تكوين معلومات الأمان المستندة إلى المجال (سياسة DNS) في الوحدة النمطية FirePOWER باستخدام ASDM (إدارة المربع)

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين معلومات الأمان المستندة إلى المجال (SI) على ASA باستخدام وحدة FirePOWER النمطية باستخدام مدير أجهزة الأمان القابل للتكيف (ASDM).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة جدار حماية ASA (جهاز الأمان القابل للتكيف)
- ASDM (مدير أجهزة الأمان المعدلة)
- معرفة وحدة FirePOWER

ملاحظة: يتطلب عامل تصفية معلومات الأمان ترخيص حماية.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- الوحدات النمطية ASA FirePOWER (ASA 5506X/5506H-X/5506W-X، ASA 5508-X، ASA 5516-X) مع إصدار البرنامج 6.0.0 أو أعلى
- وحدة ASA FirePOWER (ASA 5515-X، ASA 5525-X، ASA 5545-X، ASA 5555-X) مع برنامج 6.0.0 أو أعلى

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.

معلومات أساسية

يوفر نظام FirePOWER القدرة على اعتراض طلبات حركة مرور DNS والبحث عن اسم المجال الضار. إذا عثرت الوحدة النمطية FirePOWER على مجال ضار، يتخذ FirePOWER الإجراء المناسب للحد من الطلب وفقا للتكوين الخاص بنهج DNS.

طرق هجوم جديدة مصممة لاختراق الذكاء القائم على IP، إساءة إستخدام ميزات موازنة حمل DNS من أجل إخفاء عنوان IP الفعلي لخادم ضار. بينما تم تبادل عناوين IP المرتبطة بالهجوم إلى الداخل والخارج بشكل متكرر، يكون من النادر تغيير اسم المجال.

توفر FirePOWER القدرة على إعادة توجيه الطلب الخبيث إلى خادم Sinkhole الذي يمكن أن يكون خادم HoneyPot لاكتشاف حركة مرور الهجمات أو تبريدها أو دراستها لمعرفة المزيد حول هذه الحركة.

نظرة عامة على قوائم المجالات وموجز ويب

تحتوي قوائم المجالات وموجز ويب على قائمة اسم المجال الضار الذي تم تصنيفه كذلك في الفئة المختلفة استنادا إلى نوع الهجوم. عادة، يمكنك تصنيف موجز الويب إلى نوعين.

توفر Cisco Talos قوائم المجالات وموجز ويب

مجموع DNS: مجموعة من أسماء المجالات التي تقوم بالمسح باستمرار بحثا عن نقاط الضعف أو محاولات الاستغلال أنظمة أخرى.

DNS Bogon: مجموعة من أسماء المجالات التي لا تخصص ولكن تعيد حركة المرور، تعرف أيضا ب IPs مزورة.

DNS Bots: مجموعة من أسماء المجالات التي تشارك بنشاط كجزء من شبكة خبيثة، ويتحكم فيها جهاز تحكم معروف في الشبكة العنكبوتية.

DNS CnC: مجموعة من أسماء المجالات المحددة كخوادم تحكم Botnet معروفة.

مجموعة أدوات إستغلال نظام أسماء المجالات DNS: مجموعة من أسماء المجالات التي تحاول إستغلال أنظمة أخرى.

البرامج الضارة لـ DNS: مجموعة أسماء المجالات التي تحاول نشر البرامج الضارة أو مهاجمة أي شخص يقوم بزيارتها بشكل نشط.

DNS Open_proxy: مجموعة من أسماء المجالات التي تقوم بتشغيل Open Web Proxy وتقدم خدمات إستعراض ويب مجهولة.

DNS Open_relay: مجموعة من أسماء المجالات التي تقدم خدمات ترحيل البريد الإلكتروني المجهول المستخدمة من قبل مهاجمي البريد العشوائي والهيكل.

DNS Phish: مجموعة من أسماء المجالات التي تحاول بشكل نشط خداع المستخدمين النهائيين لإدخال معلوماتهم السرية مثل أسماء المستخدمين وكلمات المرور.

در DNS: مجموعة من أسماء المجالات التي تتم ملاحظتها بشكل متكرر في سلوك مريب أو ضار.

البريد العشوائي لـ DNS: مجموعة أسماء المجالات المحددة كمصدر يرسل رسائل بريد إلكتروني عشوائي.

DNS مريب: جمع أسماء المجالات التي تعرض نشاطا مريبا والتي قيد البحث النشط.

DNS Tor_exit_node: مجموعة من أسماء المجالات التي توفر خدمات عقد الخروج لشبكة "محول الهوية".

قوائم المجالات المخصصة وموجز ويب

القائمة السوداء العامة لـ DNS: مجموعة القائمة المخصصة لأسماء المجالات التي تم تعريفها على أنها ضارة من قبل المسؤول.

Global WhiteList for DNS: مجموعة القائمة المخصصة لأسماء المجالات التي تم تعريفها على أنها أصلية بواسطة المسؤول.

تكوين ذكاء أمان DNS

هناك عدة خطوات لتكوين معلومات الأمان المستندة إلى اسم المجال.

1. تكوين قائمة/موجز ويب DNS المخصص (إختياري)
2. تكوين كائن SINKHOLE (إختياري)
3. تكوين نهج DNS
4. تكوين سياسة التحكم في الوصول
5. نشر سياسة التحكم بالوصول

الخطوة 1. تكوين موجز/قائمة مخصص ل DNS (إختياري).

هناك قوائمان محددان مسبقا يسمحان لك بإضافة المجالات إليها. يمكنك إنشاء القوائم وموجز الويب للمجالات التي تريد حظرها.

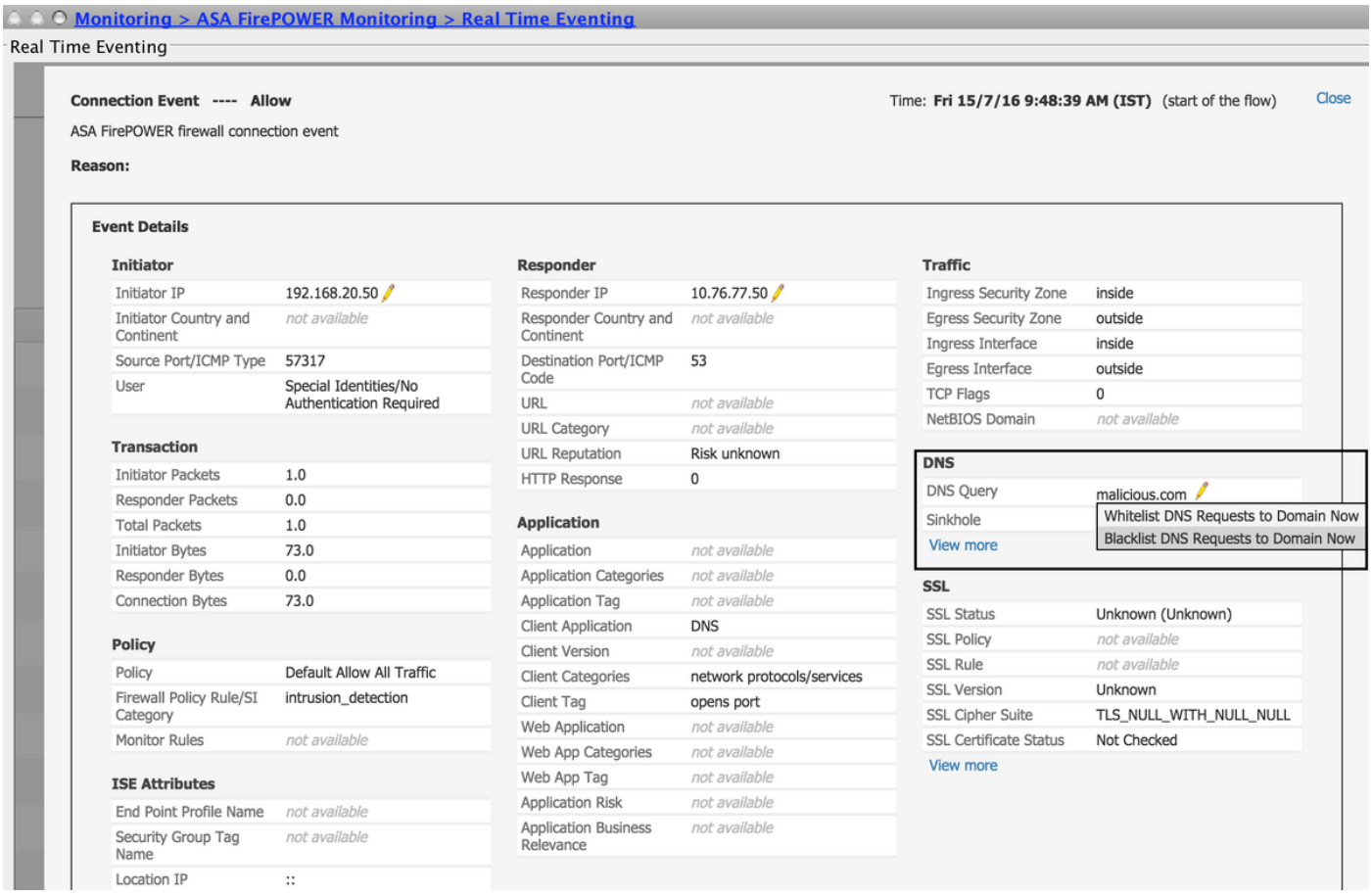
- القائمة السوداء العالمية ل DNS
- Global Whitelist for DNS

إضافة عناوين IP يدويا إلى القائمة السوداء العالمية والخوادم البيضاء العالمية

تسمح لك وحدة FirePOWER النمطية بإضافة مجالات معينة إلى القائمة السوداء العالمية عندما تعرف أنها جزء من نشاط ضار. يمكن أيضا إضافة المجالات إلى Global Whitelist إذا كنت تريد السماح بحركة المرور إلى مجالات معينة تم حظرها بواسطة مجالات BlackList. إذا قمت بإضافة أي مجال إلى Global-BlackList/Global-Whitelist، فإنه يدخل حيز التنفيذ على الفور دون الحاجة إلى تطبيق السياسة.

