

Configurazione di IDS TCP Reset 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 reset TCP per il router IOS](#)

[Verifica](#)

[Avvia attacco e reimpostazione TCP](#)

[Risoluzione dei problemi](#)

[Procedura di risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

Nel documento viene fornita una configurazione di esempio di Cisco Intrusion Detection System (IDS) tramite VPN/Security Management Solution (VMS) e IDS Management Console (IDS MC). In questo caso, è stato configurato il reset TCP dal sensore IDS a un router Cisco.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- 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](#).

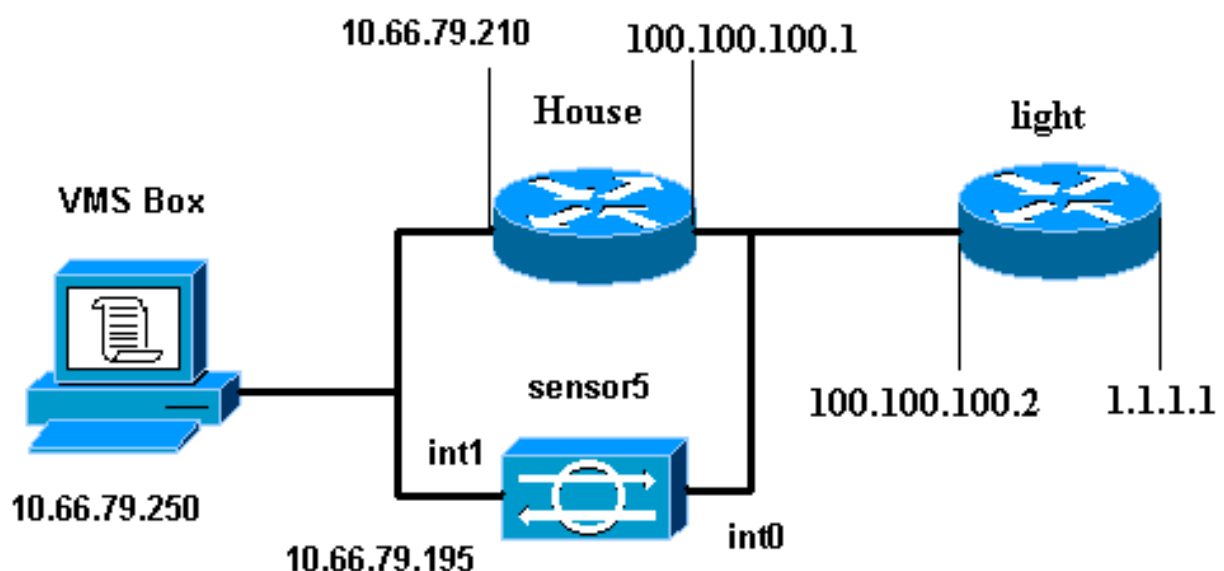
Configurazione

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 questa sezione, usare lo [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Nel documento vengono usate queste configurazioni.

- [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
  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
```

[Configurazione iniziale del sensore](#)

Nota: se l'impostazione iniziale del sensore è già stata eseguita, passare alla sezione [Importare il sensore nell'MC IDS](#).

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. Verrà richiesto di modificare la password e di digitarla nuovamente 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
```

```
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
```

[Importare il sensore in IDS MC](#)

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

1. Accedere al sensore. In questo caso, <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, il nome utente è **admin** e la password è **cisco**.
3. Scegliere **VPN/Security Management Solution > Management Center** e fare clic su **IDS Sensor**.
4. Fare clic sulla scheda **Dispositivi** e scegliere **Gruppo sensori**.
5. Evidenziare **Globale** e fare clic su **Crea sottogruppo**.

