# IME مادختساب IPS TCP نييعت ةداعإ نيوكت

### المحتويات

المقدمة المتطلبات الأساسية المتطلبات المكونات المستخدمة <u>الاصطلاحات</u> التكوين <u>الرسم التخطيطي للشبكة</u> التكوينات بدء تكوين المستشعر إضافة المستشعر إلى IME تكوين إعادة تعيين TCP لموجه Cisco IOS التحقق من الصحة تشغيل الهجوم وإعادة تعيين TCP استكشاف الأخطاء وإصلاحها <u>نصائح</u> معلومات ذات صلة

### <u>المقدمة</u>

يناقش هذا المستند تكوين إعادة تعيين TCP لنظام منع التسلل (IPS) باستخدام INE) IPS Manager Express). يتم إستخدام أجهزة إستشعار IME و IPS لإدارة موجه Cisco لإعادة تعيين TCP. عند مراجعة هذا التكوين، تذكر العناصر التالية:

- قم بتثبيت "أداة الاستشعار" وتأكد من عمل أداة الاستشعار بشكل صحيح.
- جعلت ال ينشق قارن فسحة بين دعامتين إلى المسحاج تخديد خارج القارن.

### <u>المتطلبات الأساسية</u>

#### <u>المتطلبات</u>

لا توجد متطلبات خاصة لهذا المستند.

#### <u>المكونات المستخدمة</u>

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco IPS Manager Express 7.0
  - مستشعر Cisco IPS 7.0(0.88)E3

• cisco ios مسحاج تخديد مع cisco ios برمجية إطلاق 12.4

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

#### <u>الاصطلاحات</u>

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى <u>اصطلاحات تلميحات Cisco التقنية</u>.

## <u>التكوين</u>

### <u>الرسم التخطيطي للشبكة</u>

يستخدم هذا المستند إعداد الشبكة الموضح في هذا الرسم التخطيطي.



### <u>التكوينات</u>

يستخدم هذا المستند التكوينات الموضحة هنا.

- <u>ضوء الموجه</u>
- <u>منزل الموجه</u>

### **C**urrent configuration : 906 bytes ! version 12.4 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 10.100.100.2 255.255.255.0
                           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 10.100.100.1
                        ip http server
                   ip pim bidir-enable
                                      1
                                      !
                  dial-peer cor custom
                                      !
                                      !
                            line con 0
                           line 97 108
                            line aux 0
                           line vty 0 4
                                 login
                                      !
                                    end
```

#### منزل الموجه

```
Current configuration : 939 bytes
                                            Т
                                version 12.4
            service timestamps debug uptime
              service timestamps log uptime
             no service password-encryption
                                           !
                              hostname house
                                           !
                    logging queue-limit 100
                       enable password cisco
                                           !
                              ip subnet-zero
                                           !
                                           !
                                   no ip cef
                        no ip domain lookup
                                           !
                         ip audit notify log
                 ip audit po max-events 100
                                           !
                                           !
                no voice hpi capture buffer
           no voice hpi capture destination
                                            !
                                           !
                                           1
                                            !
                  interface FastEthernet0/0
   ip address 10.66.79.210 255.255.255.224
                                duplex auto
                                 speed auto
                                           !
                  interface FastEthernet0/1
     ip address 10.100.100.1 255.255.255.0
                                duplex auto
                                 speed auto
                                           1
                            interface ATM1/0
                              no ip address
                                   shutdown
                     no atm ilmi-keepalive
                                           !
                                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 10.100.100.2
                           no ip http server
                   no ip http secure-server
                                           !
                                            !
                                           !
                                           !
                              call rsvp-sync
                                           !
                                           !
                       mgcp profile default
                                            !
                                            !
                                  line con 0
                           exec-timeout 0 0
                                  line aux 0
```

```
line vty 0 4
exec-timeout 0 0
password cisco
login
line vty 5 15
login
!
end
```

### بدء تكوين المستشعر

أكمل هذه الخطوات لبدء تكوين المستشعر.

- 1. إذا كانت هذه هي المرة الأولى التي تقوم فيها بتسجيل الدخول إلى المستشعر، فيجب عليك إدخال **Cisco** كاسم المستخدم وCisco ككلمة مرور.
- 2. عند مطالبة النظام لك، قم بتغيير كلمة المرور الخاصة بك.**ملاحظة:** Cisco123 هي كلمة قاموس ولا يسمح بها في النظام.
  - 3. اكتب setup وأكمل مطالبة النظام لإعداد المعلمات الأساسية لأجهزة الاستشعار.

