مادختساب SSL صحف ةسايس نيوكت Cisco نم FireSIGHT

المحتويات

المقدمة

تتيح لك ميزة فحص SSL إما حظر حركة المرور المشفرة دون فحصها، أو فحص حركة المرور المشفرة أو التي تم فك تشفيرها باستخدام التحكم في الوصول. يصف هذا المستند خطوات التكوين لإعداد سياسة فحص SSL على نظام FireSIGHT من Cisco.

المتطلبات الأساسية

المكونات المستخدمة

- Cisco FireSIGHT Management Center
- أجهزة Cisco Firepower 7000 أو 8000
- برنامج الإصدار 5.4.1 أو أعلى

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.

تحذير: إذا قمت بتطبيق سياسة فحص SSL على الجهاز الذي تتم إدارته، فقد تؤثر على أداء الشبكة.

التكوينات

يمكنك تكوين سياسة فحص SSL لفك تشفير حركة مرور الطرق التالية:

1. فك التشفير والاستقالة:

- الخيار 1: إستخدام FireSIGHT Center كمرجع شهادات جذر (CA)، أو
- الخيار 2: الحصول على مرجع مصدق داخلي لتوقيع الشهادة، أو
- الخيار 3: إستيراد شهادة ومفتاح مرجع مصدق

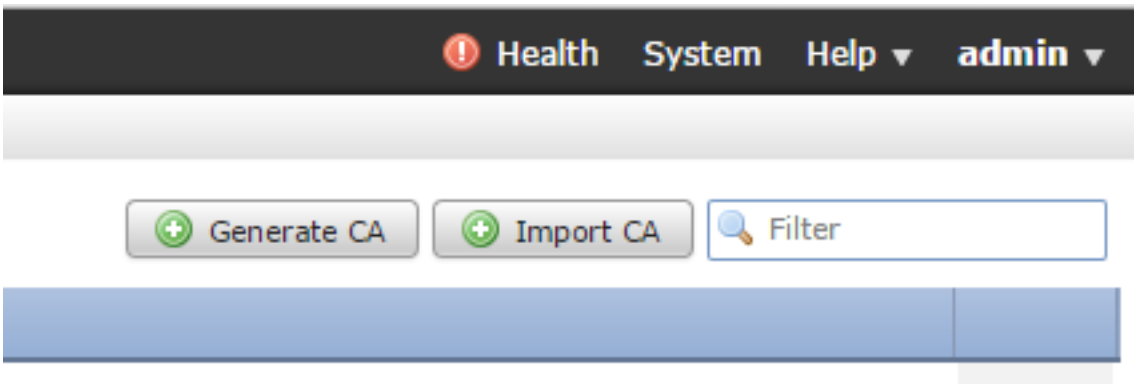
2. فك التشفير باستخدام النتيجة المعروفة:

- قم بتسجيل الدخول إلى FireSIGHT Management Center، ثم انتقل إلى **Objects**.
- في صفحة **الكائنات**، قم بتوسيع **PKI** وحدد **المراجع المصدقة الداخلية**.

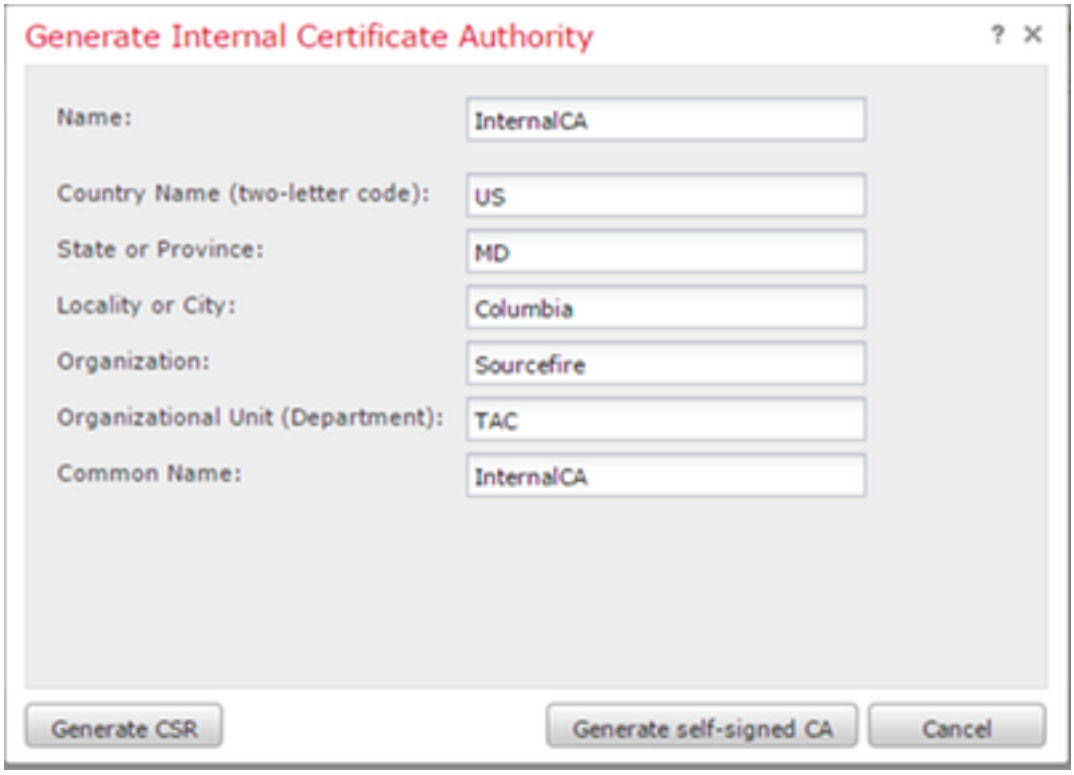
1. فك التشفير والاستقالة

الخيار 1: إستخدام FireSIGHT Center كمرجع شهادات جذر (CA)

ط. انقر على **إنشاء مرجع مصدق**.



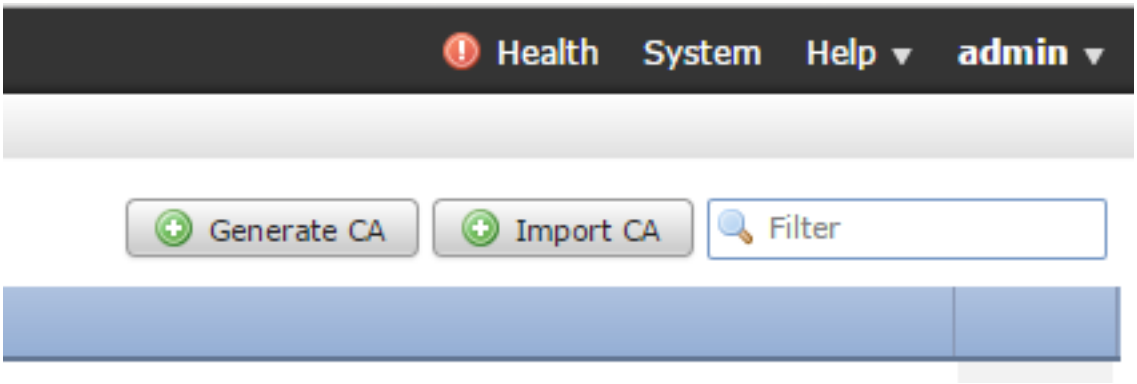
ثانيا - تعبئة المعلومات ذات الصلة



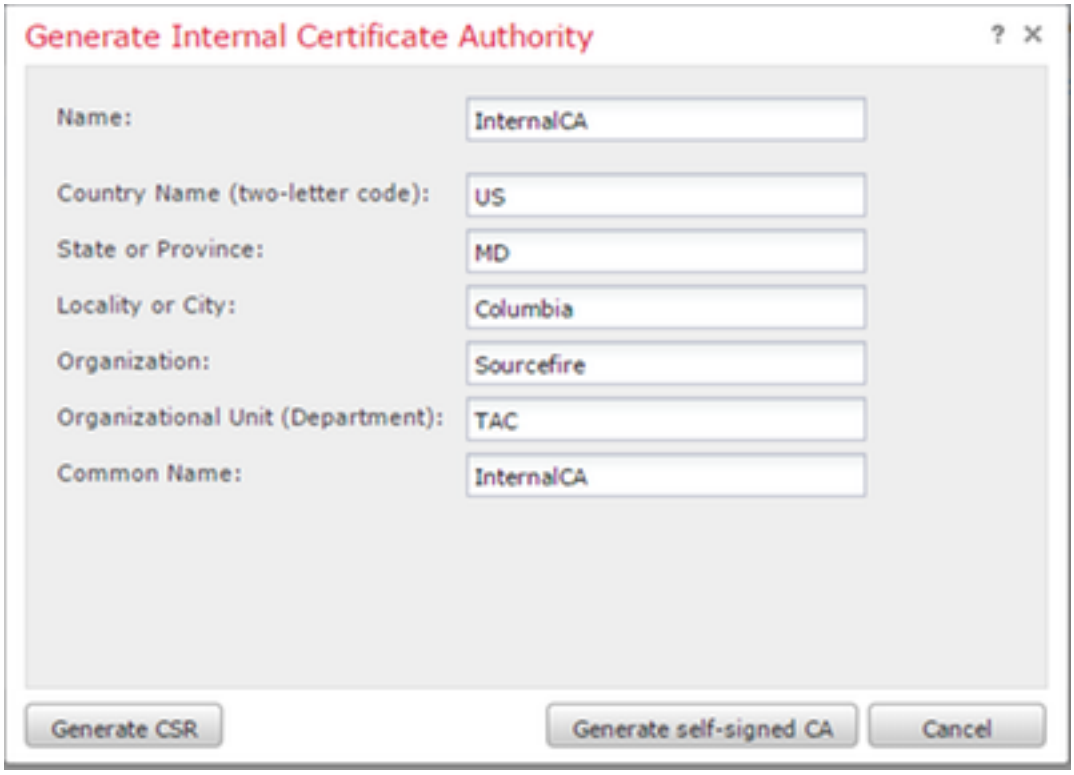
iii. انقر فوق **إنشاء CA الموقع ذاتيا**.

