

Configurazione del blocco IDS mediante VMS IDS MC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazione iniziale del sensore](#)

[Importare il sensore in IDS MC](#)

[Importare il sensore in Monitor di protezione](#)

[Utilizza IDS MC per gli aggiornamenti della firma](#)

[Configurazione del blocco per il router IOS](#)

[Verifica](#)

[Lanciare l'attacco e il blocco](#)

[Risoluzione dei problemi](#)

[Procedura di risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

Questo documento offre un esempio per la configurazione di Cisco Intrusion Detection System (IDS) tramite VPN/Security Management Solution (VMS) e IDS Management Console (IDS MC). In questo caso, è configurato il blocco da IDS Sensor a un router Cisco.

Prerequisiti

Requisiti

Prima di configurare il blocco, verificare che siano soddisfatte queste condizioni.

- Il sensore viene installato e configurato per rilevare il traffico necessario.
- L'interfaccia di sniffing viene estesa all'interfaccia esterna del router.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware.

- VMS 2.2 con IDS MC e Security Monitor 1.2.3
- Sensore Cisco IDS 4.1.3S(63)
- Router Cisco con software Cisco IOS® versione 12.3.5

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

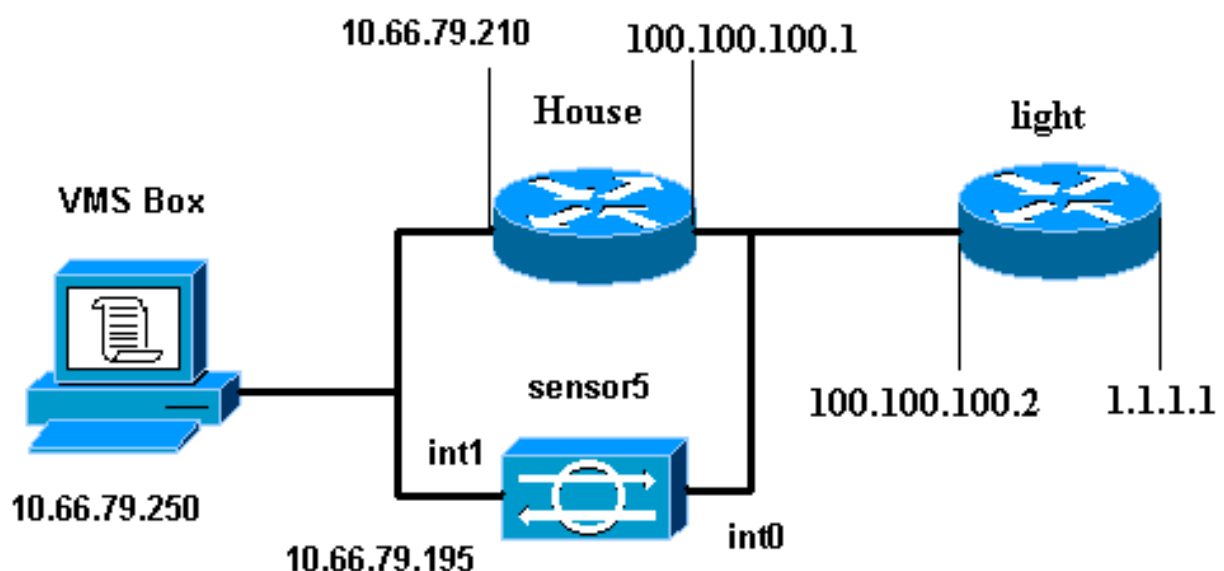
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo [strumento di ricerca dei comandi](#) (solo utenti [registrati](#)).

Esempio di rete

Nel documento viene usata l'impostazione di rete mostrata nel diagramma.



Configurazioni

Nel documento vengono usate le configurazioni mostrate di seguito.

- [Luce router](#)
- [Router House](#)

Luce router

```
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
```

Configurazione iniziale del sensore

Completare questa procedura per configurare inizialmente il sensore.

Nota: se è stata eseguita la configurazione iniziale del sensore, passare alla sezione [Importazione del sensore in IDS MC](#).

1. Collegare la console al sensore. Vengono richiesti un nome utente e una password. Se si sta effettuando la console per la prima volta nel sensore, è necessario eseguire il login con il nome utente **cisco** e la password **cisco**.
2. Viene richiesto di modificare la password e quindi digitare nuovamente la nuova password per confermarla.
3. Digitare **setup** e immettere le informazioni appropriate ad ogni richiesta di impostazione dei parametri di base per il sensore, come indicato nell'esempio seguente:

```
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. Premere **2** per salvare la configurazione.

Importare il sensore in IDS MC

Completare questa procedura per importare il sensore nell'IDS MC.

1. Accedere al sensore. In questo caso, selezionare **http://10.66.79.250:1741** o **https://10.66.79.250:1742**.
2. Eseguire l'accesso con il nome utente e la password appropriati. Nell'esempio sono stati usati il nome utente **admin** e la password **cisco**.

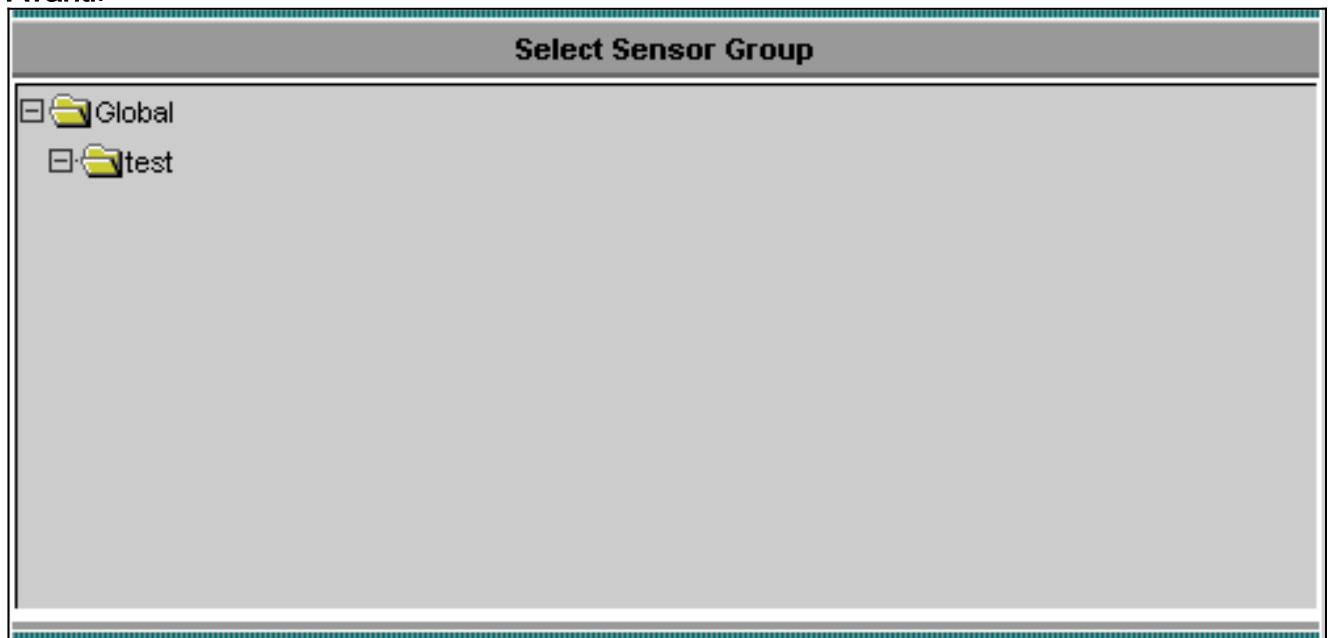
3. Selezionare **VPN/Security Management Solution > Management Center** e scegliere **IDS Sensor**.
4. Fare clic sulla scheda **Dispositivi**, selezionare **Gruppo sensori**, evidenziare **Globale** e fare clic su **Crea sottogruppo**.
5. Immettere il Nome gruppo e assicurarsi che il pulsante di scelta **Predefinito** sia selezionato, quindi fare clic su **OK** per aggiungere il sottogruppo al MC

The screenshot shows a dialog box titled "Add Group". It contains the following fields and options:

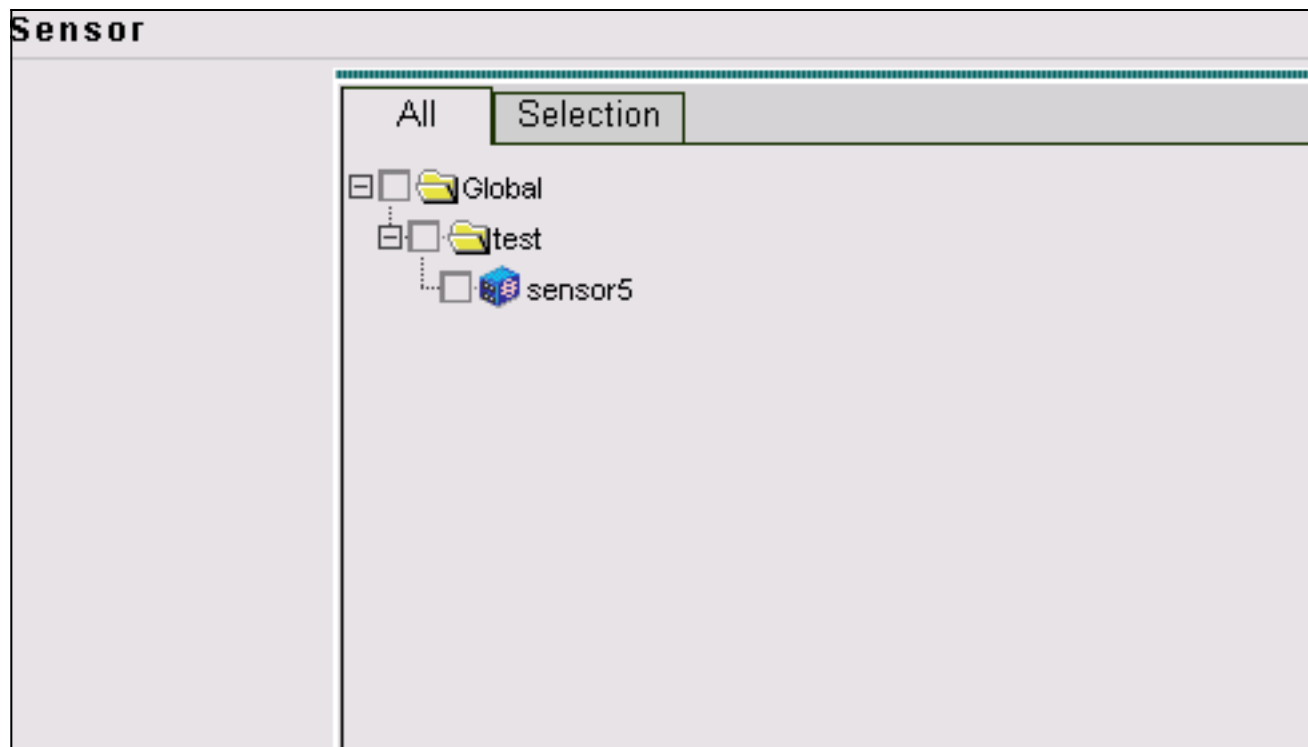
- Group Name:** A text input field containing "test". A red asterisk indicates it is a required field.
- Parent:** A dropdown menu set to "Global".
- Description:** A large empty text area with scrollbars.
- Settings:** Two radio button options:
 - Default (use parent values)
 - Copy settings from group
- Copy settings from group:** A dropdown menu set to "Global".
- Buttons:** "OK" and "Cancel" buttons.
- Note:** A note at the bottom left states "Note: * - Required Field".

6. Selezionare **Dispositivi > Sensore**, evidenziare il sottogruppo creato nel passaggio precedente (in questo caso, **test**) e fare clic su **Aggiungi**.
7. Evidenziare il sottogruppo e fare clic su

Avanti.



8. Immettere i dettagli come indicato in questo esempio, quindi fare clic su **Avanti** per continuare.



Importare il sensore in Monitor di protezione

Completare questa procedura per importare il sensore nel monitor di protezione.

1. Nel menu del server VMS, selezionare **VPN/Security Management Solution > Monitoring Center > Security Monitor**.
2. Selezionare la scheda Devices, quindi fare clic su **Import** e immettere IDS MC Server Information, come indicato in questo

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

esempio.


3. Selezionare il Sensore (in questo caso, **sensor5**) e fare clic su **Avanti** per continuare.


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. Se necessario, aggiornare l'indirizzo NAT (Network Address Translation) del sensore, quindi fare clic su **Fine** per continuare.

Showing 1 records

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

 -- Editable columns

5. Fare clic su **OK** per completare l'importazione del sensore da IDS MC in Security

Import Summary:

```

1 device(s) were imported.

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

```

OK

Monitor.

6. Importazione del sensore completata.

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 >>

[Utilizza IDS MC per gli aggiornamenti della firma](#)

Completare questa procedura per utilizzare IDS MC per gli aggiornamenti della firma.

1. Scaricare gli [aggiornamenti delle firme IDS di rete](#) (solo utenti [registrati](#)) dalla sezione Download e salvarli nella directory C:\PROGRA~1\CSCOpX\MDC\etc\ids\updates\ del server VMS.
2. Dalla console del server VMS, selezionare **VPN/Security Management Solution > Management Center > Sensor** (Soluzione di gestione VPN/sicurezza > Centro di gestione > Sensori).
3. Fare clic sulla scheda Configurazione, selezionare **Aggiornamenti** e fare clic su **Aggiorna firme ID di rete**.
4. Selezionare la firma che si desidera aggiornare dal menu a discesa e fare clic su **Applica** per continuare.

Update Network IDS Signature Settings

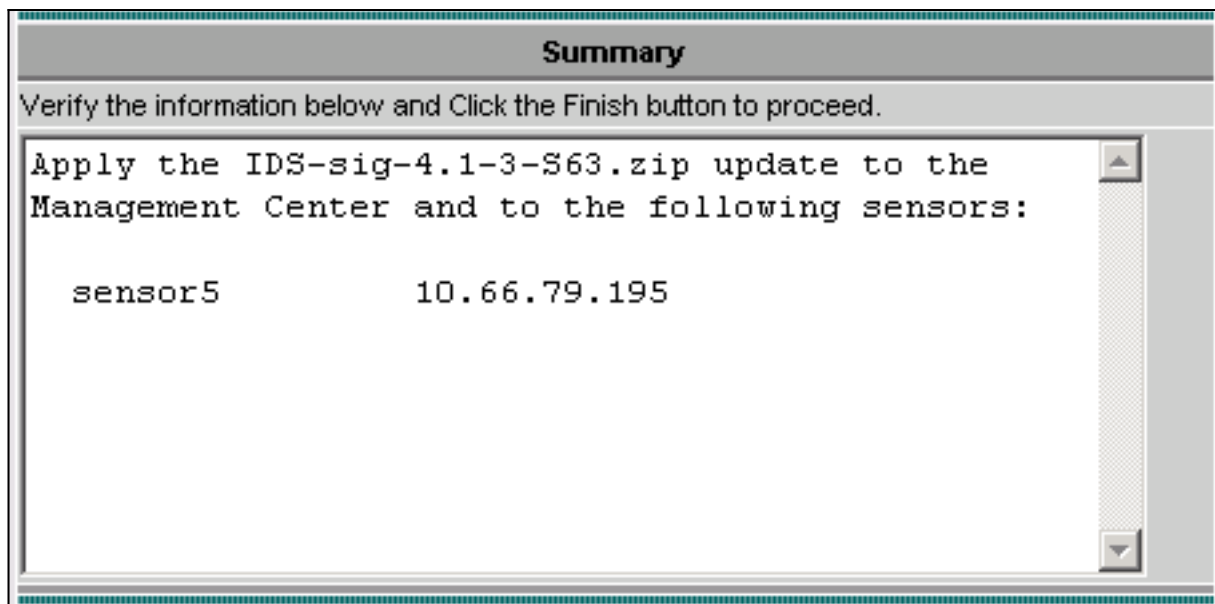
Update File:

5. Selezionare i sensori da aggiornare e fare clic su **Avanti** per continuare.

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. Dopo la richiesta di applicazione dell'aggiornamento al centro di gestione e al sensore, fare clic su **Fine** per continuare.



7. Telnet o console nell'interfaccia della riga di comando del sensore. Vengono visualizzate informazioni simili a questa:

```
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. Attendere alcuni minuti per consentire il completamento dell'aggiornamento, quindi immettere **show version** per la verifica.

```
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
```

[Configurazione del blocco per il router IOS](#)

Completare questa procedura per configurare il blocco per il router IOS.

1. Dalla console del server VMS, selezionare **VPN/Security Management Solution > Management Center > IDS Sensor**.
2. Selezionare la scheda Configurazione, selezionare il sensore in Selettore oggetti e fare clic su **Impostazioni**.
3. Selezionare **Firme**, fare clic su **Personalizzate**, quindi su **Aggiungi** per aggiungere una nuova firma.

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 >>

- Immettere il nuovo Nome firma, quindi selezionare il Motore (in questo caso, **STRING.TCP**).
- È possibile personalizzare i parametri disponibili selezionando il pulsante di opzione appropriato e facendo clic su **Modifica**. In questo esempio, il parametro ServicePorts viene modificato in modo da modificarne il valore in 23 (per la porta 23). Viene inoltre modificato il parametro RegexString per aggiungere il valore **testattack**. Al termine, fare clic su **OK** per continuare.

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

- Per modificare il livello di gravità e le azioni della firma o per attivare/disattivare la firma, fare clic sul nome della firma.

		Signature Group:	Custom	Filter Source:	Signature	<input type="text"/>	<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	Medium	None
Rows per page:		10		<< Page 1 >>			
							<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

7. In questo caso, la severità viene modificata in **Alta** e viene selezionata l'azione **Blocca host**. Fare clic su **OK** per continuare. Blocca host che attaccano host IP o subnet IP. Blocca connessione blocca le porte TCP o UDP (in base all'attacco alle connessioni TCP o

Edit Signature(s)	
Signature:	<input type="text" value="mytest"/>
	<input checked="" type="checkbox"/> Enable
Severity:	High
Actions:	<input type="checkbox"/> Log <input type="checkbox"/> Reset <input checked="" type="checkbox"/> Block Host <input type="checkbox"/> Block Connection
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

UDP).

8. La firma completa è simile alla seguente:

		Signature Group:	Custom	Filter Source:	Signature	<input type="text"/>	<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:		10		<< Page 1 >>			
							<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

9. Per configurare il dispositivo di blocco, selezionare **Blocco > Dispositivi di blocco** dal selettore oggetti (il menu sul lato sinistro della schermata), quindi fare clic su **Aggiungi** per immettere le seguenti informazioni:

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. Fare clic su **Edit Interfaces** (vedere l'acquisizione schermo precedente), fare clic su **Add**, immettere queste informazioni, quindi fare clic su **OK** per continuare.

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. Fare clic su **OK** due volte per completare la configurazione del dispositivo di blocco.

Showing 1-1 of 1 records				
	IP Address	Device Type	Comment	Source
1.	10.66.79.210	Cisco Router		sensor5
Rows per page: 10				<< Page 1 >>
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				

12. Per configurare le proprietà di blocco, selezionare **Blocco > Proprietà di blocco**. È possibile modificare la lunghezza del blocco automatico. In questo caso, viene modificato in **15 minuti**. Fare clic su **Apply** (Applica) per continuare.

