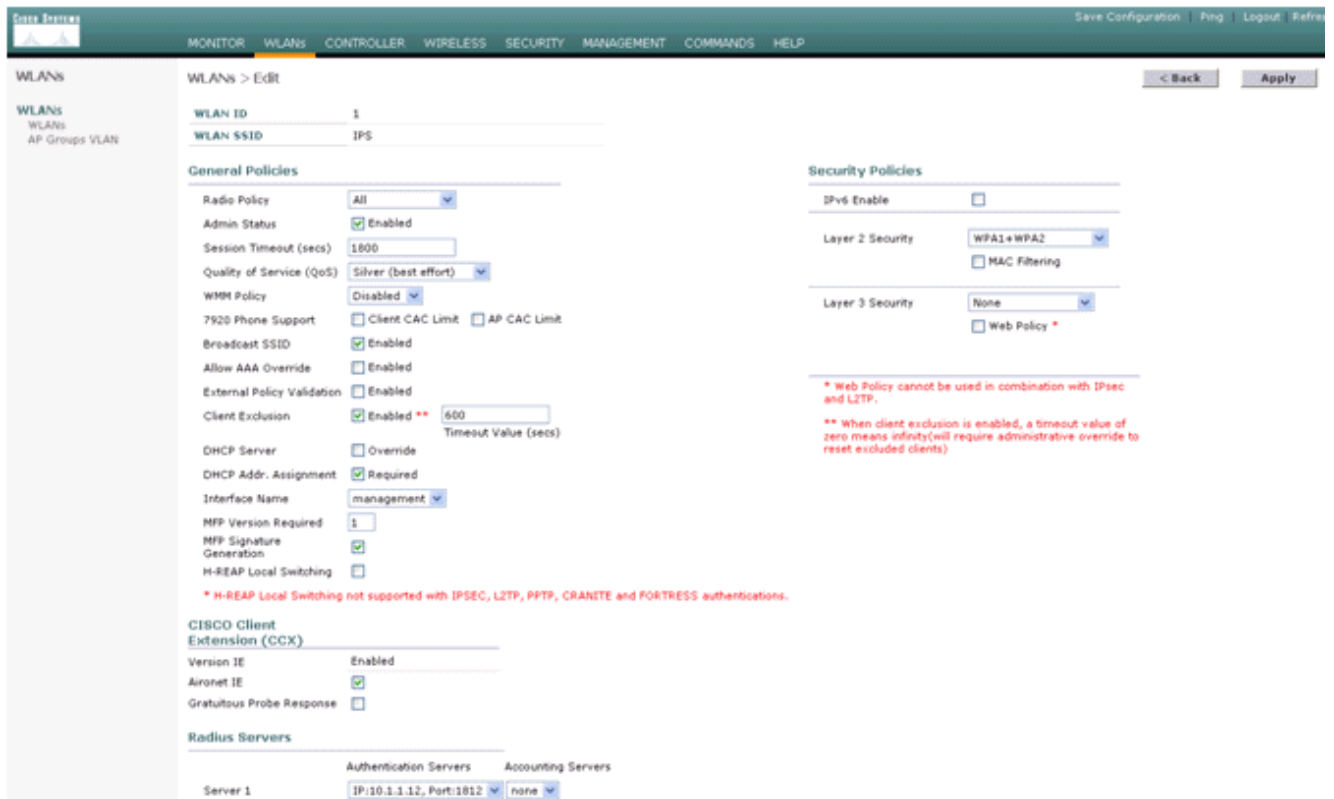
3. Vérifiez l'état de la connexion entre le capteur IPS et le WLC.

The screenshot shows the 'CIDS Sensors List' page in the Cisco IPS GUI. The left sidebar is the same as in the previous screenshot. The main content area displays a table with the following data:

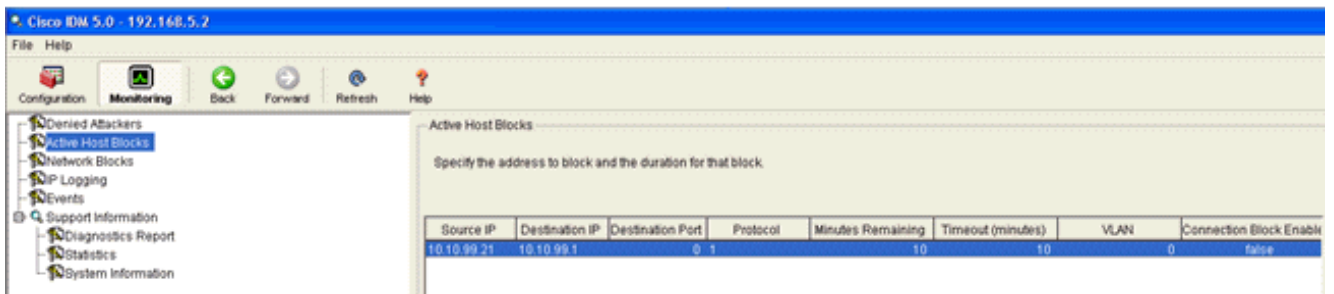
Index	Server Address	Port	State	Query Interval	Last Query (count)	
1	192.168.5.2	443	Enabled	15	Success (6083)	Detail Remove

A 'New...' button is visible at the top right of the table area.

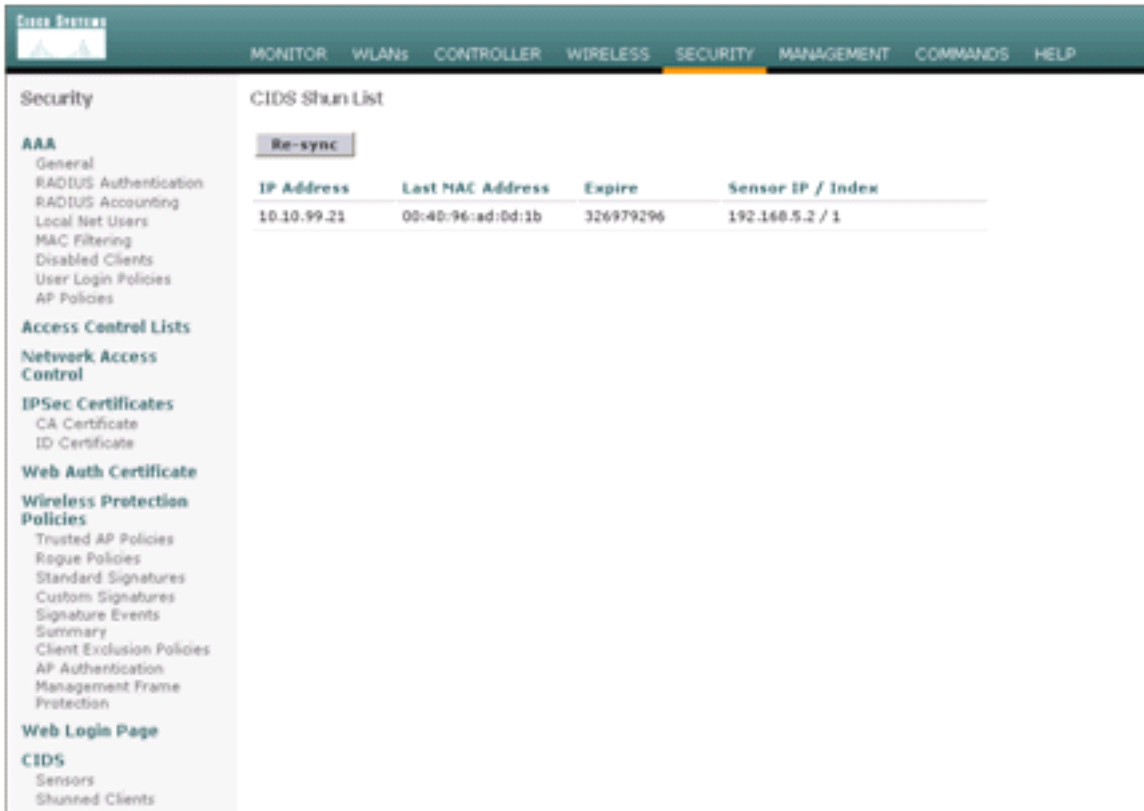
4. Une fois que vous avez établi la connectivité avec le Cisco IPS Sensor, assurez-vous que la configuration WLAN est correcte et que vous activez l'**exclusion du client**. La valeur par défaut du délai d'exclusion du client est de 60 secondes. Notez également que, indépendamment du compteur d'exclusion du client, l'exclusion du client persiste tant que le bloc client appelé par le système IDS reste actif. La durée de blocage par défaut dans le système IDS est de 30 minutes.



5. Vous pouvez déclencher un événement dans le système IPS Cisco, soit lorsque vous effectuez une analyse NMAP sur certains périphériques du réseau, soit lorsque vous envoyez une requête ping à certains hôtes surveillés par le capteur IPS Cisco. Une fois qu'une alarme est déclenchée dans le système de prévention des intrusions Cisco, accédez à **Surveillance et blocs d'hôtes actifs** afin de vérifier les détails relatifs à l'hôte.

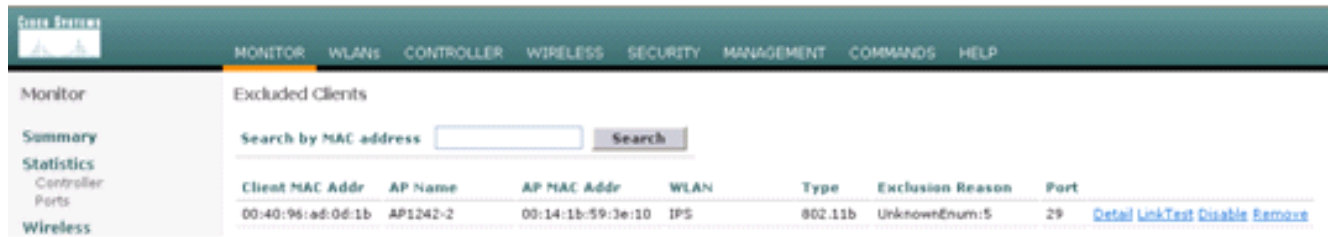


La liste des clients désactivés du contrôleur contient désormais les adresses IP et MAC de

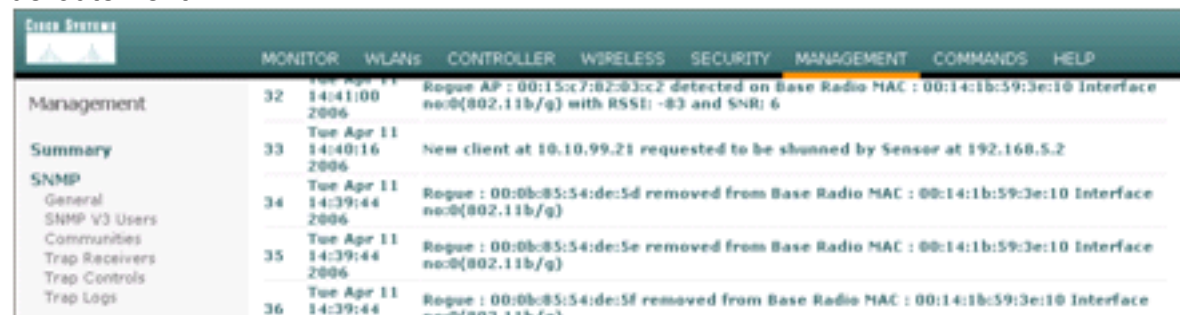


l'hôte.
 ateur est ajouté à la liste Exclusion du
 client.