الخيار 2: الحصول على مرجع مصدق داخلي لتوقيع شهادتك

انقر فوق **إنشاء المرجع المصدق**.

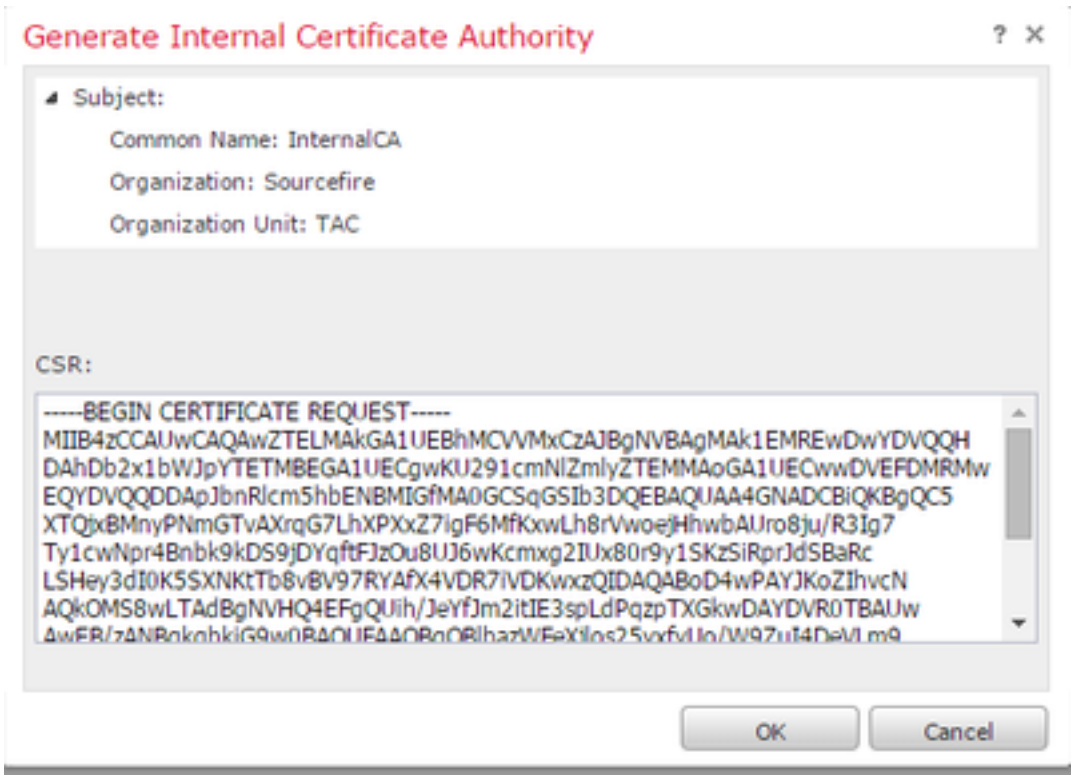


ثانيا - تعبئة المعلومات ذات الصلة.



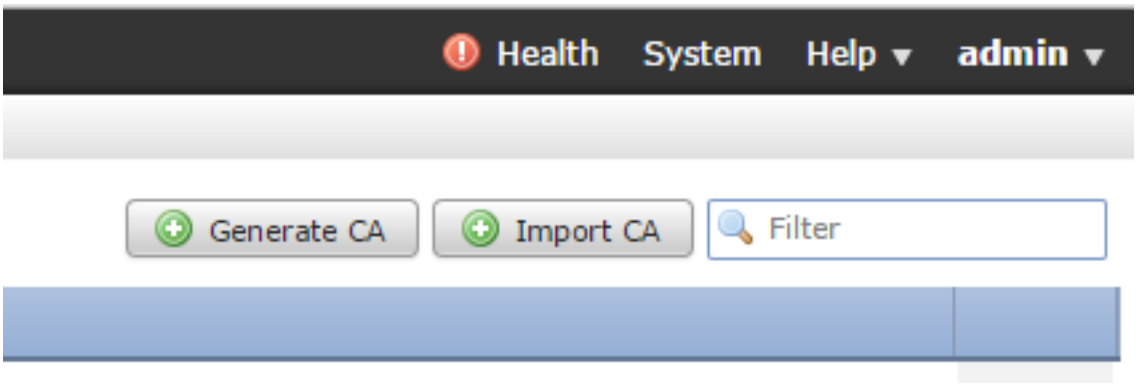
ملاحظة:قد تحتاج للاتصال بمسؤول المرجع المصدق لتحديد ما إذا كان لديهم قالب لطلب التوقيع.

iii. انسخ الشهادة بأكملها بما في ذلك —بدء طلب الشهادة - و— إنهاء طلب الشهادة- ثم احفظه في ملف نصي بامتداد .req.



ملاحظة: طلب مسؤول المرجع المصدق ملحقا آخر غير .req.

الخيار 3: إستيراد شهادة ومفتاح مرجع مصدق

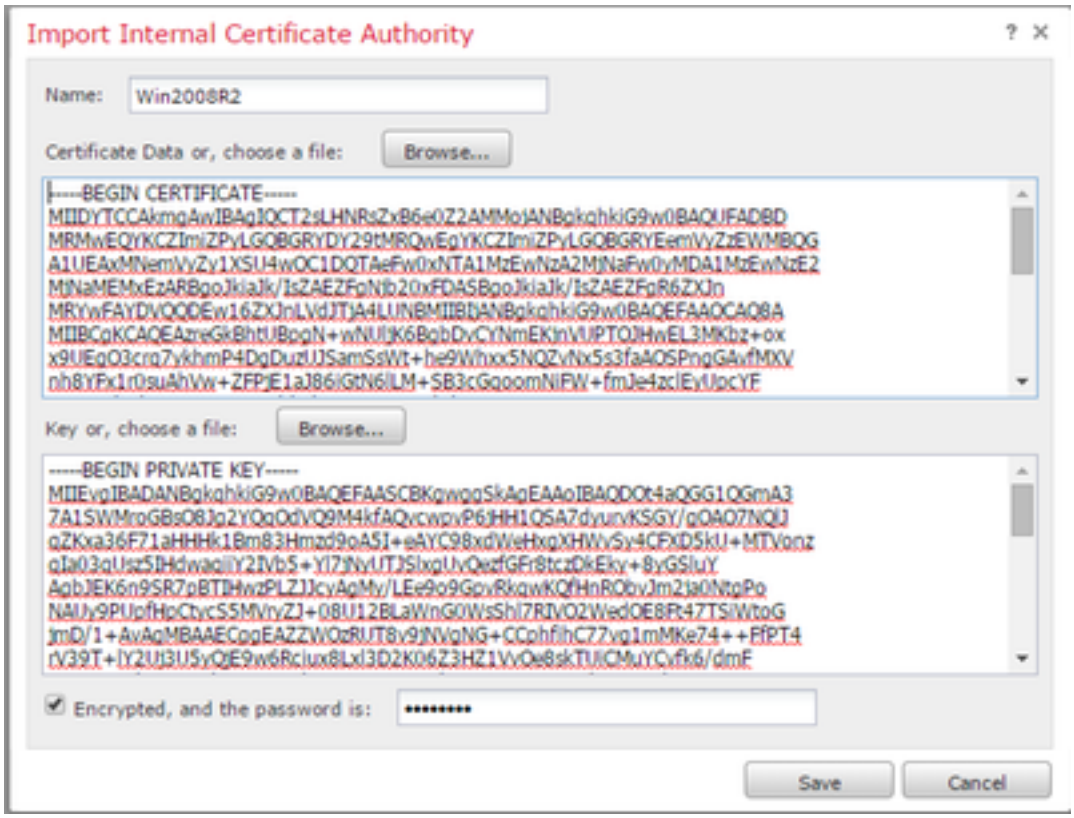


طقطقة **إستيراد مرجع مصدق**.

ii. تصفح إلى أو لصق في الشهادة.

iii. تصفح إلى المفتاح الخاص أو لصق فيه.

iv. حدد المربع المشفر واكتب في كلمة مرور.



