VMS IDS MC を使用した IDS ブロッキングの設定

目次

概要

このドキュメントでは、VPN/Security Management Solution（VMS）、IDS Management Console（IDS MC）を使用したシスコ侵入検知システム（IDS）の設定例を紹介します。 この場合、IDS センサーから Cisco ルータへのブロッキングが設定されます。

前提条件

要件

ブロッキングを設定する前に、満たしましたこれらの状態を確認して下さい。

- センサーは必要なトラフィックを検知するためにインストールされ、設定されます。
- 探知インターフェイスはルータ outside インターフェイスに及ばれます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- IDS MC およびセキュリティ モニタ 1.2.3 の VM 2.2
- Cisco IDS センサー 4.1.3S(63)
- Cisco IOS® ソフトウェア リリース 12.3.5 を実行する Ciscoルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

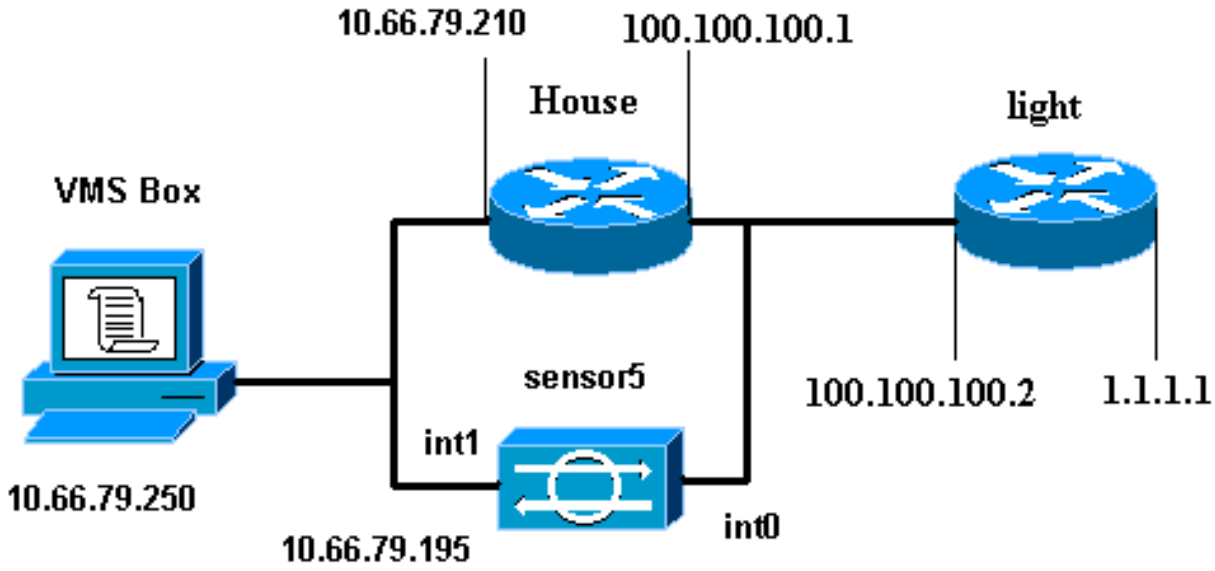
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次の図で示されるネットワーク構成を使用しています。



設定

このドキュメントでは、次に示す設定を使用しています。

- Router Light
- Router House

Router Light

```
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
```

Router 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
```

最初のセンサー設定

最初にセンサーを設定するためにこれらのステップを完了して下さい。

注: センサーの初期セットアップを実行された場合、IDS MC にセンサーをインポートするセクションに進んで下さい。

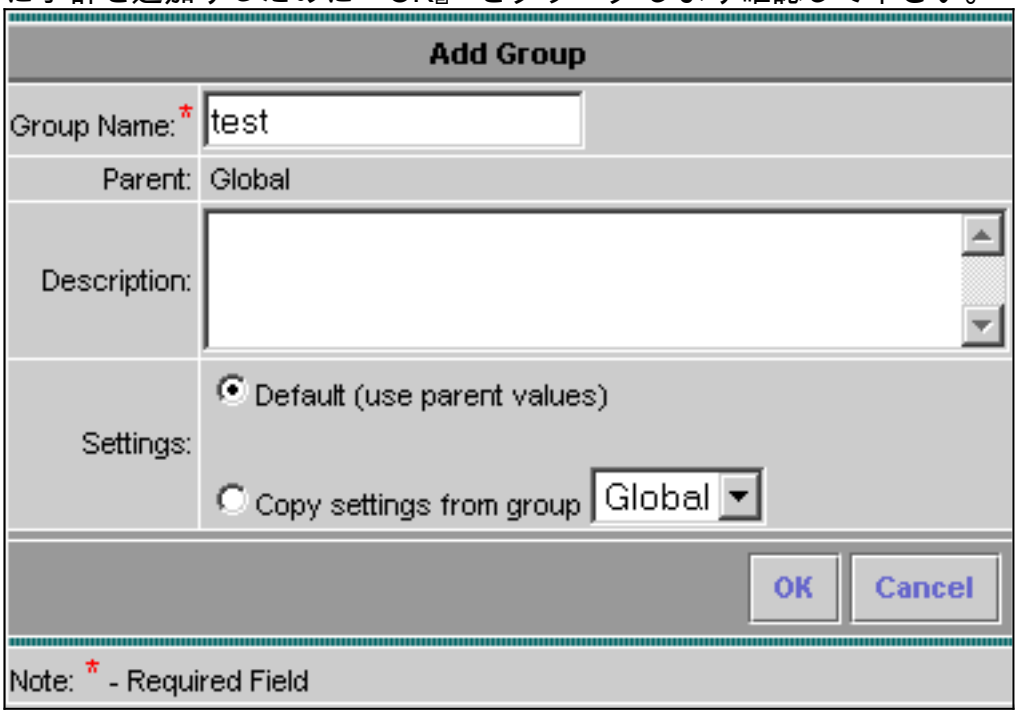
