

Настройка блокирования IDS с помощью VMS IDS MC

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Настройка](#)

[Схема сети](#)

[Конфигурации](#)

[Начальная конфигурация сенсора](#)

[Импортируйте датчик в MC IDS](#)

[Импортируйте датчик в монитор безопасности](#)

[Используйте MC IDS для обновлений подписи](#)

[Настройте блокирование для маршрутизатора IOS](#)

[Проверка](#)

[Запустите Attack and Blocking](#)

[Устранение неполадок](#)

[Процедура устранения неполадок](#)

[Дополнительные сведения](#)

Введение

Этот документ предоставляет выборку для конфигурации Cisco Intrusion Detection System (IDS) через VPN/Security Management Solution (VMS), Консоль управления IDS (MC IDS). В этом случае Блокирование от сенсора IDS до маршрутизатора Cisco настроено.

Предварительные условия

Требования

Прежде чем вы настроите Блокирование, гарантируете, что удовлетворили этим условиям.

- Датчик установлен и настроен для считывания необходимого трафика.
- Интерфейс анализатора охвачен к внешнему интерфейсу маршрутизатора.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования.

- VMS 2.2 с MC IDS и монитором безопасности 1.2.3
- Датчик Cisco IDS 4.1.3S (63)
- Cisco маршрутизатор работающий под управлением Cisco IOS® Software Release 12.3.5

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.](#)

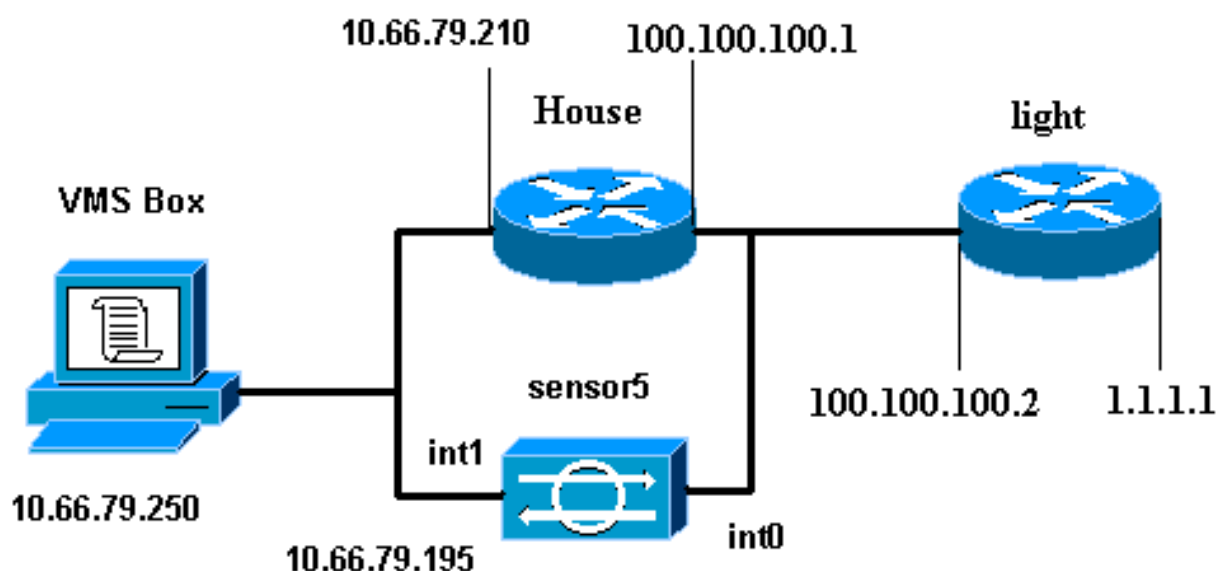
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: [Поиск дополнительной информации о командах в данном документе можно выполнить с помощью средства "Command Lookup" \(Поиск команд\) \(только для зарегистрированных клиентов\).](#)

Схема сети

В этом документе используются настройки сети, показанные на данной диаграмме.



Конфигурации

В данном документе используется следующая конфигурация.

- [Маршрутизатор light](#)
- [Маршрутизатор house](#)

Маршрутизатор 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
```

Маршрутизатор 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
```

[Начальная конфигурация сенсора](#)

Пройдите эти шаги, чтобы произвести начальное конфигурирование сенсора.

Примечание: При выполнении начальной настройки Датчика продолжитесь к разделу [Импортирующему Датчик в MC IDS](#).

