# ەنيوكتو IPS رعشتسم ةفاضإ - CS-MARS ريراقت دادعإ زاەجك

## المحتويات

<u>المقدمة</u> <u>المتطلبات الأساسية</u> <u>المكونات المستخدمة</u> <u>المنتجات ذات الصلة</u> <u>الاصطلاحات</u> <u>التحوين</u> إضافة جهاز Cisco IPS 6.x وتكوينه في MARS إضافة جهاز Cisco IPS 6.x وتكوينه في <u>MARS</u> <u>التحقق من قيام MARS بسحب الأحداث من جهاز Cisco IPS</u> <u>معلومات ذات صلة</u>

## <u>المقدمة</u>

يشرح هذا المستند كيفية إعداد جهاز Cisco لنظام منع التسلل الآمن (IPS) وأي أجهزة إستشعار افتراضية تم تكوينها للعمل كأجهزة إرسال تقارير إلى نظام Cisco لمراقبة الأمان والتحليل والاستجابة (CS-MARS).

## <u>المتطلبات الأساسية</u>

#### <u>المتطلبات</u>

بالنسبة لأجهزة SDEE 5.x و Cisco IPS 5.x و x.7، تقوم MARS بسحب السجلات باستخدام SDEE عبر SSL. لذلك، يجب أن يكون لدى MARS وصول HTTPS إلى المستشعر. لتجهيز المستشعر، يجب تمكين خادم HTTP على المستشعر، وتمكين TLS للسماح بوصول HTTPS، والتأكد من تعريف عنوان IP الخاص ب MARS كمضيف مسموح به، مضيف يمكنه الوصول إلى أحداث المستشعر والسحب. إذا تم تكوين أجهزة الاستشعار للسماح بالوصول من البيئات المضيفة المحدودة أو الشبكات الفرعية على الشبكة، فيمكنك إستخدام الأمر access-list ip\_address/netmask لتمكين هذا الوصول.

#### <u>المكونات المستخدمة</u>

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

- جهاز Cisco Secure MARS الذي يشغل الإصدار x.4.2 من البرنامج والإصدارات الأحدث
- جهاز Cisco 4200 Series IPS الذي يشغل الإصدار 6.0 من البرنامج والإصدارات الأحدث

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>المنتجات ذات الصلة</u>

يمكن إستخدام هذا التكوين أيضا مع أجهزة الاستشعار هذه:

- IPS-4240 •
- الطراز IPS-4255
  - IPS-4260 •
  - IPS-4270-20 •

#### <u>الاصطلاحات</u>

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

## <u>التكوين</u>

في هذا القسم، تقدم لك معلومات حول كيفية إضافة مستشعر Cisco لنظام منع التسلل الآمن (IPS) وتكوينه إلى جهاز Cisco لمراقبة الأمان والتحليل ونظام الاستجابة (CS-MARS).

### إضافة جهاز <u>Cisco IPS 6.x وتكوينه في MARS</u>

عند تحديد جهاز Cisco IPS 6.x أو x.7 في MARS، يمكنك اكتشاف أي أجهزة إستشعار افتراضية تم تكوينها على الجهاز. وعندما تكتشف هذه المجسات الافتراضية، يسمح هذا ل MARS بفصل الأحداث التي تم الإبلاغ عنها عن طريق المجس الظاهري. كما أنها تسمح لك بضبط قائمة الشبكات المراقبة لكل مستشعر ظاهري، مما يحسن من دقة التقارير المطلوبة.

أتمت هذا steps in order to أضفت وشكلت cisco IPS 6.x أواة في MARS:

- 1. أختر **مسؤول > إعداد النظام > الأمان وأجهزة المراقبة**. ثم انقر على **إضافة**.
- 2. أختر **Cisco IPS 6.x أو Cisco IPS أك** من قائمة نوع الجهاز. أدخّل الآن اسم المضيف للمستشعر في حقل **اسم الجهاز** كما هو موضح هنا. IPS1 هو اسم الجهاز المستخدم في هذا المثال. يجب أن تكون قيمة اسم الجهاز مطابقة لاسم المستشعر الذي تم تكوينه.