1. センサーにコンソール接続を行って下さい。ユーザ名とパスワードの入力を求められます。これが最初にあればセンサーにコンソール接続を行っています、ユーザ名 cisco およびパス

ワード cisco でログインして下さい。
2. パスワードを変更し、次に確認するために新しいパスワードを再びタイプするためにプロンプト表示されます。
3. **セットアップを**入力し、各敏速でこの例によってセンサーのための基本的なパラメータを、設定するために適切な情報を入力して下さい:`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. 設定を保存するために『2』 を押して下さい。

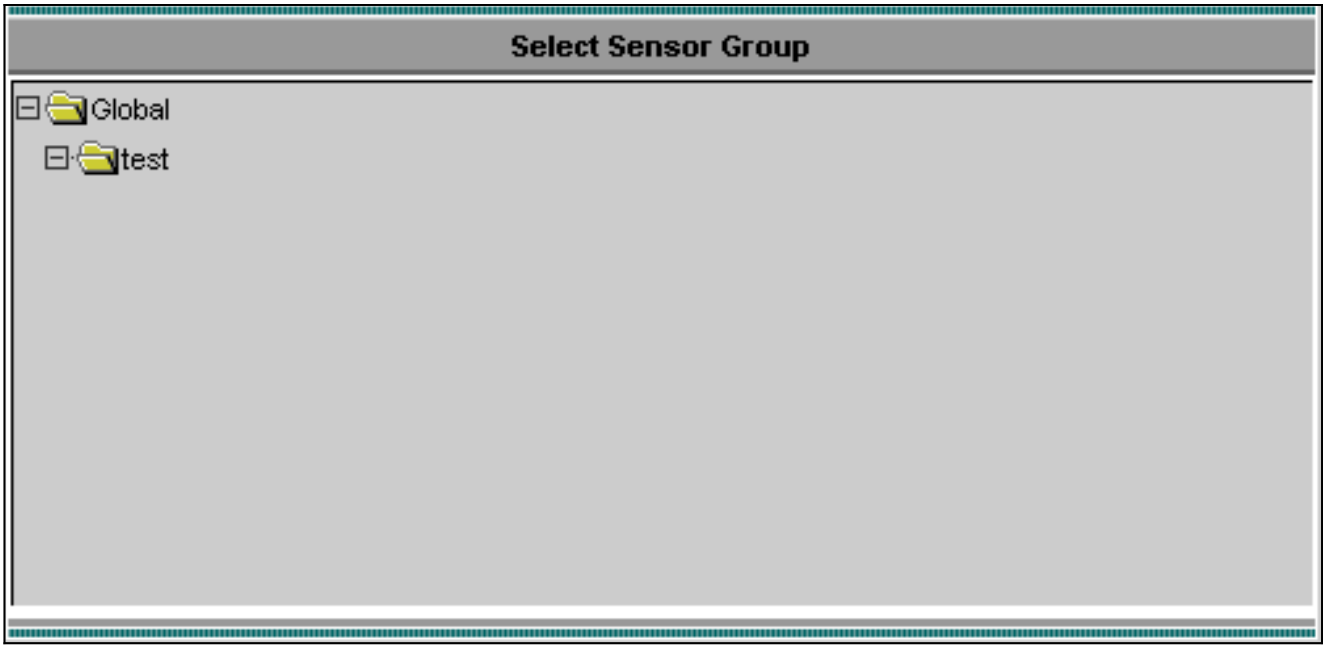
IDS MC にセンサーをインポートして下さい

IDS MC にセンサーをインポートするためにこれらのステップを完了して下さい。

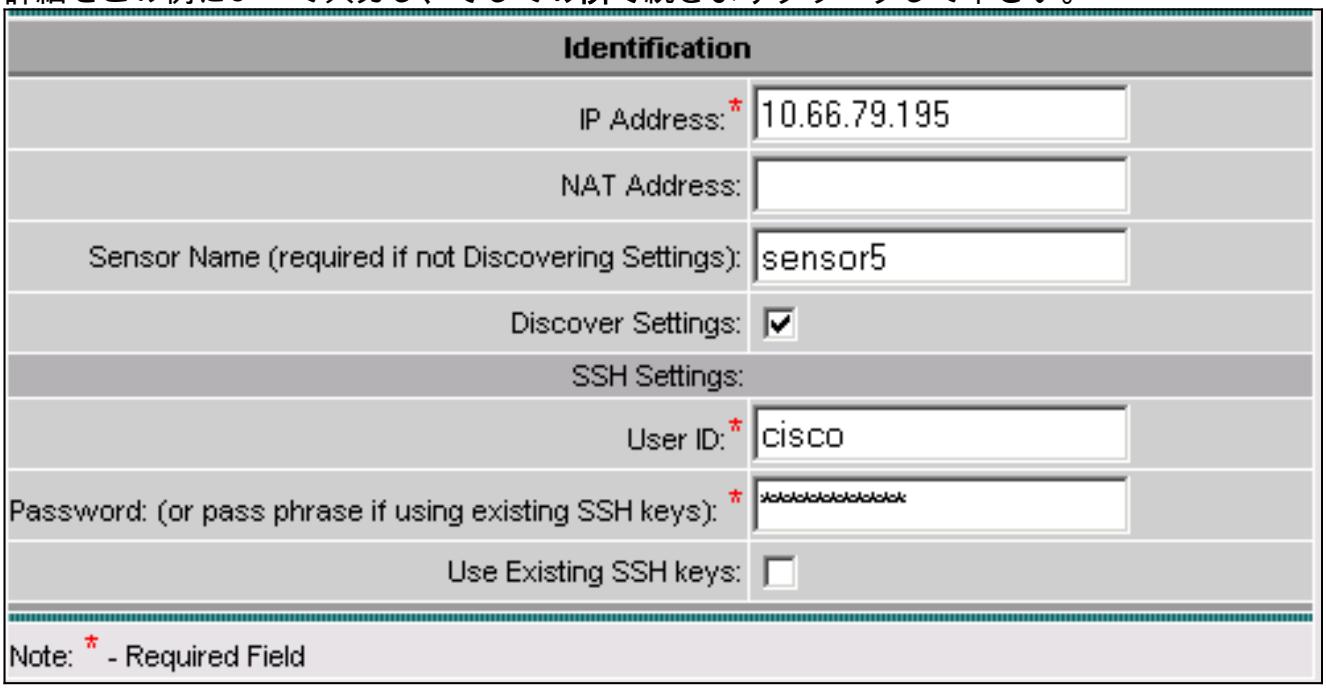
1. センサーに参照して下さい。この場合、**http://10.66.79.250:1741** か **https://10.66.79.250:1742** に参照して下さい。
2. 適切なユーザ名 および パスワードとログインして下さい。この例では、ユーザ名 **admin** およびパスワード **cisco は**使用されました。
3. VPN/Security Management Solution > Management Center の順に選択 し、『IDS Sensors』 を選択 して下さい。
4. Devices タブをクリックし、『Sensor Group』 を選択 し、**グローバル**強調表示し、『Create Subgroup』 をクリック して下さい。
5. グループ名を入力し、**DEFAULTオプション・ボタンを**選択されましたり、そして IDS MC に小群を追加するために『OK』 をクリック します確認して下さい。



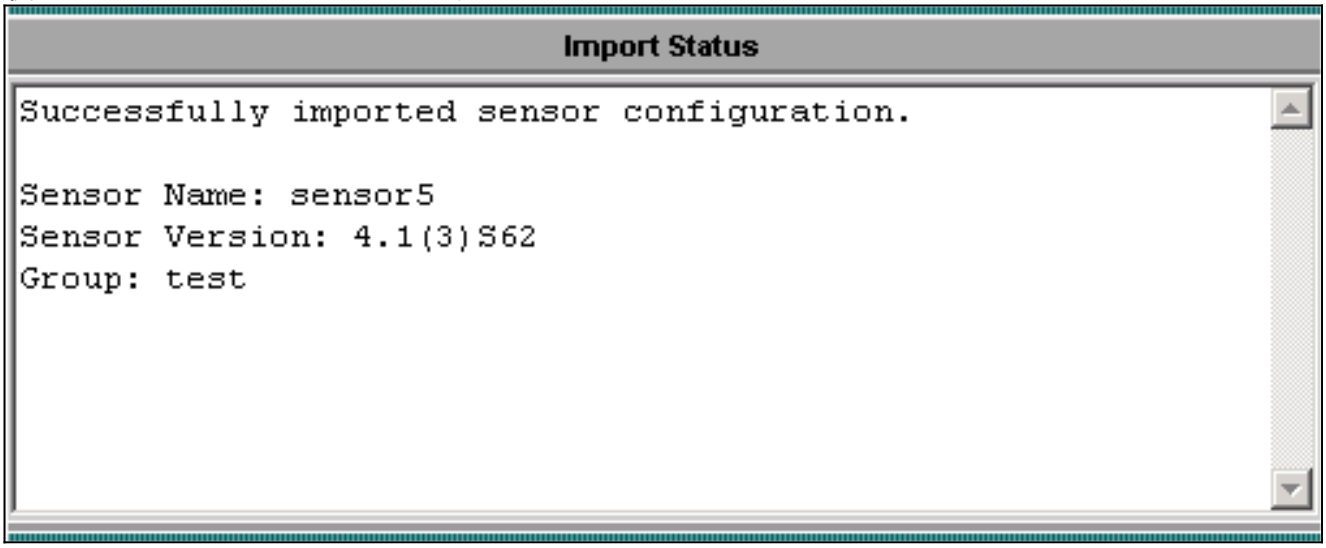
6. Devices > Sensor の順に選択 し、前のステップで作成される小群を (この場合、**テスト**) 強調表示し、『Add』 をクリック して下さい。