1. Консоль в датчик. Будет предложено ввести имя пользователя и пароль. Если это первоначально, вы подключаетесь с консоли в Датчик, необходимо войти с **именем пользователя cisco** и **паролем cisco**.
2. Вам предлагают изменить пароль и затем перепечатать новый пароль для подтверждения.
3. Введите **настройку** и введите соответствующую информацию в каждое приглашение для устанавливания основных параметров для Датчика согласно данному **примеру**:

```
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. Нажмите **2** для сохранения конфигурации.

Импортируйте датчик в MC IDS

Выполните эти шаги для импорта Датчика в MC IDS.

1. Перейдите к своему Датчику. В этом случае перейдите или к **http://10.66.79.250:1741** или к **https://10.66.79.250:1742**.
2. Вход в систему с соответствующим именем пользователя и паролем. В данном примере использовались **имя пользователя admin** и **пароль cisco**.
3. Выберите **VPN/Security Management Solution > Management Center** и выберите **IDS Sensors**.
4. Нажмите вкладку **Devices**, выберите **Sensor Group**, выделите **Глобальный** и нажмите **Create Subgroup**.
5. Введите Имя группы и гарантируйте, что переключатель **Default** установлен, затем нажмите **OK** для добавления подгруппы в MC

Add Group

Group Name: * test

Parent: Global

Description:

Settings:

Default (use parent values)

Copy settings from group Global

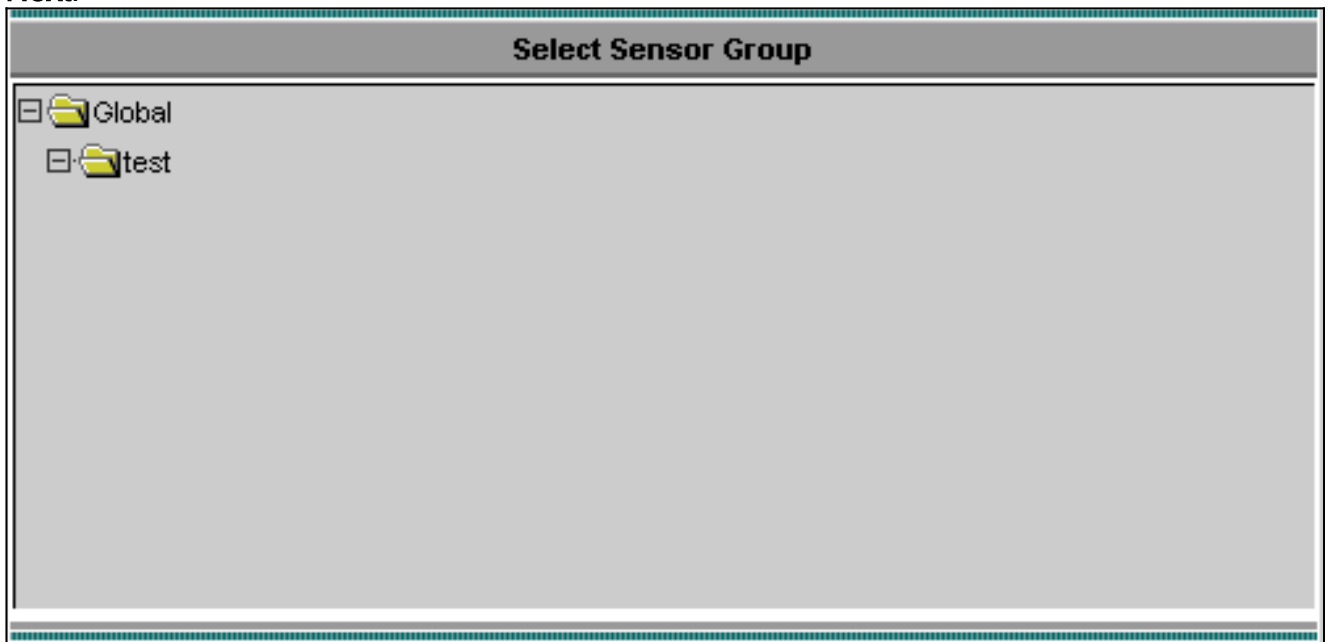
OK Cancel

Note: * - Required Field

IDS.

6. Выберите **Devices > Sensor**, выделите подгруппу, созданную в предыдущем шаге (в этом случае, **тест**), и нажмите **Add**.
7. Выделите подгруппу и нажмите

Next.

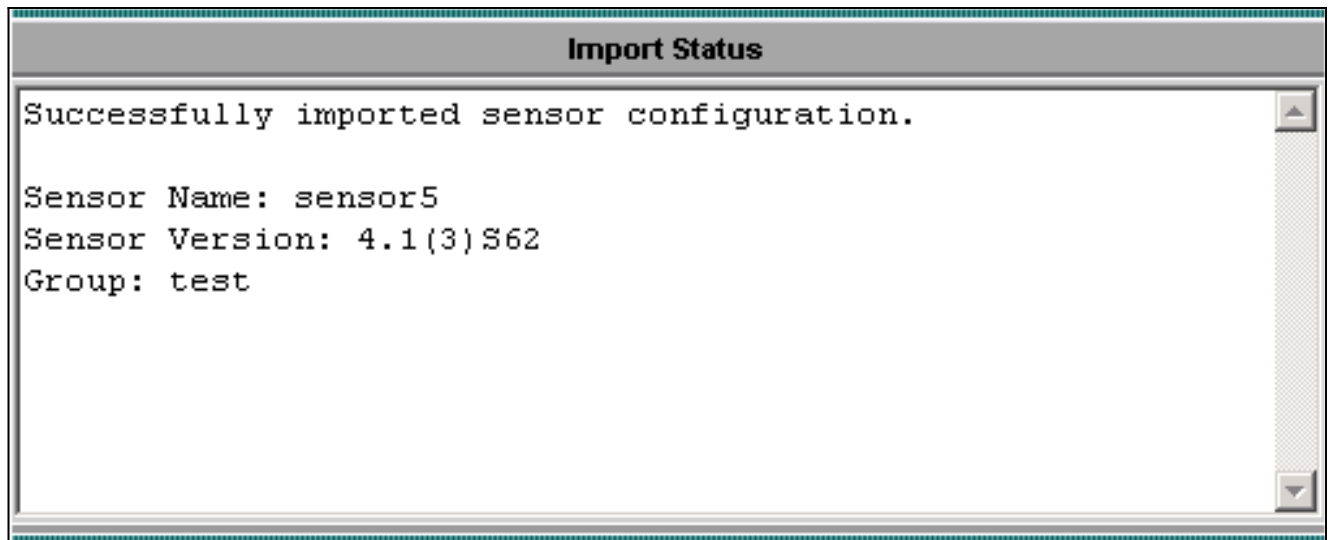


8. Введите подробные данные согласно данному примеру, затем нажмите **Next** для продолжения.

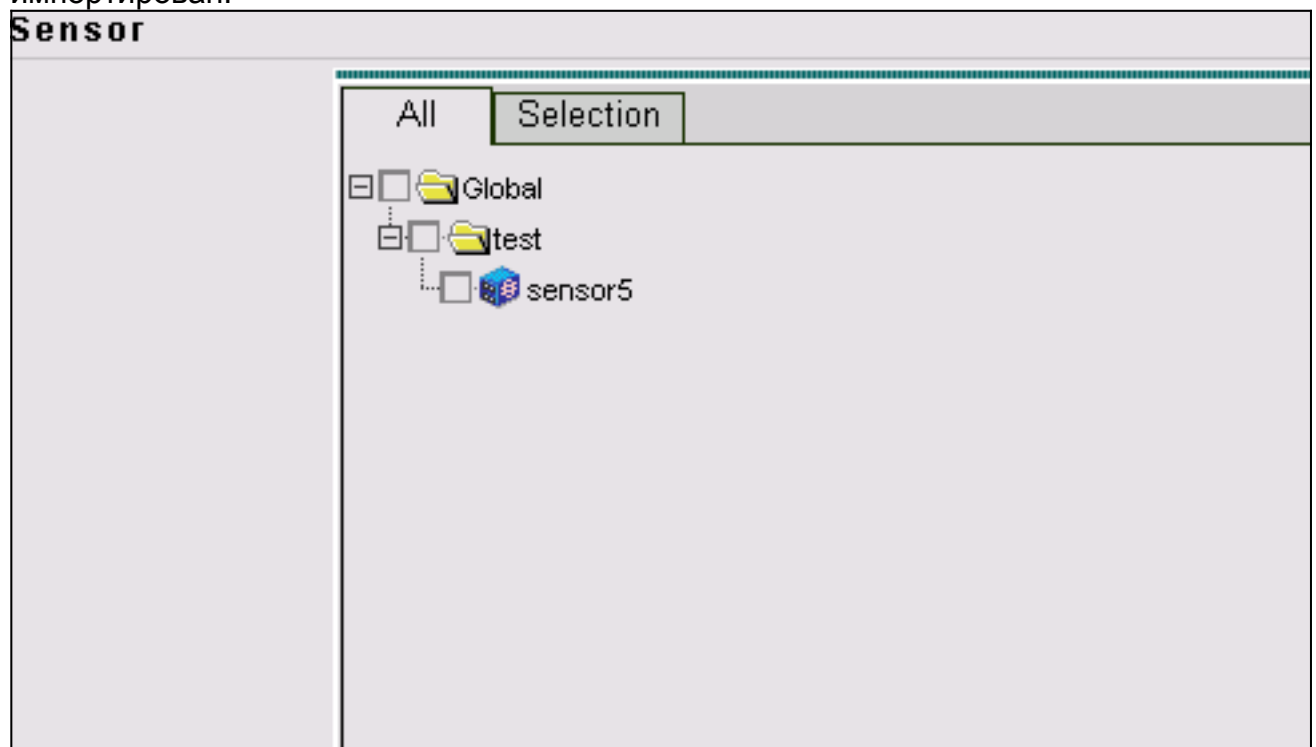
Identification	
IP Address: *	<input type="text" value="10.66.79.195"/>
NAT Address:	<input type="text"/>
Sensor Name (required if not Discovering Settings):	<input type="text" value="sensor5"/>
Discover Settings:	<input checked="" type="checkbox"/>
SSH Settings:	
User ID: *	<input type="text" value="cisco"/>
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. После того, как вам предоставляют сообщение, которое сообщает `Successfully imported sensor configuration`, нажмите **Finish** для продолжения.



10. Ваш Датчик импортирован в MC IDS. В этом случае sensor5 импортирован.



[Импортируйте датчик в монитор безопасности](#)

