

使用VMS IDS MC配置IDS阻止

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[設定](#)

[網路圖表](#)

[組態](#)

[初始感測器配置](#)

[將感測器匯入IDS MC](#)

[將感測器匯入安全監視器](#)

[使用IDS MC進行特徵碼更新](#)

[配置IOS路由器的阻塞](#)

[驗證](#)

[發動攻擊並阻止攻擊](#)

[疑難排解](#)

[疑難排解程序](#)

[相關資訊](#)

簡介

本文檔提供了通過VPN/安全管理解決方案(VMS)、IDS管理控制檯(IDS MC)配置Cisco入侵檢測系統(IDS)的示例。在這種情況下，會配置Blocking from the IDS Sensor to a Cisco router (從IDS感測器到Cisco路由器的阻塞)。

必要條件

需求

配置阻止之前，請確保已滿足這些條件。

- 感測器已安裝並配置為檢測必要的通訊量。
- 監聽介面跨越到路由器的外部介面。

採用元件

本文件中的資訊是以下列軟體和硬體版本為依據。

- VMS 2.2，帶IDS MC和安全監控器1.2.3
- Cisco IDS感應器4.1.3S(63)
- 運行Cisco IOS®軟體版本12.3.5的Cisco路由器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

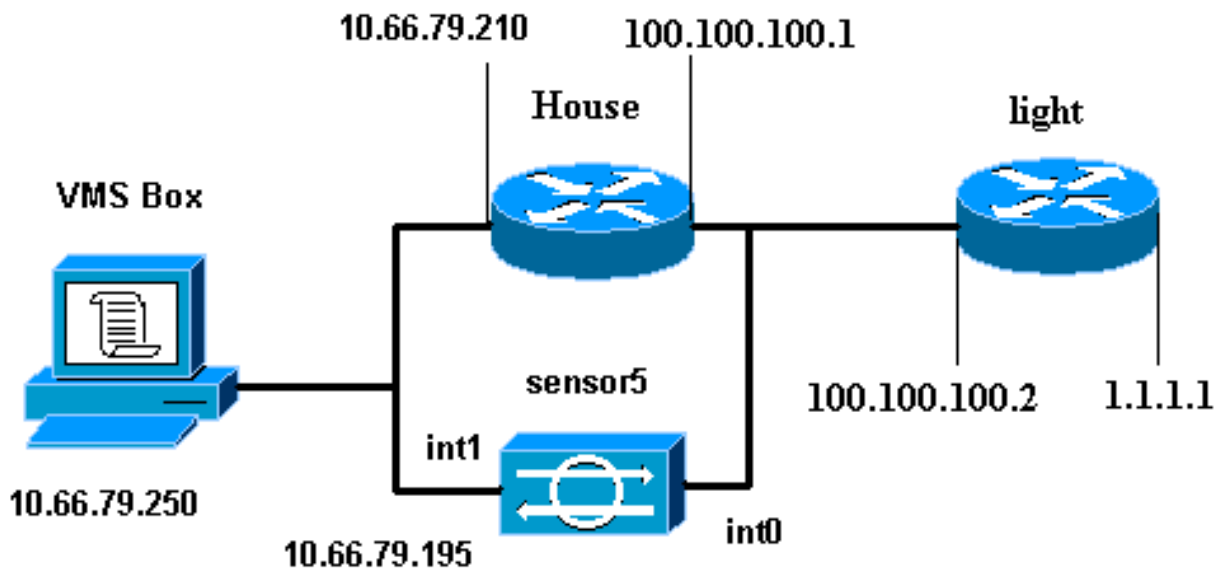
設定

本節提供用於設定本文件中所述功能的資訊。

注意：要查詢有關本文檔中使用的命令的其他資訊，請使用[命令查詢工具](#)([僅限註冊客戶](#))。

網路圖表

本檔案會使用下圖中所示的網路設定。



組態

本文檔使用此處顯示的配置。

- [路由器指示燈](#)
- [路由器外殼](#)