6. Immettere il Nome gruppo e assicurarsi che **Default** sia selezionato, quindi fare clic su **OK** per aggiungere il sottogruppo all'MC

Add Group

Group Name: * test

Parent: Global

Description:

Settings:

Default (use parent values)

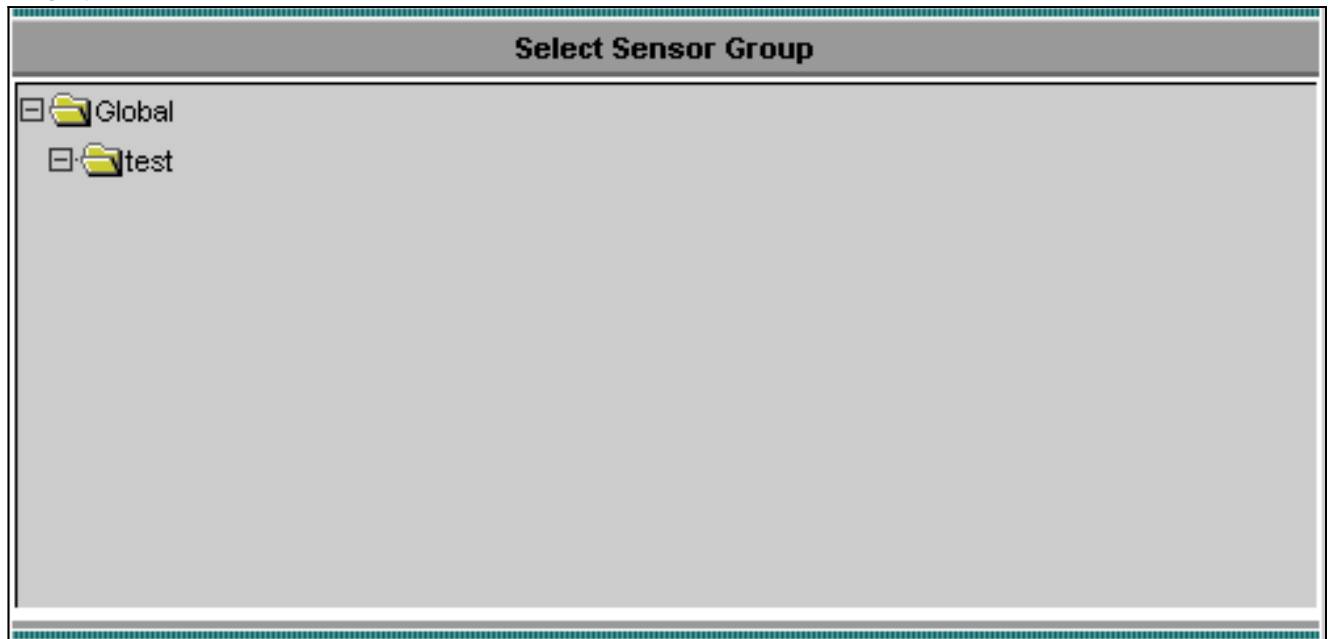
Copy settings from group Global

OK Cancel

Note: * - Required Field

IDS.

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



9. Immettere i dettagli come indicato in questo esempio e fare clic su **Avanti** per continuare.

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	

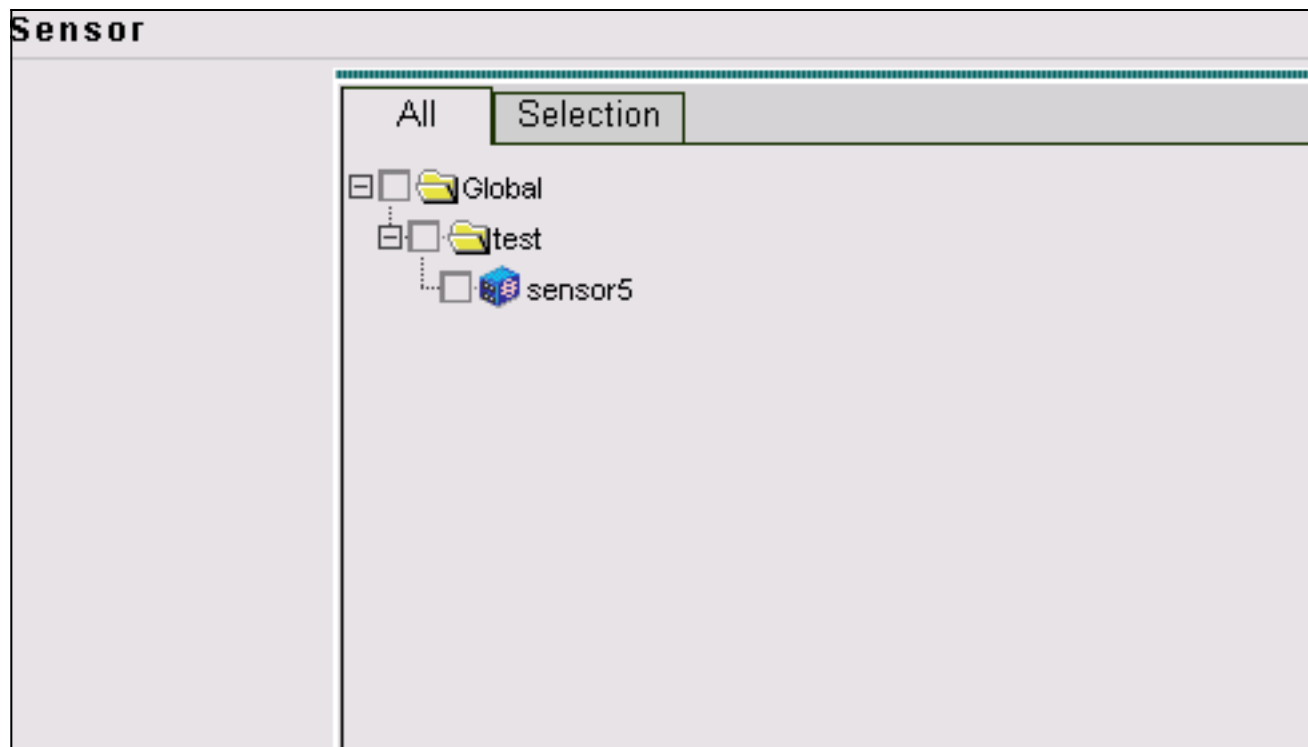
10. Quando viene visualizzato un messaggio che indica che la configurazione del sensore è stata importata correttamente, fare clic su **Fine** per continuare.

Import Status

```
Successfully imported sensor configuration.

Sensor Name: sensor5
Sensor Version: 4.1(3)S62
Group: test
```

11. Il sensore viene importato nell'IDS MC. In questo caso, viene importato il sensore 5.



Importare il sensore in Monitor di protezione

Completare questa procedura per importare il sensore in Security Monitor.

1. Nel menu del server VMS, scegliere **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

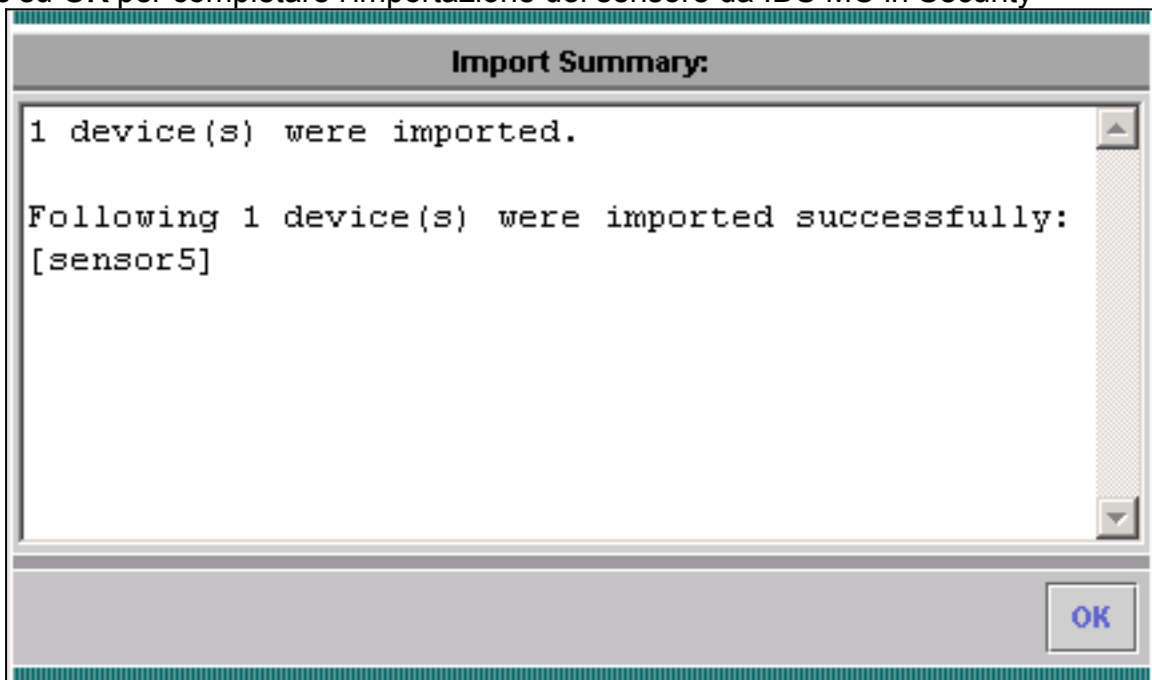
4. Se necessario, aggiornare l'indirizzo NAT del sensore, quindi fare clic su **Finish** (Fine) per continuare.

Showing 1 records

	Name	IP Address	 NAT Address
1.	sensor5	10.66.79.195	

 -- Editable columns

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



Monitor.

6. È ora possibile verificare che il sensore è stato importato correttamente

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

In questa procedura viene illustrato come utilizzare IDS MC per gli aggiornamenti delle firme.

1. Scaricare gli [aggiornamenti delle firme IDS di rete](#) (solo utenti [registrati](#)) e salvarli nella directory `C:\PROGRA~1\CSCOPx\MDC\etc\ids\updates\` del server VMS.
2. Dalla console del server VMS, scegliere **VPN/Security Management Solution > Management Center > IDS Sensor**.
3. Selezionare la scheda Configuration e fare clic su **Updates**.
4. Fare clic su **Aggiorna firme IDS di rete**.
5. Per continuare, selezionare la firma che si desidera aggiornare dal menu a discesa e fare clic su

Applica.

Update Network IDS Signature Settings

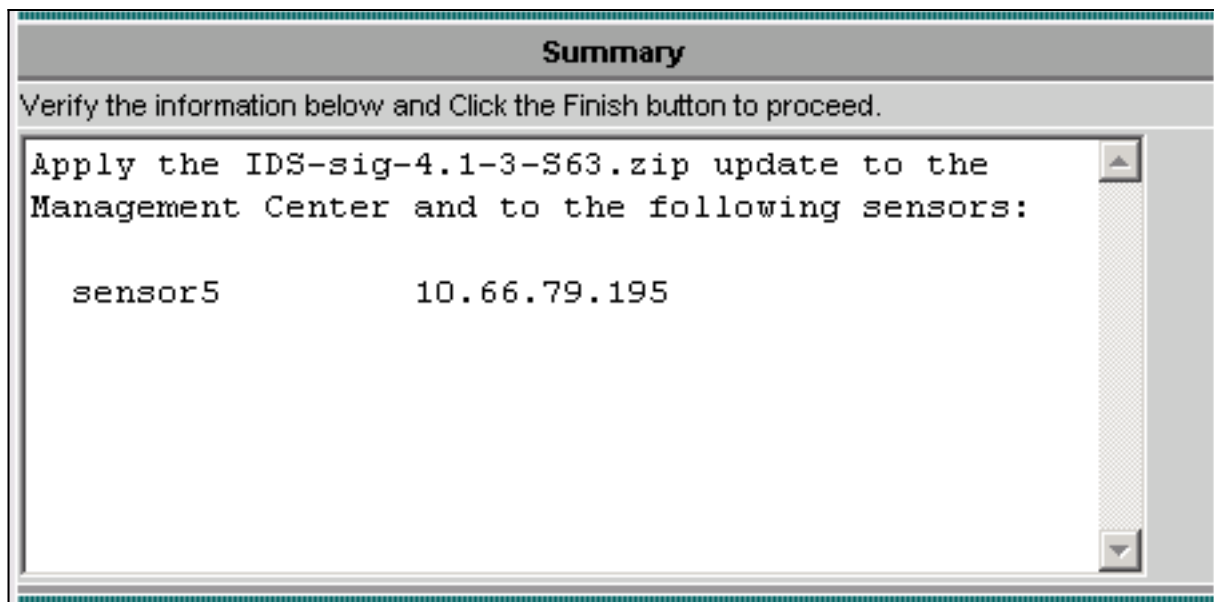
Update File:

6. 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

7. Dopo aver richiesto di applicare l'aggiornamento al centro di gestione e al sensore, fare clic su **Fine** per continuare.



8. Telnet o console nell'interfaccia della riga di comando del sensore. Vengono visualizzate informazioni simili a quelle riportate di seguito:

```
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.
```

9. 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 reset TCP per il router IOS](#)

Completare questa procedura per configurare il reset TCP del router IOS.

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

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**).
- Selezionare il pulsante di opzione appropriato per personalizzare i parametri disponibili, quindi fare 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

- Fare clic sul nome della firma per modificarne il livello di gravità e le azioni o per attivare/disattivare la firma.

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 >>

7. In questo caso, il livello di gravità viene modificato in **Alto** e viene scelta l'azione **Log & Reset**. Per continuare, fare clic su

Edit Signature(s)

Signature:

Enable

Severity:

Actions: Log Reset Block Host Block Connection

OK.

8. La firma completa è simile alla seguente:

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	Log,Reset

Rows per page: << Page 1 >>

9. Scegliere **Configurazione > In sospeso**, controllare la configurazione in sospeso per verificare che sia corretta, quindi fare clic su

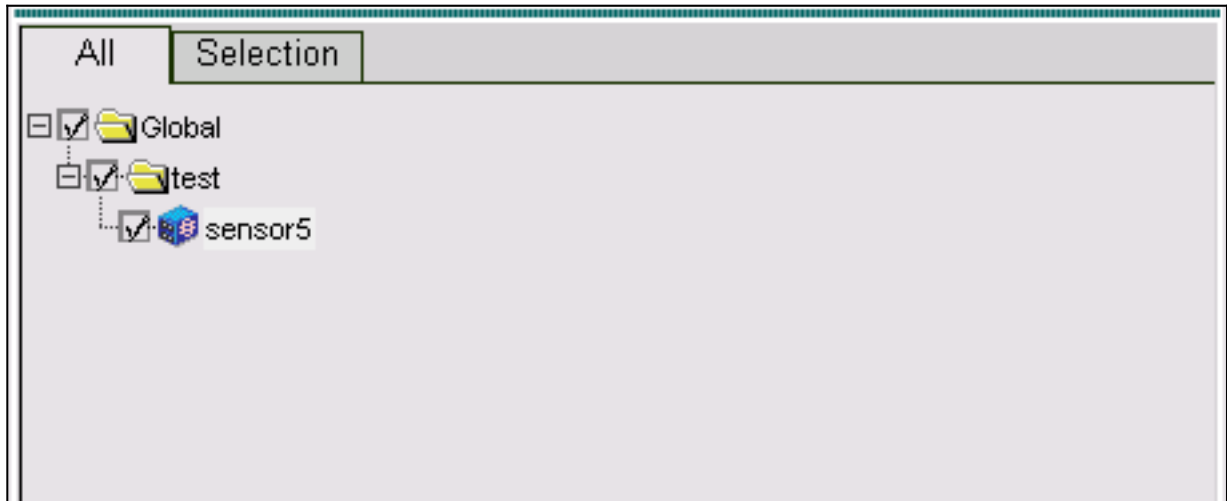
Showing 1-1 of 1 records

<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: << Page 1 >>

Salva.

10. Scegliere **Distribuzione > Genera**, quindi fare clic su **Applica** per trasferire le modifiche della configurazione al Sensore.



11. Scegliere **Distribuzione > Distribuisci** e fare clic su **Sottometti**.
12. Selezionare la casella di controllo accanto al sensore e fare clic su **Distribuisci**.
13. Selezionare la casella di spunta per il job nella coda e 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: 10 < >> Page 1 <<

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

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.)

15. Scegliere **Distribuzione > Distribuisci > In sospenso**. Attendere alcuni minuti fino al completamento di tutti i processi in sospenso. La coda dovrebbe quindi essere vuota.
16. Per confermare la distribuzione, scegliere **Configurazione > Cronologia**. Verificare che lo stato della configurazione sia **Distribuito**. Ciò significa che la configurazione del sensore è stata aggiornata correttamente.

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](#)

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

[Avvia attacco e reimpostazione TCP](#)

Avviare un attacco di prova e controllare i risultati per verificare che il processo di blocco funzioni correttamente.

1. Prima di lanciare l'attacco, scegliere **VPN/Security Management Solution > Monitoring Center**

> **Security Monitor.**

2. Selezionate **Monitor** dal menu principale e fate clic su **Events**.
3. Fare clic su **Avvia Visualizzatore eventi**.

The screenshot shows a dialog box titled "Launch Event Viewer". It has several sections: "Event Type" with a dropdown menu set to "Network IDS Alarms"; "Column Set" with a dropdown menu set to "Last Saved"; "Event Start Time" with radio buttons for "At Earliest" (selected) and "At Time" (with date and time pickers for December 15, 2003, 22:26:06); and "Event Stop Time" with radio buttons for "Don't Stop" (selected) and "At Time" (with date and time pickers for December 15, 2003, 22:26:06). A "Launch Event Viewer" button is located at the bottom right.

4. Telnet da un router all'altro e digitare **testattack** per avviare l'attacco. In questo caso, ci siamo collegati in modalità Telnet 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
```

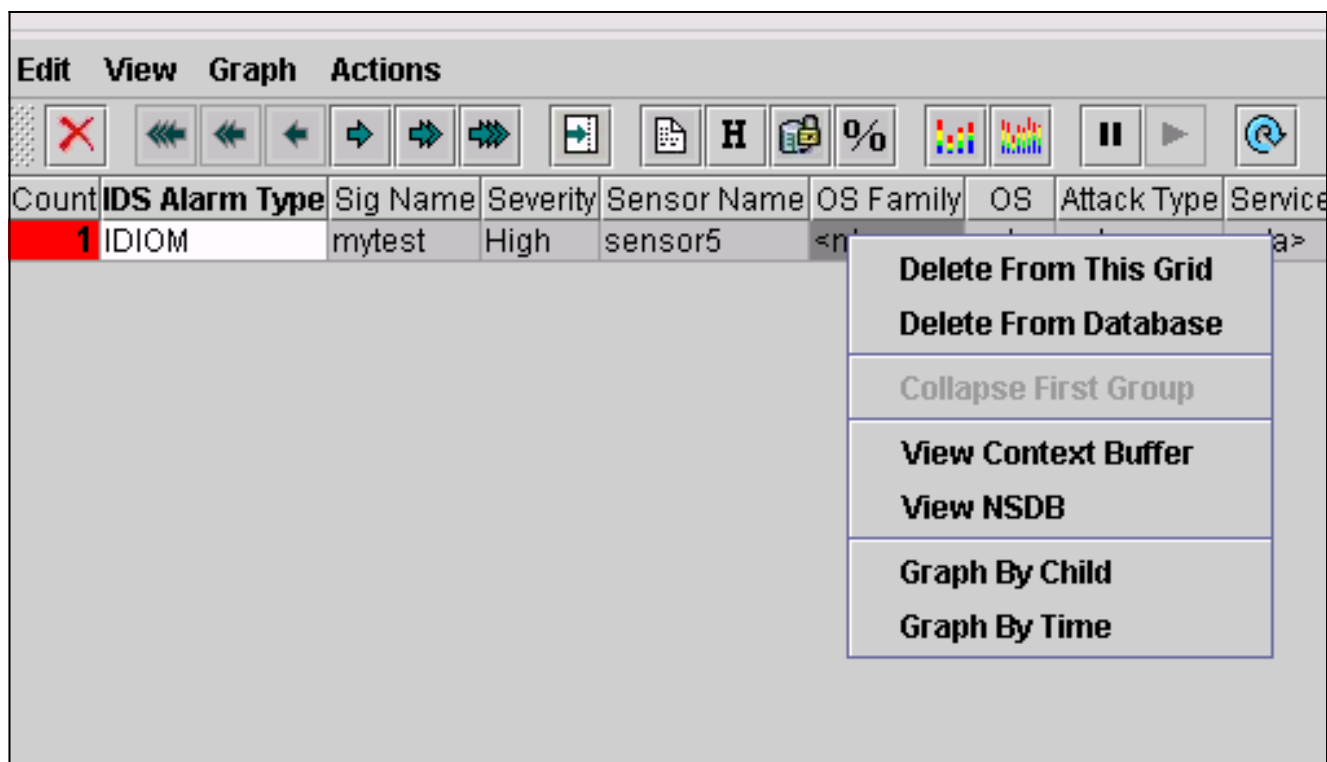
!--- The Telnet session is reset due to the !--- signature "testattack" being triggered.
[Connection to 100.100.100.1 lost]

5. Nel Visualizzatore eventi fare clic su **Esegui query su database** per i nuovi eventi. Viene visualizzato l'avviso relativo all'attacco lanciato in precedenza

The screenshot shows the "Event Viewer" interface. At the top, it says "You Are Here: Monitor > Events". Below that is a toolbar with icons for Edit, View, Graph, and Actions. The main area is a table with the following columns: 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: 1, IDS Alarm Type: IDIOM, Sig Name: mytest, Severity: High, Sensor Name: sensor5, OS Family: <n/a>, OS: <n/a>, Attack Type: <n/a>, Service: <n/a>, Protocol: <n/a>, Prot: <n/a>.

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. Nel Visualizzatore eventi, evidenziare l'allarme, fare clic con il pulsante destro del mouse e selezionare **Visualizza buffer contesto** o **Visualizza NSDB** per visualizzare informazioni più dettagliate sull'allarme.



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Procedura di risoluzione dei problemi

Per risolvere il problema, completare la procedura seguente.

1. Nel MC IDS, scegliere **Report > Genera**. A seconda del tipo di problema, ulteriori dettagli sono disponibili 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. Mentre la funzione Blocking utilizza la porta Command e Control per configurare gli elenchi degli accessi del router, i Reset TCP vengono inviati dall'interfaccia di sniffing del sensore. Verificare di aver effettuato lo spanning della porta corretta, usando il comando **set span** sullo switch, come segue:

set span

```
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. Se il comando TCP Reset non funziona, accedere al sensore e immettere il comando **show event**. Avviare l'attacco e verificare se l'allarme è attivato. Se l'allarme viene attivato, verificare che sia impostato per il tipo di azione **Reset TCP**.

[Informazioni correlate](#)

- [Pagina di supporto per Cisco Secure Intrusion Detection](#)
- [Documentazione per Cisco Secure Intrusion Detection System](#)
- [Pagina di supporto per CiscoWorks VPN/Security Management Solution](#)

- [Documentazione e supporto tecnico – Cisco Systems](#)