ملاحظة: إذا لم تكن هناك كلمة مرور، فتحقق من المربع المشفر واتركه فارغا.

2. فك التشفير باستخدام مفتاح معروف

إستيراد الشهادة المعروفة (بديل عن إلغاء التشفير والاستقالة)

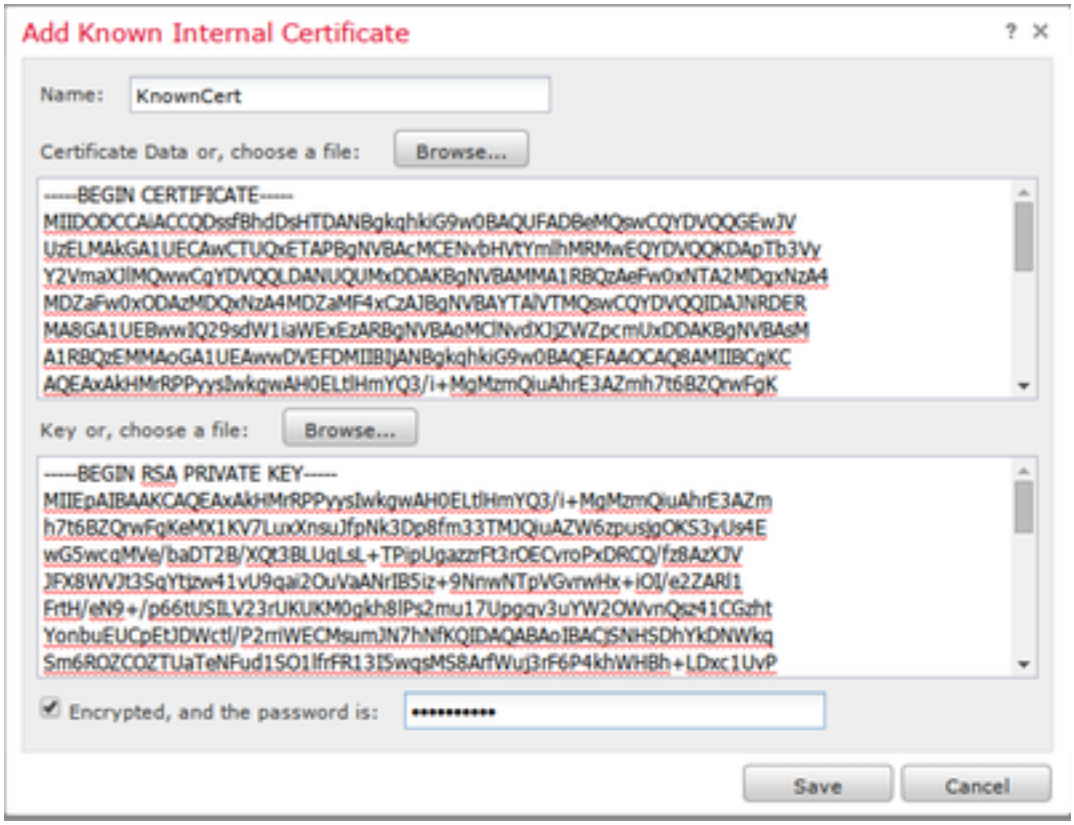
من صفحة الكائنات الموجودة على اليسار قم بتوسيع PKI وحدد النتائج الداخلية.

2. انقر فوق **إضافة شهادة داخلية**.

iii. تصفح إلى أو لصق في الشهادة.

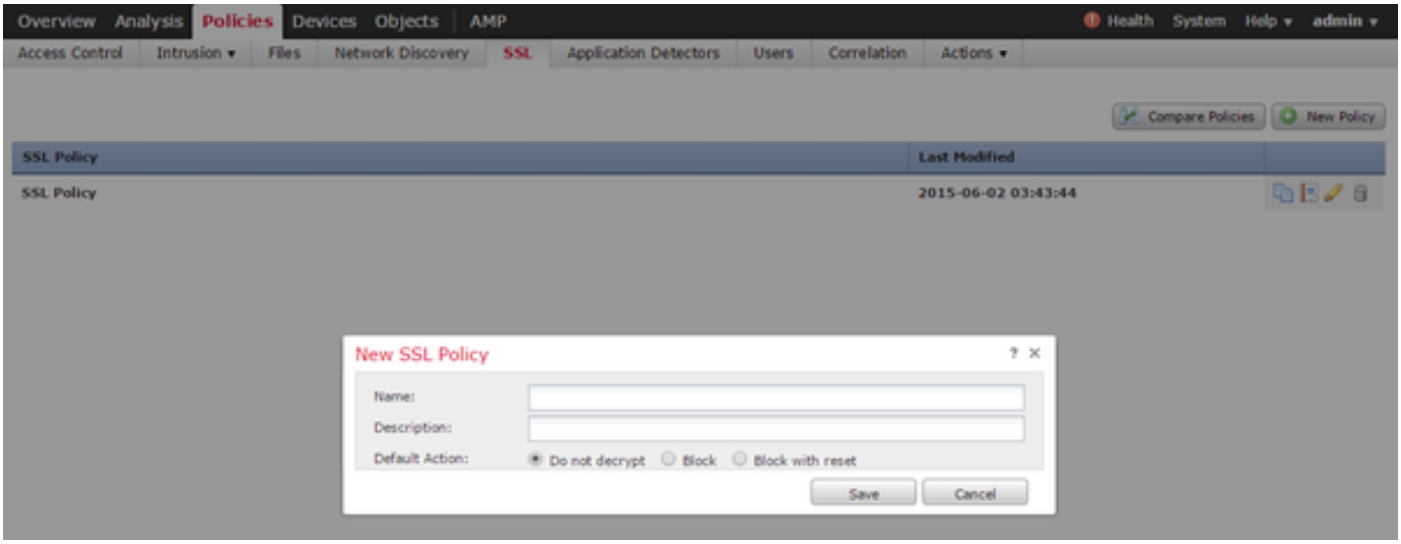
iv. تصفح إلى أو لصق في المفتاح الخاص.

v. حدد المربع **المشفر** واكتب كلمة مرور.



ملاحظة: إذا لم تكن هناك كلمة مرور، أترك المربع **المشفر** فارغا.

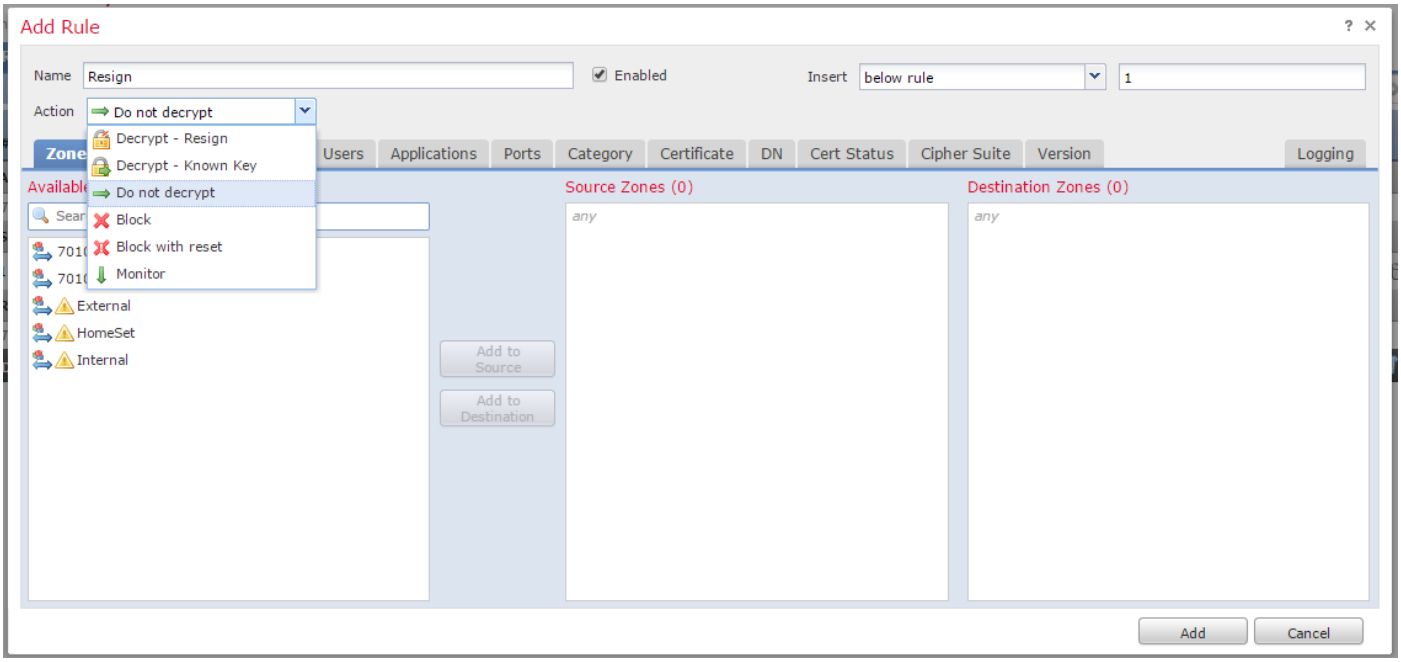
4. انتقل إلى **السياسات > SSL** ثم انقر فوق **نهج جديد**.



