

# VMS IDS MC を使用した IDS ブロッキングの設定

## 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ルータのためのブロッキングを設定して下さい](#)

[確認](#)

[攻撃およびブロッキングを起動させて下さい](#)

[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。

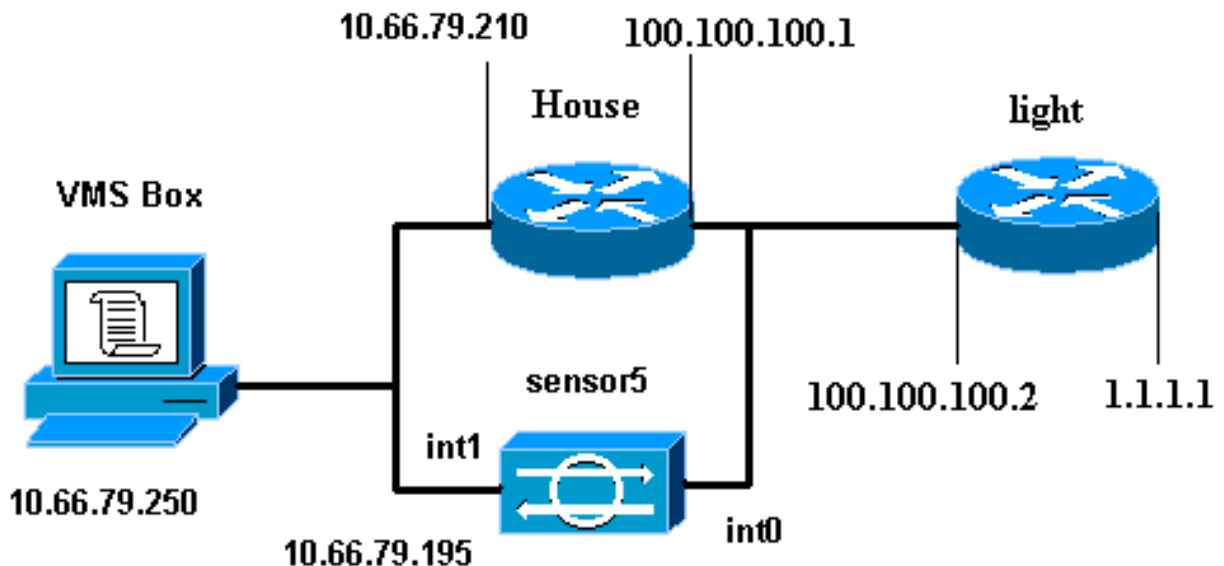
## 設定

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。

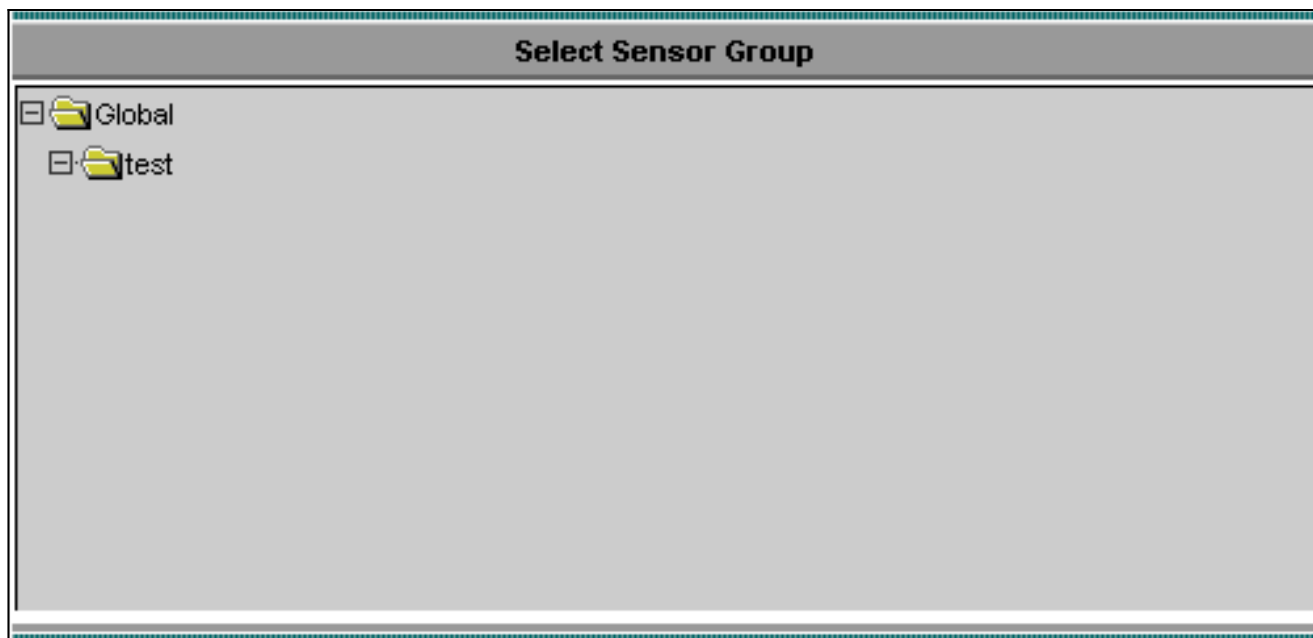
## IDS MC にセンサーをインポートして下さい

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。

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	