L'utilis

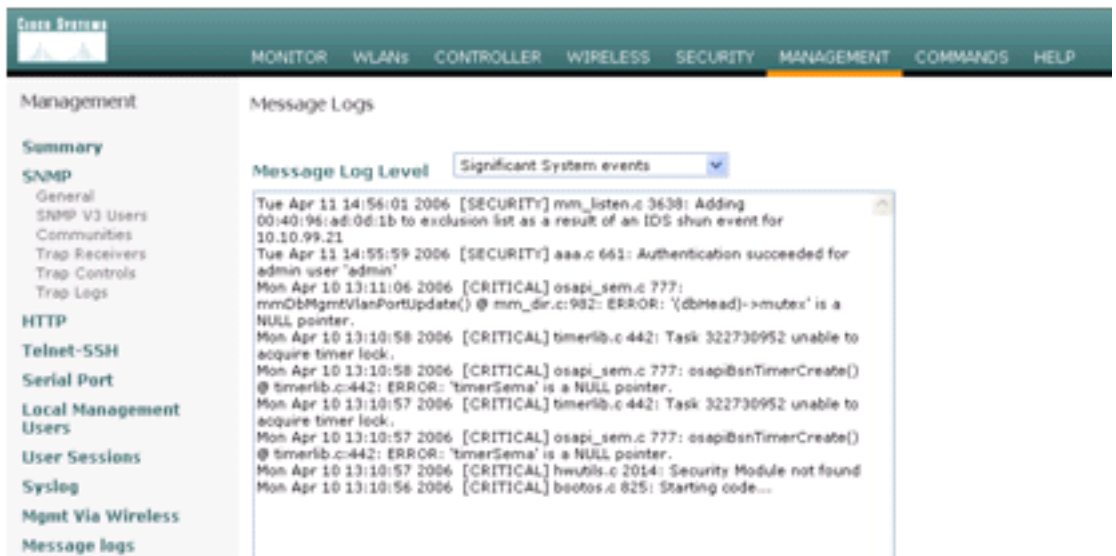


Un journal de déROUTement est généré lorsqu'un client est ajouté à la liste de déROUTement.



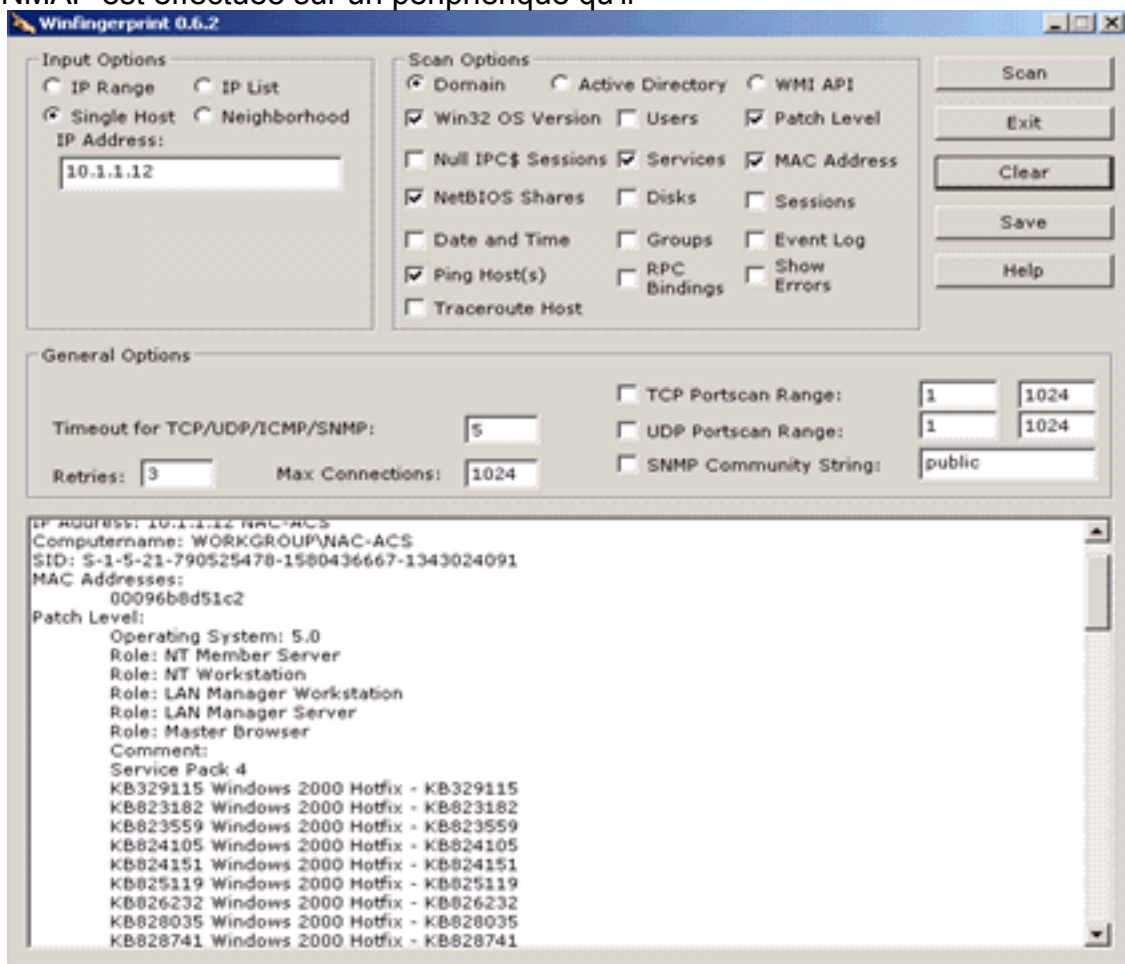
journal des messages est également généré pour

Un



l'événement.

ertains événements supplémentaires sont générés dans le Cisco IPS Sensor lorsqu'une analyse NMAP est effectuée sur un périphérique qu'il

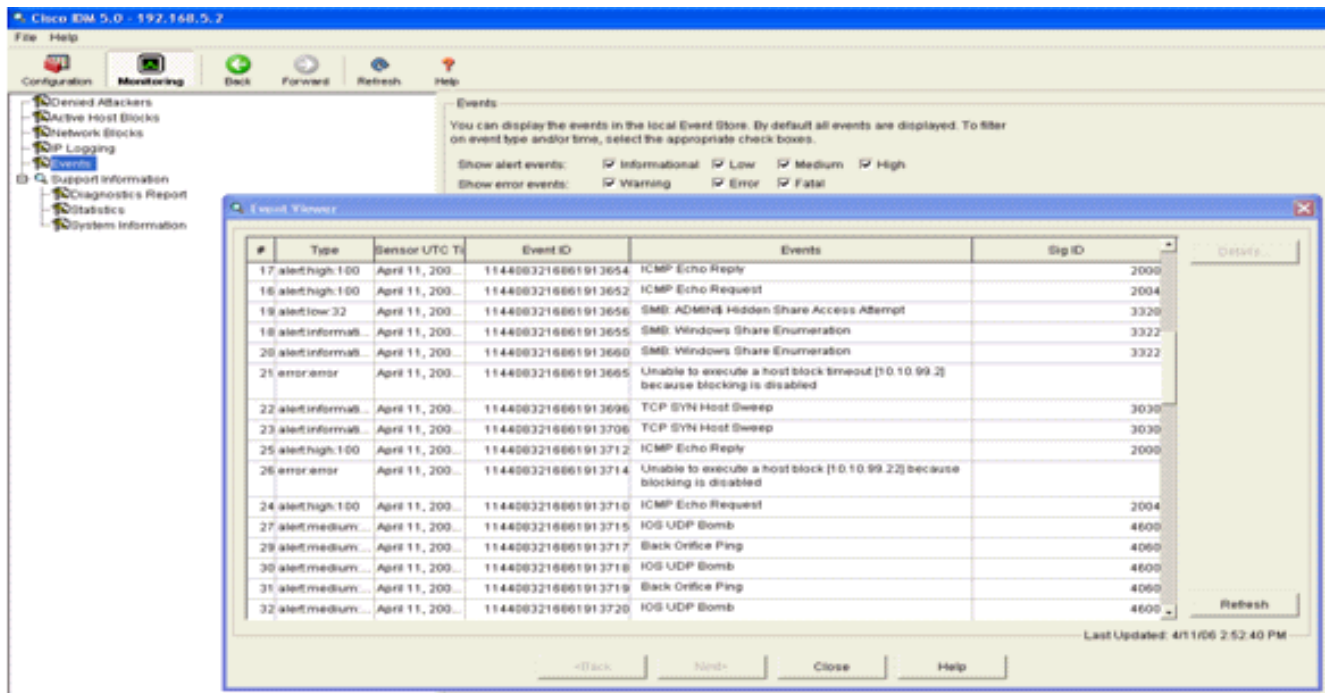


surveille.

e fenêtre affiche les événements générés dans le Cisco IPS Sensor.

