Configuration de la réinitialisation TCP IDS avec VMS IDS MC

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Configurez
Diagramme du réseau
Configurations
Configuration initiale de capteur
Importez le capteur dans des ID MC
Importez le capteur dans le contrôleur de sécurité
ID MC d'utilisation pour des mises à jour de signature
Configurez la Réinitialisation TCP pour le routeur IOS
Vérifiez
Lancez l'attaque et la Réinitialisation TCP
Dépannez
Procédure de dépannage
Informations connexes

Introduction

Le document fournit une configuration d'échantillon du Cisco Intrusion Detection System (ID) par l'intermédiaire de la solution de Gestion VPN/Security (VMS), console de gestion d'ID (ID MC). Dans ce cas, la Réinitialisation TCP du capteur d'ID à un routeur de Cisco est configurée.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Le capteur est installé et configuré pour sentir le trafic nécessaire.
- L'interface de reniflement est répartie au routeur en dehors de l'interface.

Composants utilisés

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

- VMS 2.2 avec les ID MC et le contrôleur de sécurité 1.2.3
- Capteur d'ID de Cisco 4.1.3S(63)
- Routeur de Cisco qui exécute la version de logiciel 12.3.5 de Cisco IOS®

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

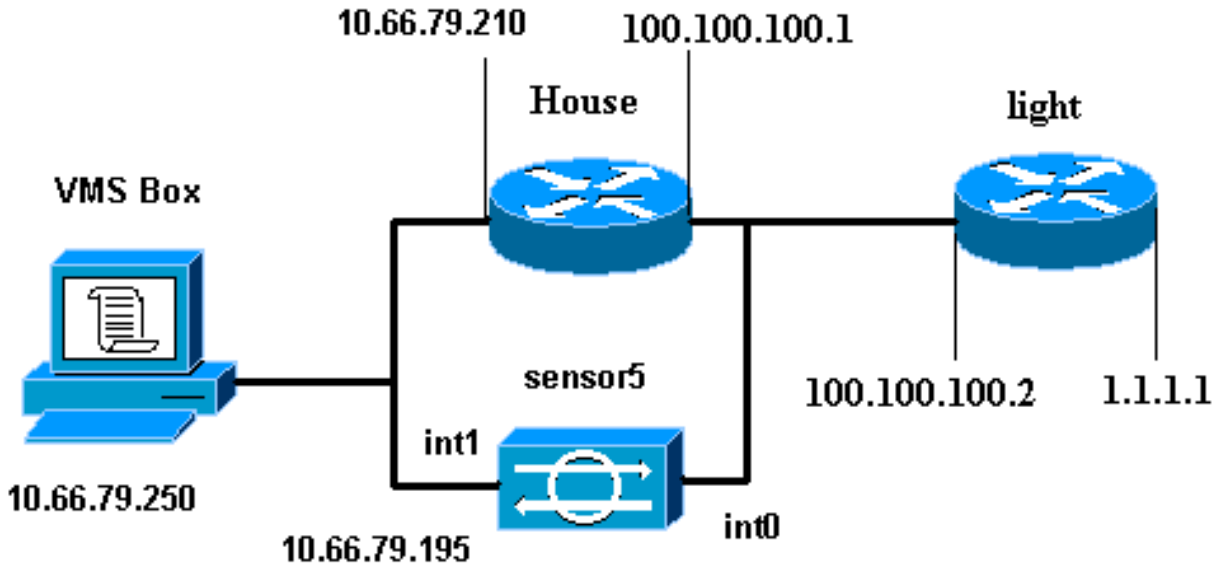
Configurez

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

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

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise les configurations suivantes.

- Lumière du routeur
- Routeur House

Lumière du routeur

```
Current configuration : 906 bytes
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname light ! enable password cisco ! username cisco
password 0 cisco ip subnet-zero ! ! ! ip ssh time-out
120 ip ssh authentication-retries 3 ! call rsvp-sync ! !
! fax interface-type modem mta receive maximum-
recipients 0 ! controller E1 2/0 ! ! ! interface
FastEthernet0/0 ip address 100.100.100.2 255.255.255.0
duplex auto speed auto ! interface FastEthernet0/1 ip
address 1.1.1.1 255.255.255.0 duplex auto speed auto !
interface BRI4/0 no ip address shutdown ! interface
BRI4/1 no ip address shutdown ! interface BRI4/2 no ip
address shutdown ! interface BRI4/3 no ip address
shutdown ! ip classless ip route 0.0.0.0 0.0.0.0
100.100.100.1 ip http server ip pim bidir-enable ! !
dial-peer cor custom ! ! line con 0 line 97 108 line aux
0 line vty 0 4 login ! end
```

Routeur House

```
Building configuration...

Current configuration : 797 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname House ! logging queue-limit 100 enable password
cisco ! ip subnet-zero no ip domain lookup ! ! interface
Ethernet0 ip address 10.66.79.210 255.255.255.224 hold-
queue 100 out ! interface Ethernet1 ip address
100.100.100.1 255.255.255.0 ip classless ip route
0.0.0.0 0.0.0.0 10.66.79.193 ip route 1.1.1.0
255.255.255.0 100.100.100.2 ip http server no ip http
secure-server ! ! ! line con 0 stopbits 1 line vty 0 4
password cisco login ! scheduler max-task-time 5000 end
```

Configuration initiale de capteur

Remarque: Si vous avez déjà exécuté la première installation de votre capteur, poursuivez à l'importation le capteur dans la section de MC d'ID.

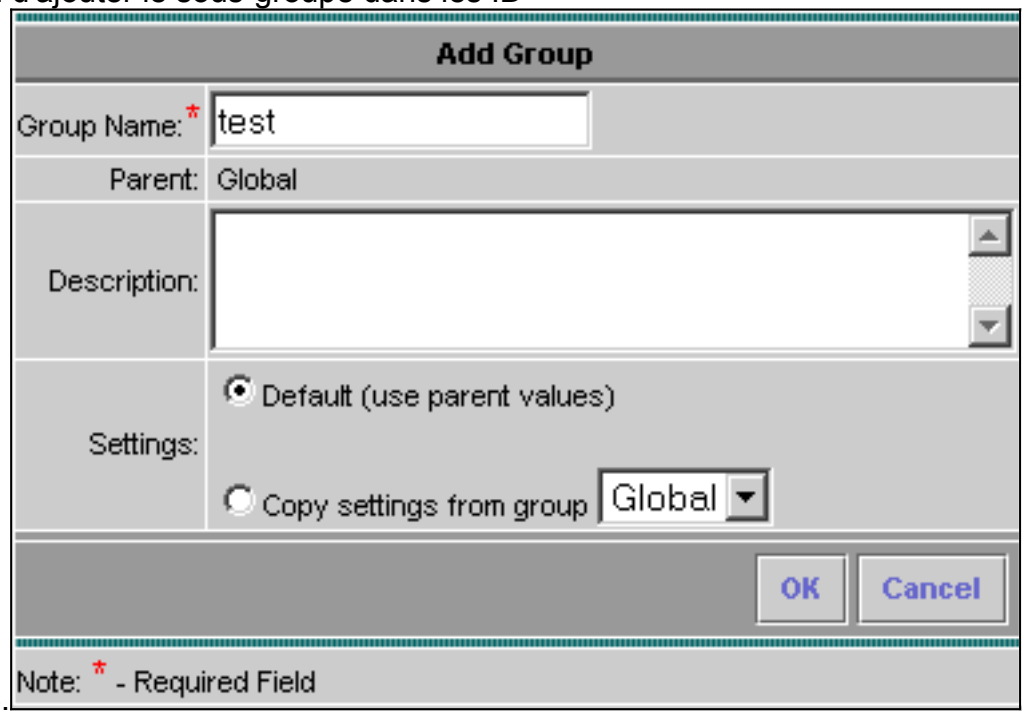
1. Console dans le capteur.Vous êtes incité pour un nom d'utilisateur et mot de passe. Si c'est la première fois vous consolez dans le capteur, vous devez ouvrir une session avec le nom d'utilisateur **Cisco** et le mot de passe cisco.
2. Vous êtes incité à changer le mot de passe et à retaper le nouveau mot de passe à la machine pour confirmer.

3. Tapez l'**installation** et écrivez l'information correcte à chaque prompt pour installer des paramètres de base pour votre capteur, selon cet exemple :`sensor5#setup --- System Configuration Dialog --- At any point you may enter a question mark '?' for help. User ctrl-c to abort configuration dialog at any prompt. Default settings are in square brackets '[]'. Current Configuration: networkParams ipAddress 10.66.79.195 netmask 255.255.255.224 defaultGateway 10.66.79.193 hostname sensor5 telnetOption enabled accessList ipAddress 10.66.79.0 netmask 255.255.255.0 exit timeParams summerTimeParams active-selection none exit exit service webServer general ports 443 exit exit 5 Save the config: (It might take a few minutes for the sensor saving the configuration) [0] Go to the command prompt without saving this config. [1] Return back to the setup without saving this config. [2] Save this configuration and exit setup. Enter your selection[2]: 2`

