Configuration de la réinitialisation TCP IDS avec VMS IDS MC

Contenu

Introduction

Le document fournit un exemple de configuration du système de détection des intrusions (IDS) Cisco via VPN/Security Management Solution (VMS), IDS Management Console (IDS MC). Dans ce cas, TCP Reset (Réinitialisation TCP) du capteur IDS vers un routeur Cisco est configuré.

Conditions préalables

Conditions requises

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

- Le capteur est installé et configuré pour détecter le trafic nécessaire.
- L’interface de reniflage est étendue à l’interface externe du routeur.

Components Used

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

- VMS 2.2 avec IDS MC et Security Monitor 1.2.3
- Capteur Cisco IDS 4.1.3S(63)
- Routeur Cisco qui exécute le logiciel Cisco IOS® Version 12.3.5

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 Conventions relatives aux conseils techniques Cisco.

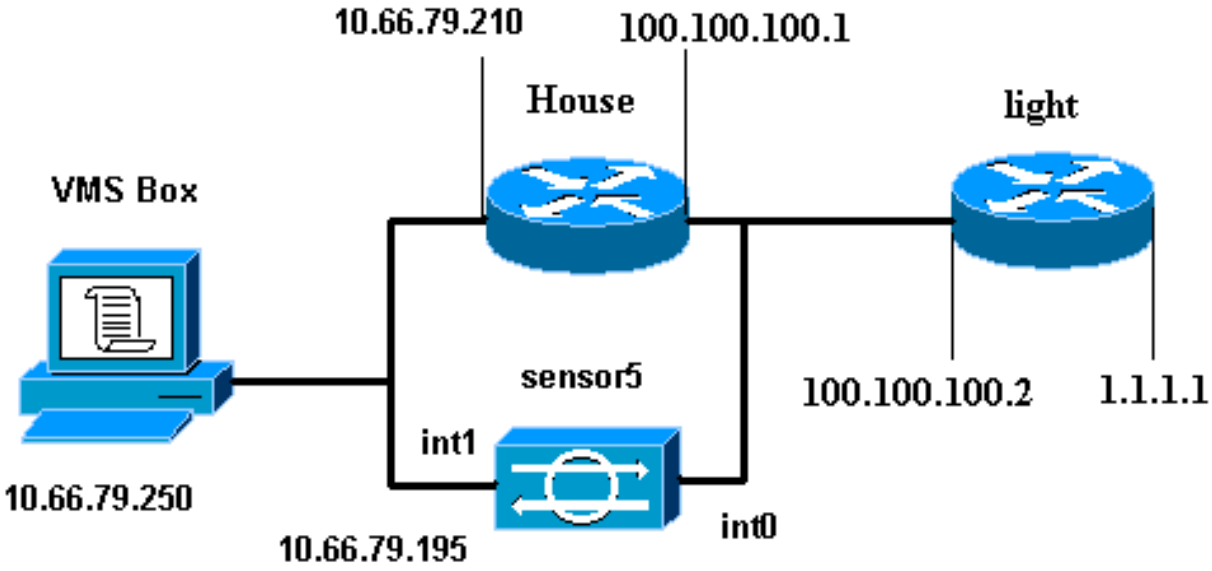
Configuration

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

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) 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.

- Voyant du routeur

- Routeur House

Voyant 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 du capteur

Remarque : Si vous avez déjà effectué la configuration initiale de votre capteur, passez à la

section Importer le capteur dans IDS MC.

1. Console dans le capteur.Vous êtes invité à saisir un nom d'utilisateur et un mot de passe. Si c'est la première fois que vous vous connectez au capteur, vous devez vous connecter avec le nom d'utilisateur **cisco** et le mot de passe **cisco**.
2. Vous êtes invité à modifier le mot de passe et à le saisir à nouveau pour confirmer.
3. Tapez **setup** et saisissez les informations appropriées à chaque invite pour configurer les paramètres de base de votre capteur, comme dans cet exemple :

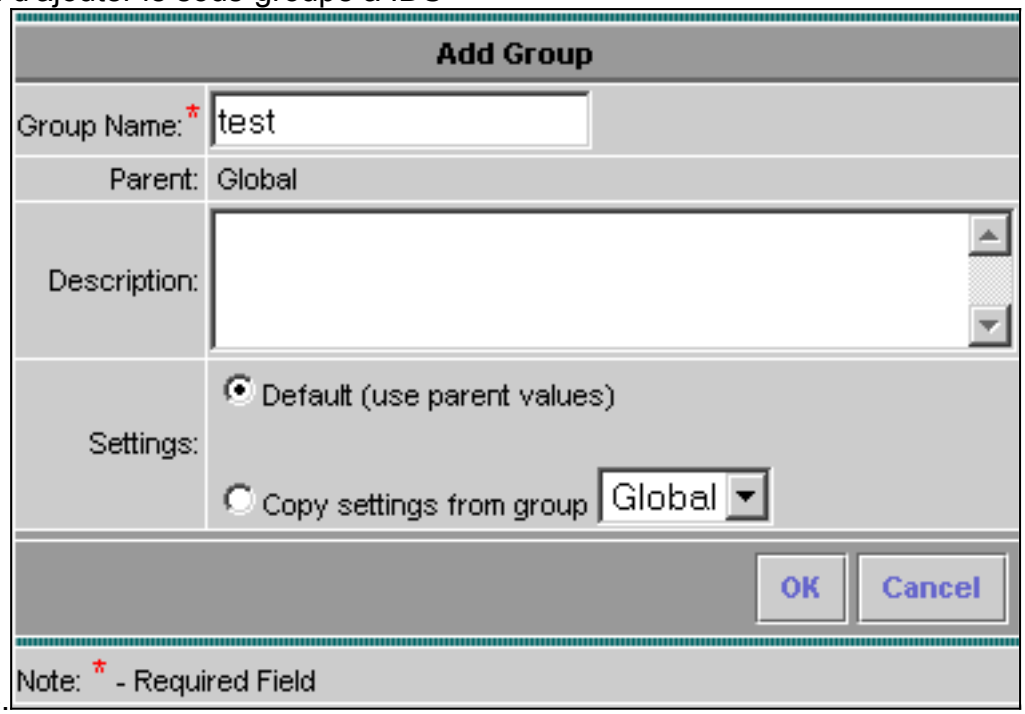
```
sensor5#setup

    --- 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
```

Importer le capteur dans IDS MC

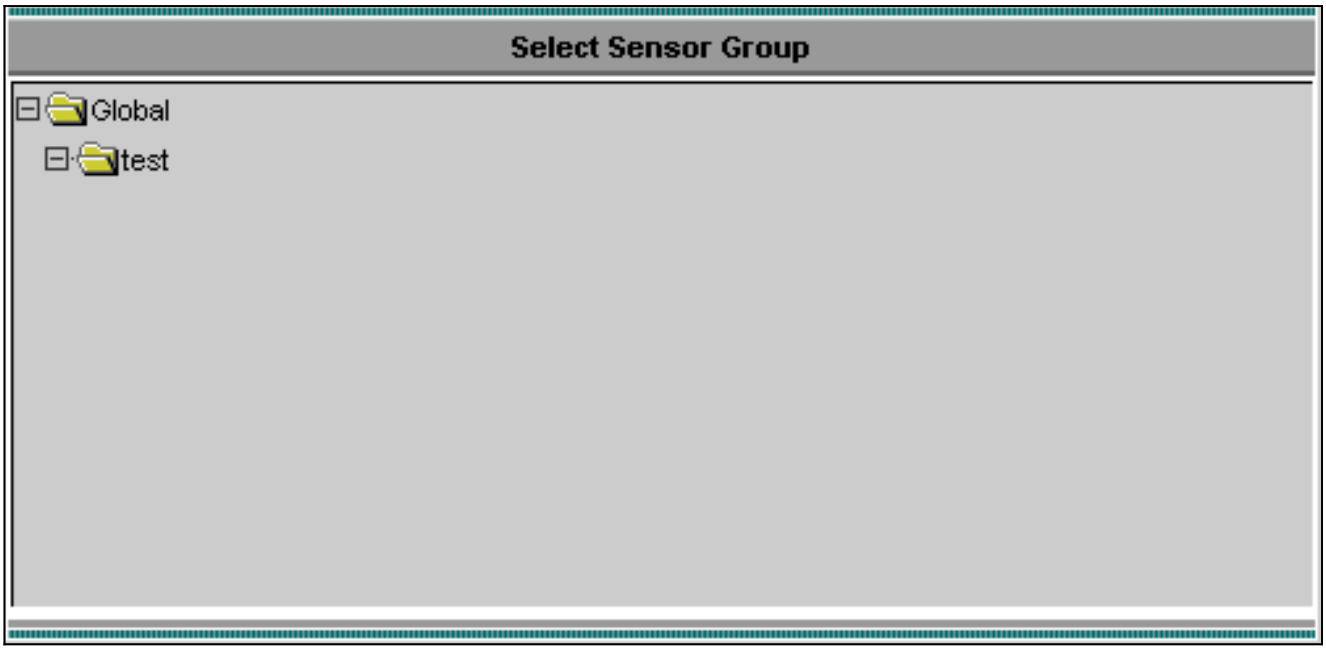
Complétez ces étapes afin d'importer le capteur dans IDS MC.