5. قم بتوفير اسم وحدد **إجراء افتراضي**. تظهر صفحة محرر نهج SSL. تعمل صفحة محرر نهج SSL نفس صفحة محرر نهج التحكم بالوصول.

ملاحظة: إذا لم تكن متأكدا من **الإجراء الافتراضي، لا تقم بفك التشفير** هي نقطة البدء الموصى بها.

6. في صفحة محرر نهج SSL، انقر فوق **إضافة قاعدة**. في نافذة إضافة قاعدة، قم بتوفير اسم للقاعدة، وقم بتعبئة كافة المعلومات الأخرى ذات الصلة.



يصف القسم التالي خيارات مختلفة في نافذة **إضافة قاعدة**:

الإجراء

فك التشفير - الاستقالة

- يعمل المستشعر كرجل في الوسط (MitM) ويقبل الاتصال بالمستخدم، ثم ينشئ اتصالا جديدا بالخادم. على سبيل المثال: أنواع المستخدمين في https://www.facebook.com في متصفح. تصل حركة المرور إلى المستشعر، ثم يقوم المستشعر بالتفاوض مع المستخدم باستخدام شهادة CA المحددة ويتم بناء نفق SSL A. في الوقت نفسه، يتصل المستشعر ب https://www.facebook.com وينشئ نفق SSL B.
- النتيجة النهائية: يرى المستخدم الشهادة في القاعدة، وليس في فيسبوك.
- يتطلب هذا الإجراء مرجع مصدق داخلي. حدد إستبدال المفتاح إذا كنت تريد إستبدال المفتاح. سيستلم المستخدم الشهادة التي تحددها.

ملاحظة: لا يمكن إستخدام هذا في الوضع الخامل.

فك التشفير - مفتاح معروف

- يحتوي المستشعر على المفتاح الذي سيتم إستخدامه لفك تشفير حركة المرور. على سبيل المثال: أنواع المستخدمين في https://www.facebook.com في متصفح. تصل حركة المرور إلى المستشعر، يقوم المستشعر بفك تشفير حركة المرور، ثم يفحص حركة المرور.
- النتيجة النهائية: يرى المستخدم شهادة Facebook
- يتطلب هذا الإجراء شهادة داخلية. هذا أضفت في **كائن>PKI> داخلي مصدر**.

ملاحظة: يجب أن تكون مؤسستك مالكة المجال والشهادة. على سبيل المثال، facebook.com ستكون الطريقة الوحيدة الممكنة لجعل المستخدم النهائي يشاهد شهادة Facebook هي إذا كنت تملك المجال فعليا facebook.com (أي أن شركتك هي Facebook، Inc) ولديك ملكية الشهادة facebook.com الموقعة من قبل مرجع مصدق عام. يمكنك فقط فك التشفير باستخدام المفاتيح المعروفة للمواقع التي تمتلكها مؤسستك.

الغرض الأساسي من فك تشفير المفتاح المعروف هو فك تشفير حركة مرور البيانات المتجهة إلى خادم HTTPS لحماية خوادمك من الهجمات الخارجية. لفحص حركة مرور العميل الجانبية إلى مواقع HTTPS الخارجية، سيتم إستخدام "فك تشفير" للاستقالة نظرا لأنك لا تمتلك الخادم ولأنك مهتم بفحص حركة مرور العميل في شبكتك المتصلة بمواقع مشفرة خارجية.

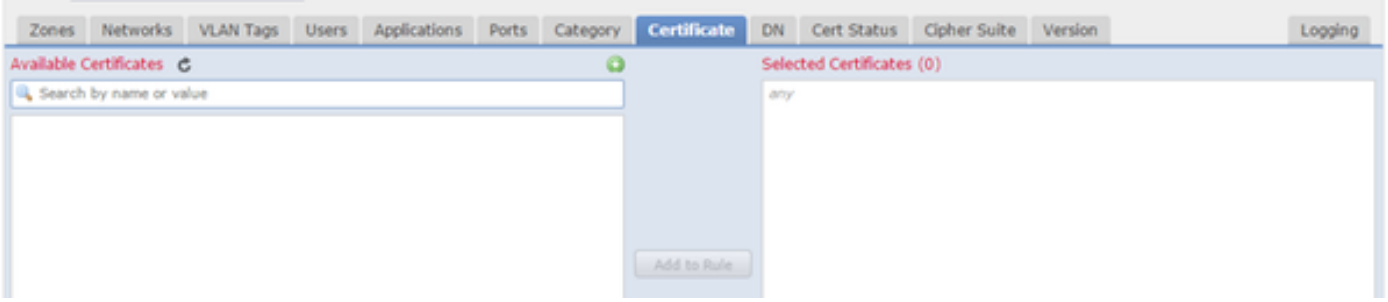
ملاحظة: لكي يقوم DHE و ECDHE بفك الترميز يجب أن نكون في الخط.

عدم فك التشفير

تتجاوز حركة المرور سياسة SSL وتستمر في اتباع نهج التحكم في الوصول.

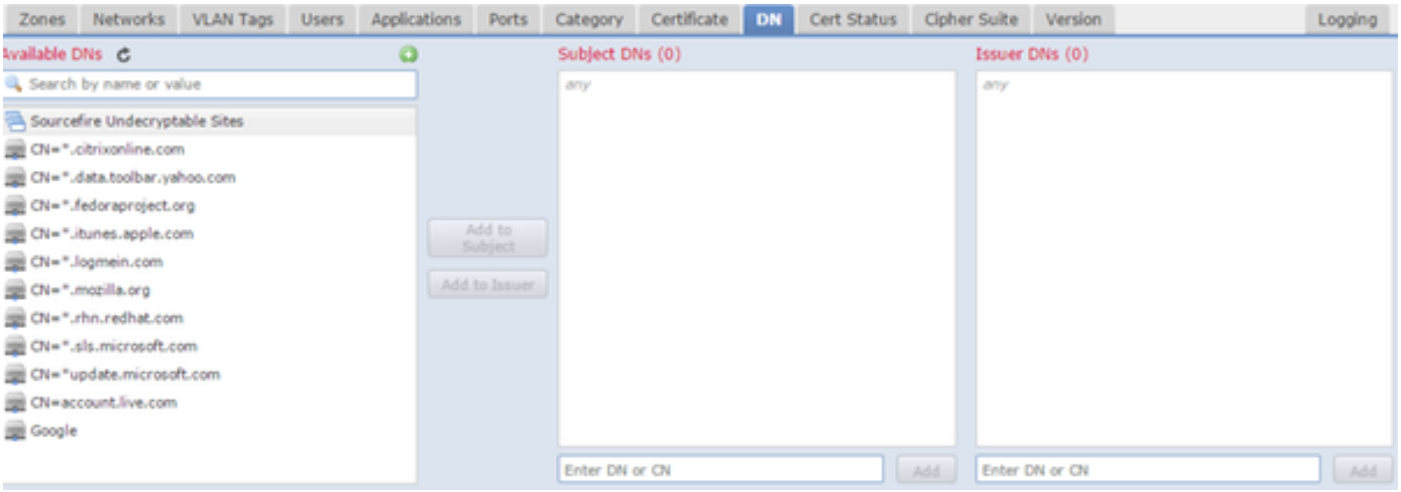
شهادة

تطابق القاعدة حركة مرور SSL باستخدام هذه الشهادة المحددة.



DN

تطابق القاعدة حركة مرور SSL باستخدام أسماء مجالات معينة في الشهادات.