7. サブグループを強調表示し、『Next』 をクリック して下さい。



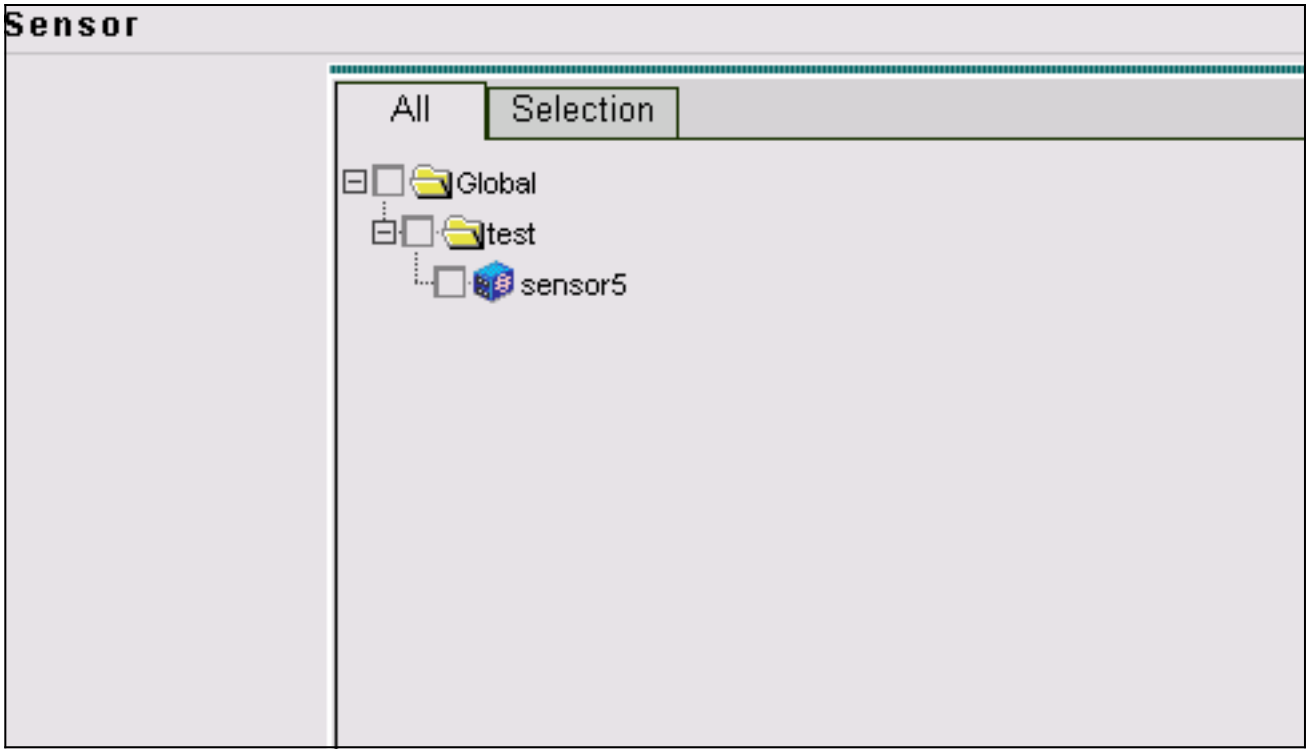
8. 詳細をこの例によって入力し、そして**の隣で**続きますクリックして下さい。



9. 状態がメッセージを記載した後、続くために『Finish』 をクリック して下さい。



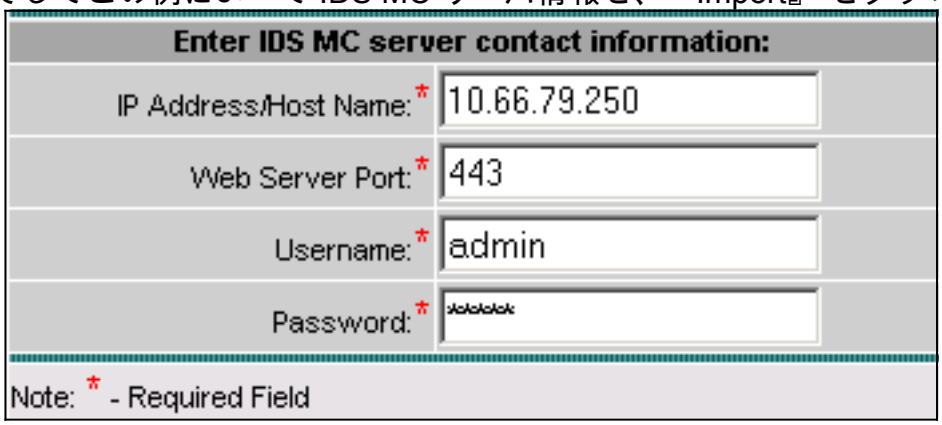
10. センサーは IDS MC にインポートされます。 この場合、sensor5 はインポートされます。



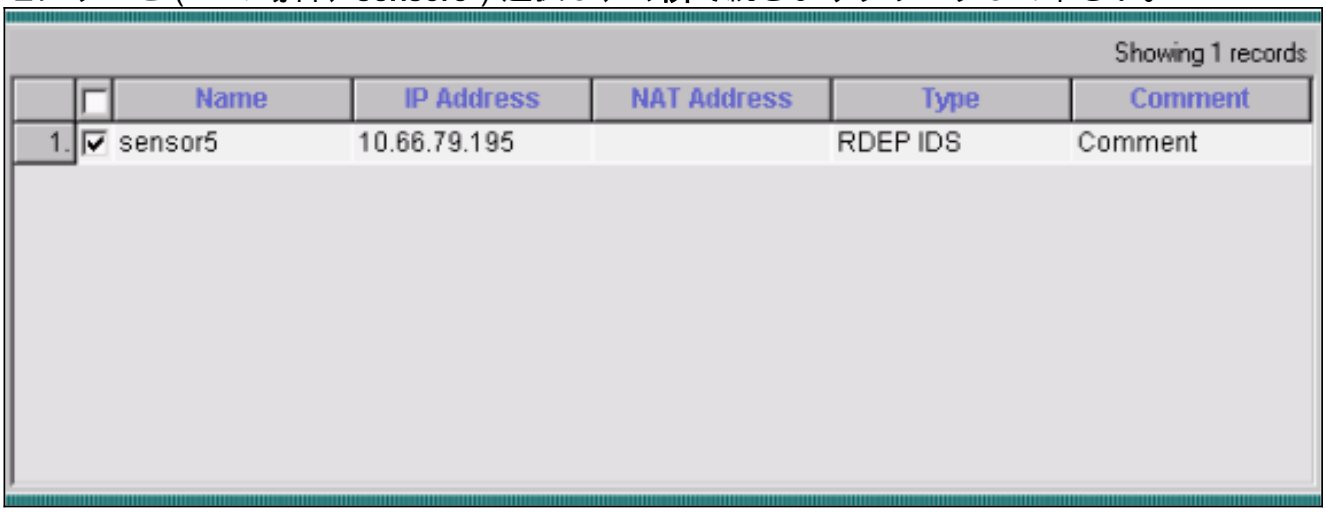
セキュリティ モニタにセンサーをインポートして下さい

セキュリティ モニタにセンサーをインポートするためにこのプロシージャを完了して下さい。

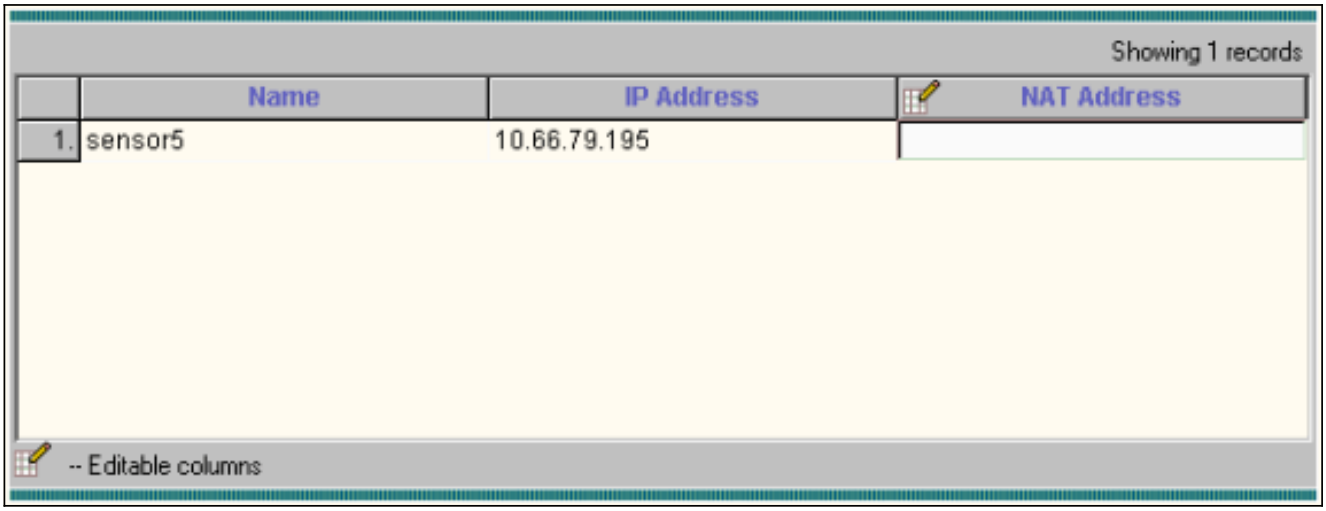
1. VMS Server メニューで、VPN/Security Management Solution > Monitoring Center > Security Monitor の順に選択 して下さい。
2. Devices タブを選択し、そしてこの例によって IDS MC サーバ情報を、『Import』 をクリック し、入力して下さい。



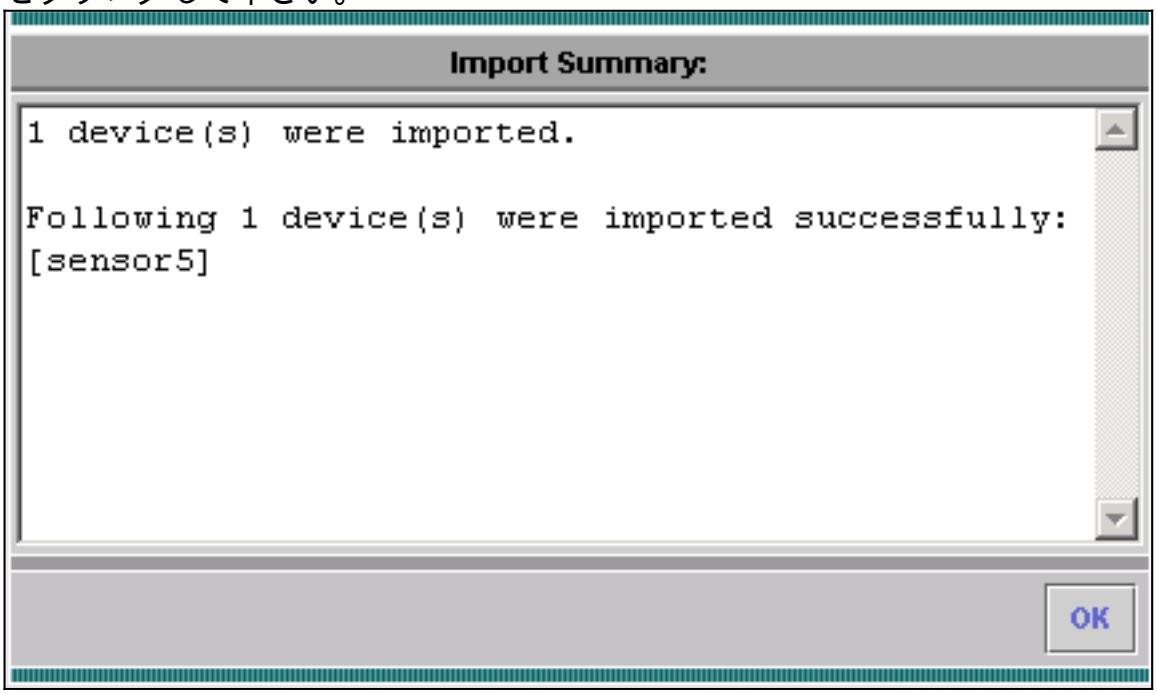
3. センサーを (この場合、**sensor5**) 選択し、**の隣で**続きますクリックして下さい。



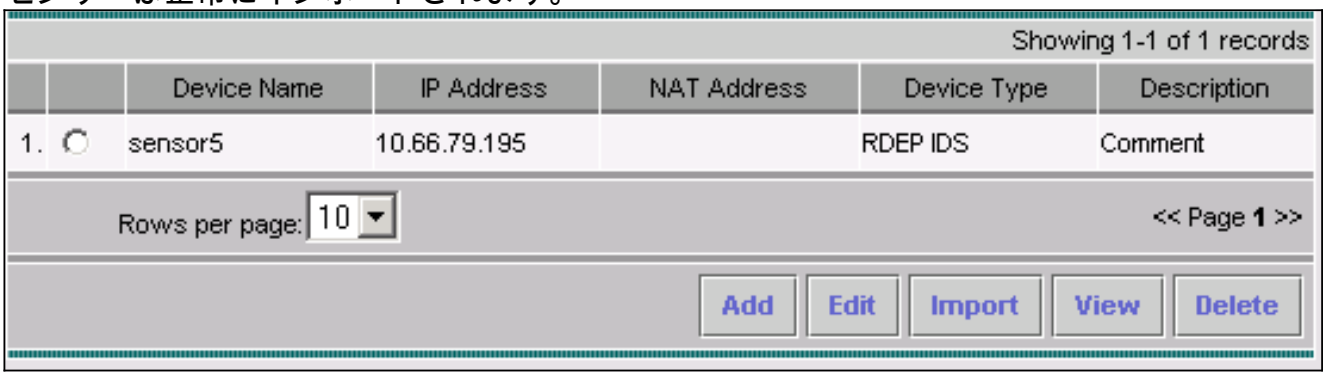
4. 必要であれば、センサーのためのネットワーク アドレス変換（NAT）アドレスをアップデートし、そして続くために『Finish』 をクリック して下さい。



5. セキュリティ モニタに IDS MC からセンサーをインポートすることを終わるために『OK』をクリック して下さい。



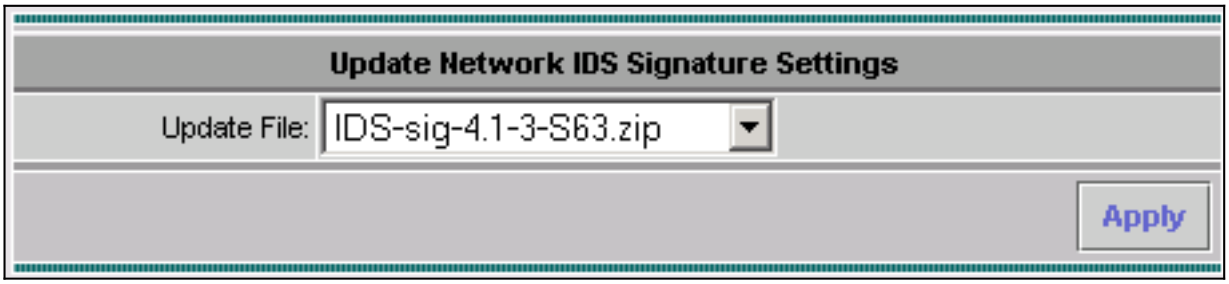
6. センサーは正常にインポートされます。



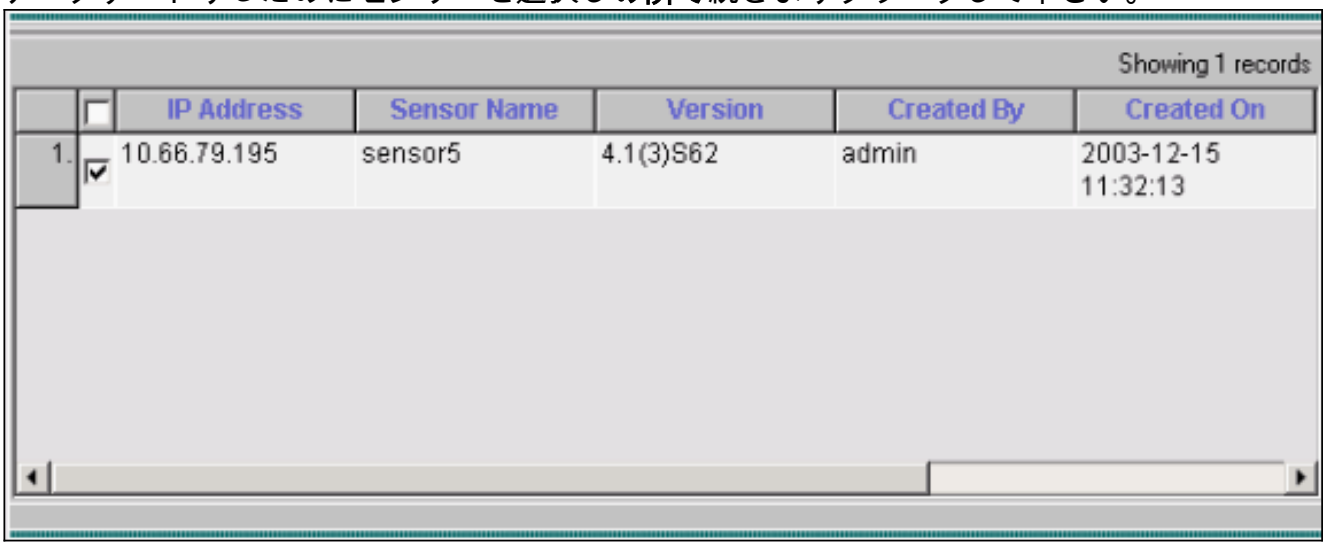
シグニチャアップデートのために IDS MC を使用して下さい

シグニチャアップデートのために IDS MC を使用するためにこのプロシージャを完了して下さい。

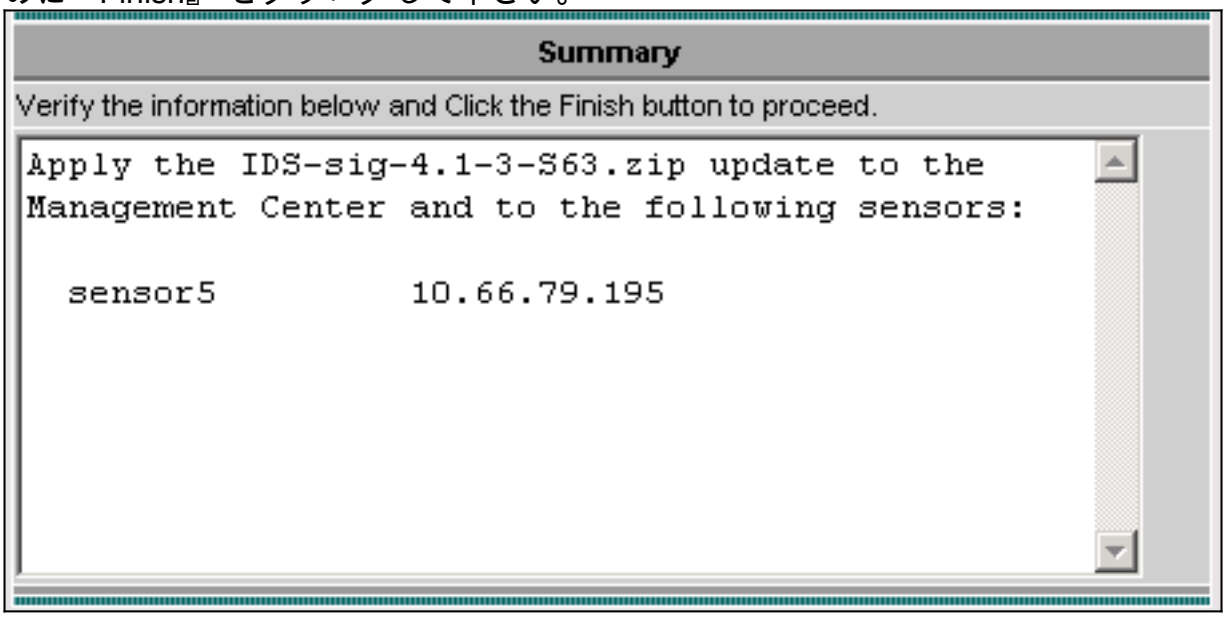
1. ネットワーク ID シグニチャアップデート（登録ユーザのみ）をダウンロードからダウンロードし、C:\PROGRA~1\CSCOpx\MDC\etc\ids\updates\ ディレクトリで VM サーバで保存して下さい。
2. VM サーバコンソールで、VPN/Security Management Solution > Management Center > Sensors の順に選択 して下さい。
3. Configuration タブをクリックし、『Updates』 を選択 し、『Update Network IDS Signatures』 をクリック して下さい。
4. ドロップダウン メニューからアップグレードし、続くために『Apply』 をクリック したいと思うシグニチャを選択して下さい。



5. アップデートするためにセンサーを選択し**の隣で**続きますクリックして下さい。



6. 管理センターにアップデート、またセンサーを加えるためにプロンプト表示された後続くために『Finish』 をクリック して下さい。



7. センサー コマンド ライン インターフェースに Telnet で接続するか、またはコンソール接続を行って下さい。 これと同じような情報は現われます:sensor5#

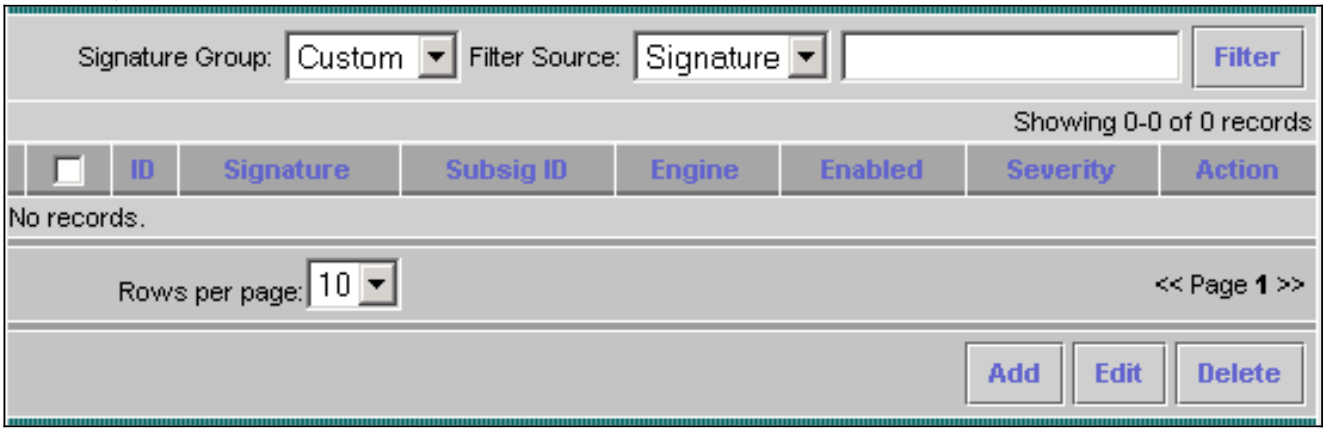
```
Broadcast message from root (Mon Dec 15 11:42:05 2003):
Applying update IDS-sig-4.1-3-S63. This may take several minutes. Please do not reboot the
sensor during this update. Broadcast message from root (Mon Dec 15 11:42:34 2003): Update
complete. sensorApp is restarting This may take several minutes.
```

8. アップグレードが完了するように数分間待ちそして確認するために **show version を**入力して下さい。`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`

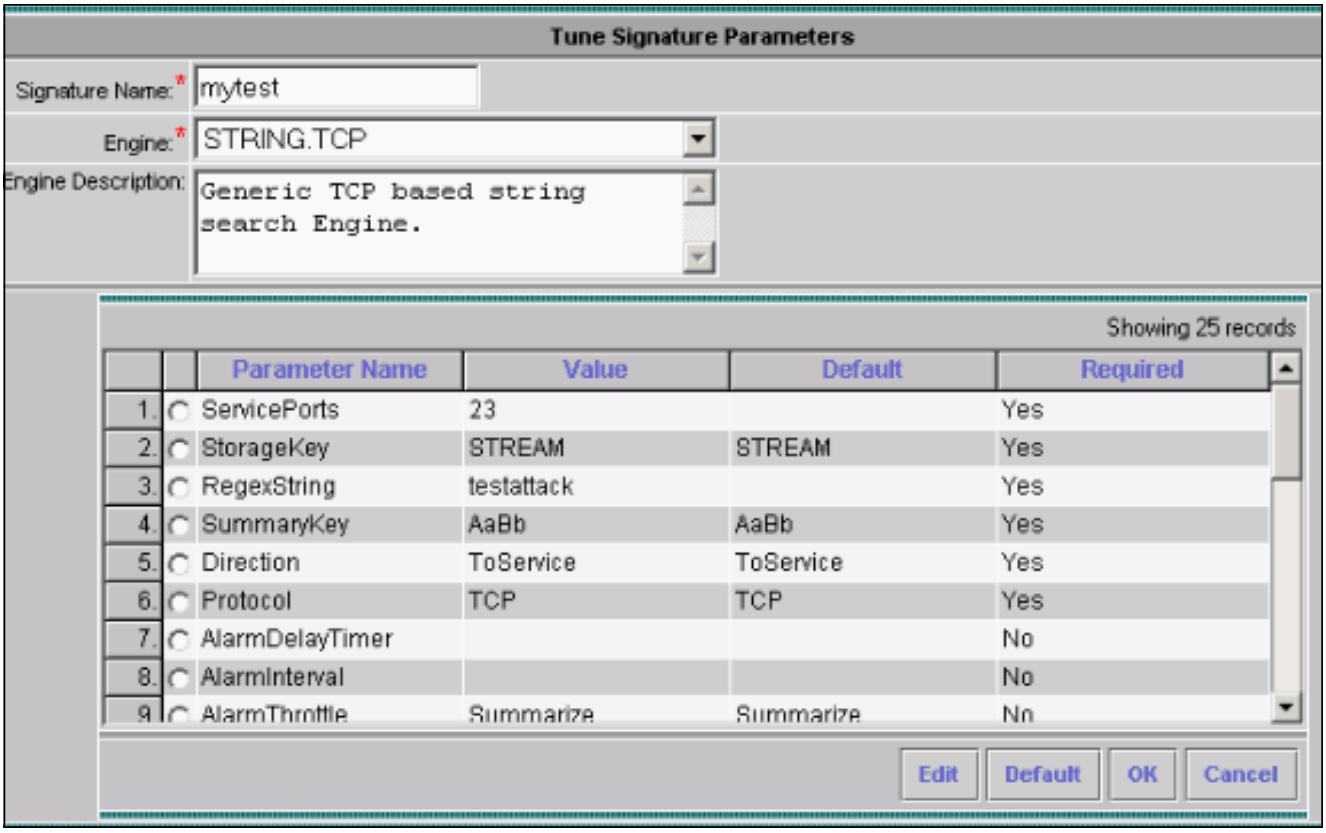
IOSルータのためのブロッキングを設定して下さい

IOSルータのためのブロッキングを設定するためにこのプロシージャを完了して下さい。

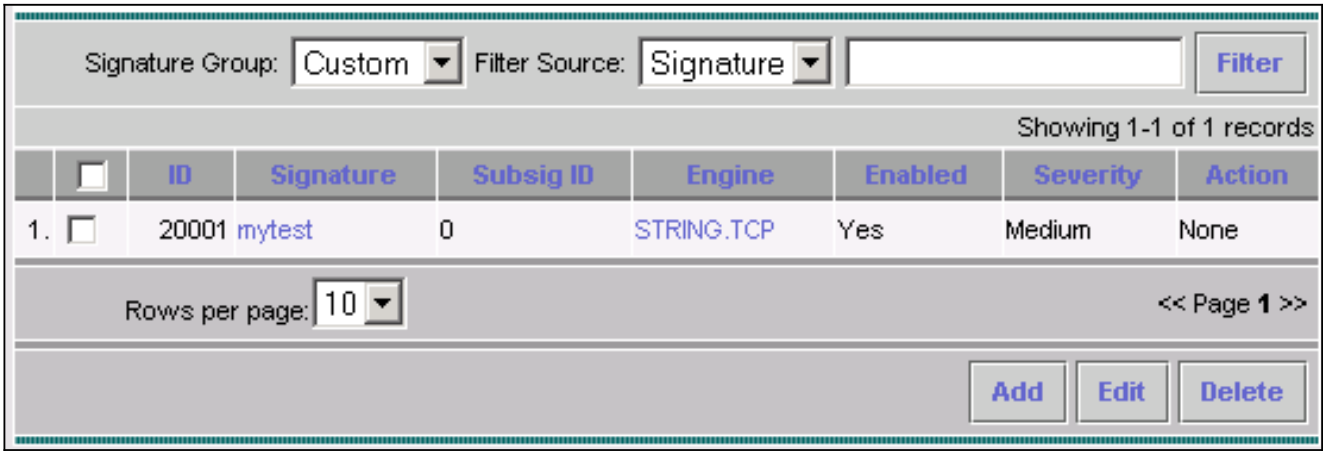
1. VM サーバコンソールで、VPN/Security Management Solution > Management Center > IDS Sensors の順に選択 して下さい。
2. Configuration タブを選択し、オブジェクト セレクタからセンサーを選択し、『Settings』をクリック して下さい。
3. 『Signatures』 を選択 して下さい新しいシグニチャを追加するために、『Custom』 をクリック し、そして『Add』 をクリック して下さい。



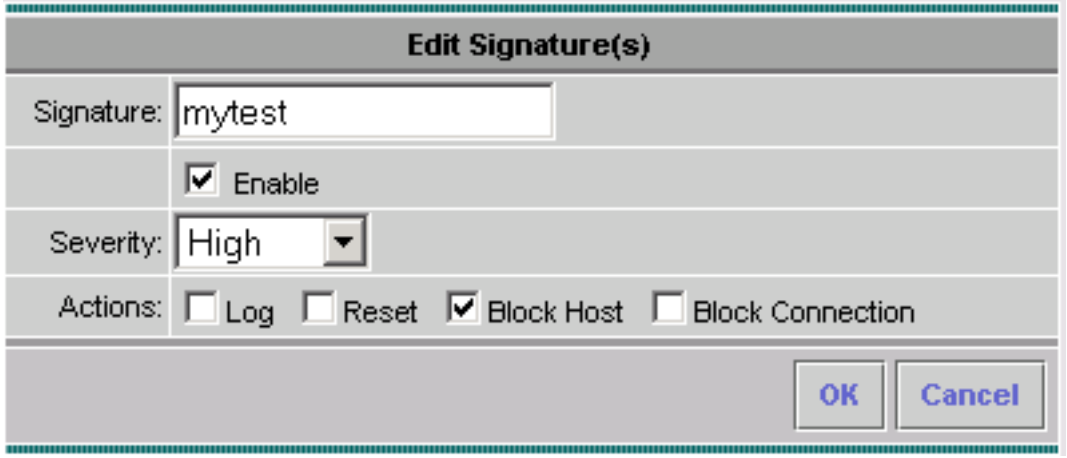
4. 新しいシグニチャ名前を入力し、そしてエンジンを選択して下さい（この場合、**STRING.TCP**）。
5. appropriate オプション・ ボタンをチェックすることおよび『Edit』 をクリック することによって利用可能 な パラメータをカスタマイズできます。この例では 23 に値を変更するために、ServicePorts パラメータは編集されます（23）ポートのために。 RegexString パラメータはまた値 **testattack を**追加するために編集されます。 これが完了するとき、続くために『OK』 をクリック して下さい。



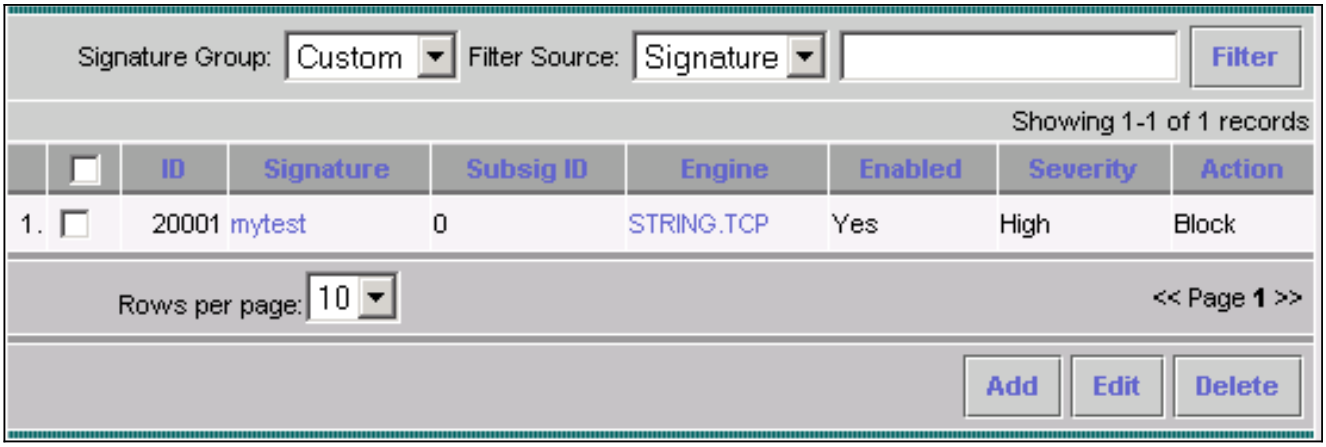
6. シグニチャ 重大度および操作を編集するか、またはシグニチャを有効または無効にするために、シグニチャの名前をクリックして下さい。



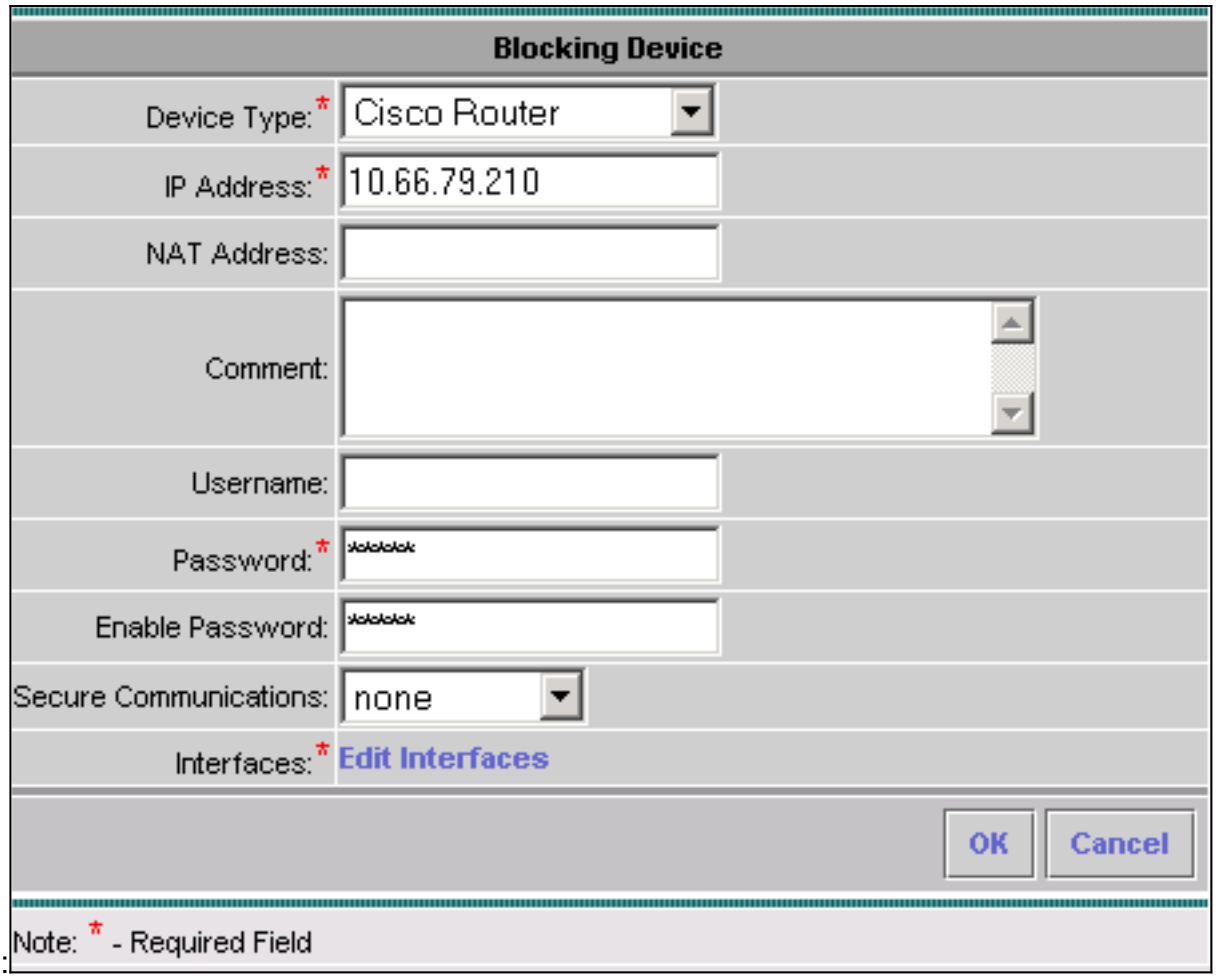
7. この場合、重大度は**最高**に変更され、**ブロック ホスト**操作は選択されます。 [OK] をクリックして、次に進みます。ブロック ホストは攻撃 IP ホストか IP サブネットをブロックします。ブロック接続ブロック TCP か UDP ポート (TCP または UDP 接続の攻撃に基づく) 。



8. 完全なシグニチャはこれに類似したに検知 します
:

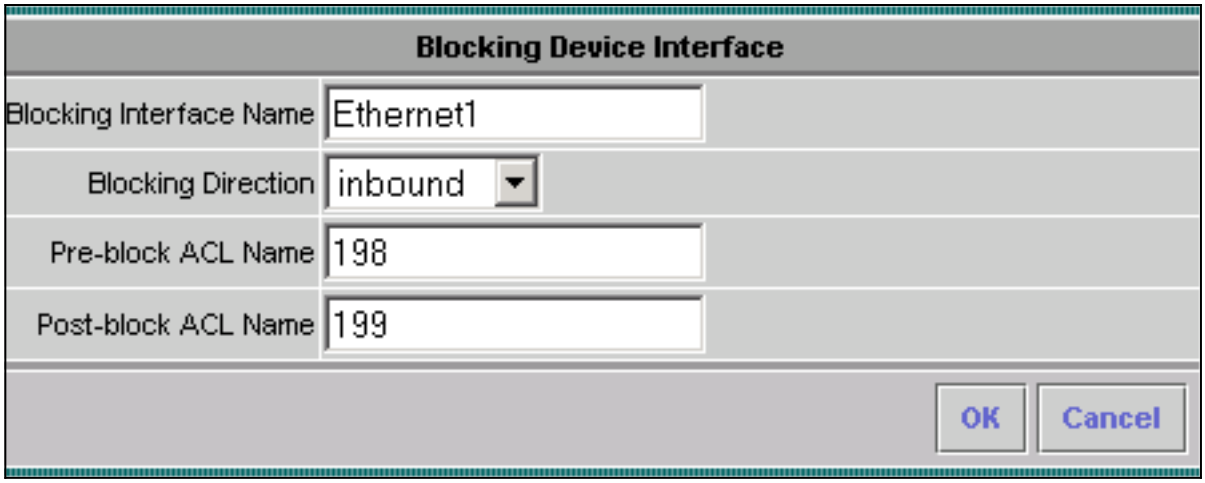


9. ブロック デバイスを設定するために、オブジェクト セレクタ (画面の左側のメニュー) から Blocking > Blocking Devices の順に選択 し、次の情報を入力するために『Add』 をクリック して下さい

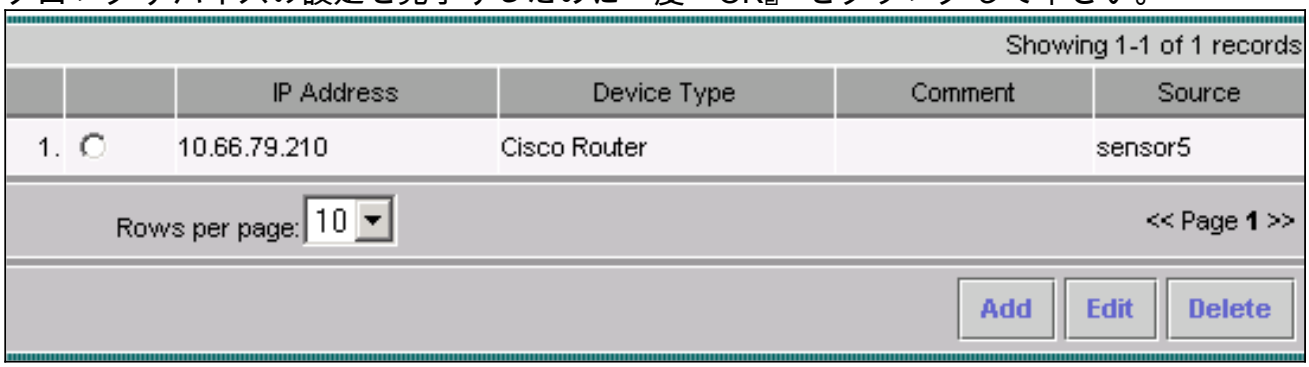


:

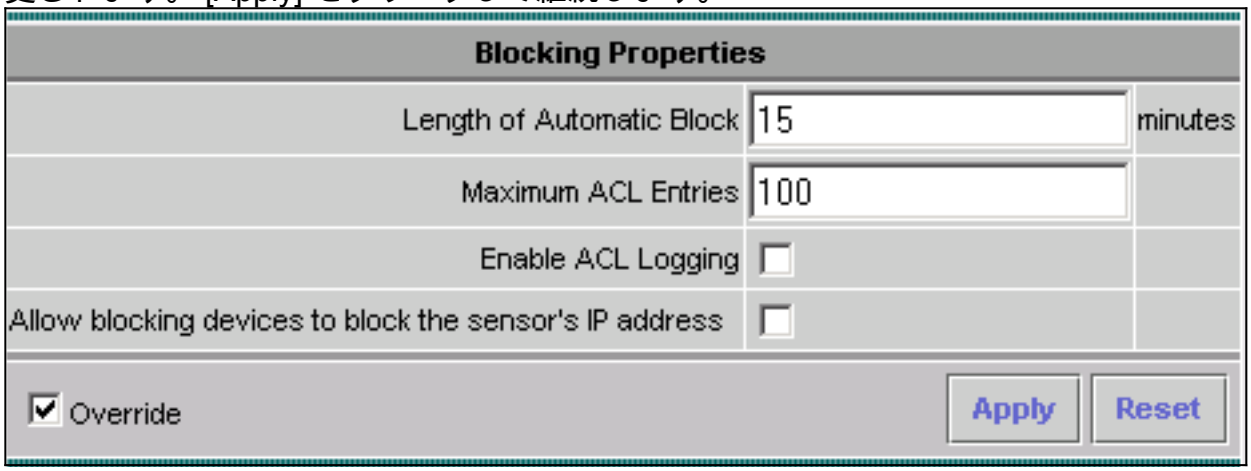
10. (前のスクリーンキャプチャーを参照して下さい) 『Edit Interfaces』 をクリック して下さい、『Add』 をクリック して下さい、この情報を入力し、そして続くために『OK』 をクリック して下さい。



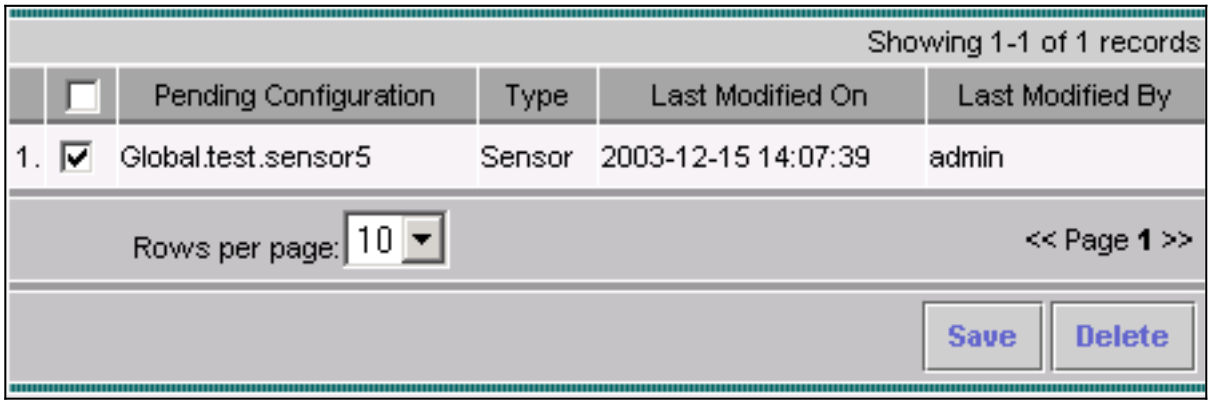
11. ブロック デバイスの設定を完了するために二度『OK』 をクリック して下さい。



12. ブロッキング Properties を設定するために、Blocking > Blocking Properties の順に選択 して下さい。自動ブロックの長さは修正することができます。 この場合、それは **15 分**に変更されます。 [Apply] をクリックして継続します。

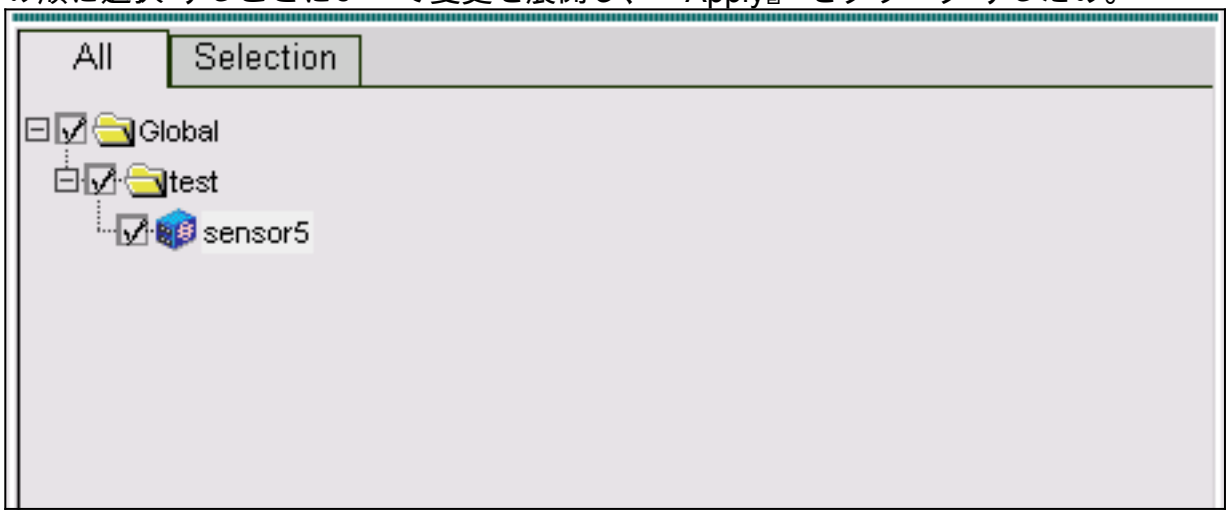


13. メインメニューから『Configuration』 を選択 し、そして保留中の設定を『Pending』 を選択 して下さい、それを正しいです確認し、『SAVE』 をクリック するためにチェックして下さい。

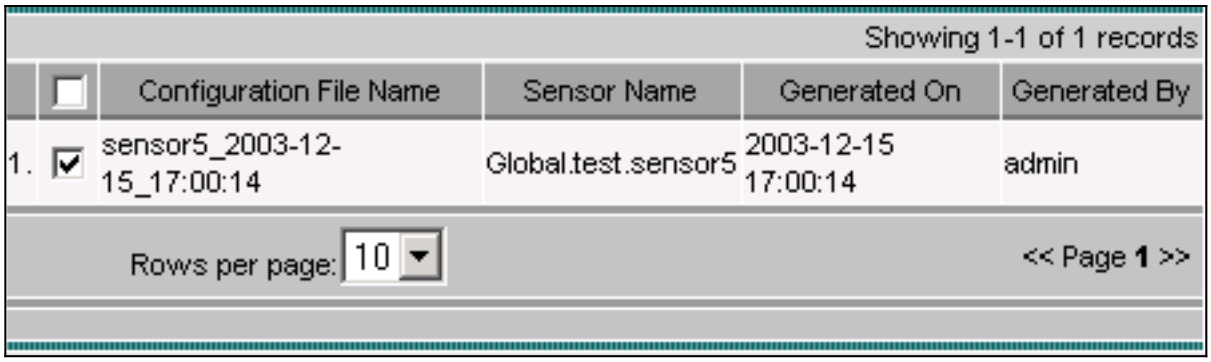


14. 次にコンフィギュレーション変更をセンサー、生成するに押し、Deployment > Generate

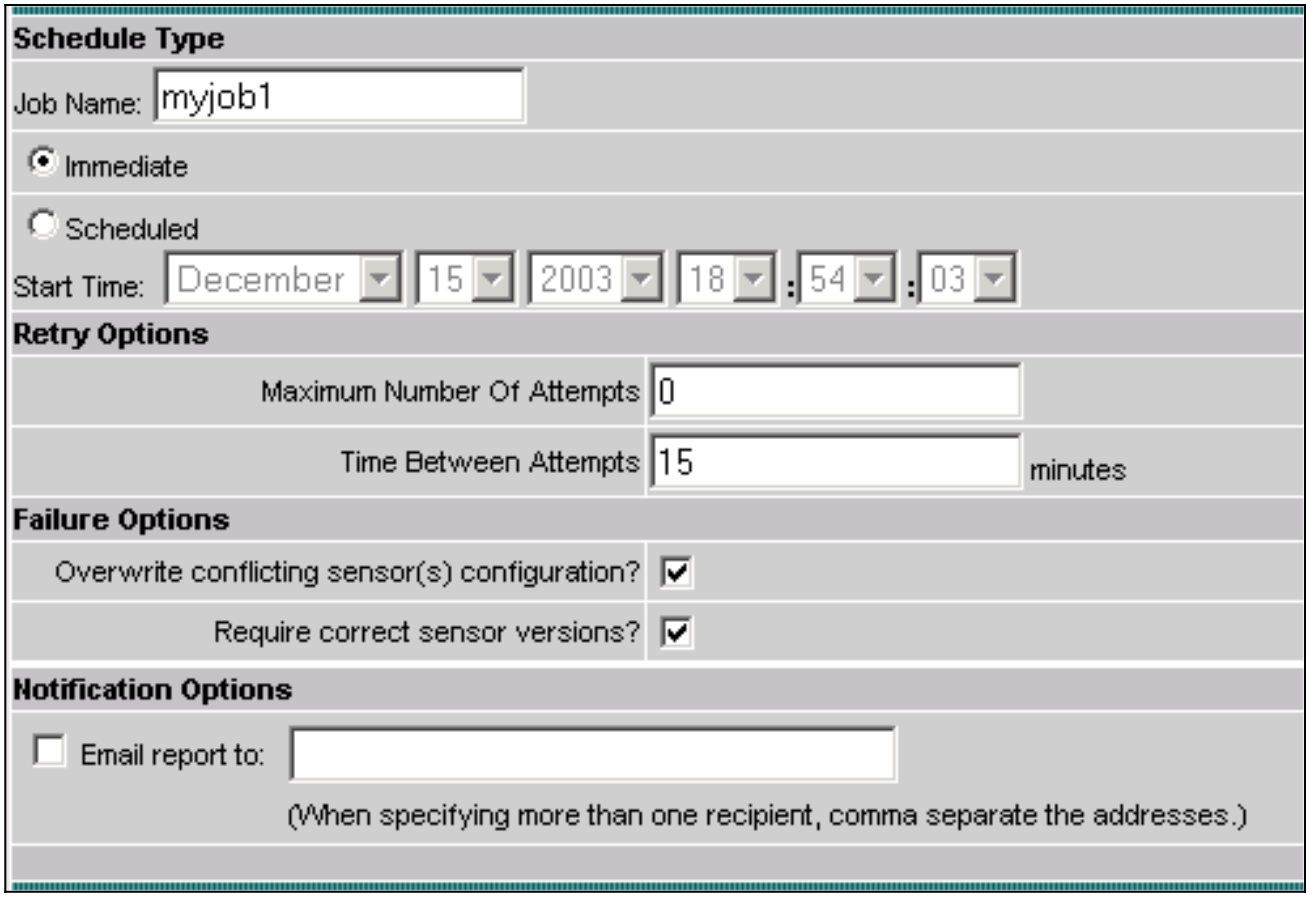
の順に選択 することによって変更を展開し、『Apply』 をクリック するため。



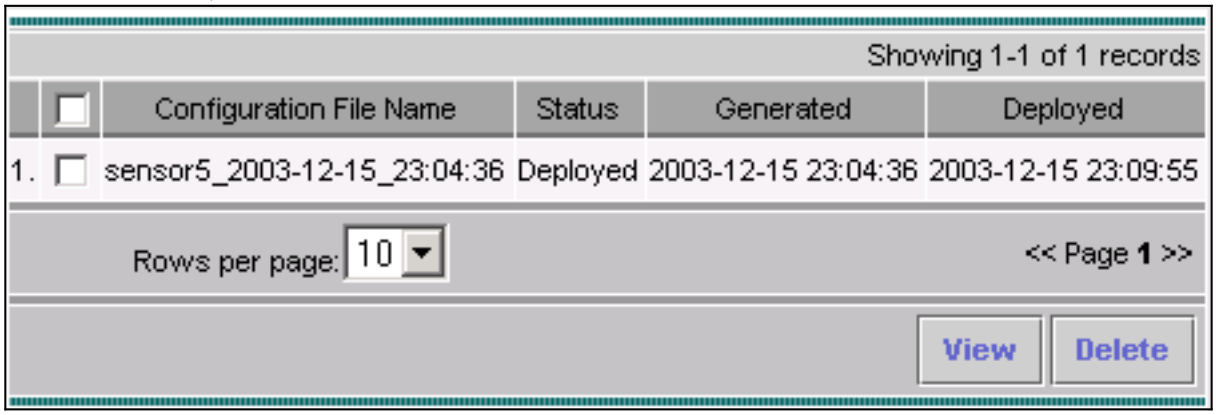
15. Deployment > Deploy の順に選択 し、そして『SUBMIT』 をクリック して下さい。
16. チェックボックスをセンサーの隣でチェックし、そして『Deploy』 をクリック して下さい。
17. チェックボックスをキューのジョブがあるように確認し、そして**の隣で**続きますクリック して下さい。



18. ジョブ 名を入力し、即時ようにジョブをスケジュールし、そして『Finish』 をクリック して下さい。



19. Deployment > Deploy > Pending の順に選択 して下さい。すべての保留中のジョブが完了するまで数分間待って下さい。 キューはそれから空です。
20. 配備を確認するために、**Configuration> 履歴を**選択して下さい。設定のステータスを表示する**展開される**ように確認して下さい。 これはセンサー設定がアップデートに成功したことを意味します。



確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

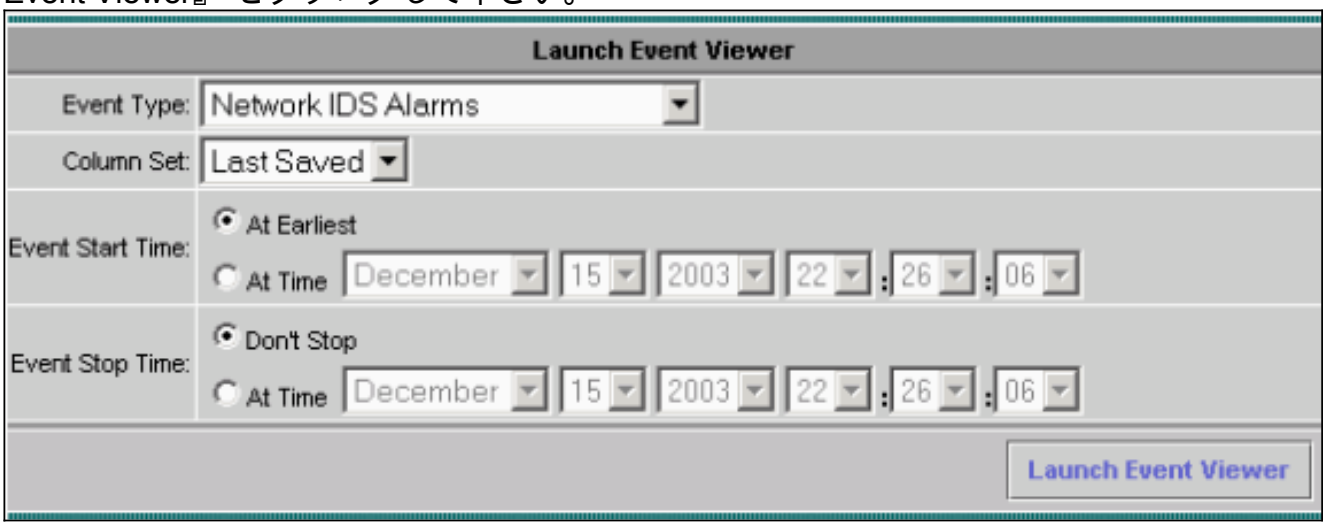
特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

攻撃およびブロッキングを起動させて下さい

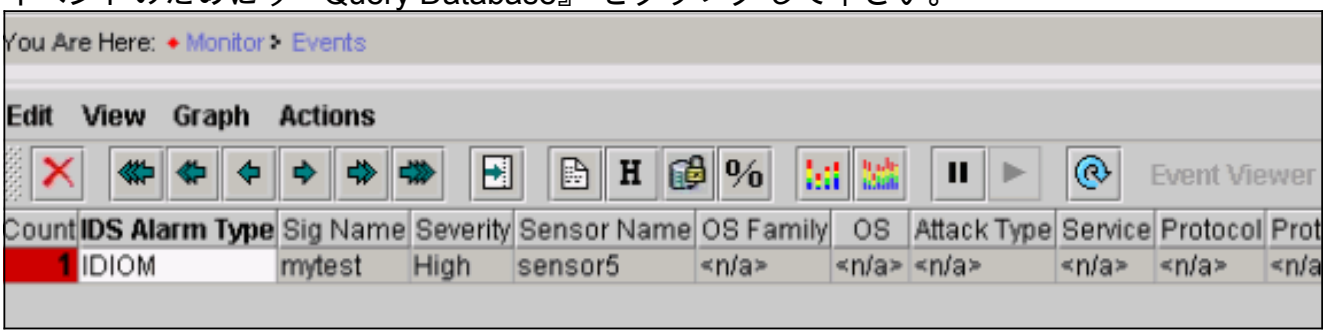
ブロッキング プロセスが正しくはたらいていることを確認するために、テスト攻撃を開始し、結

果をチェックして下さい。

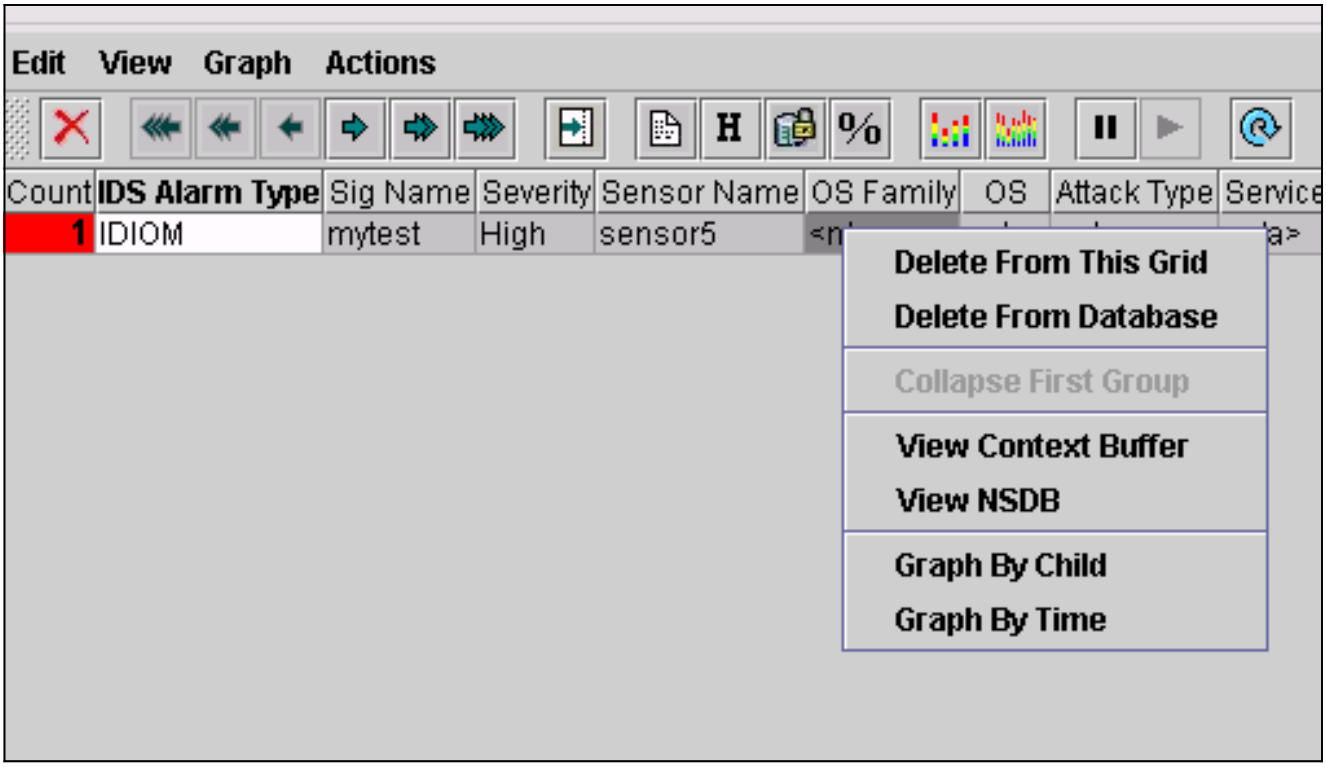
1. 攻撃を開始する前に、VPN/Security Management Solution > Monitoring Center > Security Monitor の順に選択 して下さい。
2. メインメニューから『Monitor』 を選択 し、『Events』 をクリック し、それから『Launch Event Viewer』 をクリック して下さい。



3. センサーからの通信を確認するためにルータに（この場合、家ルータへの Telnet）、Telnet で接続して下さい。`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. 攻撃を開始するために、1 つのルータから他に Telnet で接続し、**testattack を**入力して下さい。この場合、軽いルータから家ルータに接続するのに Telnet を使用しました。 押すとすぐ testattack を入力した後 **<space> か <enter> は**、Telnetセッション リセットする必要があります。`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. ルータ（家）に Telnet で接続し、コマンド **show access-list を**入力して下さい。`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. イベント ビューアから、以前に開始された攻撃のためのアラートを表示するために新しいイベントのために今『Query Database』 をクリック して下さい。



7. イベント ビューアでは、強調表示し、アラームを右クリックしか、そしてアラームについての詳細な情報を表示するために **NSDB を**『View Context Buffer』 を選択 するまたは**表示して下さい。注:** NSDB は Cisco Secure 百科事典（登録ユーザのみ）でまたオンラインで手続きできます。

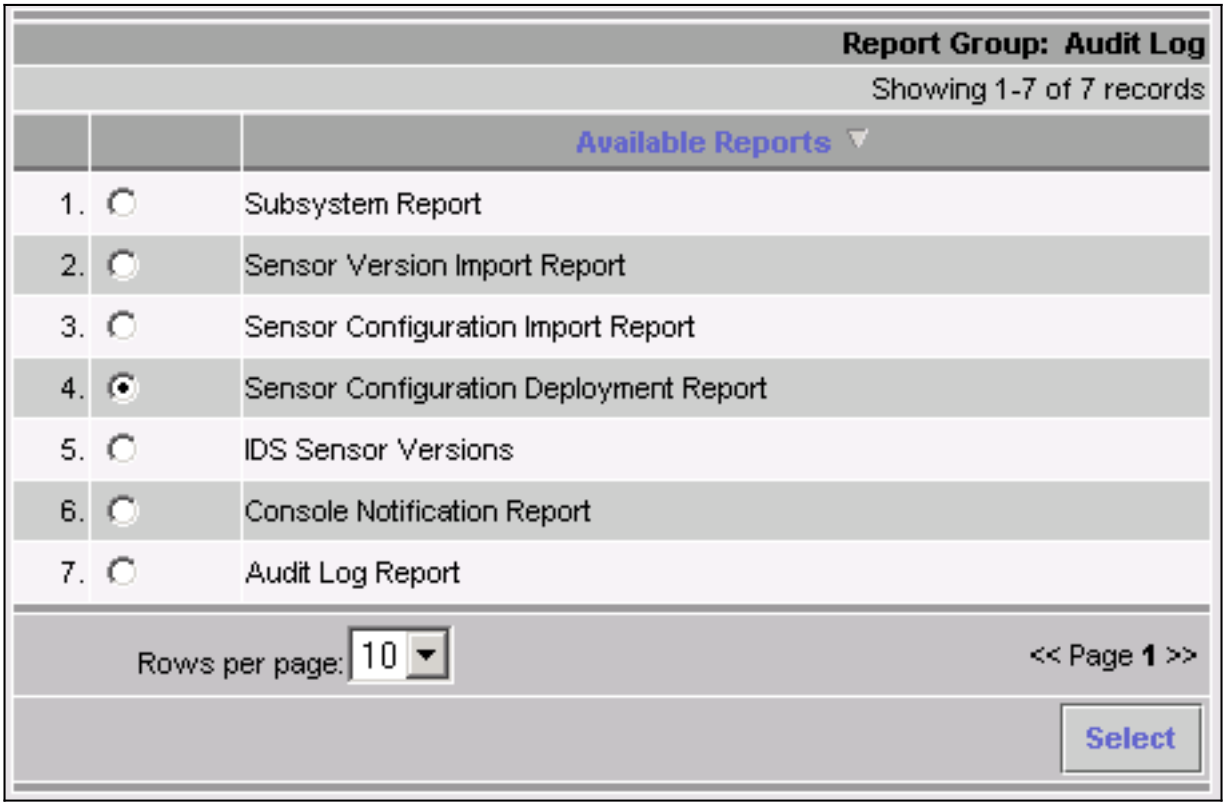


トラブルシューティング

トラブルシューティング手順

トラブルシューティングを行うのに次のプロシージャを使用して下さい。

1. IDS MC では、Reports > Generate の順に選択 して下さい。問題のタイプによって、更に詳しい情報は 7 つの利用可能 なレポートの 1 つで見つける必要があります。



2. センサー コンソールで、コマンド **show statistics networkaccess** を入力し、「状態」を確認するために出力をですアクティブ チェックして下さい。`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. 正しいプロトコルが使用されているトリプル DES の Telnet かセキュア シェル（SSH）のようなことを通信パラメータを示します、確認して下さい。手動 SSH を試みることができますまたはユーザ名 および パスワード 資格情報をチェックするために PC の SSH/Telnet クライアントから Telnet で接続するために正しくであって下さい。 それから Telnet を試みることができますまたはセンサーからの SSH 自体は、ルータへ、確認するために正常に口グインできます。

関連情報

- Cisco Secure Intrusion Detection のサポートページ
- CiscoWorks VPN/Security Management Solution サポート
- テクニカルサポートとドキュメント - Cisco Systems