

# رايخ مادختساب عادالايئاصحإةعومجم ةدحاو ةيناث ةدمل عادالايئاصحإةعومجم

## المحتويات

### المقدمة

شاشة فائقة الأداء لمدة ثانية واحدة

تمكين على الإصدار 5.4 أو أحدث

تمكين على الإصدارات السابقة ل 5.4

المستندات ذات الصلة

## المقدمة

على جهاز يشغل برنامج Sourcefire، يمكنك تكوين المعلمات الأساسية التي تراقب الأداء الخاص بها وإعداد تقارير عنه. تعد إحصائيات الأداء أمرا بالغ الأهمية لاستكشاف المشكلات المتعلقة بالأداء وإصلاحها على جهاز يعمل بنظام التشغيل Snort. يقدم هذا المستند الخطوات لتمكين هذه الميزة باستخدام مركز إدارة FireSIGHT.

**تحذير:** إذا كانت شبكتك مباشرة وقمت بتمكين أداء ثانية واحدة على نظام إنتاج، فقد يؤثر ذلك على أداء الشبكة. يجب عليك تمكين هذا فقط إذا كان هذا مطلوباً بواسطة دعم Cisco التقني لغرض استكشاف الأخطاء وإصلاحها.

**ملاحظة:** تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي).

## شاشة فائقة الأداء لمدة ثانية واحدة

تتيح لك ميزة مراقبة الأداء لمدة ثانية واحدة تحديد الفواصل الزمنية التي يقوم النظام خلالها بتحديث إحصائيات الأداء على أجهزتك من خلال تكوين ما يلي:

• عدد الثواني

• عدد الحزم المحللة

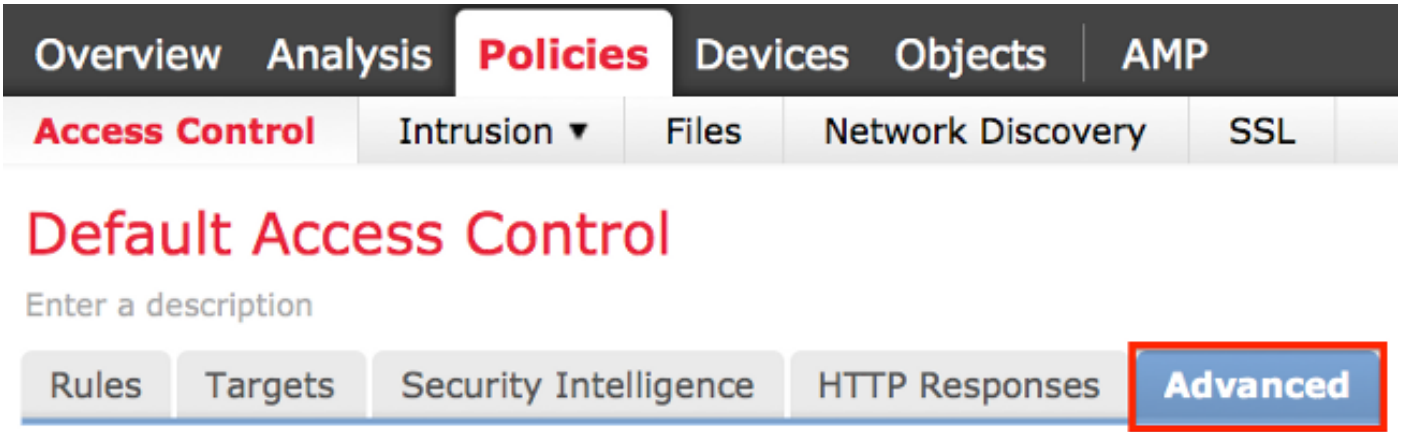
عند انقضاء عدد الثواني المحددة منذ آخر تحديث لإحصائيات الأداء، يتحقق النظام من تحليل عدد الحزم المحدد. في هذه الحالة، يقوم النظام بتحديث إحصائيات الأداء. وإذا لم تكن هناك مساحة، فسيبتظر النظام حتى يتم تحليل العدد المحدد من الحزم.

## تمكين على الإصدار 5.4 أو أحدث

الخطوة 1: حدد السياسات < التحكم في الوصول. تظهر صفحة "نهج التحكم بالوصول".

الخطوة 2: انقر فوق أيقونة القلم الرصاص بجوار نهج التحكم بالوصول الذي تريد تحريره.

الخطوة 3: حدد علامة التبويب خيارات متقدمة. تظهر صفحة الإعدادات المتقدمة لنهج التحكم بالوصول.



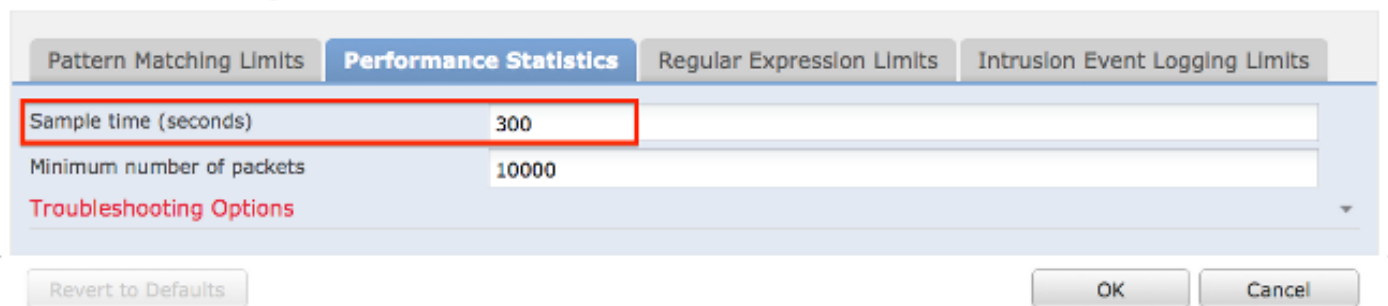
الخطوة 4: انقر أيقونة القلم الرصاص المجاورة لإعدادات الأداء.

### Performance Settings

Pattern Matching Limits - Max Pattern Match States to Analyze Per Packet	5
Performance Statistics - Sample Time (seconds)	300
Regular Expression - Limit	Default
Regular Expression - Recursion Limit	Default
Intrusion Event Logging Limits - Max Events Stored Per Packet	8

الخطوة 5: حدد علامة التبويب إحصائيات الأداء في النافذة المنبثقة التي تظهر. قم بتعديل وقت العينة أو الحد الأدنى لعدد الحزم كما هو موضح أعلاه.

### Performance Settings



الخطوة 6: إختياريا، قم بتوسيع قسم خيارات أستكشاف الأخطاء وإصلاحها وتعديل هذه الخيارات فقط إذا طلب منك ذلك بواسطة Cisco TAC.

الخطوة 7: انقر فوق موافق.

الخطوة 8: يجب حفظ نهج التحكم في الوصول وتطبيقه حتى تصبح التغييرات التي قمت بها نافذة المفعول.

## تمكين على الإصدارات السابقة ل 5.4

الخطوة 1: انتقل إلى صفحة سياسة التسلل. تسجيل الدخول إلى مركز إدارة FireSIGHT لديك. انتقل إلى السياسات

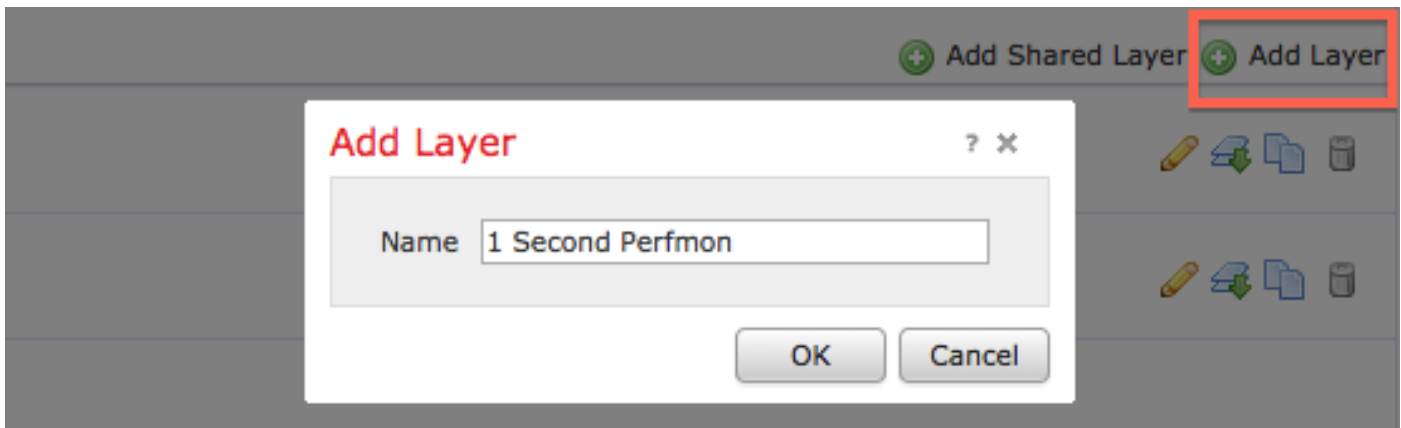
< الاقتحام > سياسة الاقتحام.