من أجل إضافة عنوان IP إلى Global-BlackList/ Global-Whitelist، انتقل إلى **المراقبة > ASA FirePOWER Monitoring > Real Time Eventing**، قم بتحريك الماوس في أحداث الاتصال وحدد **عرض التفاصيل**.

يمكنك إضافة مجالات إلى Global-BlackList/Global-Whitelist. انقر فوق **تحرير** في قسم DNS وحدد **طلبات DNS للمجال الآن/BlackList طلبات WhiteList DNS للمجال الآن** لإضافة المجال إلى القائمة المقابلة، كما هو موضح في الصورة.



للتحقق من إضافة المجالات إلى القائمة السوداء العالمية/ القائمة البيضاء العالمية، انتقل إلى **التكوين > تكوين ASA FirePOWER > إدارة الكائنات > الأمان** Intelligence **> قوائم DNS** وموجز ويب **القائمة السوداء العالمية ل DNS / القائمة البيضاء العالمية ل DNS**.

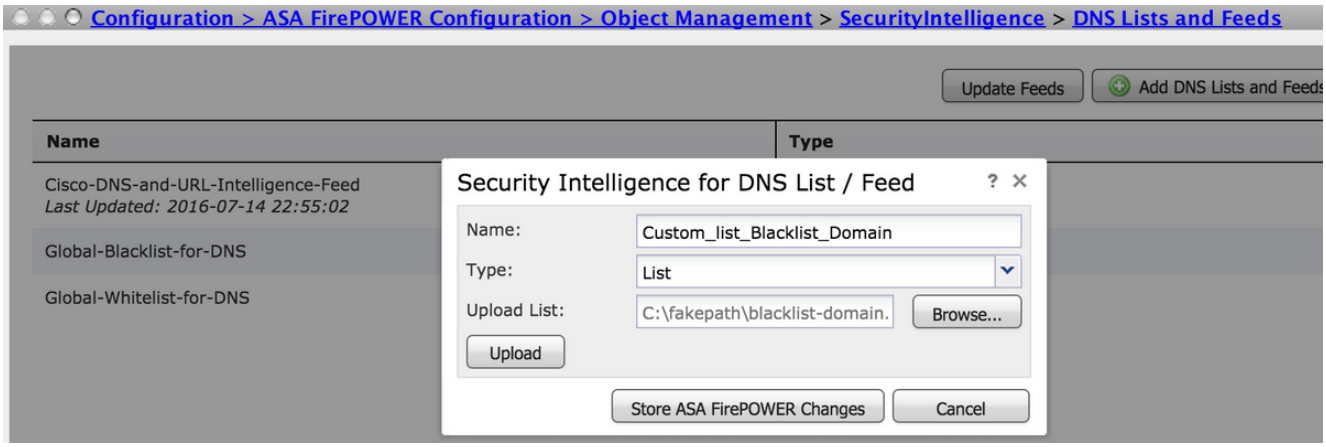
يمكنك أيضا إستخدام زر الحذف لإزالة أي مجال من القائمة.

إنشاء قائمة مخصصة بمجالات القائمة السوداء

يسمح لك Firepower بإنشاء قائمة مجالات مخصصة يمكن إستخدامها للقائمة السوداء (الحظر) باستخدام طريقتين مختلفتين.

1. يمكنك كتابة أسماء المجالات إلى ملف نصي (مجال واحد لكل سطر) وتحميل الملف إلى وحدة FirePOWER النمطية.

   لتحميل الملف، انتقل إلى **التكوين > تكوين ASA FirePOWER > إدارة الكائن > SecurityIntelligence > قوائم DNS وموجز الويب** ثم حدد **إضافة قوائم DNS وموجز ويب**
   الاسم: حدد اسم القائمة المخصصة. **النوع:** تحديد **القائمة** من القائمة المنسدلة. **قائمة التحميل:** أختر **إستعراض** لتحديد موقع الملف النصي في نظامك. حدد **تحميل** لتحميل الملف.



   انقر فوق **تخزين تغييرات FirePOWER ل ASA** لحفظ التغييرات.

2. يمكنك إستخدام أي مجالات لجهة خارجية للقائمة المخصصة التي يمكن لوحدة FirePOWER النمطية الاتصال بها بخادم جهة خارجية لجلب قائمة المجالات.

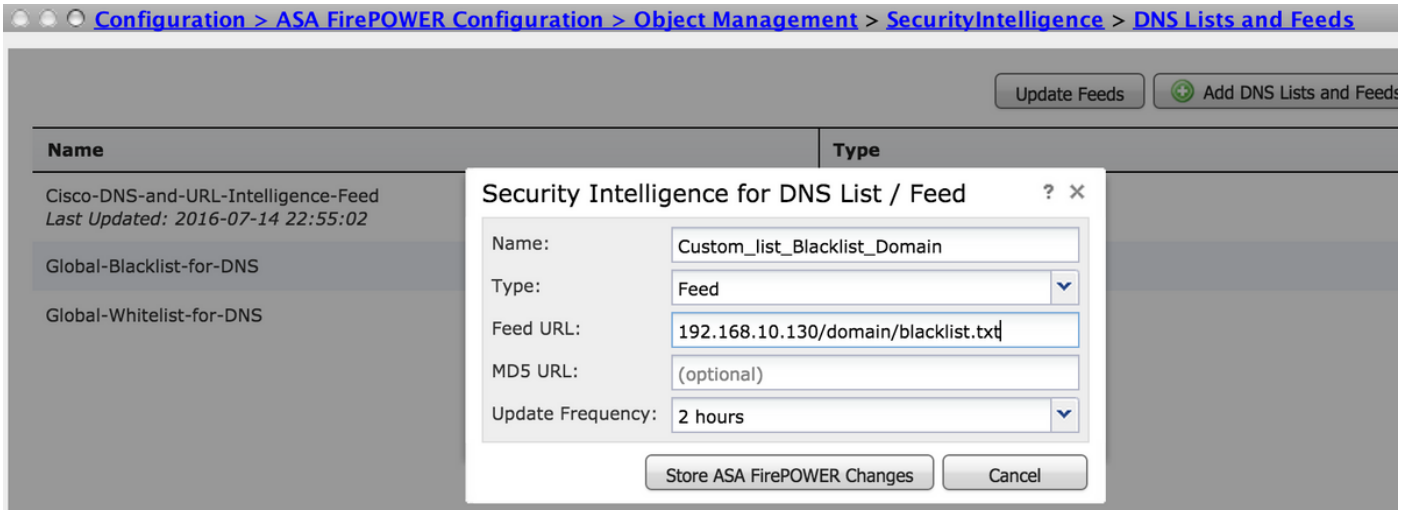
   ومن أجل تكوين هذا، انتقل إلى **التكوين > ASA FirePOWER Configuration > إدارة الكائن > ذكاء الأمان > قوائم DNS وموجز الويب** ثم حدد **إضافة قوائم DNS وموجز ويب**
   الاسم: حدد اسم موجز ويب المخصص.

   النوع: حدد **موجز الويب** من القائمة المنسدلة.

   URL موجز الويب: حدد عنوان URL الخاص بالخادم الذي يمكن للوحدة النمطية FirePOWER الاتصال به وتنزيله.

   عنوان URL ل MD5: حدد قيمة التجزئة للتحقق من مسار عنوان URL للموجز.

   تكرار التحديث: حدد الفاصل الزمني الذي تتصل فيه الوحدة النمطية بخادم موجز ويب URL.



حدد **تغييرات FirePOWER** الخاصة **بتخزين ASA** لحفظ التغييرات.

الخطوة 2. تكوين كائن StackSlot (إختياري).

يمكن إستخدام عنوان IP للفتحة كإستجابة لطلب DNS ضار. يحصل جهاز العميل على عنوان IP الخاص بخادم Sinkslot للبحث عن المجال الضار ويحاول الجهاز الطرفي الاتصال بخادم Sinkslot. وبالتالي، يمكن ان تكون هذه الحفرة نقطة عسل للتحقيق في حركة مرور الهجمات. يمكن تكوين الثقب السفلي لتشغيل مؤشر التسوية (IOC).

لإضافة الخادم الذي يعمل عبر فتحة واحدة، **التكوين > ASA FirePOWER Configuration > Object Management (إدارة الكائنات) > Sinkhole** وانقر فوق خيار **إضافة فتحة تخزين**.

الاسم: حدد اسم خادم Sinkhole.

