

VMS IDS MC を使用した IDS TCP リセットの設定

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[最初のセンサー設定](#)

[IDS MC 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 を使用して下さい](#)

[IOSルータのための TCP Reset を設定して下さい](#)

[確認](#)

[不正侵入および TCP Reset の起動](#)

[トラブルシューティング](#)

[トラブルシューティング手順](#)

[関連情報](#)

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 TCP リセットが設定されます。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- 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べれます。

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。

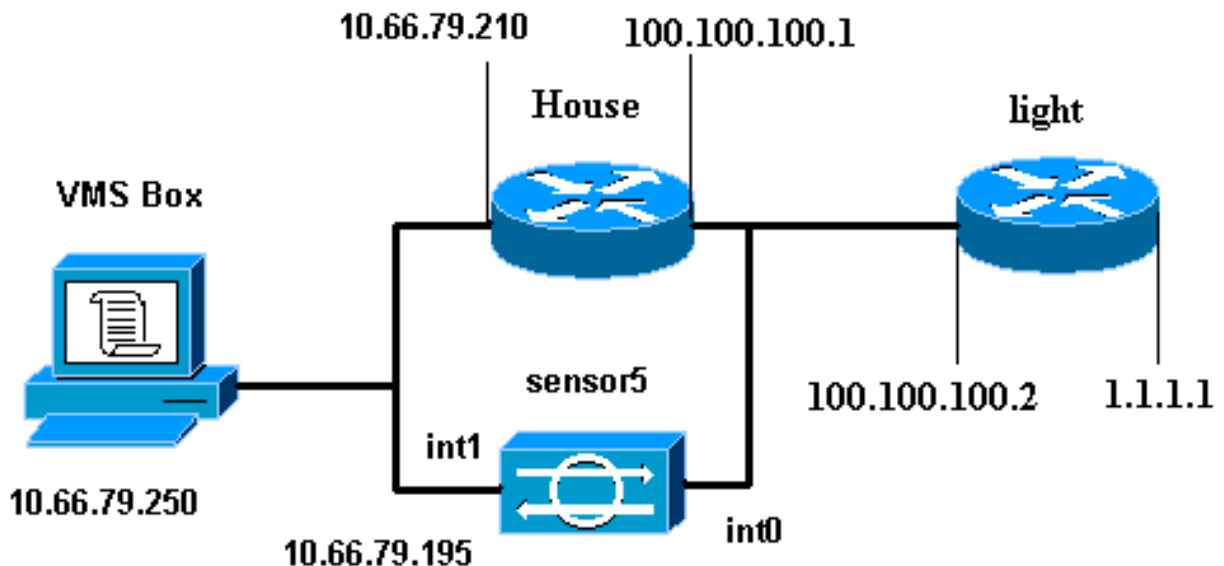
設定

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: このセクション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、次の設定を使用します。

- [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 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
```

最初のセンサー設定

注: 既にセンサーの初期セットアップを実行された場合、[センサーは IDS MC セクション インポート](#)に進みます。

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。これが最初で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、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 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
```