*Device Name:	IPS1						J	J		J	J		J							ŀ		J	l	l	J	l	J	l	l	l	J	J	J	l	J	l	J	J	l	J	l	l		l	l																																																			
• Reporting IP:	10	10	10	10		]			1		[	I		I	1		1	]	1		ĺ																											]	]	]	]	]			]	]	I			l	]	]	l	ĺ	ĺ	ĺ	ĺ						ĺ		l	ĺ									ĺ	ĺ	I	ĺ	ĺ	ĺ	ĺ	Î	ĺ			
Access Type:	SSL																																																																																															
Login:	-	22222	112262	11111	1																																																																																					1						
Password:	-				í.																																																																																											
Port:	443																																																																																															
	-																																																																																															
Monitor Resource Usage:	NO	Y																																																																																														
Pull IP Logs:	NO	4																																																																																														

⇔ Back	Test Connectivity	Submit
· · · · · · · · · · · · · · · · · · ·		· · · · · · · · · · · · · · · · · · ·

دخلت الآن العنوان إداري في **التقرير ip** مجال. عنوان IP الخاص بالتقارير هو نفس عنوان IP الإداري.

3. في حقل **تسجيل الدخول**، أدخل اسم المستخدم المقترن بالحساب الإداري الذي يتم إستخدامه للوصول إلى

جهاز التقارير. الآن، في **حقل كلمة المرور**، أدخل كلمة المرور المرتبطة باسم المستخدم المحدد في **حقل تسجيل الدخول. ال username cisco و**ال **كلمة** يستعمل **cisco123** في هذا مثال. أدخل أيضا رقم منفذ TCP الذي يستمع إليه خادم الويب الذي يعمل على المستشعر في **حقل المنفذ**. منفذ HTTPS الافتراضي هو 443.

*Device Name:	PS1		
Reporting IP:	10 10 10 10	]	
*Access Type:	SSL		
Login:	cisco'	1	
Password:			
Port:	443		
Monitor Resource Usage	: NO 🗸		
Pull IP Loos:	NO V		

🗢 Back	Test	Conne	ectivity	Y	Sub	mit

ملاحظة: بينما من الممكن تكوين HTTP فقط، فإن MARS يتطلب HTTPS.

4. تحقق الآن من إختيار NO في قائمة **إستخدام موارد المراقبة**. بينما يظهر خيار "مراقبة إستخدام الموارد" على هذه الصفحة، فإنه لا يعمل ل Cisco IPS.

+	*Device Name:	PS1			
+	Reporting IP:	10	10	10	0 10
+	Access Type:	SSL			
	Login:	ciso	o'		
	Password: Port:	443			
+	Monitor Resource Usage:	NO	~	Π	
	Pull IP Logs:	NO	Y		

- Submit
- 5. لسحب سجلات IP من المستشعر، أختر **نعم** من قائمة **سحب سجلات IP**. هذا سمة إختياري، أي يستطيع كنت استعملت إن يتطلب.

÷	*Device Name:	PS1			
÷	Reporting IP:	10	110	10	10
+	"Access Type:	551			
	Login:	ciso	x0"		
	Password:			•	
	Port:	443			
-	Monitor Resource Usage:	NO	*		
	Pull IP Logs:	NO	v		

G-Back Test Connectivity Submit

ينطبق هذا الإعداد على المستشعر بأكمله، والذي يتضمن السجلات التي تم إنشاؤها لتنبيهات أجهزة الاستشعار الظاهرية.

6. انقر فوق **إختبار الاتصال** للتحقق من التكوين وتمكين اكتشاف أجهزة الاستشعار الظاهرية.

* *Device Name:	PS1	]
Reporting IP:	10 10 10 10	
"Access Type:	55L	
Login:	cisco'	7
Password:		1
Port:	443	-
Monitor Resource Usage:	NO V	
Pull IP Loos:	NO V	

7. انقر فوق **اكتشاف** لاكتشاف أي أجهزة إستشعار افتراضية معرفة.

Reporting IP:       fg fg fg fg         * Access Type:       SSI         Login:       cisco         Password:       ee         Port:       443         Monitor Resource Usage:       NO N         Pull IP Logs:       NO N	Device Name:	PST	
*Access Type:     SSI       Login:     cisco       Password:     exerces       Port:     d43       Monitor Resource Usage:     NO *       Pull IP Logs:     NO *	Reporting IP:	fa 10 10 10	
Login:     cisco       Password:     exerce       Port:     443       Monitor Resource Usage:     NO NO       Pull IP Logs:     NO NO	*Access Type:	55L	
Monitor Resource Usage: NO S Pull IP Logs: NO S	Login: Password: Port:	Cisco ••••••• 443	
	Monitor Resource Usage: Pull IP Logs:	NO V	
	1. 10 10 10 1 CC		

**ملاحظة:** لا يعلم MARS بالتغييرات التي أجريت على المستشعر. في أي وقت تقوم فيه بإجراء تغييرات على إعدادات المستشعر الظاهري، يجب النقر فوق **اكتشاف** في صفحة تكوين المستشعر هذه لتحديث تفاصيل المستشعر الظاهري في MARS.

8. أختر خانة الاختيار المجاورة لاسم المستشعر الظاهري وانقر فوق **تحرير** لتحديد الشبكات المراقبة لكل مستشعر ظاهري. الآن تظهر صفحة وحدة IPS النمطية كما هو موضح هنا.

Reporting IP:     0     10     10       *Access Type:     SSL       Login:     cisco       Password:     ee       Port:     443       Monitor Resource Usage:     NO w       Pull TP Logs:     NO w	- Device Name:	IPSt		
*Access Type:     SSL       Login:     cisco       Password:     exerces       Port:     443       Monitor Resource Usage:     NO W       Pull TP Logs:     NO W	Reporting IP:	10 (10 10 (10	]	
Login:     cisco       Password:     eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee	Access Type:	55L		
Monitor Resource Usage: NO V Pull IP Logs: NO V	Login: Password: Port:	cisco		
	<ul> <li>Monitor Resource Usage:</li> <li>Pull IP Logs:</li> </ul>			
	Mintural Roberton Marine	Monitoring Ne	works	
Virtual Sensor Name Monitoring Networks	Tirtual sensor same		the second se	

9. لحساب مسار الهجوم والتخفيف من آثاره، حدد الشبكات التي يتم مراقبتها بواسطة المستشعر. أختر زر **تعريف** راديو **شبكة** من أجل تعريف الشبكة يدويا. ثم أكمل الخطوات التالية لتعريف شبكة:دخلت الشبكة عنوان في **الشبكة ip** مجال.أدخل قيمة قناع الشبكة المقابلة في حقل **القناع**.طقطقة **يضيف** in order to نقلت الشبكة يعين داخل ال monitore شبكة مجال.كرر الخطوات السابقة إذا كانت هناك حاجة لتعريف المزيد من الشبكات.

*Device Name: PS1:	
ptional: for attack path calculation a Monitored Networks:	nd mitigation enter monitoring networks information]
	Remove         10.10.0/255 255 255.0(n-10.10.10.0/24)            C Define a Network:         Network IP: 10 (10 (0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

Cancel Submit

**ملاحظة:** هذه ميزة إختيارية متوفرة ويمكن تخطيها إذا لم تكن مطلوبة.

10. انقر على زر **تحديد** راديو **شبكة** لتحديد الشبكات المتصلة بالجهاز. بعد ذلك أتمت هذا steps in order to أخترت الشبكات:أختر شبكة من قائمة **تحديد شبكة**.طقطقة **يضيف** in order to نقلت الشبكة يعين داخل ال monitore شبكة مجال.كرر الخطوات السابقة إذا كانت هناك حاجة لاختيار المزيد من الشبكات.

