

# تاهي بنت لاء ان ت س ا - Cisco Secure IPS ةئ ط ا خ ل ا ة ي با ج ي ا ل ا

## المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [الإنذارات السلبية والإيجابية الخاطئة](#)
- [آلة إستثناء Cisco Secure IPS](#)
- [إستبعاد مضيف](#)
- [إستبعاد شبكة](#)
- [تعطيل التوقيعات بشكل عام](#)
- [معلومات ذات صلة](#)

## المقدمة

يصف هذا المستند إستبعاد التنبهات الإيجابية الخاطئة لنظام منع التسلل الآمن (IPS) من Cisco.

## المتطلبات الأساسية

### المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الإصدار 7.0 من نظام منع التسلل الآمن (IPS) من Cisco و Cisco IPS Manager Express 7.0.

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

### الاصطلاحات

راجع [اصطلاحات تلميح Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

## الإنذارات السلبية والإيجابية الخاطئة

يقوم Cisco Secure IPS بتشغيل تنبيه عندما تطابق حزمة أو تسلسل معين من الحزم خصائص ملفات تعريف الهجوم المعروفة المعرفة في توقيعات IPS الآمنة من Cisco. معيار تصميم توقيع IPS الحرج هو تقليل ظهور الإنذارات الإيجابية والسلبية الخاطئة إلى الحد الأدنى.

تحدث العوامل الإيجابية الخاطئة (المشغلات الحميدة) عندما يقوم نظام منع الاختراقات (IPS) بالإبلاغ عن بعض الأنشطة الحميدة على أنها ضارة. يتطلب ذلك تدخلا بشريا لتشخيص الحدث. إن عددا كبيرا من الإيجابيات الكاذبة من الممكن أن تستنزف الموارد إلى حد كبير، والمهارات المتخصصة المطلوبة لتحليل هذه الإيجابيات مكلفة ومن الصعب العثور عليها.

تحدث السلبيات الخاطئة عندما لا يكتشف IPS النشاط الضار الفعلي ولا يبلغ عنه. قد تكون عاقبة ذلك كارثية، والتوقيع يجب أن تحدث باستمرار باكتشاف أي اكتشافات وتقنيات قرصنة جديدة. فالتقليل إلى أدنى حد من السلبيات الباطلة يعطى أولوية عالية جدا، وأحيانا على حساب تكرار الإيجابيات الخاطئة أكثر.

نظرا لطبيعة التوقيعات التي تستخدمها خدمات الإنترنت (IPS) للكشف عن الأنشطة الضارة، يكاد يكون من المستحيل القضاء تماما على الإيجابيات والسلبيات الزائفة دون الإضرار بشدة بفعالية خدمات الإنترنت (IPS) أو الإخلال الشديد بالبنية الأساسية للحوسبة في إحدى المؤسسات (مثل الأجهزة المضيغة والشبكات). يؤدي التوليف المخصص عند نشر بروتوكول الإنترنت (IPS) إلى تقليل الإيجابيات الخاطئة إلى الحد الأدنى. يلزم إعادة الضبط دوريا عند تغير بيئة الحوسبة (على سبيل المثال، عند نشر أنظمة وتطبيقات جديدة). يوفر نظام منع التسلسل (IPS) الأمن من Cisco إمكانية ضبط مرنة يمكنها تقليل الإيجابيات الخاطئة أثناء عمليات الحالة المستقرة.