路由器指示燈

```
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
```

路由器外殼

```
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
```

初始感測器配置

完成以下步驟以初始配置感測器。

註：如果您已執行感測器的初始設定，請繼續執行[將感測器匯入IDS MC一節](#)。

1. 通過控制檯連線到感測器。系統將提示您輸入使用者名稱和密碼。如果這是您第一次控制檯到感測器，則必須使用使用者名稱**cisco**和密碼**cisco**登入。
2. 系統將提示您更改密碼，然後重新鍵入新密碼進行確認。
3. 在每次提示時鍵入**setup**並輸入適當的資訊，以便為感測器設定基本引數，如以下示例所示：

```
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. 按**2**儲存配置。

[將感測器匯入IDS MC](#)

完成以下步驟，將感測器匯入IDS MC。

1. 瀏覽到感測器。在這種情況下，瀏覽至<http://10.66.79.250:1741>或<https://10.66.79.250:1742>。
2. 使用適當的使用者名稱和密碼登入。在本例中，使用了使用者名稱**admin**和密碼**cisco**。
3. 選擇**VPN/Security Management Solution > Management Center**，然後選擇**IDS Sensors**。
4. 按一下**Devices (裝置)** 頁籤，選擇**Sensor Group (感測器組)**，選中**Global (全域性)**，然後按一下**Create Subgroup (建立子組)**。
5. 輸入**Group Name**並確保選中**Default**單選按鈕，然後按一下**OK**將子組新增到IDS MC中。

Add Group

Group Name: * test

Parent: Global

Description:

Settings:

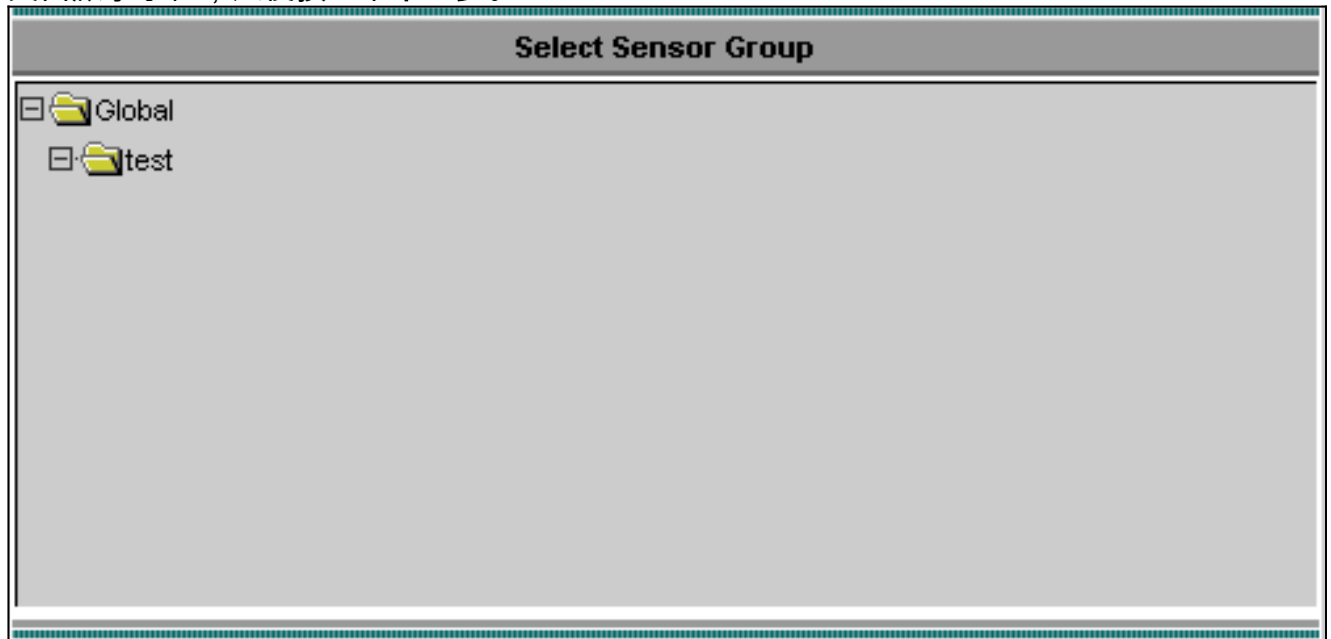
Default (use parent values)

Copy settings from group Global

OK Cancel

Note: * - Required Field

6. 選擇 **Devices > Sensor**，突出顯示在上一步中建立的子組(在本例中為 **test**)，然後按一下 **Add**。
7. 突出顯示子組，然後按一下 **下一步**。



8. 根據此示例輸入詳細資訊，然後按一下 **下一步** 繼續。

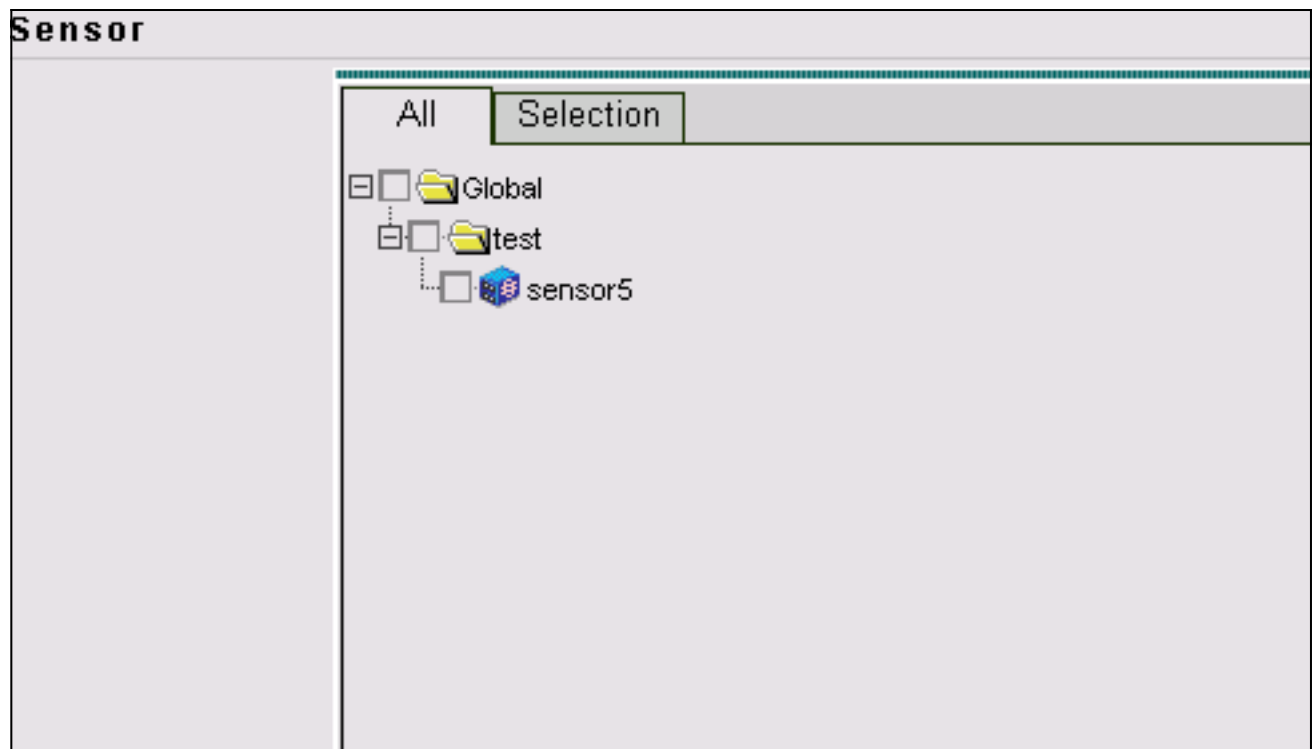
Identification	
IP Address: *	10.66.79.195
NAT Address:	
Sensor Name (required if not Discovering Settings):	sensor5
Discover Settings:	<input checked="" type="checkbox"/>
SSH Settings:	
User ID: *	cisco
Password: (or pass phrase if using existing SSH keys): *	XXXXXXXXXXXXXXXX
Use Existing SSH keys: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

Note: * - Required Field

9. 顯示消息 `Successfully imported sensor configuration` 後，按一下 **Finish** 繼續。

Import Status
<pre> Successfully imported sensor configuration. Sensor Name: sensor5 Sensor Version: 4.1(3)S62 Group: test </pre>

10. 感測器被匯入到IDS MC中。在這種情況下，會匯入感測器5。



將感測器匯入安全監視器

完成此過程，將感測器匯入安全監控器。

1. 在VMS Server選單中，選擇VPN/Security Management Solution > Monitoring Center > Security Monitor。
2. 選擇Devices (裝置) 頁籤，然後按一下Import，然後根據此示例輸入IDS MC Server Information (IDS MC伺服器資訊)。

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="*****"/>

Note: * - Required Field


3. 選擇感測器(本例中為sensor5)，然後按一下Next繼續。


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. 如果需要，請更新感測器的網路地址轉換(NAT)地址，然後按一下**完成**以繼續。

Showing 1 records

	Name	IP Address	 NAT Address
1.	sensor5	10.66.79.195	<input type="text"/>

 -- Editable columns

5. 按一下**OK**以完成將感測器從IDS MC匯入到Security Monitor。

Import Summary:

```

1 device(s) were imported.

Following 1 device(s) were imported successfully:
[sensor5]
  
```

OK

6. 已成功匯入感測器。

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 >>

使用IDS MC進行特徵碼更新

完成此過程以使用IDS MC進行特徵碼更新。

1. 從下載中下載[網路IDS簽名更新](#)(僅供註冊客戶使用)，並將其儲存在VMS伺服器上的 C:\PROGRA~1\CSCOPx\MDC\etc\ids\updates\目錄中。
2. 在VMS伺服器控制檯上，選擇VPN/安全管理解決方案 > 管理中心 > 感測器。
3. 按一下Configuration頁籤，選擇Updates，然後按一下Update Network IDS Signatures。
4. 從下拉選單中選擇要升級的簽名，然後按一下Apply繼續。

Update Network IDS Signature Settings

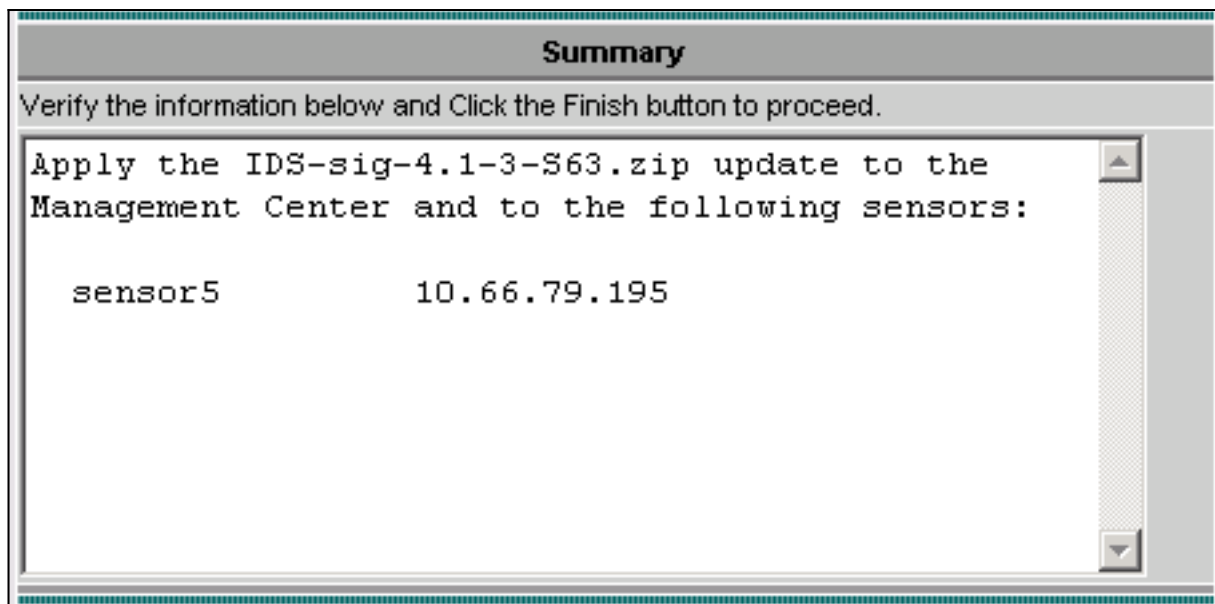
Update File:

5. 選擇要更新的感測器，然後按一下下一步繼續。

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. 當系統提示您將更新應用於管理中心和感測器後，按一下完成繼續。



7. 通過Telnet或控制檯連線到感測器命令列介面。將顯示類似以下內容的資訊：

```
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. 請等待幾分鐘，以允許升級完成，然後輸入show version以進行驗證。

```
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
```

[配置IOS路由器的阻塞](#)

完成以下步驟即可為IOS路由器配置阻止。

1. 在VMS伺服器控制檯上，選擇VPN/Security Management Solution > Management Center > IDS Sensors。
2. 選擇Configuration (配置) 頁籤，從Object Selector (對象選擇器) 中選擇Sensor (感測器)，然後按一下Settings (設定)。
3. 選擇Signatures，按一下Custom，然後按一下Add新增新簽名。

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 >>

- 輸入新的簽名名稱，然後選擇引擎(在本例中為STRING.TCP)。
- 您可以通過選中相應的單選按鈕並按一下編輯來自定義可用引數。在本示例中，編輯 ServicePorts 引數將其值更改為23 (對於埠23)。也會編輯RegexString 引數以新增value testattack。完成此操作後，按一下OK繼續。

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

- 要編輯簽名嚴重性和操作或啟用/禁用簽名，請按一下簽名名稱。

Signature Group: Filter Source:

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: << Page 1 >>

- 在這種情況下，嚴重性會更改為高，並會選擇Block Host操作。按一下OK繼續。Block Host阻止攻擊IP主機或IP子網。Block Connection阻止TCP或UDP埠(基於攻擊TCP或UDP連線)。

Edit Signature(s)

Signature:

Enable

Severity:

Actions: Log Reset Block Host Block Connection

8. 完整的簽名類似於以下內容

Signature Group: Filter Source:

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: << Page 1 >>

9. 要配置阻塞裝置，請從對象選擇器（螢幕左側的選單）中選擇Blocking > Blocking Devices，然後按一下Add輸入以下資訊

Blocking Device

Device Type: *

IP Address: *

NAT Address:

Comment:

Username:

Password: *

Enable Password:

Secure Communications:

Interfaces: * [Edit Interfaces](#)

Note: * - Required Field

10. 按一下**Edit Interfaces** (請參見以前的螢幕捕獲)，按一下**Add**，輸入此資訊，然後按一下**OK**繼續。

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. 按一下**OK**兩次以完成阻塞裝置的配置。

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. 要配置阻止屬性，請選擇**Blocking > Blocking Properties**。可以修改「自動阻止的長度」。在這種情況下，將更改為**15分鐘**。按一下「**Apply**」以繼續。

