IME مادختساب IPS رظح نيوكت

المحتويات

المقدمة <u>المتطلبات الأساسية</u> المتطلبات المكونات المستخدمة <u>الاصطلاحات</u> التكوين <u>الرسم التخطيطي للشب</u>كة التكوينات بدء تكوين المستشعر إضافة المستشعر إلى IME تكوين الحظر لموجه Cisco IOS التحقق من الصحة <u>شن الهجوم والعرقلة</u> استكشاف الأخطاء وإصلاحها <u>نصائح</u> معلومات ذات صلة

<u>المقدمة</u>

يناقش هذا المستند تكوين حظر نظام منع التسلل (IPS) باستخدام IPS Manager Express (IME). يتم إستخدام أجهزة الاستشعار IME و IPS لإدارة موجه Cisco لحظر البيانات. تذكر هذه العناصر عند مراعاة هذا التكوين:

- 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
- سحاج تخديد مع cisco ios برمجية إطلاق 12.4 $^{ ext{ extbf{8}}}$

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>

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

<u>التكوين</u>

<u>الرسم التخطيطي للشبكة</u>

يستخدم هذا المستند إعداد الشبكة التالي.



<u>التكوينات</u>

يستخدم هذا المستند هذه التكوينات.

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

ضوء الموجه

```
Current 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
                                      !
                                      !
                  dial-peer cor custom
                                      1
                                      !
                            line con 0
                            line 97 108
                             line aux 0
                           line vty 0 4
                                 login
                                      !
                                    end
                            منزل الموجه
```

```
Current configuration : 939 bytes
                                                         I
                                             version 12.4
                         service timestamps debug uptime
                           service timestamps log uptime
                          no service password-encryption
                                                         !
                                           hostname house
                                                         1
                                  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
                                                         !
                                                         !
                                                         !
                                                         !
                                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
            ip access-group IDS_FastEthernet0/1_in_0 in
      After you configure blocking, !--- IDS Sensor ---!
   inserts this line. duplex auto speed auto ! 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
                                                         !
                                                         1
        ip access-list extended IDS_FastEthernet0/1_in_0
                        permit ip host 10.66.79.195 any
                                      permit ip any any
      After you configure blocking, !--- IDS Sensor ---!
    inserts this line. ! 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
                                                         1
                                                         !
                                                       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 واتبع 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 time: Thu Oct 22 21:19:51 2009
                                                         :Setup Configuration last modified
                                                                   :[Enter host name[sensor
                                          :[Enter IP interface[10.66.79.195/24,10.66.79.193
                                                           :[Modify current access list?[no
                                                               :Current access list entries