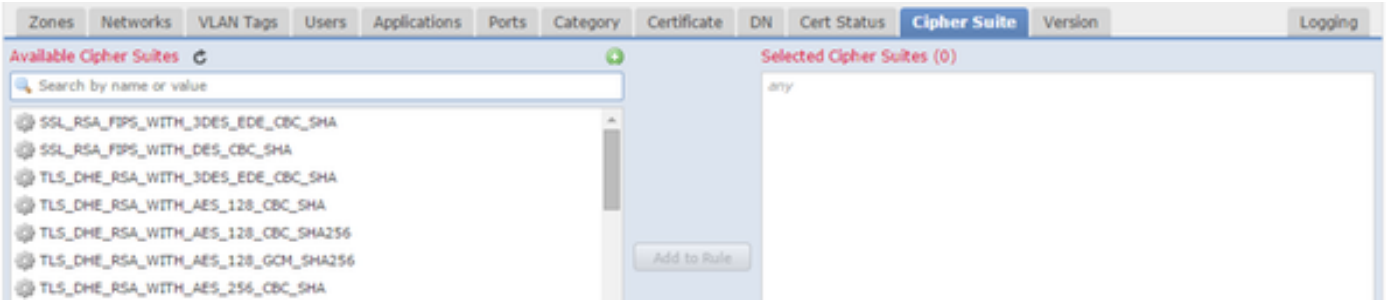


حالة CERT

تطابق القاعدة حركة مرور SSL مع حالات الشهادات هذه.

شفرة

تطابق القاعدة حركة مرور SSL باستخدام مجموعات التشفير هذه.



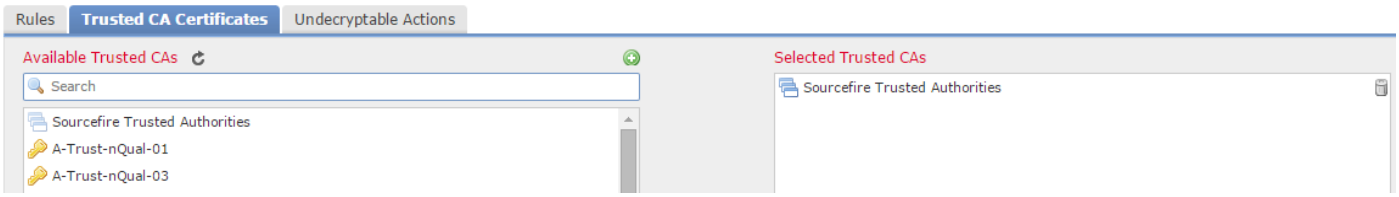
الإصدار

تنطبق القواعد فقط على حركة مرور SSL باستخدام الإصدارات المحددة من SSL.

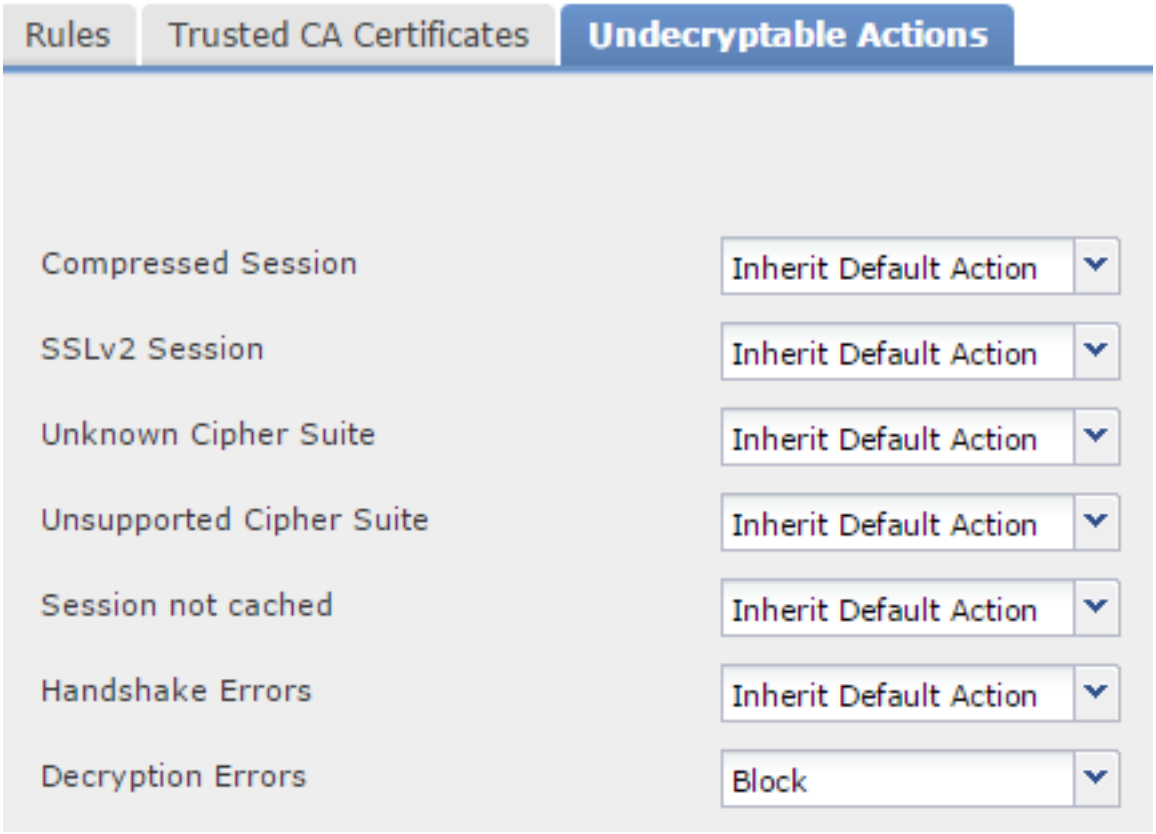
التسجيل

قم بتمكين التسجيل للاطلاع على أحداث الاتصال لحركة مرور SSL.

7. انقر على **شهادة مرجع مصدق ثقة**. هذا هو المكان الذي تتم فيه إضافة المرجع المصدق الموثوق به إلى النهج.



8. انقر فوق **إجراءات إلغاء التشفير**. فيما يلي الإجراءات التي لا يمكن للمستشعر فك تشفير حركة المرور من أجلها. يمكنك العثور على التعريفات من التعليمات عبر الإنترنت (**تعليمات > عبر الإنترنت**) الخاصة بمركز إدارة FireSIGHT.



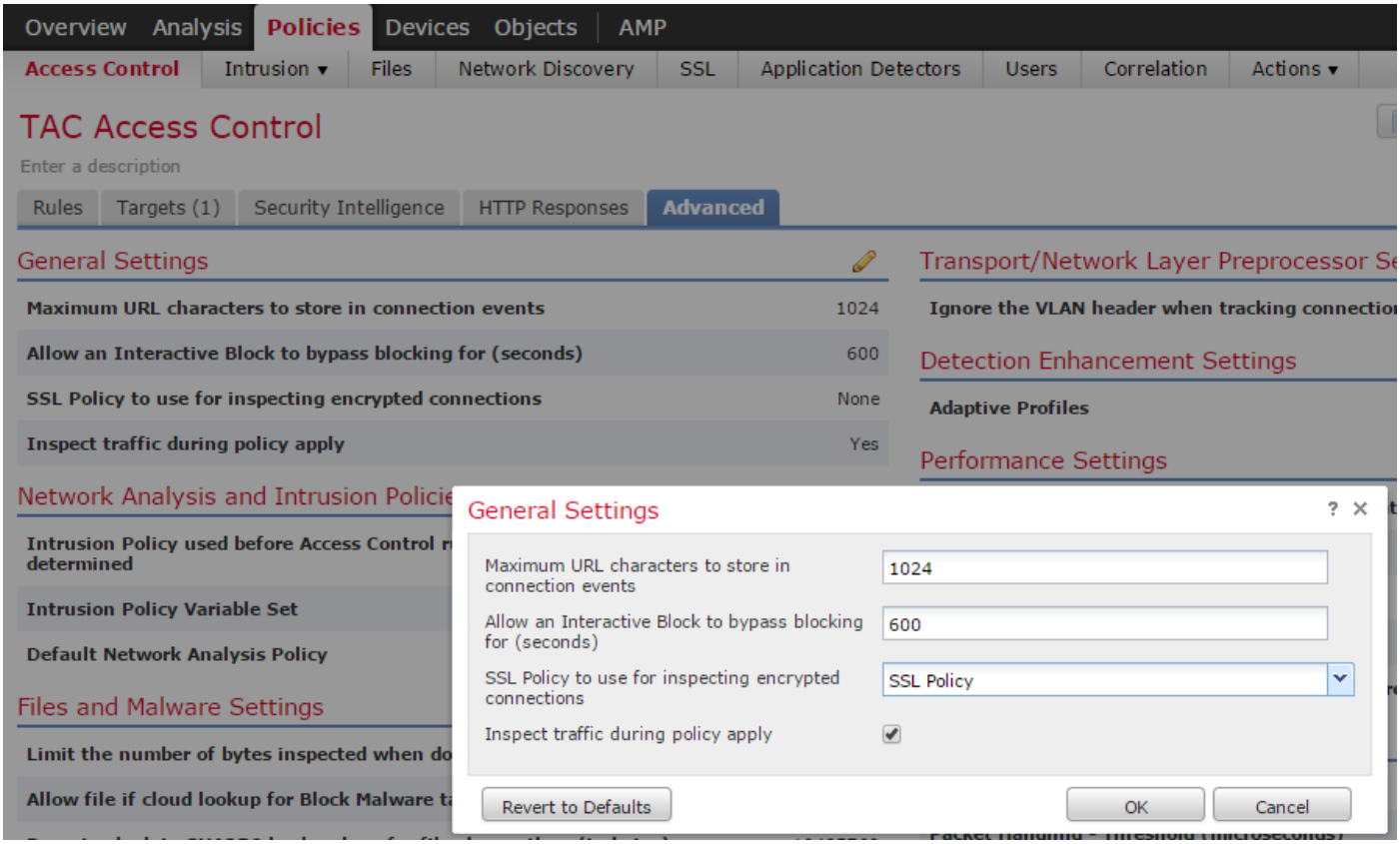
- **الجلسة المضغوطة**: تطبق جلسة SSL أسلوب ضغط بيانات.
- **جلسة SSLv2**: يتم تشفير الجلسة باستخدام SSL الإصدار 2. لاحظ أنه يمكن فك تشفير حركة المرور إذا كانت رسالة ترحيب العميل هي SSL 2.0، وكان المتبقي من حركة المرور المرسلة هو SSL 3.0.
- **مجموعة تشفير غير معروفة**: لا يتعرف النظام على مجموعة التشفير.
- **مجموعة تشفير غير مدعومة**: لا يدعم النظام فك التشفير استنادا إلى مجموعة التشفير المكتشفة.
- **جلسة العمل غير مخزنة مؤقتا**: جلسة عمل SSL بها إعادة إستخدام جلسة العمل الممكنة، وأعاد العميل والخادم تأسيس جلسة العمل بمعرف جلسة العمل، ولم يقم النظام بتخزين معرف جلسة العمل هذه مؤقتا.
- **أخطاء المصافحة**: حدث خطأ أثناء تفاوض مصافحة SSL.
- **أخطاء فك التشفير**: حدث خطأ أثناء فك تشفير حركة مرور البيانات.

ملاحظة: وترث هذه بشكل افتراضي الإجراء الافتراضي. إذا كان الإجراء الافتراضي هو "حظر"، فقد تواجه مشاكل غير متوقعة

9. قم بحفظ النهج.

10. انتقل إلى **السياسات > التحكم في الوصول**. قم بتحرير النهج أو إنشاء نهج جديد للتحكم في الوصول.

11. انقر على **متقدم** وحرر **الإعدادات العامة**.



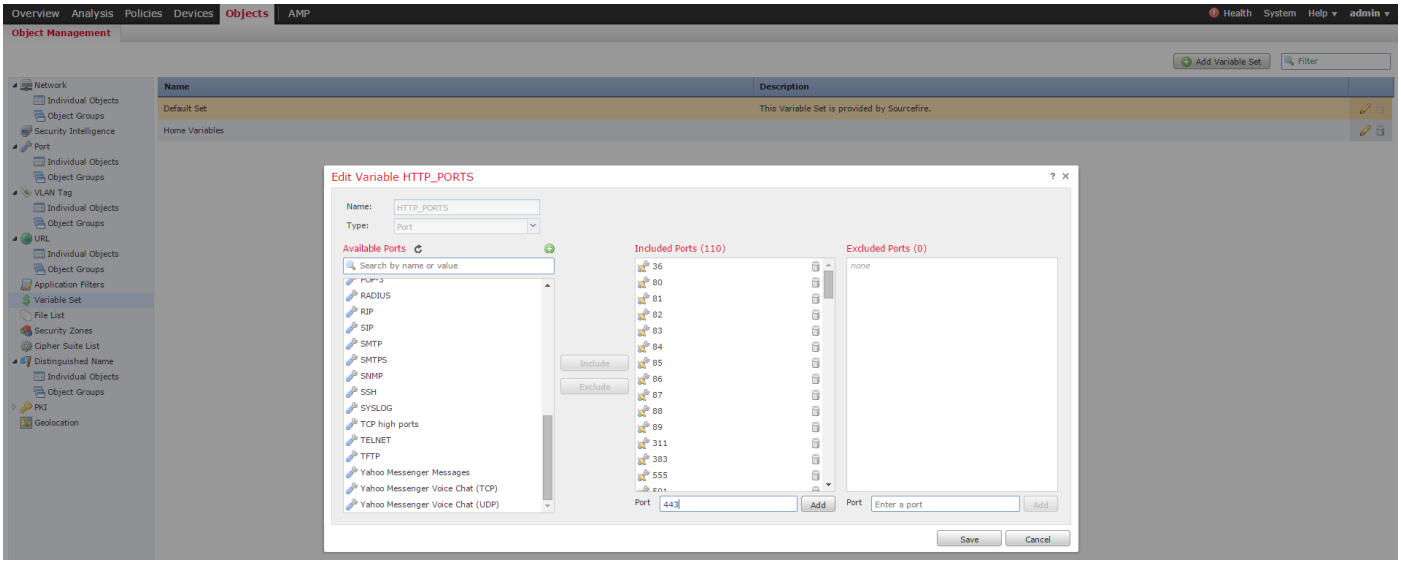
12. من القائمة المنسدلة، حدد **نهج SSL** الخاص بك.

13. انقر فوق **موافق**للحفظ.

تكوينات إضافية

يجب إجراء التغييرات التالية على سياسات الاقتحام من أجل تحديد الهوية بشكل صحيح:

i. يجب أن يتضمن متغير $HTTP_Ports المنفذ 443 وأي منافذ أخرى ذات حركة مرور https التي سيتم فك تشفيرها بواسطة النهج (**الكائنات > إدارة الكائن > مجموعة المتغيرات > تحرير**مجموعة المتغيرات).



ii. يجب أن يحتوي نهج تحليل الشبكة الذي يقوم بفحص حركة المرور المشفرة على المنفذ 443 (وأي منافذ أخرى مع حركة مرور https سيتم فك تشفيرها بواسطة النهج الخاص بك) مضمنة في حقل المنافذ لإعدادات معالج HTTP

المسبق وإلا فلن يتم نشر أي من قواعد HTTP مع معدلات محتوى http (أي http_uri وhttp_header وما إلى ذلك) نظرا لأن هذا يعتمد على منافذ HTTP المحددة ولن يتم نشر المخازن المؤقتة ل HTTP في الشورت لحركة المرور التي لا تتجاوز المنافذ المحددة.

iii. (إختياري ولكن موصى به لفحص أفضل) أضف منافذ HTTPS إلى إعدادات **تكوين تدفق TCP** في **حقل تنفيذ إعادة تجميع الدفق على كلا المنفذين**.

رابعا - إعادة تطبيق السياسة المنقحة لمراقبة الدخول خلال إطار صيانة مجدول.

تحذير: يمكن أن يتسبب هذا النهج المعدل في مشاكل أداء مهمة. يجب إختبار هذا الأمر خارج ساعات الإنتاج لتقليل مخاطر انقطاع الشبكة أو تشغيلها.