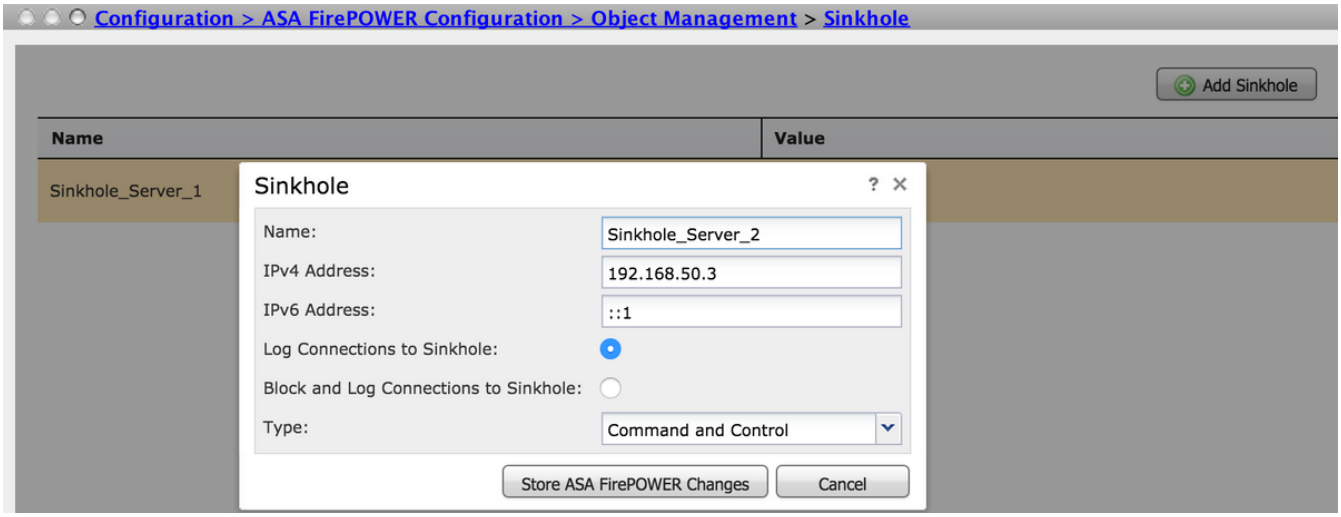
عنوان IP: حدد عنوان IP الخاص بخادم Sinkhole.

تسجيل الاتصالات ب Sinkhole: تمكين هذا الخيار لتسجيل كل الاتصالات بين نقطة النهاية وخادم Sinkhole.

منع الاتصالات وتسجيلها إلى Sinkhole: تمكين هذا الخيار لحظر الاتصال وتسجيل فقط في بداية اتصال التدفق. إن ال يكون هناك طبيعي ثقب ناد، أنت يستطيع عينت أي عنوان وأنت يستطيع رأيت التوصيل حاد و مشغل IOC.

الكتابة: حدد موجز الويب من القائمة المنسدلة التي تريد تحديد نوع IOC (مؤشر التسوية) المرتبط بأحداث ثقب البالوعة. هناك ثلاثة أنواع من الثقب البرمجي يمكن تمييزها.

- برمجيات خبيثة
- القيادة والسيطرة
- فيش



الخطوة 3. تكوين نهج DNS.

يجب تكوين نهج DNS لتحديد الإجراء الخاص بقائمة/موجز وبي DNS. انتقل إلى **التكوين > تكوين ASA FirePOWER > السياسات > سياسة DNS.**

يحتوي نهج DNS الافتراضي على قاعدتين افتراضيتين. تحتوي القاعدة الأولى، **Global Whitelist for DNS**، على القائمة المخصصة للمجال المسموح به (**Global-Whitelist-for-DNS**). توجد هذه القاعدة في الأعلى لمطابقتها أولا قبل أن يحاول النظام مطابقة أي مجال للقائمة السوداء. تحتوي القاعدة الثانية، **Global BlackList for DNS**، على القائمة المخصصة للمجال المحظور (**Global-Blacklist for-DNS**).

يمكنك إضافة المزيد من القواعد لتعريف الإجراءات المختلفة **لقوائم المجال وموجز وبي الخاصين ب Cisco TALOS المتوفر**. لإضافة قاعدة جديدة، حدد **إضافة قاعدة DNS.**