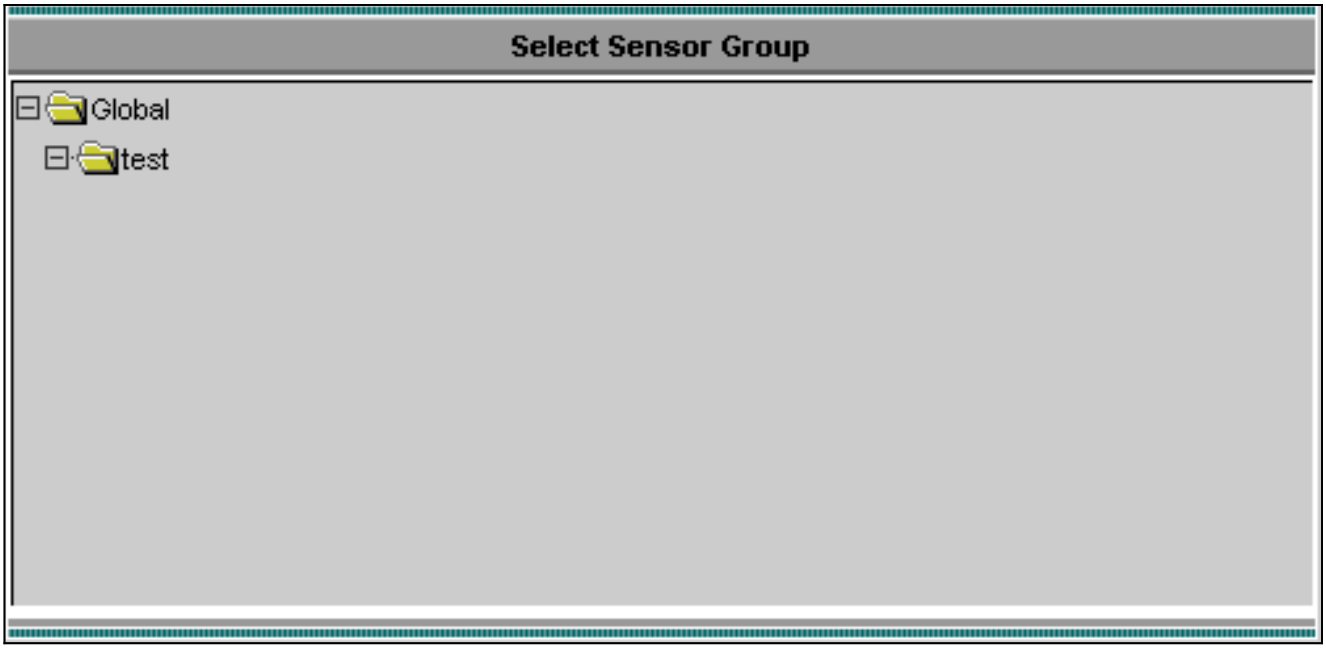
Importez le capteur dans des ID MC

Terminez-vous ces étapes afin d'importer le capteur dans les ID MC.

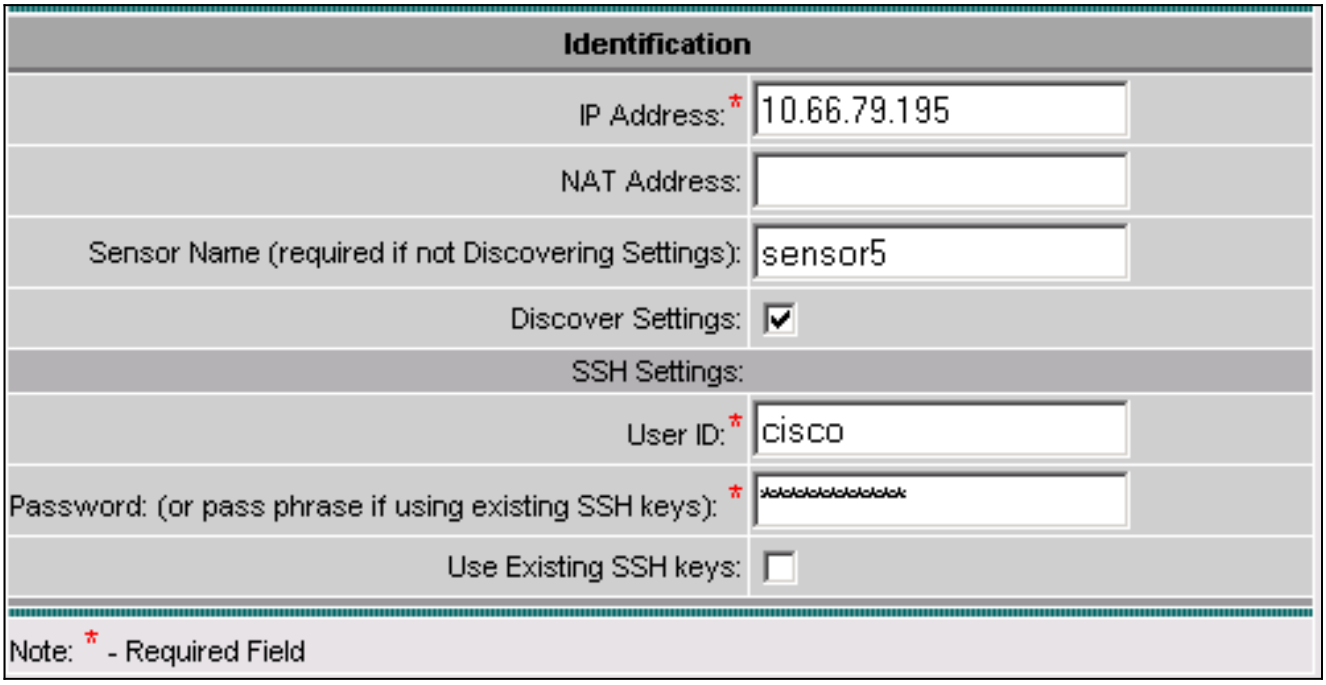
1. Parcourez à votre capteur. Dans ce cas, **http://10.66.79.250:1741** ou **https://10.66.79.250:1742**.
2. Procédure de connexion avec le nom d'utilisateur et mot de passe approprié.Dans cet exemple, le nom d'utilisateur est **admin** et le mot de passe est **Cisco**.
3. Choisissez la **solution de Gestion VPN/Security** > le **centre de Gestion** et cliquez sur les **capteurs d'ID**.
4. Cliquez sur l'onglet de périphériques et choisissez le **groupe de capteur**.
5. Le point culminant **global** et le clic **créent le sous-groupe**.
6. Écrivez le nom de groupe et assurez-vous que le **par défaut** est choisi, puis cliquent sur OK afin d'ajouter le sous-groupe dans les ID MC.



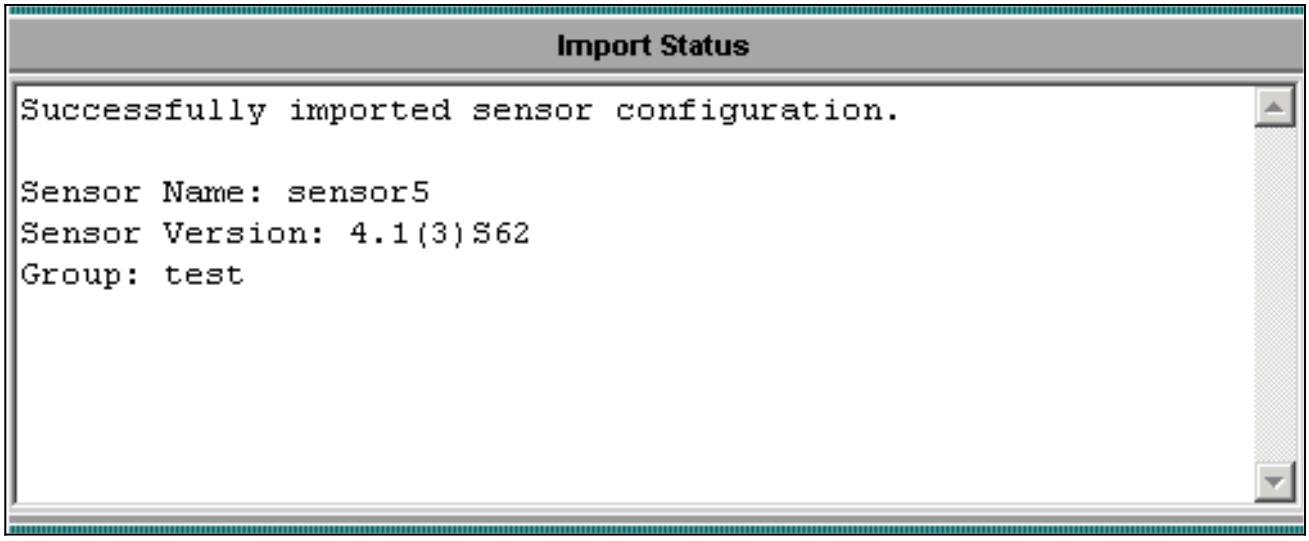
7. Choisissez les **périphériques** > le **capteur**, mettez en valeur le sous-groupe créé dans l'étape précédente (dans ce cas, **test**), et cliquez sur Add.
8. Mettez en valeur le sous-groupe et cliquez sur Next.