```
4. أدخل هذه المعلومات:
sensor5#setup
```

--- System Configuration Dialog ---

At any point you may enter a question mark '?' for help. !--- Use **ctrl-c** to abort the ---! .'[]' 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 Corp-IPS telnetOption enabled Permit the IP address of workstation or network with IME 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. قم بحفظ التكوين.قد يستغرق الأمر بضع دقائق حتى يتمكن المستشعر من حفظ التكوين.

- .Go to the command prompt without saving this config [0]
  - .Return back to the setup without saving this config [1]
    - .Save this configuration and exit setup [2]
      - Enter your selection[2]: 2



أتمت هذا steps in order to أضفت المستشعر داخل IME:

- 1. انتقل إلى Windows PC الذي قام بتثبيت IPS Manager Express، وافتح IPS Manager.
  - 2. أختر **الصفحة الرئيسية > إضافة**

| es d        | Home > Devices > De                   | evice List                 | 110        |
|-------------|---------------------------------------|----------------------------|------------|
| Device List | Add Z Edit Del                        | lete 🛛 🕨 Start 👻 📓 Stop 👻  | 🗞 Status   |
|             | Time Device Name                      | IP Address Device Ty       | rpe   Even |
|             | 😨 Edit Device                         |                            | ×          |
|             |                                       |                            |            |
|             | Sensor Name:                          | Corp-IPS                   |            |
|             | Sensor IP Address:                    | 10.66.79.195               |            |
|             | User Name:                            | cisco                      |            |
|             | Password:                             | •••••                      |            |
|             | Web Server Port:                      | 443                        |            |
|             | Communication protoco                 | ol                         |            |
|             | <ul> <li>Use encrypted con</li> </ul> | nnection (https)           |            |
|             | Use non-encrypted                     | d connection (http)        |            |
|             | Event Start Time (UTC)                | )                          |            |
|             | Most Recent Alerts                    | s                          |            |
|             | Start Date (YYYY:M                    | 4M:DD): : : : :            |            |
|             | Start Time (HH:MM                     | 1:55):                     | ]          |
|             | Exclude alerts of the fo              | ollowing severity level(s) |            |
|             |                                       |                            |            |

- 3. اكتب في هذه المعلومات وانقر فوق **موافق** لإنهاء التكوين. 4. أخترت **أداة>Corp-IPS** in order to دققت المستشعر وضع وبعد ذلك déclic in order to أخترت **أداة وضع**.تأكد من إمكانية مشاهدة

| onnection Status: Subscription successfully opened.   |   |
|---|---|
| ensor Version:  |   |
| Cisco Intrusion Prevention System, Version 7.0(0.88)E3<br>Host:<br>Realm Keys key1.0<br>Signature Definition:<br>Signature Update S310.0 2007-12-05<br>Virus Update VI.2 2005-11-24   | ~   |
| omponent Statistics Information: (Press CTRL+F to start searching.)   |   |
| <ul> <li>Provide Statistics - Analysis Englise Statistics</li> <li>Receiver Statistic - Total Packets Total number of IP packets processed since reset = 0</li> <li>IpPackets - Total number of IP packets processed since reset = 0</li> <li>TransmitterStats - Transmitter Statistics</li> <li>TransmitterStats - Total number of packets denied = 0</li> <li>ResetPackets - Total number of packets denied = 0</li> <li>ResetPackets - Total number of packets reset = 0</li> <li>FRU - Fragment Reassembly Unit Statistics</li> <li>currentFragmentsHeld - Number of fragments currently in FRU = 0</li> <li>currentPartialDatagrams - Number of datagrams currently in FRU = 0</li> <li>StreamReasemblyUnit - TCP Stream Reassembly Unit Statistics</li> <li>embryoricStreams - TCP streams currently in the established state = 0</li> <li>dosingStreams - TCP streams currently in the established state = 0</li> <li>currentStreams - TCP streams currently in the system = 0</li> <li>CurrentQueuePackets - TCP Packets currently queue for reassembly =</li> <li>SignatureDEStats - TCP is for Streams currently in the system = 0</li> <li>CUPAABb - TCP nodes keyed on both IP addresses and both ports = 0</li> <li>UDPAABb - UDP nodes keyed on both IP addresses and both ports = 0</li> <li>SigEvents - Statistics for Signature Events</li> <li>TotalEvents - Number of SigEvents since reset = 0</li> <li>ActionsExecuted - Statistics for Actions executed on a SigEvent produceAert - Number of Alerts written to the IdsEventStore = 0</li> <li>Inspection Stats - Charles written to the IdsEventStore = 0</li> </ul> | Press CTRL+F to start searching. Press up/down<br>next or previous matching word. |

## <u>تكوين إعادة تعيين TCP لموجه Cisco IOS</u>

أكمل هذه الخطوات لتكوين إعادة تعيين TCP لموجه Cisco IOS:

- 1. من جهاز IME، افتح مستعرض الويب وانتقل إلى https://10.66.79.195.
  - 2. انقر على **موافق** لقبول شهادة HTTPS التي تم تنزيلها من المستشعر.
- 3. في نافذة تسجيل الدخول، أدخل **Cisco** لاسم المستخدم و**123cisco123** لكلمة المرور.تظهر واجهة إدارة IME هذه:

| Home 🤔 Configuration 🏧 E           | venti | Monitoring  | Reports 🦻 He             | lp  | _             | _        |          |          |
|------------------------------------|-------|-------------|--------------------------|---|---------------|----------|----------|----------|
| Configuration > Corp-IPS > Policie | 5 > 5 | Signatur    | e Definitions > sig0 > A | Active Sign   | atures        |          |          |          |
| Corp-IPS                           |       |             |                          |   |               |          |          |          |
| 💓 IPS Policies                     | 1     | C Edit A    | ctions 🥥 Enable 🧭 Dis    | able 🔿 Re   | store Default | 1 show   | Events + | N M      |
| Signature Definitions              |       |             |                          |   |               |          |          | . 9.7    |
| - Sigu                             |       | Filter: Sig | ID 💌                     |   |               |          |          |          |
|                                    |       | a 1.        |                          |   | Sec. 17       | Fidelity | Base     | Signatu  |
| 🔓 Attack                           |       | ID 1        | Name                     | Enabled   | Severity      | Rating   | RR       | Alert an |
| DDo5                               |       | 1000/0      | IP options-Bad Option    |   | 1 Infor       | 75       | 18       | E. Alert |
| Dos                                |       | 1004/0      | IP options-Loose Sour    |   | High          | 100      | 100      | Alert    |
| Email                              |       | 1006/0      | IP options-Strict Sourc  | Image: A start of the start          | High          | 100      | 100      | Alert    |
| S Instant Messaging                |       | 1007/0      | IPv6 over IPv4           |   | L Infor       | 100      | 25       | Alert    |
| S L2/L3/L4 Protocol                |       | 1101/0      | Unknown IP Protocol      | ¥   | 👗 Infor       | 75       | 18       | Alert    |
|                                    |       | 1102/0      | Impossible IP Packet     |   | High          | 100      | 100      | Alert    |
| 🛜 OS                               |       | 1104/0      | IP Localhost Source S    | <ul> <li>Image: A start of the start of</li></ul> | High          | 100      | 100      | Alert    |
| Other Services                     |       | 1107/0      | RFC 1918 Addresses       |   | 1 Infor       | 100      | 25       | Alert    |
| P2P                                |       | 1108/0      | IP Packet with Proto 11  | ~   | High          | 100      | 100      | Alert    |
| Reconnaissance                     |       | 1109/0      | Cisco IOS Interface DoS  |   | Medium        | 75       | 56       | Alert    |
| Releases                           |       | 1109/1      | Cisco IOS Interface DoS  |   | 🤗 Medium      | 75       | 56       | Alert    |