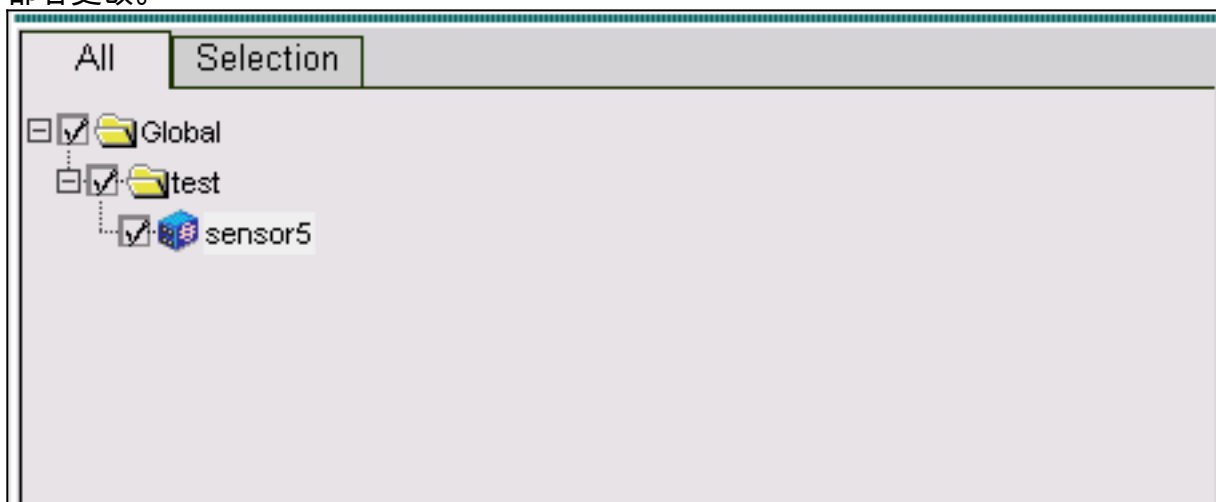
Blocking Properties	
Length of Automatic Block	<input type="text" value="15"/> minutes
Maximum ACL Entries	<input type="text" value="100"/>
Enable ACL Logging	<input type="checkbox"/>
Allow blocking devices to block the sensor's IP address	<input type="checkbox"/>
<input checked="" type="checkbox"/>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

13. 從主選單中選擇**Configuration**，然後選擇**Pending**，檢查掛起的配置以確保其正確，然後按一下**Save**。

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. 若要將配置更改推送到感測器，請通過選擇**Deployment > Generate**並按一下**Apply**來生成並

部署更改。



15. 選擇 **Deployment > Deploy**，然後按一下 **Submit**。
16. 勾選感測器旁邊的覈取方塊，然後按一下 **Deploy**。
17. 選中隊列中作業的覈取方塊，然後按一下下一步繼續。

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. 輸入作業名稱並將作業安排為立即，然後按一下 **完成**。

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. 選擇 **Deployment > Deploy > Pending**。請等待幾分鐘，直到完成所有掛起的作業。然後隊列

為空。

20. 要確認部署，請選擇**Configuration > History**。確保配置狀態顯示為**Deployed**。這意味著已成功更新感測器配置。

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 >>

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

[輸出直譯器工具](#) (僅供註冊客戶使用) 支援某些show命令，此工具可讓您檢視show命令輸出的分析。

發動攻擊並阻止攻擊

要驗證阻止過程是否正常工作，請發起測試攻擊並檢查結果。

1. 發起攻擊之前，請選擇**VPN/安全管理解決方案 > Monitoring Center > Security Monitor**。
2. 從主選單中選擇**Monitor**，按一下**Events**，然後按一下**Launch Event Viewer**。

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

3. Telnet到路由器 (本例中為Telnet到House路由器)，檢驗來自感測器的通訊。

```
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. 要發起攻擊，請從一台路由器Telnet到另一台路由器，然後鍵入**testattack**。在這種情況下，我們使用Telnet從Light路由器連線到House路由器。輸入testattack後，只要按<space>或

<enter>鍵，就應重置Telnet會話。

```
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至路由器(House)並輸入命令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. 在事件檢視器中，按一下Query Database (立即查詢新事件)以檢視先前發起的攻擊的警報

o

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. 在事件檢視器中，突出顯示並按一下右鍵警報，然後選擇View Context Buffer或View NSDB以檢視警報的詳細資訊。注意：NSDB也可在Cisco Secure Encyclopedia(僅限註冊客戶)上線上提供。

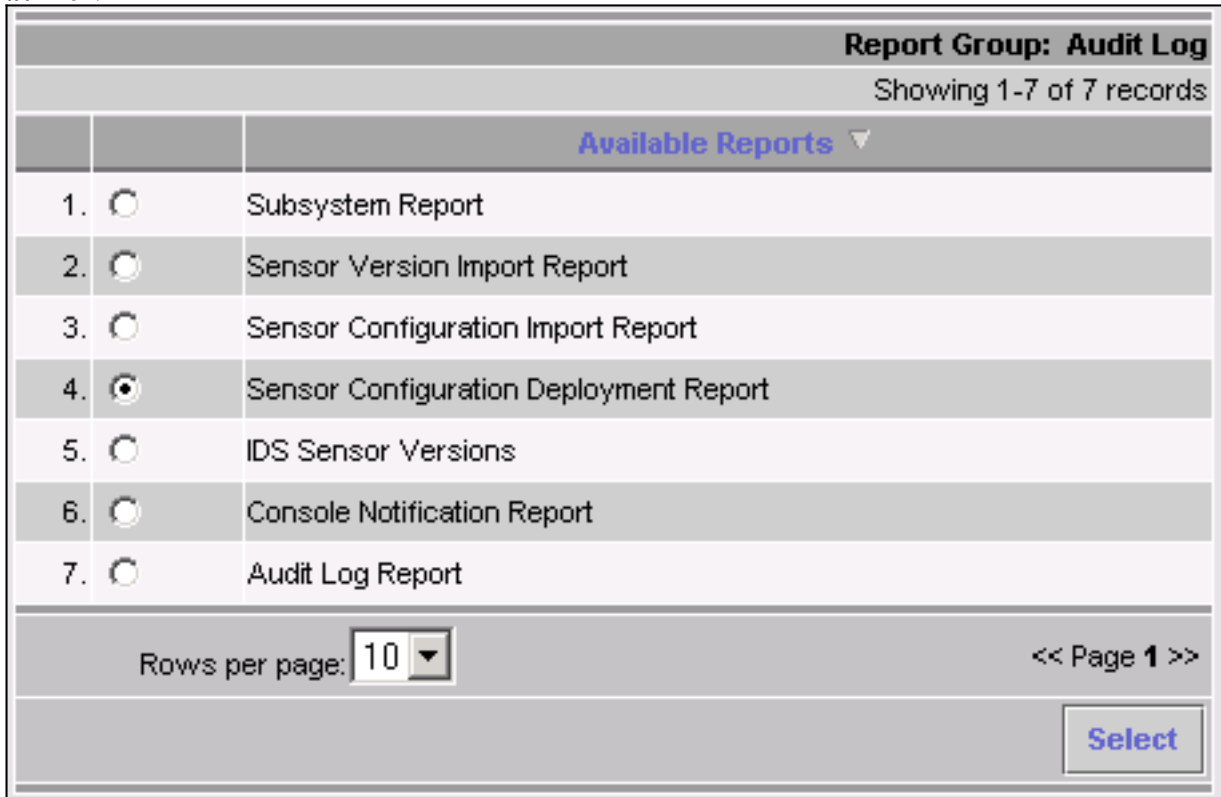
Count	IDS Alarm Type	Sig Name	Severity	Sensor Name	OS Family	OS	Attack Type	Service
1	IDIOM	mytest	High	sensor5	<n/a>	<n/a>	<n/a>	<n/a>

- Delete From This Grid
- Delete From Database
- Collapse First Group
- View Context Buffer
- View NSDB
- Graph By Child
- Graph By Time

疑難排解程序

使用以下步驟進行故障排除。

1. 在IDS MC中，選擇**Reports > Generate**。根據問題型別，應在七份可用報告中之一找到更多詳細資訊。



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 >>

2. 在感測器控制檯中，輸入命令**show statistics networkaccess**並檢查輸出以確保「state」處於活動狀態。

```
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. 確保通訊引數顯示使用的協定正確，例如使用3DES的Telnet或安全外殼(SSH)。您可以從PC上的SSH/Telnet客戶端嘗試手動SSH或Telnet，檢查使用者名稱和密碼憑據是否正確。然後，您可以嘗試從感測器本身到路由器的Telnet或SSH，以確保能夠成功登入。

相關資訊

- [思科安全入侵偵測支援頁面](#)
- [CiscoWorks VPN/安全管理解決方案支援](#)
- [技術支援與文件 - Cisco Systems](#)