C

Cett



Exemple de configuration du capteur Cisco IDS

Voici le résultat du script de configuration de l'installation :

```

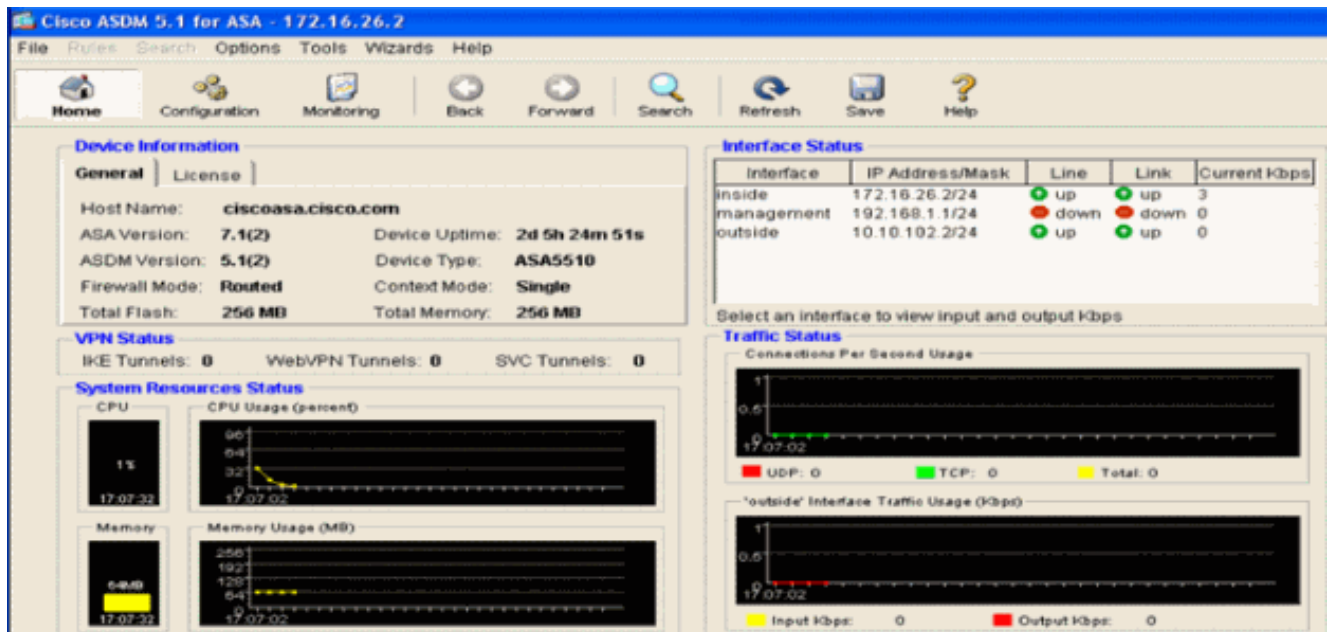
sensor#show config
! -----
! Version 5.0(2)
! Current configuration last modified Mon Apr 03 15:32:07 2006
! -----
service host
network-settings
host-ip 192.168.5.2/25,192.168.5.1
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list 40.0.0.0/8
exit
time-zone-settings
offset 0
standard-time-zone-name 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

```

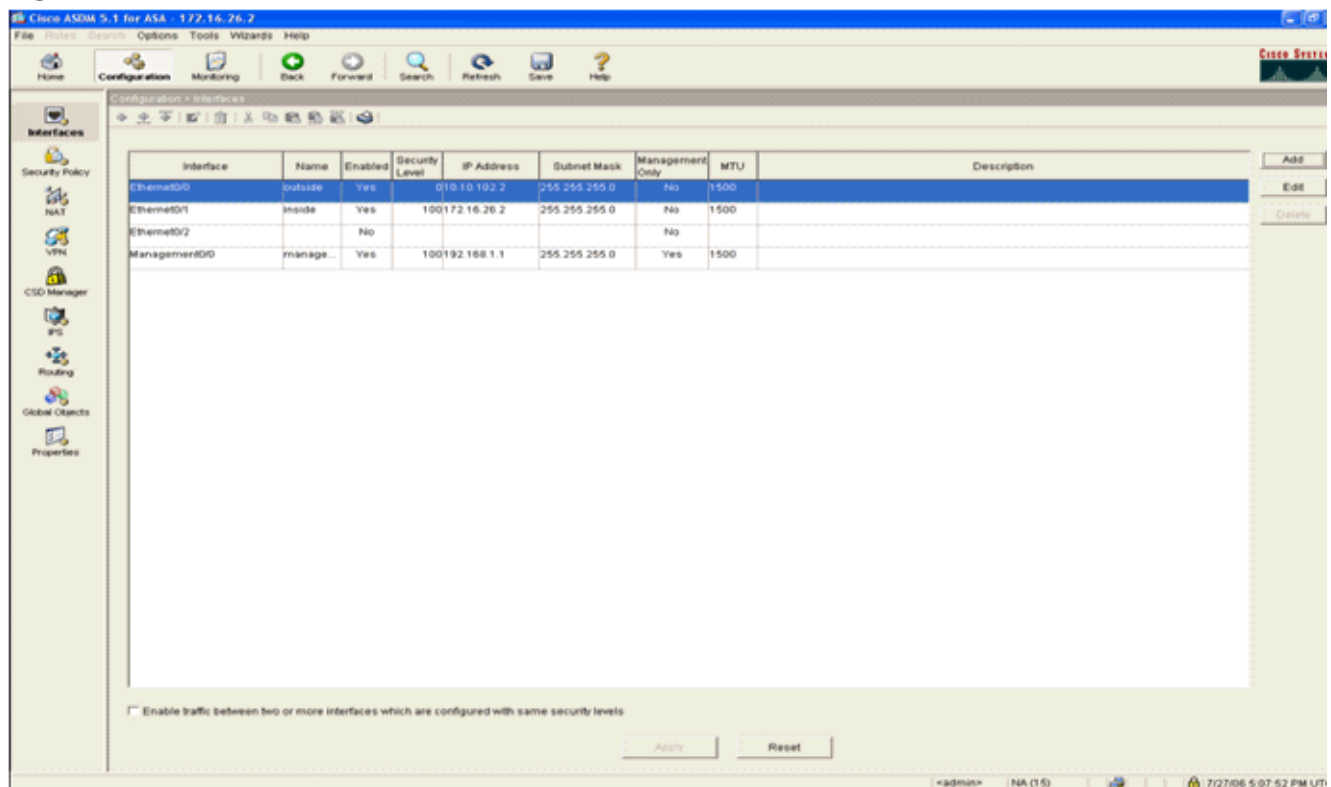
```
exit
signatures 2002 0
alert-severity high
status
enabled true
exit
exit
signatures 2003 0
alert-severity high
status
enabled true
exit
exit
signatures 2004 0
alert-severity high
engine atomic-ip
event-action produce-alert|request-block-host
exit
status
enabled true
exit
exit
exit
! -----
service 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#
```

[Configurer un ASA pour IDS](#)

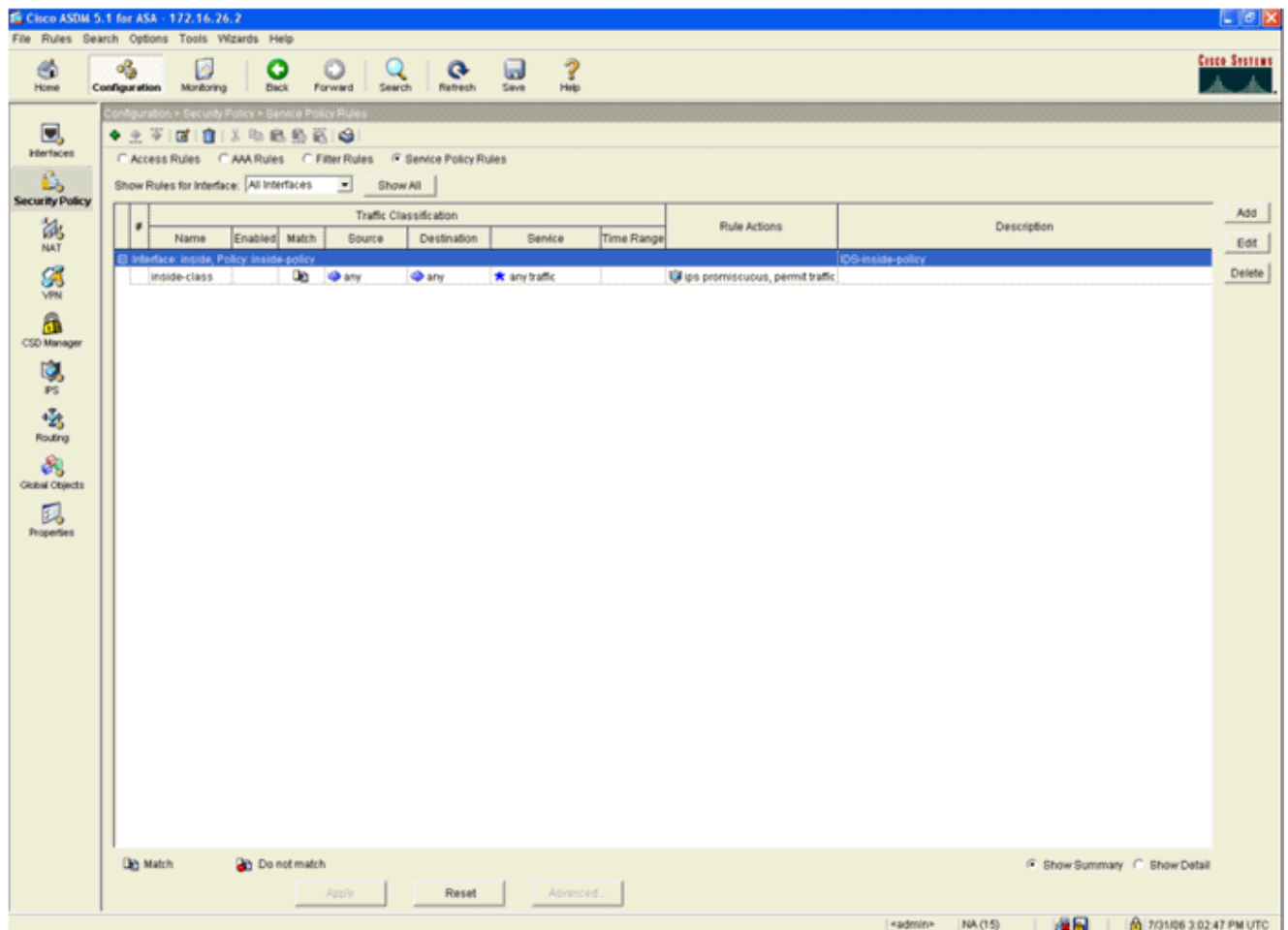
Contrairement à un capteur de détection d'intrusion traditionnel, un ASA doit toujours se trouver dans le chemin de données. En d'autres termes, au lieu d'étendre le trafic d'un port de



2. Cliquez sur **Configuration** en haut de la page. La fenêtre bascule vers une vue des interfaces ASA.



3. Cliquez sur **Stratégie de sécurité** dans la partie gauche de la fenêtre. Dans la fenêtre résultante, sélectionnez l'onglet **Règles de stratégie de service**.



4. Cliquez sur **Ajouter** afin de créer une nouvelle stratégie. L'Assistant Ajout de règle de stratégie de service s'ouvre dans une nouvelle fenêtre. Cliquez sur **Interface**, puis choisissez l'interface correcte dans la liste déroulante afin de créer une nouvelle stratégie liée à l'une des interfaces qui transmettent le trafic. Donnez à la stratégie un nom et une description de ce qu'elle fait à l'aide des deux zones de texte. Cliquez sur **Suivant** pour passer à l'étape suivante.

Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:

Step 1: Configure a service policy.

Step 2: Configure the traffic classification criteria for the service policy rule.

Step 3: Configure actions on the traffic classified by the service policy rule.

Create a service policy and apply to:

Interface:

Policy Name:

Description:

Global - applies to all interfaces

Policy Name:

Description:

< Back Next > Cancel Help

5. Créez une nouvelle classe de trafic à appliquer à la stratégie. Il est raisonnable de créer des classes spécifiques afin d'inspecter des types de données spécifiques, mais dans cet exemple, Any Traffic est sélectionné pour la simplicité. Cliquez sur **Suivant** pour continuer.

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class:

Description (optional):

Traffic match criteria

Default Inspection Traffic

Source and Destination IP Address (uses ACL)

Tunnel Group

TCP or UDP Destination Port

RTP Range

IP DiffServ CodePoints (DSCP)

IP Precedence

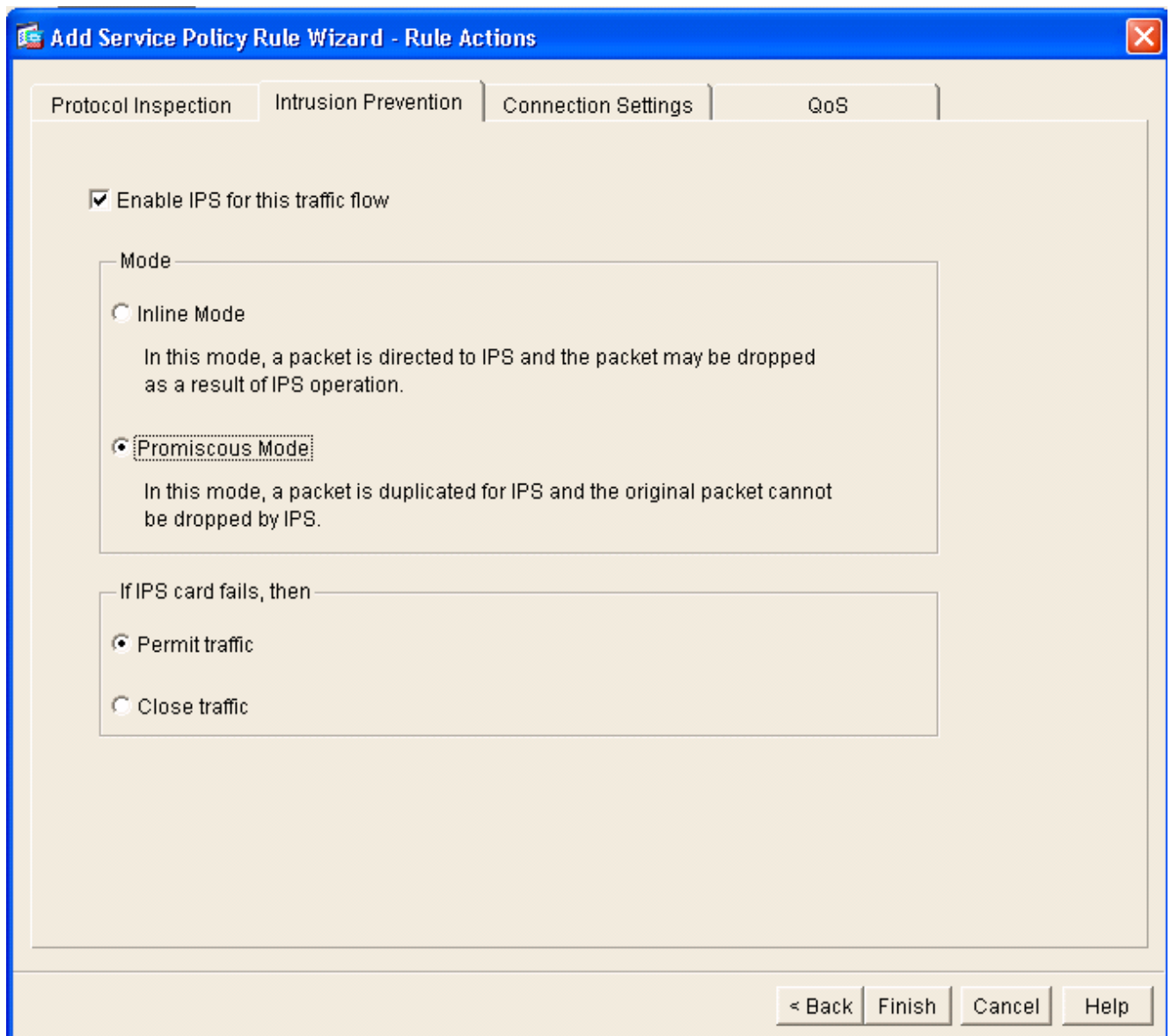
Any traffic

If traffic does not match a existing traffic class, then it will match the class-default traffic class.
Class-default can be used in catch all situation.

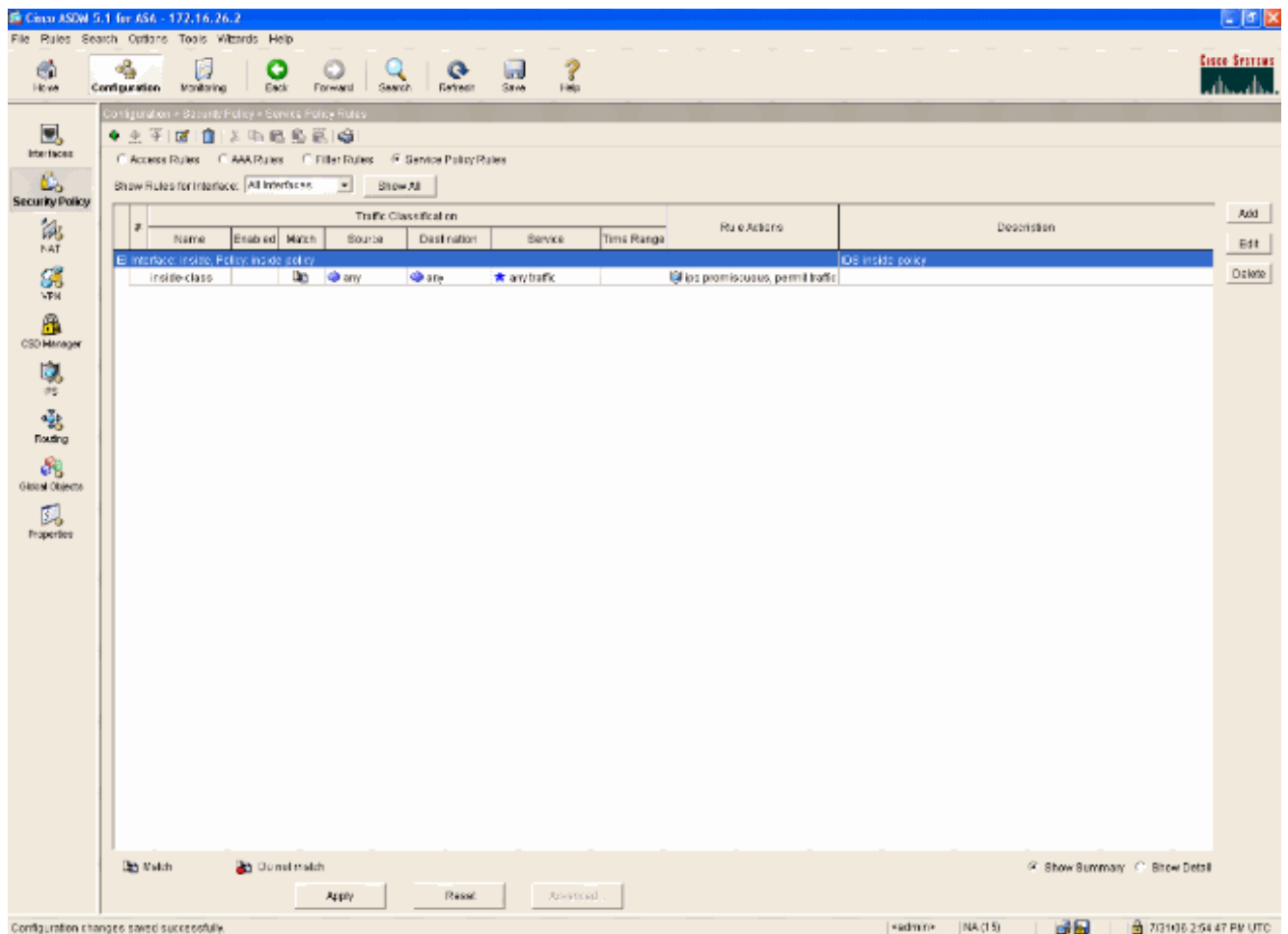
Use class-default as the traffic class.

< Back Next > Cancel Help

6. Complétez ces étapes afin de demander à l'ASA de diriger le trafic vers son AIP-SSM. Cochez **Enable IPS pour ce flux de trafic** afin d'activer la détection des intrusions. Définissez le mode sur **Promiscuité** afin qu'une copie du trafic soit envoyée au module hors bande au lieu de placer le module en ligne avec le flux de données. Cliquez sur **Autoriser le trafic** afin de vous assurer que l'ASA passe à l'état d'ouverture en cas de défaillance de l'AIP-SSM. Cliquez sur **Terminer** afin de valider la modification.



