

Konfigurieren von IDS-TCP-Zurücksetzen mithilfe von VMS IDS MC

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Erstkonfiguration des Sensors](#)

[Importieren des Sensors in den IDS MC](#)

[Importieren des Sensors in den Sicherheitsmonitor](#)

[IDS MC für Signatur-Updates verwenden](#)

[Konfigurieren des TCP-Resets für den IOS-Router](#)

[Überprüfen](#)

[Attack und TCP Reset starten](#)

[Fehlerbehebung](#)

[Fehlerbehebungsverfahren](#)

[Zugehörige Informationen](#)

Einführung

Das Dokument enthält eine Beispielkonfiguration des Cisco Intrusion Detection System (IDS) über die VPN/Security Management Solution (VMS), IDS Management Console (IDS MC). In diesem Fall wird TCP Reset vom IDS-Sensor zu einem Cisco Router konfiguriert.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Der Sensor wird installiert und konfiguriert, um den erforderlichen Datenverkehr zu erfassen.
- Die Sniffing-Schnittstelle ist über die externe Router-Schnittstelle verbunden.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- VMS 2.2 mit IDS MC und Security Monitor 1.2.3
- Cisco IDS-Sensor 4.1.3S(63)
- Cisco Router mit Cisco IOS® Softwareversion 12.3.5

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

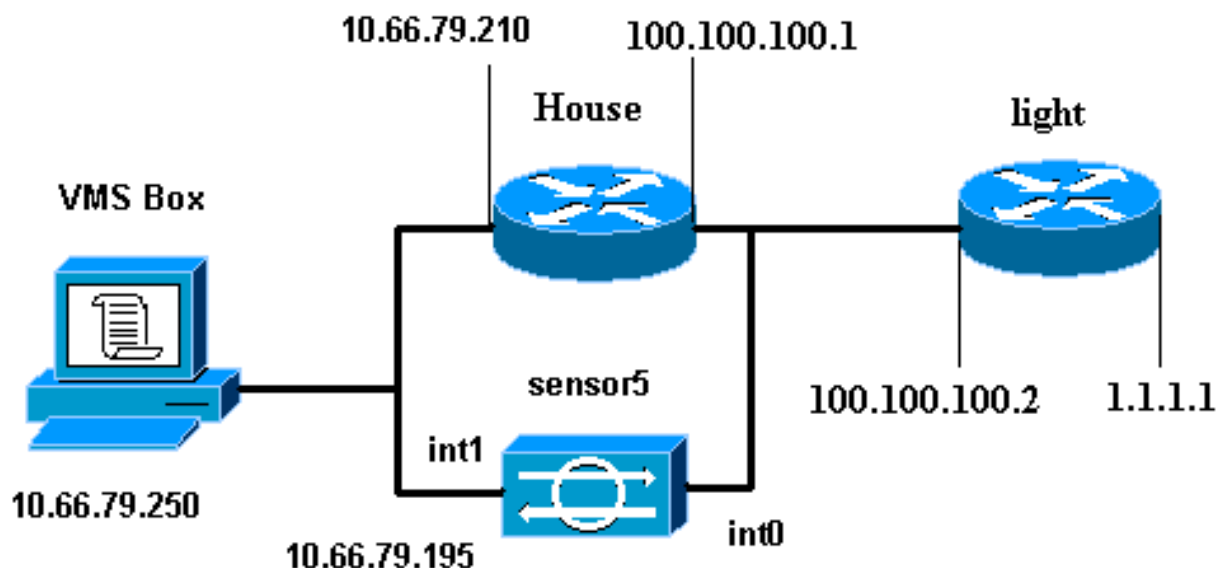
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden diese Konfigurationen verwendet.

- [Routerleuchte](#)
- [Router-Haus](#)

Routerleuchte

```
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-Haus

```
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
```

[Erstkonfiguration des Sensors](#)

Hinweis: Wenn Sie die Ersteinrichtung Ihres Sensors bereits durchgeführt haben, fahren Sie mit dem Abschnitt [Importieren des Sensors in IDS MC](#) fort.

1. Schließen Sie den Sensor an. Sie werden aufgefordert, einen Benutzernamen und ein Kennwort einzugeben. Wenn Sie sich zum ersten Mal beim Sensor anmelden, müssen Sie sich mit dem Benutzernamen **cisco** und dem Kennwort **cisco** anmelden.
2. Sie werden aufgefordert, das Kennwort zu ändern und das neue Kennwort zur Bestätigung erneut einzugeben.
3. Geben Sie **setup ein**, und geben Sie an jeder Eingabeaufforderung die entsprechenden Informationen ein, um die Eckwerte für den Sensor festzulegen. Beispiel:

```
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
```

[Importieren des Sensors in den IDS MC](#)

Führen Sie diese Schritte aus, um den Sensor in den IDS MC zu importieren.

1. Navigieren Sie zu Ihrem Sensor. In diesem Fall entweder **http://10.66.79.250:1741** oder **https://10.66.79.250:1742**.
2. Melden Sie sich mit dem entsprechenden Benutzernamen und Kennwort an. In diesem Beispiel lautet der Benutzernamen **admin** und das Kennwort **cisco**.
3. Wählen Sie **VPN/Security Management Solution > Management Center aus**, und klicken Sie auf **IDS Sensors**.

4. Klicken Sie auf die Registerkarte Geräte, und wählen Sie **Sensorgruppe** aus.
5. Markieren Sie **Global**, und klicken Sie auf **Untergruppe erstellen**.
6. Geben Sie den Gruppennamen ein, und stellen Sie sicher, dass **Default** ausgewählt ist. Klicken Sie dann auf **OK**, um die Untergruppe dem IDS MC

Add Group

Group Name: * test

Parent: Global

Description:

Settings:

Default (use parent values)

Copy settings from group Global

OK Cancel

Note: * - Required Field

hinzuzufügen.

7. Wählen Sie **Geräte** > **Sensor**, markieren Sie die im vorherigen Schritt erstellte Untergruppe (in diesem Fall **Test**), und klicken Sie auf **Hinzufügen**.
8. Markieren Sie die Untergruppe, und klicken Sie auf **Weiter**.

Select Sensor Group

- [-] Global
- [-] test

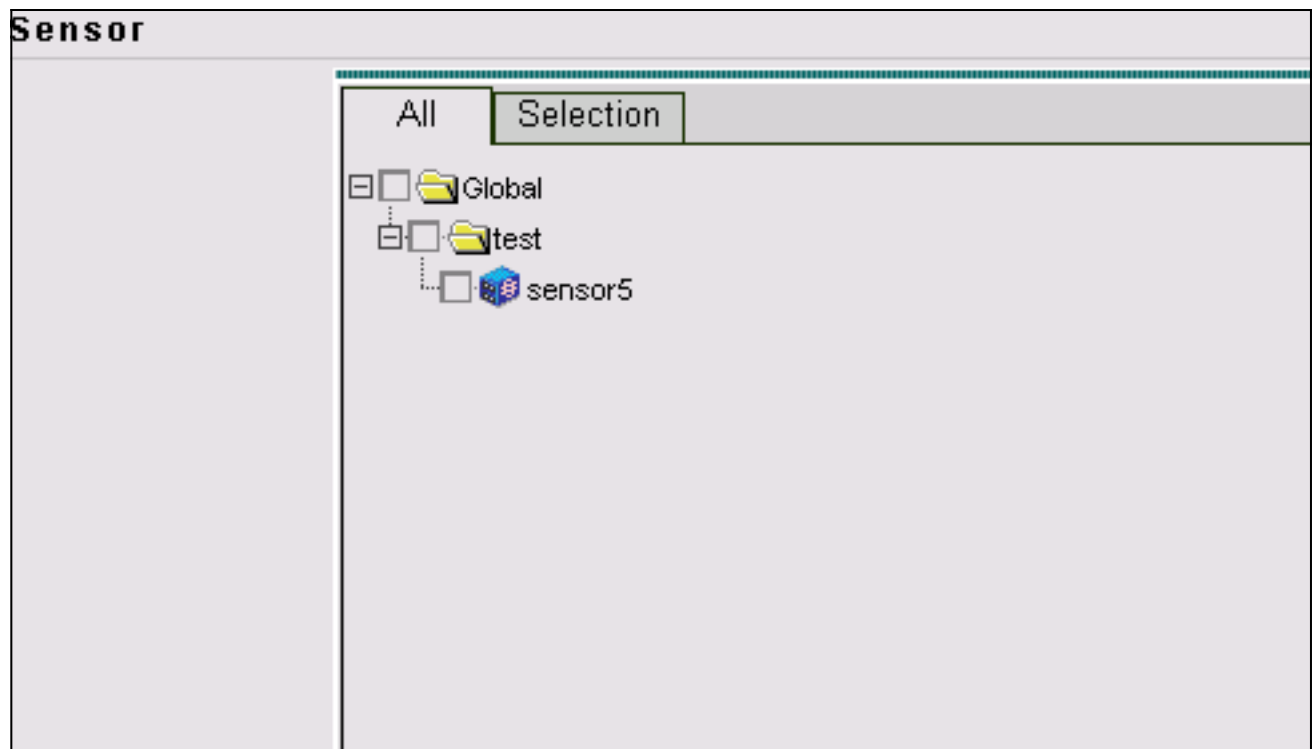
9. Geben Sie die Details gemäß diesem Beispiel ein, und klicken Sie auf **Weiter**, um fortzufahren.

| 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 | |

10. Wenn Ihnen die Meldung `Erfolgreich importierte Sensorkonfiguration` angezeigt wird, klicken Sie auf **Fertig stellen**, um fortzufahren.

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

11. Ihr Sensor wird in den IDS MC importiert. In diesem Fall wird `Sensor5` importiert.



Importieren des Sensors in den Sicherheitsmonitor

Führen Sie diese Schritte aus, um den Sensor in den Sicherheitsmonitor zu importieren.

1. Wählen Sie im Menü VMS Server die Option **VPN/Security Management Solution > Monitoring Center > Security Monitor** aus.
2. Wählen Sie die Registerkarte Geräte aus, klicken Sie dann auf **Importieren**, und geben Sie die IDS MC Server Information ein (siehe dieses

| 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

Beispiel).


3. Wählen Sie Ihren Sensor (in diesem Fall **Sensor 5**) und klicken Sie auf **Weiter**, um fortzufahren.


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. Aktualisieren Sie ggf. die NAT-Adresse für Ihren Sensor, und klicken Sie dann auf **Fertig stellen**, um fortzufahren.

Showing 1 records

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

 -- Editable columns

5. Klicken Sie auf **OK**, um den Sensor vom IDS MC in Security Monitor zu

Import Summary:

```

1 device(s) were imported.

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

```

OK

importieren.

6. Sie können jetzt sehen, dass der Sensor erfolgreich importiert wurde.

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 >>

[IDS MC für Signatur-Updates verwenden](#)

In diesem Verfahren wird die Verwendung von IDS MC für Signatur-Updates erläutert.

1. Laden Sie die [Netzwerk-IDS-Signatur-Updates](#) (nur [registrierte](#) Kunden) herunter, und speichern Sie sie im Verzeichnis C:\PROGRA~1\CSCOpX\MDC\etc\ids\updates\ auf Ihrem VMS-Server.
2. Wählen Sie in der VMS-Serverkonsole **VPN/Security Management Solution > Management Center > IDS Sensors** aus.
3. Wählen Sie die Registerkarte Konfiguration aus, und klicken Sie auf **Updates**.
4. Klicken Sie auf **Netzwerk-IDS-Signaturen aktualisieren**.
5. Wählen Sie im Dropdown-Menü die Signatur aus, die Sie aktualisieren möchten, und klicken Sie auf **Übernehmen**, um fortzufahren.

Update Network IDS Signature Settings

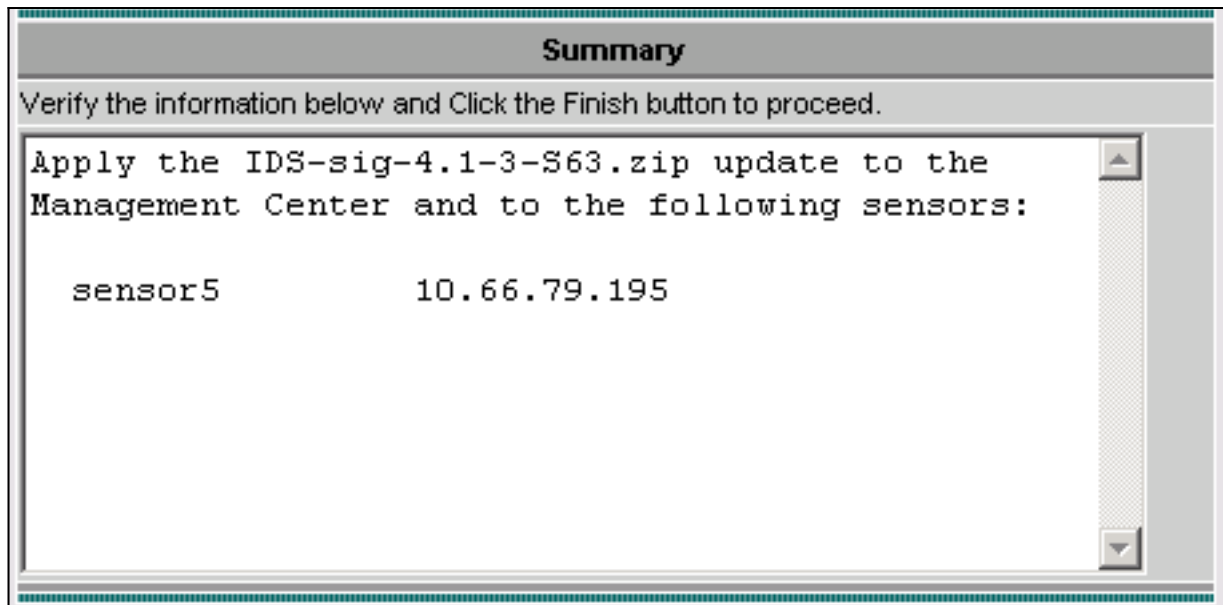
Update File:

6. Wählen Sie die zu aktualisierenden Sensoren aus, und klicken Sie auf **Weiter**, um fortzufahren.

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. Wenn Sie aufgefordert werden, die Aktualisierung auf das Management Center und den Sensor anzuwenden, klicken Sie auf **Fertig stellen**, um fortzufahren.



8. Telnet oder Konsole über die Befehlszeilenschnittstelle Sensor. Sie sehen ähnliche Informationen:

```

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. Warten Sie einige Minuten, bis das Upgrade abgeschlossen ist, und geben Sie dann **show version** ein, um zu überprüfen.

```

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

```

[Konfigurieren des TCP-Resets für den IOS-Router](#)

Führen Sie diese Schritte aus, um das Zurücksetzen von TCP für den IOS-Router zu konfigurieren.

1. Wählen Sie **VPN/Security Management Solution > Management Center > IDS Sensors aus**.
2. Wählen Sie die Registerkarte Konfiguration aus, wählen Sie Ihren Sensor aus dem Objektauswahl-Fenster aus, und klicken Sie dann auf **Einstellungen**.
3. Wählen Sie **Signaturen aus**, klicken Sie auf **Benutzerdefiniert**, und klicken Sie auf **Hinzufügen**, um eine neue Signatur hinzuzufügen.

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 >>

- Geben Sie den neuen Signaturnamen ein, und wählen Sie dann die Engine (in diesem Fall **STRING.TCP**) aus.
- Aktivieren Sie das entsprechende Optionsfeld, um die verfügbaren Parameter anzupassen, und klicken Sie dann auf **Bearbeiten**. In diesem Beispiel wird der ServicePorts-Parameter bearbeitet, um seinen Wert auf **23** zu ändern (für Port 23). Der RegexString-Parameter wird ebenfalls bearbeitet, um den Wert **testattack** hinzuzufügen. Wenn der Vorgang abgeschlossen ist, klicken Sie auf **OK**, um fortzufahren.

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 |

- Klicken Sie auf den Namen der Signatur, um den Schweregrad und die Aktionen der Signatur zu bearbeiten oder die Signatur zu aktivieren/deaktivieren.

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. In diesem Fall wird der Schweregrad auf **Hoch** geändert, und die Aktion **Log & Reset** wird ausgewählt. Klicken Sie auf **OK**, um

Edit Signature(s)

Signature:

Enable

Severity: High

Actions: Log Reset Block Host Block Connection

OK Cancel

fortzufahren.

8. Die vollständige Signatur sieht ähnlich aus wie folgt:

Signature Group: Custom Filter Source: ID 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 | Log,Reset |

Rows per page: 10 << Page 1 >>

Add Edit Delete

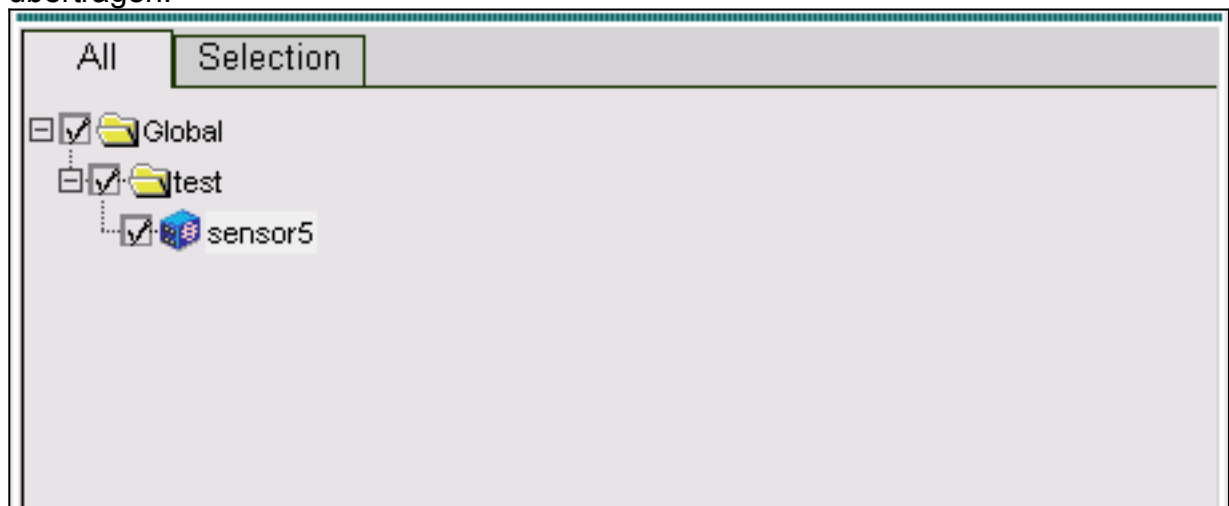
9. Wählen Sie **Konfiguration > Ausstehend**, überprüfen Sie die aktuelle Konfiguration auf Richtigkeit, und klicken Sie auf **Speichern**.

| 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 >>

[Save](#) [Delete](#)

10. Wählen Sie **Deployment > Generate (Bereitstellung > Generieren)**, und klicken Sie dann auf **Apply (Übernehmen)**, um die Konfigurationsänderungen an den Sensor zu übertragen.



11. Wählen Sie **Bereitstellung > Bereitstellen** aus, und klicken Sie auf **Senden**.
 12. Aktivieren Sie das Kontrollkästchen neben Ihrem Sensor, und klicken Sie auf **Bereitstellen**.
 13. Aktivieren Sie das Kontrollkästchen für den Job in der Warteschlange, und klicken Sie auf **Weiter**, um fortzufahren.

| 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. Geben Sie den Auftragsnamen ein, und planen Sie den Job als **Sofort**, und klicken Sie dann auf **Fertig stellen**.

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. Wählen Sie **Bereitstellung > Bereitstellen > Ausstehend aus**.Warten Sie einige Minuten, bis alle ausstehenden Aufträge abgeschlossen sind. Die Warteschlange sollte dann leer sein.
16. Wählen Sie **Konfiguration > History**, um die Bereitstellung zu bestätigen.Stellen Sie sicher, dass der Konfigurationsstatus als **Deployed** angezeigt wird. Dies bedeutet, dass die Sensorkonfiguration erfolgreich aktualisiert wurde.

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 >>

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Attack und TCP Reset starten

Starten Sie einen Testangriff, und überprüfen Sie die Ergebnisse, um sicherzustellen, dass der Blockierungsvorgang ordnungsgemäß funktioniert.

1. Bevor der Angriff gestartet wird, wählen Sie **VPN/Security Management Solution >**

Monitoring Center > Security Monitor.

- Wählen Sie **Monitor** im Hauptmenü aus, und klicken Sie auf **Events (Ereignisse)**.
- Klicken Sie auf **Ereignisanzeige** starten.

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

- Telnet von einem Router zum anderen und geben Sie **testattack** ein, um den Angriff zu starten. In diesem Fall haben wir von der Router-LED zum Router-Haus Telnetted. Sobald Sie **<space>** oder **<enter>** drücken, **solte** nach Eingabe von **testattack** Ihre Telnet-Sitzung zurückgesetzt werden.

```
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]
```

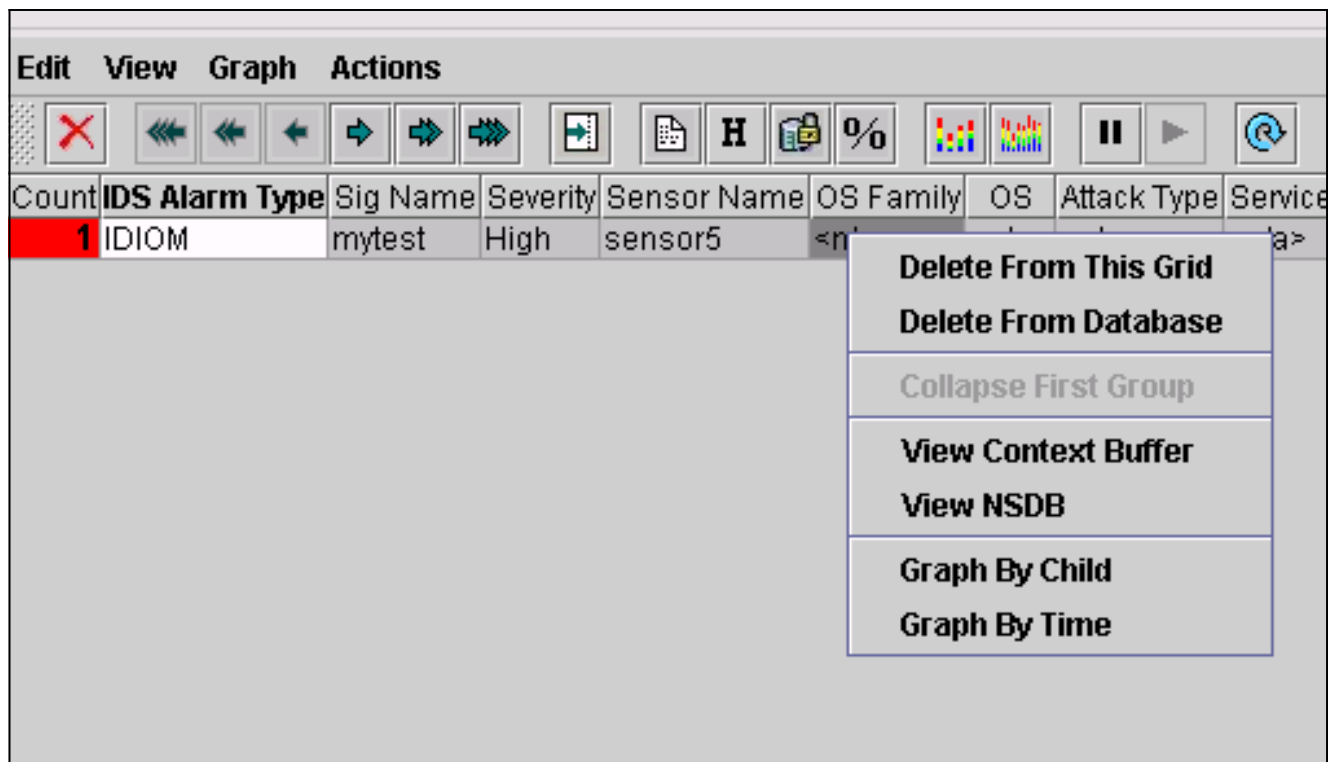
- Klicken Sie in der Ereignisanzeige auf **Datenbank abfragen**, um neue Ereignisse anzuzeigen. Sie sehen die Warnmeldung für den zuvor gestarteten Angriff.

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> |

- Markieren Sie in der Ereignisanzeige den Alarm, klicken Sie mit der rechten Maustaste darauf, und wählen Sie entweder **View Context Buffer** (Kontextpuffer anzeigen) oder **View NSDB** (NSDB anzeigen) aus, um detailliertere Informationen zum Alarm anzuzeigen.



[Fehlerbehebung](#)

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

[Fehlerbehebungsverfahren](#)

Führen Sie diese Schritte aus, um eine Fehlerbehebung durchzuführen.

1. Wählen Sie im IDS-MC **Berichte > Generieren aus**. Je nach Problemtyp finden Sie weitere Details in einem der sieben verfügbaren Berichte.

| 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. Während die Sperre den Command-and-Control-Port verwendet, um die Zugriffslisten des Routers zu konfigurieren, werden TCP-Resets von der Sniffing-Schnittstelle des Sensors gesendet. Stellen Sie sicher, dass Sie den richtigen Port mithilfe des Befehls **set span** auf dem Switch, ähnlich dem folgenden, über Spanning verlegt haben:

```
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. Wenn TCP Reset nicht funktioniert, melden Sie sich beim Sensor an, und geben Sie den Befehl **show event** ein. Starten Sie den Angriff, und prüfen Sie, ob der Alarm ausgelöst wird. Wenn der Alarm ausgelöst wird, überprüfen Sie, ob er für den Aktionstyp **TCP reset** eingestellt ist.

Zugehörige Informationen

- [Support-Seite für Cisco Secure Intrusion Detection](#)
- [Dokumentation für das Cisco Secure Intrusion Detection System](#)

- [Support-Seite für die CiscoWorks VPN/Security Management-Lösung](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)