Blocking Properties	
Length of Automatic Block	15 minutes
Maximum ACL Entries	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. Selezionare **Configurazione** dal menu principale, quindi selezionare **In sospeso**, controllare la configurazione in sospeso per assicurarsi che sia corretta e fare clic su

Showing 1-1 of 1 records

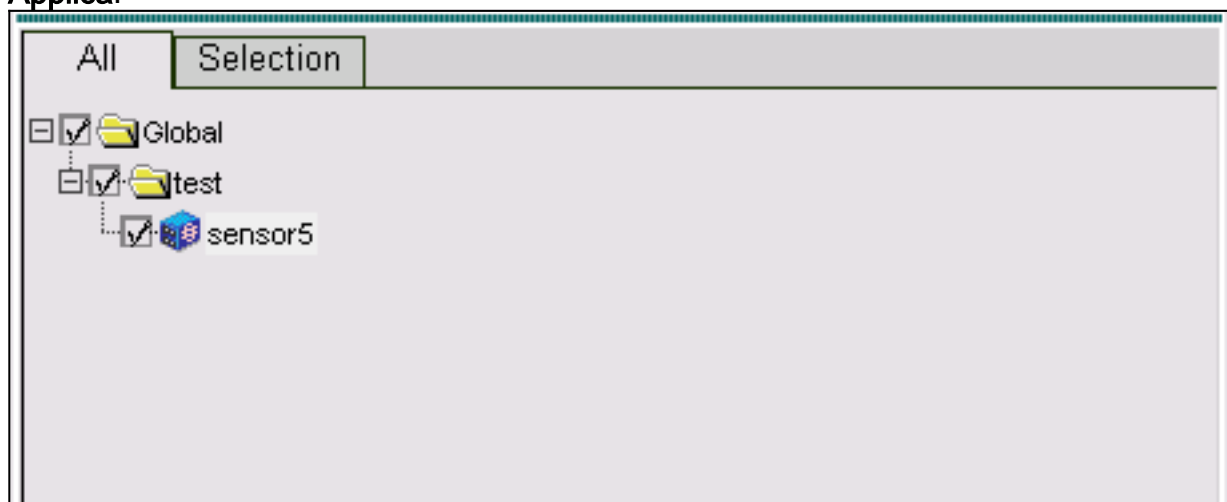
<input type="checkbox"/>	Pending Configuration	Type	Last Modified On	Last Modified By
1. <input checked="" type="checkbox"/>	Global.test.sensor5	Sensor	2003-12-15 14:07:39	admin

Rows per page: 10 << Page 1 >>

Salva.

14. Per eseguire il push delle modifiche di configurazione nel sensore, generare e distribuire le modifiche selezionando **Distribuzione > Genera** e facendo clic su

Applica.



15. Selezionare **Distribuzione > Distribuisci**, quindi fare clic su **Invia**.
16. Selezionare la casella di controllo accanto al sensore, quindi fare clic su **Distribuisci**.
17. Selezionare la casella di controllo relativa al processo nella coda, quindi fare clic su **Avanti** per continuare.

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. Immettere il nome del job e programmare il job come Immediato, quindi fare clic su **Fine**.

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.)	

19. Selezionare **Distribuzione > Distribuisci > In sospenso**. Attendere alcuni minuti fino al completamento di tutti i processi in sospenso. La coda è quindi vuota.
20. Per confermare la distribuzione, selezionare **Configurazione > Cronologia**. Verificare che lo stato della configurazione sia **Distribuito**. La configurazione del sensore è stata aggiornata.

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 >>

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show** sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

Lanciare l'attacco e il blocco

Per verificare che il processo di blocco funzioni correttamente, avviare un attacco di prova e verificare i risultati.

1. Prima di lanciare l'attacco, selezionare **VPN/Security Management Solution > Centro di monitoraggio > Monitor di sicurezza**.
2. Scegliere **Monitor** dal menu principale, fare clic su **Eventi** e quindi su **Avvia Visualizzatore eventi**.