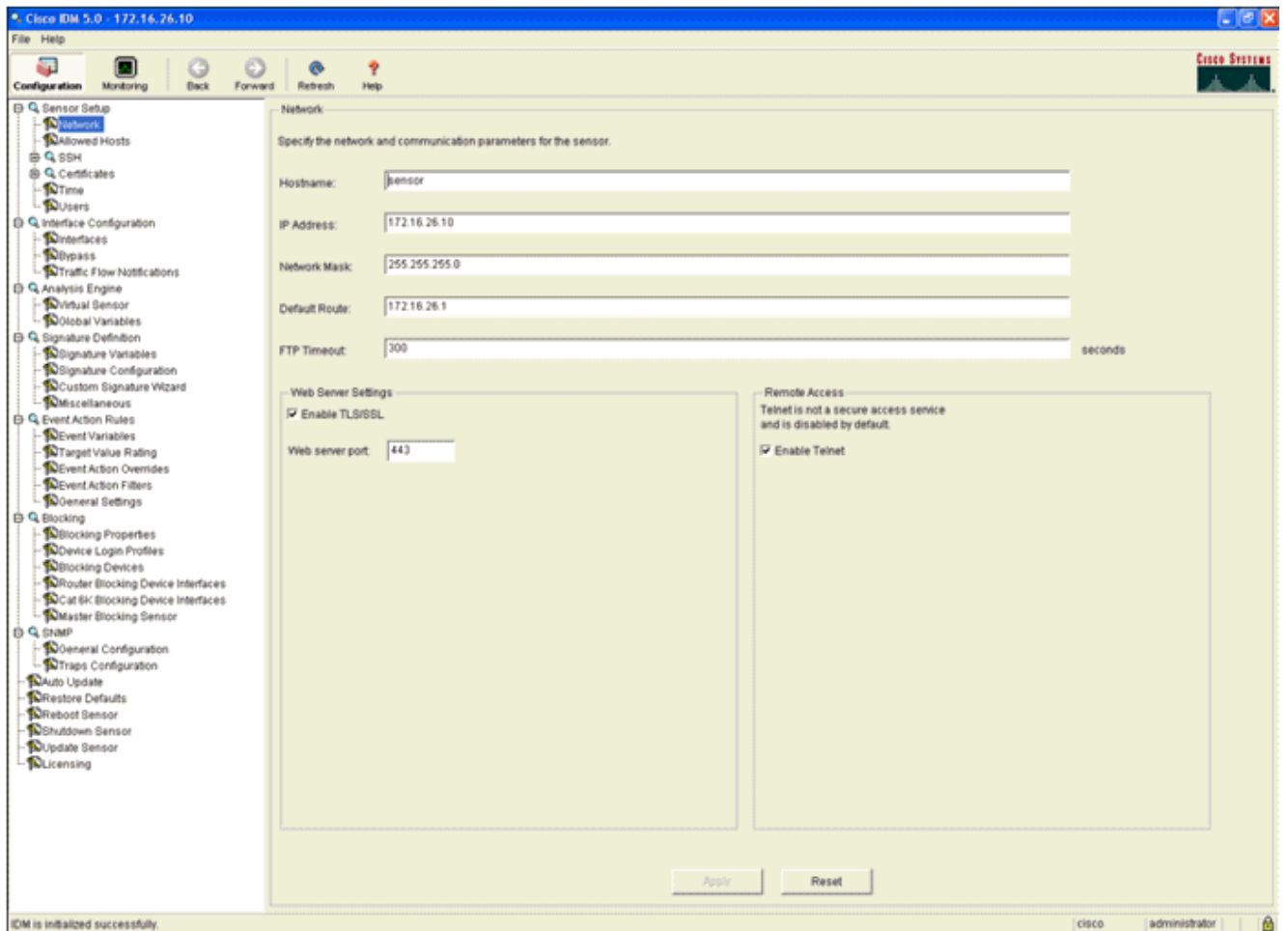
7. L'ASA est maintenant configuré pour envoyer le trafic au module IPS. Cliquez sur **Enregistrer** sur la ligne supérieure afin d'écrire les modifications dans l'ASA.



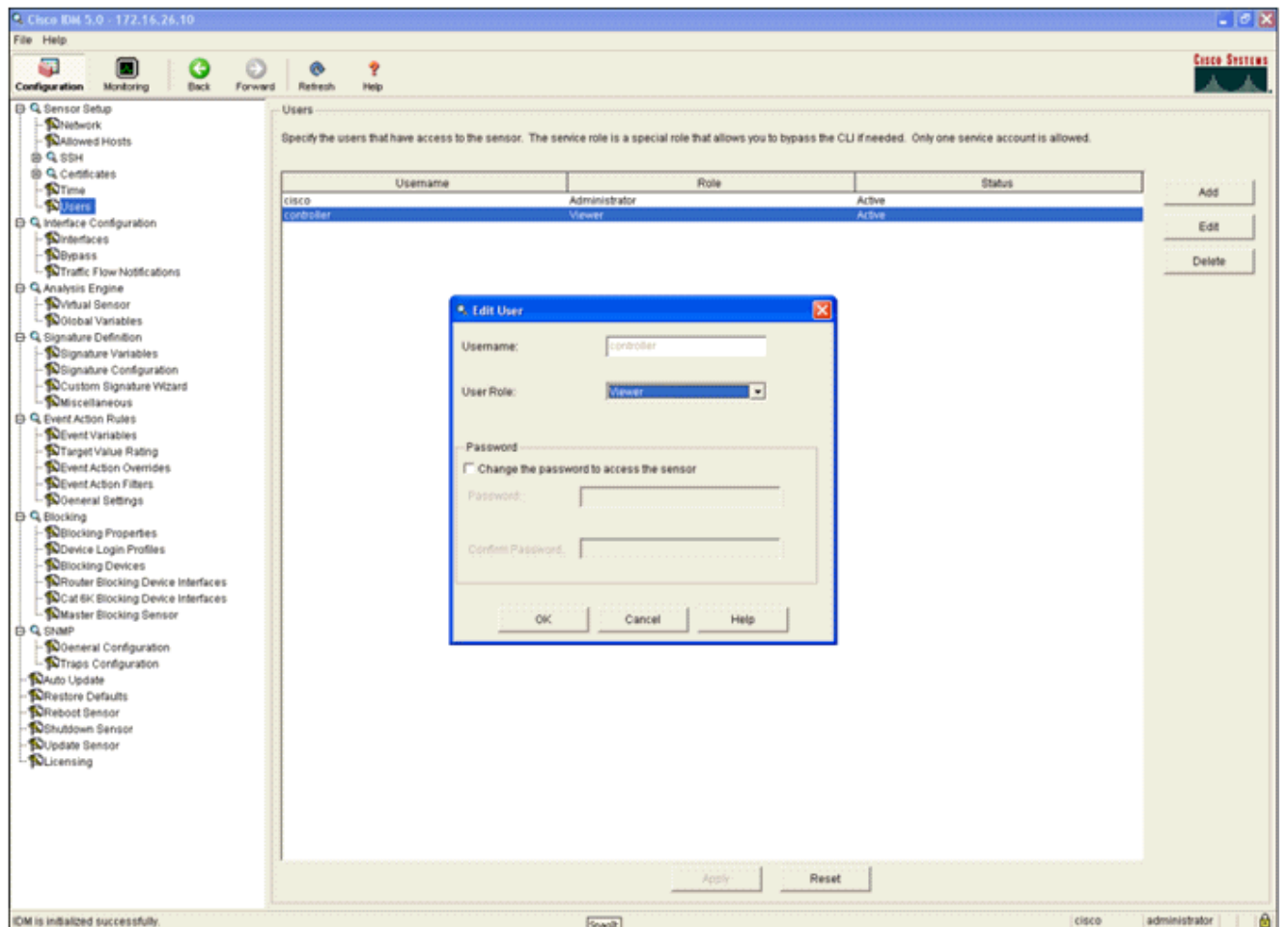
Configurer AIP-SSM pour l'inspection du trafic

Pendant que l'ASA envoie des données au module IPS, associez l'interface AIP-SSM à son moteur de capteur virtuel.

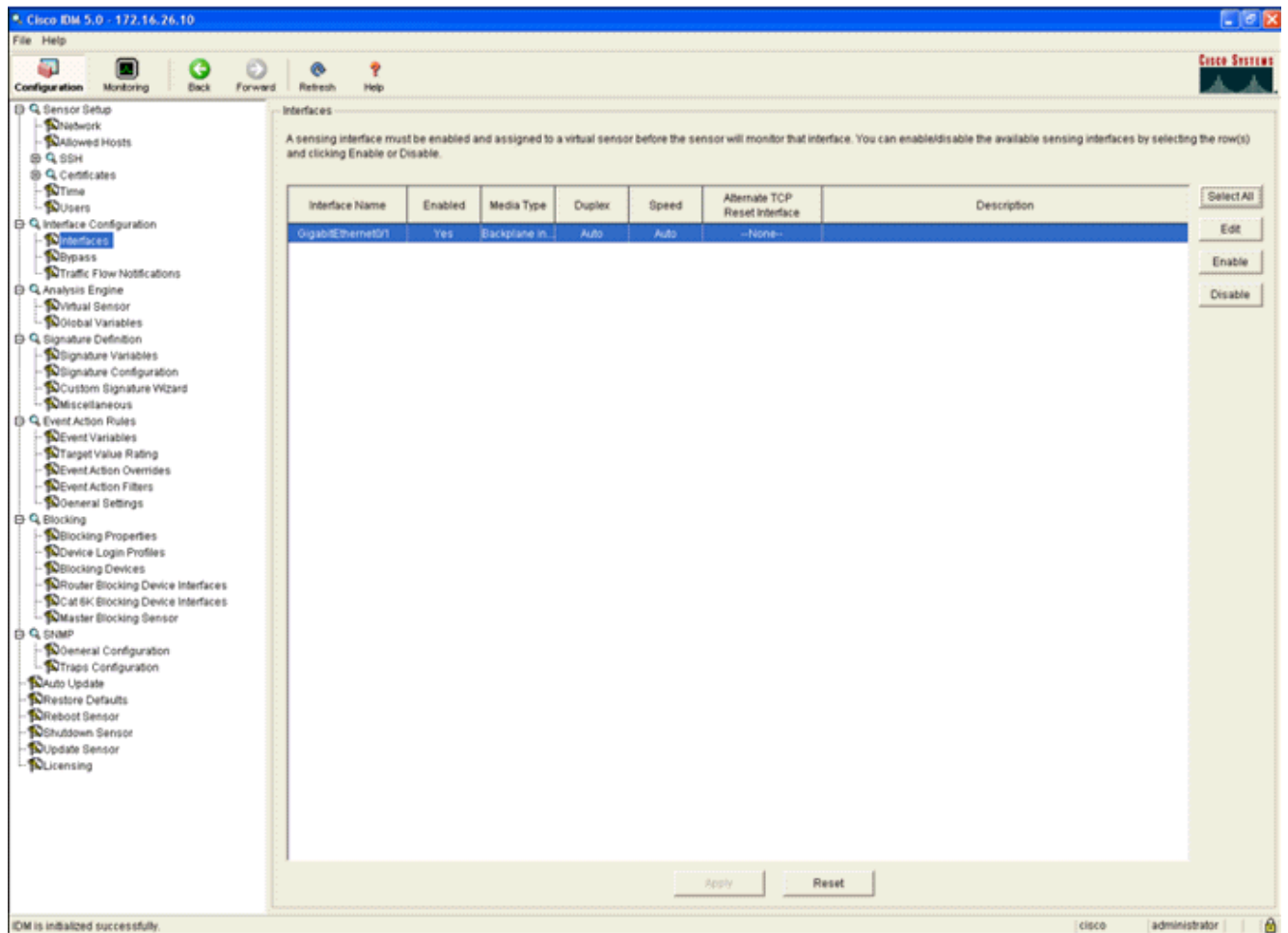
1. Connectez-vous à AIP-SSM à l'aide d'IDM.