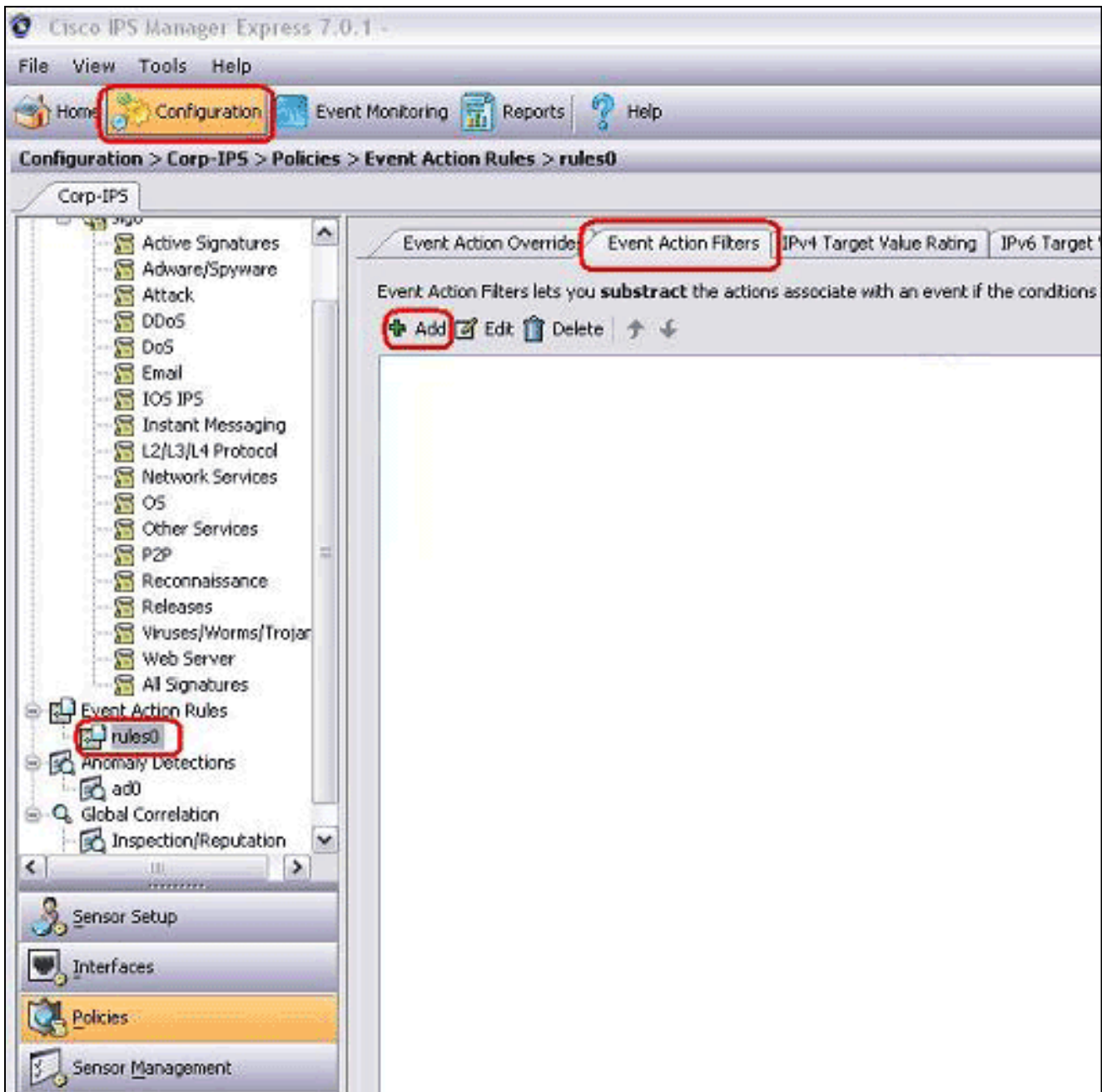
## آلية إستثناء Cisco Secure IPS

يوفر Cisco Secure IPS إمكانية إستبعاد توقيع معين من أو إلى مضيف معين أو عناوين شبكة معينة. لا تقوم التوقيعات المستبعدة بإنشاء أيقونات تنبيه أو سجلات سجل عندما يتم تشغيلها من البيئات المضيغة أو الشبكات التي يتم إستبعادها بشكل محدد من خلال هذه الآلية. على سبيل المثال، قد تقوم محطة إدارة شبكة بإجراء اكتشاف الشبكة من خلال تشغيل عمليات تمشيط شبكة ICMP، والتي تقوم بتشغيل "كنس شبكة ICMP" باستخدام توقيع "إيكو" (معرف التوقيع 2100). إذا قمت باستبعاد التوقيع، فلا تحتاج إلى تحليل التنبيه وحذفه في كل مرة يتم فيها تشغيل عملية اكتشاف الشبكة.

### إستبعاد مضيف

أتمت هذا steps in order to استثنت مضيف خاص (مصدر عنوان) من توليد توقيع تنبيه خاص:

1. أخترت تشكيل <Corp-IPS> سياسة <حدث إجراء قاعدة> قاعدة 0، وطققة الحدث إجراء مرشح.



2. انقر فوق إضافة (Add).
3. اكتب اسم المرشح ومعرف التوقيع وعنوان IPv4 للمهاجم والإجراء الخاص بالطرح في الحقول المناسبة، ثم انقر فوق

**Add Event Action Filter**

Name: Excluded Host

Enabled:  Yes  No

Signature ID: 2100

Subsignature ID:

Attacker IPv4 Address: 10.10.10.10

Attacker IPv6 Address:

Attacker Port: 0-65535

Victim IPv4 Address: 0.0.0.0-255.255.255.255

Victim IPv6 Address:

Victim Port: 0-65535

Risk Rating: 0 to 100

Actions to Subtract: Produce Alert

More Options

OK Cancel Help

ملاحظة:

موافق.

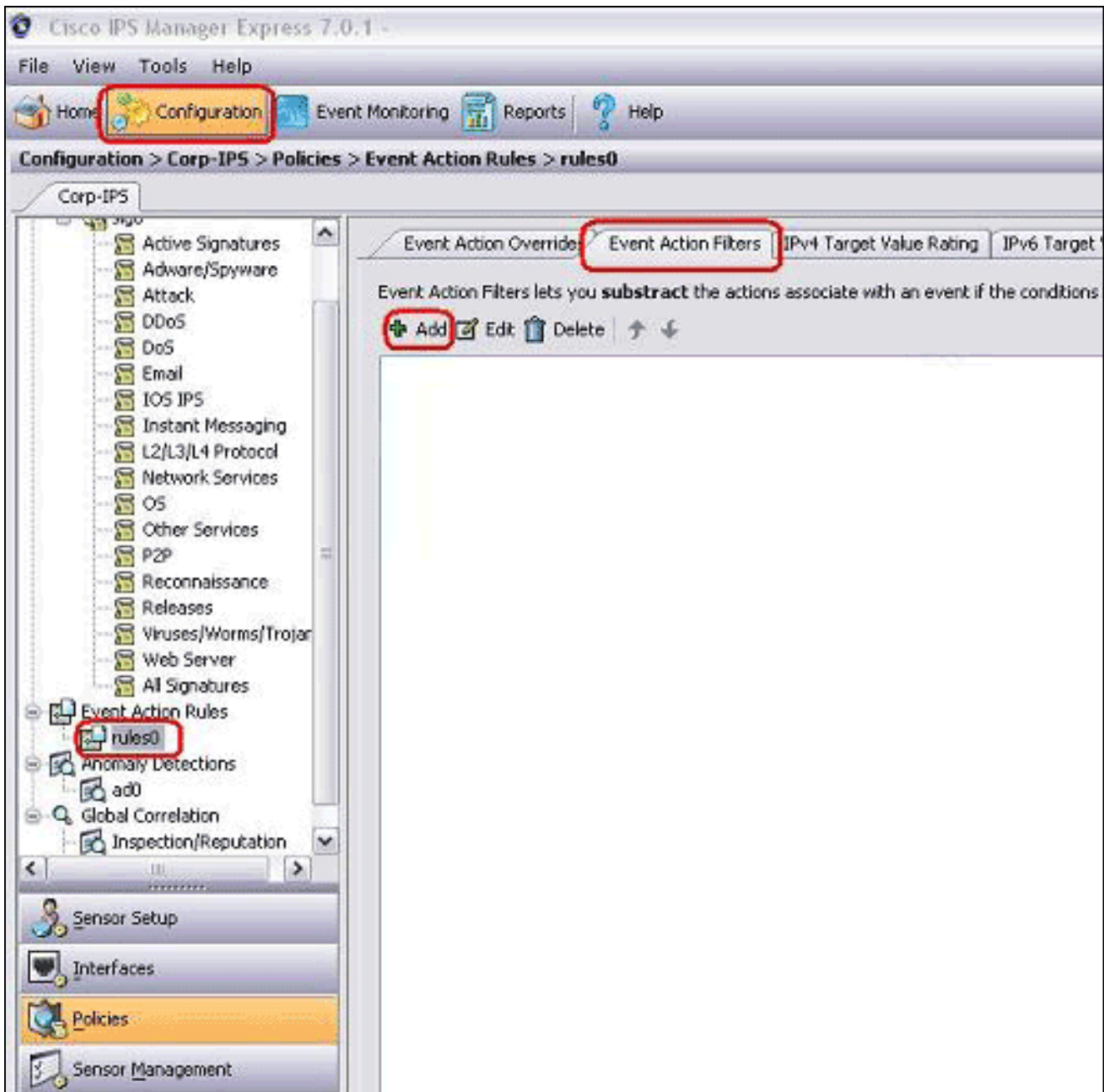
إذا احتجت لاستبعاد عناوين IP متعددة من شبكات مختلفة، فيمكنك استخدام الفاصلة كمحدد. على أي حال، إذا كنت تستخدم فاصلة، تجنب مسافة زائدة بعد الفاصلة؛ وإلا، فقد تتلقى خطأ. ملاحظة: بالإضافة إلى ذلك، يمكنك استخدام المتغيرات المعرفة في صفحة متغيرات الحدث. تكون هذه المتغيرات مفيدة عندما يجب تكرار نفس القيمة في مرشحات إجراءات حدث متعددة. يجب استخدام علامة الدولار (\$) كبادئة للمتغير. يمكن أن يكون المتغير أحد هذه التنسيقات: عنوان IP كامل، على سبيل المثال، 10.77.23.23. نطاق عناوين IP؛ على سبيل المثال، 10.9.2.155-10.9.2.10. مجموعة من نطاق عناوين IP؛ على سبيل المثال، 172.16.33.15-192.168.100.11-172.16.33.100، 192.168.100.1

## إستبعاد شبكة

كما يستثنى عامل تصفية إجراء الحدث توقعات معينة لإطلاق تنبيه استنادا إلى عنوان شبكة مصدر أو وجهة.

أتمت هذا steps in order to استثنيت شبكة من توليد توقيع تنبيه خاص:

1. انقر فوق علامة التبويب عوامل تصفية إجراء الحدث.



2. انقر فوق إضافة (Add).
3. اكتب اسم المرشح، معرف التوقيع، عنوان الشبكة بقناع شبكة فرعية، والإجراء الخاص بالطرح في الحقول المناسبة، ثم انقر فوق

**Add Event Action Filter**

Name: Excluded Network

Enabled:  Yes  No

Signature ID: 2100

Subsignature ID: 0-255

Attacker IPv4 Address: 10.10.10.0-255.255.255.0

Attacker IPv6 Address:

Attacker Port: 0-65535

Victim IPv4 Address: 0.0.0.0-255.255.255.255

Victim IPv6 Address:

Victim Port: 0-65535

Risk Rating: 0 to 100

Actions to Subtract: Produce Alert

More Options

OK Cancel Help

موافق.

## تعطيل التوقيعات بشكل عام

قد ترغب في تعطيل توقيع من غير مفلق في أي وقت. لتمكين التوقيعات وتعطيلها واستعادتها، أكمل الخطوات التالية:

1. قم بتسجيل الدخول إلى IME باستخدام حساب ذي امتيازات المسؤول أو عامل التشغيل.
2. أخترت تشكيل <مستشعر\_name> نهج <توقيع تعريفات> sig0 كل التوقيعات.
3. لتحديد موقع توقيع، أختار خيار فرز من القائمة المنسدلة مرشح. على سبيل المثال، إذا كنت تبحث عن توقيع مسح شبكة ICMP، أختار كل التوقيعات تحت sig0، ثم ابحث باستخدام معرف التوقيع أو الاسم. يقوم جزء sig0 بتحديث تلك التوقيعات التي تطابق معايير الفرز الخاصة بك وعرضها فقط.
4. لتمكين أو تعطيل توقيع موجود، أختار التوقيع، وإكمال الخطوات التالية: عرض العمود "ممكن" لتحديد حالة التوقيع. التوقيع الذي تم تمكينه له خانة الاختيار. لتمكين توقيع معطل، حدد خانة الاختيار ممكن. لتعطيل توقيع تم تمكينه، قم بإلغاء تحديد خانة الاختيار تمكين. لاستبعاد توقيع أو أكثر، أختار التوقيع (التوقيعات)، وانقر بزر الماوس الأيمن، ثم انقر فوق تغيير الحالة إلى < مستبعد.
5. انقر فوق تطبيق لتطبيق التغييرات التي قمت بها وحفظ التكوين الذي تمت مراجعته.



Configuration > Corp-IPS > Policies > Signature Definitions > sig0 > Attack

Corp-IPS

IPS Policies

Signature Definitions

sig0

Active Signatures

Adware/Spyware

Attack

DDoS

DOS

Email

IOS IPS

Instant Messaging

L2/L3/L4 Protocol

Network Services

OS

Other Services

P2P

Reconnaissance

Releases

Viruses/Worms/Trojan

Web Server

All Signatures

Event Action Rules

rules0

Anomaly Detections

Sensor Setup

Interfaces

Policies

Sensor Management

Sensor Monitoring

Edit Actions Enable Disable Restore Default Show Events MySDN Edit Add Delete Clone Ex

Select: All-Attack Filter: Sig ID 2100

ID	Name	Enabled	Severity	Fidelity Rating	Base RR	Signature Actions			Type	Engn
						Alert and Log	Deny	Other		
2100 0	ICMP Network Sweep	<input checked="" type="checkbox"/>	Low	100	50	Alert			Tuned	S

Total Signatures: 2745 Enabled Signatures: 1161 Signatures in this category: 2527 Enabled in this category: 1069

MySDN (Embedded)

Description: Triggers when IP datagrams are received directed at multiple hosts on the network with the protocol field of the IP header set to 8 (Echo Request). This is indicative that a reconnaissance sweep of your network may be in progress. This may be

Signature ID: 2100|0 Signature Name: ICMP Network Sweep w/Echo

Release Date: 2/2/2001 Release Version: S2

Explanation / Related Threats

Apply Reset Advanced...

## معلومات ذات صلة

- نهاية البيع لمدير Cisco Secure IDS
- صفحة دعم اكتشاف التسلسل الآمن من Cisco
- الدعم التقني والمستندات - Cisco Systems

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نء مء دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءء. ةصاأل مء تءل ب  
Cisco ةللخت. فرتمة مچرت مء مء دق ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل  
ىل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل  
(رفوتم طبارل) ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل