Configuration du blocage IDS avec VMS IDS MC

Contenu

Introduction

Ce document fournit un échantillon pour la configuration 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, bloquant du capteur d'ID à un routeur de Cisco est configuré.

Conditions préalables

Conditions requises

Avant que vous configuriez le blocage, assurez que vous avez rempli ces conditions.

- 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 dans ce document sont basées sur les versions de logiciel et matériel 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)
- Version de logiciel 12.3.5 courante de Cisco IOS® de routeur de Cisco

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 des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

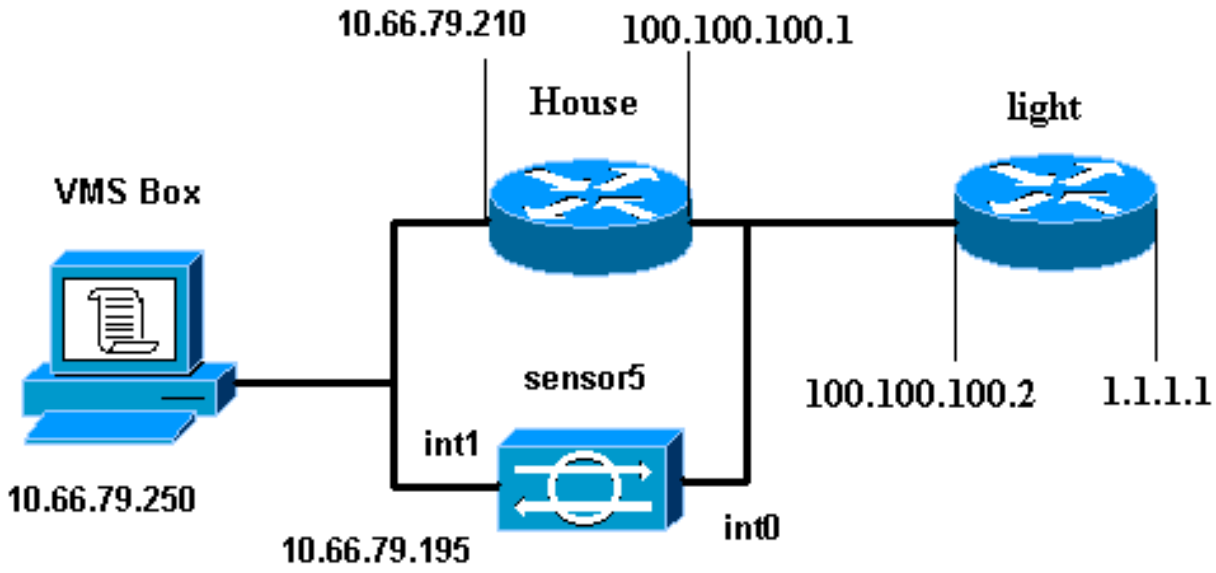
Configurez

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

Remarque: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés seulement).

Diagramme du réseau

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



Configurations

Ce document utilise les configurations indiquées ici.

- 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 !--- 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 de capteur

Terminez-vous ces étapes pour configurer au commencement le capteur.

Remarque: Si vous avez exécuté la première installation de votre capteur, poursuivez à la section important le capteur dans des ID MC.

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

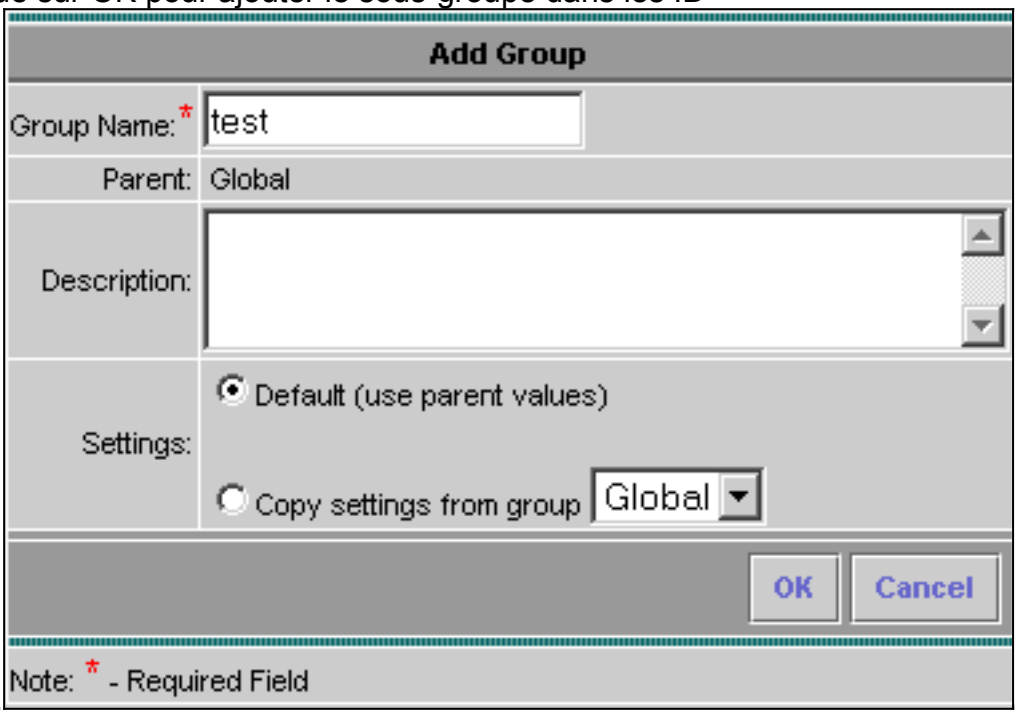
d'utilisateur **Cisco** et le mot de passe cisco.

2. Vous êtes incité à changer le mot de passe et puis 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`
4. Presse **2** afin de sauvegarder votre configuration.

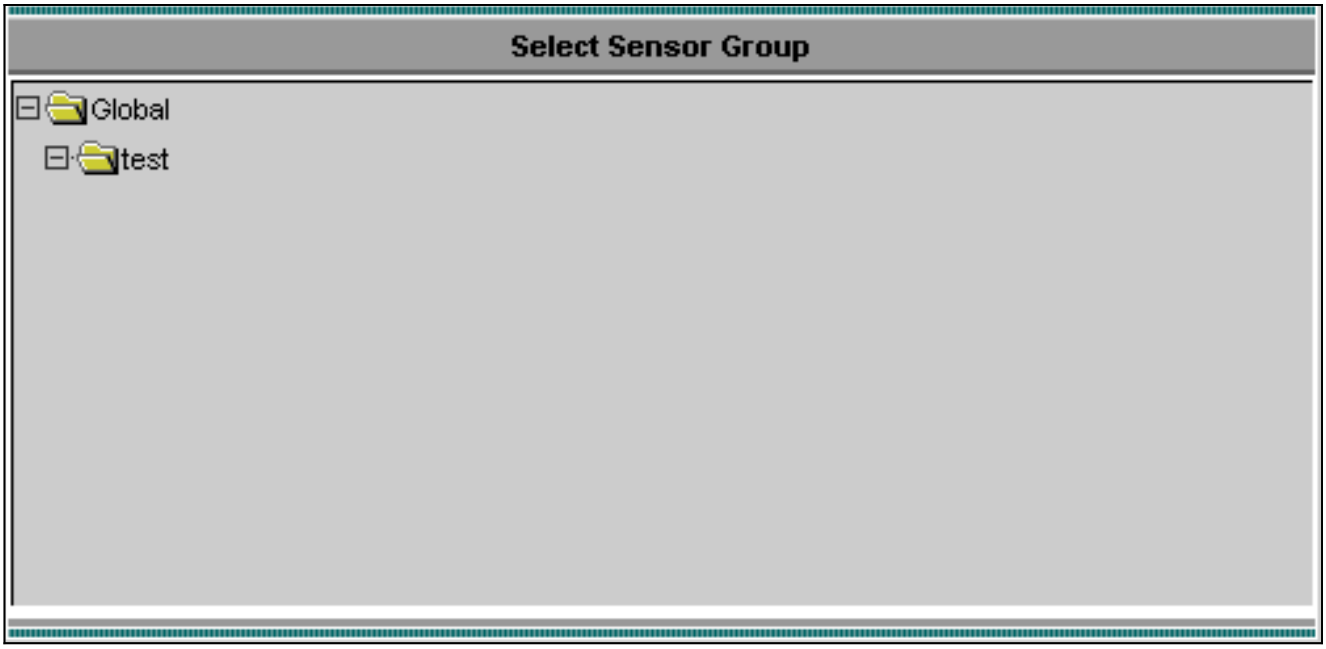
Importez le capteur dans des ID MC

Terminez-vous ces étapes pour importer le capteur dans les ID MC.

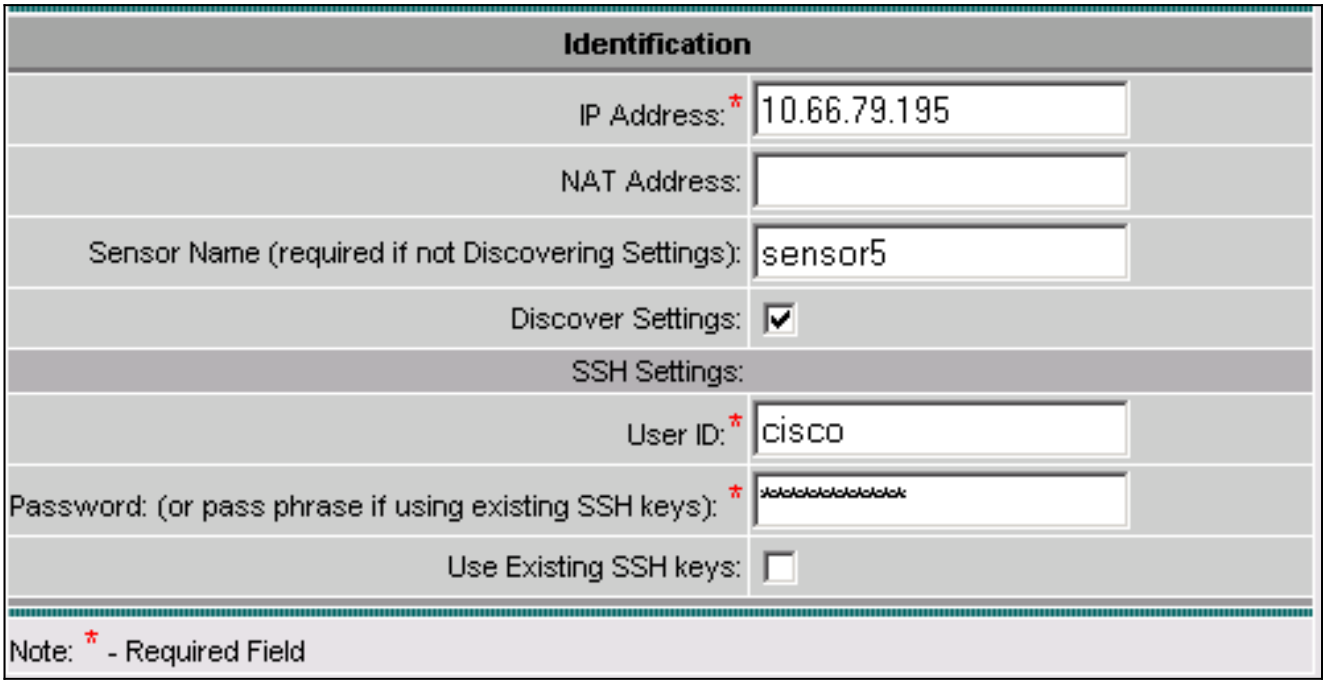
1. Parcourez à votre capteur.Dans ce cas, parcourez à **http://10.66.79.250:1741** ou à **https://10.66.79.250:1742**.
2. Procédure de connexion avec le nom d'utilisateur et mot de passe approprié.Dans cet exemple, l'**admin** et le mot de passe cisco de nom d'utilisateur ont été utilisés.
3. **La solution de Gestion VPN/Security** > le **centre** choisis de **Gestion** et choisissent des **capteurs d'ID**.
4. Cliquez sur l'onglet de périphériques, **groupe** choisi de **capteur**, mettez en valeur **global**, et le clic **créent le sous-groupe**.
5. Écrivez le nom de groupe et l'assurez que la case d'option **par défaut** est sélectionnée, puis clique sur OK pour ajouter le sous-groupe dans les ID MC.



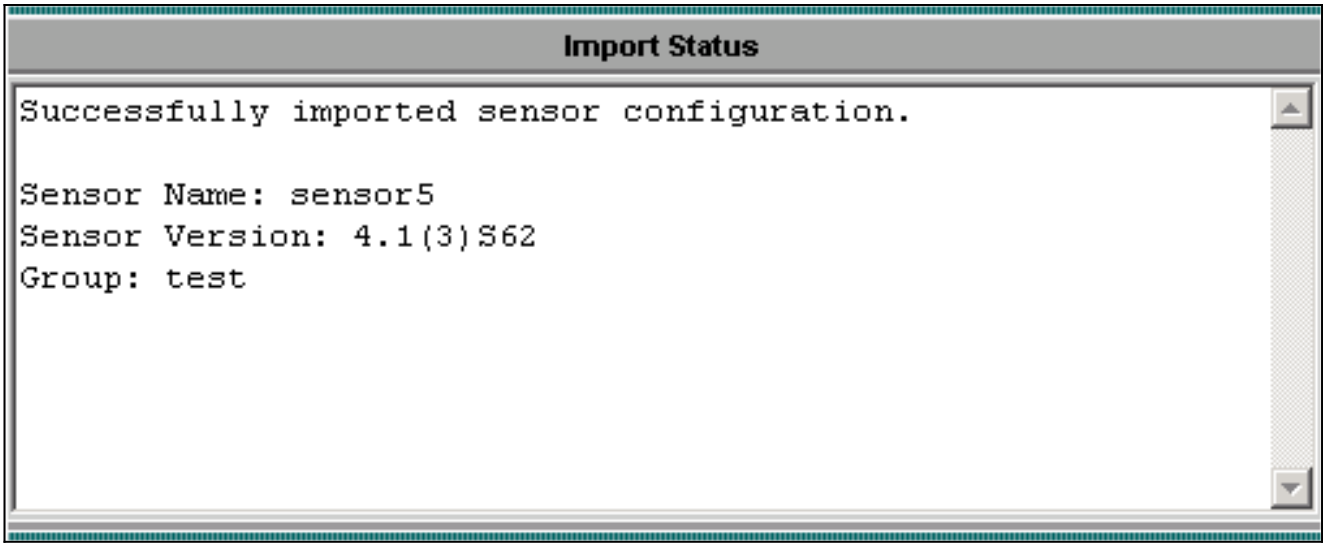
6. **Les périphériques** > le **capteur** choisis, mettent en valeur le sous-groupe créé dans l'étape précédente (dans ce cas, **test**), et cliquent sur Add.
7. Mettez en valeur le sous-groupe, et cliquez sur Next.



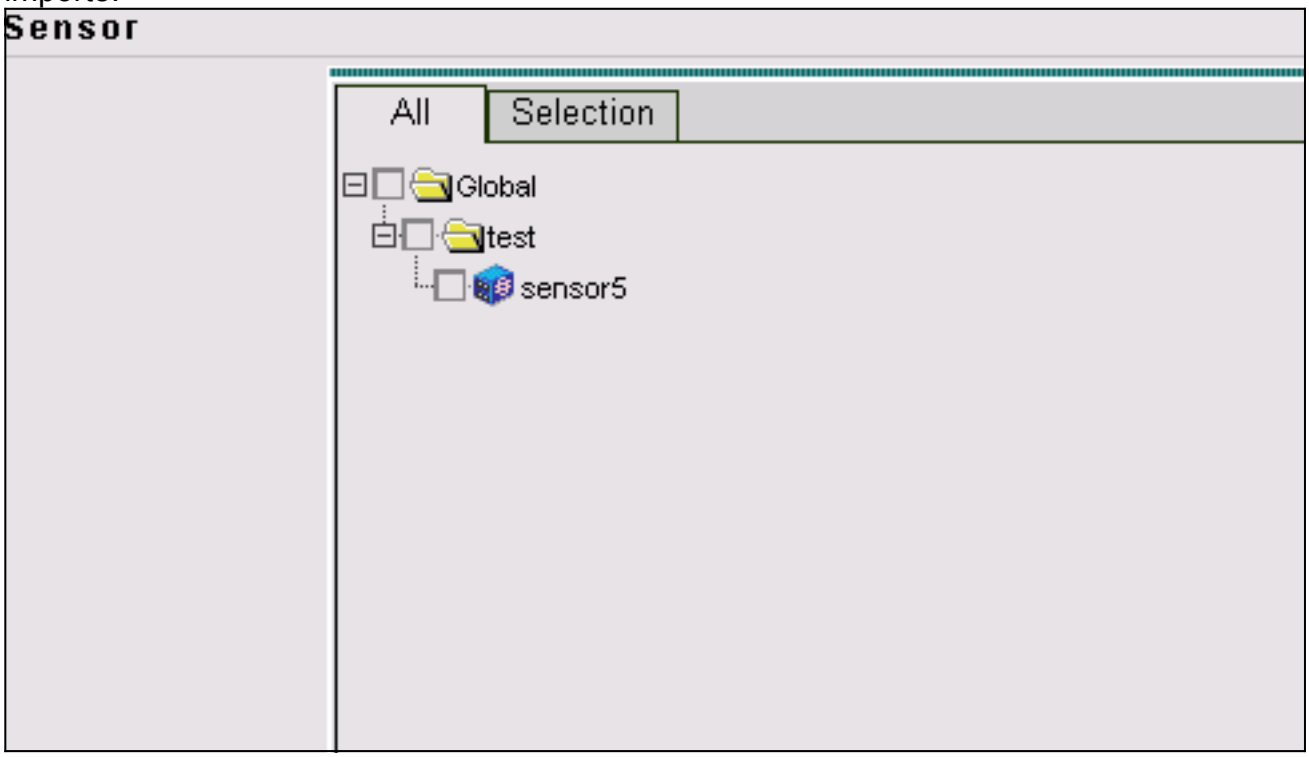
8. Écrivez les détails selon cet exemple, puis cliquez sur **à côté de** continuent.



9. Après que vous soyez présenté avec un message que les états `ont avec succès importé la configuration de capteur`, cliquez sur Finish pour continuer.



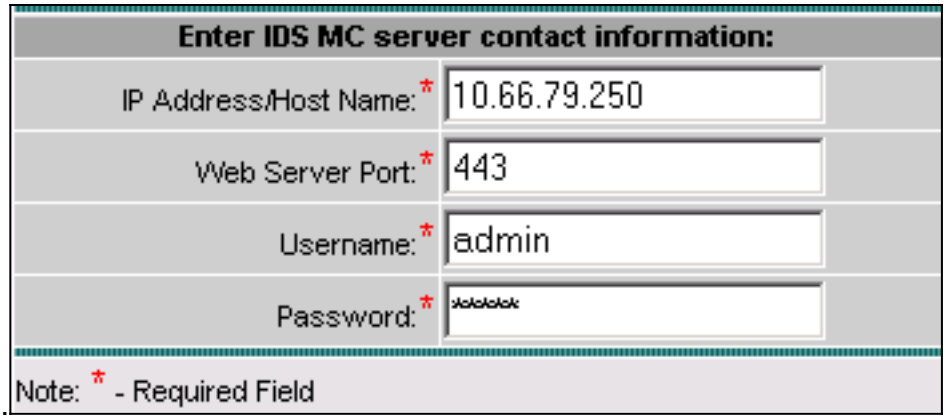
10. Votre capteur est importé dans les ID MC. Dans ce cas, sensor5 est importé.



Importez le capteur dans le contrôleur de sécurité

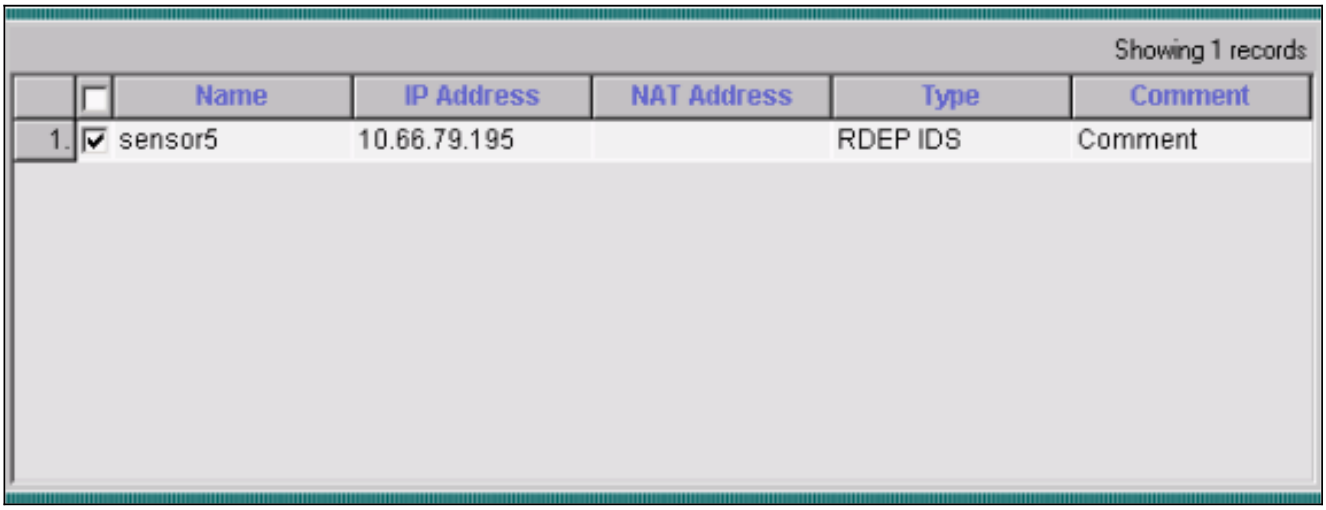
Remplissez cette procédure pour importer le capteur dans le moniteur de Sécurité.

1. Au menu de serveur VMS, **solution de Gestion VPN/Security > centre > contrôleur de sécurité** choisis 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

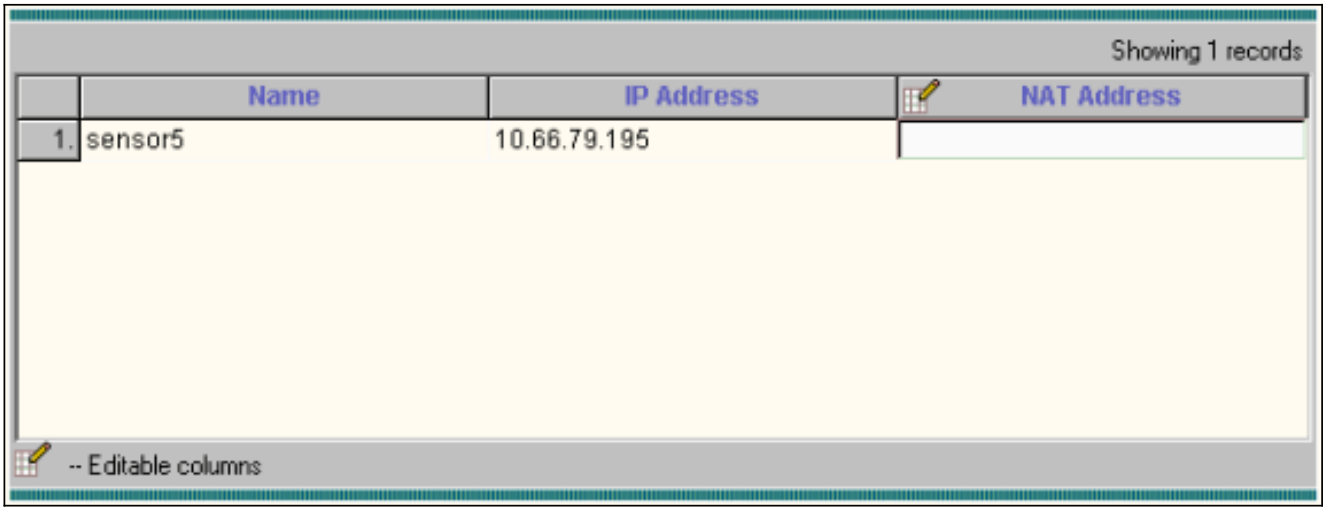


exemple.

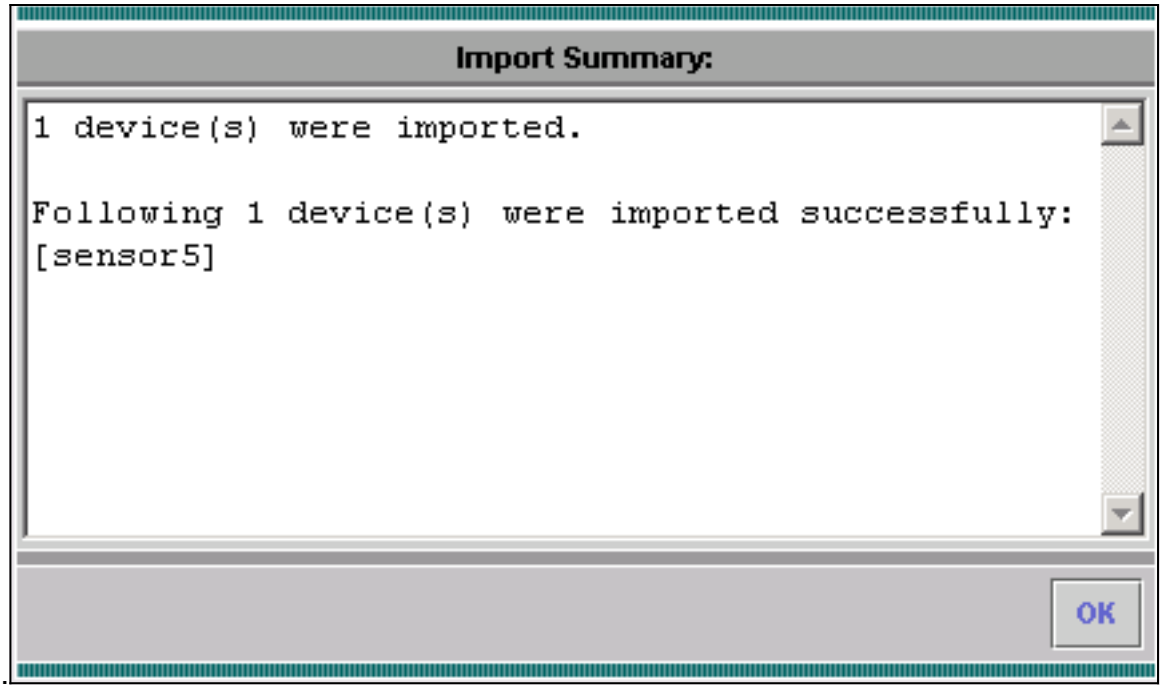
3. Sélectionnez votre capteur (dans ce cas, **sensor5**) et cliquez sur **à côté de** continuent.



4. Si besoin est, mettez à jour l'adresse de Traduction d'adresses de réseau (NAT) pour votre capteur, puis cliquez sur Finish pour continuer.

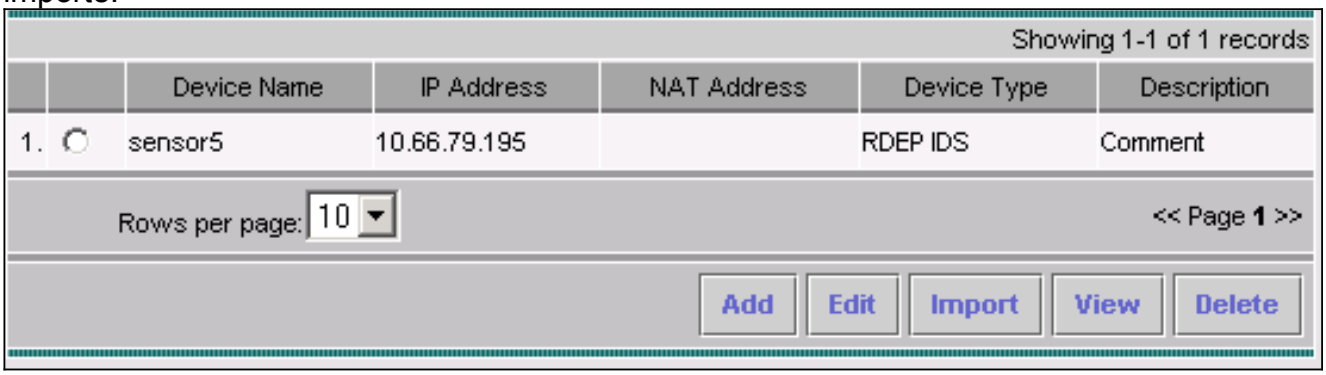


5. Cliquez sur OK pour terminer importer le capteur des ID MC dans le contrôleur de



sécurité.

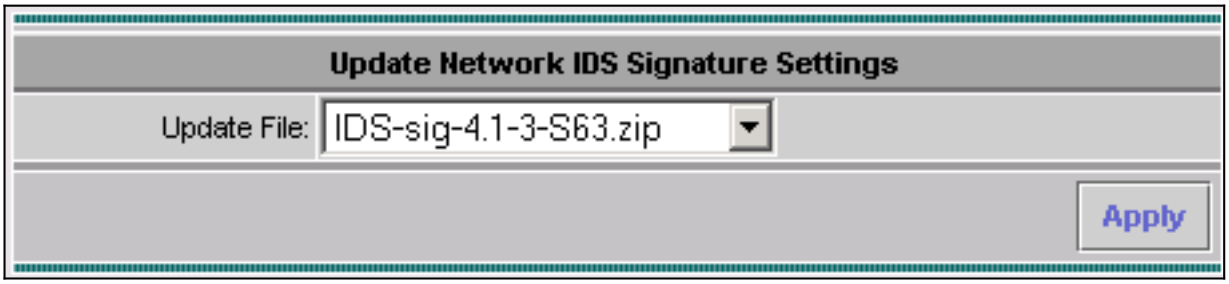
6. Votre capteur est avec succès importé.



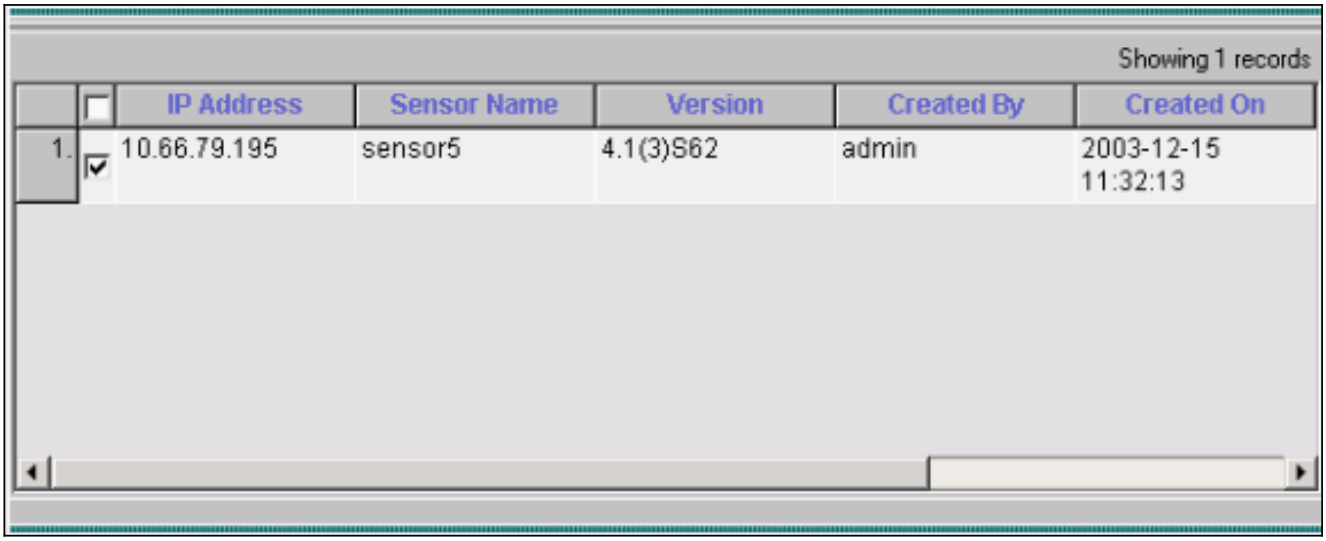
ID MC d'utilisation pour des mises à jour de signature

Remplissez cette procédure pour utiliser les ID MC pour des mises à jour de signature.

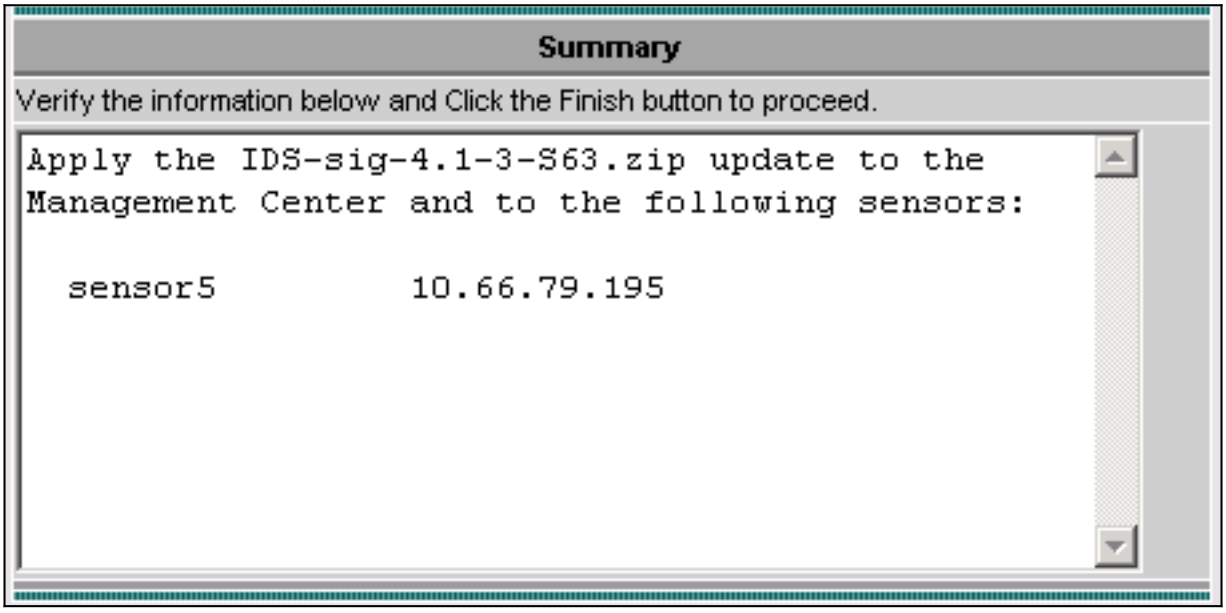
1. Téléchargez les mises à jour de signature d'ID de réseau (clients enregistrés seulement) des téléchargements et sauvegardez-les dans le répertoire C:\PROGRA~1\CSCOpx\MDC\etc\ids\updates\ sur votre serveur VMS.
2. Àla console de serveur VMS, **solution de Gestion VPN/Security > centre > capteurs**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



5. Sélectionnez les capteurs pour mettre à jour, et le clic **à côté de** continuent.



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



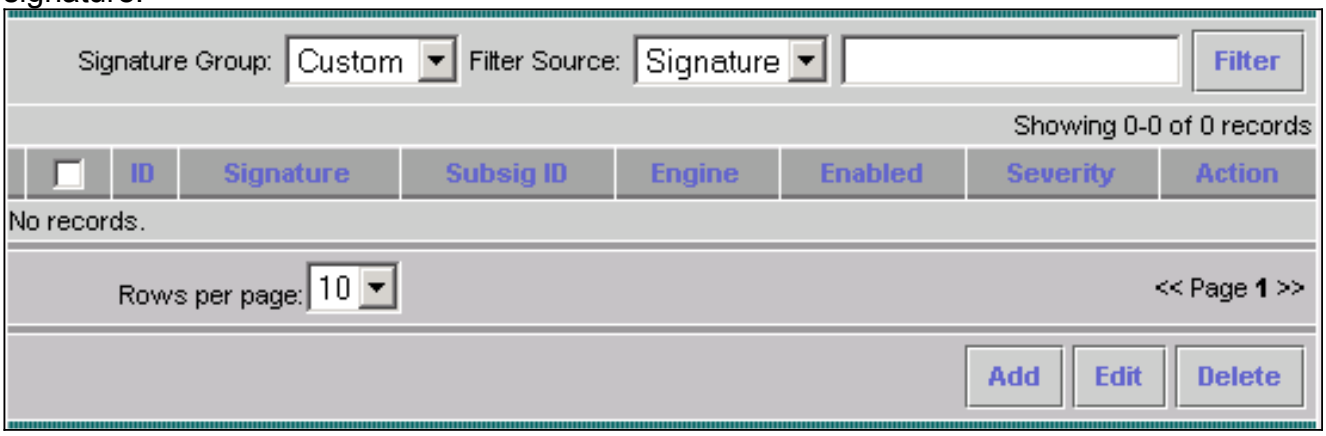
7. Telnet ou console dans l'interface de ligne de commande de capteur. Les informations semblables à ceci apparaissent :`sensor5#`
`Broadcast message from root (Mon Dec 15 11:42:05 2003):`
`Applying update` **`IDS-sig-4.1-3-S63. This may take several minutes.`** `Please do not reboot the sensor during 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 à la mise à jour pour se terminer, puis écrivez le **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`**

Configurez le blocage pour le routeur IOS

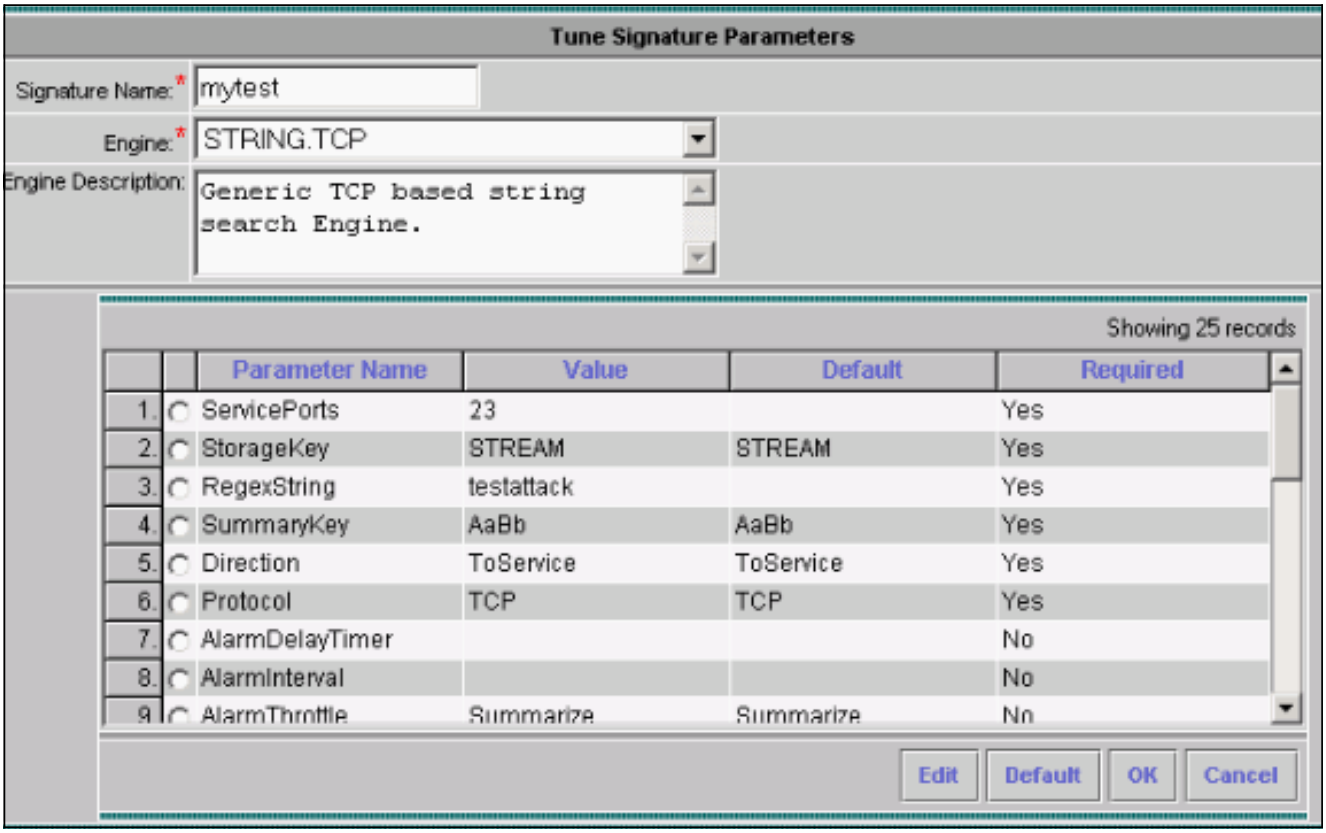
Remplissez cette procédure pour configurer le blocage pour le routeur IOS.

1. Àla console de serveur VMS, **solution de Gestion VPN/Security > centre de Gestion > capteurs** choisis d'**ID**.

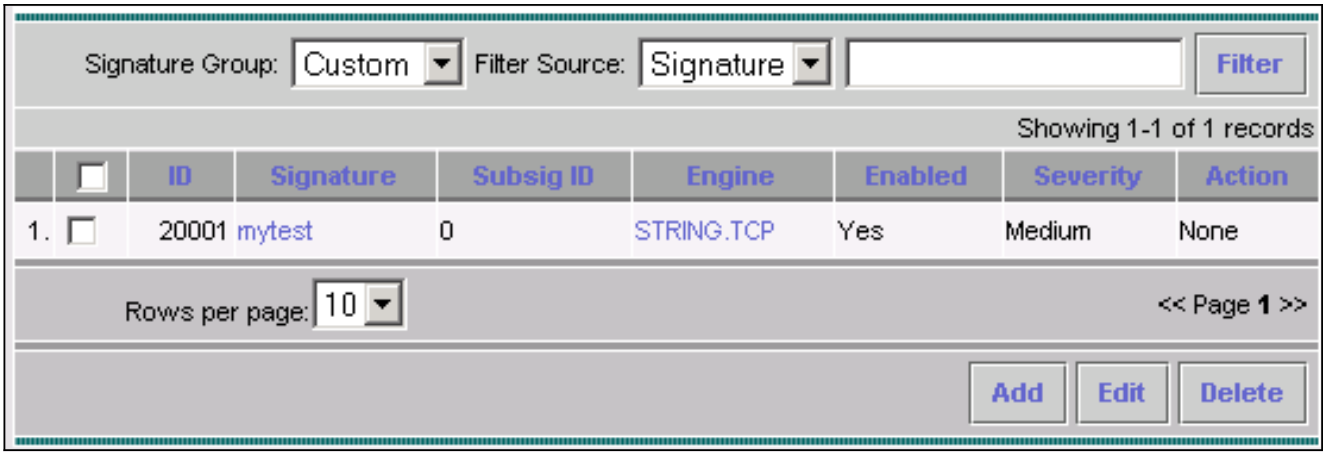
2. Sélectionnez l'onglet de configuration, sélectionnez votre capteur de sélecteur d'objet, et cliquez sur les **configurations**.
3. **Les signatures** choisies, **coutume de** clic, cliquent sur Add alors pour ajouter une nouvelle signature.



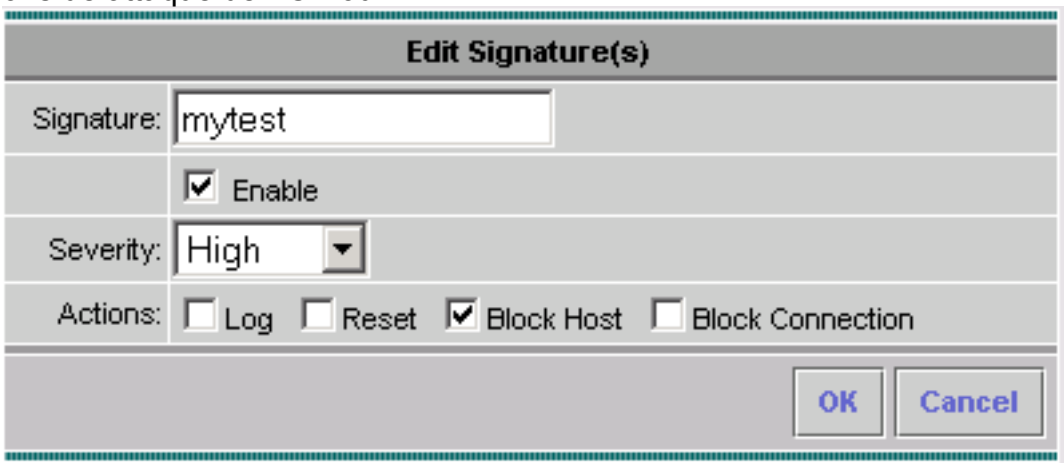
4. Écrivez le nouveau nom de signature, puis sélectionnez l'engine (dans ce cas, **STRING.TCP**).
5. Vous pouvez personnaliser les paramètres disponibles en vérifiant la case d'option appropriée et en cliquant sur Edit.Dans cet exemple, le paramètre de ServicePorts est édité pour changer sa valeur à 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.



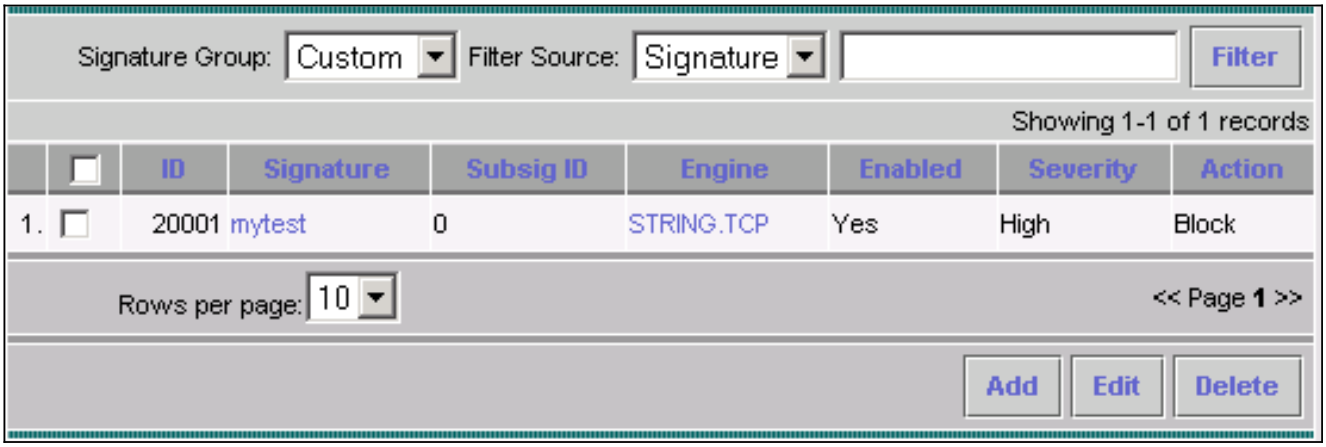
6. Pour éditer la sévérité et les actions de signature ou activer/la signature, cliquez sur le nom de la
signature.



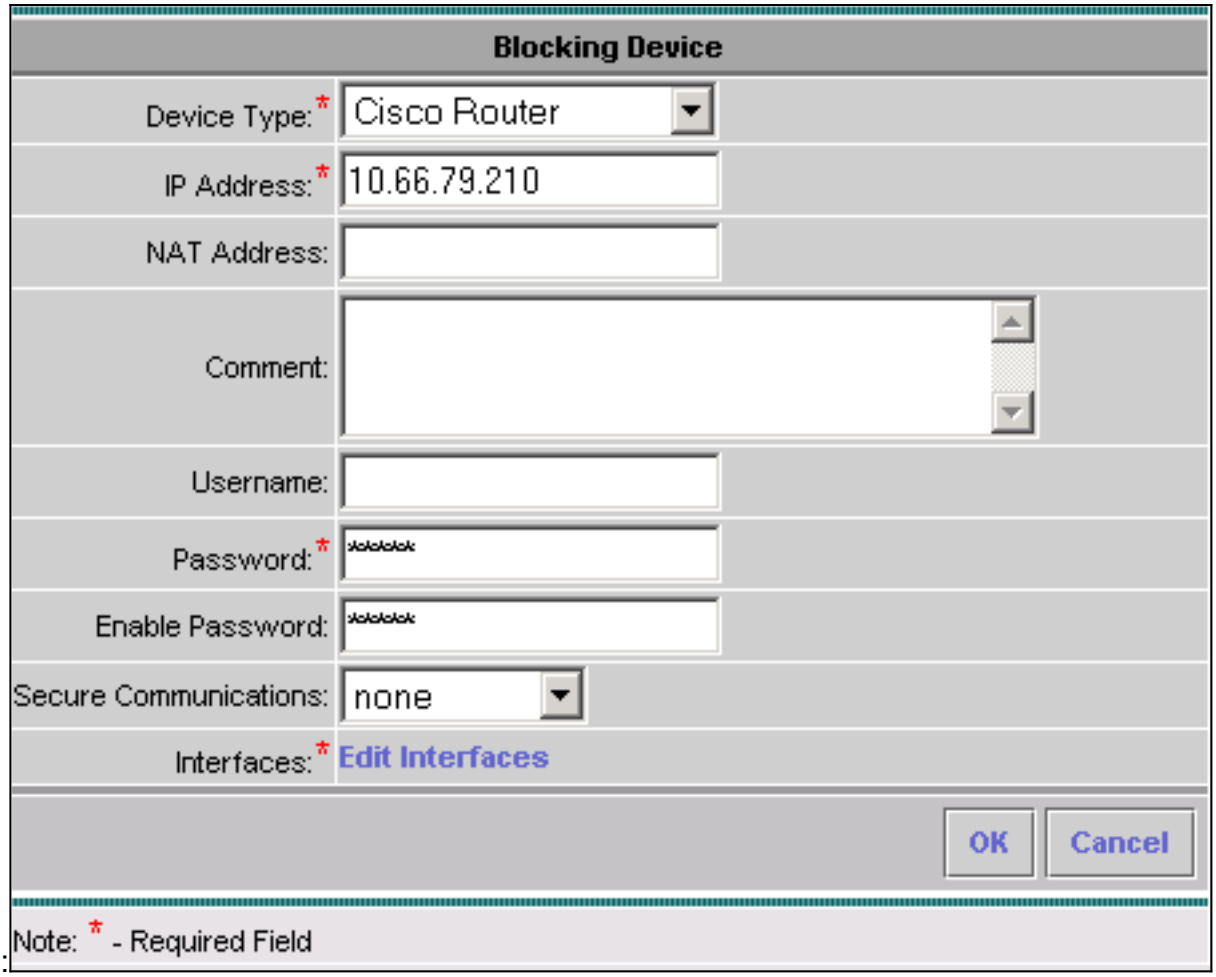
7. Dans ce cas, la sévérité est changée à la **haute** et l'action d'**hôte de bloc** est sélectionnée. Cliquez sur **OK** pour continuer.Les blocs d'hôte de bloc attaquant des hôtes IP ou des sous-réseaux IP.Le TCP ou les ports UDP de blocs de connexion de bloc (basés sur les connexions de attaque de TCP ou d'UDP).



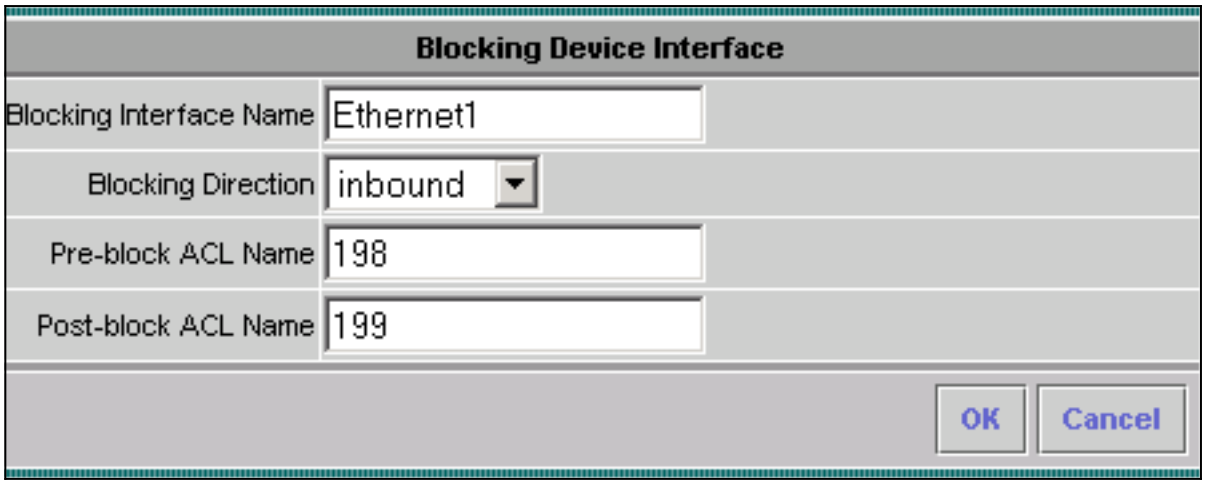
8. La signature complète semble semblable à ceci :



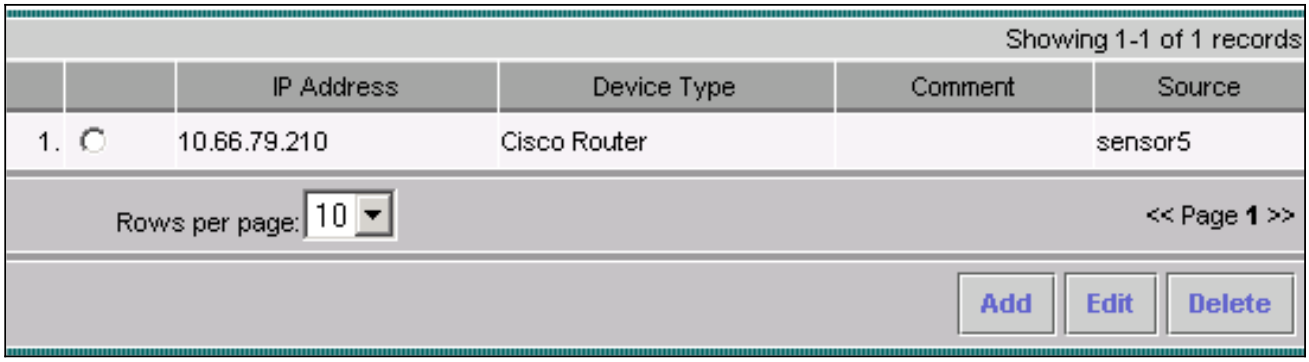
9. Afin de configurer le périphérique en mode bloc, sélectionnez les **périphériques en mode bloc de blocage >** du sélecteur d'objet (le menu du côté gauche de l'écran), et cliquez sur Add pour écrire les informations suivantes



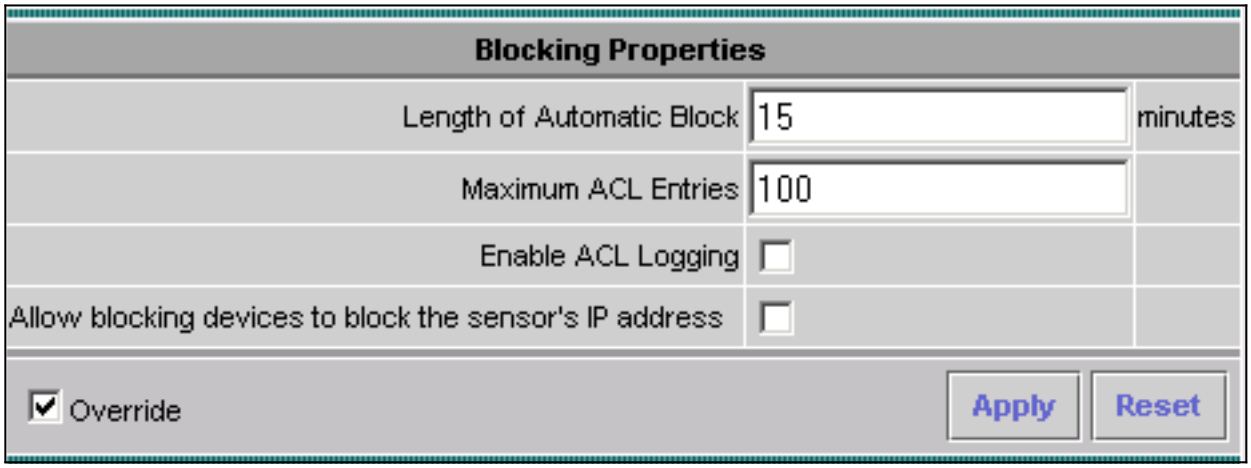
10. Cliquez sur Edit les **interfaces** (voir la capture d'écran précédente), cliquez sur Add, écrivez ces informations, puis cliquez sur OK pour continuer.



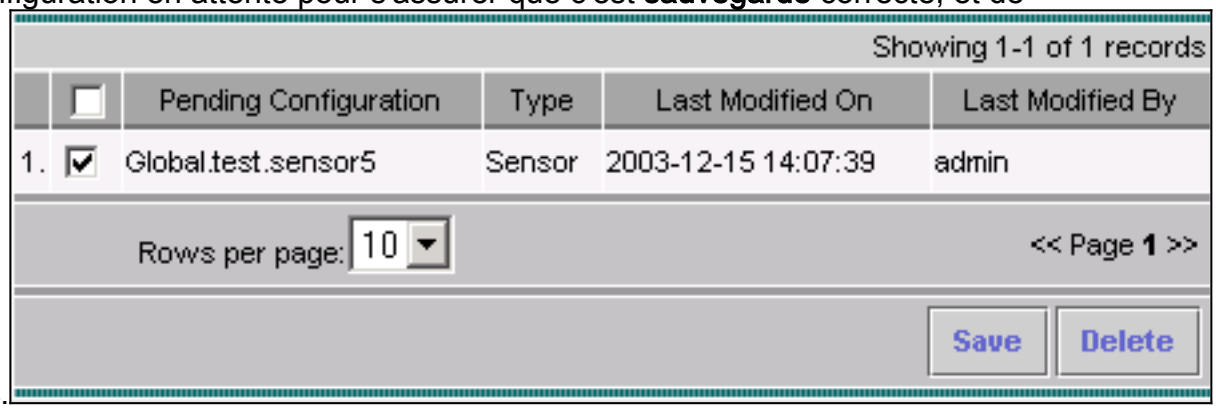
11. Cliquez sur OK deux fois pour se terminer la configuration du périphérique en mode bloc.



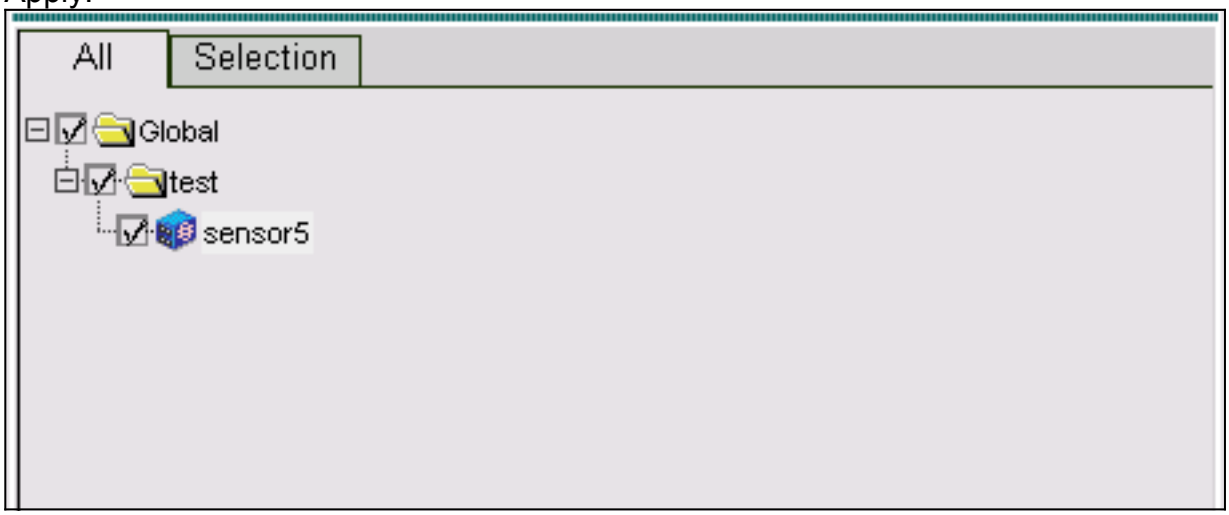
12. Pour configurer bloquer Properties, **blocage** choisi > **blocage de Properties**.La longueur du bloc automatique peut être modifiée. Dans ce cas, il est changé à **15 minutes**. Cliquez sur Apply pour
continuer.



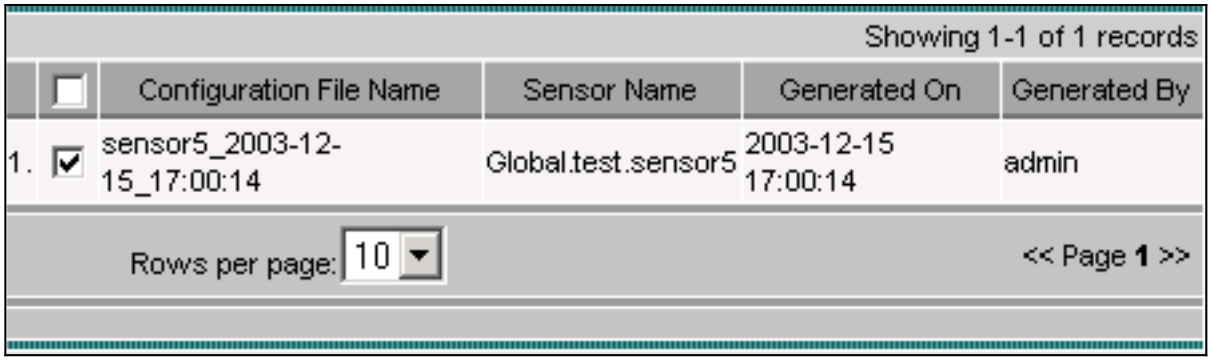
13. **La configuration** choisie du menu principal, sélectionnent alors **en suspens**, vérifient la configuration en attente pour s'assurer que c'est **sauvegarde** correcte, et de clic.



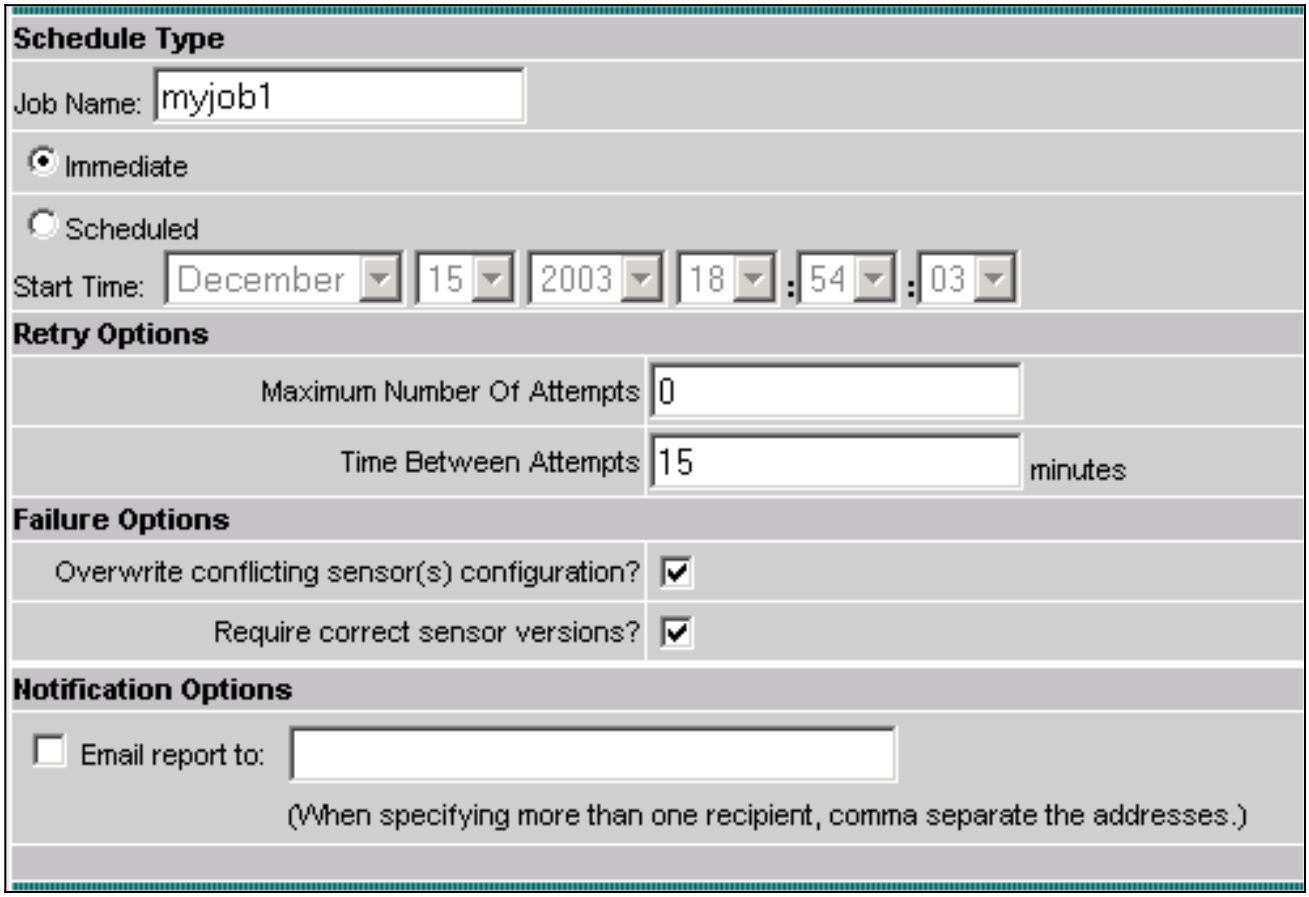
14. Pour pousser les modifications de configuration au capteur, générez et puis déployez les modifications en sélectionnant le **déploiement > se produisent** et cliquent sur Apply.



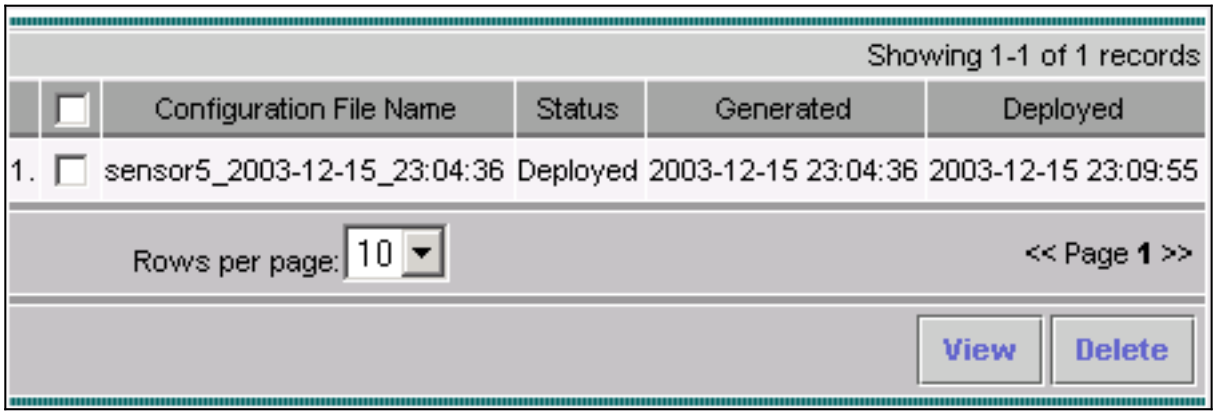
15. **Le déploiement** choisi > **se déploient**, puis cliquent sur Submit.
16. Vérifiez la case à cocher à côté de votre capteur, puis cliquez sur **se déploient**.
17. Vérifiez la case à cocher pour le travail dans la file d'attente, puis cliquez sur **à côté de** continuent.



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



19. **Le déploiement** choisi **> se déploient > en suspens**.Attendez quelques minutes jusqu'à ce que tous les travaux en attente aient été terminés. La file d'attente est alors vide.
20. Pour confirmer le déploiement, **historique** choisi de **Configuration>**.Assurez que le statut de la configuration est affiché comme **déployé**. Ceci signifie que la configuration de capteur a été mise à jour avec
succès.



Vérifiez

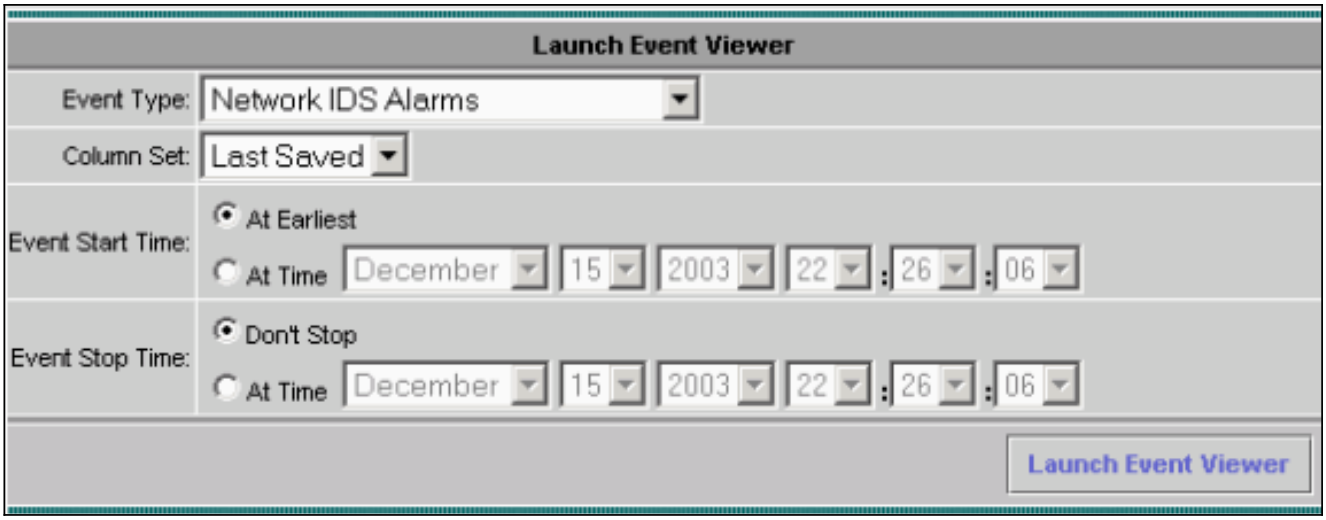
Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

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.

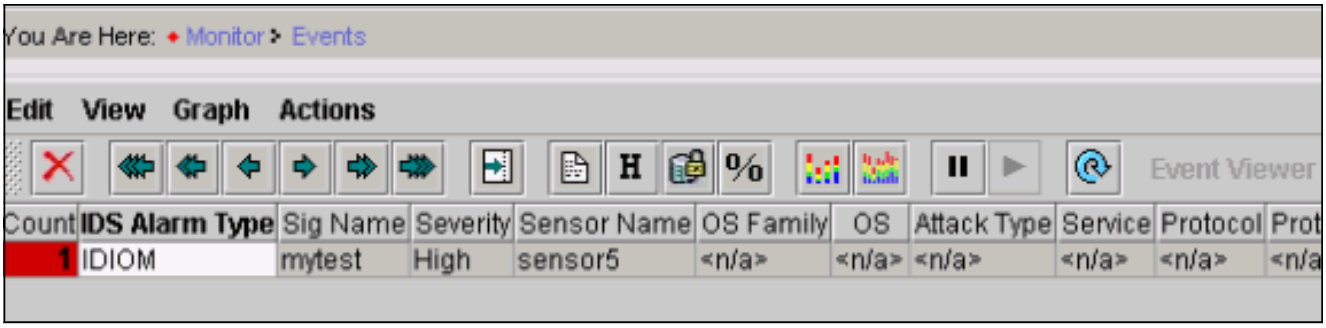
Lancez l'attaque et le blocage

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

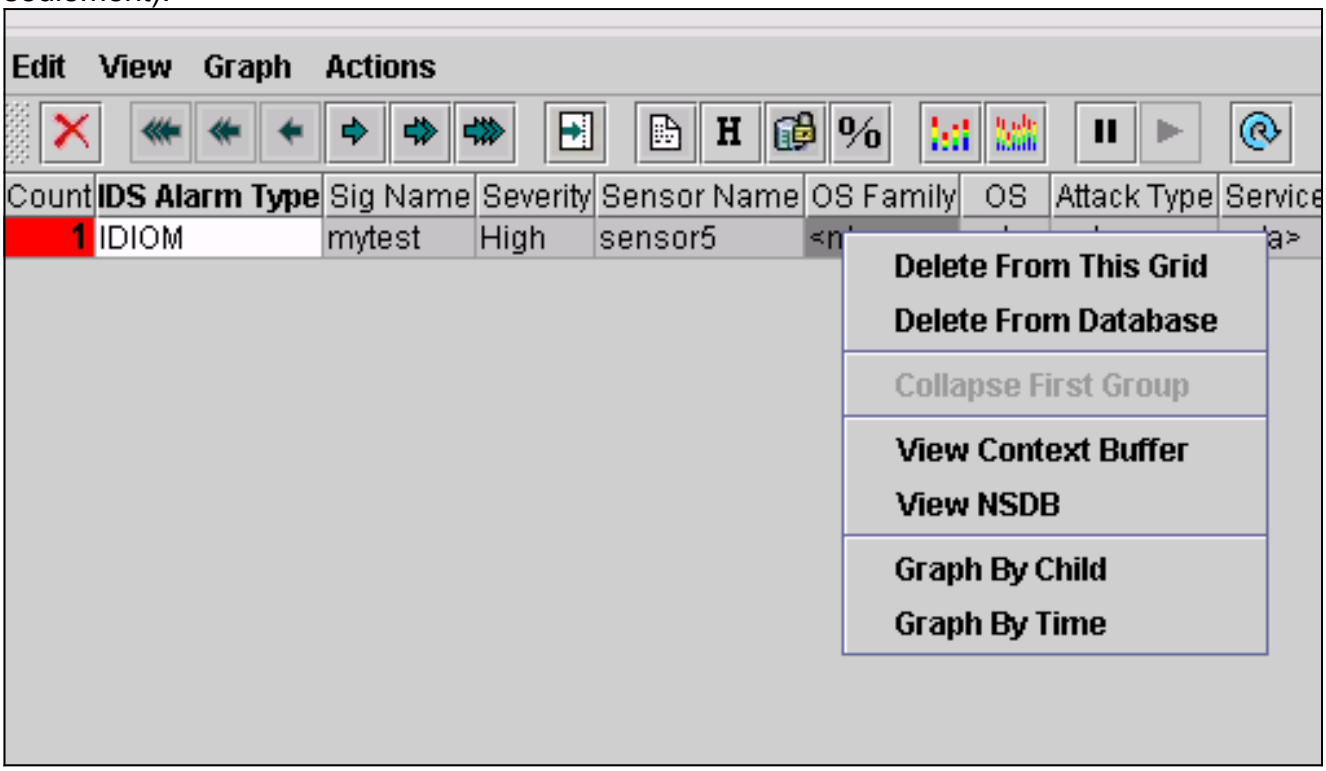
1. Avant de lancer l'attaque, **solution de Gestion VPN/Security > centre > contrôleur de sécurité** choisis de **surveillance**.
2. Choisissez le **moniteur du** menu principal, cliquez sur les **événements** et puis cliquez sur le **visualisateur d'événements de lancement**.



3. Telnet au routeur (dans ce cas, telnet au routeur de Chambre), pour vérifier la transmission 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, telnet d'un routeur au **testattack d'**autre et de type.Dans ce cas, nous avons utilisé le telnet pour nous connecter du routeur léger au routeur de Chambre. Dès que vous appuierez sur le **<space>** ou le **<enter>**, après avoir tapé le testattack, votre session de telnet devrait être remis 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`** *`!--- Host 100.100.100.2 has been blocked due to the !--- signature "testattack" being triggered.`* **`[Connection to 100.100.100.1 lost]`**
5. Le telnet au routeur (Chambre) et écrivent la **liste d'accès d'exposition de** commande.`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. Du visualisateur d'événements, **base de données de requête de** clic pour de nouveaux événements maintenant pour visualiser l'alerte pour l'attaque précédemment lancée.



7. En cas le visualiseur, point culminant et cliquent avec le bouton droit l'alarme, puis sélectionnent la **mémoire tampon** ou la **vue NSDB de contexte de vue** pour visualiser plus d'informations détaillées au sujet de l'alarme.**Remarque:** Le NSDB est également accessible en ligne à l'encyclopédie Cisco Secure (clients enregistrés seulement).

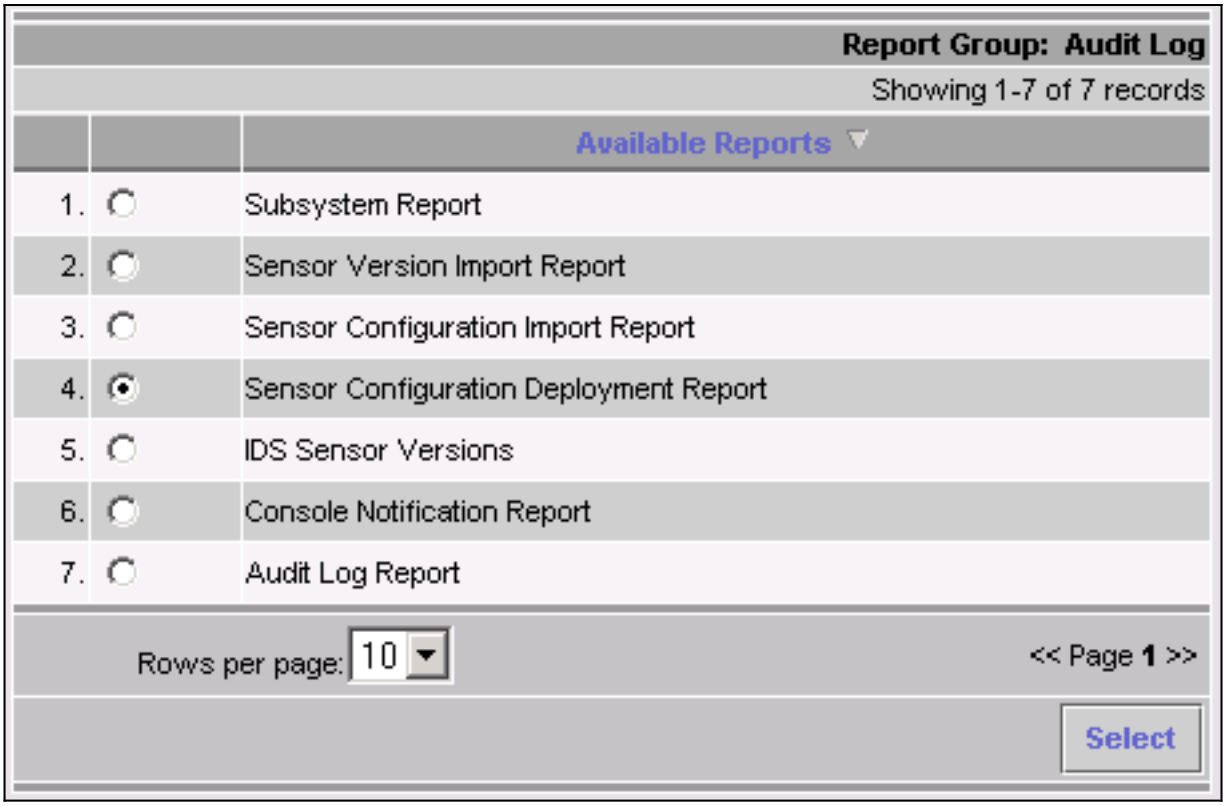


Dépannez

Procédure de dépannage

Utilisez la procédure suivante pour dépanner des buts.

1. Dans les ID MC, les **états** choisis **> se produisent**.Selon le type de problème, davantage de détail devrait être trouvé dans un des sept états disponibles.



2. Àla console de capteur, écrivez les **networkaccess de statistiques d'exposition de** commande et vérifiez la sortie pour s'assurer que le « état » est en activité.`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 que le paramètre de transmission prouve que le protocole correct est utilisé, comme le telnet ou le Protocole Secure Shell (SSH) avec 3DES.Vous pouvez essayer un SSH manuel ou le telnet d'un client SSH/Telnet sur un PC pour vérifier des qualifications de nom d'utilisateur et mot de passe sont correct. Vous pouvez alors essayer le telnet ou le SSH du capteur lui-même, au routeur, pour vous assurer peuvent ouvrir une session avec succès.

Informations connexes

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