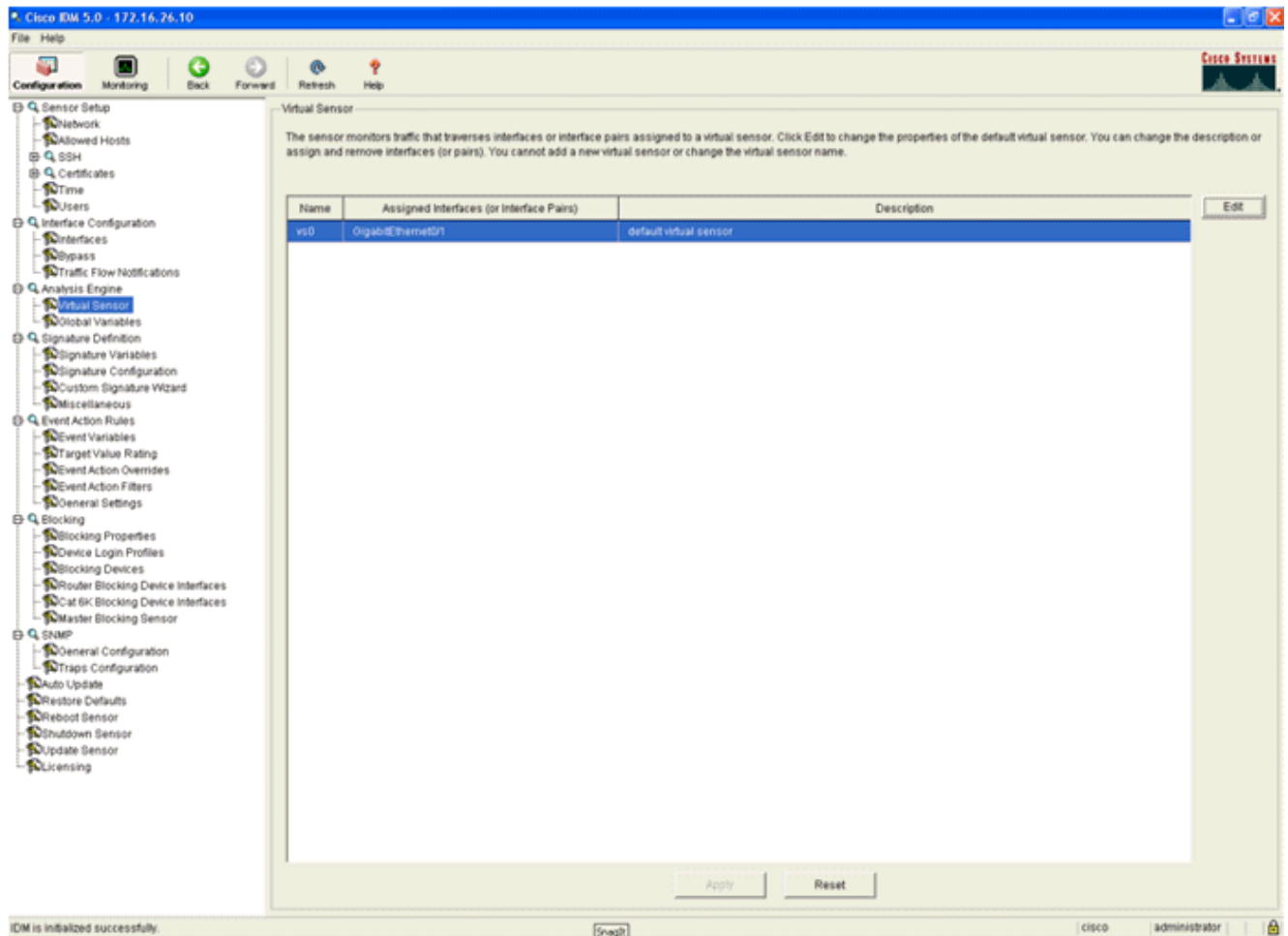
2. Ajoutez un utilisateur avec au moins des privilèges de visionneuse.



3. Activez l'interface.



4. Vérifiez la configuration du capteur virtuel.



[Configurer un WLC pour interroger l'AIP-SSM pour les blocs de clients](#)

Effectuez ces étapes une fois que le capteur est configuré et prêt à être ajouté au contrôleur :

1. Choisissez **Security > CIDS > Sensors > New** in the WLC.
2. Ajoutez l'adresse IP, le numéro de port TCP, le nom d'utilisateur et le mot de passe que vous avez créés dans la section précédente.
3. Afin d'obtenir l'empreinte du capteur, exécutez cette commande dans le capteur et ajoutez l'empreinte SHA1 sur le WLC (sans le deux-points). Cette option permet de sécuriser la communication d'interrogation contrôleur/IDS.

```
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
```

The screenshot shows the Cisco Systems Security configuration interface. The left sidebar contains a navigation menu with categories like AAA, Access Control Lists, IPsec Certificates, Web Auth Certificate, Wireless Protection Policies, Web Login Page, and CIDS. The main content area is titled 'CIDS Sensor Edit' and displays the following configuration details:

- Index:** 2
- Server Address:** 172.16.26.10
- Port:** 443
- Username:** controller
- Password:** *****
- State:**
- Query Interval:** 10 seconds
- Fingerprint (SHA1 hash):** 90C9969B4EFA74F8528092BBBC483C45B4876C55 (40 hex chars) (hash key is already set)
- Last Query (count):** Success (1400)

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

The screenshot shows the Cisco Systems Security configuration interface for the 'CIDS Sensors List'. The left sidebar is identical to the previous screenshot. The main content area displays a table with the following data:

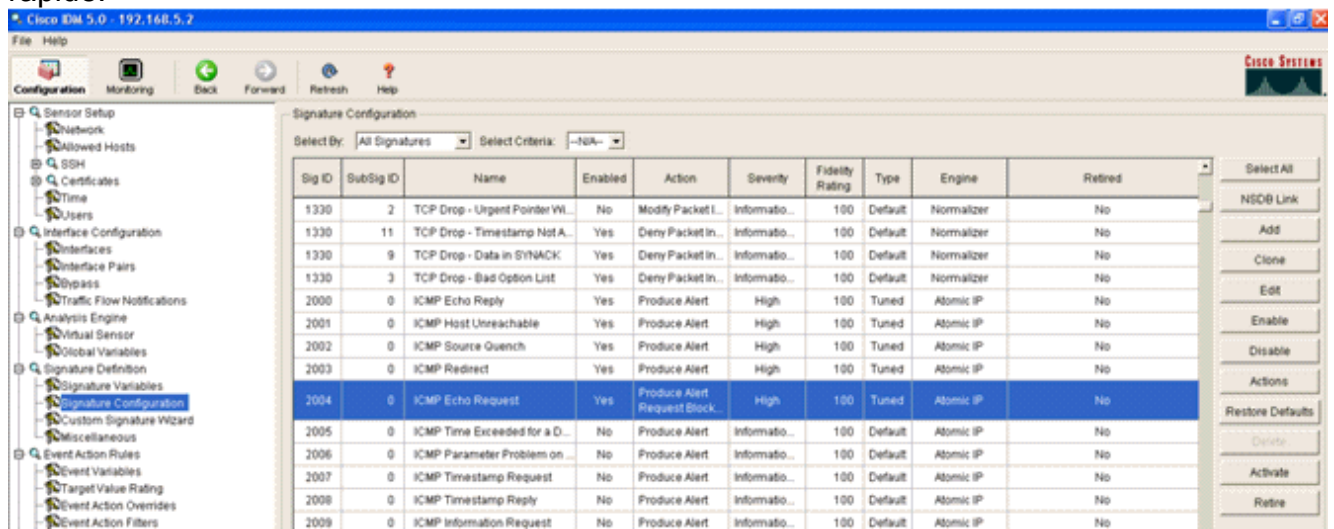
Index	Server Address	Port	State	Query Interval	Last Query (count)	
1	192.168.5.2	443	Enabled	15	Unauthorized (1)	Detail Remove
2	172.16.26.10	443	Enabled	10	Success (1444)	Detail Remove

[Ajouter une signature de blocage à AIP-SSM](#)

Ajoutez une signature d'inspection pour bloquer le trafic. Bien qu'il existe de nombreuses signatures pouvant effectuer le travail en fonction des outils disponibles, cet exemple crée une signature qui bloque les paquets ping.

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

rapide.



2. Activez la signature, définissez la gravité de l'alerte sur **Élevé** et définissez l'action d'événement sur **Produire l'alerte** et l'**hôte de bloc de requête** afin de terminer cette étape de vérification. Notez que l'action Hôte de bloc de requête est la clé pour signaler au WLC de créer des exceptions 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

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

Name	Value
Signature ID:	2004
SubSignature ID:	0
Alert Severity:	Informational
Sig Fidelity Rating:	100
Promiscuous Delta:	0
Sig Description:	
Signature Name:	ICMP Echo Request
Alert Notes:	
User Comments:	
Alert Traits:	0
Release:	81
Engine: Atomic IP	
Event Action:	Request Block Host
Fragment Status:	

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.

