Configuration du blocage IDS avec VMS IDS MC

Contenu

Introduction

Ce 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, le blocage du capteur IDS vers un routeur Cisco est configuré.

Conditions préalables

Conditions requises

Avant de configurer le blocage, assurez-vous que vous avez rempli ces conditions.

- 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 dans ce document sont basées sur les versions de logiciel et matériel suivantes :

- VMS 2.2 avec IDS MC et Security Monitor 1.2.3
- Capteur Cisco IDS 4.1.3S(63)
- Routeur Cisco exécutant 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 des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

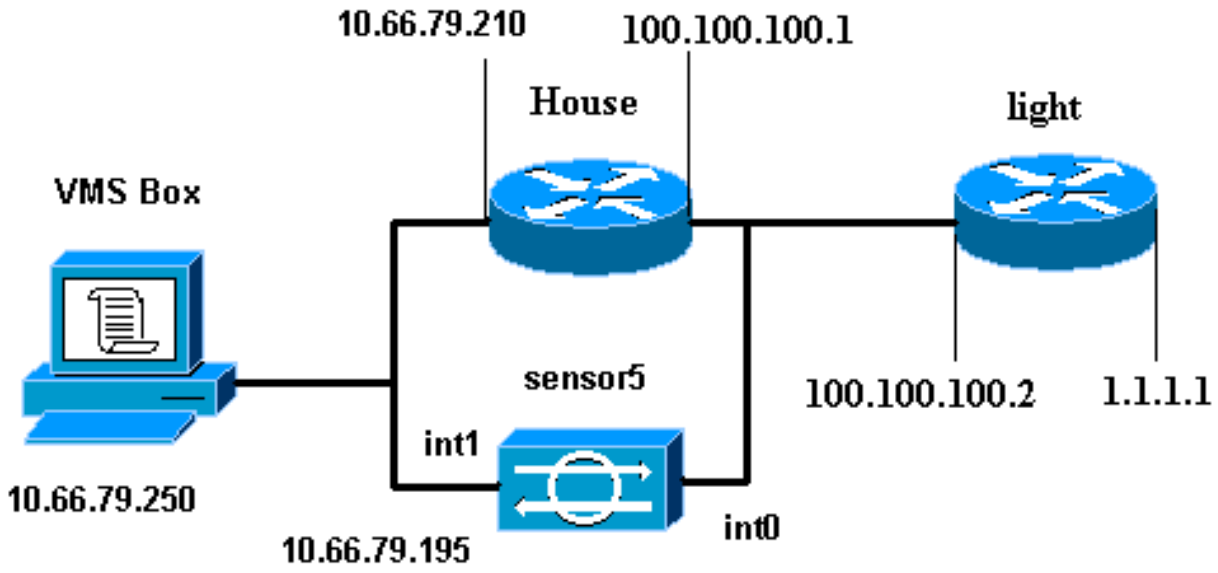
Configuration

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

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez l'outil de recherche de commandes (clients inscrits seulement).

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant.



Configurations

Ce document utilise les configurations indiquées ici.

- 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
!--- After Blocking is configured, the IDS Sensor !---
adds this access-group ip access-group.
IDS_Ethernet1_in_0 in
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
!
!--- After Blocking is configured, the IDS Sensor !---
adds this access list. ip access-list extended
IDS_Ethernet1_in_0.
 permit ip host 10.66.79.195 any
 permit ip any any
!
line con 0
 stopbits 1
line vty 0 4
 password cisco
 login
!
scheduler max-task-time 5000
end
```

Configuration initiale du capteur

Effectuez ces étapes pour configurer initialement le capteur.

Remarque : Si vous avez effectué la configuration initiale de votre capteur, passez à la section Importation du capteur dans IDS MC.

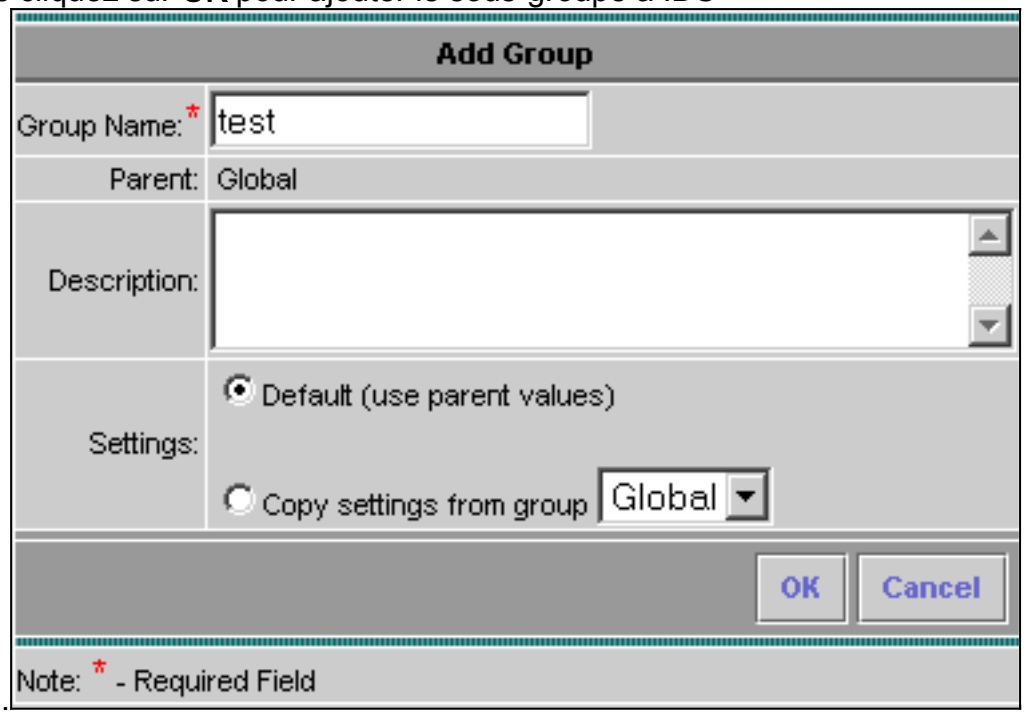
1. Console dans le capteur.Vous êtes invité à saisir un nom d'utilisateur et un mot de passe. Si c'est la première fois que vous vous connectez au capteur, vous devez vous connecter avec le nom d'utilisateur **cisco** et le mot de passe **cisco**.
2. Vous êtes invité à modifier le mot de passe, puis 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
```
4. Appuyez sur **2** afin d'enregistrer votre configuration.

Importer le capteur dans IDS MC

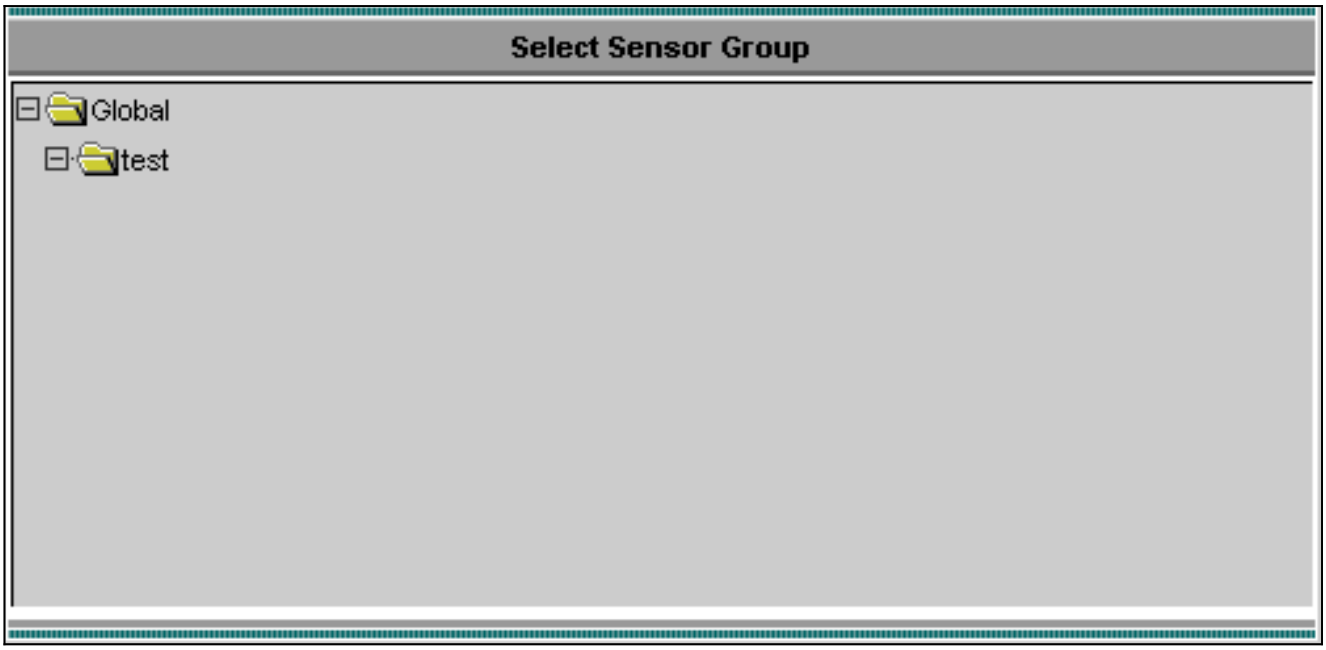
Suivez ces étapes pour importer le capteur dans IDS MC.

1. Accédez à votre capteur.Dans ce cas, accédez à **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 **admin** et le mot de passe **cisco** ont été utilisés.
3. Sélectionnez **VPN/Security Management Solution > Management Center** et choisissez **IDS Sensors**.
4. Cliquez sur l'onglet Périphériques, sélectionnez **Groupe de capteurs**, mettez en surbrillance **Global**, puis cliquez sur **Créer un sous-groupe**.

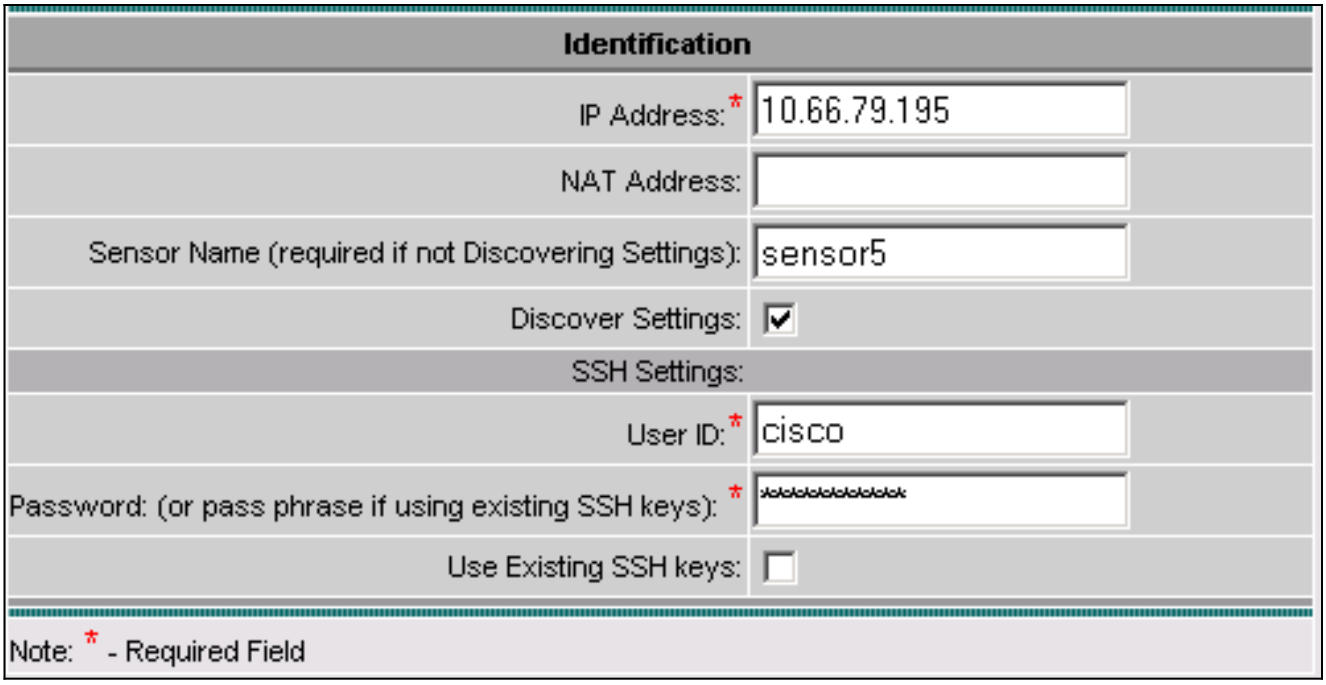
5. Entrez le nom du groupe et assurez-vous que le bouton radio **Par défaut** est sélectionné, puis cliquez sur **OK** pour ajouter le sous-groupe à IDS MC.



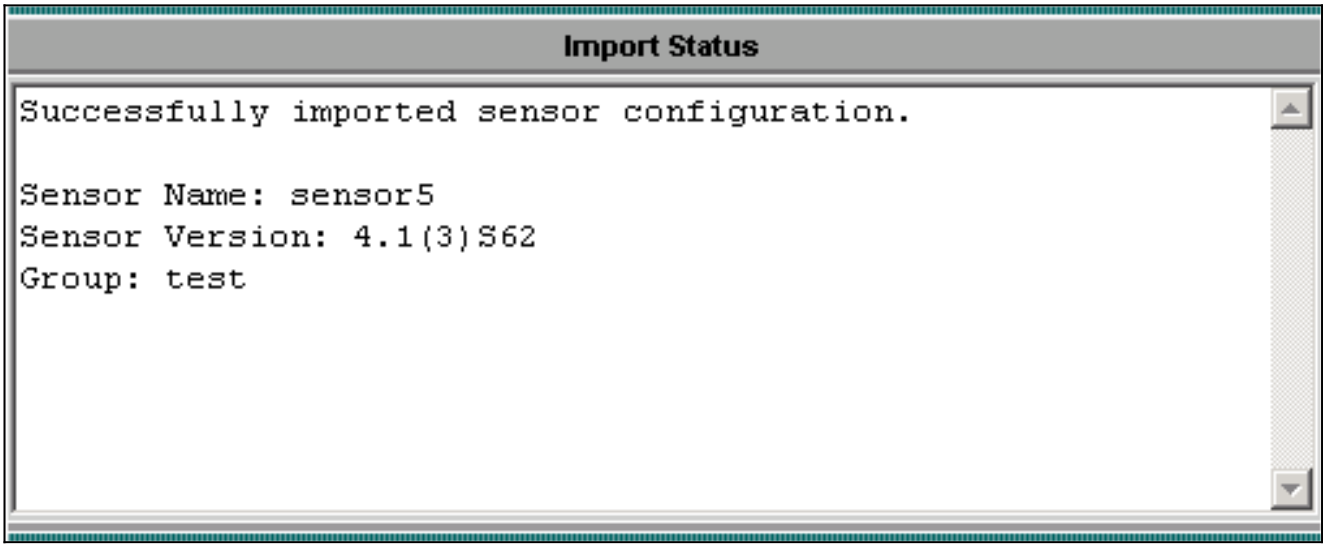
6. Sélectionnez **Devices** > **Sensor**, mettez en surbrillance le sous-groupe créé à l'étape précédente (dans ce cas, **test**), puis cliquez sur **Add**.
7. Mettez le sous-groupe en surbrillance, puis cliquez sur **Suivant**.



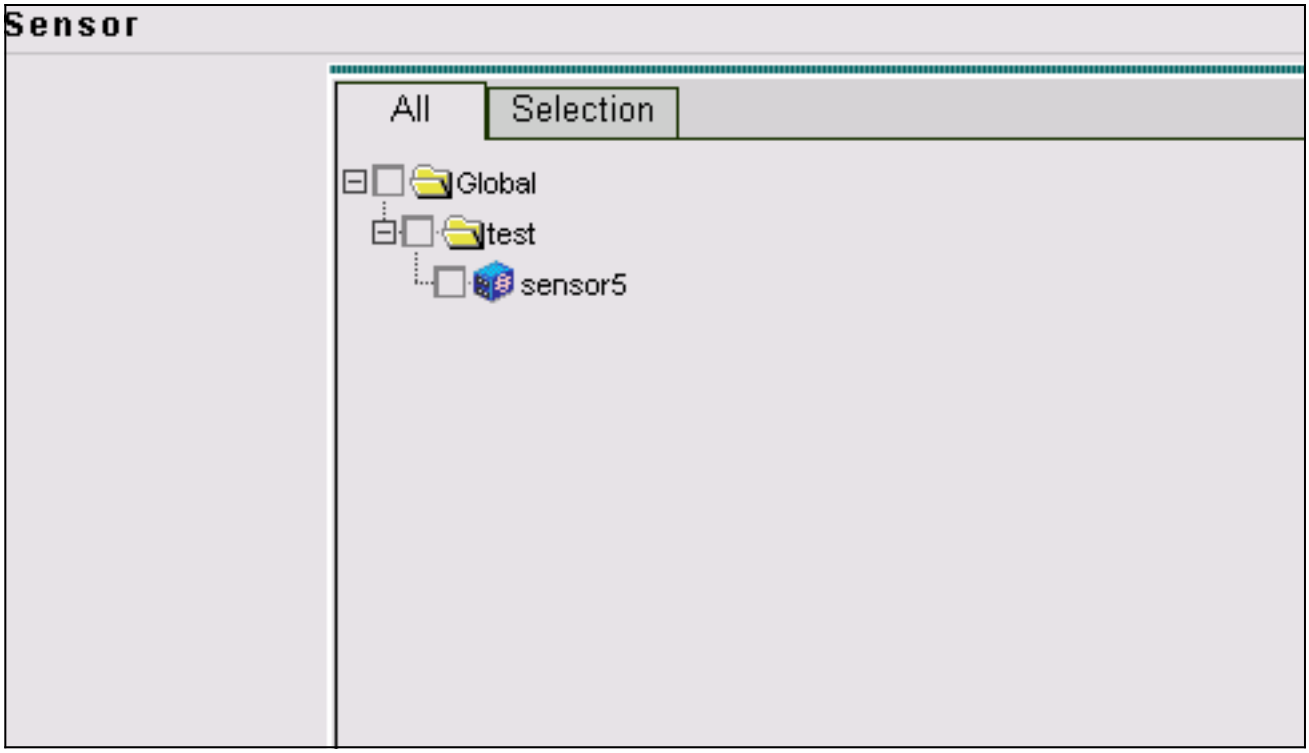
8. Entrez les détails conformément à cet exemple, puis cliquez sur **Suivant** pour continuer.



9. Après avoir reçu un message indiquant la `configuration du capteur correctement importée`, cliquez sur **Terminer** pour continuer.



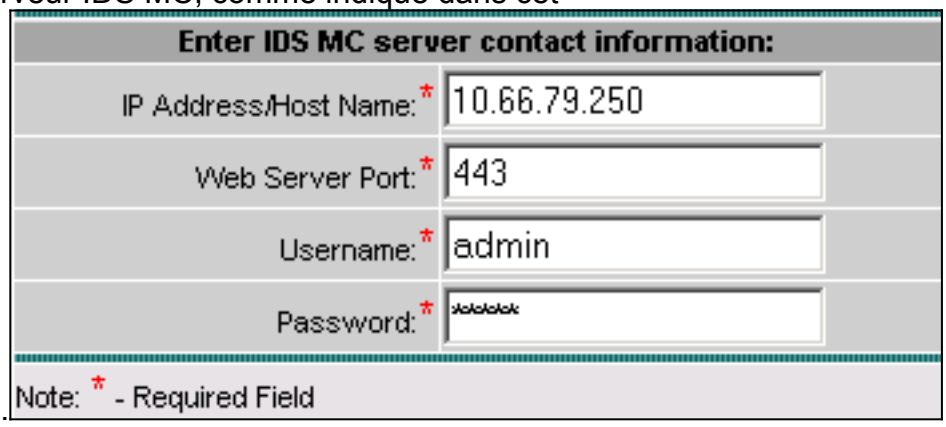
10. Votre capteur est importé dans la MC IDS. Dans ce cas, le capteur5 est importé.