| Web Server                         |       | 1109/2      | Cisco IO5 Interface Do5  |   | Medium        | 75       | 56       | Alert    |
| All Signatures                     |       | 1109/3      | Cisco IOS Interface DoS  |   | 😑 Medium      | 75       | 56       | Alert    |
| E Perent Action Rules              |       | 1200/0      | IP Fragmentation Buff    | ~   | L Infor       | 100      | 25       | Alert    |
| - 💭 rules0                         |       | 1201/0      | IP Fragment Overlap      |   | i Infor       | 100      | 25       | Alert    |
| 🖻 🔂 Anomaly Detections             |       | 1202/0      | IP Fragment Overrun      | Image: A start of the start          | High          | 100      | 100      | Alert    |
| ol - 10                            |       | 1000 la     | ID F                     | 57  |               | 100      | 100      | (T       |

- 4. من علامة التبويب تكوين، انقر فوق **التوقيعات النشطة**.
  - 5. ثم انقر فوق **معالج** الت**ەقىع**

| Corp-IP5              |             |                                |  |                | 🔇 Refrest                |
|-----------------------|-------------|--------------------------------|--|----------------|--------------------------|
| Signature Definitions | Filter: Sig | tions 🕥 Enable 💋 Dis<br>ID 🛛 🖌 | ab   | lelp<br>Filter | ter 🛛 🔍 Signature Wizard |
|                       | ID *1       | Name                           | E  | f.             |                          |
| - 🔀 DDoS              | 1000/0 1    | P options-Bad Option           | and the second s |                | ^                        |
| 🕅 DoS                 | ann ain in  |                                |  |                |                          |

6. في المعالج، أختر **نعم** واختر **سلسلة TCP** كمحرك التوقيع. انقر فوق **Next** (**التالي)**.



7. يمكنك ترك هذه المعلومات كعنوان أو إدخال معرف التوقيع واسم التوقيع وملاحظات المستخدم الخاصة بك. انقر فوق Next

| The state of the | Signature Identification   |  |
|------------------|--|--|
|                  | Signature identification parameters identify and describe th<br>signature behavior. You must specify a Signature ID and So<br>default values, but each required value must be unique (no | e signature, but do not affect the<br>ubSignature ID. You can override the<br>it used by another signature). |
|                  | Signature ID: 60000  |  |
| Date Bar         | SubSignature ID: 0   |  |
| - Contract       | Signature Name: String.tcp   |  |
| HHHH             | Alert Notes: My Sig Info   |  |
|                  | User Comments: Sig Comment   |  |

8. أختر **إجراء الحدث**، واختر **إنتاج تنبيه** و**إعادة ضبط اتصال TCP**. طقطقت ok وبعد ذلك **بعد ذلك عار ال** 

| and the second se | Engine Specific Parameters   | *  |             |
|---|--|--|-------------|
|   | Engine-specific parameters deta<br>to fire. You can set the followin   | rmine what the signature looks for and what causes the signatu<br>g String TCP engine parameters used for this signature.  | <i>i</i> re |
|   | Name   | Value  |             |
|   | Event Action   | Select item(s)   | X           |
| Email FTP VolP Web  | Strip Telnet Options<br>Specify Min Match Length<br>Regex String<br>Service Ports<br>Direction<br>Specify Exact Match Offset<br>Specify Max Match Offset<br>Specify Min Match Offset<br>Swap Attacker Victim | <ul> <li>Deny Attacker Inline</li> <li>Deny Attacker Service Pair Inline</li> <li>Deny Attacker Victim Pair Inline</li> <li>Deny Connection Inline</li> <li>Deny Packet Inline</li> <li>Log Attacker Packets</li> <li>Log Pair Packets</li> <li>Log Victim Packets</li> <li>Log Victim Packets</li> <li>V Produce Alert</li> <li>Produce Verbose Alert</li> <li>Request Block Connection</li> <li>Request Block Host</li> <li>Reset TCP Connection</li> <li>OK Cancel</li> </ul> | ne          |
|   | Parameter uses the Def<br>Parameter uses a User-   | ault Value. Click the value field to edit the value.<br>Defined Value. Click the icon to restore the default value.  |             |

9. أدخل تعبيرا منتظما، ويتم إستخدام <sub>testattack</sub> في هذا المثال. دخلت **23** ل خدمة ميناء، أخترت **أن يعمل** ل الإتجاه، وطقطقة **بعد ذلك** in order to .