Завершите эту процедуру для импорта Датчика в монитор безопасности.

1. В Меню сервера VMS выберите **VPN/Security Management Solution>> Security Monitoring Center Монитор**.
2. Выберите вкладку **Devices**, затем нажмите **Import** и введите Информацию сервера MC IDS согласно данному

Enter IDS MC server contact information:

IP Address/Host Name: *	10.66.79.250
Web Server Port: *	443
Username: *	admin
Password: *	*****

Note: * - Required Field

примеру.


3. Выберите свой Датчик (в этом случае, **sensor5**) и нажмите **Next** для продолжения.


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

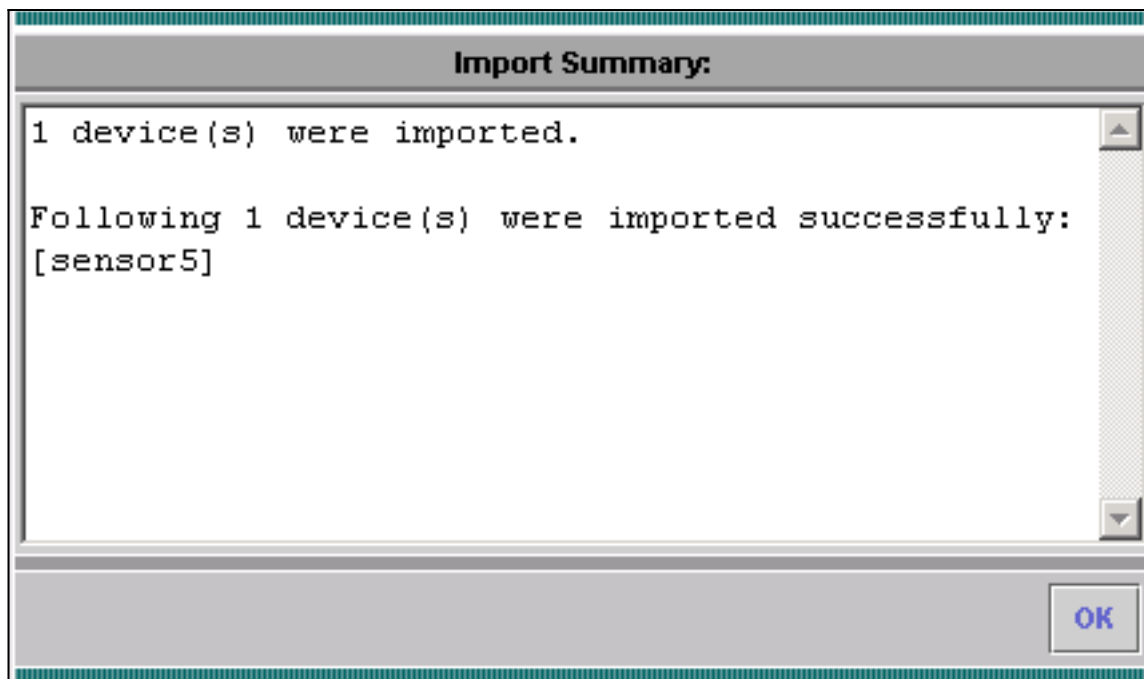
4. Если потребуется, обновите адрес Технологии NAT для своего Датчика, затем нажмите **Finish** для продолжения.

Showing 1 records

	Name	IP Address	 NAT Address
1.	sensor5	10.66.79.195	

 -- Editable columns

5. Нажмите **OK**, чтобы закончить импортировать Датчик из MC IDS в Монитор Безопасности.



6. Ваш Датчик успешно импортирован.

Showing 1-1 of 1 records

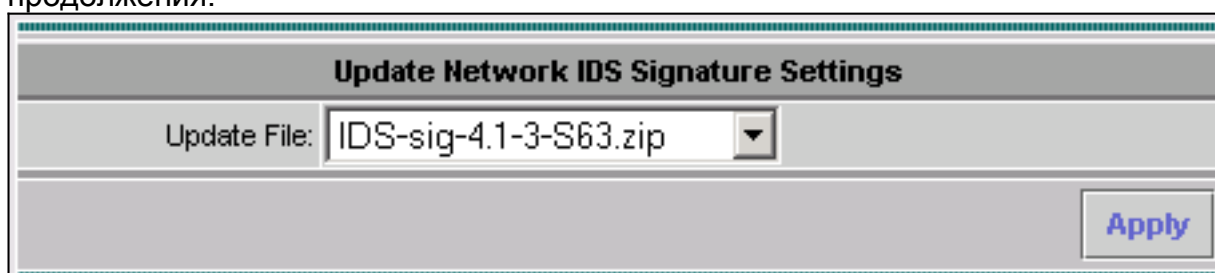
	Device Name	IP Address	NAT Address	Device Type	Description
1. <input type="radio"/>	sensor5	10.66.79.195		RDEP IDS	Comment

Rows per page: << Page 1 >>

[Используйте MC IDS для обновлений подписи](#)