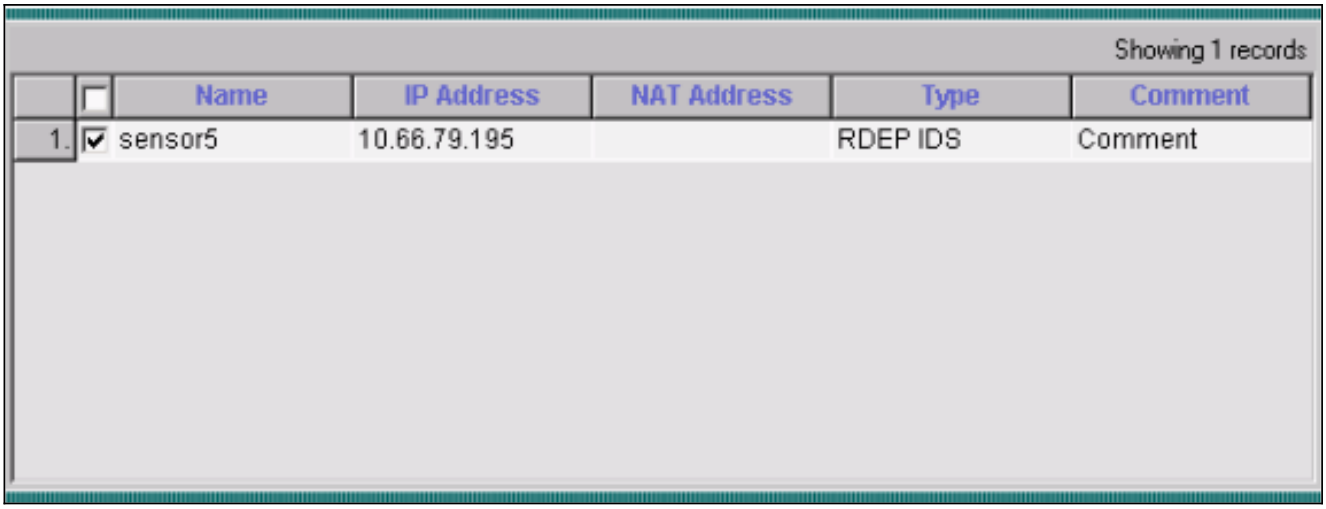
Importer le capteur dans Security Monitor

Suivez cette procédure pour importer le capteur dans le moniteur de sécurité.

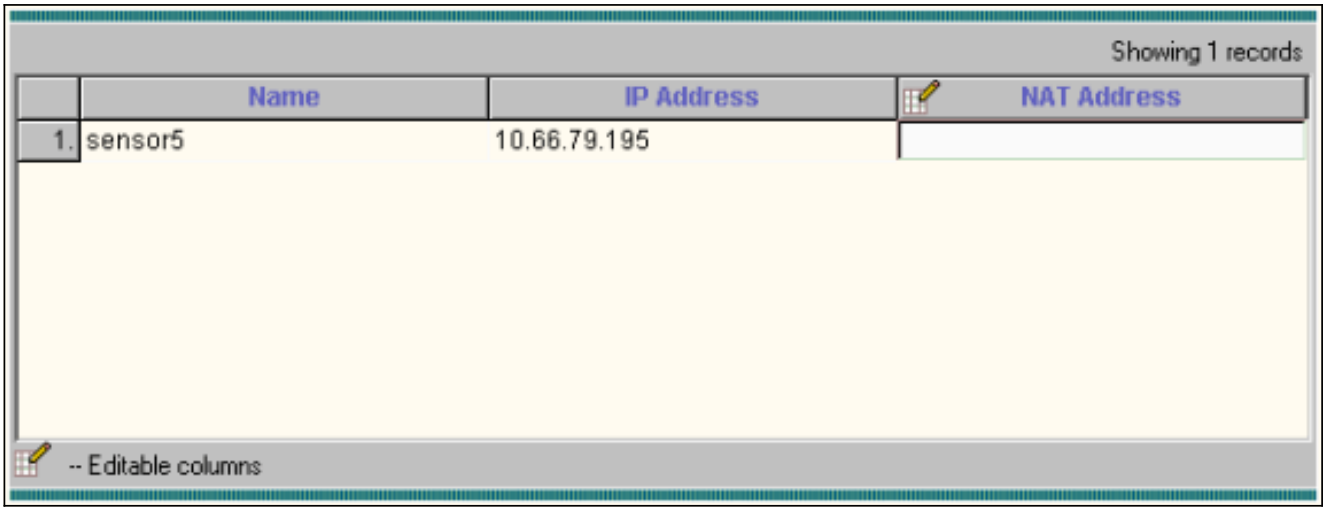
1. Dans le menu Serveur VMS, sélectionnez **VPN/Security Management Solution > Monitoring Center > Security Monitor**.
2. Sélectionnez l'onglet Périphériques, puis cliquez sur **Importer** et saisissez les informations sur le serveur IDS MC, comme indiqué dans cet exemple.



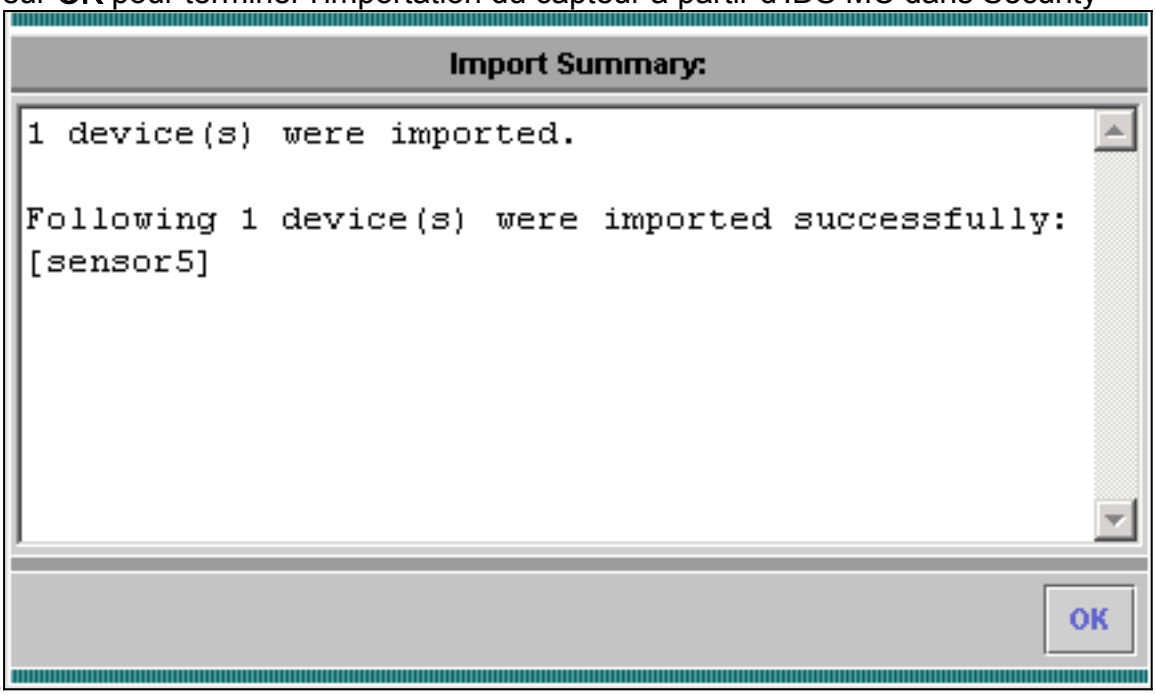
3. Sélectionnez votre capteur (dans ce cas, **capteur5**) et cliquez sur **Suivant** pour continuer.



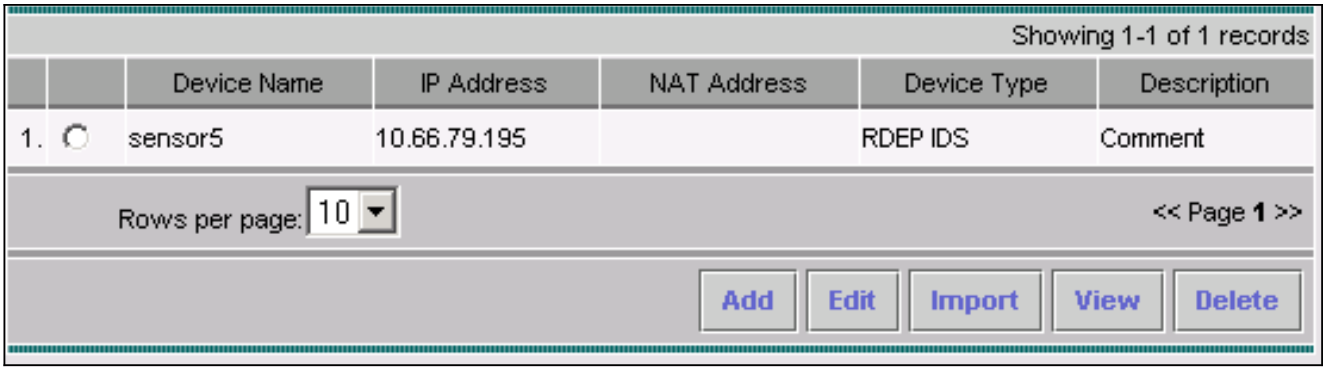
4. Si nécessaire, mettez à jour l'adresse NAT (Network Address Translation) de votre capteur, puis cliquez sur **Terminer** pour continuer.



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



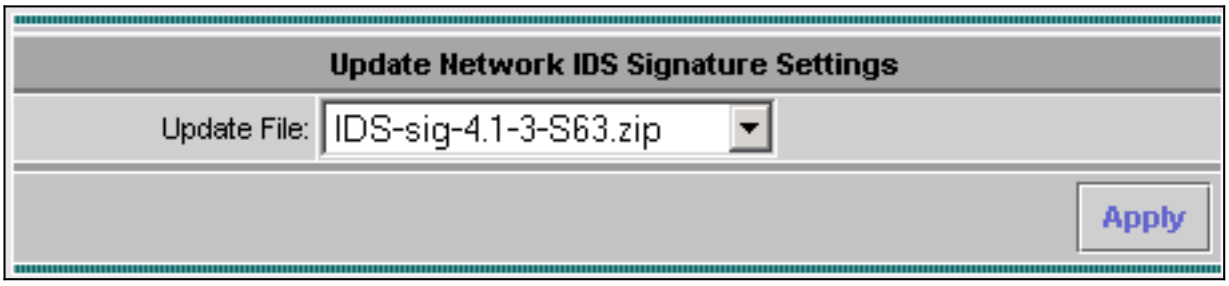
6. Votre capteur a été importé.



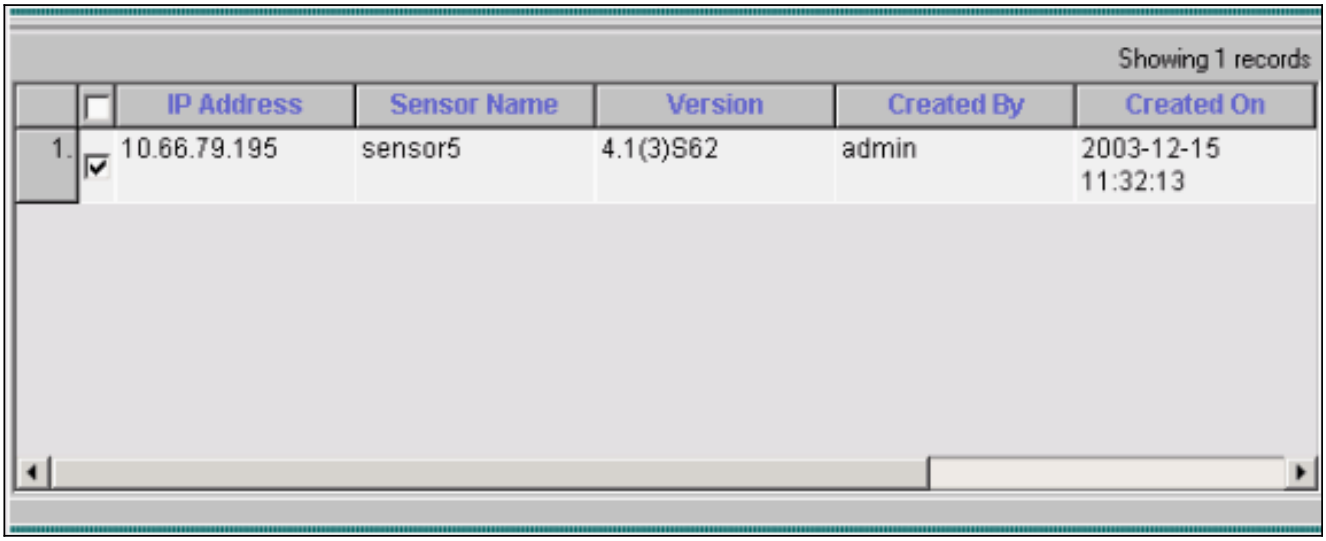
Utiliser IDS MC pour les mises à jour des signatures

Suivez cette procédure pour utiliser IDS MC pour les mises à jour de signature.

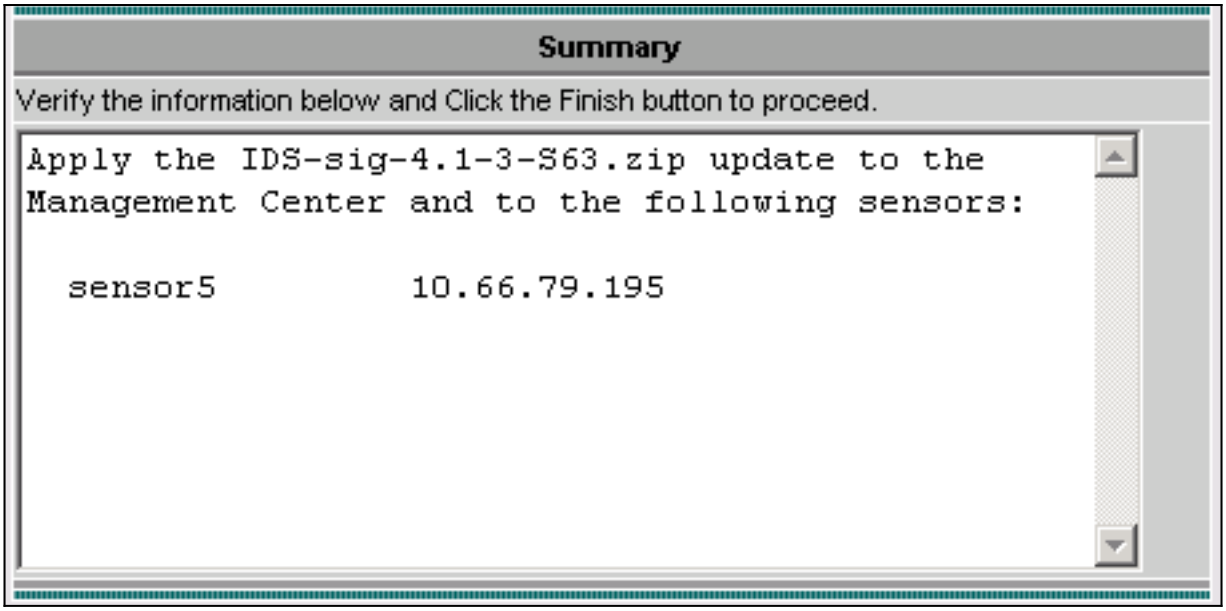
1. Téléchargez les mises à jour des signatures IDS du réseau (clients enregistrés uniquement) à partir des téléchargements et enregistrez-les dans C:\PROGRA~1\CSCOpx\MDC\etc\ids\updates\ directory on your VMS server.
2. Sur la console du serveur VMS, sélectionnez **VPN/Security Management Solution > Management Center > Sensors**.
3. Cliquez sur l'onglet Configuration, sélectionnez **Updates**, puis cliquez sur **Update Network IDS Signatures**.
4. Sélectionnez la signature à mettre à niveau dans le menu déroulant et cliquez sur **Appliquer** pour
continuer.



5. Sélectionnez le ou les capteurs à mettre à jour, puis cliquez sur **Suivant** pour
continuer.



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



7. Établissez une connexion Telnet ou console dans l'interface de ligne de commande du capteur. Des informations similaires apparaissent :

```
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.
```

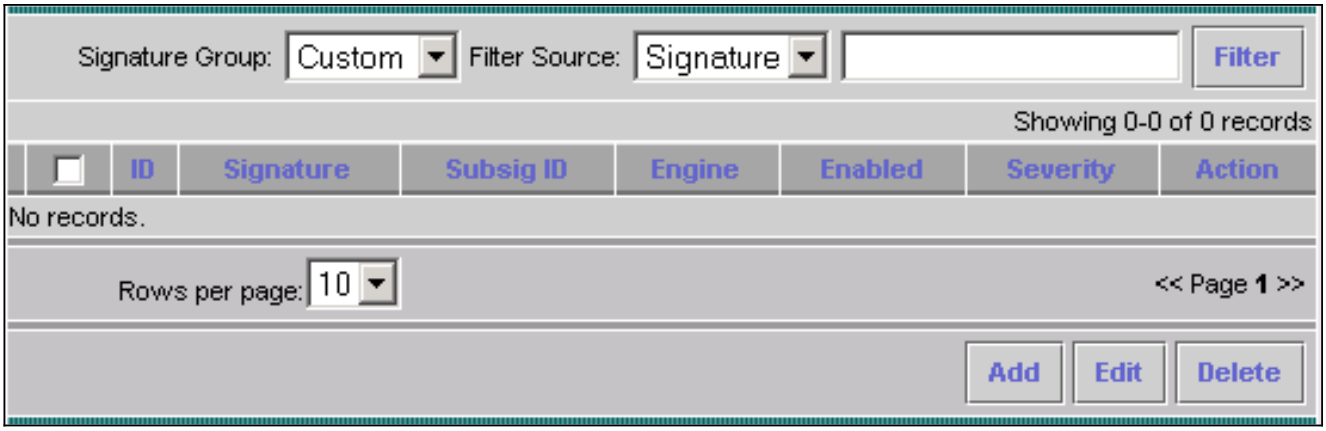
8. Attendez quelques minutes pour permettre la mise à niveau, puis entrez **show version** pour vérifier.

```
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
```

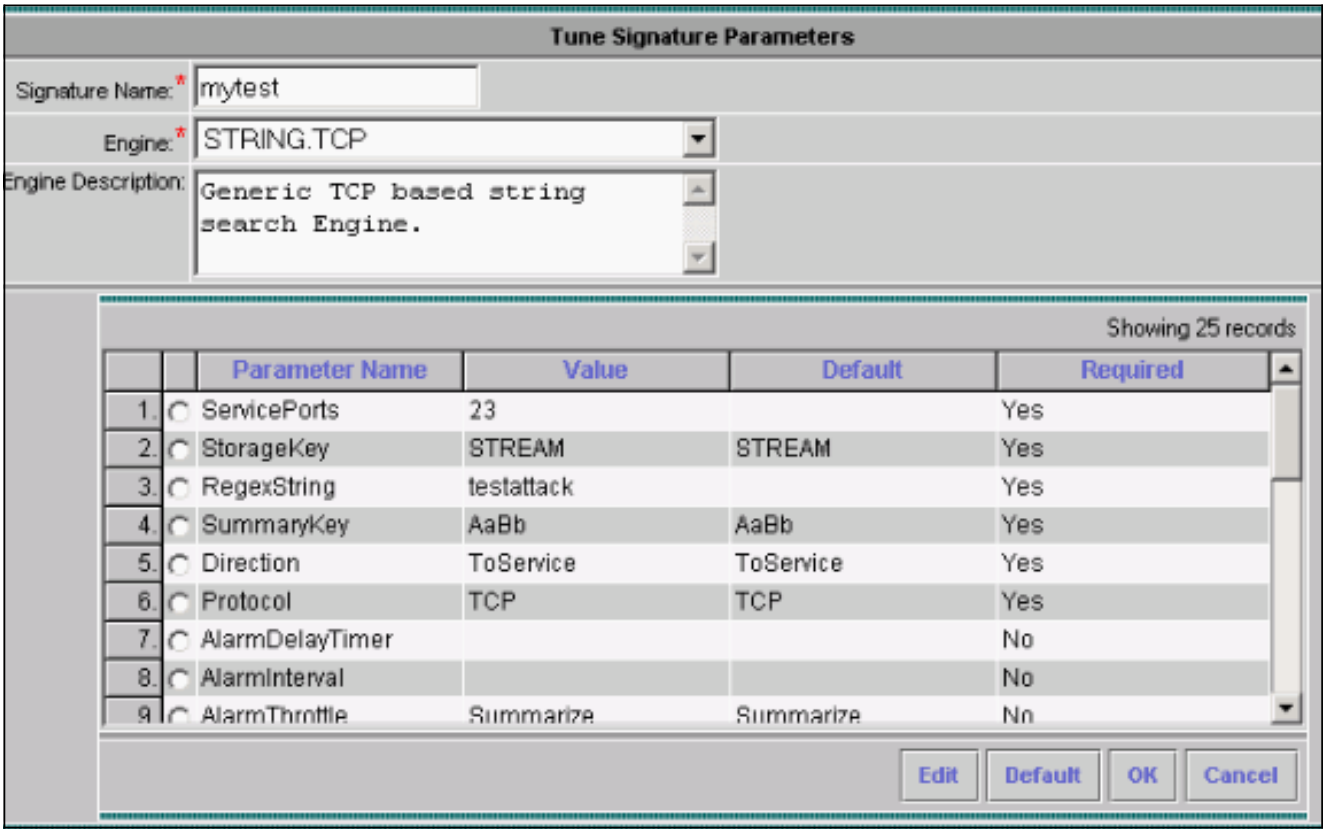
Configuration du blocage pour le routeur IOS

Exécutez cette procédure pour configurer le blocage pour le routeur IOS.

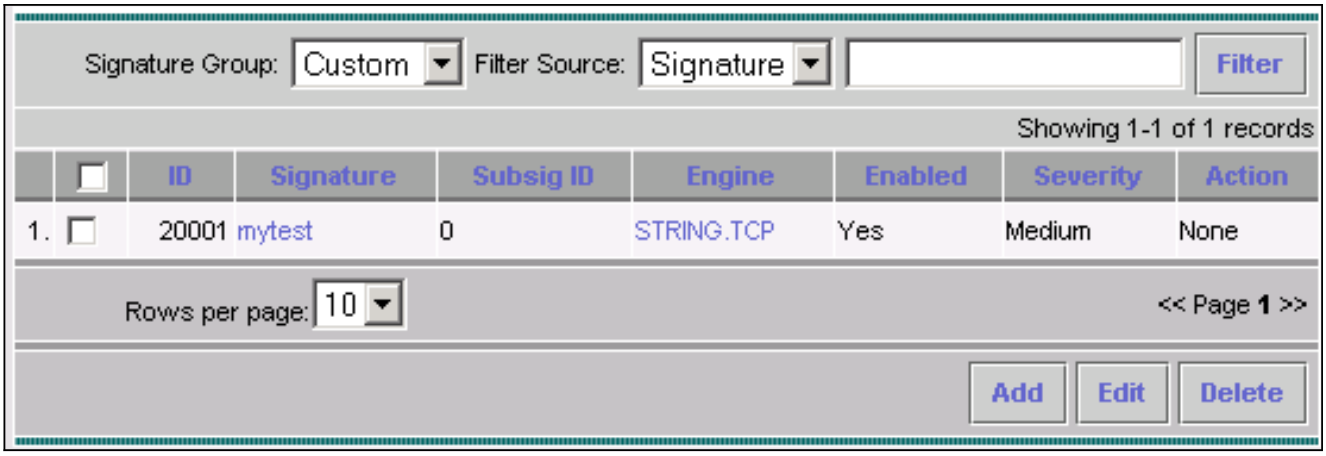
1. Sur la console du serveur VMS, sélectionnez **VPN/Security Management Solution > Management Center > IDS Sensors**.
2. Sélectionnez l'onglet Configuration, sélectionnez votre capteur dans le sélecteur d'objets, puis cliquez sur **Paramètres**.
3. Sélectionnez **Signatures**, cliquez sur **Personnalisé**,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



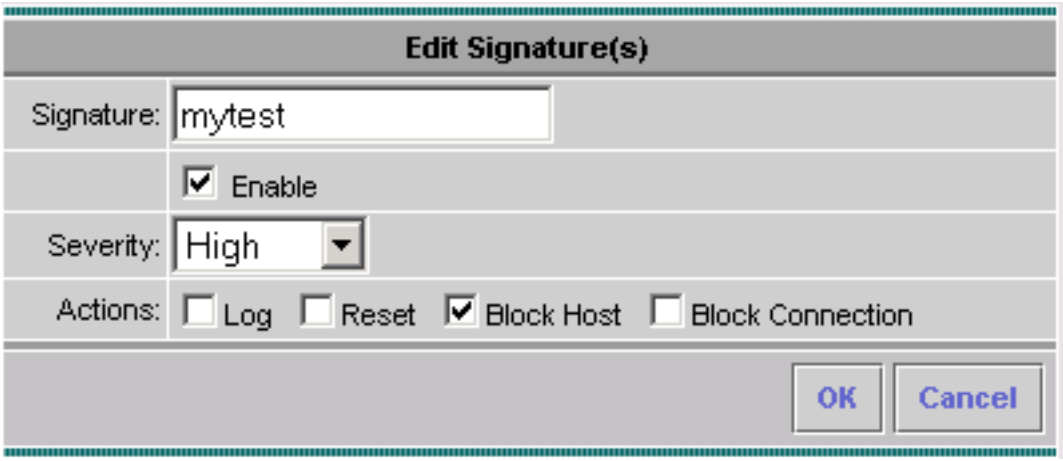
4. Entrez le nouveau nom de signature, puis sélectionnez le moteur (dans ce cas, **STRING.TCP**).
5. Vous pouvez personnaliser les paramètres disponibles en cochant la case d'option appropriée et en cliquant sur **Modifier**.Dans cet exemple, le paramètre ServicePorts est modifié pour modifier sa valeur 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. Pour modifier la gravité et les actions de la signature ou pour activer/désactiver la signature, cliquez sur le nom de la signature.

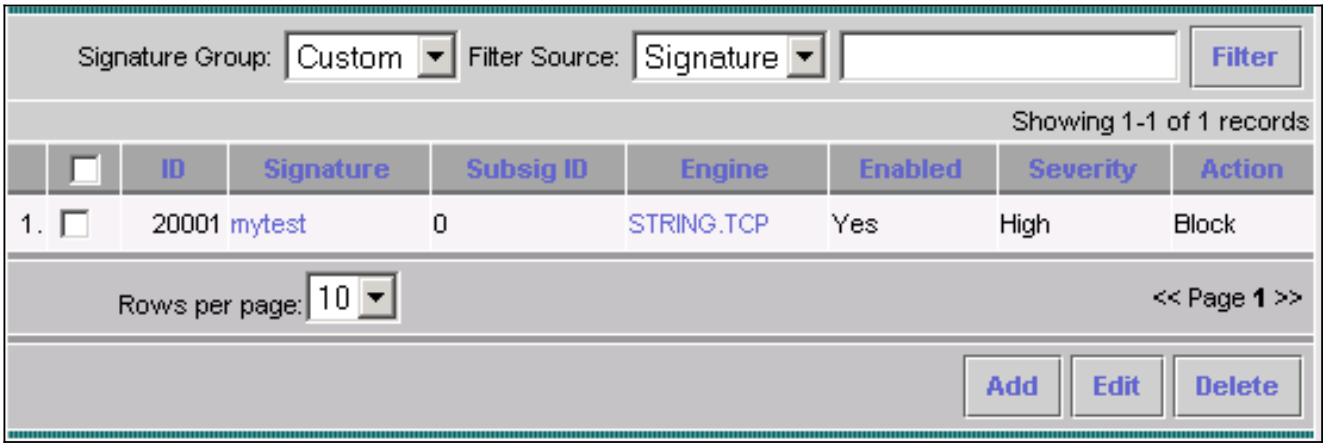


7. Dans ce cas, la gravité devient **Élevée** et l'action **Bloquer l'hôte** est sélectionnée. Cliquez sur **OK pour continuer.**L'hôte de bloc bloque l'attaque d'hôtes IP ou de sous-réseaux IP.Le blocage de la connexion bloque les ports TCP ou UDP (en fonction de l'attaque des connexions TCP ou

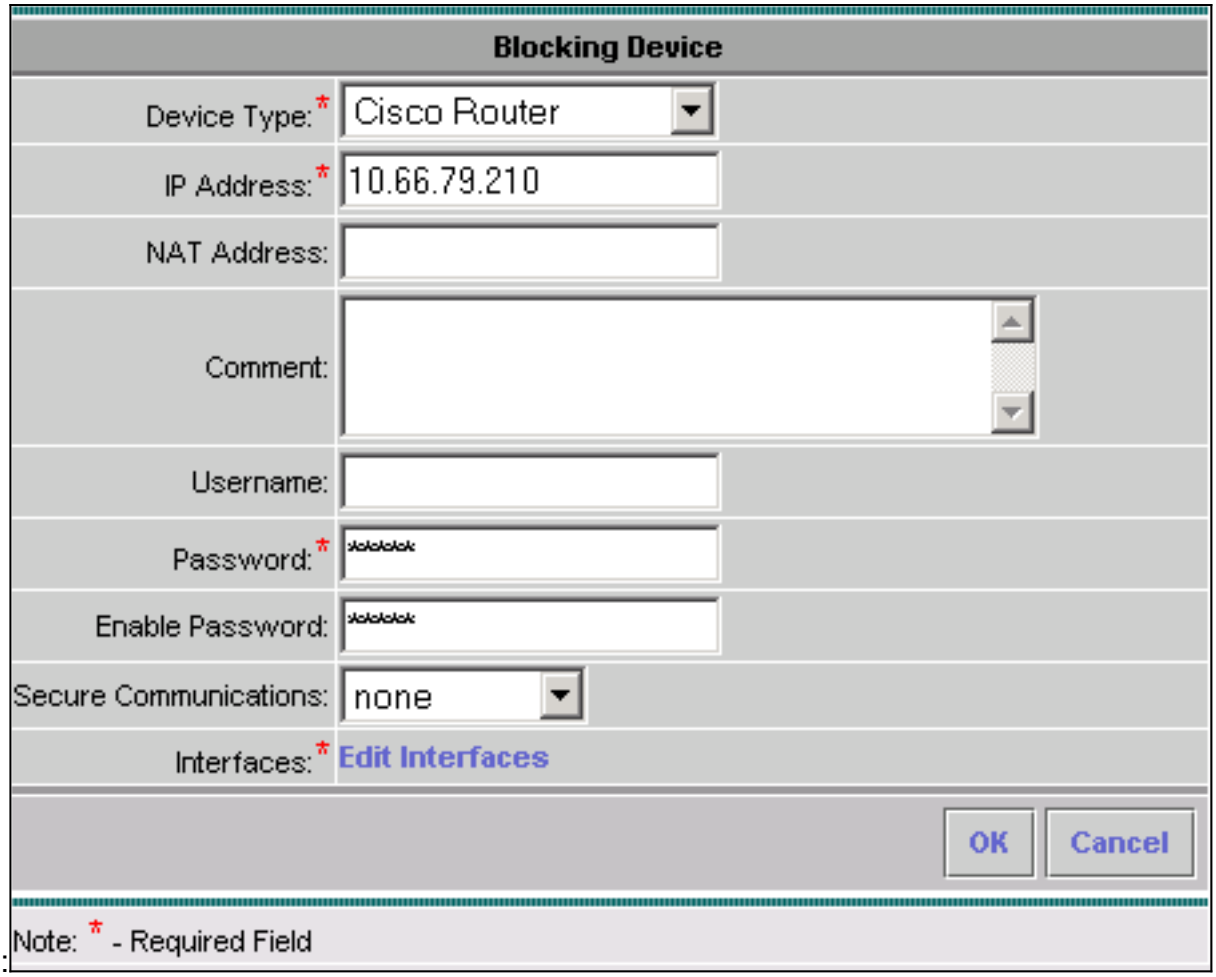


UDP).

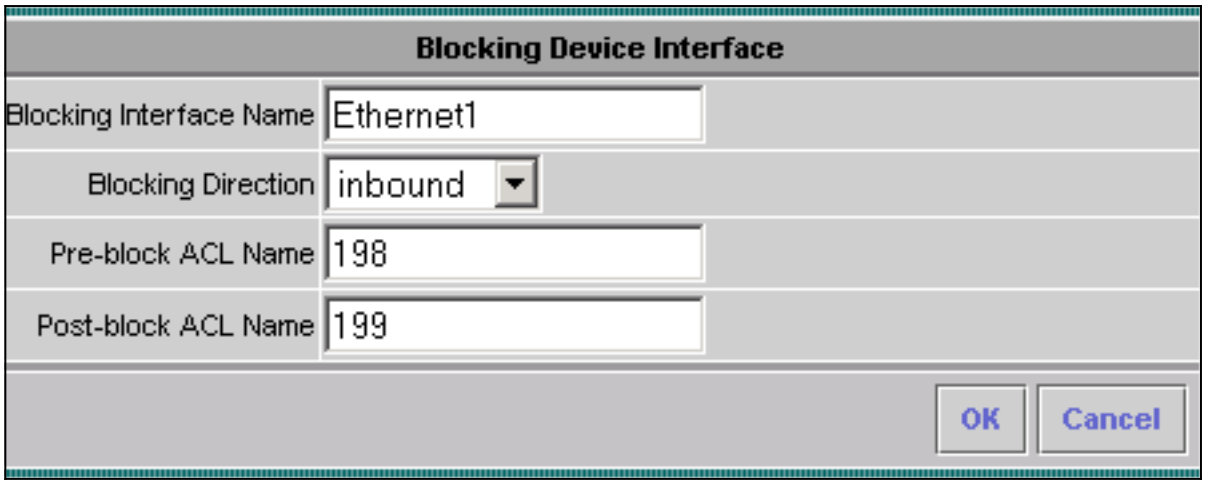
8. La signature complète ressemble à ceci :



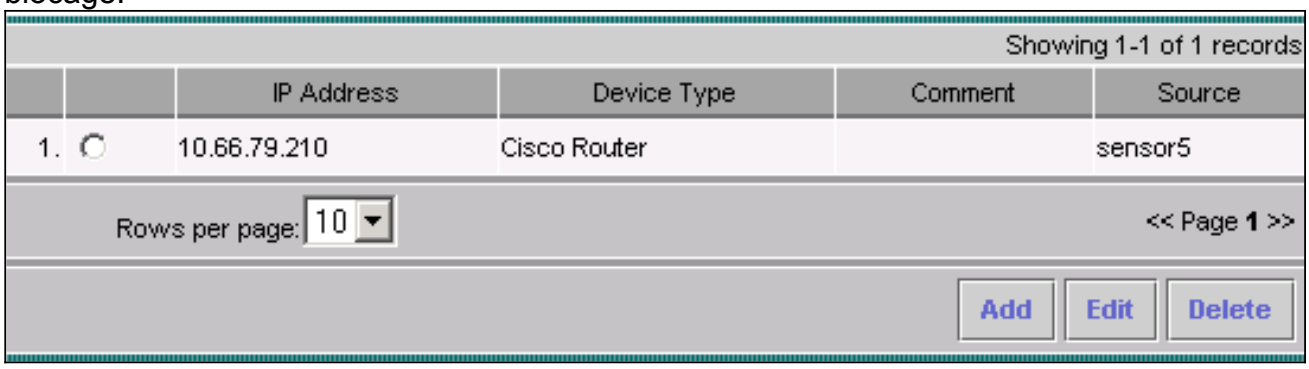
9. Afin de configurer le périphérique de blocage, sélectionnez **Blocage** > **Blocage** dans le sélecteur d'objets (menu à gauche de l'écran), puis cliquez sur **Ajouter** pour entrer les informations suivantes



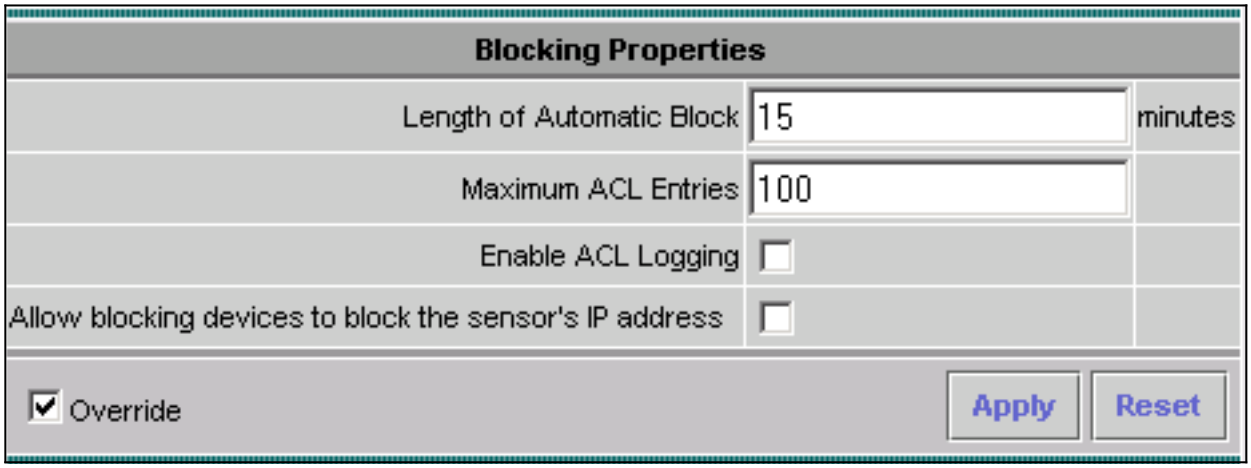
10. Cliquez sur **Modifier les interfaces** (voir capture d'écran précédente), cliquez sur **Ajouter**, entrez ces informations, puis cliquez sur **OK** pour continuer.



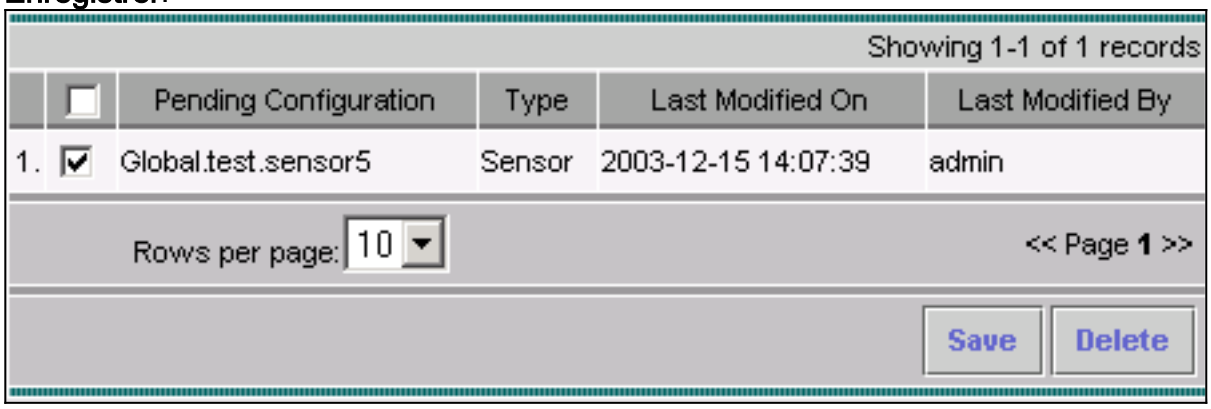
11. Cliquez deux fois sur **OK** pour terminer la configuration du périphérique de blocage.



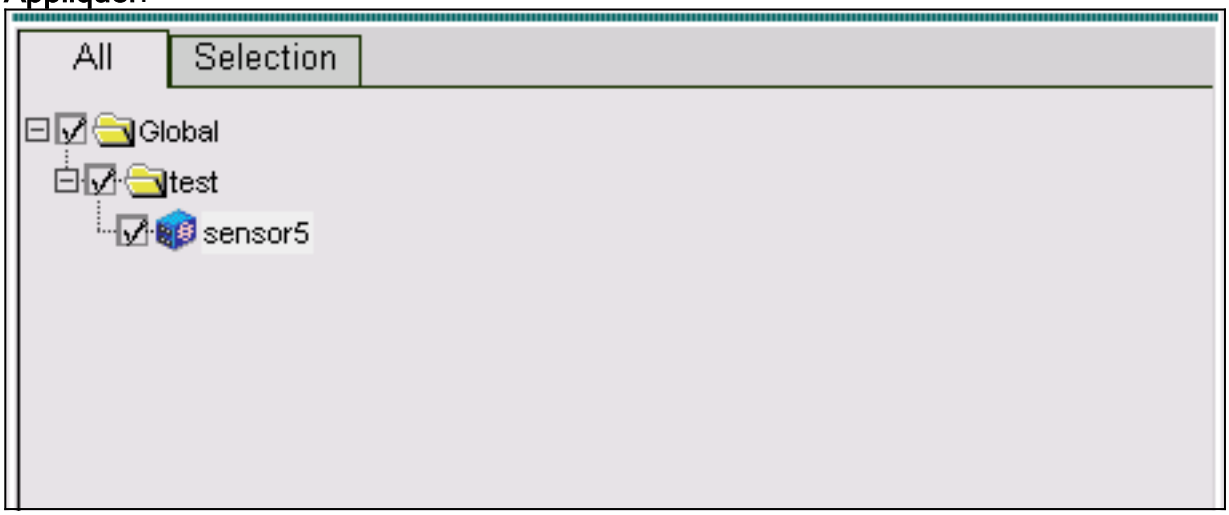
12. Pour configurer les propriétés de blocage, sélectionnez **Blocage > Propriétés de blocage**.La longueur du bloc automatique peut être modifiée. Dans ce cas, il est remplacé par **15 minutes**. Cliquez sur **Apply** pour continuer.



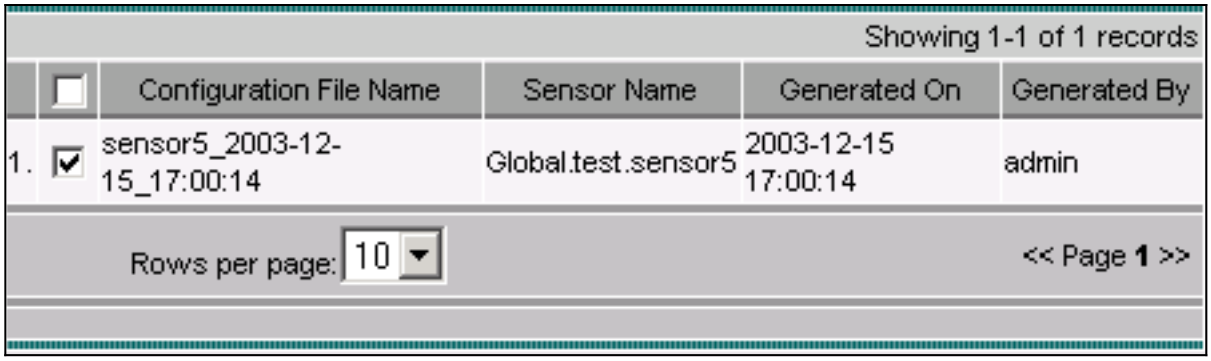
13. Sélectionnez **Configuration** dans le menu principal, puis sélectionnez **En attente**, vérifiez la configuration en attente pour vous assurer qu'elle est correcte, puis cliquez sur **Enregistrer**.



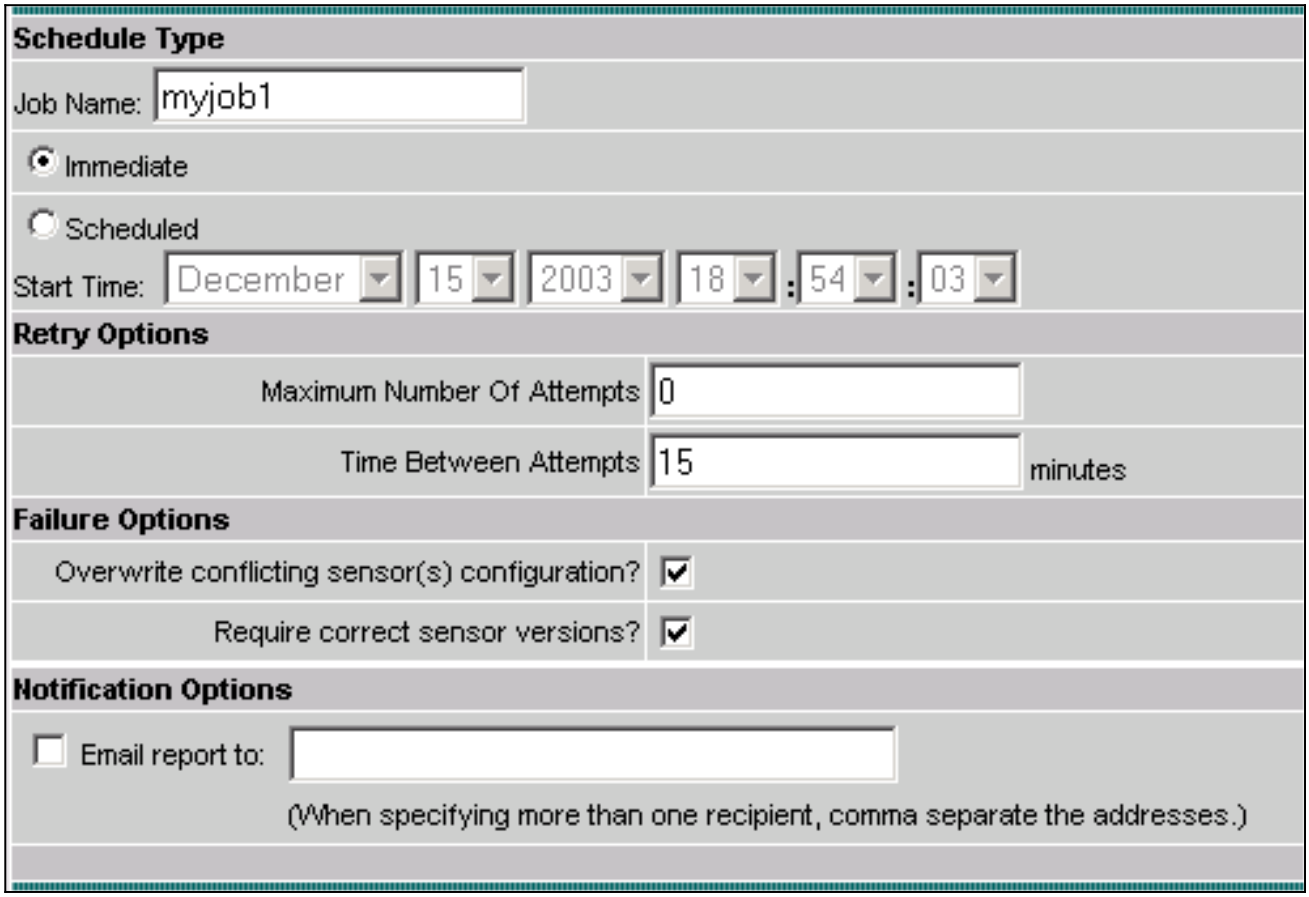
14. Pour appliquer les modifications de configuration au capteur, générez et déployez les modifications en sélectionnant **Déploiement > Générer** et cliquez sur **Appliquer**.



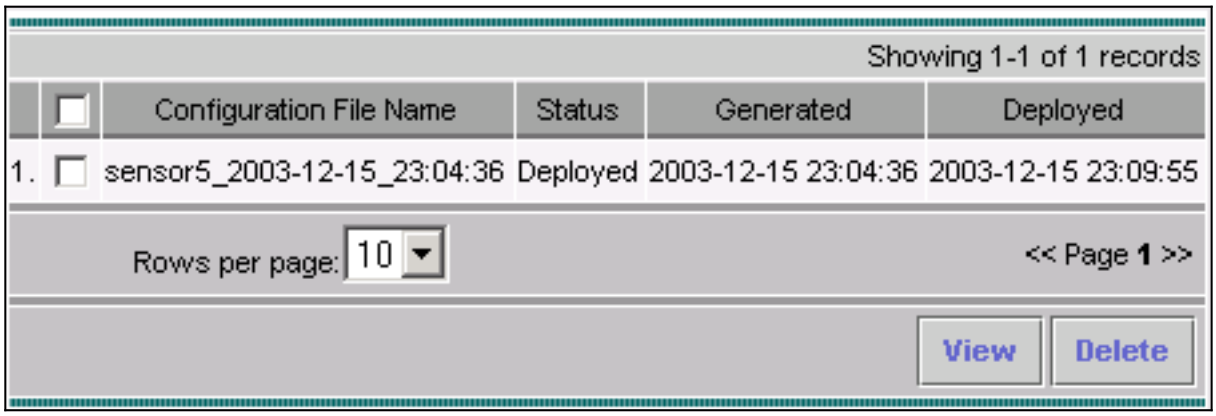
15. Sélectionnez **Déploiement > Déploiement**, puis cliquez sur **Soumettre**.
16. Cochez la case en regard de votre capteur, puis cliquez sur **Déployer**.
17. Cochez la case du travail dans la file d'attente, puis cliquez sur **Suivant** pour continuer.



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



19. Sélectionnez **Déploiement > Déploiement > En attente**.Patientez quelques minutes jusqu'à ce que tous les travaux en attente soient terminés. La file d'attente est alors vide.
20. Pour confirmer le déploiement, sélectionnez **Configuration> Historique**.Assurez-vous que l'état de la configuration est affiché en tant que **Déployé**. Cela signifie que la configuration du capteur a été mise à jour avec
succès.



Vérification

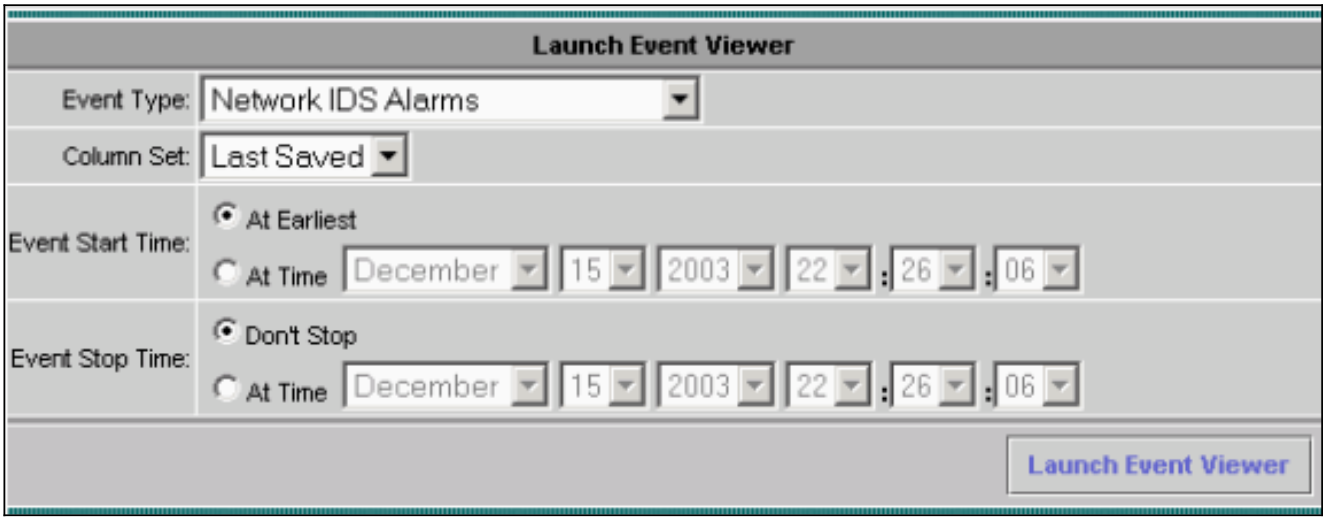
Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Lancer l'attaque et bloquer

Pour vérifier que le processus de blocage fonctionne correctement, lancez une attaque de test et vérifiez les résultats.

1. Avant de lancer l'attaque, sélectionnez **VPN/Security Management Solution > Monitoring Center > Security Monitor**.
2. Choisissez **Monitor** dans le menu principal, cliquez sur **Events**, puis cliquez sur **Launch Event Viewer**.



3. Établissez une connexion Telnet avec le routeur (dans ce cas, une connexion Telnet avec le routeur House) pour vérifier la communication à partir du capteur.

```
house#show user
    Line       User       Host(s)              Idle       Location
*   0 con 0                idle                 00:00:00
 226 vty 0                 idle                 00:00:17 10.66.79.195
house#show access-list
Extended IP access list IDS_Ethernet1_in_0
    10 permit ip host 10.66.79.195 any
    20 permit ip any any (20 matches)
House#
```

4. Pour lancer l'attaque, établissez une connexion Telnet d'un routeur à l'autre et tapez **testattack**.Dans ce cas, nous avons utilisé Telnet pour connecter le routeur Light au routeur House. Dès que vous appuyez sur **<space>** ou **<enter>**, après avoir tapé testattack, votre session Telnet doit être réinitialisée.

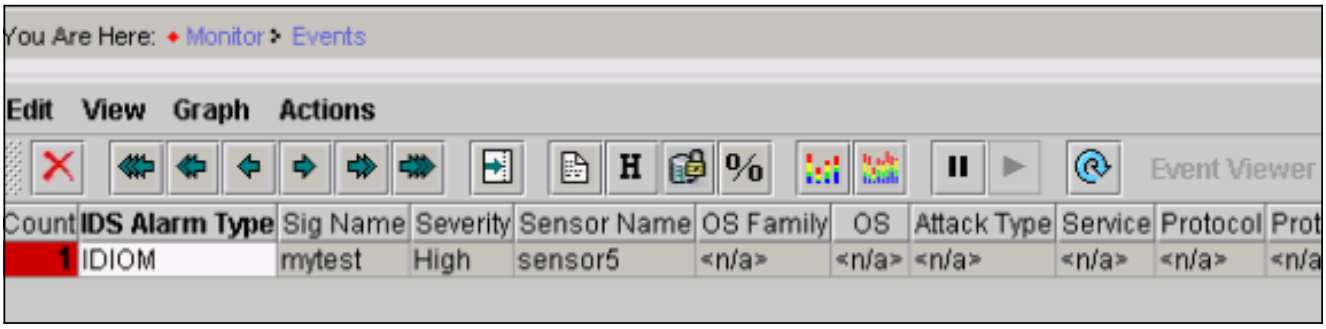
```
light#telnet 100.100.100.1
Trying 100.100.100.1 ... Open
User Access Verification
Password:
house>en
Password:
house#testattack
!--- Host 100.100.100.2 has been blocked due to the !--- signature "testattack" being
```

```
triggered. [Connection to 100.100.100.1 lost]
```

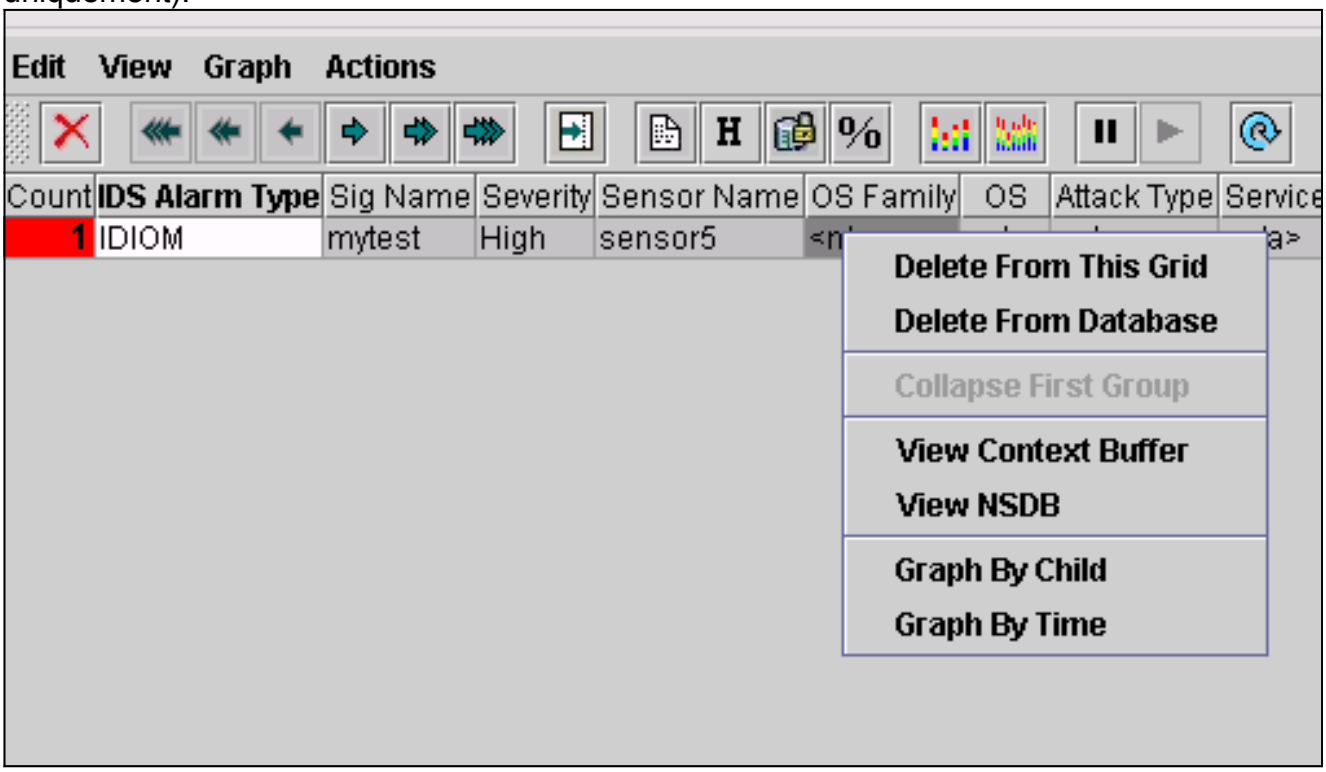
5. Établissez une connexion Telnet avec le routeur (House) et entrez la commande **show access-list**.

```
house#show access-list
Extended IP access list IDS_Ethernet1_in_1
10 permit ip host 10.66.79.195 any
!--- You will see a temporary entry has been added to !--- the access list to block the
router from which you connected via Telnet previously. 20 deny ip host 100.100.100.2 any
(37 matches)
30 permit ip any any
```

6. Dans l'Observateur d'événements, cliquez sur **Base de données** de **requêtes** pour afficher les nouveaux événements pour afficher l'alerte de l'attaque précédemment lancée.



7. Dans l'Observateur d'événements, mettez en surbrillance l'alarme et cliquez avec le bouton droit de la souris, puis sélectionnez **Afficher la mémoire tampon de contexte** ou **Afficher NSDB** pour afficher des informations plus détaillées sur l'alarme.**Remarque :** La NSDB est également disponible en ligne sur l'encyclopédie sécurisée Cisco (clients enregistrés uniquement).

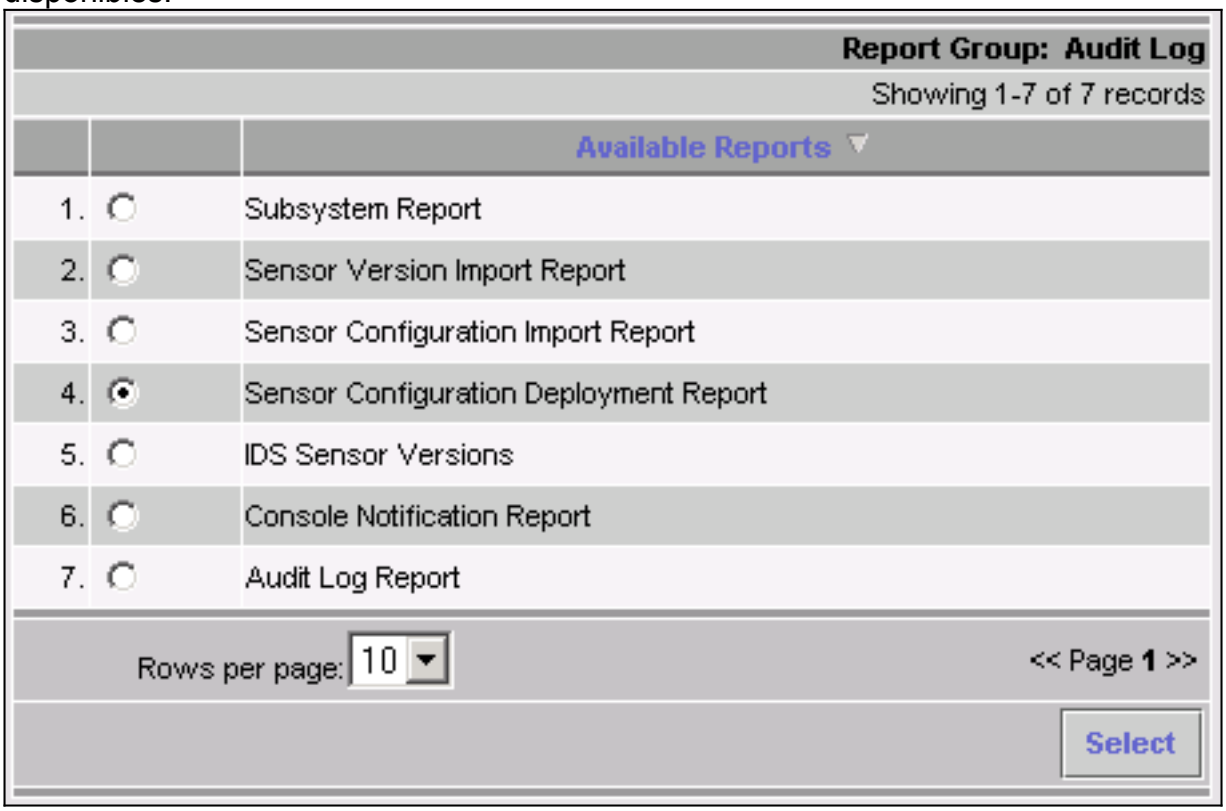


Dépannage

Procédure de dépannage

Utilisez la procédure suivante à des fins de dépannage.

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



2. Sur la console Sensor, entrez la commande **show statistics networkaccess** et vérifiez le résultat pour vous assurer que l'état est actif.

```
sensor5#show statistics networkAccess
Current Configuration
   AllowSensorShun = false
   ShunMaxEntries = 100
   NetDevice
      Type = Cisco
      IP = 10.66.79.210
      NATAddr = 0.0.0.0
      Communications = telnet
      ShunInterface
         InterfaceName = FastEthernet0/1
         InterfaceDirection = in
State
   ShunEnable = true
   NetDevice
      IP = 10.66.79.210
      AclSupport = uses Named ACLs
      State = Active
   ShunnedAddr
      Host
         IP = 100.100.100.2
         ShunMinutes = 15
         MinutesRemaining = 12
sensor5#
```

3. Assurez-vous que le paramètre de communication indique que le protocole correct est utilisé, tel que Telnet ou Secure Shell (SSH) avec 3DES.Vous pouvez essayer un SSH ou Telnet manuel à partir d'un client SSH/Telnet sur un PC pour vérifier que le nom d'utilisateur et les informations d'identification du mot de passe sont corrects. Vous pouvez ensuite essayer

Telnet ou SSH à partir du capteur lui-même, vers le routeur, pour vous assurer que vous pouvez vous connecter correctement.

Informations connexes

- Page d'assistance Cisco Secure Intrusion Detection
- Prise en charge de la solution de gestion de la sécurité/VPN CiscoWorks
- Support et documentation techniques - Cisco Systems