       permit the ip address of workstation or network with IME Permit: 10.66.79.0/24 ---!
                                                                                     :Permit
                                                         :[Modify system clock settings?[no
                                                        :[Modify summer time settings?[no
                                                     :[Use USA SummerTime Defaults?[yes
                                                :[Recurring, Date or Disable?[Recurring
                                                                    :[Start Month[march
                                                                    :[Start Week[second
                                                                     :[Start Day[sunday
                                                                  :[Start Time[02:00:00
                                                                   :[End Month[november
                                                                       :[End Week[first
                                                                       :[End Day[sunday]
                                                                    :[End Time[02:00:00
                                                                            :[]DST Zone
                                                                            :[Offset[60
                                                             :[Modify system timezone?[no
                                                                         :[Timezone[UTC
                                                                         :[UTC Offset[0
                                                                        Use NTP?[no]: yes
                                                               :[]NTP Server IP Address
                                                       Use NTP Authentication?[no]: yes
                                                                      NTP Key ID[]: 1
                                                             NTP Key Value[]: 8675309
                                  5. قم بحفظ التكوين.قد يستغرق المستشعر بضع دقائق لحفظ 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

<u>إضافة المستشعر إلى IME</u>

أكمل هذه الخطوات لإضافة المستشعر إلى IME.

IPS Manager Express الذي قام بتثبيت IPS Manager Express وافتح IPS Manager Express Express.

2. أختر **الصفحة الرئيسية > إضافة**.

لإنهاء	موافق	فوق	وانقر	المعلومات	هذه	في	اکتب	.3
							. < .11	

📇 Device List		Add 🗣	🗗 Edit 📋 Dele	te 👂 Start 👻	📕 Stop 👻 🍕	👌 Status
		Time	Device Name	IP Address	Device Type	Even
		C Ed	it Device		_	×
		Senso	r Name	Sepsor5	_	
		Sensor IP Address:		10.66.79.195		
		User Name:		cisco		
		Password: Web Server Port:		•••••		
				443		
		Comn	nunication protoco	b *		
		<u>ົ</u> ບ	se encrypted conr	nection (https)		
		00	se non-encrypted	connection (http)		
		Event	Start Time (UTC)			
		M	ost Recent Alerts			
		st	art Date (YYYY:MI	M:DD)::	:	
		St	art Time (HH:MM:	55): 🔄 :		
		Exclu	de alerts of the fo	llowing severity lev	el(s)	
			formational	ow Medium	High	

4. أختر **أجهزة > مستشعر 5** للتحقق من حالة المستشعر ثم انقر بزر الماوس الأيمن لاختيار **الحالة**.تأكد من إمكانية مشاهدة *فتح الاشتراك بنجاح.* الرسالة.

o Device Status - Corp-IPS	<u> </u>
Connection Status: Subscription successfully opened.	
Sensor Version:	
Cisco Intrusion Prevention System, Version 7.0(0.88)E3 Host: Realm Keys key1.0 Signature Definition: Signature Update \$310.0 2007-12-05 Virus Update VI.2 2005-11-24	~
Component Statistics Information: (Press CTRL+F to start searching.)	