*Device Name:	IPS1			
nal: for attack pa Monitored Net	th calculation a	nd mitigation ente	r monitoring n	etworks information]
			Remove	(7: Select a Network: 10.10.10.0/255.255.255.0(n-10.10.10.0/24)
				Define a Network:     Network IP: 10 10 10 0     Mask: 255 255 0

Cancel Submit

**ملاحظة:** هذه ميزة إختيارية متوفرة ويمكن تخطيها إذا لم تكن مطلوبة.

- 11. كرر **الخطوة 8** حتى **الخطوة 1**0 لكل مستشعر ظاهري.
- 12. انقر فوق **إرسال** لحفظ التغييرات التي قمت بها. يظهر اسم الجهاز ضمن قائمة معلومات الأمان والمراقبة. تقوم عملية الإرسال بتسجيل التغييرات في جداول قاعدة البيانات. ولكنه لا يحمل التغييرات في ذاكرة العمل الخاصة بجهاز MARS. قامت عملية التنشيط بإرسال التغييرات إلى ذاكرة العمل.
- 13. انقر فوق **تنشيط** لتمكين MARS لبدء تجزئة الأحداث من هذا الجهاز.تبدأ MARS في عقد جلسات للأحداث

الناتجة عن هذه الوحدة النمطية وتقييم تلك الأحداث باستخدام قواعد الفحص والإفلات المحددة. يمكن الاستعلام عن أي أحداث تم نشرها بواسطة الجهاز إلى MARS قبل التنشيط باستخدام عنوان IP الخاص بالإبلاغ كمعيار مطابقة. ارجع إلى <u>تنشيط أجهزة إعداد التقارير والتخفيف.</u> للحصول على مزيد من المعلومات حول إجراء التنشيط.

## <u>التحقق من قيام MARS بسحب الأحداث من جهاز Cisco IPS</u>

من الشائع إنشاء أحداث حميدة على الشبكة للتحقق من تدفق البيانات. أكمل هذه الخطوات للتحقق من تدفق البيانات بين جهاز Cisco IPS و MARS:

- 1. على جهاز Cisco IPS، قم بتمكين التوقيعات 2000 و 2004 والتنبيه لها. تراقب التوقيعات رسائل ICMP (إختبارات الاتصال).
- 2. يؤز جهاز على الشبكة الفرعية التي يستمع إليها جهاز Cisco IPS. هذه الأحداث تم توليدها وسحبها بواسطة المريخ.
  - 3. تحقق من ظهور الأحداث في واجهة ويب MARS. يمكنك إجراء استعلام باستخدام جهاز Cisco IPS.
- 4. بمجرد التحقق من تدفق البيانات، يمكنك تعطيل توقيعات 2000 و 2004 على جهاز Cisco IPS.**ملاحظة:** إذا لم تفشل عملية الاتصال بالاختبار أثناء تكوين جهاز Cisco IPS في واجهة ويب MARS، فسيتم تمكين الاتصالات. تتيح لك هذه المهمة التحقق بشكل إضافي من إنشاء التنبيهات وسحبها بشكل صحيح.

## <u>استكشاف الأخطاء وإصلاحها</u>

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

## <u>معلومات ذات صلة</u>

- <u>صفحة دعم نظام مراقبة الأمان والتحليل والاستجابة من Cisco</u>
  - <u>صفحة دعم نظام منع الاقتحام من Cisco</u>
- نظام Cisco لمراقبة الأمان والتحليل والاستجابة معلومات التوافق
  - <u>طلبات التعليقات (RFCs)</u>
  - الدعم التقني والمستندات <u>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