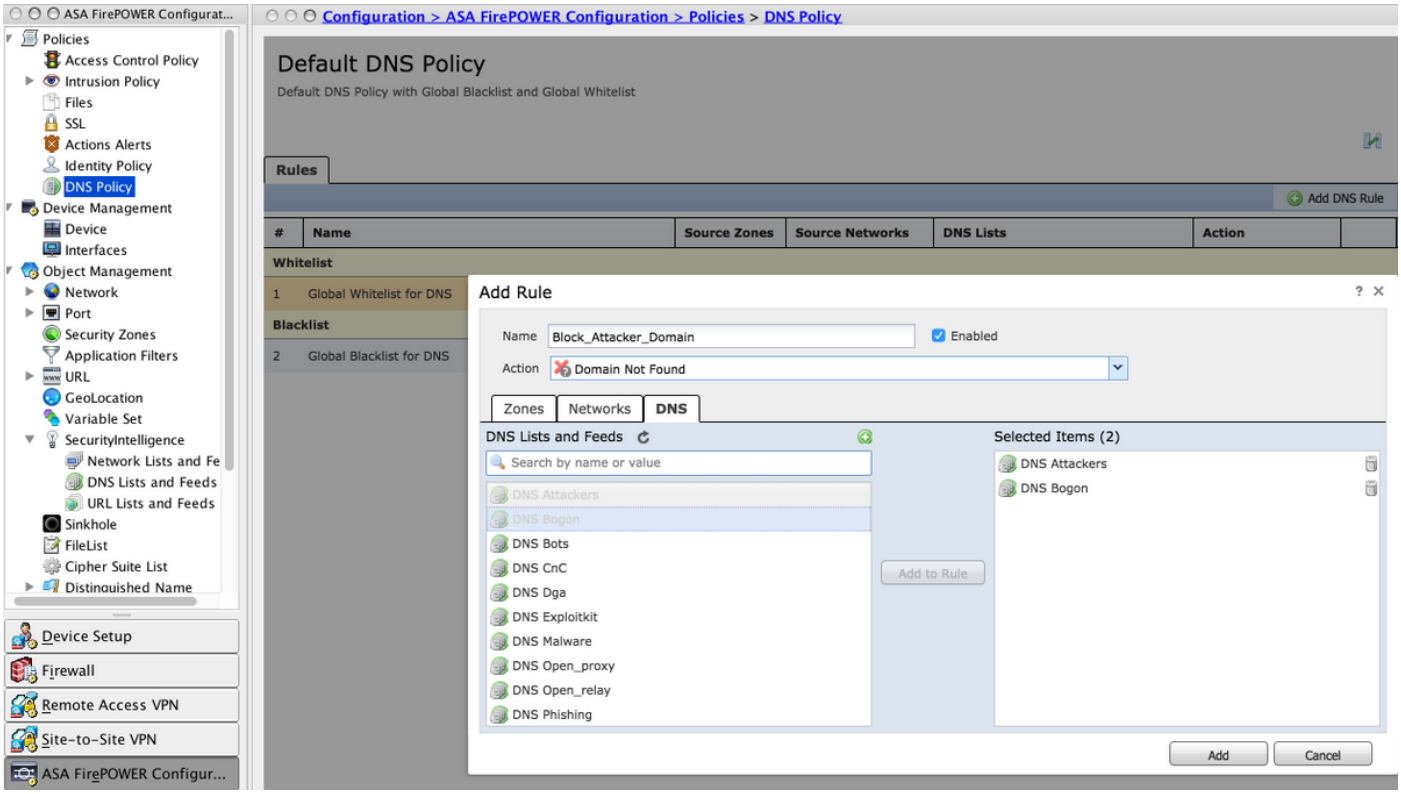
الاسم: حدد اسم القاعدة.

الإجراء: حدد الإجراء المطلوب تشغيله عند تطابق هذه القاعدة.

- **Whitelist:** يسمح هذا باستعلام DNS.
- **مدرب:** يقوم هذا الإجراء بإنشاء الحدث لاستعلام DNS وتستمر حركة المرور في مطابقة القواعد التالية.
- **لم يتم العثور على المجال:** يرسل هذا الإجراء إستجابة DNS نظرا لعدم العثور على المجال (مجال غير موجود).
- **drop:** يقوم هذا الإجراء بحظر استعلام DNS وإسقاطه بصمت.
- **Sinkhole:** يرسل هذا الإجراء عنوان IP الخاص بخادم Sinkhole كاستجابة لطلب DNS.

حدد **المناطق/ الشبكة** لتحديد شروط القاعدة. في علامة التبويب DNS، أختر **قوائم DNS وموجز الويب** وانتقل إلى خيار **العناصر المحددة** حيث يمكنك تطبيق الإجراء الذي تم تكوينه.

يمكنك تكوين قواعد DNS المتعددة لقوائم DNS المختلفة وموجز وبي بإجراء مختلف استنادا إلى إحتياجات مؤسستك.

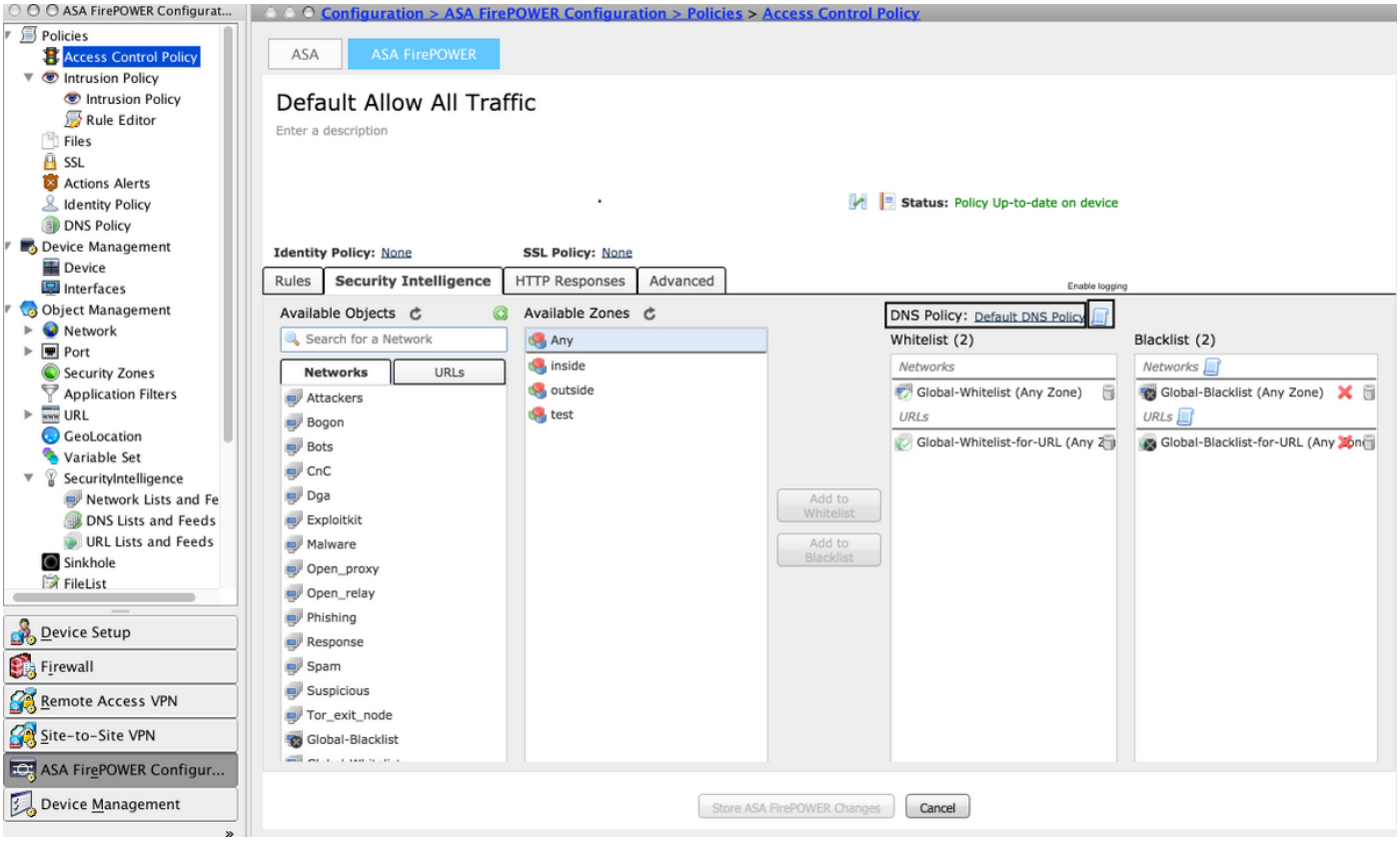


انقر فوق الخيار **إضافة** لإضافة القاعدة.

الخطوة 4. تكوين نهج التحكم في الوصول.

لتكوين معلومات الأمان المستندة إلى DNS، انتقل إلى **التكوين > ASA Firepower Configuration > السياسات > سياسة التحكم في الوصول**، حدد علامة التبويب **معلومات الأمان**.

تأكد من تكوين نهج DNS واختياريا، يمكنك تمكين السجلات عند النقر فوق رمز السجلات كما هو موضح في الصورة.



أختر خيار **تخزين تغييرات ASA FirePOWER** لحفظ تغييرات سياسة التيار المتردد.

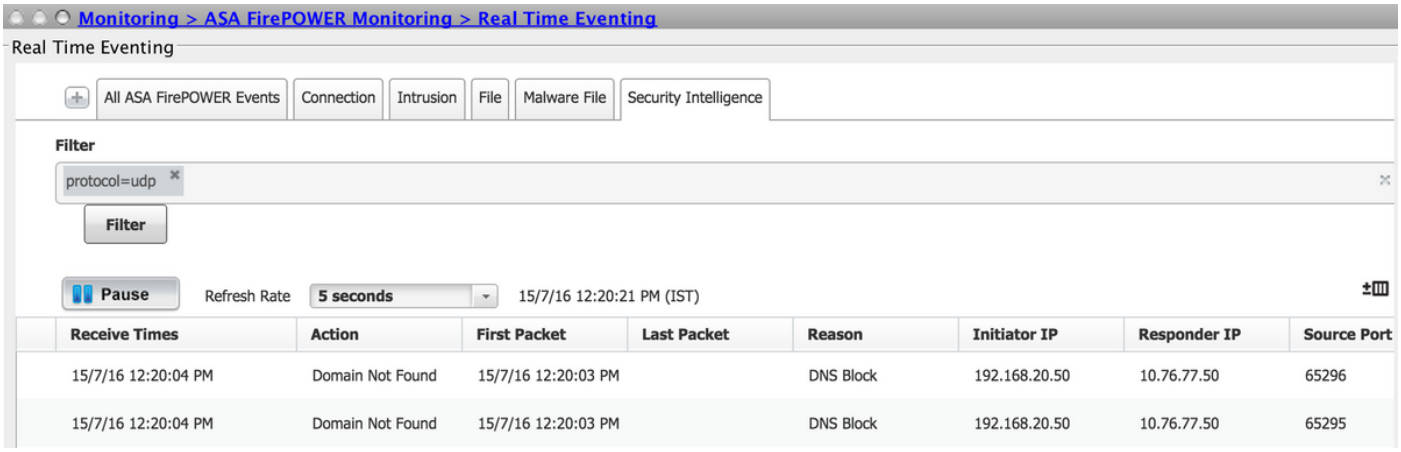
الخطوة 5. سياسة التحكم بالوصول إلى النشر.