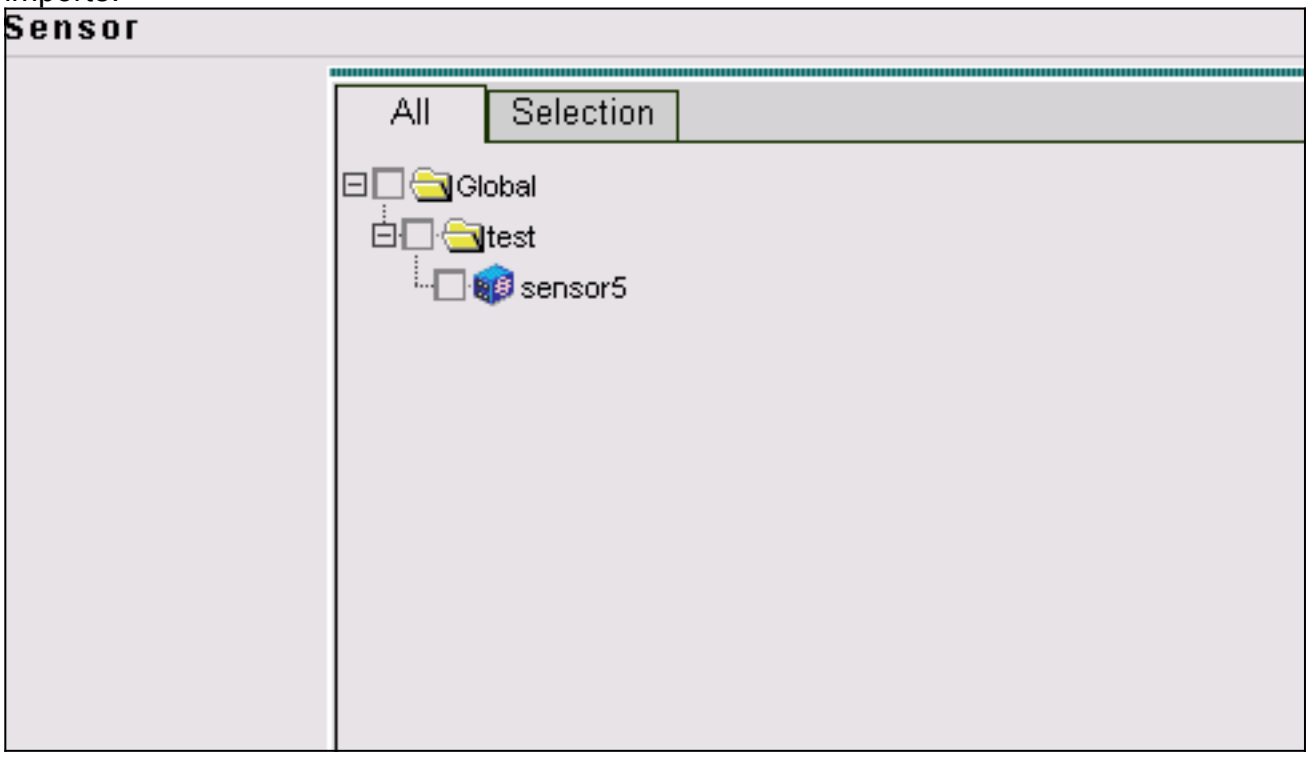
9. Écrivez les détails selon cet exemple et cliquez sur Next afin de continuer.



10. Quand vous êtes présenté avec un message que les états `ont avec succès importé la configuration de capteur`, cliquez sur Finish afin de continuer.



11. Votre capteur est importé dans les ID MC. Dans ce cas, Sensor5 est importé.

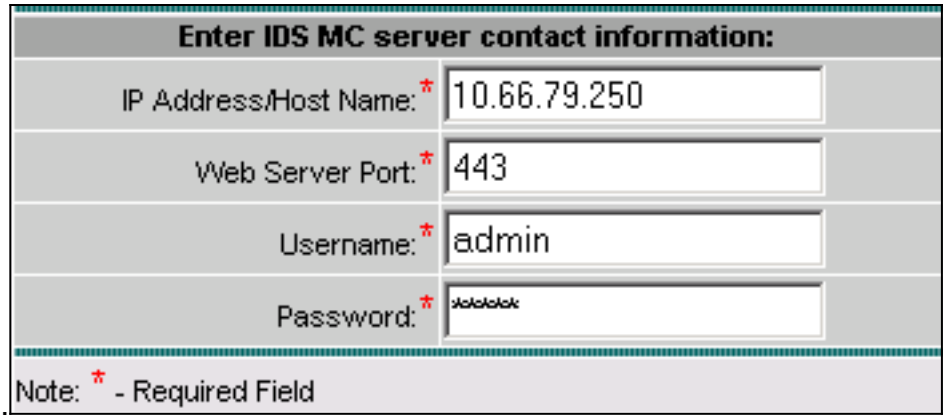


Importez le capteur dans le contrôleur de sécurité

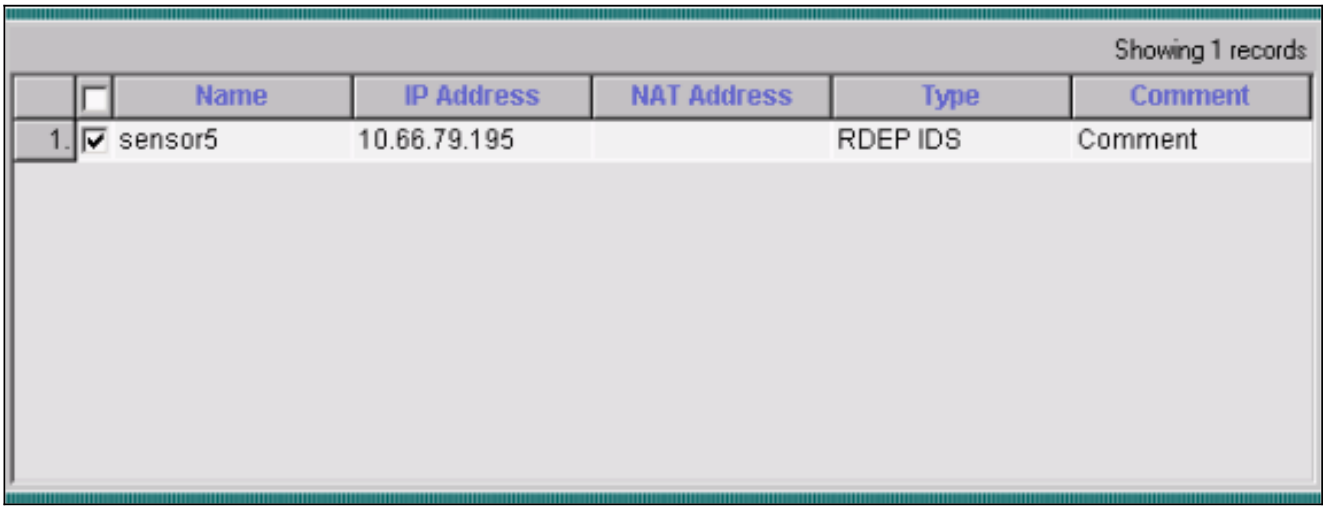
Terminez-vous ces étapes afin d'importer le capteur dans le contrôleur de sécurité.

1. Au menu de serveur VMS, choisissez la **solution de Gestion VPN/Security** > le **centre** > le **contrôleur de sécurité de surveillance**.
2. Sélectionnez l'onglet de périphériques, puis cliquez sur l'**importation** et écrivez les informations du serveur de MC d'ID, selon cet

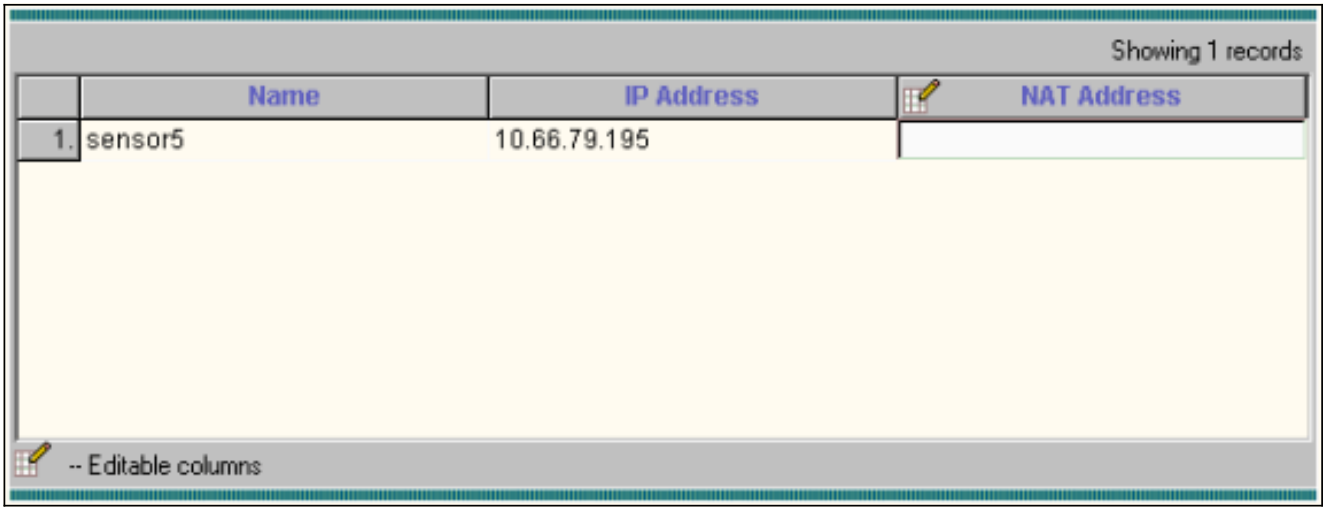
exemple.



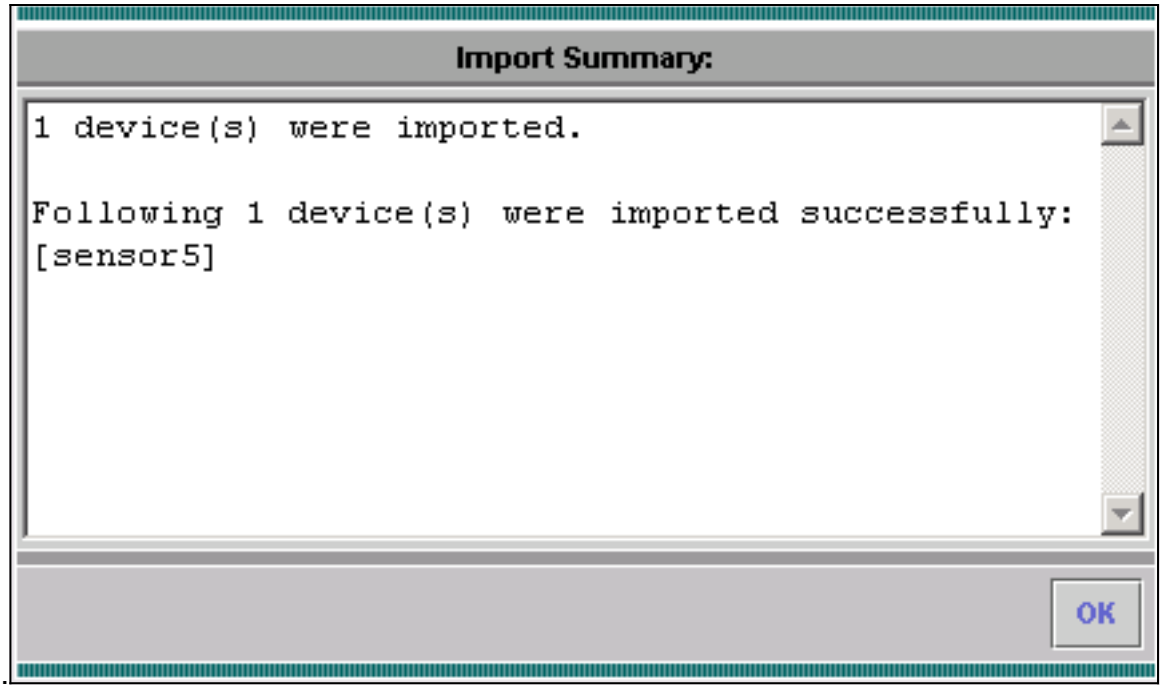
3. Sélectionnez votre capteur (dans ce cas, **sensor5**) et cliquez sur Next afin de continuer.



4. Si nécessaire, mettez à jour l'adresse NAT pour votre capteur, alors cliquez sur Finish afin de
continuer.

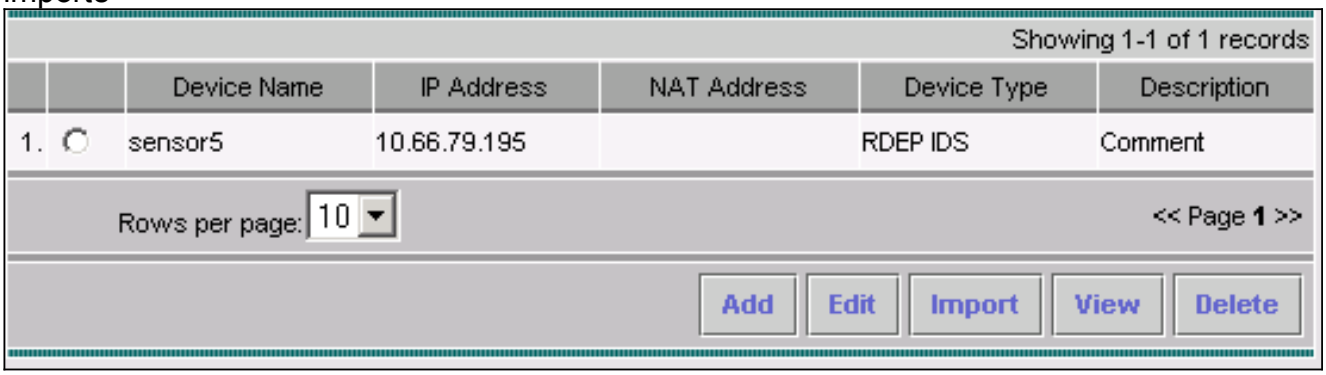


5. Cliquez sur OK afin de terminer importer le capteur des ID MC dans le contrôleur de



sécurité.

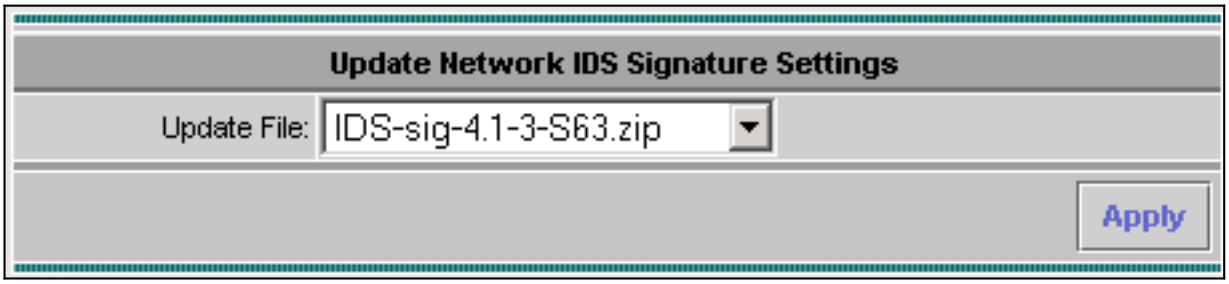
6. Vous pouvez maintenant voir que votre capteur est avec succès importé



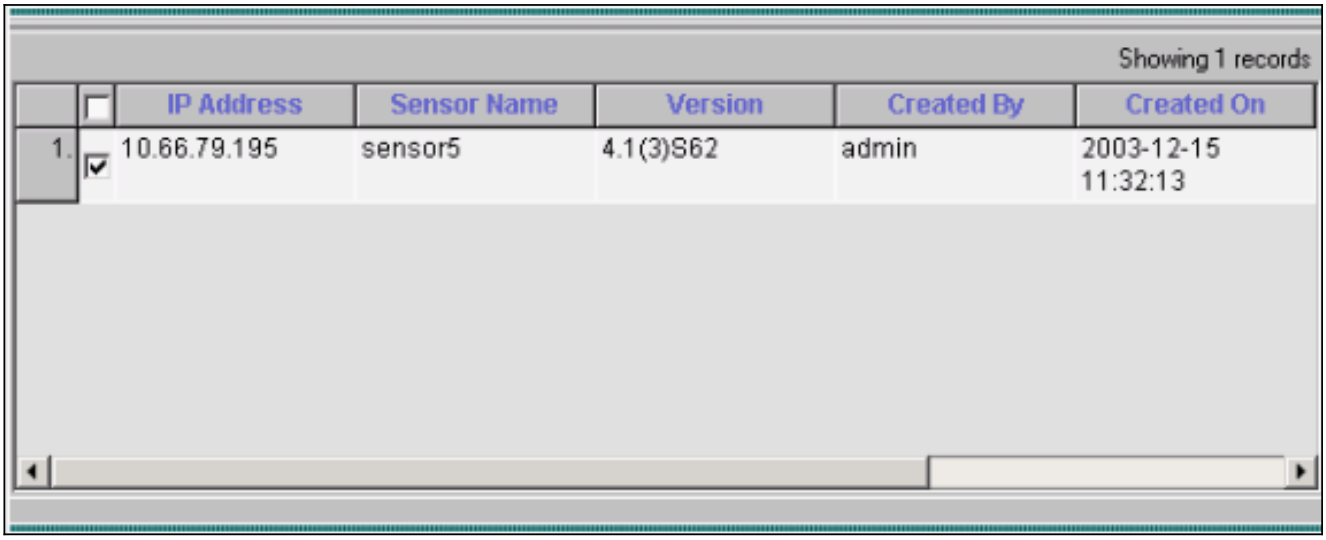
ID MC d'utilisation pour des mises à jour de signature

Cette procédure explique comment utiliser des ID MC pour des mises à jour de signature.

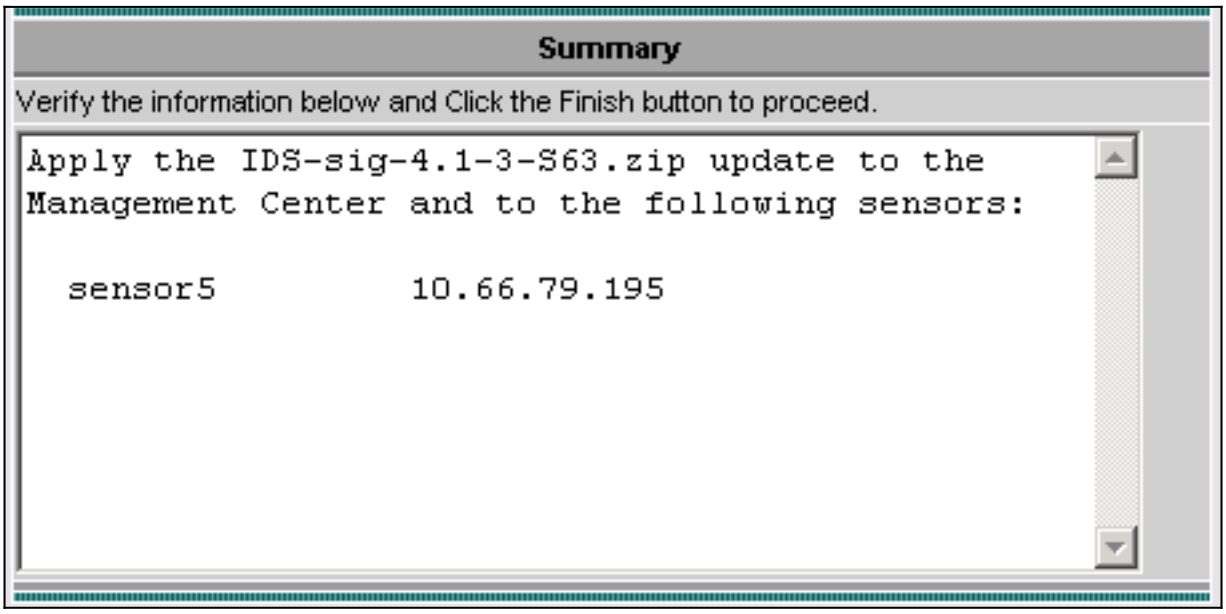
1. Téléchargez les mises à jour de signature d'ID de réseau (clients enregistrés seulement) et sauvegardez-les dans le répertoire **C:\PROGRA~1\CSCOpx\MDC\etc\ids\updates** sur votre serveur VMS.
2. Àla console de serveur VMS, choisissez la **solution de Gestion VPN/Security** > le **centre de Gestion** > les **capteurs d'ID**.
3. Sélectionnez l'onglet de configuration et cliquez sur les **mises à jour**.
4. **Signatures d'ID de réseau de mise à jour de** clic.
5. Sélectionnez la signature que vous voulez améliorer du menu déroulant et cliquer sur Apply afin de continuer.



6. Sélectionnez les capteurs pour mettre à jour et cliquer sur Next afin de continuer.



7. Après que vous soyez incité à appliquer la mise à jour au centre de Gestion, aussi bien que le capteur, cliquez sur Finish afin de continuer.



8. Telnet ou console dans l'interface de ligne de commande de capteur. Vous voyez les informations semblables à ceci :`sensor5#`
`Broadcast message from root (Mon Dec 15 11:42:05 2003):`
`Applying update` **`IDS-sig-4.1-3-S63. This may take several minutes.`** `Please do not reboot the sensor during this update. Broadcast message from root (Mon Dec 15 11:42:34 2003):` **`Update complete. sensorApp is restarting This may take several minutes.`**
9. Attendez quelques minutes pour permettre à la mise à jour pour se terminer, puis écrivez le **show version** afin de vérifier.`sensor5#`**`show version`** `Application Partition:` **`Cisco Systems Intrusion Detection Sensor, Version 4.1(3)S63 Upgrade History: * IDS-sig-4.1-3-S62 07:03:04 UTC Thu Dec 04 2003 IDS-sig-4.1-3-S63.rpm.pkg 11:42:01 UTC Mon Dec 15 2003`**

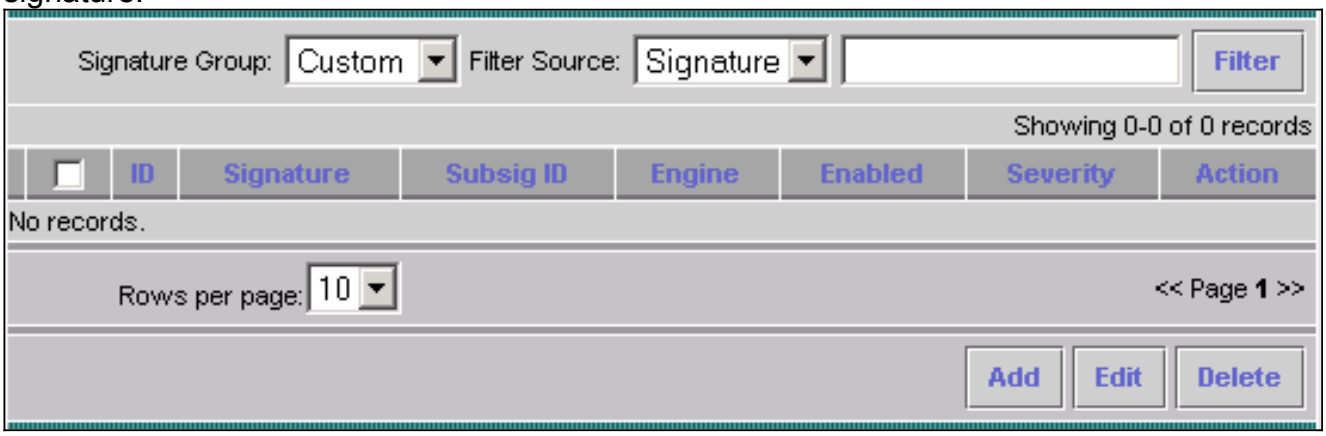
Configurez la Réinitialisation TCP pour le routeur IOS

Terminez-vous ces étapes afin de configurer la Réinitialisation TCP pour le routeur IOS.

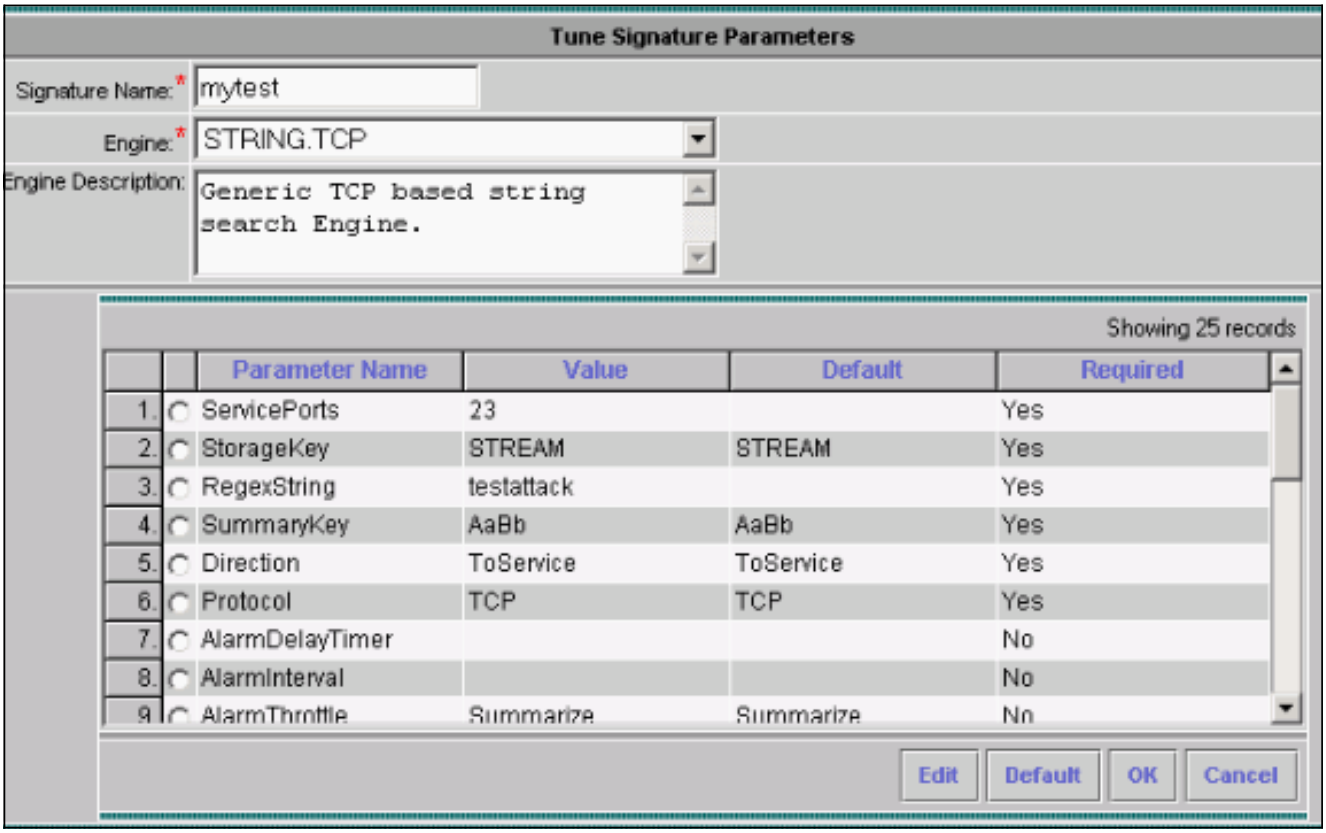
1. Choisissez la **solution de Gestion VPN/Security** > le **centre de Gestion** > les **capteurs d'ID**.
2. Sélectionnez l'onglet de configuration, sélectionnez votre capteur de sélecteur d'objet, puis

cliquez sur les **configurations**.

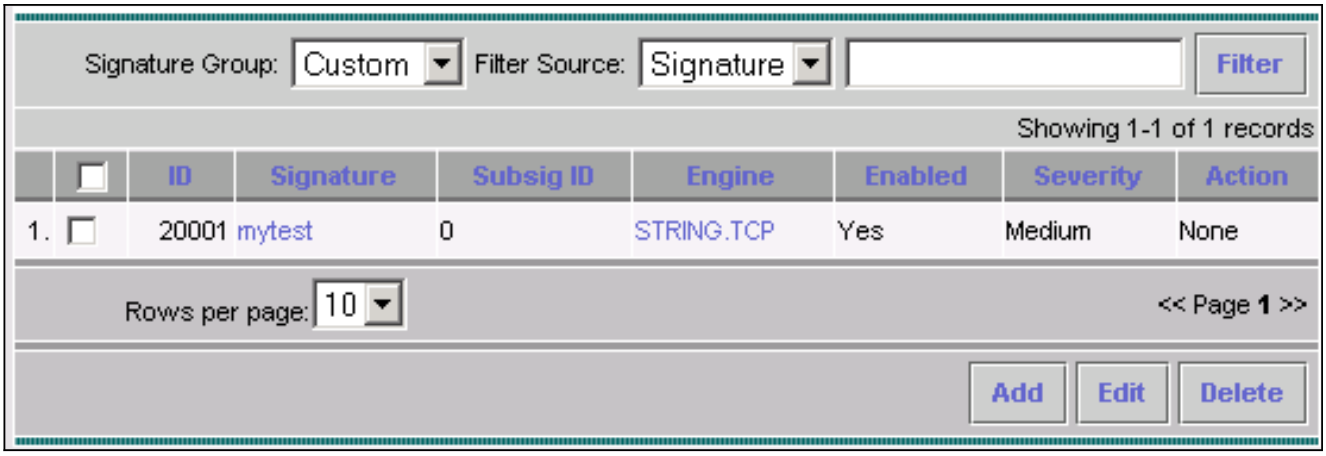
3. **Les signatures** choisies, la **coutume de** clic, et cliquent sur Add afin d'ajouter une nouvelle signature.



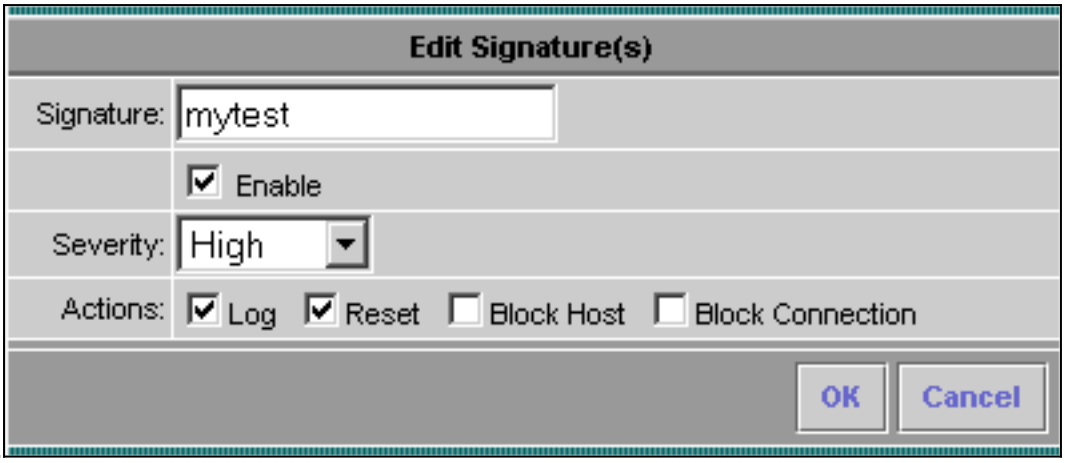
4. Écrivez le nouveau nom de signature, puis sélectionnez l'engine (dans ce cas, **STRING.TCP**).
5. Vérifiez la case d'option appropriée afin de personnaliser les paramètres disponibles et puis cliquer sur Edit.Dans cet exemple, le paramètre de ServicePorts est édité pour changer sa valeur à **23** (pour port 23). Le paramètre de RegexString est également édité pour ajouter le **testattack de** valeur. Quand c'est complet, cliquez sur OK pour continuer.



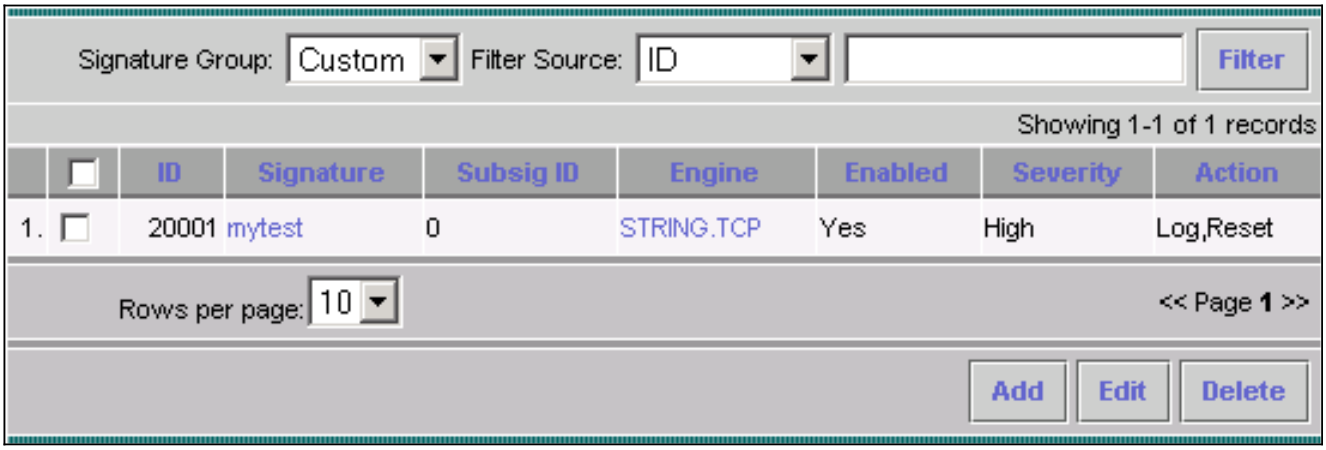
6. Cliquez sur le nom de la signature afin d'éditer la sévérité et les actions de signature ou activer/la signature.



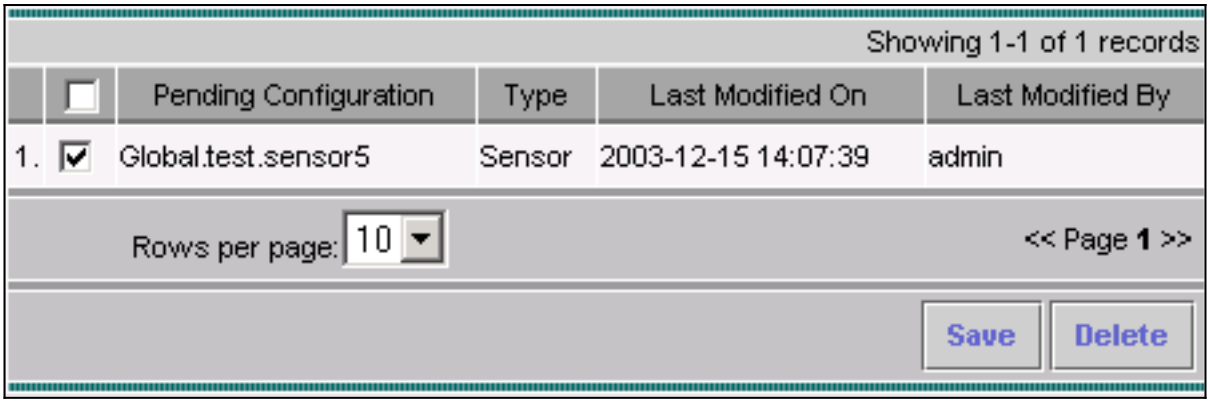
7. Dans ce cas, la sévérité est changée à la **haute** et le **log et la remise d'**action est choisi. Cliquez sur OK afin de continuer.



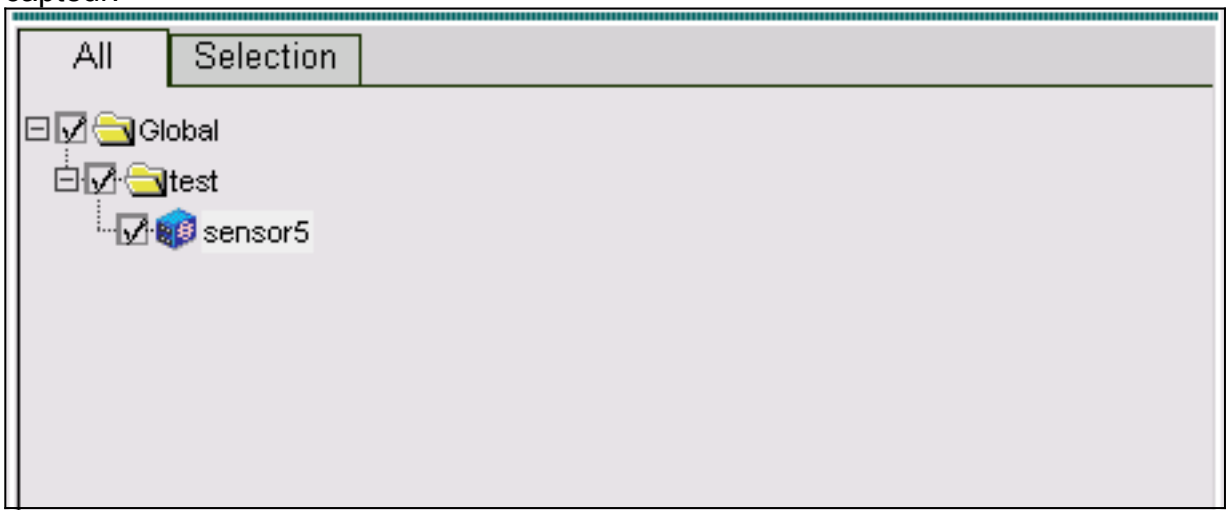
8. La signature complète semble semblable à ceci :



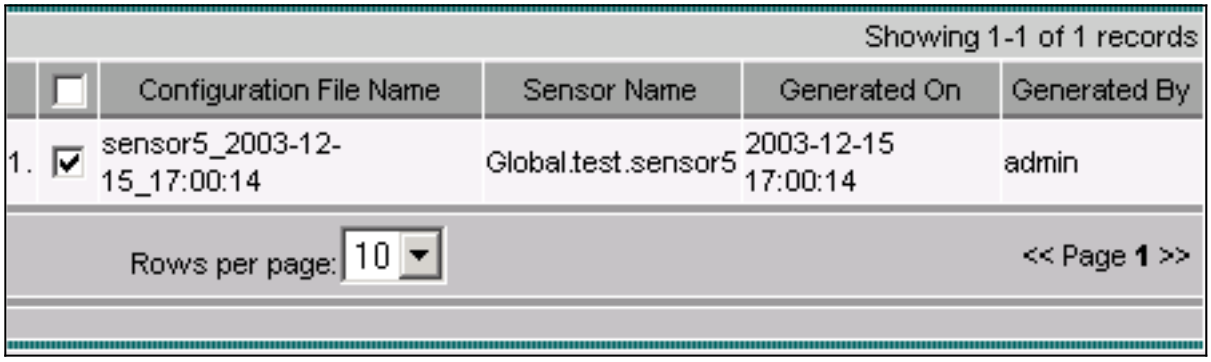
9. Choisissez la **configuration > en suspens**, vérifiez la configuration en attente pour s'assurer qu'elle est correcte, et clique sur la **sauvegarde**.



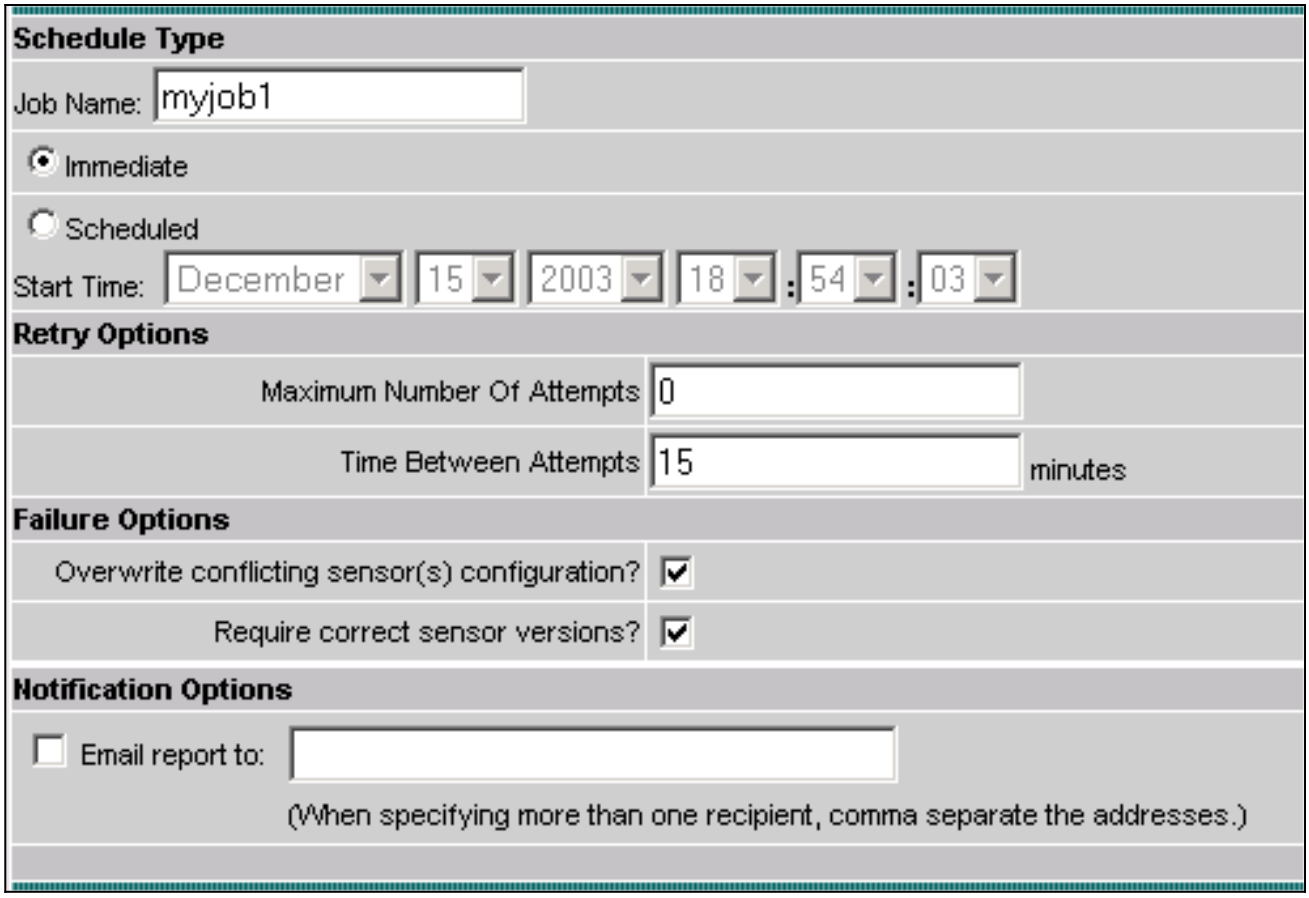
10. Choisissez le **déploiement > se produisent**, et puis cliquent sur Apply afin de pousser les modifications de configuration au capteur.



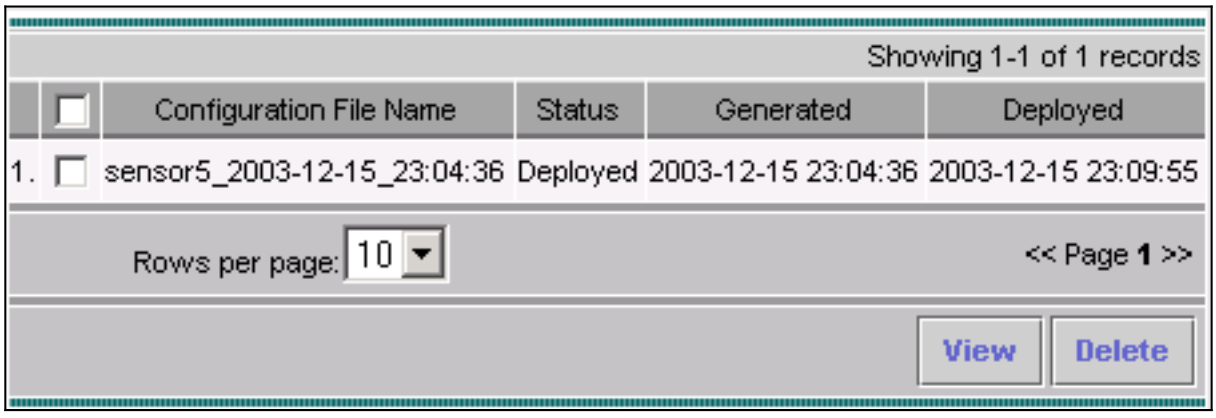
11. Choisissez le **déploiement > se déploient** et cliquent sur Submit.
12. Vérifiez la case à cocher à côté de votre capteur et le clic **se déploient**.
13. Vérifiez la case à cocher pour le travail dans la file d'attente et cliquez sur Next afin de continuer.



14. Écrivez le nom de JOB et programmez le travail comme **immédiat**, puis cliquez sur Finish.



15. Choisissez le **déploiement > se déploient > en suspens**.Attendez quelques minutes jusqu'à ce que tous les travaux en attente aient été terminés. La file d'attente devrait alors être vide.
16. Choisissez la **configuration** > l'**historique** afin de confirmer le déploiement.Assurez que le statut de la configuration est affiché comme **déployé**. Ceci signifie que la configuration de capteur est mise à jour avec
succès.



Vérifiez

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

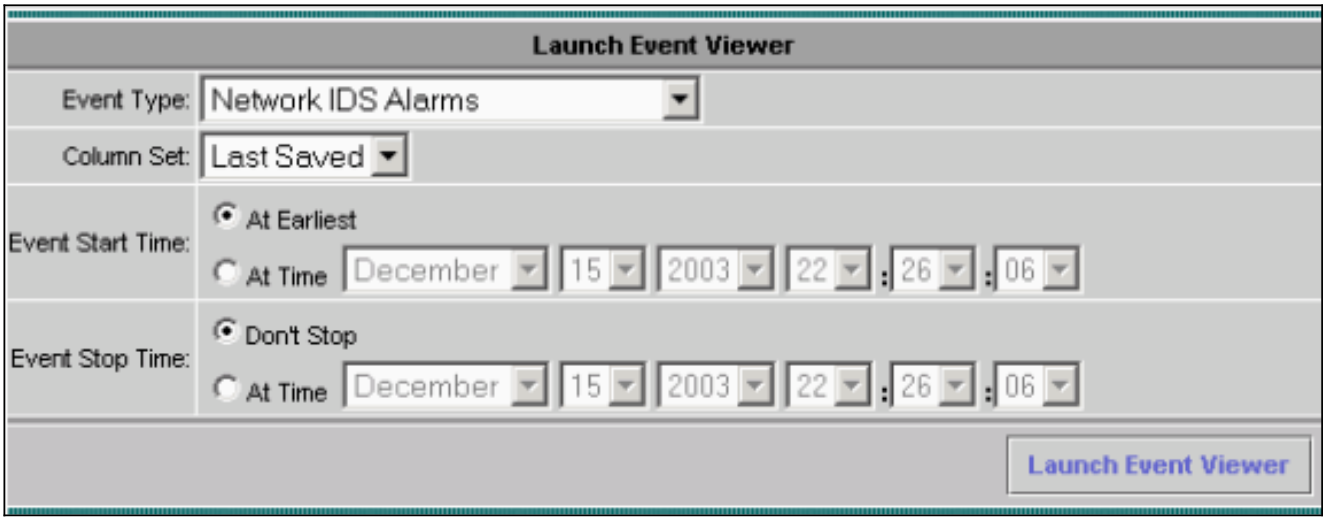
Lancez l'attaque et la Réinitialisation TCP

Lancez une attaque de test et vérifiez les résultats afin de vérifier que les travaux par processus de blocage correctement.

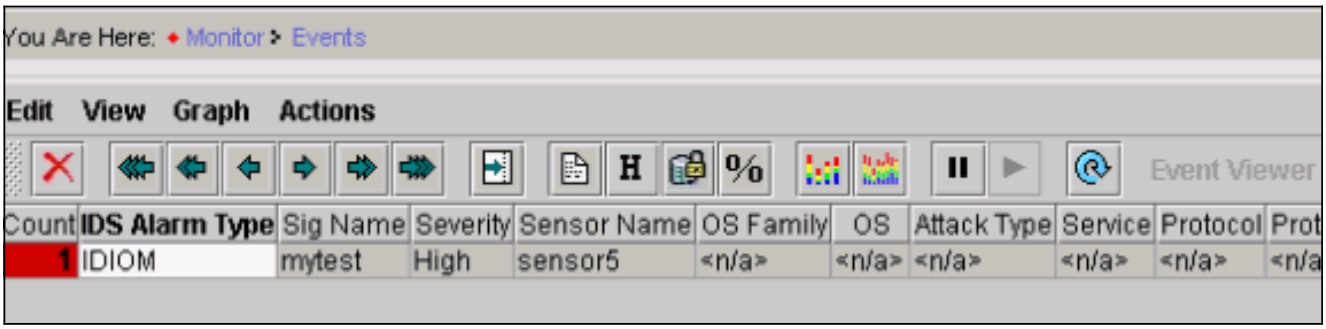
1. Avant que l'attaque soit lancée, choisissez la **solution de Gestion VPN/Security** > le **centre** >

le **contrôleur de sécurité de surveillance**.