AnalysisEngineStatistics Analysis Engine Statistics ReceiverStats Receiver Statistics TotalPackets Total number of packets processed since reset = 0 IpPackets Total number of IP packets processed since reset = 0 TransmitterStats Transmitter Statistics TransmittedPackets Total number of packets transmitted = 0 DeniedPackets Total number of packets denied = 0 ResetPackets Total number of packets denied = 0 ResetPackets Total number of packets denied = 0 ResetPackets Total number of packets reset = 0 FRU FragmentReassembly Unit Statistics currentFragmentsHeld Number of fragments currently in FRU = 0 currentPartialDatagrams Number of datagrams currently in FRU = 0 StreamReassemblyUnit TCP Stream Reassembly Unit Statistics embryonicStreams TCP streams currently in the embryonic state = 0 dosingStreams TCP streams currently in the established state = 0 currentStreams TCP streams currently in the system = 0 CurrentQueuedPackets TCP Packets currently queued for reassembly = SignatureDEStats The Signature Database Statistics. Total Total nodes active = 0 TCPAa8b TCP nodes keyed on both IP addresses and both ports = 0 UDPAa8b UDP nodes keyed on both IP addresses and both ports = 0 SigEvents Statistics for Signature Events TotalEvents Number of SigEvents since reset = 0 ActionsExecuted Statistics for Actions executed on a SigEvent produceAert Number of Alerts written to the IdsEventStore = 0 Inspection Stats Inspection Stats statuse to use a statist of the statusten to the IdsEventStore = 0 Inspection Stats Inspection Stats	Press CTRL+F to start searching. Press up/down ar next or previous matching word.

<u>تكوين الحظر لموجه Cisco IOS</u>

أكمل هذه الخطوات لتكوين الحظر للمسار 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 <u> 🇞</u> Configuration 🌆 E	iven	t Monitoring	a 🚮 Reports 🛛 🧖 He	lp				
Configuration > Corp-IPS > Policie	es >	Signatur	e Definitions > sig0 > A	Active Sign	atures			
Corp-IPS								
- 🧐 IPS Policies		Cal Edit A	Actions @ Enable @ Dis	able 🔿 Br	store Default	1 show	Events •	C.M
Signature Definitions								
- Sigu		Filter: Si	gID 🖌					
Adware/Spyware		a 14			2005 C/	Fidelity	Base	Signatu
🔤 🔓 Attack	ш	10 -1	Name	Enabled	Sevenity	Rating	RR	Alert ar
DDo5		1000/0	IP options-Bad Option	 Image: A start of the start of	L Infor	75	18	Alert
DoS		1004/0	IP options-Loose Sour		High	100	100	Alert
	ш	1006/0	IP options-Strict Sourc	Image: A start a st	High	100	100	Alert
S Instant Messaging	10	1007/0	IPv6 over IPv4		L Infor	100	25	Alert
2 L2/L3/L4 Protocol	3	1101/0	Unknown IP Protocol	¥	👗 Infor	75	18	Alert
		1102/0	Impossible IP Packet	•	High	100	100	Alert
	ш	1104/0	IP Localhost Source S	V	High	100	100	Alert
🔓 Other Services	ш	1107/0	RFC 1918 Addresses		🚹 Infor	100	25	Alert
P2P	ш	1108/0	IP Packet with Proto 11	 Image: A start of the start of	High	100	100	Alert
Balassance		1109/0	Cisco IOS Interface DoS		🦲 Medium	75	56	Alert
S Viruses Worms (Trojan	ш	1109/1	Cisco IOS Interface DoS		🤗 Medium	75	56	Alert
Web Server	ш	1109/2	Cisco IOS Interface DoS		😑 Medium	75	56	Alert
🔤 All Signatures	-11	1109/3	Cisco IOS Interface DoS		😑 Medium	75	56	Alert
Event Action Rules		1200/0	IP Fragmentation Buff	 	👔 Infor	100	25	Alert
💭 rules0		1201/0	IP Fragment Overlap		👗 Infor	100	25	🚮 Alert
Anomaly Detections		1202/0	IP Fragment Overrun	Image: A start and a start	High	100	100	Alert
		4 and 1a	10 C 1 C 1 C 1	E.21	and the f	100	100	1000 11 1

- 4. من علامة التبويب تكوين، انقر فوق **التوقيعات النشطة**.
 - 5. بعد ذلك، انقر فوق **معالَج** التم**ق**بع

Configuration > Corp-IPS > Policies	g0 > Act	تي ي الم	
Attack	Edit Actions Enable Filter: Sig ID	Ø Disab	Q, Signature Wizard
DDoS	1000/0 IP options-Bad Op	ion	

ملاحظة: تم قص لقطة الشاشة السابقة إلى جزئين بسبب ضيق المساحة. 6. أخترت **نعم** و**خيط TCP** كتوقيع محرك. انقر فوق Next



7. يمكنك ترك هذه المعلومات كافتراضي أو إدخال معرف التوقيع واسم التوقيع وملاحظات المستخدم الخاصة بك.

		انقر فوق Next
🔁 Custom Signature Wiza	rd	(التالي). 🔽
	Signature Identification	
	Signature identification parameters identify and describe the sign signature behavior. You must specify a Signature ID and SubSign default values, but each required value must be unique (not user	ature, but do not affect the ature ID. You can override the d by another signature).
	Signature ID: 60000	
ET HALF BAR	SubSignature ID: 0	
au logan	Signature Name: String.tcp	
<i>Hittiti</i>	Alert Notes: My Sig Info	
	User Comments: Sig Comment	

8. أخترت **حدث إجراء** واخترت **إنتاج تنبيه** و **طلب قالب مضيف**. طقطقت **بعد ذلك** in order to

Contraction and the second	Engine Specific Paramete	irs	
	Engine-specific parameters de to fire. You can set the follow	etermine what the signature looks for and what cause: ring String TCP engine parameters used for this signati	s the signature ure.
	Name	Value	
Email FTP VolP Web	 Event Action Strip Telnet Options Specify Min Match Length Regex String Service Ports Direction Specify Exact Match Offs Specify Max Match O Specify Min Match Off Swap Attacker Victim 	Select item(s) Deny Attacker Inline Deny Attacker Service Pair Inline Deny Attacker Victim Pair Inline Deny Connection Inline Deny Packet Inline Log Attacker Packets Log Pair Packets fiset Log Victim Packets Fiset Produce Alert Produce Verbose Alert Request Block Host Request SNMP Trap Reset TCP Connection OK Cancel	Select All Select None

9. دخلت تعبير عادي، أي في هذا مثال *testattack*، **23** ل خدمة ميناء، أخترت **أن خدمة** ل الإتجاه، وطقطقة **بعد ذلك** in order to تابعت.

Constanta, 740	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.				
	Name	Value			
	Event Action	Produce Alert Request Block Host			
	Strip Telnet Options	No			
L DAZ	Specify Min Match Length	No			
	-Regex String	testattack			
- I O I I I I I I I I I I I I I I I I I	Service Ports	23			
ATTER	Direction	To Service			
HHHHH	Specify Exact Match Offset	No			
шш	Specify Max Match Offset	No			
	Specify Min Match Offset				
	Swap Attacker Victim	No			

10. يمكنك ترك هذه المعلومات كافتراضي. انقر فوق Next

CON STORE	Alert Response					
	You can assign the following values to this signature that reflect both your confidence in the identity 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 dimension.					
	signature.					
TAGES	Signature Fidelity Rating: 75					

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

Custom Signature Wizar	d – 🔀
	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. 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.
Email FTP VolP Web Pages	The sensor will not automatically upgrade (or downgrade) to global summarization mode. To accept this alert behavior and create the custom signature, click Finish. To change the alert behavior, click Advanced. 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

Name	Value
⊡-Signature Definition	5 <u></u>
Signature ID	60000
SubSignature ID	0
Alert Severity	Medium
🖌 Sig Fidelity Rating	75
- 🖾 Promiscuous Delta	0
-Sig Description	2 ⁻
Signature Name	String.tcp
Alert Notes	My Sig Info
- 🐨 User Comments	Sig Comment
- Alert Traits	0
Release	custom
-Engine	String TCP
Event Action	Produce Alert Request Block Host
	No
	No
-Regex String	testattack
-Service Ports	23
- Virection	To Service
S-Specify Exact Match Offset	No
Specify Max Match Offset	No
-Specify Min Match Offset	No
	No
- Frank Caratan	1
Parameter uses a User-Defined Value. Cick the OK OK OK In order to انقر فوق حظر. من الجزء الأيسر، أختر خصا	انده العاد الله value. Icon to restore the default value. Cancel Help data to يؤكد أنت ويطقطق ال apply زر المستشعر"، المستشعر"،
SSH	لکین pecify the blocking properties and the ado Enable blocking
Certificates	Log all block events and errors Enable ACL logging
Blocking	
Martin and Martin	Aavimum Block Entries: 250

الحظر 15. انتقل الآن من الجزء الأيسر إلى **ملف تعريف تسجيل دخول الجهاز**. طقطقة in order to خلقت توصيف جديد، **يضيف**. طقطقة ما إن يخلق **ok ويطبق** in order to مستشعر وتابع.

Maximum Rate Limit Entries:

250

Blocking Properties Jevice Login Profiles

Blocking Devices

Certificates	S Add Device Login	i Profile 🛛 👔
 Blocking Blocking Properties Blocking Properties Device Login Profiles 	Profile Name: Username (optional):	Router Test
Router Blocking Devices Router Blocking Device In Solution Cat 6K Blocking Device In Solution Master Blocking Sensor Solution Solution	Confirm New Password (op	word:
Traps Configuration External Product Interfaces Passwords Licensing Sensor Health IP Logging Variables	Enable Password (o New Password: Confirm New Pass	sword:
Auto/Cisco.com Update	ОК	Cancel Help

16. تتمثل الخطوة التالية في تكوين الموجه كجهاز حظر. من الجزء الأيسر، أختر **حظر الجهاز**، انقر فوق **إضافة** لإضافة هذه المعلومات. ثم انقر فوق **موافق** و**تطبيق.**

Kalinusteu musts	19		0
Server Certificate	Q Add Blocking Device		
b Blocking			
Blocking Properties			
Device Login Profiles	IP Address:	10.10.10.10	
Blocking Devices	Sensor's NAT Address (optional):		
Cat 6K Blocking Device Inl	Device Login Profile:	Router	×
Master Blocking Sensor		the second second	
👹 SNMP	Device Type:	Cisco Router	×
General Configuration	Response Capabilities: 🔽 Bloc	:k 🔲 Rate Limit	
External Product Interfaces	Communication:	Telnet	v
III Passwords		1	
Licensing			
🖁 Sensor Health	OK Cancel	Help	
🕹 IP Logging Variables			8. I

17. الآن من الجزء الأيسر قم بتكوين واجهات جهاز الحظر. إضافة المعلومات، انقر فوق **موافق** و**تطبيق**.

Certificates	🛛 😨 Add Router Blocking Device Interface 🛛 🔊		
Trusted Hosts	Router Blocking Device:	10 100 100 1	
Blocking Reading Proportion	Roader bioening bevice.	10.100.100.1	
Device Login Profiles	Blocking Interface:	Fe0/1	
Blocking Devices	Direction:	In	~
Router Blocking Device Interface	Pre-Block ACL (optional):	blaster	
Cat 6K Blocking Device Interface	Post-Block ACL (optional):	101	
General Configuration	ОК Са	incel Help	

<u>التحقق من الصحة</u>

<u>شن الهجوم والعرقلة</u>

أكمل الخطوات التالية لإطلاق الهجوم والحجب:

- 1. قبل أن تقوم بتشغيل الهجوم، انتقل إلى IME، واختر **مراقبة الحدث > عرض الهجمات التي تم إسقاطها** واختر المستشعر من الجانب الأيمن.
 - 2. Telnet إلى منزل الموجه والتحقق من الاتصال من الخادم باستخدام هذه الأوامر. house#**show user**

Line User Host(s) Idle Location con 0 idle 00:00:00 0 * vty 0 idle 00:00:17 10.66.79.195 226

house#**show access-list**

3. من إضاءة الموجه، ومن برنامج Telnet إلى منزل الموجه ونوع **هجوم التجربة**.اضغط إما <**space>** أو جenter> 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 lost] Host 10.100.100.2 has been blocked due to the !--- signature "testattack" ---! . triggered 4. قم باستخدام برنامج Telnet إلى منزل الموجه واستخدم الأمر show access-list كما هو موضح هنا.

۵. کم باستخدام برنامج Fender اپنی میرن الموجه واستخدم الامر Snow access-list house#show access-list Extended IP access list IDS_FastEthernet0/1_in_0 permit ip host 10.66.79.195 any 10 (deny ip host 10.100.100.2 any (71 matches 20)

permit ip any any 30

5. من لوحة المعلومات الخاصة بعارض أحداث IDS، يظهر الإنذار الأحمر بمجرد تشغيل المحمد

			وم.
Date	Time	Sig. Name	Sig. ID
Device: Corp-IPS	(188 items)		
🚊 Severity; high	n (188 items)		14744- <u></u>
10/23/2009	09:59:13	String.tcp	60000/0
	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:

- من المستشعر نظر في إخراج show statistics access إلى الشبكة وتأكد من أن نشطة. من وحدة التحكم أو SSH إلى المستشعر، يتم عرض هذه المعلومات: sensor5#show statistics network-access Current Configuration AllowSensorShun = false ShunMaxEntries = 100 NetDevice Type = Cisco IP = 10.66.79.210NATAddr = 0.0.0.0Communications = telnet ShunInterface InterfaceName = FastEthernet0/1 InterfaceDirection = in State ShunEnable = true NetDevice IP = 10.66.79.210AclSupport = uses Named ACLs State = Active ShunnedAddr Host IP = 10.100.100.2ShunMinutes = 15MinutesRemaining = 12 sensor5# • تأكد من أن معلمة الاتصال توضح أنه يتم إستخدام البروتوكول الصحيح مثل Telnet أو SSH مع 3DES. يمكنك تجربة بروتوكول SSH أو Telnet يدويا من عميل SSH/Telnet على جهاز كمبيوتر للتحقق من صحة بيانات اعتماد اسم المستخدم وكلمة المرور. ثم حاول إستخدام Telnet أو SSH من المستشعر نفسه إلى الموجه
 - وانظر ما إذا كان يمكنك تسجيل الدخول بنجاح إلى الموجه.

<u>معلومات ذات صلة</u>

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

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