The screenshot shows the 'Launch Event Viewer' dialog box. It has a title bar 'Launch Event Viewer'. The 'Event Type' dropdown is set to 'Network IDS Alarms'. The 'Column Set' dropdown is set to 'Last Saved'. Under 'Event Start Time', the 'At Earliest' radio button is selected. Under 'Event Stop Time', the 'Don't Stop' radio button is selected. A 'Launch Event Viewer' button is located at the bottom right of the dialog.

3. Telnet su router (in questo caso, Telnet su router House), per verificare la comunicazione dal sensore.

```
house#show user
  Line      User      Host(s)      Idle      Location
*  0 con 0
  226 vty 0      idle      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. Per lanciare l'attacco, digitare **testattack** in modalità Telnet da un router all'altro. In questo caso, abbiamo utilizzato Telnet per connettersi dal router Light al router House. Non appena si preme **<space>** o **<enter>**, dopo aver digitato **testattack**, la sessione Telnet dovrebbe essere reimpostata.

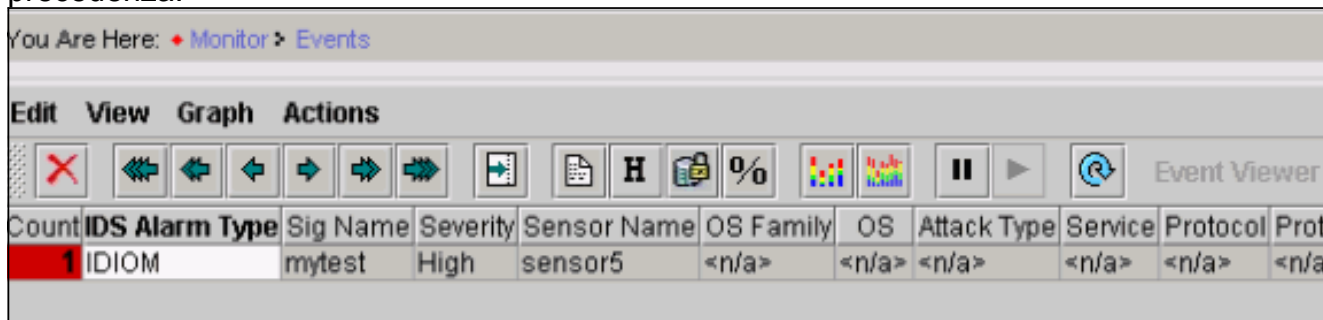
```
light#telnet 100.100.100.1
Trying 100.100.100.1 ... Open
User Access Verification
Password:
house>en
Password:
house#testattack
!--- Host 100.100.100.2 has been blocked due to the !--- signature "testattack" being
```

triggered. [Connection to 100.100.100.1 lost]

5. Telnet su router (House) e immettere il comando **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
```

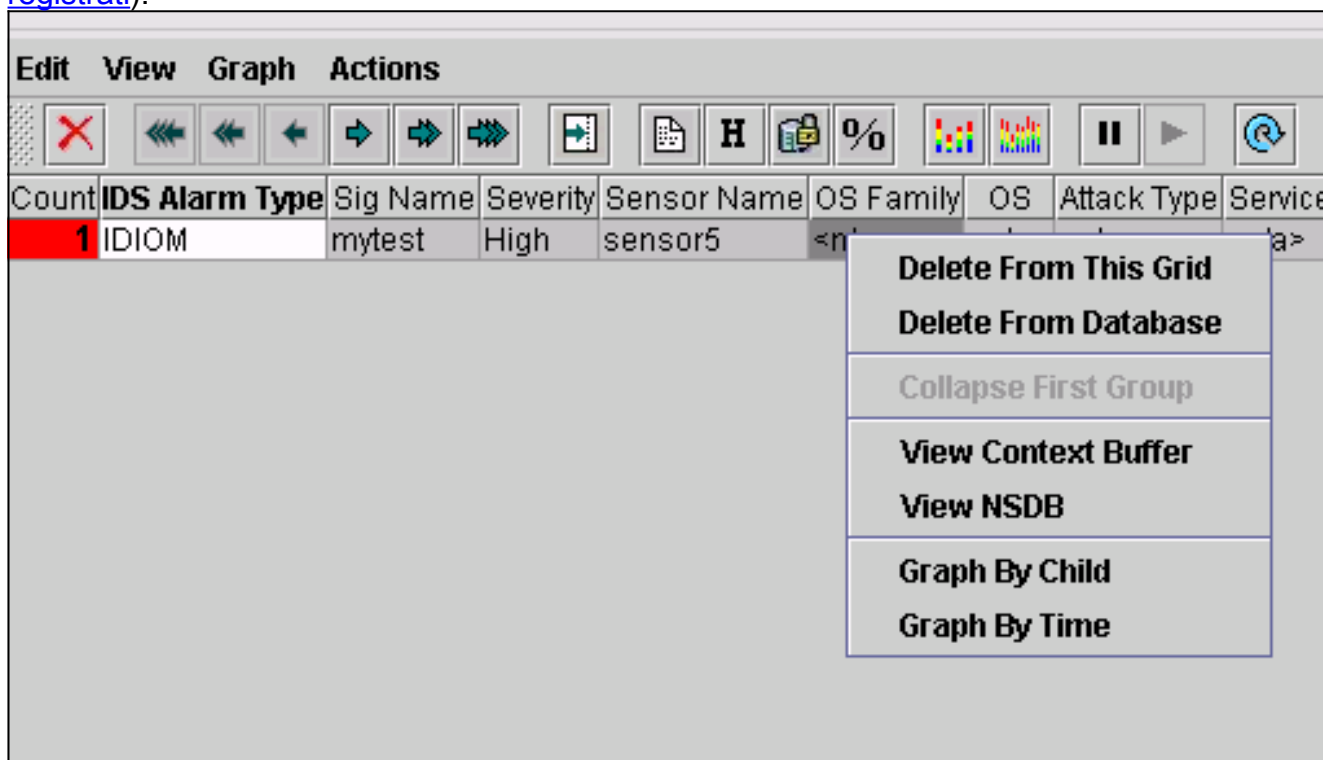
6. Dal Visualizzatore eventi, fare clic su **Esegui query su database** per i nuovi eventi per visualizzare l'avviso relativo all'attacco avviato in precedenza.



The screenshot shows the 'Event Viewer' interface with a table of events. The table has columns for Count, IDS Alarm Type, Sig Name, Severity, Sensor Name, OS Family, OS, Attack Type, Service, Protocol, and Prot. The first row is highlighted in red and contains the following data:

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. Nel Visualizzatore eventi, evidenziare e fare clic con il pulsante destro del mouse sull'allarme, quindi selezionare **Visualizza buffer contesto** o **Visualizza NSDB** per visualizzare informazioni più dettagliate sull'allarme. **Nota:** l'NSDB è disponibile anche online su [Cisco Secure Encyclopedia](#) (solo utenti registrati).



The screenshot shows the 'Event Viewer' interface with a table of events. The first row is highlighted in red. A context menu is open over the first row, showing the following options:

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

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>

[Risoluzione dei problemi](#)

[Procedura di risoluzione dei problemi](#)

Utilizzare la procedura seguente per la risoluzione dei problemi.

1. Nel MC IDS, selezionare **Report > Genera**. A seconda del tipo di problema, è possibile trovare ulteriori dettagli in uno dei sette rapporti disponibili.

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. Alla console del sensore, immettere il comando **show statistics network access** e controllare l'output per verificare che "state" sia attivo.

```

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. Verificare che il parametro di comunicazione indichi che viene utilizzato il protocollo corretto, ad esempio Telnet o Secure Shell (SSH) con 3DES. È possibile provare un'autenticazione SSH o Telnet manuale da un client SSH/Telnet su un PC per verificare che le credenziali di nome utente e password siano corrette. È quindi possibile provare a utilizzare Telnet o SSH dal sensore stesso al router per verificare che l'accesso sia riuscito.

Informazioni correlate

- [Pagina di supporto per Cisco Secure Intrusion Detection](#)
- [Supporto CiscoWorks VPN/Security Management Solution](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)