Завершите эту процедуру для использования MC IDS для обновлений подписи.

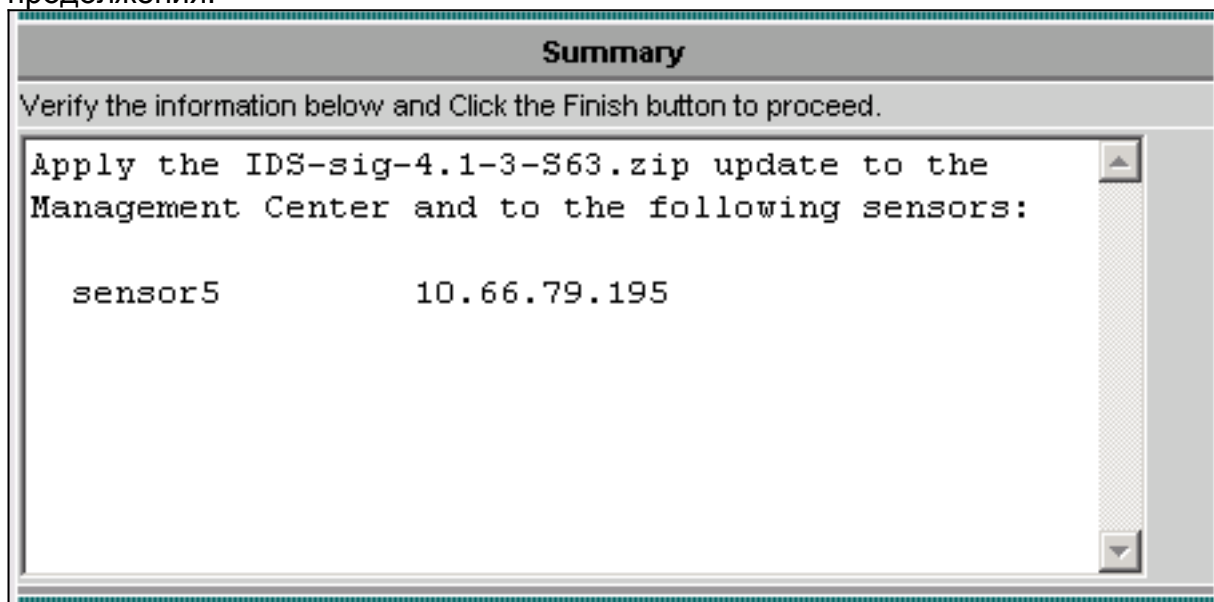
1. Загрузите [Обновления подписи Обнаружения несанкционированного доступа к сети \(только зарегистрированные клиенты\)](#) от Загрузок и сохраните их в каталоге C:\PROGRA~1\CSCOPx\MDC\etc\ids\updates\на вашем сервере VMS.
2. В консоли сервера VMS выберите **VPN/Security Management Solution> Management Center> Sensors**.
3. Нажмите Вкладку конфигурация, выберите **Updates** и нажмите **Update Network IDS Signatures**.
4. Выберите подпись, которую вы хотите обновить от раскрывающегося меню и нажать **Apply** для продолжения.



5. Выберите Sensor, чтобы обновить, и нажать **Next** для продолжения.

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. После того, как вам предложат применить обновление Центра управления, а также Датчик, нажмите **Finish** для продолжения.



7. Telnet или консоль в интерфейс командной строки Датчика. Информация, подобная ЭТОМУ, ПОЯВЛЯЕТСЯ: 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. Ждите в течение нескольких минут, чтобы позволить обновлению завершиться, затем вводить **show version** для проверки. 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
```