1. Accédez à votre capteur. Dans ce cas, **http://10.66.79.250:1741** ou **https://10.66.79.250:1742**.
2. Connectez-vous avec le nom d'utilisateur et le mot de passe appropriés.Dans cet exemple, le nom d'utilisateur est **admin** et le mot de passe est **cisco**.
3. Choisissez **VPN/Security Management Solution > Management Center** et cliquez sur **IDS Sensors**.
4. Cliquez sur l'onglet Périphériques et sélectionnez **Groupe de capteurs**.
5. Sélectionnez **Global** et cliquez sur **Créer un sous-groupe**.

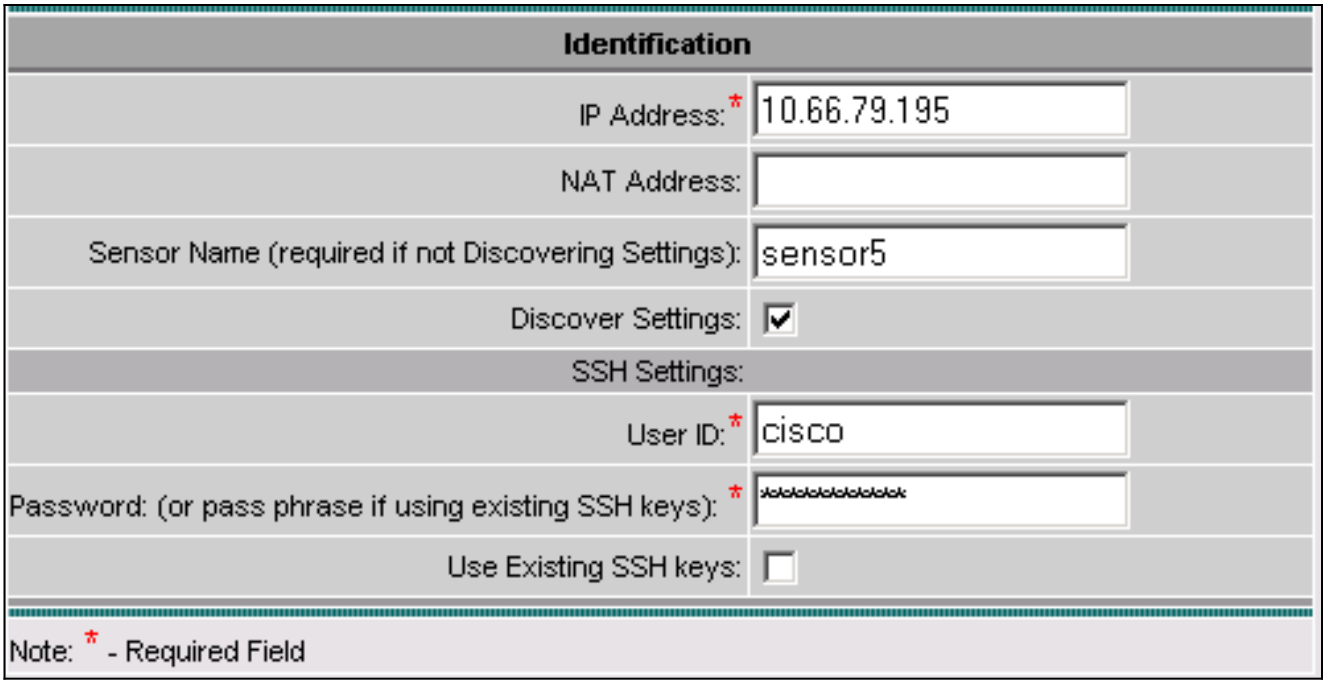
6. Entrez le nom du groupe et assurez-vous que **Default** est sélectionné, puis cliquez sur **OK** afin d'ajouter le sous-groupe à IDS MC.



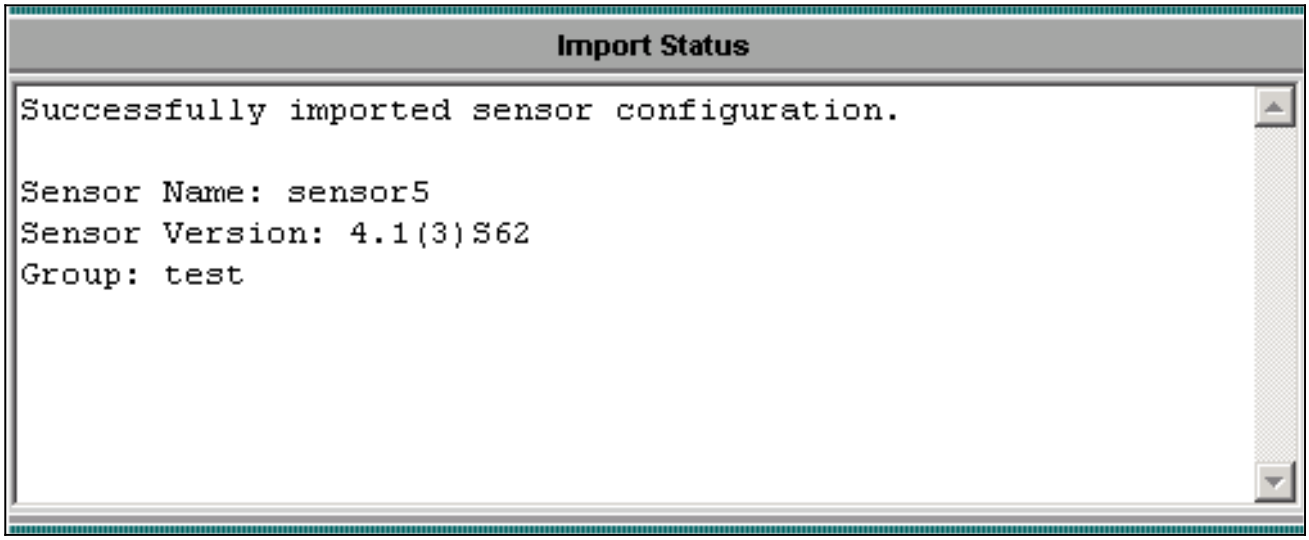
7. Choisissez **Devices > Sensor**, mettez en surbrillance le sous-groupe créé à l'étape précédente (dans ce cas, **test**), puis cliquez sur **Add**.
8. Mettez le sous-groupe en surbrillance et cliquez sur **Suivant**.



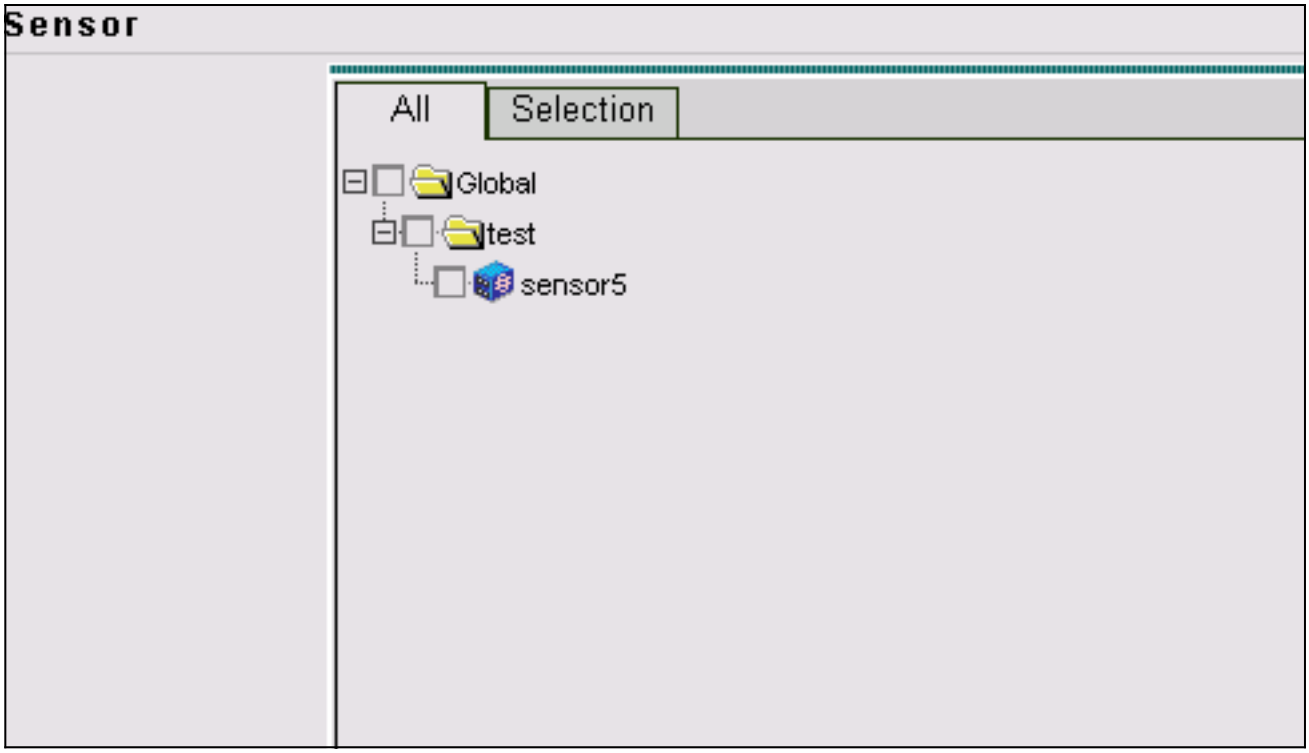
9. Entrez les détails conformément à cet exemple et cliquez sur **Suivant** pour continuer.