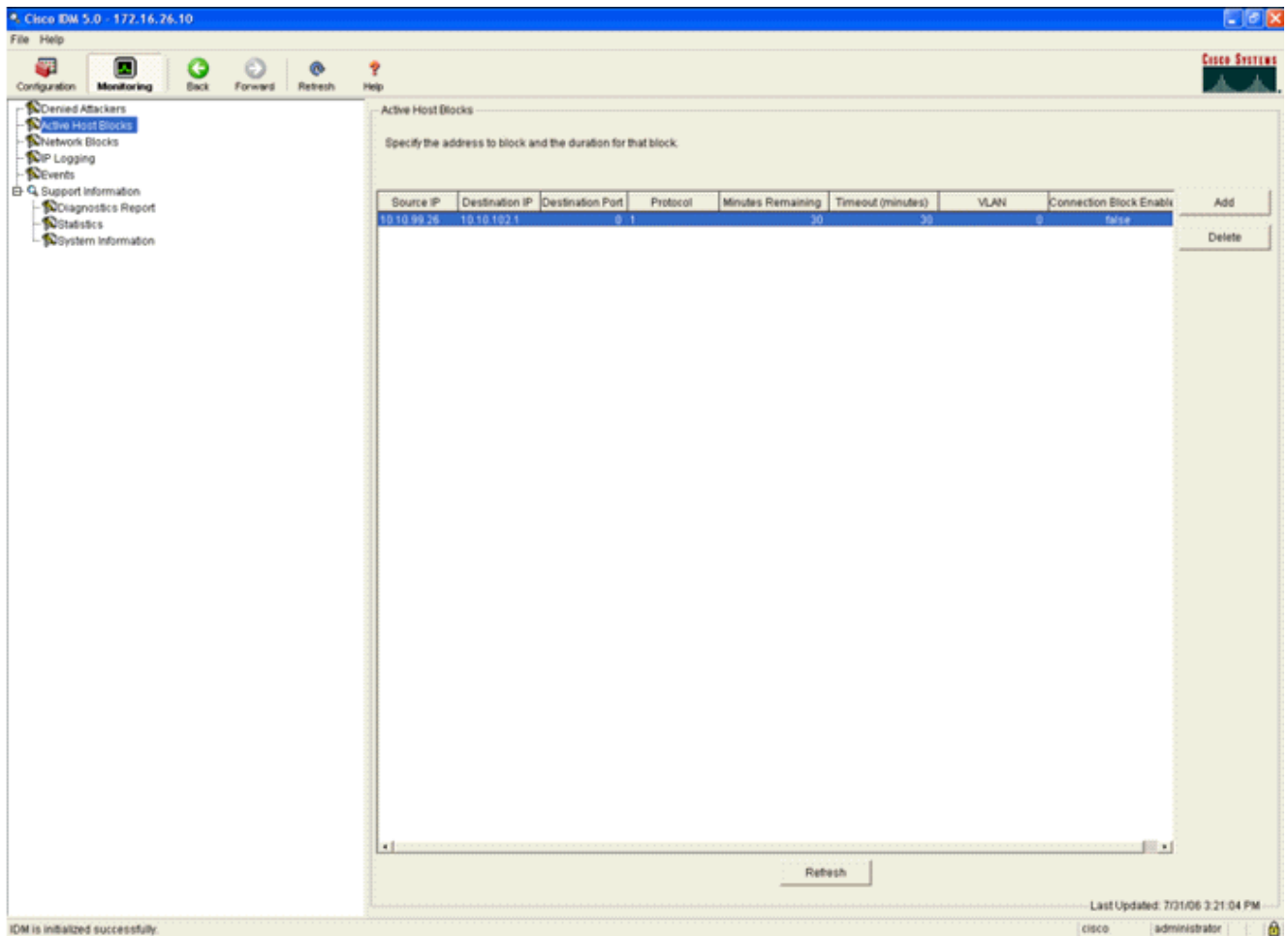
OK Cancel Help

3. Cliquez sur **OK** pour enregistrer la signature.
4. Vérifiez que la signature est active et qu'elle est configurée pour effectuer une action de blocage.
5. Cliquez sur **Apply** afin de valider la signature sur le module.

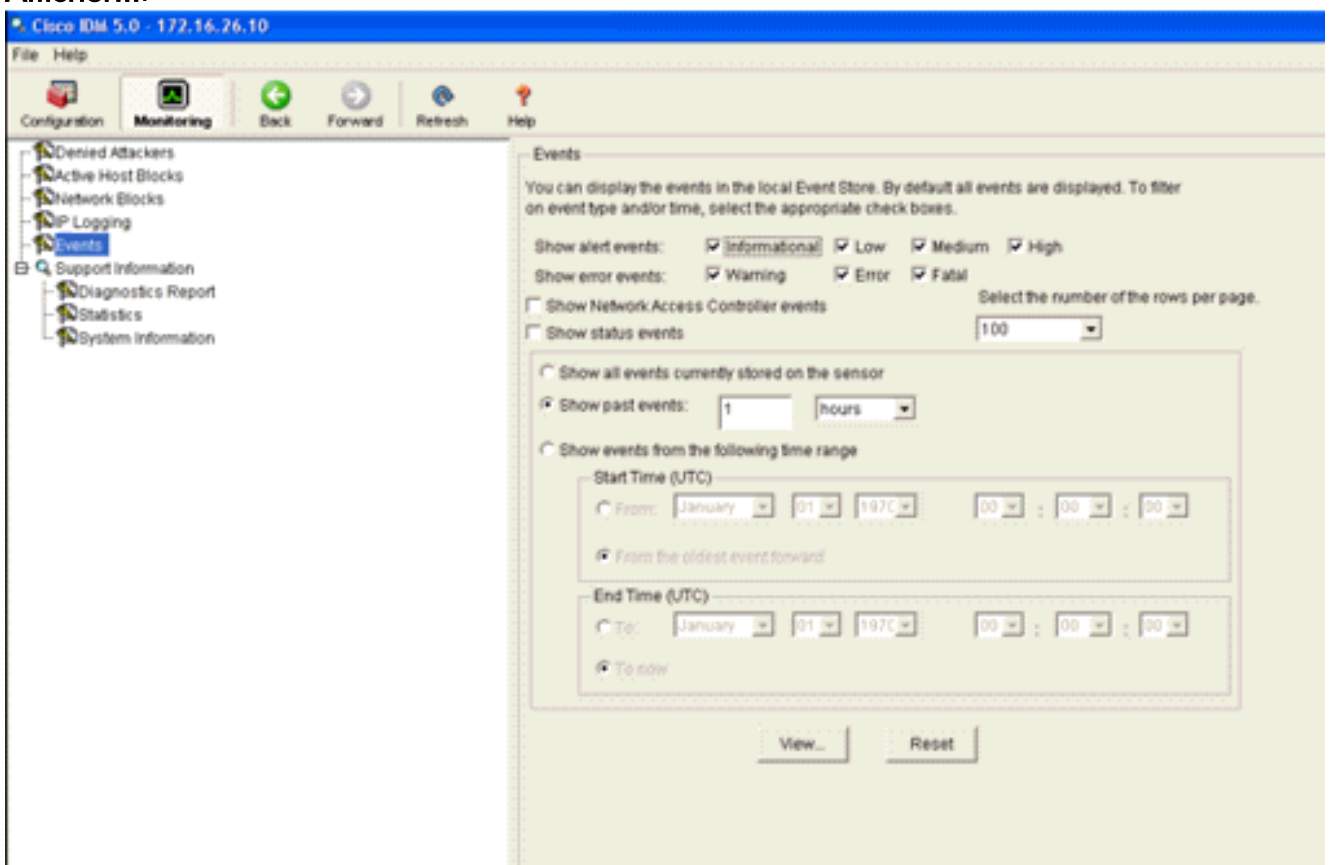
Blocage et événements de surveillance avec IDM

Procédez comme suit :

1. Lorsque la signature est correctement déclenchée, il y a deux endroits dans IDM pour le noter. La première méthode montre les blocs actifs installés par AIP-SSM. Cliquez sur **Surveillance** le long de la ligne supérieure des actions. Dans la liste des éléments qui s'affiche à gauche, sélectionnez **Blocs d'hôtes actifs**. À chaque fois que la signature ping se déclenche, la fenêtre Blocs d'hôte actif affiche l'adresse IP du contrevenant, l'adresse du périphérique attaqué et l'heure pour laquelle le blocage est en vigueur. La durée de blocage par défaut est de 30 minutes et est réglable. Cependant, la modification de cette valeur n'est pas abordée dans ce document. Consultez la documentation de configuration ASA si nécessaire pour plus d'informations sur la façon de modifier ce paramètre. Supprimez le bloc immédiatement, sélectionnez-le dans la liste, puis cliquez sur **Supprimer**.



La deuxième méthode d'affichage des signatures déclenchées utilise le tampon d'événements AIP-SSM. Dans la page Surveillance IDM, sélectionnez **Événements** dans la liste des éléments située sur le côté gauche. L'utilitaire de recherche Événements s'affiche. Définissez les critères de recherche appropriés et cliquez sur **Afficher....**



- L'Observateur d'événements apparaît ensuite avec une liste d'événements correspondant aux critères donnés. Faites défiler la liste et recherchez la signature ICMP Echo Request modifiée lors des étapes de configuration précédentes. Recherchez dans la colonne Événements le nom de la signature ou recherchez le numéro d'identification de la signature dans la colonne ID de signature.

#	Type	Sensor UTC Time	EventID	Events	Sig ID	Details...
1	error:error	July 31, 2006 2:59:52 PM U...	1145383740954940828	Unable to execute a host block [10.10.99.26] because blocking is not configured		
2	error:warning	July 31, 2006 3:16:51 PM U...	1145383740954941447	while sending a TLS warning alert close_notify, the following error occurred: socket error [3,32]		
3	alert:informati...	July 31, 2006 3:19:16 PM U...	1145383740954941574	ICMP Echo Request	2004	
4	error:error	July 31, 2006 3:19:16 PM U...	1145383740954941577	Unable to execute a host block [10.10.99.26] because blocking is not configured		
5	alert:informati...	July 31, 2006 3:19:46 PM U...	1145383740954941597	ICMP Echo Request	2004	