باشرت.

تابعت.

|  | Engine Specific Parameters  | Engine Specific Parameters Engine-specific parameters determine what the signature looks for and what causes the signature to fire. You can set the following String TCP engine parameters used for this signature. |  |  |  |
|--|---|---|--|--|--|
|  | Engine-specific parameters determine what<br>to fire. You can set the following String TC |   |  |  |  |
|  | Name  | Value   |  |  |  |
|  |   | Produce Alert   Reset TCP Connection  |  |  |  |
| HHH  | Strip Telnet Options  | No  |  |  |  |
|  | Specify Min Match Length  | No  |  |  |  |
| Ho Paca  | Regex String  | testattack  |  |  |  |
|  | -Service Ports  | 23  |  |  |  |
| 171171   | Direction   | To Service  |  |  |  |
| tititit  | Specify Exact Match Offset  | No  |  |  |  |
|  | Specify Max Match Offset  | No  |  |  |  |
| and the second s | Specify Min Match Offset  | No  |  |  |  |
|  |   | No  |  |  |  |

#### 10. يمكنك ترك هذه المعلومات كافتراضي. انقر فوق Next (التالي).

| A DE SIDORI   | Alert Response  |
|---|---|
| Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa<br>Handa | You can assign the following values to this signature that reflect both your confidence in the fidelity of the signature and the severity of the attack it represents. The Signature Fidelity Rating is any number from 0 to 100, with 100 reflecting the most confidence in this signature. This number is used to help calculate the Risk Rating, which helps determine what actions result from the firing of this signature.          Signature Fidelity Rating:       75         Severity of the Alert:       High |

11. طقطقة **إنجاز** in order to أنهيت بيرين

المعالج.

| 😨 Custom Signature Wizar   | d 🛛 🔀   |
|--|---|
| N OB SOUTH   | Alert Behavior  |
|  | The sensor sends the first alert for each address set, and then a summary of all the alerts that occur on this address set over the next 15 seconds.<br>The summary alert contains the same information as the original alert and provides an interval summary that shows the number of total alerts per time interval. A summary counts signature firings on attacker address. |
| Entropy of the second s | The sensor will not automatically upgrade (or downgrade) to global summarization mode.  |
| Email FTP VolP Web<br>Pages  | To accept this alert behavior and create the custom signature, Advanced   |
|  | <back next=""> Finish Cancel Help</back>  |

12. أخترت **تشكيل > sig id>توقيع نشط** in order to حددت ال newly created توقيع ب **sig id** أو sig name. طقطقة **يحرر** in order to شاهدت التوقيع.

| Name  | Value  |
|---|--|
| Signature Definition  |  |
| Signature ID  | 60000  |
| SubSignature ID   | 0  |
| 😿 Alert Severity  | Medium   |
| 😿 Sig Fidelity Rating   | 75   |
| 🖬 Promiscuous Delta   | 0  |
|   |  |
| Signature Name  | string.tcp   |
| 🗹 Alert Notes   | My Sig Info  |
| Ser Comments  | Sig Comment  |
| 🗔 Alert Traits  | 0  |
| Release   | custom   |
| Engine  | String TCP   |
| 😿 Event Action  | Produce Alert   Reset TCP Connection                   |
| Strip Telnet Options  | No   |
| Specify Min Match Length  | No   |
| Regex String  | testattack   |
| Service Ports   | 23   |
| 😿 Direction   | To Service   |
| Specify Exact Match Offset  | No   |
| Specify Max Match Offset  | No   |
| Specify Min Match Offset  | No   |
| Swap Attacker Victim  | No   |
| A Current Courselow   |  |
| Parameter uses the Default Value. Click the value fiel<br>Parameter uses a User-Defined Value. Click the icon N | ld to edit the value.<br>to restore the default value. |
| OK (  | Cancel Help  |

13. طقطقة ok بعد أن يؤكد أنت ويطقطق **ال apply** زر in order to طبقت التوقيع إلى المستشعر.

### <u>التحقق من الصحة</u>

### <u>تشغيل الهجوم وإعادة تعيين TCP</u>

أكمل الخطوات التالية لتشغيل الهجوم وإعادة تعيين TCP:

- 1. قبل بدء الهجوم، انتقل إلى **IME**، واختر **مراقبة الحدث > عرض الهجمات التي تم إسقاطها** واختر المستشعر من الجانب الأيمن.
  - 2. من ضوء الموجه، ومن Telnet إلى منزل الموجه وأدخل **هجوم التجربة**.اضغط إما <space> أو <enter> لإعادة ضبط جلسة عمل برنامج Telnet. light#telnet 10.100.100.1

Trying 10.100.100.1 ... Open

User Access Verification :Password