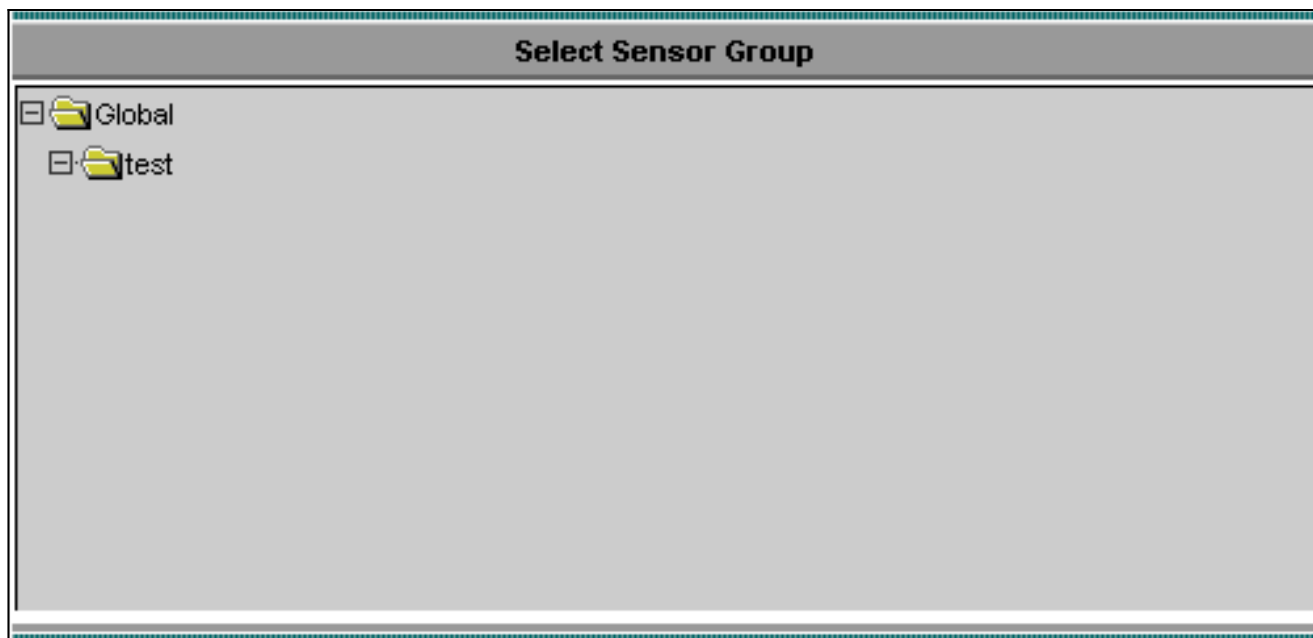
IDS MC にセンサーをインポートして下さい

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>。
2. 適切なユーザ名 および パスワードのログイン。この例では、ユーザ名は **admin** であり、パスワードは **cisco** です。
3. VPN/Security Management Solution > Management Center の順に選択し、『IDS Sensors』をクリックして下さい。
4. Devices タブをクリックし、『Sensor Group』を選択して下さい。
5. グローバル強調表示し、『Create Subgroup』をクリックして下さい。
6. グループ名を入力し、そして IDS MC にサブグループを追加するために『OK』をクリックします **デフォルトが選択されるようにして下さい**。

Add Group	
Group Name: *	test
Parent:	Global
Description:	
Settings:	<input checked="" type="radio"/> Default (use parent values) <input type="radio"/> Copy settings from group Global
OK Cancel	
Note: * - Required Field	

7. 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。
8. サブグループを強調表示し、『Next』をクリックして下さい。

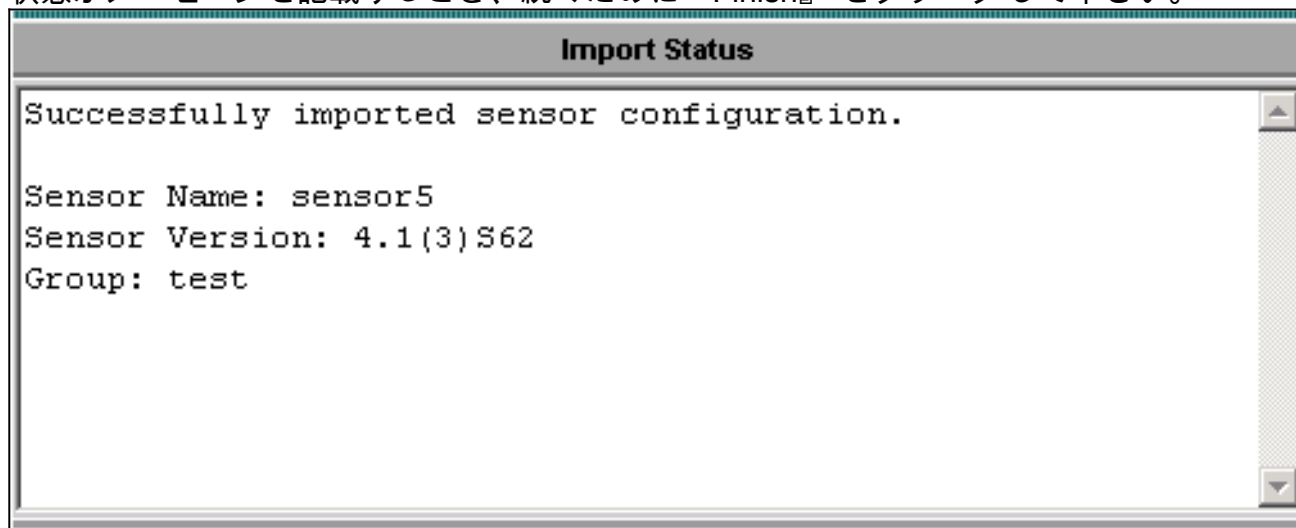


9. 詳細をこの例によって入力し、続くために『Next』をクリックして下さい。

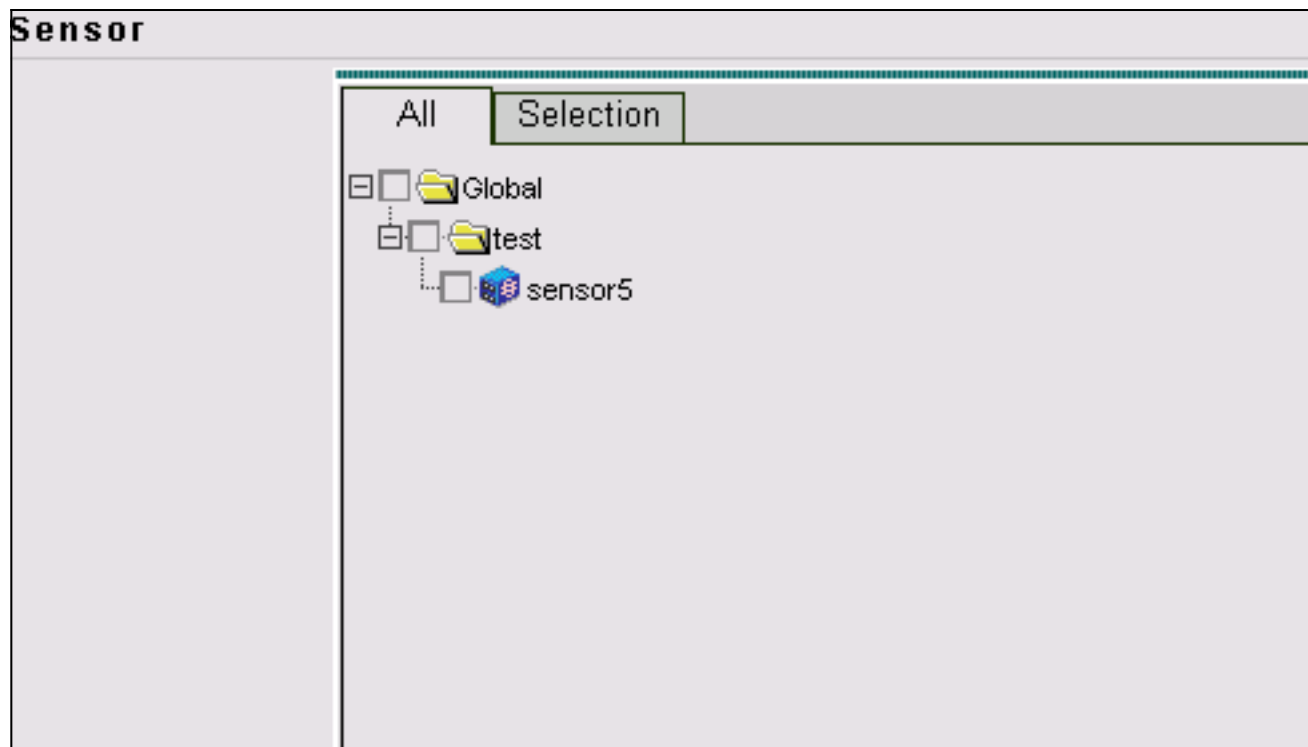
Identification	
IP Address: *	<input type="text" value="10.66.79.195"/>
NAT Address:	<input type="text"/>
Sensor Name (required if not Discovering Settings):	<input type="text" value="sensor5"/>
Discover Settings:	<input checked="" type="checkbox"/>
SSH Settings:	
User ID: *	<input type="text" value="cisco"/>
Password: (or pass phrase if using existing SSH keys): *	<input type="password" value="XXXXXXXXXXXX"/>
Use Existing SSH keys:	<input type="checkbox"/>

Note: * - Required Field

10. 状態がメッセージを記載するとき、続くために『Finish』をクリックして下さい。



11. 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れらのステップを完了して下さい。

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

Enter IDS MC server contact information:	
IP Address/Host Name: *	<input type="text" value="10.66.79.250"/>
Web Server Port: *	<input type="text" value="443"/>
Username: *	<input type="text" value="admin"/>
Password: *	<input type="password" value="XXXXXXXX"/>
Note: * - Required Field	

クシ、入力して下さい。

3. センサーを (この場合、**sensor5**) 選択し、続くために『Next』 をクリックして下さい。

Showing 1 records						
	<input type="checkbox"/>	Name	IP Address	NAT Address	Type	Comment
1.	<input checked="" type="checkbox"/>	sensor5	10.66.79.195		RDEP IDS	Comment

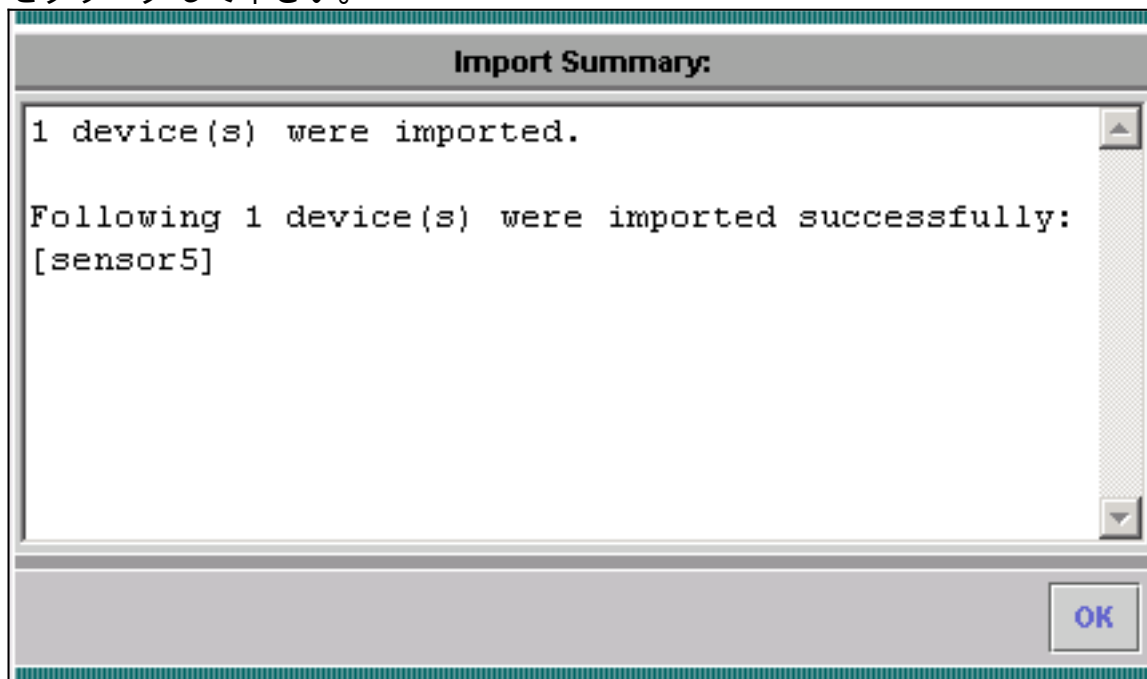
4. もし必要なら、センサーのための NAT アドレスをアップデートし、そして続けるために『Finish』 をクリックして下さい。

	Name	IP Address	NAT Address
1.	sensor5	10.66.79.195	

Showing 1 records

-- Editable columns

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. 今センサーが正常にインポートされることがわかります

	Device Name	IP Address	NAT Address	Device Type	Description
1.	sensor5	10.66.79.195		RDEP IDS	Comment

Showing 1-1 of 1 records

Rows per page: 10

<< Page 1 >>

Add Edit Import View Delete

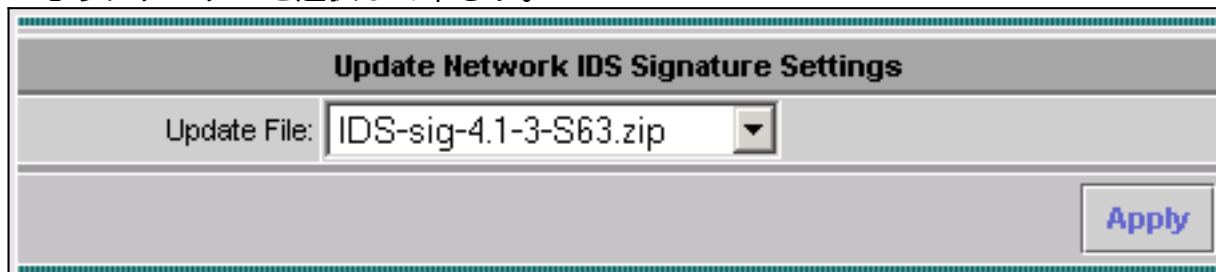
[シグニチャアップデートのために IDS MC を使用して下さい](#)

このプロシージャはシグニチャアップデートのために IDS MC を使用する方法を説明します。

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

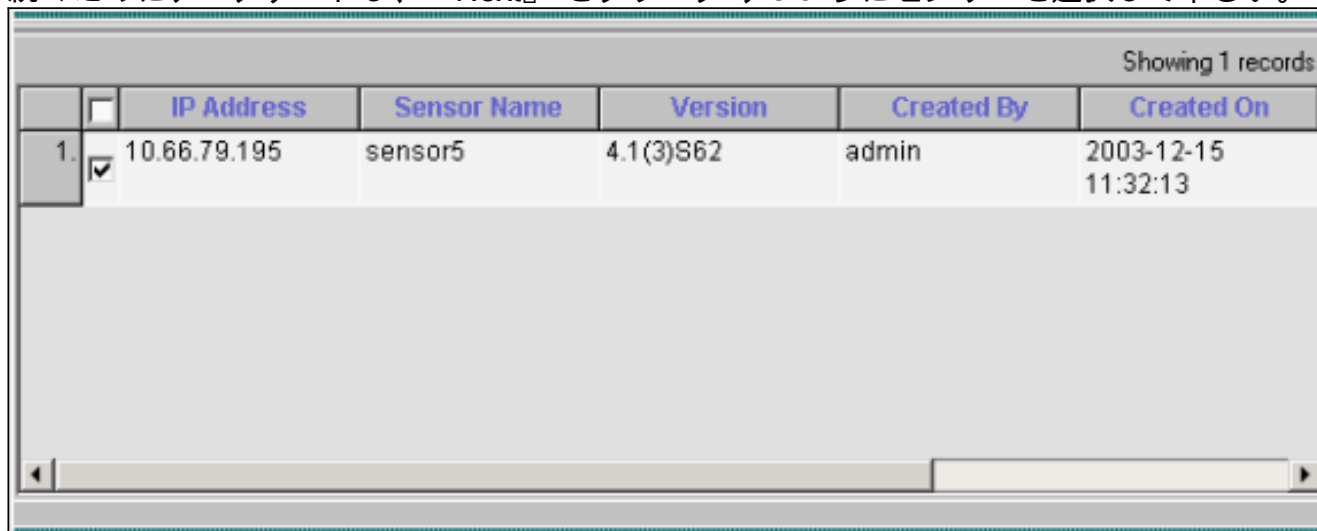
2. VM サーバコンソールで、VPN/Security Management Solution > Management Center > IDS Sensors の順に選択して下さい。
3. Configuration タブを選択し、『Updates』をクリックして下さい。
4. 『Update Network IDS Signatures』をクリックして下さい。
5. ドロップダウンメニューからアップグレードし、続かために『Apply』をクリックしたいと思うシグニチャを選択して下さい。



Update Network IDS Signature Settings

Update File:

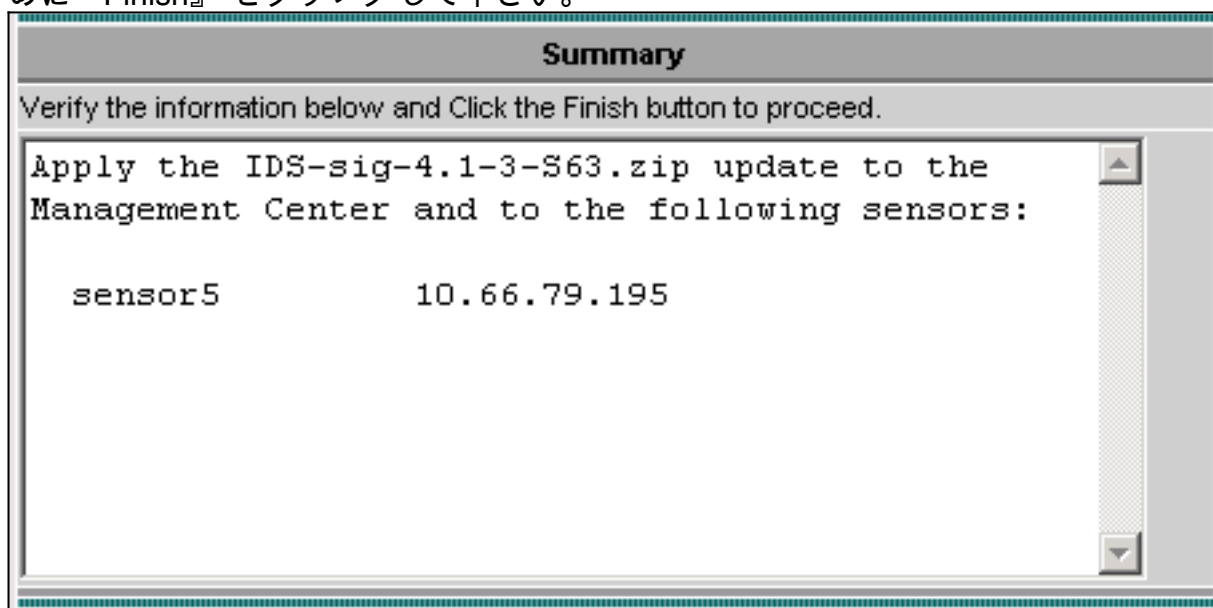
6. 続かためにアップデートし、『Next』をクリックするようにセンサーを選択して下さい。



Showing 1 records

	<input type="checkbox"/>	IP Address	Sensor Name	Version	Created By	Created On
1.	<input checked="" type="checkbox"/>	10.66.79.195	sensor5	4.1(3)S62	admin	2003-12-15 11:32:13

7. 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かために『Finish』をクリックして下さい。



Summary

Verify the information below and Click the Finish button to proceed.

Apply the IDS-sig-4.1-3-S63.zip update to the Management Center and to the following sensors:

sensor5 10.66.79.195

8. 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を見ます:
: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.**

- 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 TCP Reset を設定して下さい

IOSルータのための TCP Reset を設定するためにこれらのステップを完了して下さい。

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

<input type="checkbox"/>	ID	Signature	Subsig ID	Engine	Enabled	Severity	Action
Showing 0-0 of 0 records							
No records.							
Rows per page: 10							<< Page 1 >>
							<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

- 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**)。
- 利用可能なパラメータをカスタマイズし、次に『Edit』 をクリック するために appropriate オプション・ ボタンをチェックして下さい。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。

Tune Signature Parameters

Signature Name: * mytest

Engine: * STRING.TCP

Engine Description: Generic TCP based string search Engine.

Showing 25 records				
	Parameter Name	Value	Default	Required
1.	<input type="radio"/> ServicePorts	23		Yes
2.	<input type="radio"/> StorageKey	STREAM	STREAM	Yes
3.	<input type="radio"/> RegexString	testattack		Yes
4.	<input type="radio"/> SummaryKey	AaBb	AaBb	Yes
5.	<input type="radio"/> Direction	ToService	ToService	Yes
6.	<input type="radio"/> Protocol	TCP	TCP	Yes
7.	<input type="radio"/> AlarmDelayTimer			No
8.	<input type="radio"/> AlarmInterval			No
9.	<input type="radio"/> AlarmThrottle	Summarize	Summarize	Nn

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。

Signature Group: Custom Filter Source: Signature

Showing 1-1 of 1 records

	<input type="checkbox"/>	ID	Signature	Subsig ID	Engine	Enabled	Severity	Action
1.	<input type="checkbox"/>	20001	mytest	0	STRING.TCP	Yes	Medium	None

Rows per page: 10 << Page 1 >>

7. この場合、重大度は最高に変更され、操作ログ及びリセットは選択されます。[OK] をクリックして続行します。

Edit Signature(s)

Signature: mytest

Enable

Severity: High

Actions: Log Reset Block Host Block Connection

8. 完全なシグニチャはこれに類似したに検知します

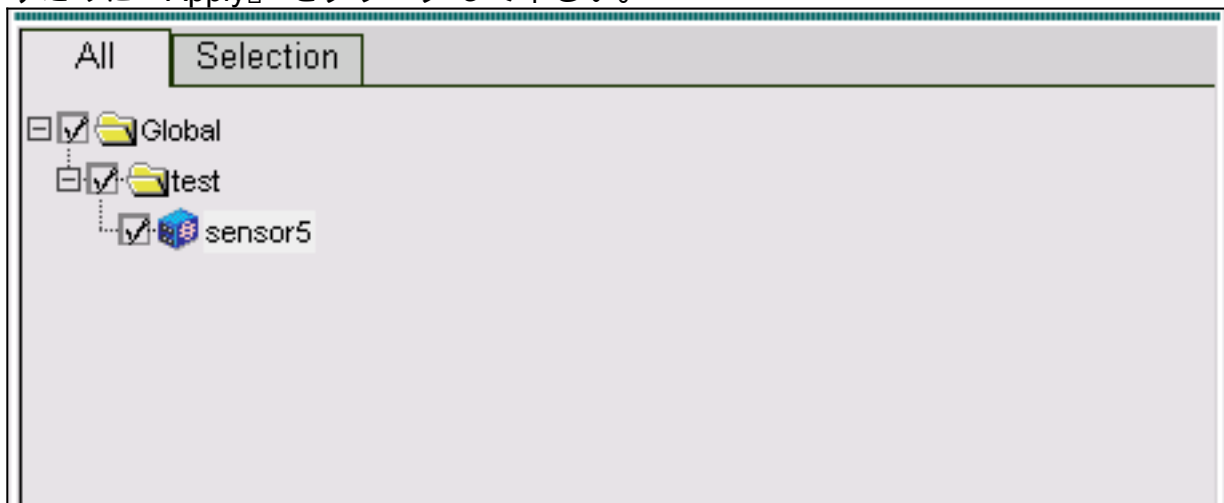
:

Signature Group: <input type="text" value="Custom"/>		Filter Source: <input type="text" value="ID"/>		<input type="text" value=""/>		<input type="button" value="Filter"/>		
Showing 1-1 of 1 records								
<input type="checkbox"/>	ID	Signature	Subsig ID	Engine	Enabled	Severity	Action	
1. <input type="checkbox"/>	20001	mytest	0	STRING.TCP	Yes	High	Log,Reset	
Rows per page: <input type="text" value="10"/>						<< Page 1 >>		
						<input type="button" value="Add"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

9. >保留中『Configuration』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保留中の設定をチェックして下さい。

Showing 1-1 of 1 records					
<input type="checkbox"/>	Pending Configuration	Type	Last Modified On	Last Modified By	
1. <input checked="" type="checkbox"/>	Global.test.sensor5	Sensor	2003-12-15 14:07:39	admin	
Rows per page: <input type="text" value="10"/>				<< Page 1 >>	
				<input type="button" value="Save"/>	<input type="button" value="Delete"/>

10. Deployment > Generate の順に選択し、次にセンサーにコンフィギュレーション変更を押すために『Apply』をクリックして下さい。



11. Deployment > Deploy の順に選択し、『SUBMIT』をクリックして下さい。
 12. チェックボックスをセンサーの隣でチェックし、『Deploy』をクリックして下さい。
 13. 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、続くために『Next』をクリックして下さい。

Showing 1-1 of 1 records				
<input type="checkbox"/>	Configuration File Name	Sensor Name	Generated On	Generated By
1. <input checked="" type="checkbox"/>	sensor5_2003-12-15_17:00:14	Global.test.sensor5	2003-12-15 17:00:14	admin
Rows per page: <input type="text" value="10"/>				<< Page 1 >>

14. 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。

Schedule Type	
Job Name:	<input type="text" value="myjob1"/>
<input checked="" type="radio"/> Immediate	
<input type="radio"/> Scheduled	
Start Time:	<input type="text" value="December"/> <input type="text" value="15"/> <input type="text" value="2003"/> <input type="text" value="18"/> : <input type="text" value="54"/> : <input type="text" value="03"/>
Retry Options	
Maximum Number Of Attempts	<input type="text" value="0"/>
Time Between Attempts	<input type="text" value="15"/> minutes
Failure Options	
Overwrite conflicting sensor(s) configuration?	<input checked="" type="checkbox"/>
Require correct sensor versions?	<input checked="" type="checkbox"/>
Notification Options	
<input type="checkbox"/> Email report to:	<input type="text"/>
(When specifying more than one recipient, comma separate the addresses.)	

15. 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あるはずですが。
16. >履歴配備を確認するために『Configuration』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することを意味します。

Showing 1-1 of 1 records				
<input type="checkbox"/>	Configuration File Name	Status	Generated	Deployed
1. <input type="checkbox"/>	sensor5_2003-12-15_23:04:36	Deployed	2003-12-15 23:04:36	2003-12-15 23:09:55

Rows per page: << Page 1 >>

確認

ここでは、設定が正常に動作していることを確認します。

不正侵入および TCP Reset の起動

テスト攻撃を開始し、ブロッキングプロセスが正しくはたらくことを確認するために結果をチェックして下さい。

1. 攻撃が開始する前に、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』をクリックして下さい。
3. 『Launch Event Viewer』をクリックして下さい。

The screenshot shows the 'Launch Event Viewer' dialog box with the following settings:

- Event Type: Network IDS Alarms
- Column Set: Last Saved
- Event Start Time: At Earliest
- Event Stop Time: Don't Stop

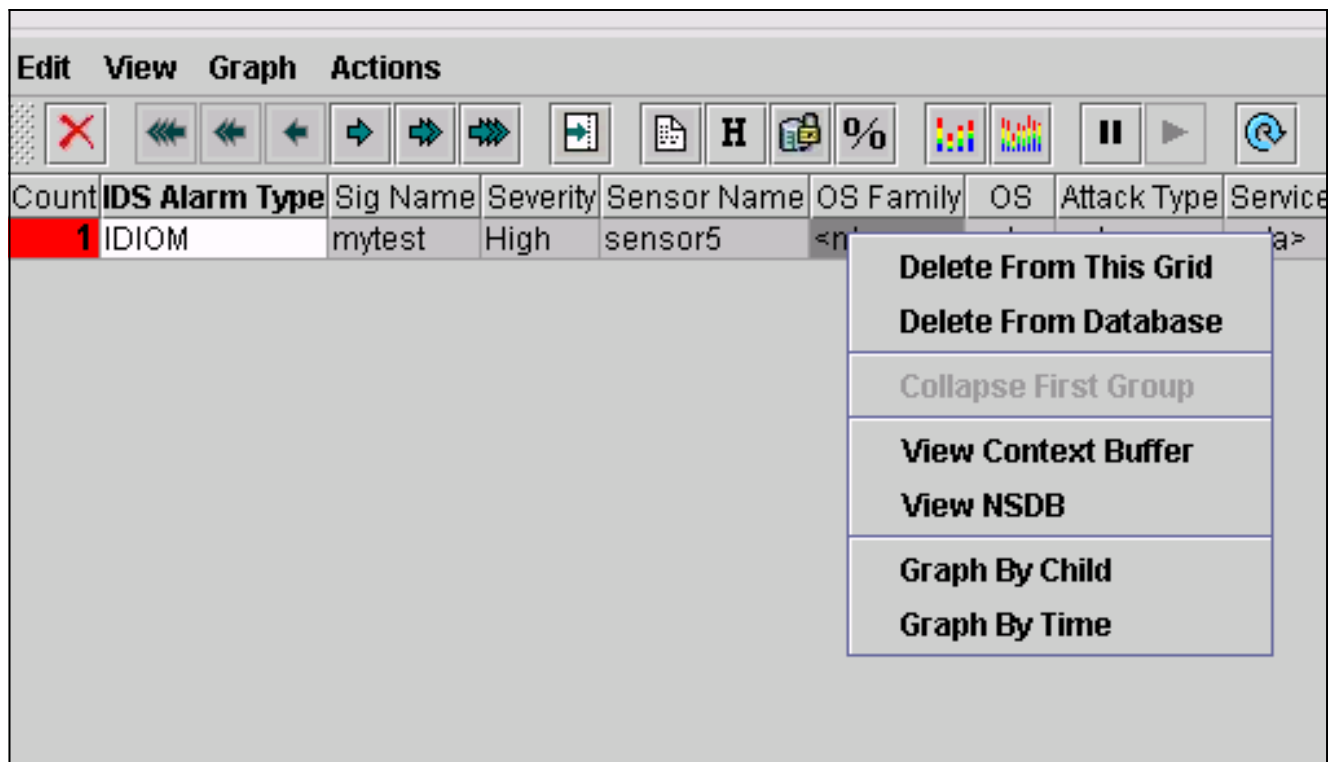
A 'Launch Event Viewer' button is located at the bottom right of the dialog.

4. 1つのルータから他に Telnet で接続し、攻撃を開始するために **testattack** を入力して下さい。この場合、ルータ Light からルータ House に Telnet で接続しました。<space> か <enter> を押すとすぐ、**testattack** を入力した後、Telnetセッションは再設定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 !--- The Telnet session is reset due to the !--- signature "testattack" being triggered. [Connection to 100.100.100.1 lost]
5. イベントビューアから、新しいイベントのために今『Query Database』をクリックして下さい。以前に開始された攻撃についてはアラートを見ます

The screenshot shows the Event Viewer interface with the following table of events:

Count	IDS Alarm Type	Sig Name	Severity	Sensor Name	OS Family	OS	Attack Type	Service	Protocol	Prot
1	IDIOM	mytest	High	sensor5	<n/a>	<n/a>	<n/a>	<n/a>	<n/a>	<n/a>

6. イベントビューアでは、アラームを強調表示し、それを右クリックし、どちらかのビューコンテキストバッファを選択するか、またはアラームについての詳細な情報を表示するために NSDB を表示して下さい。



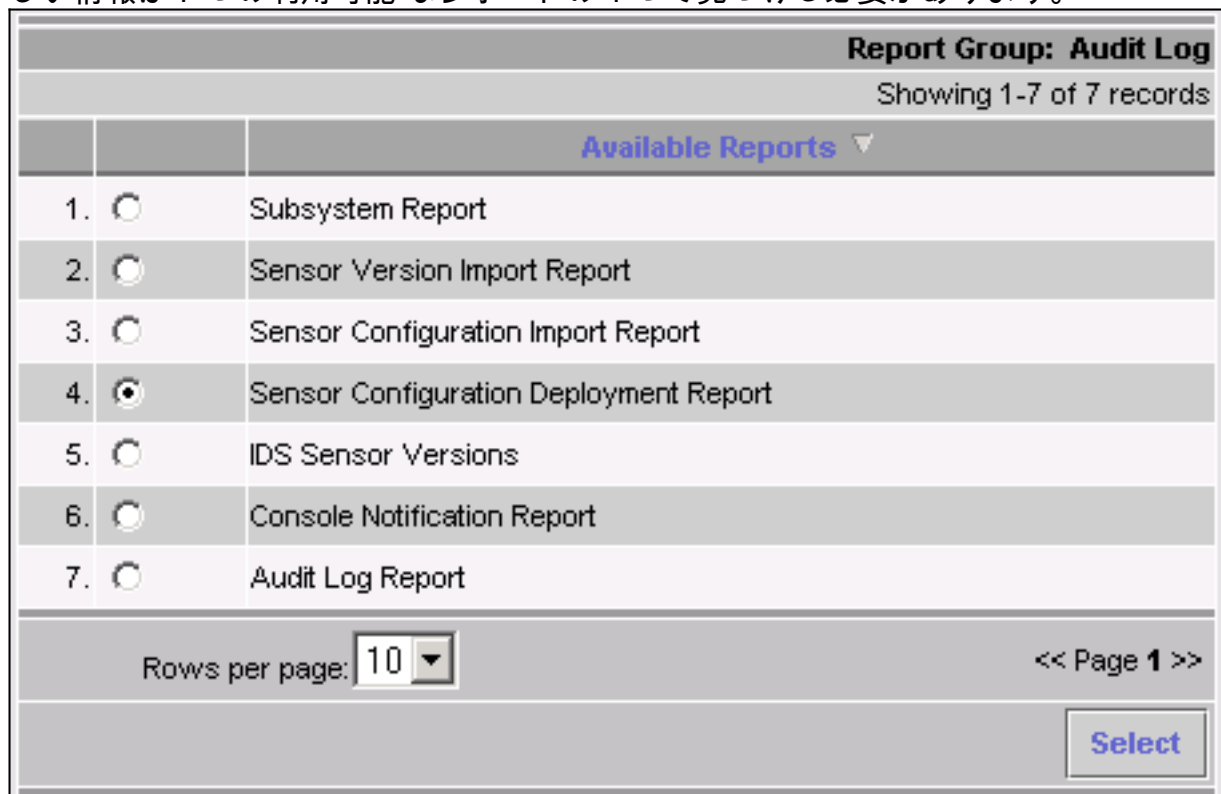
トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

トラブルシューティング手順

解決するためにこれらのステップを完了して下さい。

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. ルータ アクセスリストを設定するのにブロックがコマンドおよびコントロール ポートを利用する間、TCP リセットはセンサーの探知インターフェイスから送信されます。及びましたこれと同じようなスイッチの **set span** コマンドを使用して正しいポートに、確認して下さい:

```
set span <src_mod/src_port><dest_mod/dest_port> both inpkts enable banana (enable) set span
2/12 3/6 both inpkts enable Overwrote Port 3/6 to monitor transmit/receive traffic of Port
2/12 Incoming Packets enabled. Learning enabled. Multicast enabled. banana (enable) banana
(enable) banana (enable) show span Destination : Port 3/6 !--- Connect to sniffing
interface of the Sensor. Admin Source : Port 2/12 !--- In this case, connect to Ethernet1
of Router House. Oper Source : Port 2/12 Direction : transmit/receive Incoming Packets:
enabled Learning : enabled Multicast : enabled
```

3. TCP Reset がはたらかない場合、センサーにログインし、**show event** コマンドを入力して下さい。攻撃を開始し、アラームが引き起こされるかどうか確認して下さい。アラームが引き起こされる場合、それを確認するチェックはアクションの種類 **TCP Reset** のために設定されます。

関連情報

- [Cisco Secure Intrusion Detection のサポートページ](#)
- [Cisco Secure Intrusion Detection System に関する文書](#)
- [CiscoWorks VPN/Security Management Solution サポートページ](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)