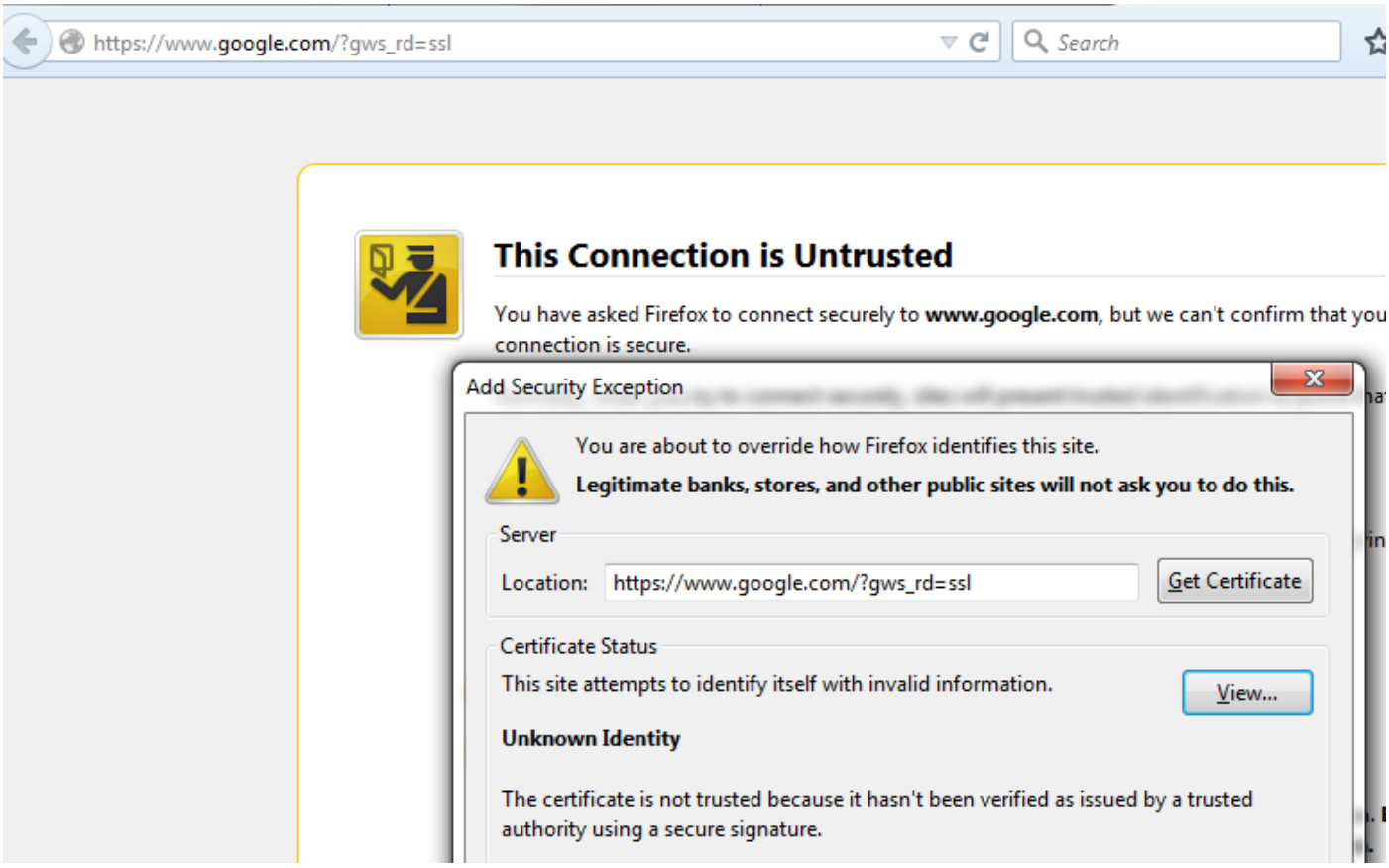
التحقق

فك التشفير - الاستقالة

1. افتح مستعرض ويب.

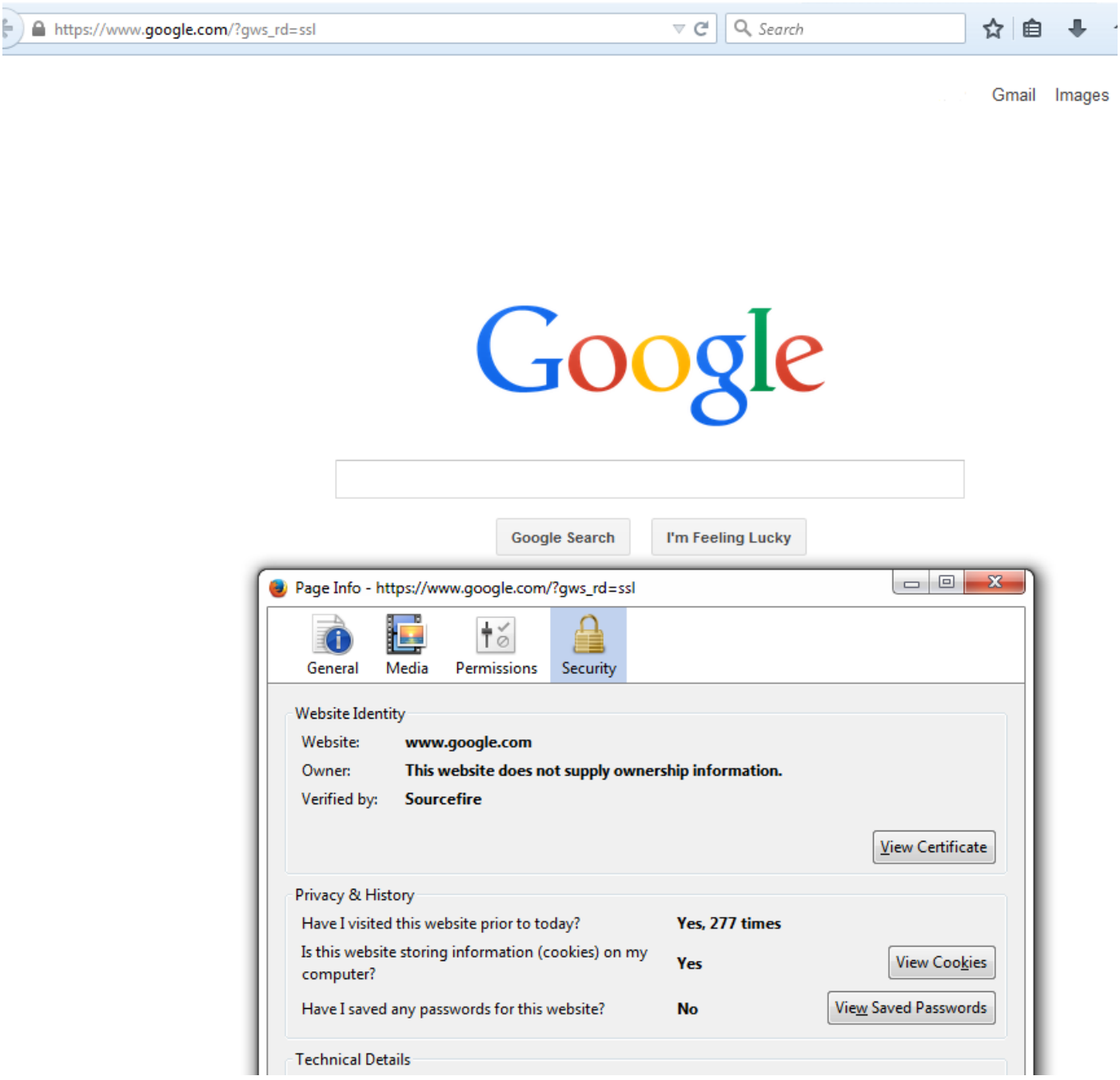
ملاحظة: يتم إستخدام مستعرض Firefox في المثال التالي. قد لا ينجح هذا المثال في الكروم. راجع قسم أستكشاف الأخطاء وإصلاحها للحصول على التفاصيل.

2. انتقل إلى موقع SSL على الويب. وفي المثال الوارد أدناه https://www.google.com، سوف تعمل أيضا المواقع الشبكية للمؤسسات المالية. سترى إحدى الصفحات التالية:



ملاحظة:سترى الصفحة أعلاه إذا لم تكن الشهادة نفسها موثوق بها ولم يكن المستعرض الخاص بك يثق في شهادة المرجع المصدق للتوقيع. لمعرفة كيفية تحديد المستعرض لشهادات المرجع المصدق الثقة، راجع قسم

المراجع المصدقة الموثوقة أدناه.



ملاحظة: إذا تم رؤية هذه الصفحة، فعليك إعادة توقيع حركة المرور بنجاح. لاحظ القسم **الذي تم التحقق منه بواسطة: Sourcefire**.

Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	www.google.com
Organization (O)	Google Inc
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	13:E3:D5:7D:4E:5F:8F:E7

Issued By

Common Name (CN)	Sourcefire TAC
Organization (O)	Sourcefire
Organizational Unit (OU)	Tac

Period of Validity

Begins On	5/6/2015
Expires On	8/3/2015

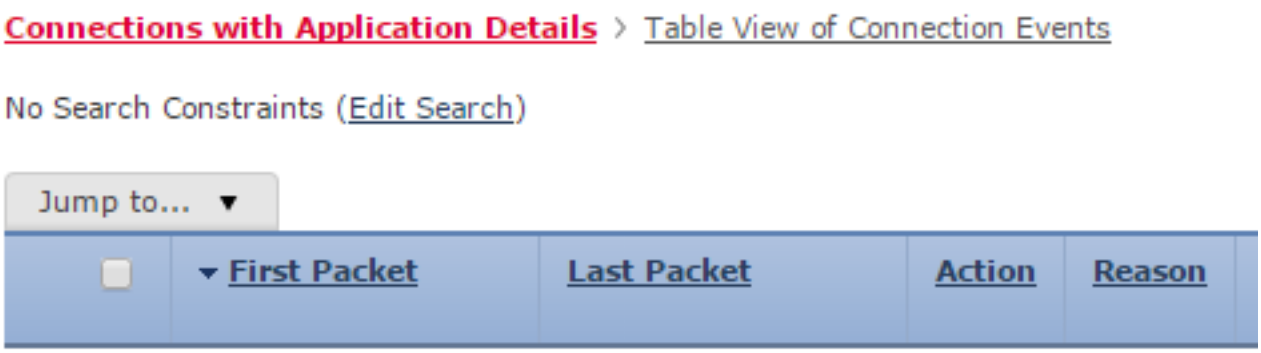
Fingerprints

SHA-256 Fingerprint	20:00:CB:25:13:8B:1F:89:4D:4A:CF:C5:E2:21:38:92: 06:66:00:2E:B7:83:27:72:98:EA:B1:6A:10:B3:67:A1
SHA1 Fingerprint	1B:C2:30:D9:66:84:DB:97:CF:A9:5E:5F:29:DA:4C:3F:13:E9:DE:5D

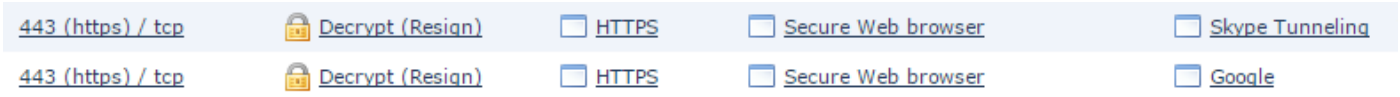
ملاحظة: هذه نظرة عن قرب إلى نفس الشهادة.