[Настройте блокирование для маршрутизатора IOS](#)

Завершите эту процедуру для настройки Блокирования для маршрутизатора IOS.

1. В консоли сервера VMS выберите **VPN/Security Management Solution> Management Center> IDS Sensors**.

- Выберите Вкладку конфигурация, выберите свой Датчик от Селектора объектов и нажмите **Settings**.
- Выберите **Signatures**, нажмите **Custom**, затем нажмите **Add** для добавления новой подписи.

Signature Group: Filter Source:

Showing 0-0 of 0 records

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

Rows per page: << Page 1 >>

- Введите новое Имя Подписи, затем выберите Engine (в этом случае, **Строка TCP**).
- Можно настроить доступные параметры путем проверки соответствующей кнопки с зависимой фиксацией и нажатия **Edit**. В данном примере параметр ServicePorts отредактирован для изменения его значения на 23 (для порта 23). Параметр RegexString также отредактирован для добавления **testattack** значения. Когда это будет завершено, нажмите **OK** для продолжения.

Tune Signature Parameters

Signature Name:

Engine:

Engine Description:

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	No

- Для редактирования Строгости подписи и Действий или к Позволить/запретить подпись нажмите название подписи.

Signature Group: Custom Filter Source: Signature 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	Medium	None

Rows per page: 10 << Page 1 >>

Add Edit Delete

7. В этом случае степени серьезности ошибки изменены на **Высокий**, и **Блочное** действие Хоста выбрано. **Для продолжения нажмите кнопку ОК.**Блочные блоки Хоста, нападая на IP-узлы или IP-подсети.Блочный TCP Блоков соединений или порты UDP (на основе нападения на TCP или UDP -

Edit Signature(s)

Signature: mytest

Enable

Severity: High

Actions: Log Reset Block Host Block Connection

OK Cancel

подключения).

8. Завершенная подпись выглядит подобной этому:

Signature Group: Custom Filter Source: Signature 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: 10 << Page 1 >>

Add Edit Delete

9. Для настройки Устройства блокировки выберите **Blocking > Blocking Devices** от Селектора объектов (меню на левой стороне экрана) и **нажмите Add** для ввода следующей информации:

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

10. Нажмите **Edit Interfaces** (см. предыдущий снимок экрана), нажмите **Add**, введите эту информацию, затем нажмите **OK** для продолжения.

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

11. Нажмите **OK** дважды для завершения конфигурации Устройства блокировки.

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. Для настройки Слеживаемости выберите **Blocking> Blocking Properties**. Длина Автоматического Блока может модифицироваться. В этом случае это изменено на **15 минут**. Нажмите **Apply** для продолжения.

The screenshot shows the 'Blocking Properties' configuration window. It contains the following fields and controls:

- Length of Automatic Block:** A text input field containing '15' and a label 'minutes' to its right.
- Maximum ACL Entries:** A text input field containing '100'.
- Enable ACL Logging:** A checkbox that is currently unchecked.
- Allow blocking devices to block the sensor's IP address:** A checkbox that is currently unchecked.
- Override:** A checkbox that is checked.
- Buttons:** 'Apply' and 'Reset' buttons are located at the bottom right.