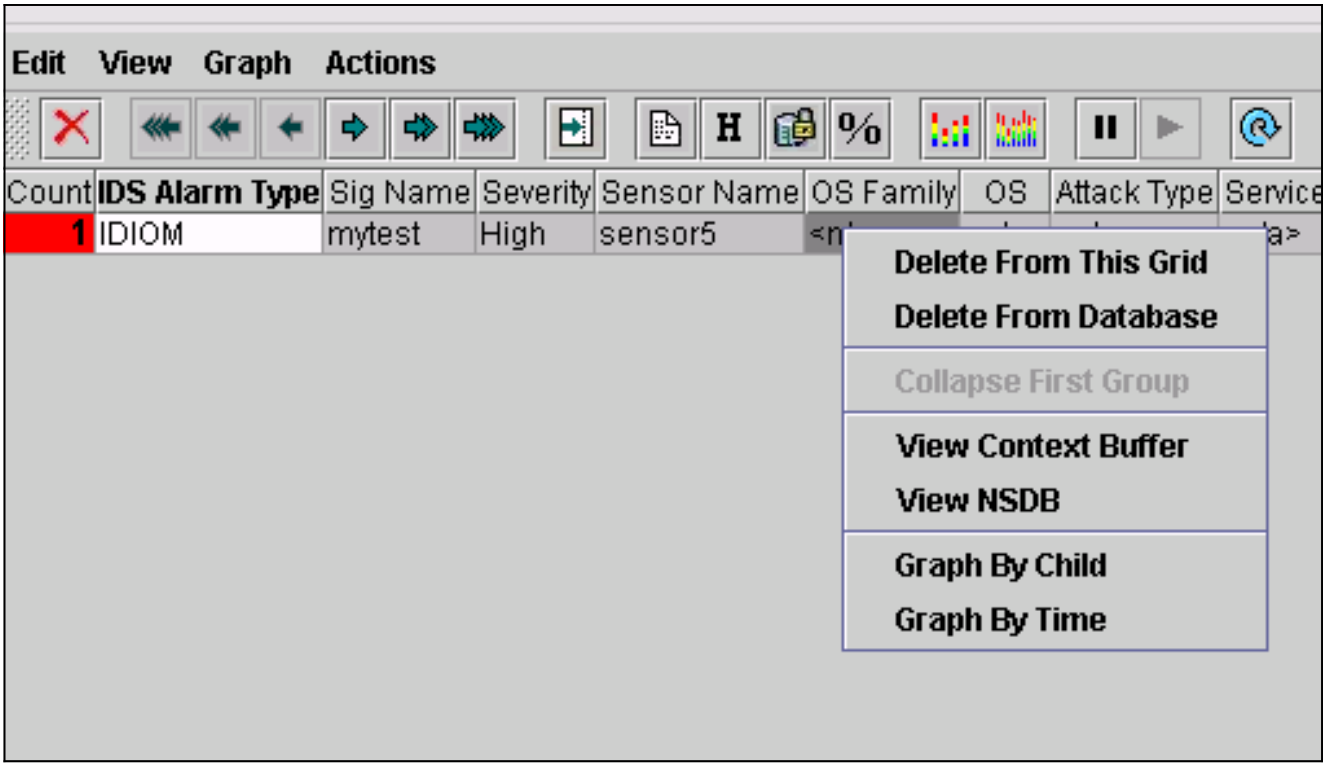
2. Choisissez le **moniteur du** menu principal et cliquez sur les **événements**.
3. **Visualisateur d'événements de lancement de**
   clic.



4. Telnet d'un routeur au **testattack d'**autre et de type afin de lancer l'attaque.Dans ce cas, nous Telnetted de la lumière du routeur à la Chambre de routeur. Dès que vous appuierez sur le **<space>** ou le **<enter>**, après que vous tapiez le **testattack**, votre session de telnet devrait être remise à l'état initial.`light#telnet 100.100.100.1 Trying 100.100.100.1 ... Open User Access Verification Password: house>en Password: house#testattack !--- The Telnet session is reset due to the !--- signature "testattack" being triggered. [Connection to 100.100.100.1 lost]`
5. Du visualisateur d'événements, **base de données de requête de** clic pour de nouveaux événements maintenant.Vous voyez l'alerte pour l'attaque précédemment
   lancée



6. En cas le visualiseur, mettent en valeur l'alarme, la cliquent avec le bouton droit et sélectionnent la **mémoire tampon** ou la **vue NSDB de contexte de vue** pour visualiser plus d'informations détaillées au sujet de
   l'alarme.



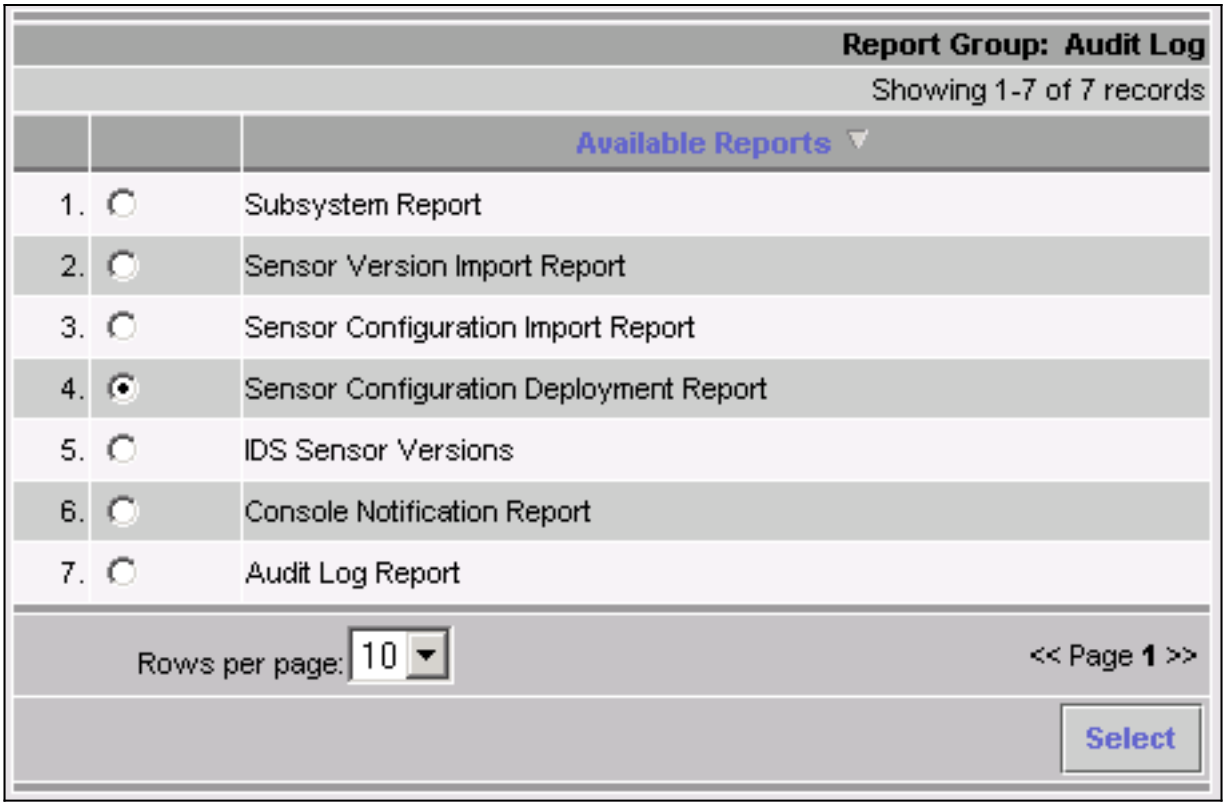
Dépannez

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

Procédure de dépannage

Terminez-vous ces étapes afin de dépanner.

1. Dans les ID MC, choisissez les **états > se produisent**.Selon le type de problème, d'autres détails devraient être trouvés dans un des sept états disponibles.



2. Tandis que le blocage utilise le port de commandement et de contrôle de configurer les listes d'accès de routeur, des remises de TCP sont envoyées de l'interface de reniflement du capteur. Assurez que vous avez réparti le port approprié, utilisant la commande de **set span** sur le commutateur, semblable à ceci :
```
set span <src_mod/src_port><dest_mod/dest_port> both inpkts enable banana (enable) set span 2/12 3/6 both inpkts enable Overwrote Port 3/6 to monitor transmit/receive traffic of Port 2/12 Incoming Packets enabled. Learning enabled. Multicast enabled. banana (enable) banana (enable) banana (enable) show span Destination : Port 3/6 !--- Connect to sniffing interface of the Sensor. Admin Source : Port 2/12 !--- In this case, connect to Ethernet1 of Router House. Oper Source : Port 2/12 Direction : transmit/receive Incoming Packets: enabled Learning : enabled Multicast : enabled
```
3. Si la Réinitialisation TCP ne fonctionne pas, ouvrez une session au capteur et sélectionnez la commande d'**événement d'exposition**.Lancez l'attaque, et le contrôle pour voir si l'alarme est déclenchée. Si l'alarme est déclenchée, le contrôle pour l'assurer est placé pour la **Réinitialisation TCP de** type d'action.

Informations connexes

- Page Cisco Secure de prise en charge de la détection d'intrusion
- Documentation pour le système de détection d'intrusion Cisco Secure
- Page de support de CiscoWorks VPN/Security Management Solution
- Support et documentation techniques - Cisco Systems