3. في مركز الإدارة، انتقل إلى **التحليل > الاتصالات > الأحداث**.

4. وفقا لسير عملك، قد ترى أو لا ترى خيار فك تشفير SSL. انقر على **عرض جدول لأحداث الاتصال**.

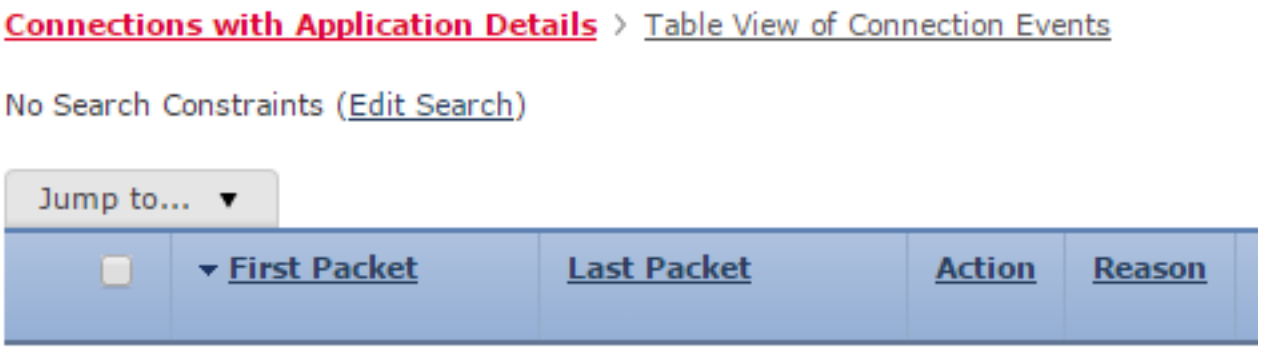


5. قم بالتمرير إلى اليمين وابحث عن حالة SSL. يجب أن ترى خيارات مشابهة لما يلي:

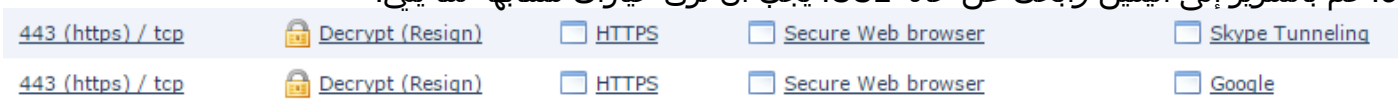


فك التشفير - الشهادة المعروفة

1. في مركز إدارة FireSIGHT، انتقل إلى **Analysis > Connections > Events**.
2. وفقا لسير عملك، قد ترى أو لا ترى خيار فك تشفير SSL. انقر على **عرض جدول لأحداث الاتصال**.



3. قم بالتمرير إلى اليمين وابحث عن حالة SSL. يجب أن ترى خيارات مشابهة لما يلي:



استكشاف الأخطاء وإصلاحها

الإصدار 1: قد لا يتم تحميل بعض مواقع الويب على مستعرض Chrome

مثال

www.google.com قد لا يتم التحميل مع فك التشفير - الاستقالة باستخدام Chrome.

سبب

متصفح غوغل كروم قادر على اكتشاف شهادات الغش لملكية غوغل من أجل منع هجوم الدخيل. إذا حاول مستعرض Chrome (العميل) الاتصال بمجال google.com (خادم) وتم إرجاع شهادة ليست شهادة Google صالحة، فسيرفض المستعرض الاتصال.

الحل

إذا واجهت هذا الأمر، فقم بإضافة قاعدة **عدم فك التشفير** ل DN=*.google.com، *.gmail.com، *.youTube.com. ثم قم بمسح ذاكرة التخزين المؤقت للمستعرض والمحفوظات.

المشكلة 2: الحصول على تحذير/خطأ غير موثوق به في بعض المستعرضات

مثال

عند إتصالك بموقع يستخدم Internet Explorer و Chrome، لا تتلقى تحذير أمان، ولكن عند إستخدام مستعرض Firefox، يجب أن تثق بالاتصال في كل مرة تقوم فيها بإغلاق المستعرض وإعادة فتحه.

سبب

تعتمد قائمة المراجع المصدقة الموثوق بها على المستعرض. عندما تثق في شهادة ما، فإن هذا لا يتم إستخدامه عبر المستعرضات، وعادة ما يستمر الإدخال الموثوق به فقط أثناء فتح المستعرض، لذلك بمجرد إغلاقه سيتم تنقيح كافة الشهادات الموثوق بها، وفي المرة القادمة التي تقوم فيها بفتح المستعرض وزيارة الموقع، يجب إضافته إلى قائمة الشهادات الموثوق بها مرة أخرى.

الحل

في هذا السيناريو، يستخدم كل من IE و Chrome قائمة المراجع المصدقة الموثوقة في نظام التشغيل ولكن يحتفظ Firefox بقائمته الخاصة. تم إستيراد شهادة المرجع المصدق إلى متجر نظام التشغيل ولكن لم يتم إستيرادها إلى مستعرض Firefox. لتجنب الحصول على تحذير الأمان في Firefox يجب إستيراد شهادة CA إلى المستعرض كمرجع مصدق موثوق به.

مراجع الشهادات الموثوق بها

عندما يتم إجراء اتصال SSL، يتحقق المستعرض أولا لمعرفة ما إذا كانت هذه الشهادة موثوق بها (أي أنك كنت في هذا الموقع من قبل وأمرت المستعرض يدويا بأن يثق بهذه الشهادة). إذا لم تكن الشهادة موثوق بها يتأكد المستعرض من شهادة المرجع المصدق (CA) التي دققت الشهادة لهذا الموقع. إذا كان المستعرض يثق في شهادة المرجع المصدق فإنها تعتبرها شهادة موثوق بها وتسمح بالاتصال. إذا كانت شهادة المرجع المصدق غير موثوق بها يعرض المستعرض تحذير تأمين ويجبرك على إضافة الشهادة يدويا على هيئة شهادة موثوق بها.

تعتمد قائمة المراجع المصدقة الموثوقة في المستعرض اعتمادا كاملا على تنفيذ الملقم ويمكن لكل متصفح ملء القائمة الموثوق بها الخاصة به بشكل مختلف عن المستعرضات الأخرى. بشكل عام، هناك طريقتان تقوم المستعرضات الحالية بتعميم قائمة من المراجع المصدقة الموثوق بها:

1. إنهم يستخدمون قائمة المراجع المصدقة الموثوق بها التي يثق بها نظام التشغيل
2. فهم يقومون بشحن قائمة بالمخابرات الموثوق بها مع البرنامج، كما أنها مضمنة في المستعرض.

بالنسبة لأكثر المستعرضات شيوعا، يتم تعبئة المراجع المصدقة الموثوقة كما يلي:

- **جوجل كروم**: نظام التشغيل قائمة المرجع المصدق عليها
- **فايرفوكس**: يحتفظ بقائمة مرجع مصدق ثقة خاص به
- **Internet Explorer**: قائمة المرجع المصدق (CA) الموثوق بها لنظام التشغيل
- **سفاري**: قائمة المرجع المصدق الموثوقة الخاصة بنظام التشغيل

ومن المهم أن تعرف الفرق لأن السلوك الذي ستشهده الزبون يختلف تبعا لذلك. على سبيل المثال، لإضافة مرجع مصدق ثقة ل Chrome و IE يجب إستيراد شهادة المرجع المصدق إلى مخزن المرجع المصدق الموثوق به الخاص بنظام التشغيل. إذا قمت باستيراد شهادة المرجع المصدق إلى مخزن المرجع المصدق الموثوق به الخاص بنظام التشغيل، فلن تعود تتلقى أي تحذير عند الاتصال بالمواقع التي تحتوي على شهادة موقعة من قبل هذا المرجع المصدق. على متصفح Firefox، يجب عليك إستيراد شهادة CA يدويا إلى مخزن CA الموثوق به في المتصفح نفسه. بعد القيام بهذا الإجراء، لن تتلقى تحذيرا أمنيا عند الاتصال بالمواقع التي تم التحقق منها بواسطة المرجع المصدق.

المراجع

- بدء إستخدام قواعد SSL

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).