10. Lorsque vous recevez un message indiquant la `configuration du capteur correctement importée`, cliquez sur **Terminer** pour continuer.



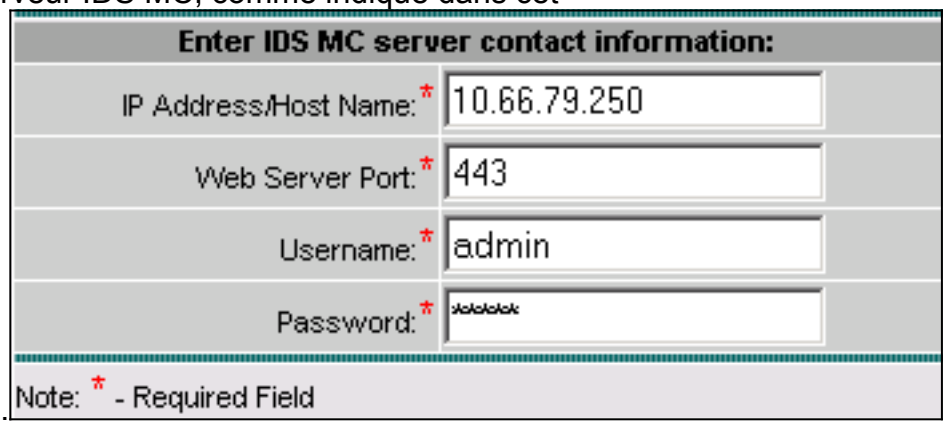
11. Votre capteur est importé dans la MC IDS. Dans ce cas, le capteur 5 est importé.



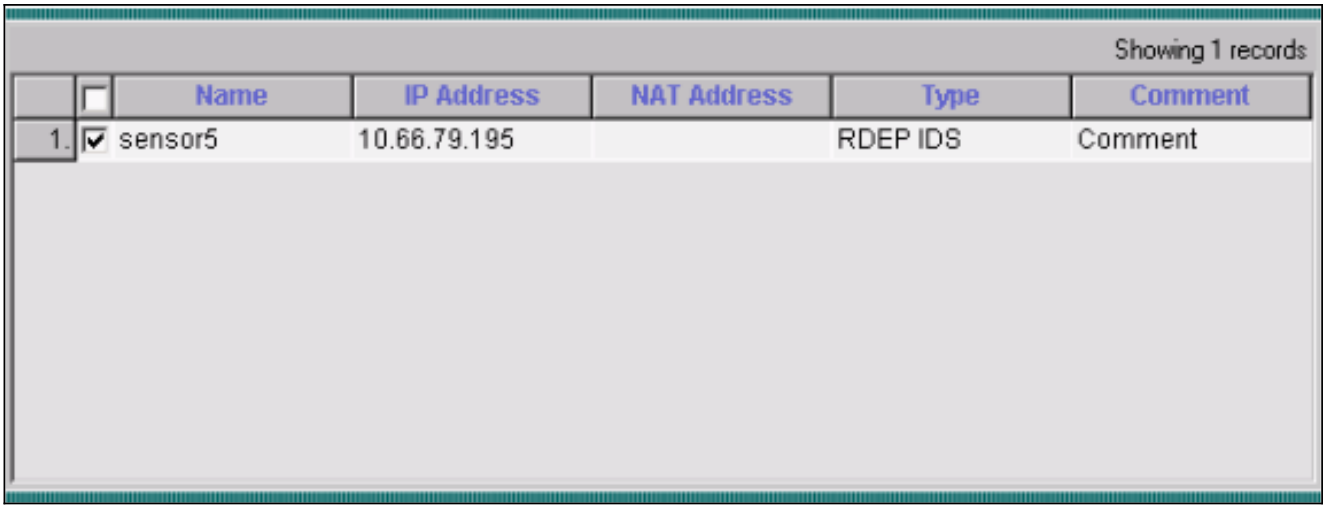
Importer le capteur dans Security Monitor

Complétez ces étapes afin d'importer le capteur dans Security Monitor.

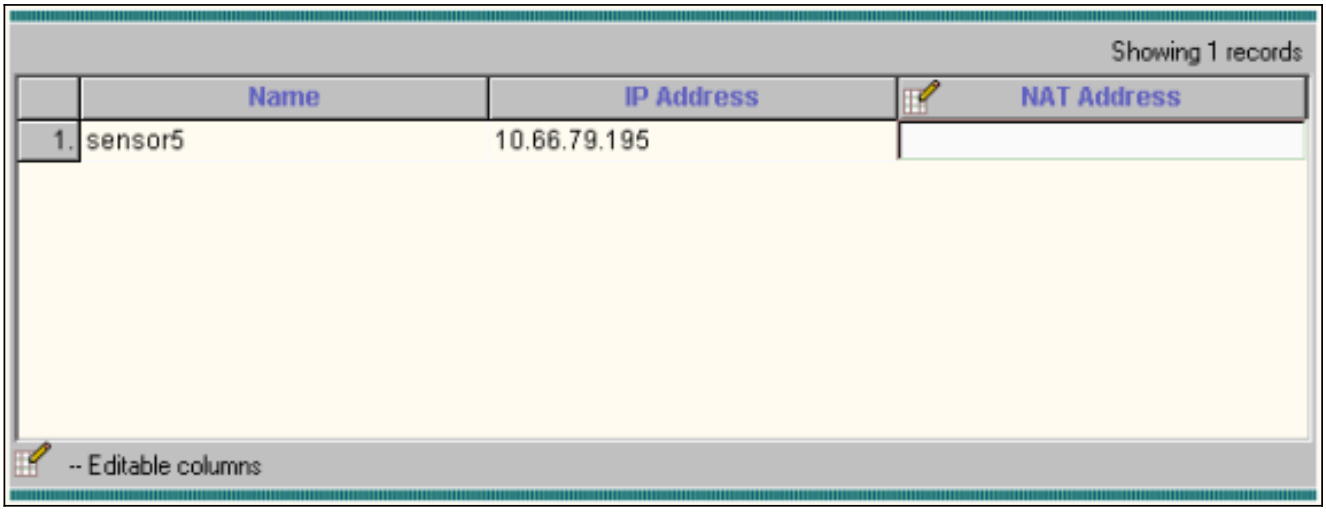
1. Dans le menu Serveur VMS, choisissez **VPN/Security Management Solution > Monitoring Center > Security Monitor**.
2. Sélectionnez l'onglet Périphériques, puis cliquez sur **Importer** et saisissez les informations sur le serveur IDS MC, comme indiqué dans cet exemple.



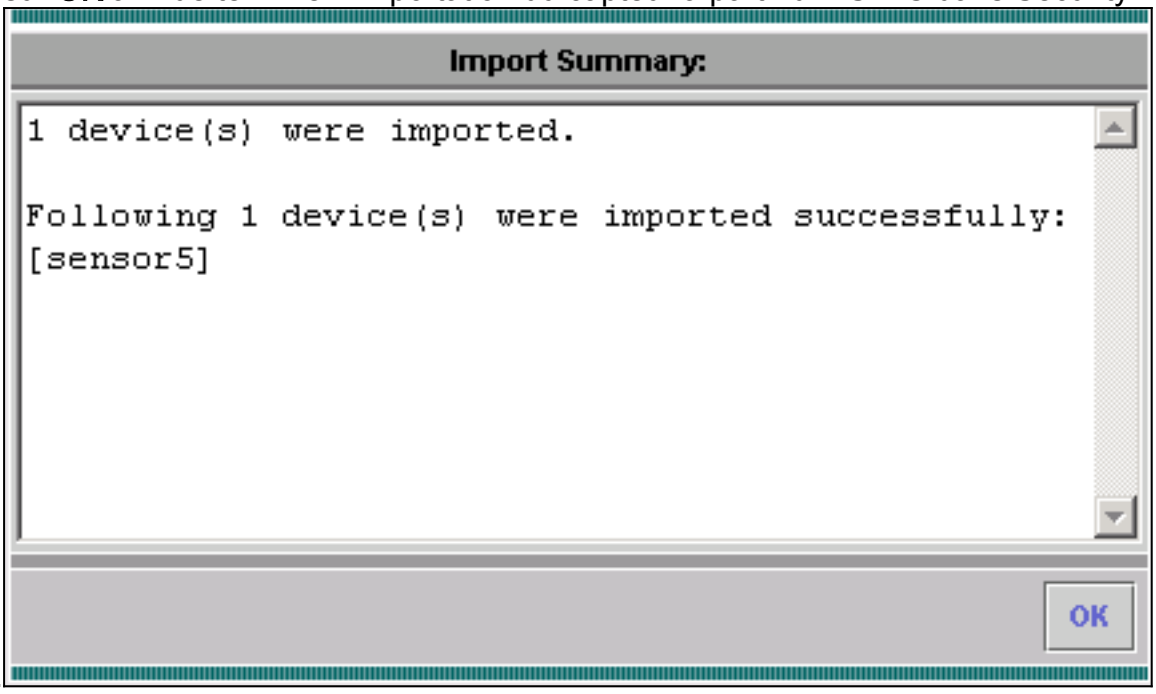
3. Sélectionnez votre capteur (dans ce cas, **capteur5**) et cliquez sur **Suivant** pour continuer.



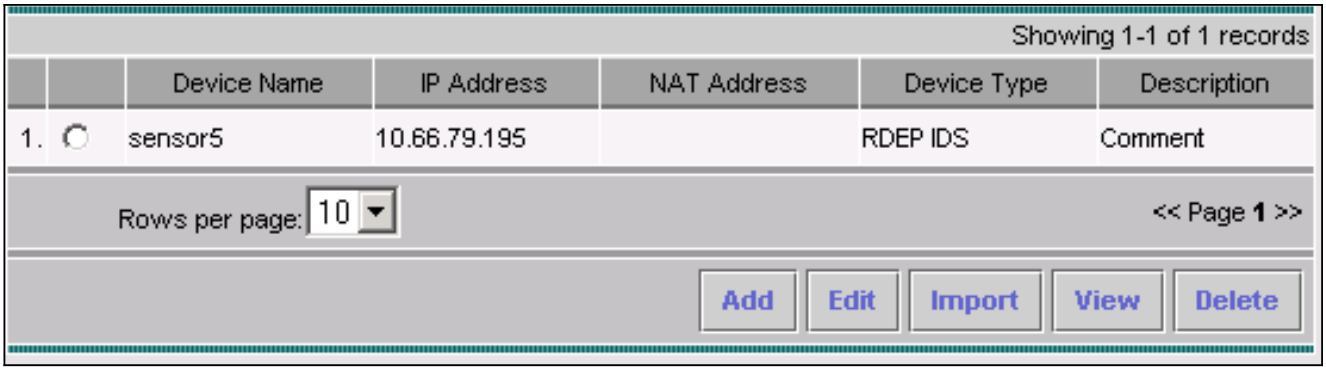
4. Si nécessaire, mettez à jour l'adresse NAT de votre capteur, puis cliquez sur **Terminer** afin de
continuer.



5. Cliquez sur **OK** afin de terminer l'importation du capteur à partir d'IDS MC dans Security Monitor.



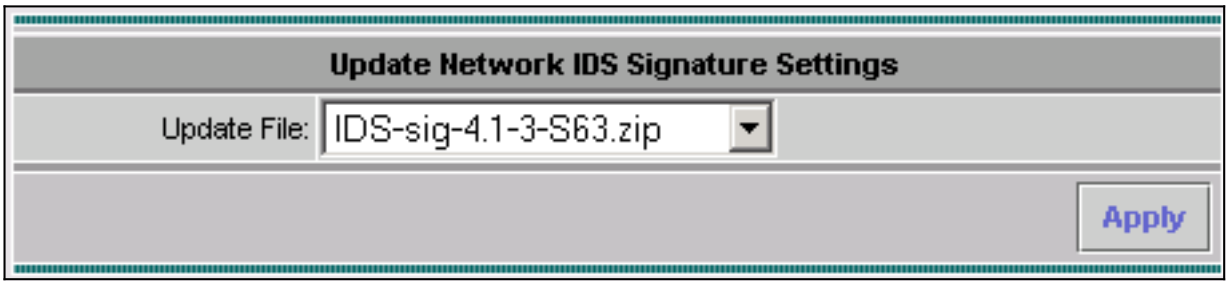
6. Vous pouvez maintenant voir que votre capteur a été importé avec
succès



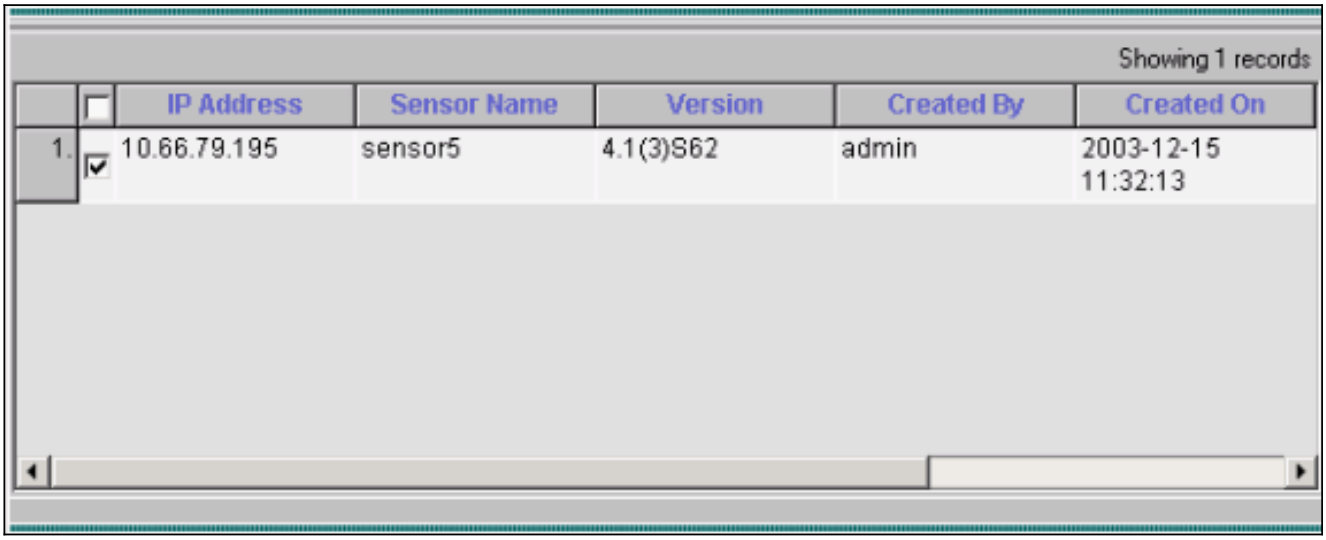
Utiliser IDS MC pour les mises à jour des signatures

Cette procédure explique comment utiliser IDS MC pour les mises à jour de signatures.

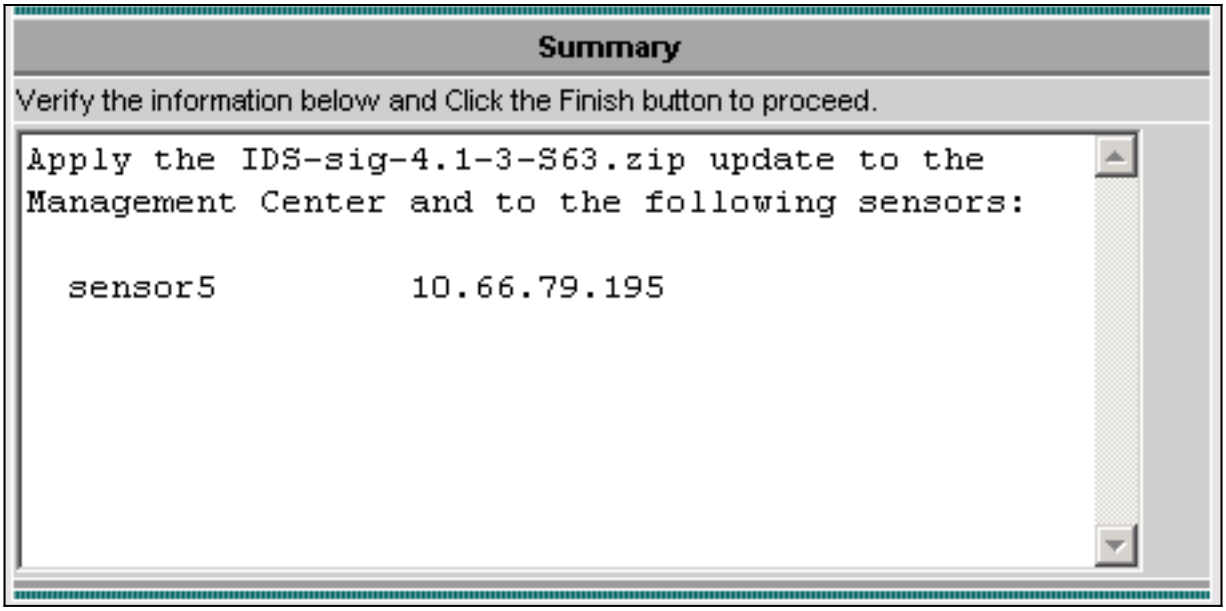
1. Téléchargez les mises à jour des signatures IDS du réseau (clients enregistrés uniquement) et enregistrez-les dans le répertoire **C:\PROGRA~1\CSCOpx\MDC\etc\ids\updates** de votre serveur VMS.
2. Sur la console du serveur VMS, sélectionnez **VPN/Security Management Solution > Management Center > IDS Sensors**.
3. Sélectionnez l'onglet Configuration et cliquez sur **Mises à jour**.
4. Cliquez sur **Mettre à jour les signatures IDS du réseau**.
5. Sélectionnez la signature à mettre à niveau dans le menu déroulant et cliquez sur **Appliquer** pour
   continuer.



6. Sélectionnez le ou les capteurs à mettre à jour et cliquez sur **Suivant** pour
   continuer.



7. Après avoir été invité à appliquer la mise à jour à Management Center, ainsi qu'au capteur, cliquez sur **Terminer** pour
   continuer.



8. Établissez une connexion Telnet ou console dans l'interface de ligne de commande du capteur. Vous voyez des informations similaires à celles-ci :

```
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.
```

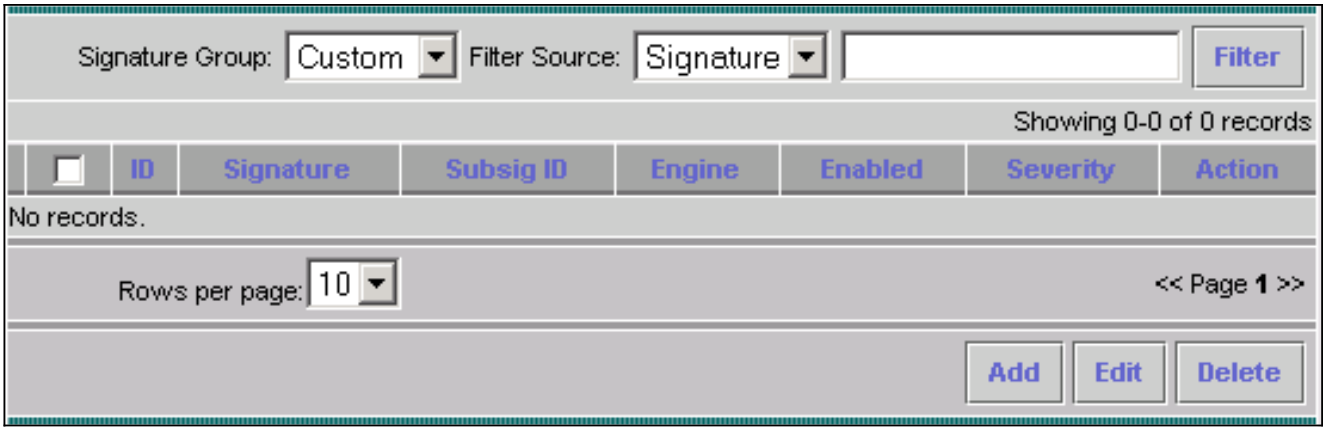
9. Attendez quelques minutes pour permettre la mise à niveau, puis entrez **show version** afin de vérifier.

```
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
```

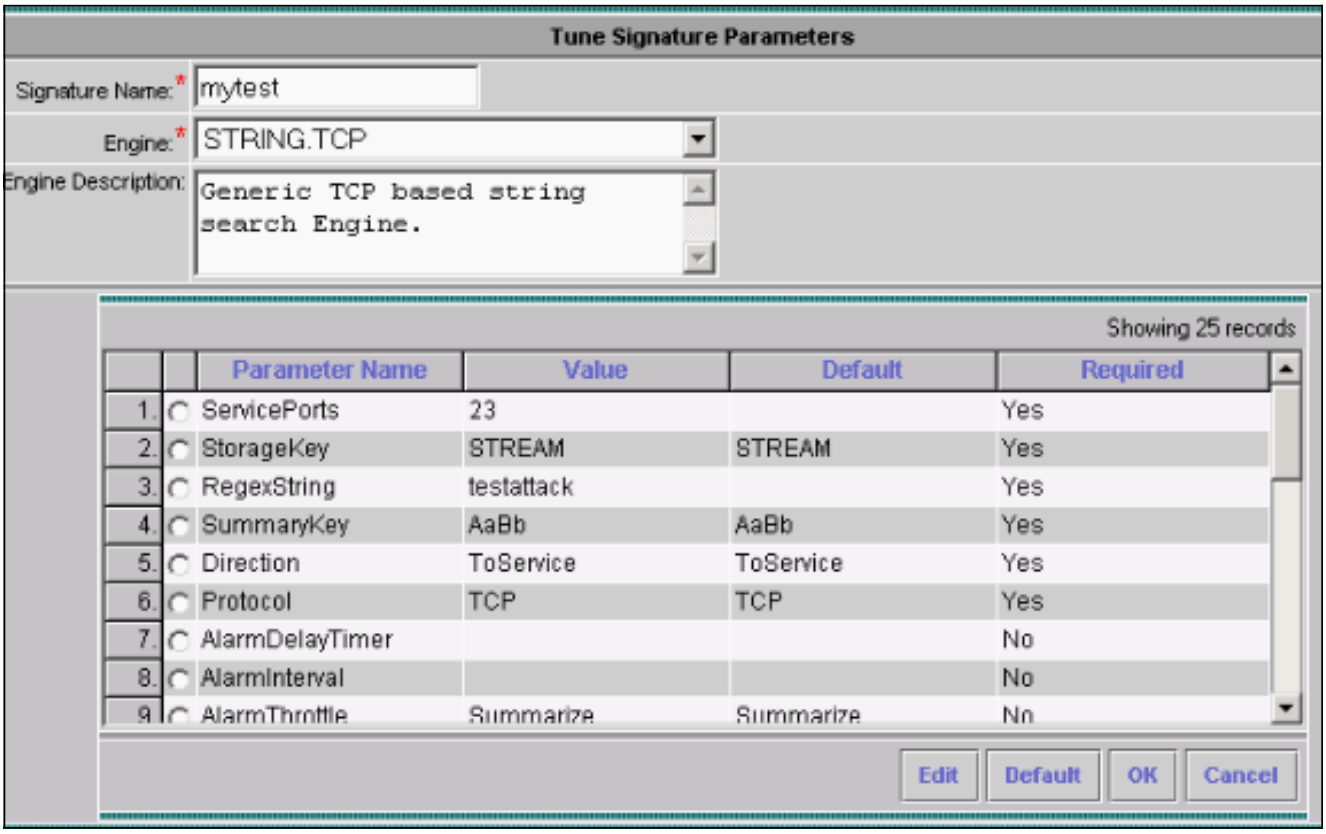
Configuration de la réinitialisation TCP pour le routeur IOS

Complétez ces étapes afin de configurer la réinitialisation TCP pour le routeur IOS.

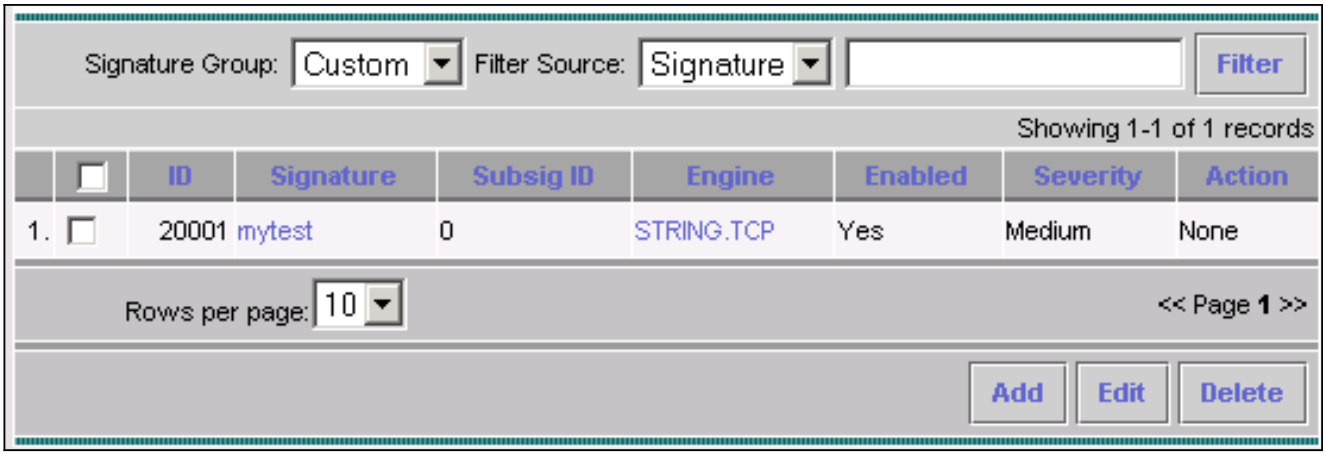
1. Choisissez **VPN/Security Management Solution > Management Center > IDS Sensors**.
2. Sélectionnez l'onglet Configuration, sélectionnez votre capteur dans le sélecteur d'objets, puis cliquez sur **Paramètres**.
3. Sélectionnez **Signatures**, cliquez sur **Personnalisé**, puis cliquez sur **Ajouter** afin d'ajouter une nouvelle
signature.



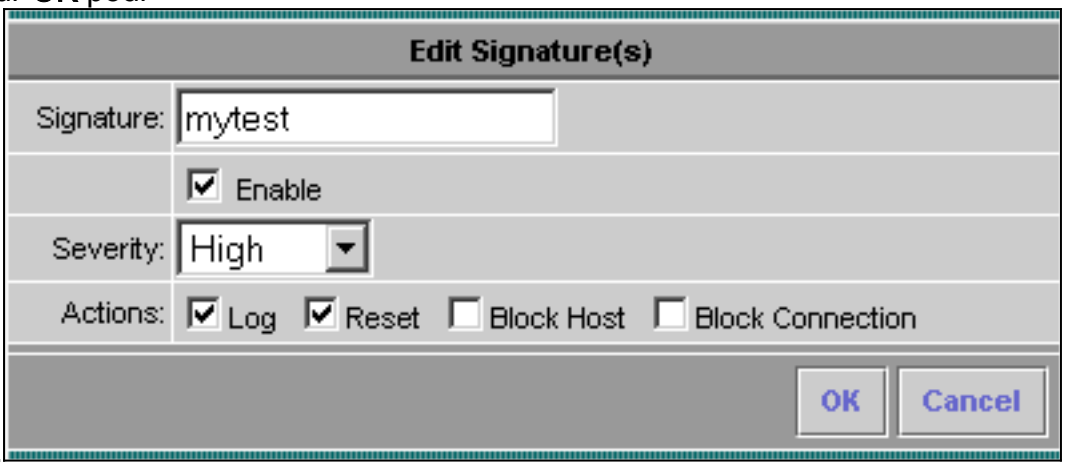
4. Entrez le nouveau nom de signature, puis sélectionnez le moteur (dans ce cas, **STRING.TCP**).
5. Cochez la case d'option appropriée afin de personnaliser les paramètres disponibles, puis cliquez sur **Modifier**.Dans cet exemple, le paramètre ServicePorts est modifié pour modifier sa valeur à **23** (pour le port 23). Le paramètre RegexString est également modifié pour ajouter la valeur **testattack**. Une fois cette opération terminée, cliquez sur **OK** pour continuer.



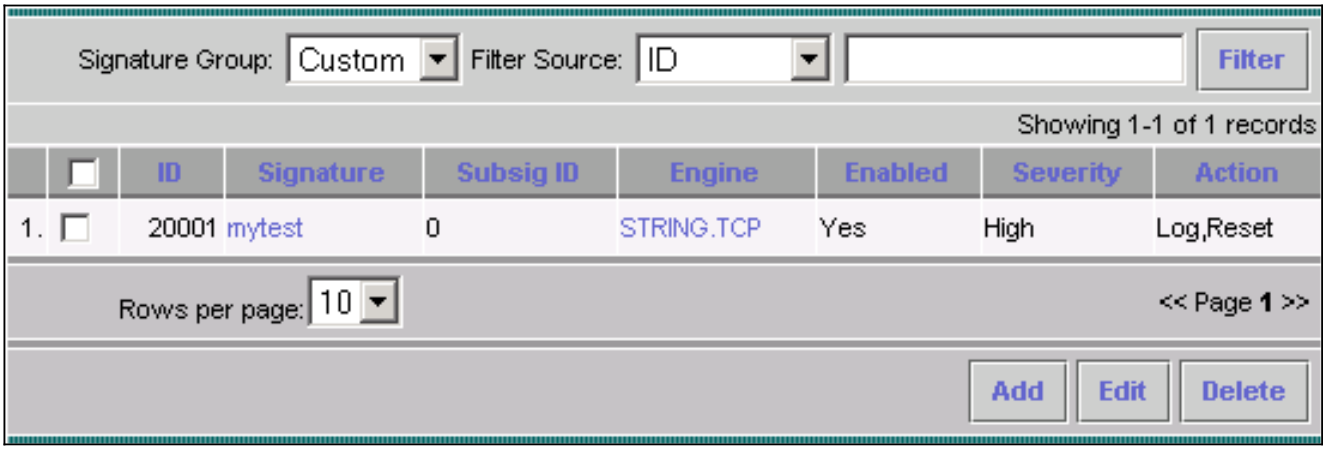
6. Cliquez sur le nom de la signature afin de modifier la gravité et les actions de la signature ou pour activer/désactiver la
signature.



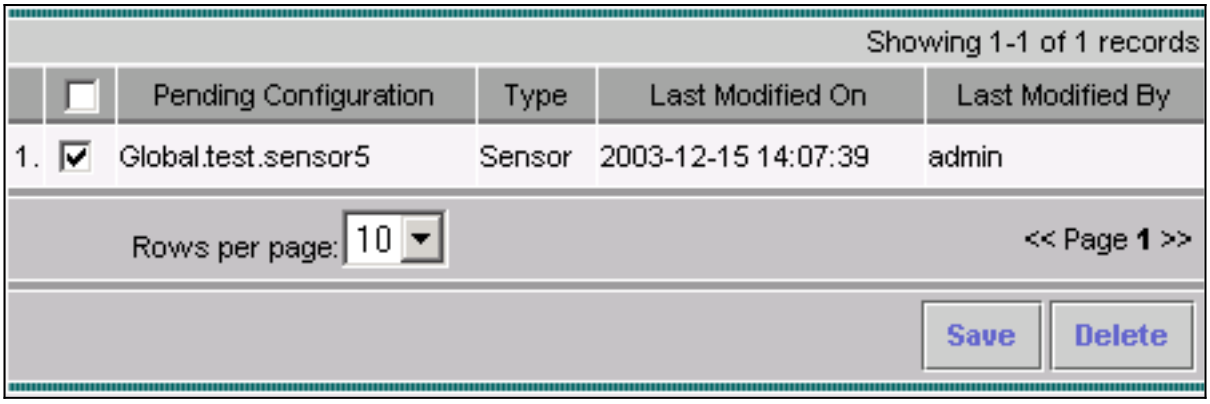
7. Dans ce cas, la gravité passe à **Élevé** et l'action **Journal & Réinitialisation** est choisie. Cliquez sur **OK** pour continuer.



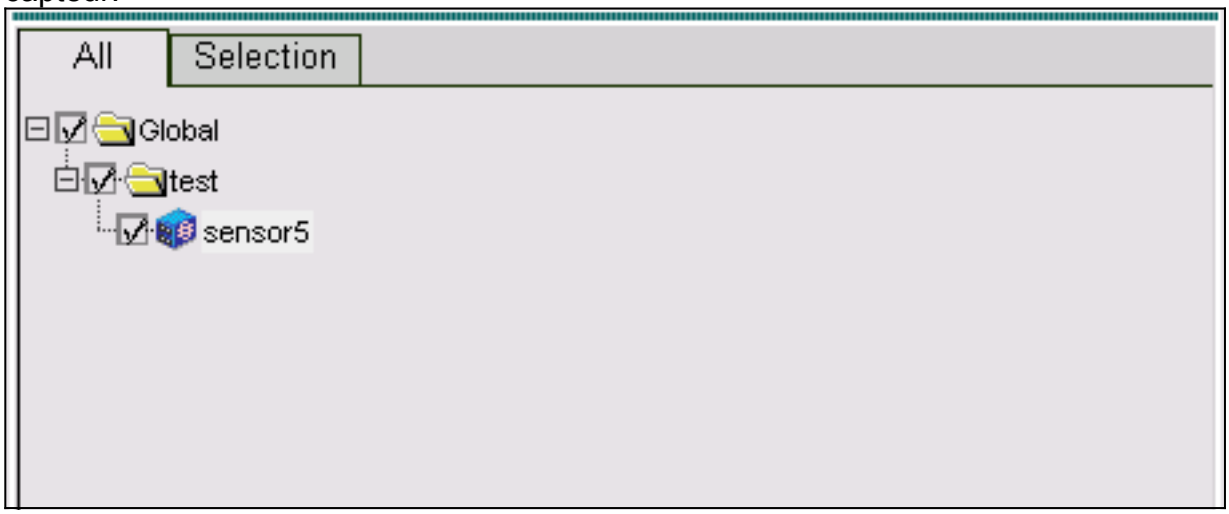
8. La signature complète ressemble à ceci :



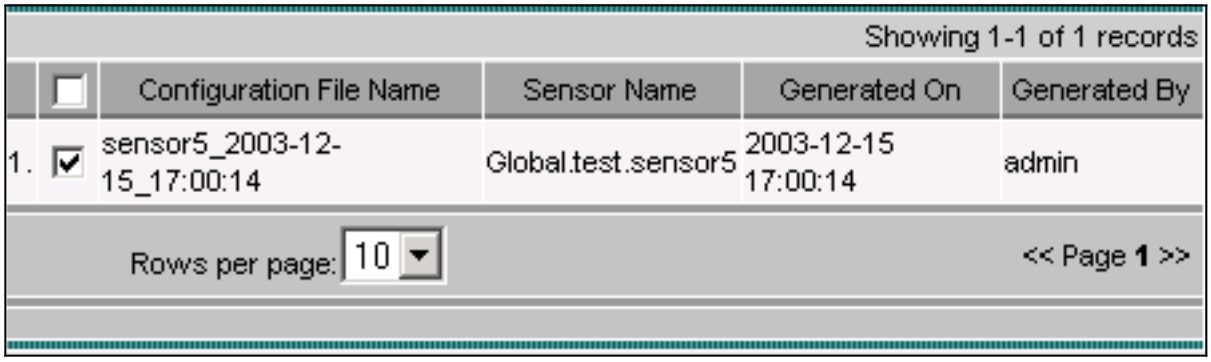
9. Choisissez **Configuration > En attente**, vérifiez la configuration en attente pour vous assurer qu'elle est correcte, puis cliquez sur **Enregistrer**.



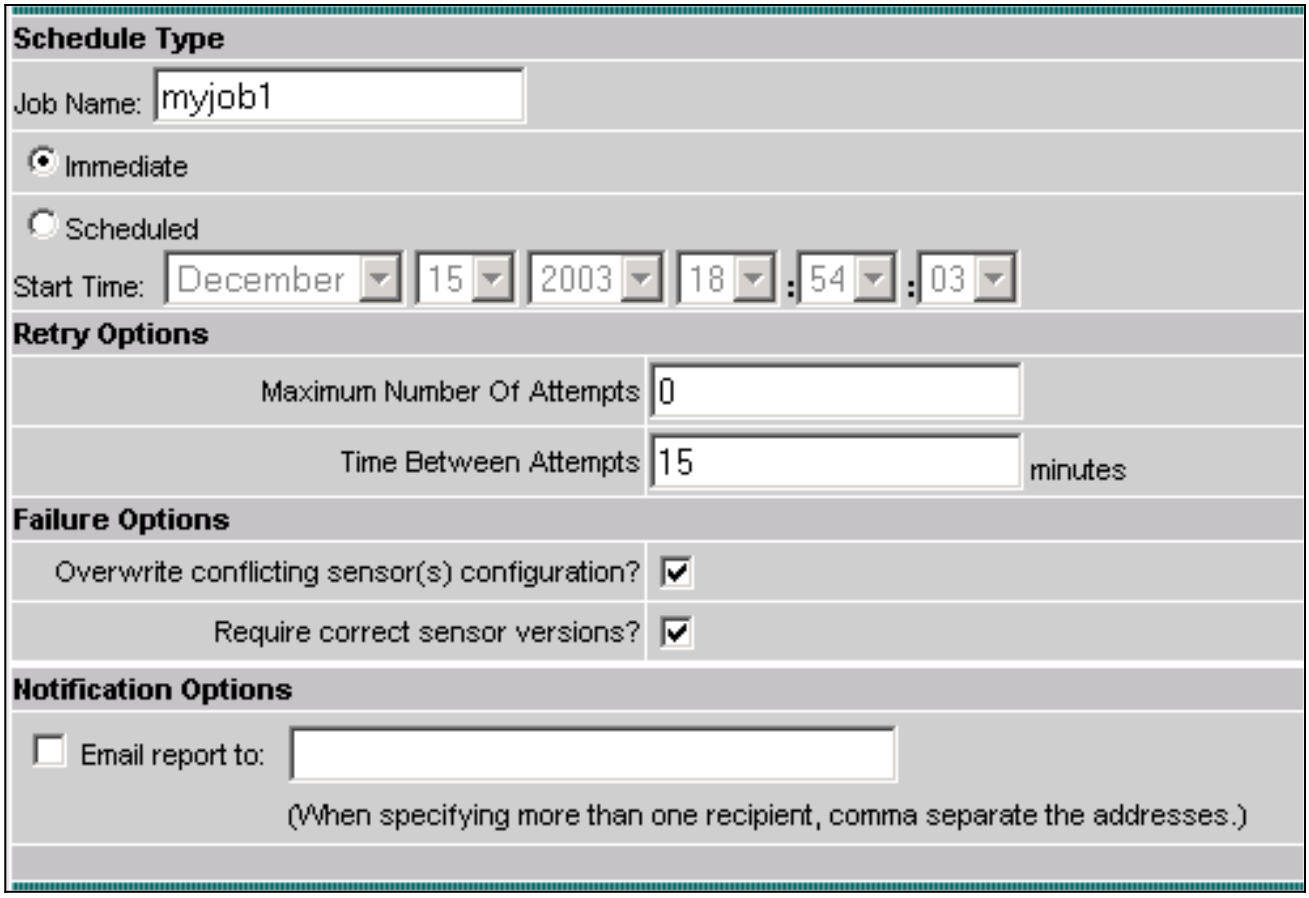
10. Choisissez **Deployment > Generate**, puis cliquez sur **Apply** afin de transmettre les modifications de configuration au capteur.



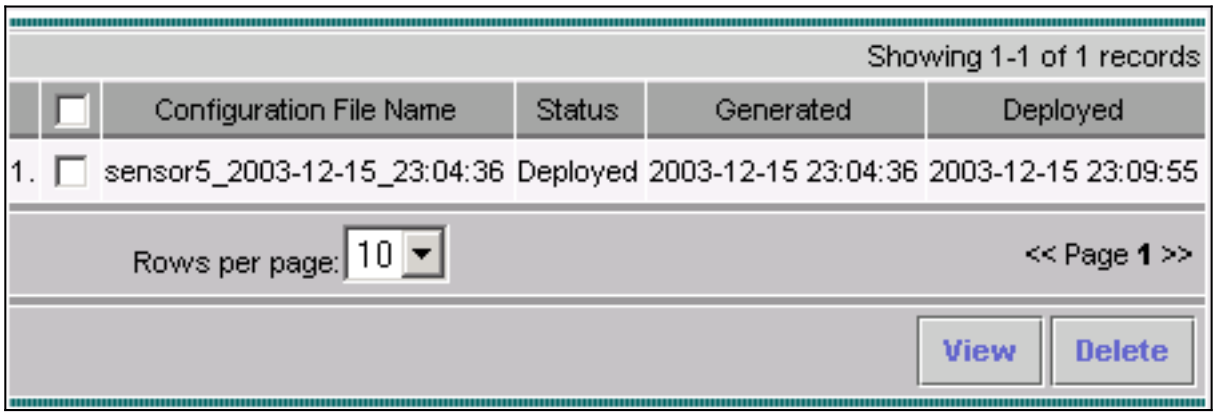
11. Choisissez **Deployment > Deploy** et cliquez sur **Submit**.
12. Cochez la case en regard de votre capteur et cliquez sur **Déployer**.
13. Cochez la case du travail dans la file d'attente et cliquez sur **Suivant** pour continuer.



14. Entrez le nom du travail et planifiez le travail comme **Immédiat**, puis cliquez sur **Terminer**.



15. Choisissez **Déploiement > Déploiement > En attente**.Patientez quelques minutes jusqu'à ce que tous les travaux en attente soient terminés. La file d'attente doit alors être vide.
16. Choisissez **Configuration > History** afin de confirmer le déploiement.Assurez-vous que l'état de la configuration est affiché en tant que **Déployé**. Cela signifie que la configuration du capteur est mise à jour avec
succès.



Vérification

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

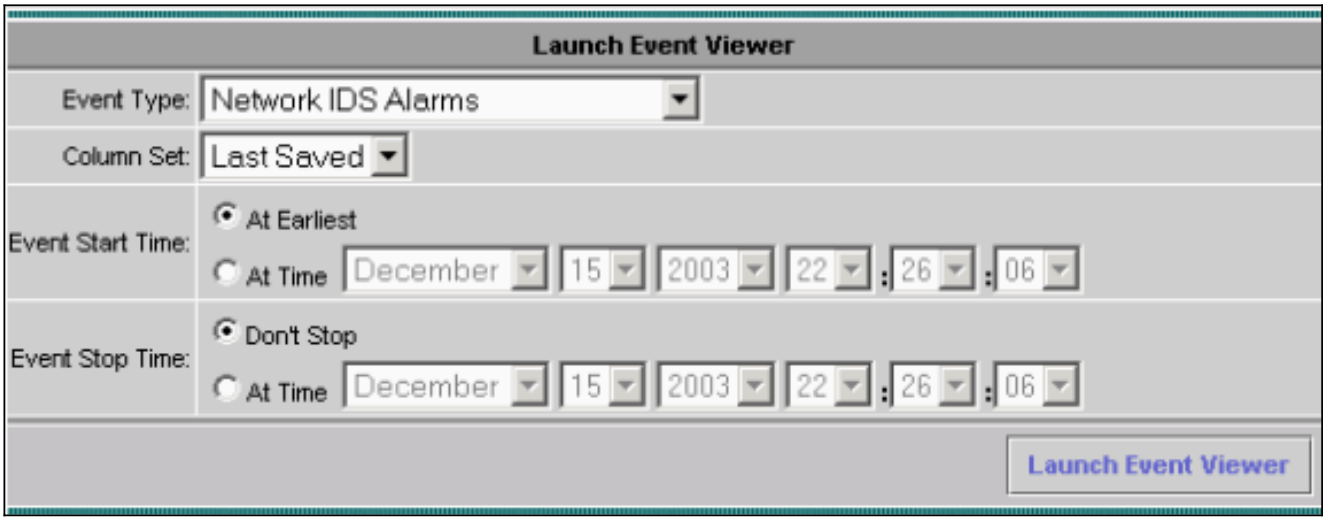
Lancer l'attaque et réinitialiser TCP

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

1. Avant de lancer l'attaque, sélectionnez **VPN/Security Management Solution > Monitoring**

Center > Security Monitor.

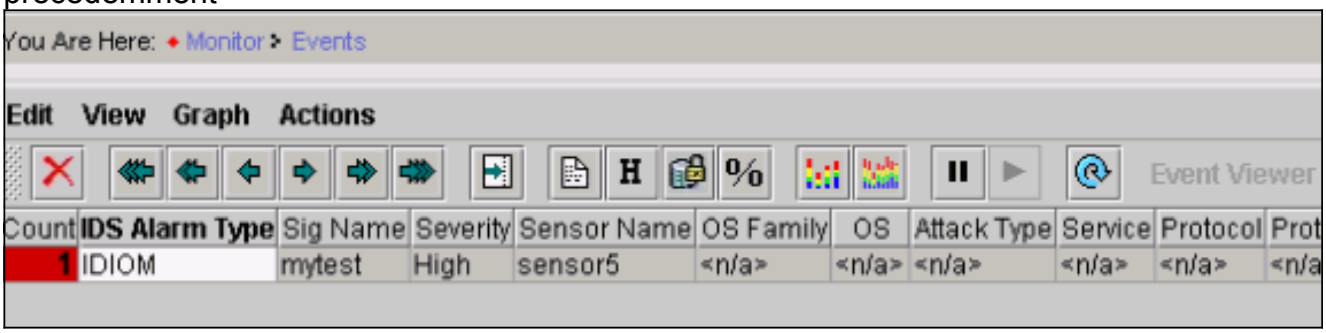
2. Choisissez **Monitor** dans le menu principal et cliquez sur **Events**.
3. Cliquez sur **Lancer l'Observateur d'événements**.



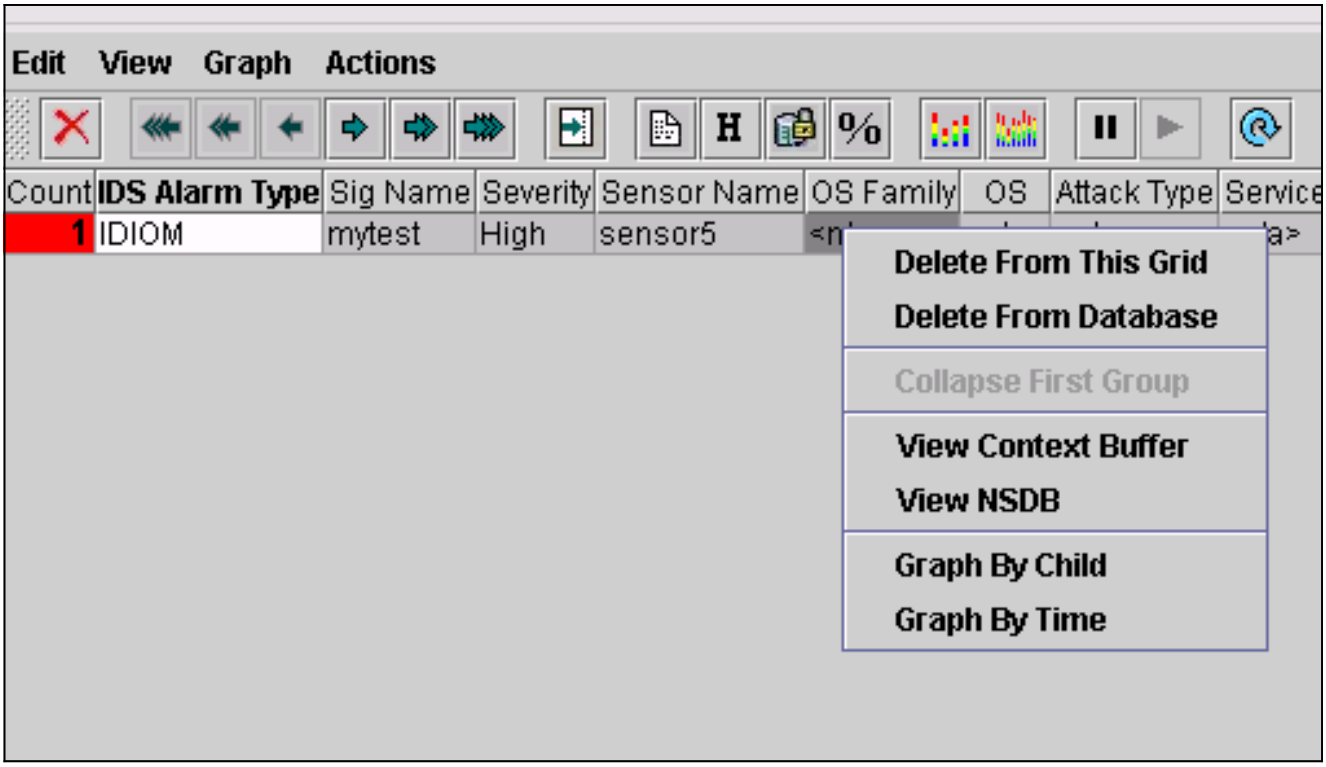
4. Établissez une connexion Telnet d'un routeur à l'autre et tapez **testattack** afin de lancer l'attaque.Dans ce cas, nous avons établi une connexion Telnet entre le voyant du routeur et la maison du routeur. Dès que vous appuyez sur **<space>** ou **<enter>**, après avoir tapé **testattack**, votre session Telnet doit être réinitialisée.

```
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. Dans l'Observateur d'événements, cliquez sur **Base de données de requête** pour les nouveaux événements maintenant.Vous voyez l'alerte de l'attaque lancée précédemment



6. Dans l'Observateur d'événements, mettez l'alarme en surbrillance, cliquez dessus avec le bouton droit et sélectionnez **Afficher le tampon de contexte** ou **Afficher NSDB** pour afficher des informations plus détaillées sur l'alarme.



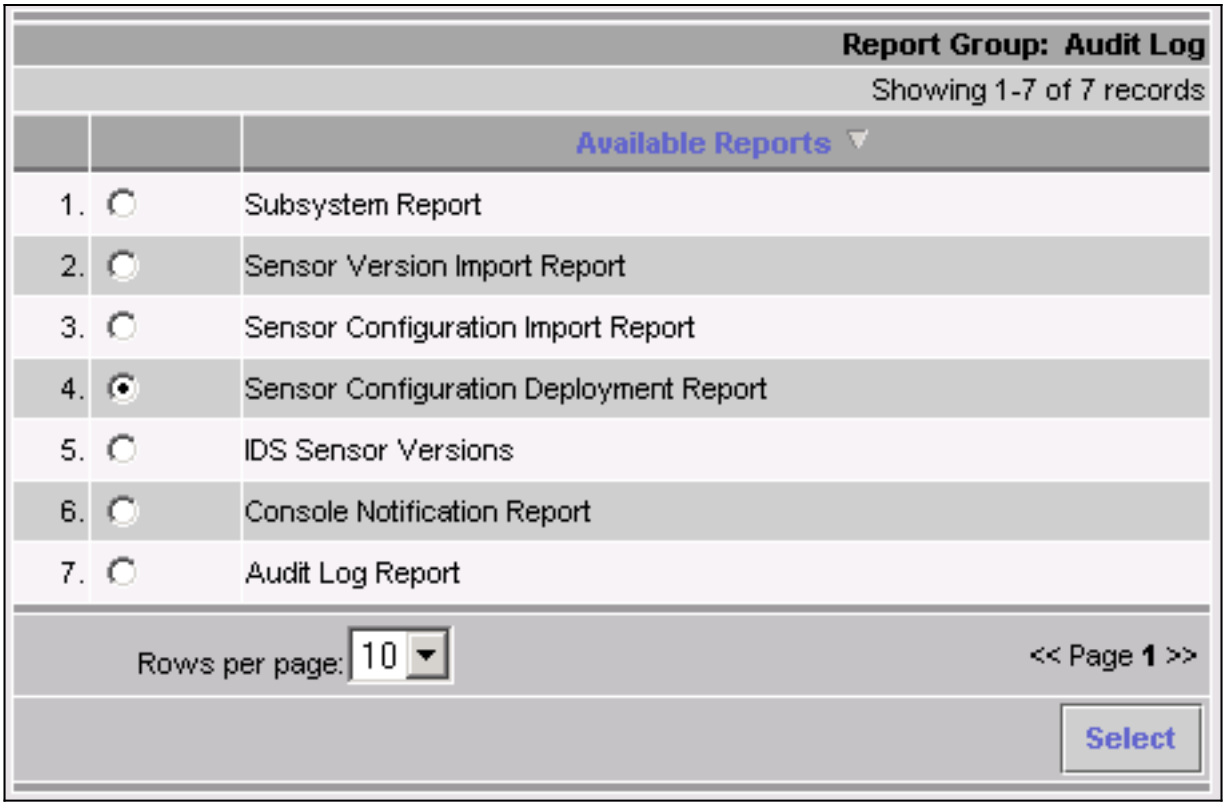
Dépannage

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

Procédure de dépannage

Effectuez ces étapes afin de procéder au dépannage .

1. Dans IDS MC, sélectionnez **Rapports > Générer**.Selon le type de problème, des détails supplémentaires doivent être trouvés dans l'un des sept rapports disponibles.



2. Tandis que Blocking utilise le port Command and Control pour configurer les listes d'accès du routeur, les réinitialisations TCP sont envoyées à partir de l'interface de reniflage du capteur. Assurez-vous que vous avez fractionné le port correct à l'aide de la commande **set span** sur le commutateur, comme suit :

```
set span
```

```
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 TCP Reset ne fonctionne pas, connectez-vous au capteur et entrez la commande **show event**.Lancez l'attaque et vérifiez si l'alarme est déclenchée ou non. Si l'alarme est déclenchée, vérifiez qu'elle est définie pour le type d'action **TCP reset**.

Informations connexes

- Page d'assistance Cisco Secure Intrusion Detection
- Documentation pour Cisco Secure Intrusion Detection System
- Page d'assistance de CiscoWorks VPN/Security Management Solution

- Support et documentation techniques - Cisco Systems