13. Выберите **Configuration** из главного меню, затем выберите **Pending**, проверьте конфигурацию ожидания, чтобы гарантировать, что это корректно, и нажмите

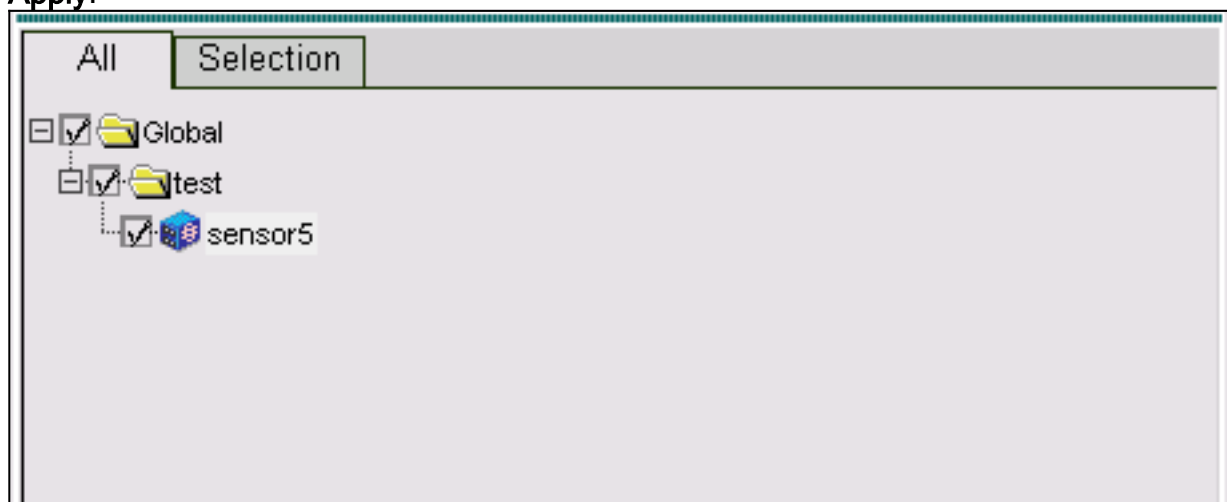
The screenshot shows a table with the following data:

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

Below the table, there is a 'Rows per page:' dropdown menu set to '10' and a '<< Page 1 >>' indicator. At the bottom right, there are 'Save' and 'Delete' buttons.

Save.

14. Для продвижения изменений конфигурации к Датчику генерируйте и затем разверните изменения путем выбора **Deployment> Generate** и нажмите **Apply**.



15. Выберите **Deployment> Deploy**, затем нажмите **Submit**.
16. Проверьте флажок рядом со своим Датчиком, затем нажмите **Deploy**.
17. Проверьте флажок для задания в очереди, затем нажмите **Next** для продолжения.

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: << Page 1 >>

18. Введите Имя задания и планируйте задание как Непосредственное, затем нажмите **Finish**.

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. Выберите **Deployment> Deploy> Pending**. Ждите несколько минут, пока не были завершены все ожидающие задания. Очередь тогда пуста.
20. Для подтверждения развертываний выберите **Configuration> History**. Гарантируйте, что статус конфигурации отображен как **Развернутый**. Это означает, что Конфигурация сенсора была обновлена успешно.

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 >>

Проверка

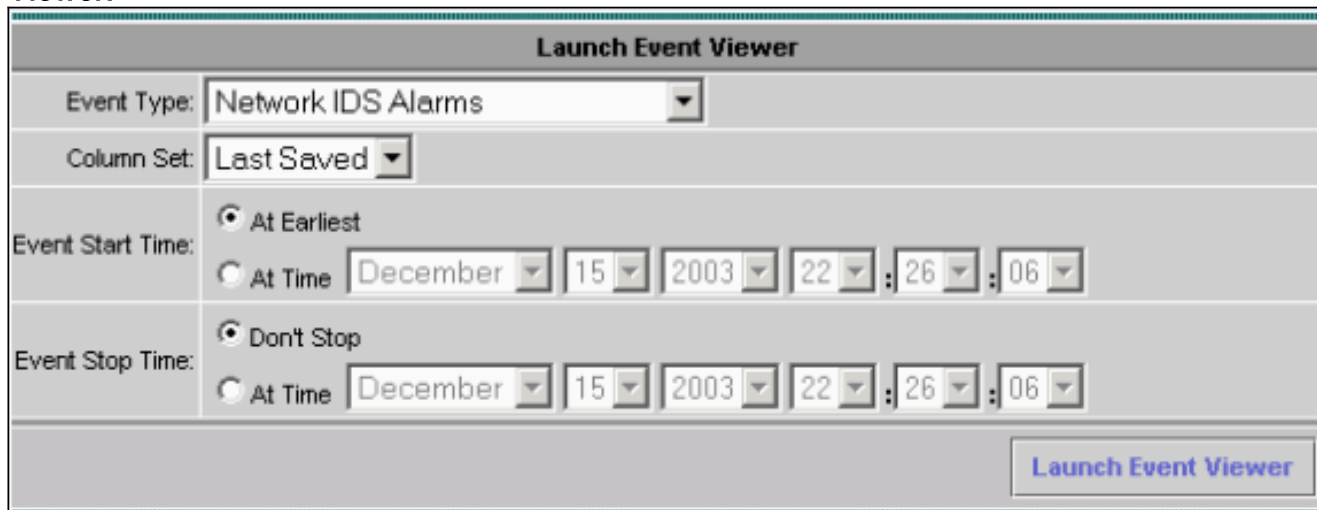
В этом разделе содержатся сведения, которые помогают убедиться в надлежащей работе конфигурации.

Некоторые команды `show` поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды `show`.

Запустите Attack and Blocking

Чтобы проверить, что Блокирующий процесс работает правильно, пойдите в тестовое наступление и проверьте результаты.

1. Прежде, чем пойти в наступление, выберите **VPN/Security Management Solution>> Security Monitoring Center Монитор**.
2. Выберите **Monitor** из главного меню, нажмите **Events** и затем нажмите **Launch Event Viewer**.



Launch Event Viewer	
Event Type:	Network IDS Alarms
Column Set:	Last Saved
Event Start Time:	<input checked="" type="radio"/> At Earliest <input type="radio"/> At Time December 15 2003 22 : 26 : 06
Event Stop Time:	<input checked="" type="radio"/> Don't Stop <input type="radio"/> At Time December 15 2003 22 : 26 : 06
Launch Event Viewer	

3. Telnet к маршрутизатору (в этом случае, Telnet к маршрутизатору палаты), для проверки связи от Датчика.

```
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. Чтобы начать атаку, телнет от одного маршрутизатора к другому и напечатайте `testattack`. В этом случае мы использовали Telnet для соединения от маршрутизатора Light до маршрутизатора палаты. Как только вы нажимаете **<располагают с интервалами>** или **<входят>**, после ввода `testattack`, ваш сеанс Telnet должен быть перезагружен.


```
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. Telnet к маршрутизатору (House) и вводит команду `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. От Просмотра событий нажмите **Query Database** для новых событий теперь для просмотра предупреждения для наступления, в которое ранее

ПОШЛИ.

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. В конечном счете Средство просмотра, выделите и щелкните правой кнопкой мыши сигнал тревоги, затем выберите **View Context Buffer** или **View NSDB** для просмотра более подробной информации о сигнале тревоги. **Примечание:** NSDB также доступен онлайн в [Энциклопедии Cisco Secure \(только зарегистрированные клиенты\)](#).

Edit View Graph Actions



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

Delete From This Grid

Delete From Database

Collapse First Group

View Context Buffer

View NSDB

Graph By Child

Graph By Time

[Устранение неполадок](#)

[Процедура устранения неполадок](#)

Используйте следующую процедуру для целей устранения проблем.

1. В MC IDS выберите **Reports> Generate**. В зависимости от типа проблемы более подробная информация должна быть найдена в одном из семи доступных отчётов.

Report Group: Audit Log		
Showing 1-7 of 7 records		
Available Reports ▾		
1.	<input type="radio"/>	Subsystem Report
2.	<input type="radio"/>	Sensor Version Import Report
3.	<input type="radio"/>	Sensor Configuration Import Report
4.	<input checked="" type="radio"/>	Sensor Configuration Deployment Report
5.	<input type="radio"/>	IDS Sensor Versions
6.	<input type="radio"/>	Console Notification Report
7.	<input type="radio"/>	Audit Log Report

Rows per page: ▾

<< Page 1 >>

- В консоли Датчика введите команду **show statistics networkaccess** и проверьте выходные данные, чтобы гарантировать, что "состояние" активно.


```
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#
```
- Гарантируйте, что коммуникационный параметр показывает, что соответствующий протокол используется, такие как Telnet или Secure Shell (SSH) с 3DES. Можно попробовать ручной SSH или Telnet от SSH/клиента Telnet на ПК, чтобы проверить, что учетные данные имени пользователя и пароля корректны. Можно тогда попробовать Telnet или SSH от самого Датчика к маршрутизатору, чтобы гарантировать, что вы в состоянии войти успешно.

Дополнительные сведения

- [Страница поддержки системы обнаружения несанкционированного доступа Cisco](#)
- [Поддержка Решения CiscoWorks VPN/Security Management Solution](#)
- [Cisco Systems – техническая поддержка и документация](#)