لكي تصبح التغييرات سارية المفعول، يجب نشر نهج التحكم بالوصول. قبل تطبيق النهج، راجع الإشارة إلى ما إذا كان نهج التحكم في الوصول غير محدث على الجهاز أم لا.

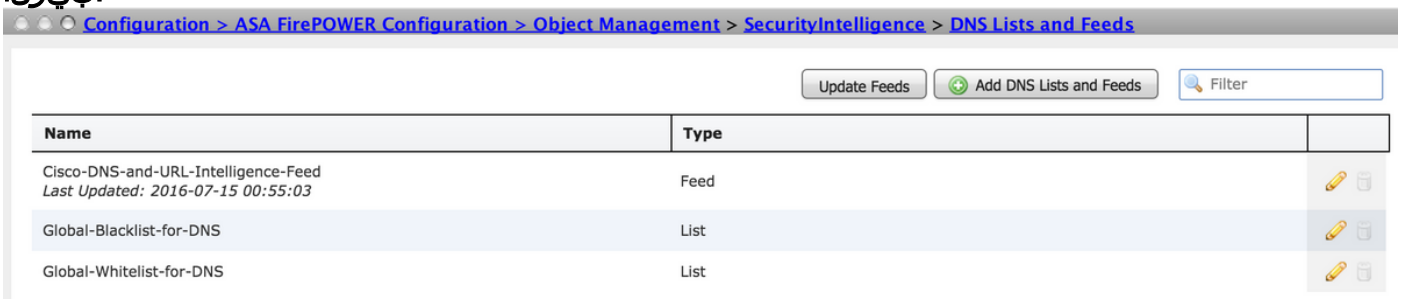
لنشر التغييرات على المستشعر، انقر فوق **نشر** واختر **نشر تغييرات FirePOWER** ثم حدد **نشر** في النافذة المنبثقة لنشر التغييرات.

> **ملاحظة**: في الإصدار 5.4.x، لتطبيق سياسة الوصول على المستشعر، يلزمك النقر فوق **تطبيق تغييرات ASA FirePOWER**.

ملاحظة: انتقل إلى المراقبة > مراقبة ASA FirePOWER > حالة المهمة. تأكد من اكتمال المهمة لتأكيد تغييرات التكوين. التحقق من الصحة يمكن التحقق من التكوين فقط في حالة تشغيل حدث. لذا، يمكنك فرض استعلام DNS على جهاز. ومع ذلك، كن حذرا من التداعيات عند استهداف خادم ضار معروف. بعد أن تقوم بإنشاء هذا الاستعلام، يمكنك رؤية الحدث في قسم تصحيح الوقت الحقيقي.مراقبة حدث ذكاء أمان DNS لمشاهدة ذكاء الأمان بواسطة وحدة FirePOWER، انتقل إلى المراقبة > مراقبة ASA FirePOWER > التدقيق في الوقت الفعلي. حدد علامة التبويب معلومات الأمان. هذا يظهر الأحداث كما هو موضح في
الصورة:



استكشاف الأخطاء وإصلاحهاوفر هذا القسم المعلومات التي يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.لضمان أن تلقيمات معلومات الأمان الذكية محدثة، انتقل إلى التكوين > تكوين ASA FirePOWER > إدارة الكائن > ذكاء الأمان > قوائم DNS وموجز الويب وحدد الوقت الذي تم فيه تحديث موجز الويب آخر مرة. يمكنك إختيار Edit (تحرير) لتعيين تكرار تحديث موجز الويب.



تأكد من اكتمال نشر نهج التحكم بالوصول بنجاح. راقبت عالمة التبويب تصحيح الوقت الحقيقي لإستخبارات الأمان لمعرفة ما إذا تم حظر حركة المرور أم لا.

معلومات ذات صلة

- دليل البدء السريع للوحدة النمطية Cisco ASA FirePOWER Module
- الدعم التقني والمستندات - Cisco Systems

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).