```
house>en
:Password
house#testattack
[Connection to 10.100.100.1 closed by foreign host]
.Telnet session has been reset due to the !--- signature "String.tcp" triggered ---!
```

3. من لوحة المعلومات الخاصة بعارض أحداث IPS، يظهر "الإنذار الأحمر" بمجرد بدء تشغيل

|                  |             |                     | وم.     |
|------------------|-------------|---------------------|---------|
| Date             | Time        | 📗 Sig. Name         | Sig. ID |
| Device: Corp-IPS | (188 items) |                     |         |
| 🚊 Severity: high | (188 items) |                     |         |
| 10/23/2009       | 09:59:13    | String.tcp          | 60000/0 |
| -10/23/2009      | 09:59:02    | ZOTOB Worm Activity | 5570/0  |
|                  | 09:58:57    | Anig Worm File Tran | 5599/0  |
|                  | 09:59:00    | Anig Worm File Tran | 5599/0  |
|                  | 09:58:58    | Anig Worm File Tran | 5599/0  |
|                  | 09:59:17    | Nachi Worm ICMP E   | 2158/0  |

## <u>استكشاف الأخطاء وإصلاحها</u>

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

#### <u>نصائح</u>

أستخدم تلميحات أستكشاف المشكلات وإصلاحها التالية:

• يجنب الأعمال خارج منفذ الأمر والتحكم لإعادة برمجة قوائم التحكم في الوصول إلى الموجه (ACLs). يتم إرسال عمليات إعادة ضبط TCP من **واجهة** sniffing الخاصة بالمستشعر. عندما **يثبت أنت فسحة بين دعامتين** في المفتاح، استعملت **المجموعة فسحة بين دعامتين <src\_mod/src\_port><dest\_mod/dest\_port>** أمر مع كلا ربط قادم يمكن كما هو موضح هنا. 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 connect to FastEthernet0/0 of Router House ---! Oper Source : Port 2/12 : transmit/receive Direction Incoming Packets: enabled Multicast : enabled • إذا كانت عمليات إعادة ضبط TCP تعمل، فتحقق مما إذا كان تم تشغيل التنبيه لنوع الإجراء إعادة تعيين TCP. إذا ظهر التنبيه، فتحقق من تعيين نوع التوقيع على إعادة تعيين TCP.قم بتسجيل الدخول باستخدام حساب الخدمة كجذر وإصدار هذا الأمر. يفترض هذا الأمر تعيين واجهة الاستشعار على th0. root@sensor1 root]#tcpdump -i eth0 -n] **ملاحظة:** يتم إرسال 100 إعادة توجيه TCP إلى الضحية/الهدف ثم يتم إرسال 100 منها إلى المهاجم/العميل.هذا مثال للمخرجات: < 64.104.209.205.1409 03:06:00.598777 telnet: R 107:107(0) ack 72 win 0.10.66.79.38

< 64.104.209.205.1409 03:06:00.598794 telnet: R 108:108(0) ack 72 win 0.10.66.79.38

< telnet.10.66.79.38 03:06:00.599360 R 72:72(0) ack 46 win 0 :64.104.209.205.1409 < telnet.10.66.79.38 03:06:00.599377 R 73:73(0) ack 46 win 0 :64.104.209.205.1409

## <u>معلومات ذات صلة</u>

- <u>صفحة دعم منع التسلل الآمن من Cisco</u> <u>وثائق نظام Cisco لمنع الاقتحام الآمن</u> <u>الدعم التقني والمستندات Cisco Systems</u>

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما