يتم حظر عنوان IP أو إدراجه في القائمة السوداء بواسطة الاستخبارات الأمنية لنظام FireSIGHT من Cisco

المحتويات

المقدمة

تتيح لك ميزة ذكاء الأمان تحديد حركة مرور البيانات التي يمكن أن تجتاز شبكتك استنادا إلى عنوان IP للمصدر أو الوجهة. ويكون هذا مفيدا بشكل خاص إذا كنت تريد إدراج عناوين IP المحددة على القائمة السوداء - رفض حركة المرور منها وإليها، قبل إخضاع حركة المرور للتحليل بواسطة قواعد التحكم في الوصول. يوضح هذا المستند كيفية معالجة السيناريوهات عند حظر عنوان IP أو إدراجه في القائمة السوداء بواسطة نظام FireSIGHT من Cisco.

المتطلبات الأساسية

المتطلبات

توصي cisco أن يتلقى أنت معرفة على cisco FireSIGHT إدارة مركز.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات المكونات المادية والبرامج التالية:

- Cisco FireSIGHT Management Center
- جهاز أمان FirePOWER من Cisco

- ASA من Cisco مع وحدة FirePOWER (SFR)
- الإصدار 5.2 من البرنامج وأ إصدار أحدث

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

الفرق بين قائمة موجز المعلومات الاستخبارية والاستخبارات

هناك طريقتان لاستخدام ميزة "معلومات الأمان" في نظام FireSIGHT:

تغذية المعلومات الإستخباراتية الأمنية

يعد موجز معلومات الأمان مجموعة ديناميكية من عناوين IP التي يقوم مركز الدفاع بتنزيلها من خادم HTTP أو HTTPS. لمساعدتك على إنشاء قوائم سوداء، توفر Cisco *موجز معلومات الأمان*، والذي يمثل عناوين IP التي يحددها فريق أبحاث الثغرات (VRT) للحصول على سمعة سيئة.

قائمة الاستخبارات الأمنية

قائمة الذكاء الأمني، بالتباين مع موجز، هي قائمة ثابتة بسيطة من عناوين IP التي تقوم بتحميلها يدويا إلى مركز إدارة FireSIGHT.

تم حظر عنوان IP الشرعي أو إدراجه في القائمة السوداء

التحقق من وجود عنوان IP في موجز معلومات الأمان

إذا تم حظر عنوان IP بواسطة القائمة السوداء لموجز معلومات الأمان، فيمكنك اتباع الخطوات أدناه للتحقق من ذلك:

الخطوة 1: الوصول إلى واجهة سطر الأوامر (CLI) الخاصة بجهاز FirePOWER أو الوحدة النمطية للخدمة.

الخطوة 2: قم بتشغيل الأمر التالي. استبدلت <ip_address> مع العنوان أن أنت تريد أن يبحث عن:

```
admin@Firepower:~$ grep
```

على سبيل المثال، إن يريد أنت أن يبحث عن عنوان 198.51.100.1، يركض الأمر التالي:

```
admin@Firepower:~$ grep 198.51.100.1 /var/sf/iprep_download/*.blf
```

إذا قام هذا الأمر بإرجاع أي تطابق لعنوان IP الذي قمت بتوفيره، فإنه يشير إلى أن عنوان IP

موجود على القائمة السوداء لموجز معلومات الأمان.

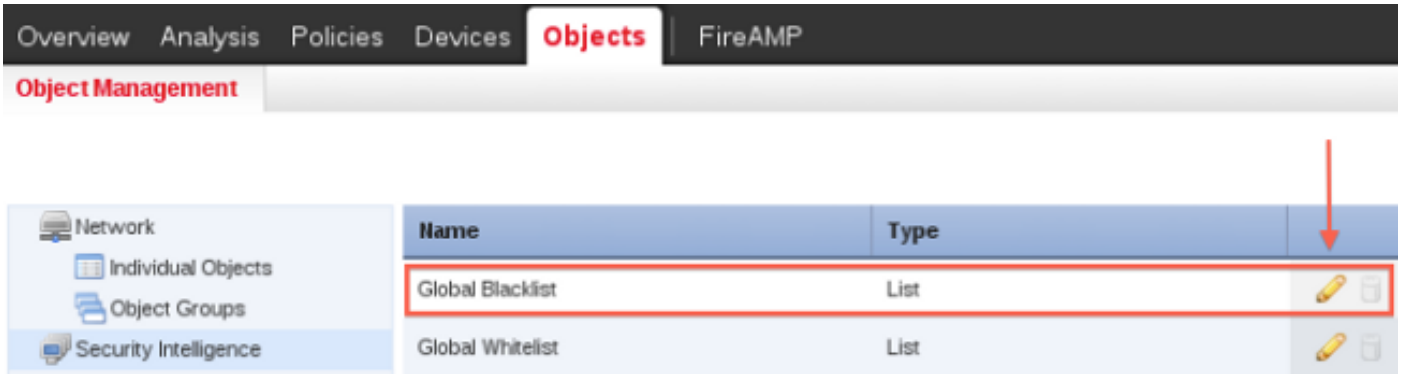
تحقق من القائمة السوداء

للعثور على قائمة بعناوين IP التي قد تكون مدرجة في القائمة السوداء، اتبع الخطوات التالية:

الخطوة 1: الوصول إلى واجهة الويب الخاصة بمركز إدارة FireSIGHT.

الخطوة 2: انتقل إلى **الكائنات > إدارة الكائنات > ذكاء الأمان**.

الخطوة 3: انقر فوق رمز *القلم الرصاص* لفتح **القائمة السوداء العامة** أو تحريرها. تظهر نافذة منبثقة بقائمة من عناوين IP.



العمل باستخدام عنوان IP محظور أو مدرج في القائمة السوداء

إذا تم حظر عنوان IP معين أو إدراجه في القائمة السوداء بواسطة موجز إستخبارات الأمان، فيمكنك مراعاة أي من الخيارات التالية للسماح به.

الخيار 1: خبراء الاستخبارات الأمنية

يمكنك تبييض عنوان IP المدرج على القائمة السوداء من قبل إستخبارات الأمن. رجل أبيض يتخطى قائمتك السوداء. يقوم نظام FireSIGHT بتقييم حركة المرور باستخدام عنوان IP للمصدر أو الوجهة البيضاء باستخدام قواعد التحكم في الوصول، حتى إذا كان عنوان IP مدرجا في القائمة السوداء أيضا. لذلك، يمكنك إستخدام أبيض عندما تكون القائمة السوداء ما تزال مفيدة، لكنها واسعة جدا في النطاق وتحظر حركة المرور التي تريد فحصها بشكل غير صحيح.

على سبيل المثال، إذا قام موجز ويب مشهور بمنع وصولك إلى مورد حيوي بشكل غير صحيح ولكنه مفيد بشكل عام لمؤسستك، فيمكنك إزالة عناوين IP المصنفة بشكل غير صحيح فقط، بدلا من إزالة موجز الويب بالكامل من القائمة السوداء.

> **تحذير**: بعد إجراء أي تغيير في نهج التحكم في الوصول، يجب إعادة تطبيق النهج على الأجهزة المدارة.

الخيار 2: فرض عامل تصفية المعلومات الاستخبارية الأمنية حسب المنطقة الأمنية

للحصول على مستويات إضافية، يمكنك فرض تصفية معلومات الأمان استنادا إلى ما إذا

كان عنوان IP للمصدر أو الوجهة في اتصال ما موجودا في منطقة أمان معينة.

لتمديد المثال الأبيض أعلاه، يمكنك تحديد عناوين IP المصنفة بشكل غير صحيح، ولكن بعد ذلك تقييد الكائن الأبيض باستخدام منطقة أمان يستخدمها أولئك في مؤسستك الذين يحتاجون إلى الوصول إلى عناوين IP هذه. وبهذه الطريقة، يمكن فقط لهؤلاء الذين يحتاجون إلى عمل الوصول إلى عناوين IP البيضاء. وكمثال آخر، قد ترغب في إستخدام موجز بريد إلكتروني عشوائي من طرف خارجي لإدراج حركة مرور البيانات في قائمة سوداء في منطقة أمان خادم البريد الإلكتروني.

الخيار 3: المراقبة، بدلا من القائمة السوداء

إذا لم تكن متأكدا من رغبتك في إدراج عنوان IP أو مجموعة من العناوين على القائمة السوداء، فيمكنك إستخدام إعداد "المراقبة فقط"، الذي يسمح للنظام بتمرير الاتصال المطابق إلى قواعد التحكم في الوصول، ولكنه يقوم أيضا بتسجيل المطابقة إلى القائمة السوداء. لاحظ أنه لا يمكنك تعيين القائمة السوداء العمومية على جهاز العرض فقط

ضع في الاعتبار سيناريو تريد فيه إختبار موجز ويب خاص بجهة خارجية قبل تنفيذ الحظر باستخدام موجز الويب هذا. عند تعيين موجز الويب على المراقبة فقط، يسمح النظام للاتصالات التي كان سيتم حظرها ليتم تحليلها بشكل أكبر بواسطة النظام، ولكنه يقوم أيضا بتسجيل سجل لكل من هذه الاتصالات لتقييمك.

خطوات تكوين معلومات الأمان باستخدام الإعداد "monitor-only":

1. في علامة التبويب "**معلومات الأمان**" الموجودة في نهج التحكم في الوصول، انقر فوق رمز التسجيل. يظهر مربع الحوار "خيارات القائمة السوداء".
2. حدد خانة الاختيار **إتصالات السجل** لتسجيل أحداث بدء الاتصال عندما تفي حركة مرور البيانات بشروط معلومات الأمان.
3. حدد مكان إرسال أحداث الاتصال.
4. انقر فوق **موافق** لتعيين خيارات التسجيل الخاصة بك. تظهر علامة التبويب "معلومات الأمان" مرة أخرى.
5. طقطقة **حفظ**. يجب تطبيق نهج التحكم في الوصول لتفعيل التغييرات التي أجريتها.

الخيار 4: الاتصال بمركز المساعدة التقنية ل Cisco

يمكنك دائما الاتصال بمركز المساعدة التقنية ل Cisco، إذا:

- لديك أسئلة حول الخيارات المذكورة أعلاه 1 أو 2 أو 3.
- تحتاج إلى مزيد من البحث والتحليل حول عنوان IP المدرج على القائمة السوداء بواسطة إستخبارات الأمان.
- تحتاج إلى شرح حول وضع عنوان IP في القائمة السوداء بواسطة الاستخبارات الأمنية.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).