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。

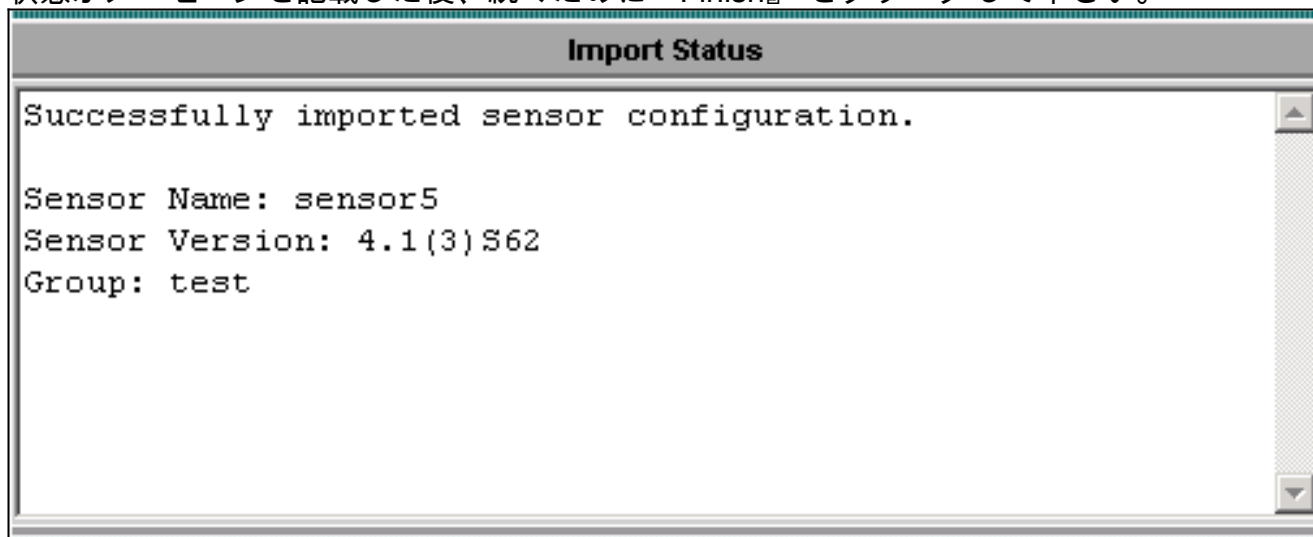


8. 詳細をこの例によって入力し、そして隣の隣で続きますクリックして下さい。

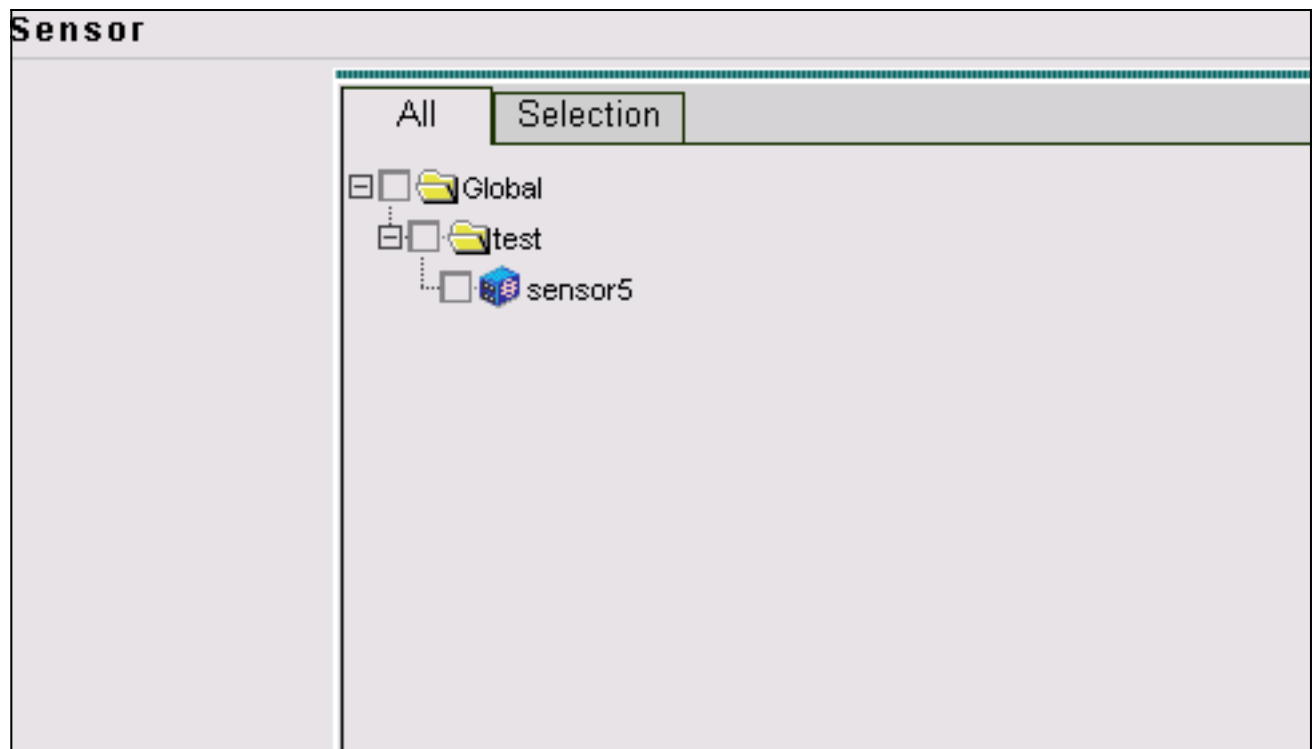
Identification	
IP Address: *	<input type="text" value="10.66.79.195"/>
NAT Address:	<input type="text"/>
Sensor Name (required if not Discovering Settings):	<input type="text" value="sensor5"/>
Discover Settings:	<input checked="" type="checkbox"/>
SSH Settings:	
User ID: *	<input type="text" value="cisco"/>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

Note: \* - Required Field

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

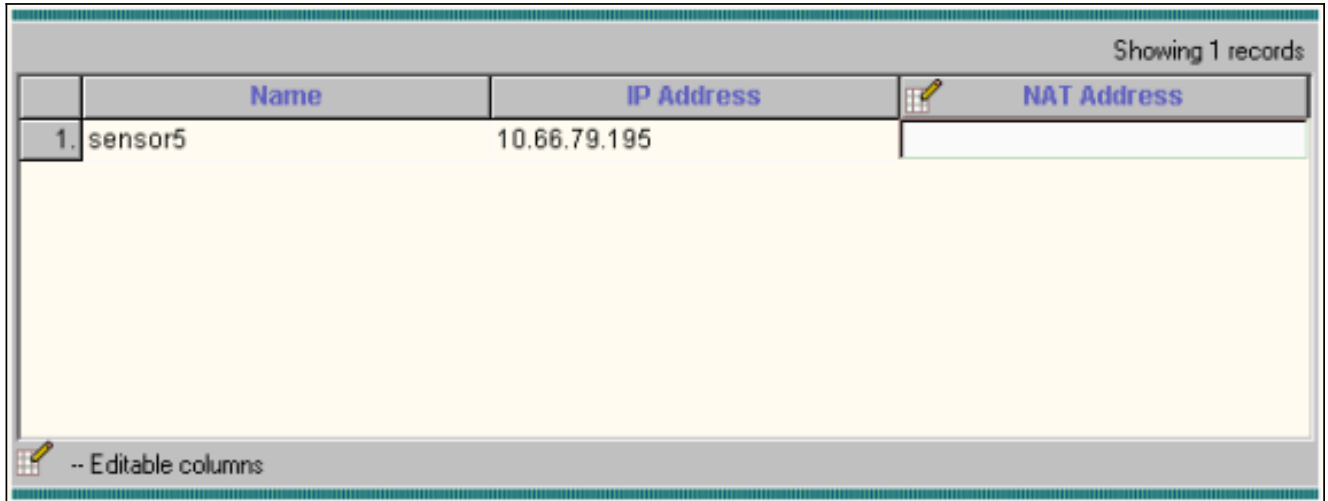
Enter IDS MC server contact information:	
IP Address/Host Name: *	<input type="text" value="10.66.79.250"/>
Web Server Port: *	<input type="text" value="443"/>
Username: *	<input type="text" value="admin"/>
Password: *	<input type="password" value="XXXXXXXX"/>
Note: * - Required Field	

クシ、入力して下さい。

3. センサーを (この場合、**sensor5**) 選択し、**の隣**で続きます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. 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。

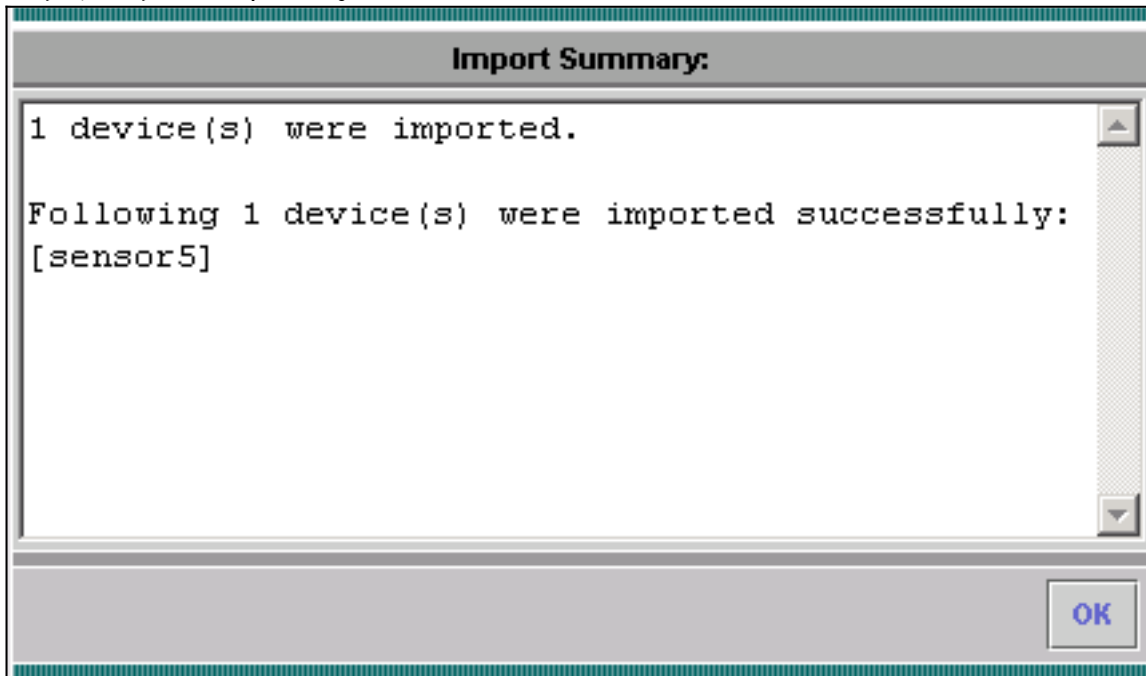


Showing 1 records

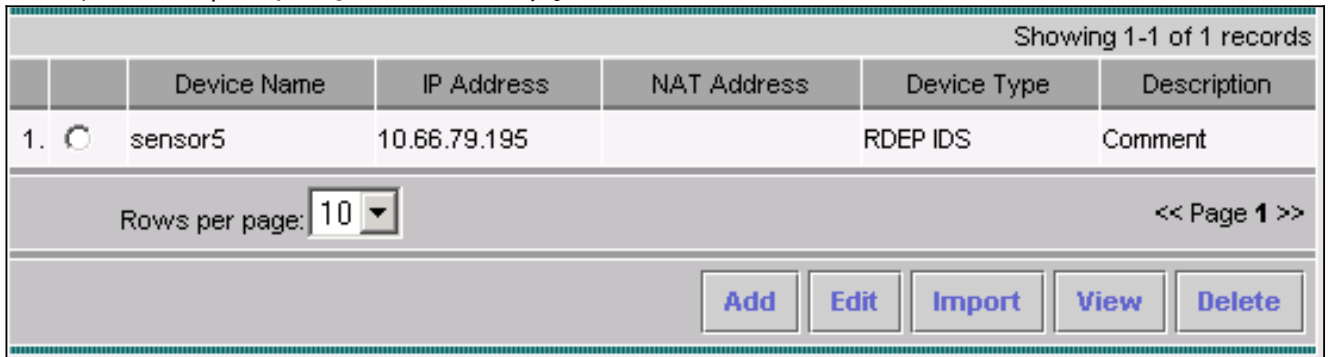
	Name	IP Address	NAT Address
1.	sensor5	10.66.79.195	

-- 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. センサーは正常にインポートされます。



Showing 1-1 of 1 records

	Device Name	IP Address	NAT Address	Device Type	Description
1.	<input type="radio"/> sensor5	10.66.79.195		RDEP IDS	Comment

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](#)

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: IDS-sig-4.1-3-S63.zip

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。

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

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。

**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
```

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**.

- 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セスを完了して下さい。

- 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。
- 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。
- 『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。

<input type="checkbox"/>	ID	Signature	Subsig ID	Engine	Enabled	Severity	Action
No records.							

- 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)。
- 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。

**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、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)。

**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="Signature"/>		<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	Block
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. 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

Blocking Device	
Device Type: *	<input type="text" value="Cisco Router"/>
IP Address: *	<input type="text" value="10.66.79.210"/>
NAT Address:	<input type="text" value=""/>
Comment:	<input type="text" value=""/>
Username:	<input type="text" value=""/>
Password: *	<input type="password" value="*****"/>
Enable Password:	<input type="password" value="*****"/>
Secure Communications:	<input type="text" value="none"/>
Interfaces: *	<a href="#">Edit Interfaces</a>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	
Note: * - Required Field	

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。

Blocking Device Interface	
Blocking Interface Name	<input type="text" value="Ethernet1"/>
Blocking Direction	<input type="text" value="inbound"/>
Pre-block ACL Name	<input type="text" value="198"/>
Post-block ACL Name	<input type="text" value="199"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

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。

Showing 1-1 of 1 records				
	IP Address	Device Type	Comment	Source
1.	<input type="radio"/>	10.66.79.210	Cisco Router	sensor5
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"/>				

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] をクリックして続けます。

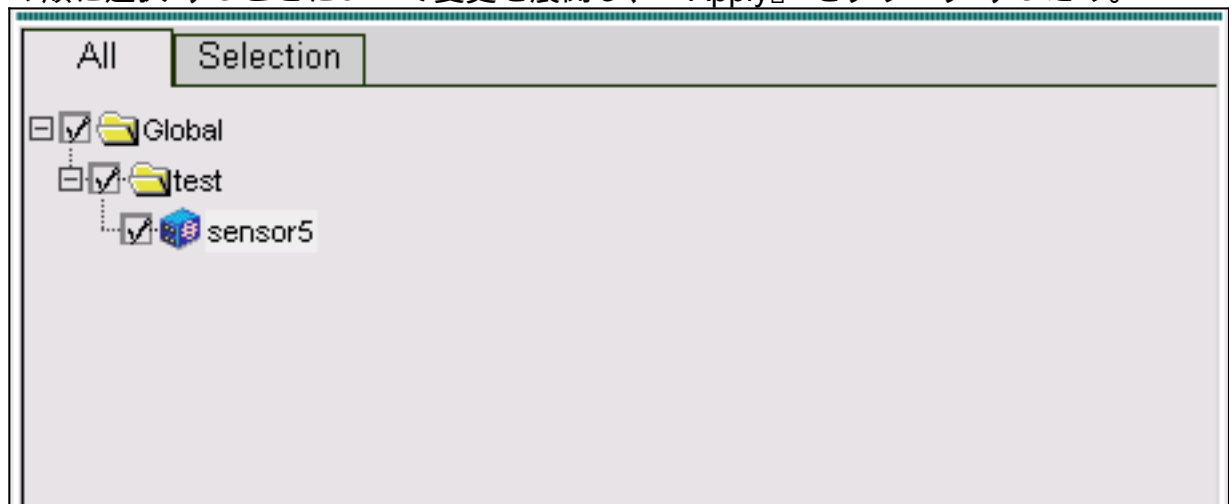
Blocking Properties	
Length of Automatic Block	<input type="text" value="15"/> minutes
Maximum ACL Entries	<input type="text" value="100"/>
Enable ACL Logging	<input type="checkbox"/>
Allow blocking devices to block the sensor's IP address	<input type="checkbox"/>
<input checked="" type="checkbox"/> Override	<input type="button" value="Apply"/> <input type="button" value="Reset"/>

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。

Showing 1-1 of 1 records				
	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"/>				

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。

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: 10 < >> Page 1 <<

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。

**Schedule Type**

Job Name:

Immediate

Scheduled

Start Time:     :  :

**Retry Options**

Maximum Number Of Attempts

Time Between Attempts  minutes

**Failure Options**

Overwrite conflicting sensor(s) configuration?

Require correct sensor versions?

**Notification Options**

Email report to:

(When specifying more than one recipient, comma separate the addresses.)

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。

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っ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。

Launch Event Viewer

Event Type: Network IDS Alarms

Column Set: Last Saved

Event Start Time:  At Earliest  
 At Time December 15 2003 22 : 26 : 06

Event Stop Time:  Don't Stop  
 At Time December 15 2003 22 : 26 : 06

Launch Event Viewer

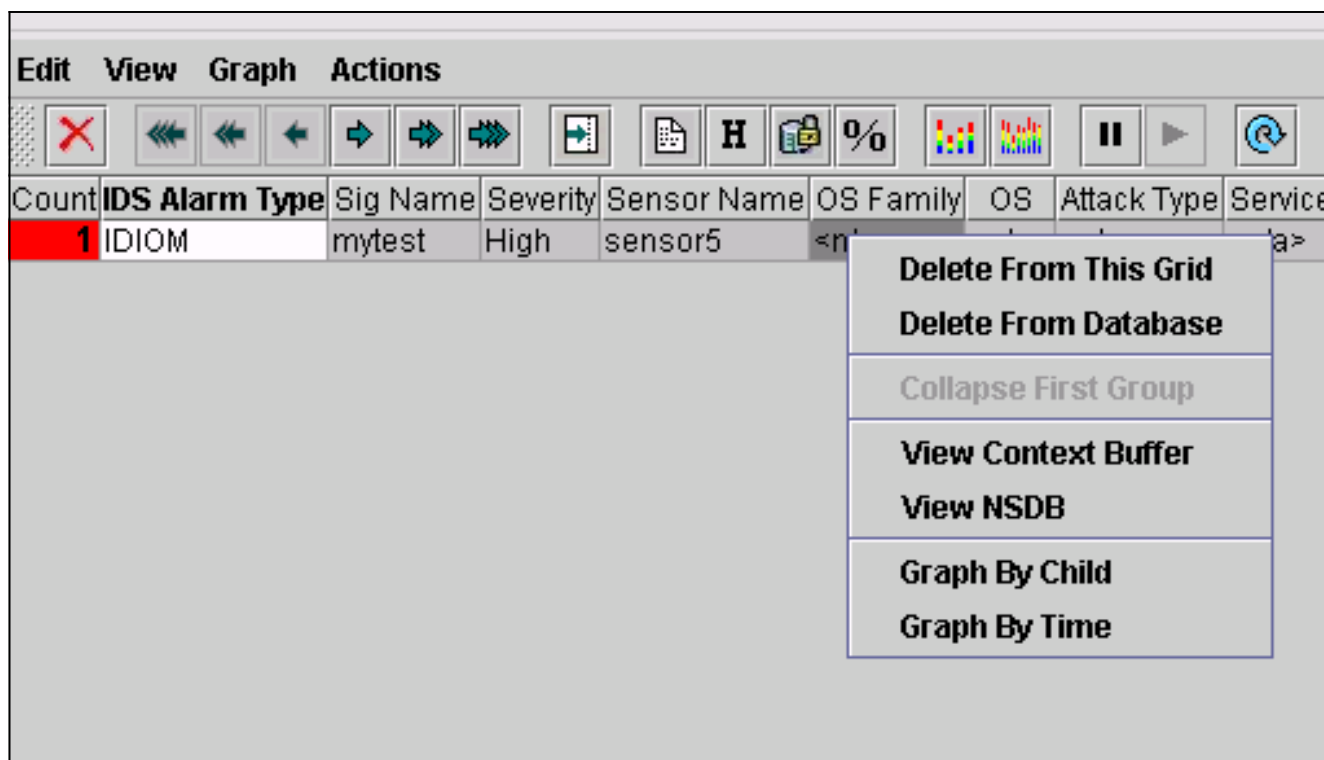
3. センサーからの通信を確認するためにルータに（この場合、家ルータへの Telnet）、Telnet で接続して下さい。house#show user Line User Host(s) Idle Location \* 0 con 0 idle 00:00:00 226 vty 0 idle 00:00:17 10.66.79.195 house#show access-list Extended IP access list IDS\_Ethernet1\_in\_0 10 permit ip host 10.66.79.195 any 20 permit ip any any (20 matches) 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。

You Are Here: Monitor > Events

Edit View Graph Actions

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>

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、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。

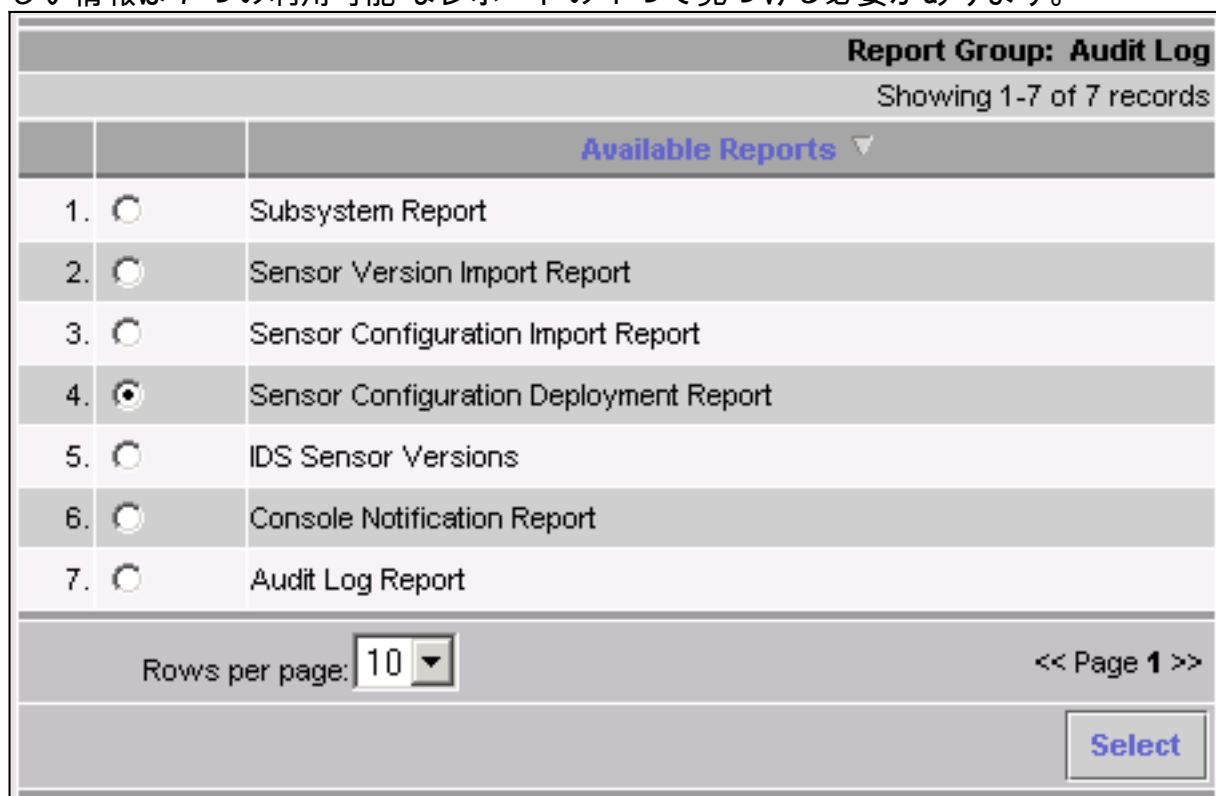


## トラブルシューティング

### 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必ずアクティブ 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#
```

- 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](#)