Last Updated: 7/31/06 3:22:39 PM

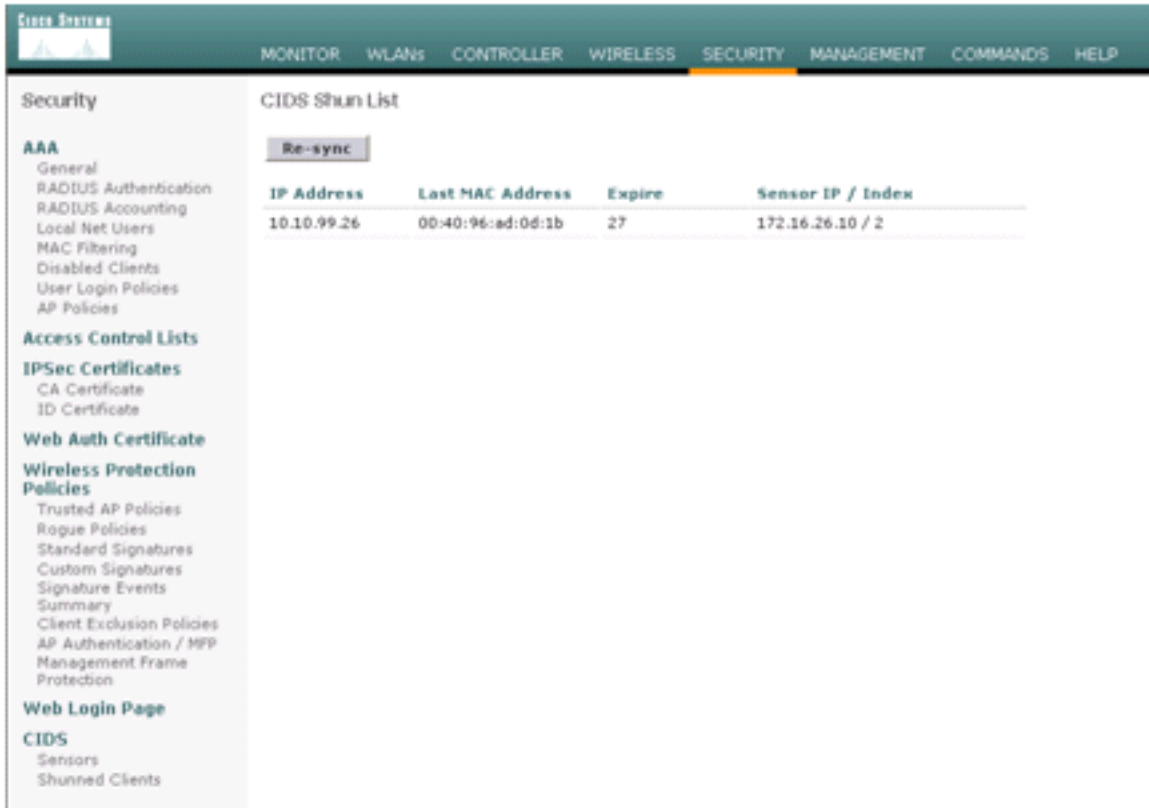
- Après avoir localisé la signature, double-cliquez sur l'entrée afin d'ouvrir une nouvelle fenêtre. La nouvelle fenêtre contient des informations détaillées sur l'événement qui a déclenché la signature.

```

evIdsAlert: eventId=1145383740954941597 vendor=Cisco severity=informational
originator:
  hostId: sensor
  appName: sensorApp
  appInstanceId: 341
time: July 31, 2006 3:19:46 PM UTC offset=0 timeZone=UTC
signature: description=ICMP Echo Request id=2004 version=S1
  subsigId: 0
interfaceGroup:
vlan: 0
participants:
  attacker:
    addr: 10.10.99.26 locality=OUT
  target:
    addr: 10.10.102.1 locality=OUT
summary: 4 final=true initialAlert=1145383740954941574 summaryType=Regular
alertDetails: Regular Summary: 4 events this interval ;
riskRatingValue: 25
interface: ge0_1
protocol: icmp
  
```

Contrôle de l'exclusion du client dans un contrôleur sans fil

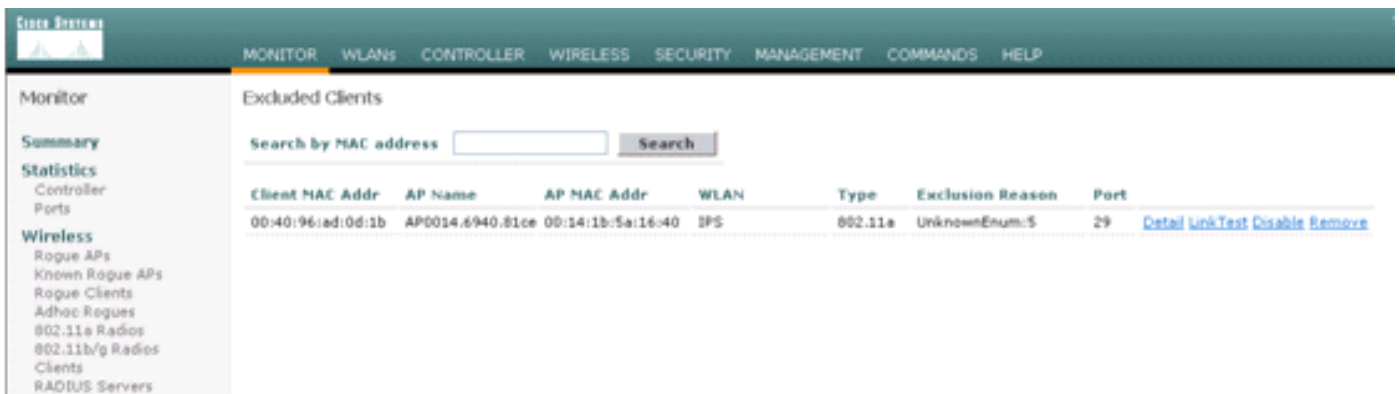
La liste des clients désactivés du contrôleur est renseignée à ce stade avec l'adresse IP et MAC de l'hôte.



The screenshot shows the Cisco WCS interface with the 'SECURITY' tab selected. The left sidebar contains a navigation menu with categories like AAA, Access Control Lists, IPsec Certificates, Web Auth Certificate, Wireless Protection Policies, and Web Login Page. The main content area is titled 'CIDS Shun List' and features a 'Re-sync' button. Below the button is a table with the following data:

IP Address	Last MAC Address	Expire	Sensor IP / Index
10.10.99.26	00:40:96:ad:0d:1b	27	172.16.26.10 / 2

L'utilisateur est ajouté à la liste Exclusion du client.



The screenshot shows the Cisco WCS interface with the 'MONITOR' tab selected. The left sidebar contains a navigation menu with categories like Summary, Statistics, and Wireless. The main content area is titled 'Excluded Clients' and features a search bar labeled 'Search by MAC address' with a 'Search' button. Below the search bar is a table with the following data:

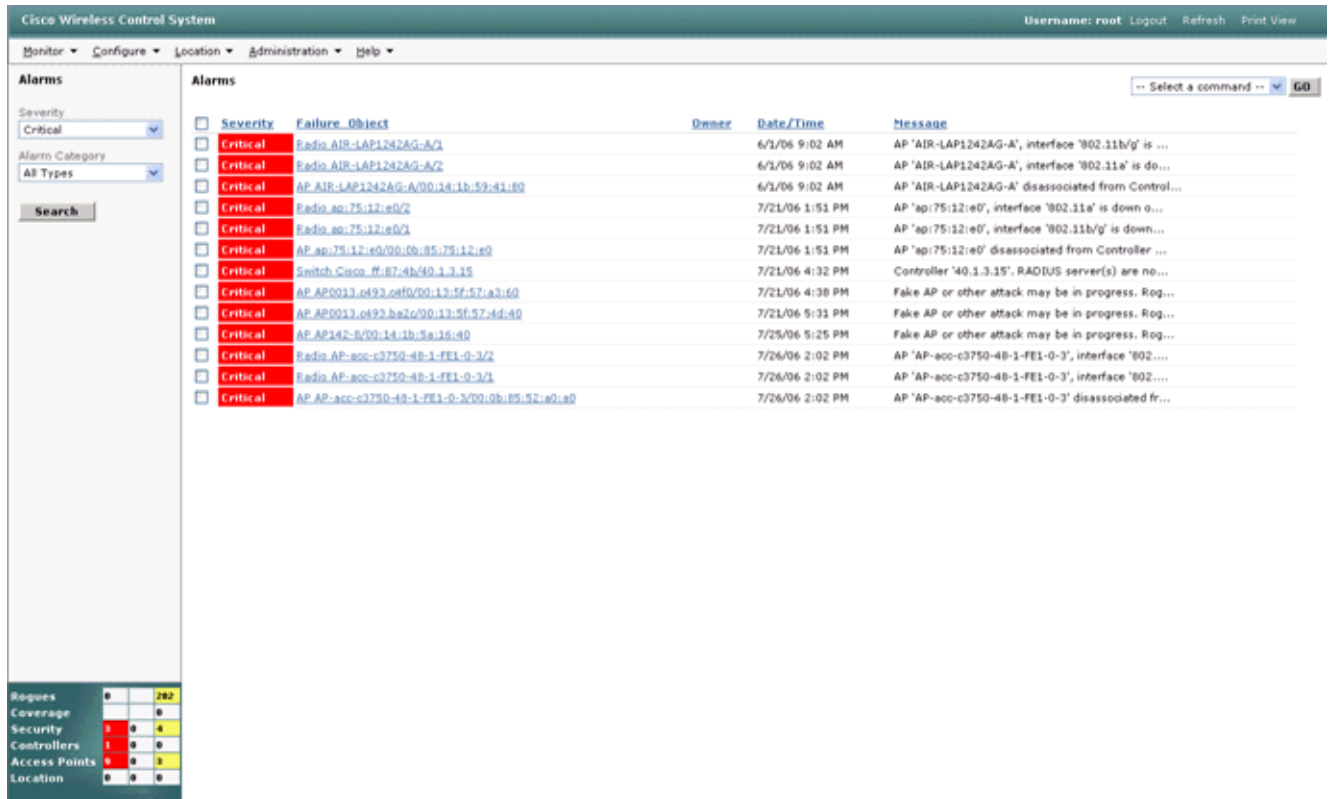
Client MAC Addr	AP Name	AP MAC Addr	WLAN	Type	Exclusion Reason	Port	
00:40:96:ad:0d:1b	AP0014.6940.81ce	00:14:1b:5a:16:40	IPS	802.11a	UnknownEnum:5	29	Detail Link Text Disable Remove

Surveiller les événements dans WCS

Les événements de sécurité qui déclenchent un blocage dans AIP-SSM font que le contrôleur ajoute l'adresse du délinquant à la liste d'exclusion du client. Un événement est également généré dans WCS.

1. Utilisez l'utilitaire **Monitor > Alarms** du menu principal de WCS afin d'afficher l'événement d'exclusion. WCS affiche initialement toutes les alarmes non effacées et présente également une fonction de recherche sur le côté gauche de la fenêtre.

- Modifiez les critères de recherche pour trouver le bloc client. Sous Gravit , s lectionnez **Mineur**, puis d finissez la cat gorie d'alarme sur **S curit **.
- Cliquez sur **Rechercher**.



- La fen tre Alarm r pertorie ensuite uniquement les alarmes de s curit  avec une gravit  mineure. Pointez la souris sur l' v nement qui a d clench  le blocage dans AIP-SSM. En particulier, WCS affiche l'adresse MAC de la station client qui a d clench  l'alarme. En pointant l'adresse appropri e, WCS affiche une petite fen tre avec les d tails de l' v nement. Cliquez sur le lien pour afficher ces m mes d tails dans une autre fen tre.



Exemple de configuration 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#

```

Exemple de configuration du capteur du système de prévention des 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#
```

Vérification

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

Dépannage

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

Informations connexes

- [Installation et utilisation de Cisco Intrusion Prevention System Device Manager 5.1](#)
- [Appareils de sécurité adaptatifs de la gamme Cisco ASA 5500 - Guides de configuration](#)
- [Configuration du capteur Cisco Intrusion Prevention System à l'aide de l'interface de ligne de commande 5.0 - Configuration des interfaces](#)
- [Guide de configuration WLC 4.0](#)
- [Assistance 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](#)
- [Configuration des solutions de sécurité](#)
- [Support et documentation techniques - Cisco Systems](#)