الخطوة 2: قم بتحرير سياسة التطفل التي تريد تطبيقها. انقر أيقونة القلم الرصاص لتحرير السياسة.

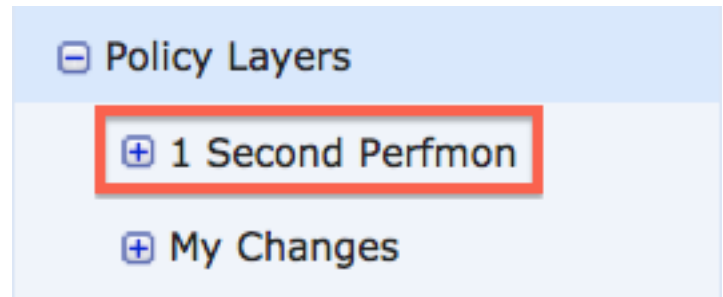


ملاحظة: نظرا لتصميم هذا الإعداد المتقدم، يجب عليك تعديل هذا التكوين فقط ضمن نهج إقتحام يتم استخدامه كإجراء افتراضي لنهج التحكم بالوصول الخاص بك.

الخطوة 3: إضافة طبقة نهج. انقر طبقات السياسة ثم إضافة طبقة. قم بتسمية الطبقة 1 Perfmon ثانية".









تحقق من طبقات السياسة في اللوحة اليسرى، وتأكد أن الطبقة الجديدة 1 ثانية " أعلى كل الطبقات الأخرى.



الخطوة 4: قم بتمكين تكوين إحصائيات الأداء. تحت إعدادات الأداء، حدد زر الخيار يمكن بجوار إحصائيات الأداء تشكيل، وانقر تحرير.

## Performance Settings

Event Queue Configuration	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	 Edit
Latency-Based Packet Handling	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	 Edit
Latency-Based Rule Handling	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	 Edit
Performance Statistics Configuration	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	 Edit
Regular Expression Limits	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	 Edit
Rule Processing Configuration	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	 Edit

**الخطوة 5:** تعديل وقت العينة الافتراضي إلى 1 ثانية، والحد الأدنى لعدد الحزم إلى 100 حزمة.

### Performance Statistics Configuration

#### Settings

Sample time	<input type="text" value="1"/>	seconds
Minimum number of packets	<input type="text" value="100"/>	

**الخطوة 6:** انقر فوق **معلومات النهج** في اللوحة اليسرى وقم بتنفيذ التغييرات وقم بتطبيق السياسة المحدثة على الأجهزة التي تريد توصيفها.

### Policy Information

- Variables
- Rules
- FireSIGHT Recommendations
- Advanced Settings

**الخطوة 7:** عكس الإعدادات بعد تجميع البيانات. من أجل الإرجاع، ببساطة احذف طبقة النهج 1 ثانية".

**تحذير:** لا تنس إرجاع التكوين. وإلا، فقد يؤدي ذلك إلى حدوث مشكلة في الأداء.

## المستندات ذات الصلة

- [عرض أداء حدث التطفل](#)
- [إنشاء رسومات بيانية لإحصائيات أداء أحداث التطفل](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت  
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبل او  
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاغل مه تلبل  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىل إأمئاد ةوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco  
Systems (رفوتم طبارل) يلصلأل يزىلچنل دن تسمل