مركز إدارة جدار الحماية/جدار الحماية المعتمد من Cisco - انعدام الثقة في الحالات الطارئة بسلطات الشهادات الوسيطة والجذور الإلكترونية

المحتويات

الغرض

يصف هذا المستند كيفية تكوين مركز Cisco Secure Firewall Management Center (FMC) وجهاز Cisco Secure Firewall Threat Defense (FTD) لتلقي تحديثات حزمة شهادات خدمة FMC المحلية من Cisco، وكيفية استيراد شهادة CA لخدمة TrustPool التلقائية من ASA، وكيفية تكوين الثقة في الحالات الطارئة بسلطات الشهادات الوسيطة والجذور في eMulkmRa.

تحديثات حزمة شهادات خدمة FMC المحلية من Cisco

يمكن أن تقوم FMC و FTD تلقائيا بتحديث حزمة CA محلية تستخدم لاتصالات TLS من الجهاز إلى خدمات Cisco، بما في ذلك الترخيص الذكي والبرامج، و VDB، و SRU، وتحديثات الموقع الجغرافي. تتوفر ميزات Cisco التي تتحقق النظام. يتحقق النظام يوميا في وقت محدد من قبل النظام. وهذه هي حدود الميزات، وليست وجهات الترقية بدءا من FMC/FTD 7.0.5 و 7.1.0.3 و 7.2.4 و 7.3.0+. حدد هدف ترقية باستخدام النظام الأساسي الدقيق والإصدار المصدر الموصى بها؛ راجع إصدار Cisco الحالية. [3، و4] ومتطلبات التوافق وإرشادات

على FMC أو CLI ل FTD مدعوم، إظهار تقارير التحديث التلقائي حالة التحديث، والجدول اليومي، ووقت آخر تعديل للحزمة. شكلت تحديث إخبار قديم إذا كانت الحزمة محلي حالي وما إذا كان تحديث موصولية جاهز. [6 و 5 و 4]

تكون حزمة خدمة Cisco هذه منفصلة عن كائنات/مجموعات CA الموثوق بها التي تم تكوينها بالأجهزة ومن نقاط الثقة SSL ريفشت ك من قبل فك تشفير إستخدامها التي يتم إستخدامها ل FTD و VPN. ستحتاج إلى التحقق من أنه لم تتم إضافة أي من هذه الشهادات المستخدمة لشهادات الهوية أو التكوين. [5، و6] الشهادات يدويا إلى التكوين.

إستيراد ASA CA TrustPool تلقائيا

لحمل .يحمل شهادات ASA، دعت TrustPool ونقاط الثقة المسماة ميزات منفصلة لإدارة الشهادات في ASA، كما يتم فصل إستيراد ASA التلقائي لتجميع المستندات عن تحديث حزمة خدمة FMC/FTD من Cisco-Service المرضح أعلاه. [8، و9]

لتحقق للقراءة فقط، قم بتشغيل show crypto ca trustPool policy لمراجعة عدد شهادات TrustPool المسموح بها، والمحاولة المجدولة التالية، والنتائج، وتفاصيل النهج والحالة الاستيراد والثقة المجمع الفعالة. قم بتشغيل show run crypto ca trustPool policy لمراجعة سطور نهج المجمع الثقة التي تم تكوينها. وثائق Cisco إستيراد تلقائي إيقاف تشغيل بشكل افتراضي. عندما يتم إستخدام 22:00 في ساعة 24 لكل محاولة محددة مجدولة، يكون الجدول الزمني دون تجاوزات، يتم تمكينها. يمكن للوقت المكون أو عنوان URL تغيير هذه القيمة؛ عنوان URL الافتراضي من Cisco. إستخدام التلقائي أو الاستيراد التمكين افتراض من بد الفعلي ASA الخارج من التحقق [8، و9] الجدول الافتراضي.

وأظهر هذه التحققات السياسة والحالة الاستيراد؛ فهي لا توفر جدا للشهادة بالشهادة أو الشهادات المضمنة في الحزمة. لا يثبت أن أي شهادة مسماة من الشهادات المضمنة مثبتة أو مازال أو غير موثوق بها. كدليل على TrustPool في ASA من FMC/FTD cert-update، والتعامل مع حالة تستدل على سلوك TrustPool آخر. تأكد من إصدار الشهادات التي تم تكوينها تحت TrustPoint معينة أو مخزن الثقة المطبق. أي حاجة إلى اتخاذ قرار بشأن ما إذا كان هناك الشهادة قبل المعتمدة على الشهادة والخدمة الصحيح ASA إجراء خاص بالمنتج. [8، و9]

حل بديل محتمل باستخدام برنامج FTD لحماية أجهزتك التي لم تتم معالجتها

الغرض

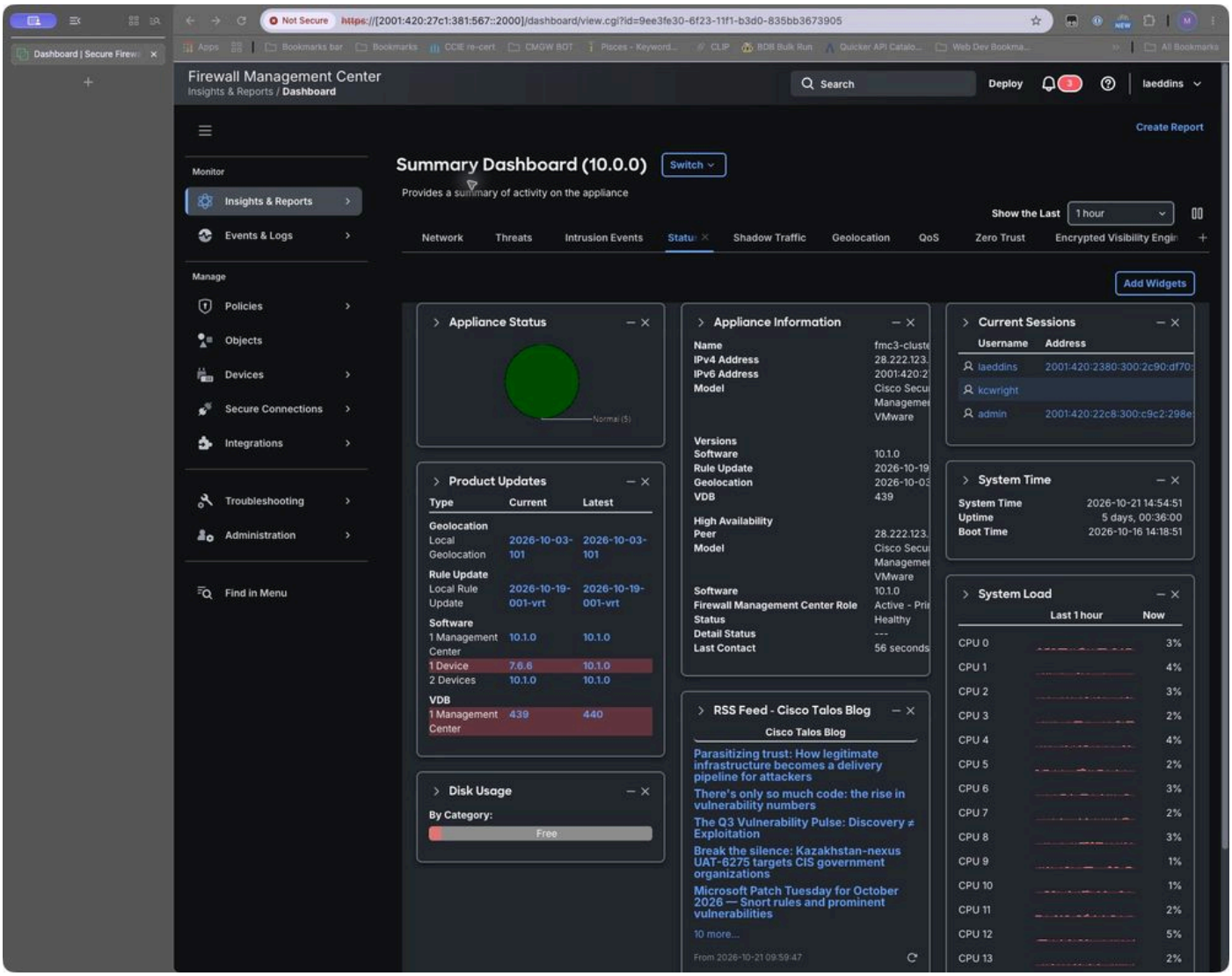
تسمح TLS التي تمنع سياسة قواعد Cisco من (FMC) الآمن الحماية جدار إدارة مركز المستخدم بأسرار الخادم الشهادات. يمكن لعنصر الشهادات المتأثرة الإلكترونية المعروفة. هذا التحكم الذي تقليل التعرض للعملاء والخوادم التي لا تحتوي على أي وثوق والتي لم تتلق التحديثات المطلوبة بعد، ولكن لا يمنع الاتصالات الخاصة بها في مخزن ثقة التطبيقات. تقوم باستيراد الشهادة. لا تتابع إصلاح مخزن الثقة والتحديثات في جميع السيناريوهات. مرجع مصدق ثقة لهذا الإجراء.

المتطلبات الأساسية

تم التحقق من صحة المعلومات في هذه المقالة على FMC 10.1.0. تم التقاط شاشات التكوين في مختبر إجراء تم لم. 7.6.6 على وجهاز 10.0.0 على مديني. تم إختبار حركة مرور. قبل التحقق من النهج، ووضع الإنذار، و Snort Engine، و FTD الهدف إصدار لتسجيل قم بتشغيل، التنفيذ

السياسة إلى الوصول، ونهج TLS. تأكد من أن حركة المرور الصادرة المتأثرة تصل إلى الوجهة المقصودة.

شكل 1. FMC 10.1.0 برامج الأجهزة المدارة.



تكوين مطابقة المصدر

شروط Cisco Document Source-dn لمطابقة المرجع المصدق الذي أصدر شهادة الخادم. إضافة كائن DN مع إضافة إلى المصدر في محرر القاعدة. يعتمد التنقل والتسميات المتوفرة على الإصدار. [1، و2]

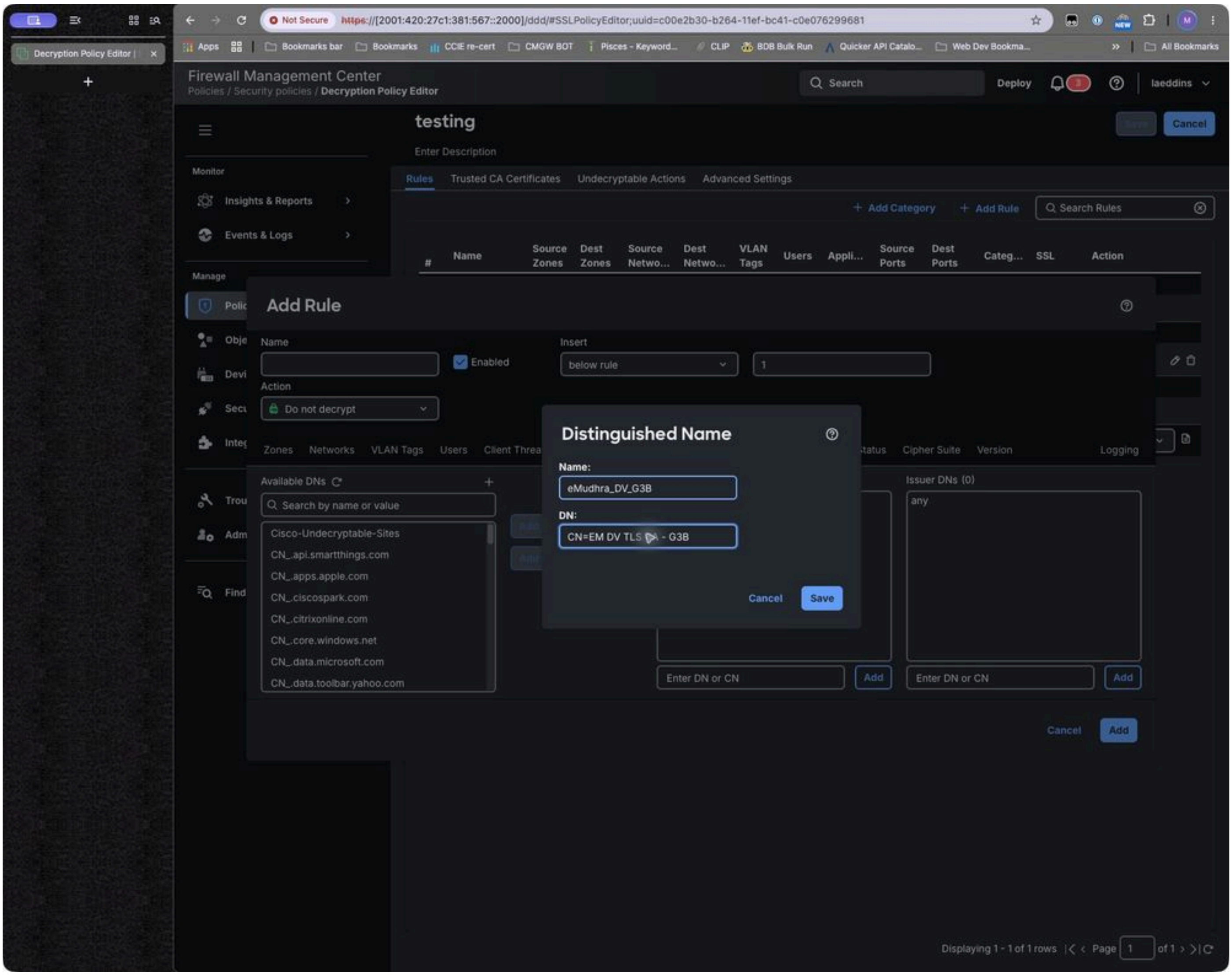
1 إنشاء الكائنات

جدول الكائنات

DN	اسم كائن DN المقترح
CN=EM DV TLS CA - G3b	eMudhra_DV_G3B
cn=EM DV TLS CA - G3C	eMudhra_DV_G3C
cn=EM EV TLS CA - G3B	eMudhra_EV_G3B
cn=EM EV TLS CA - G3C	eMudhra_EV_G3C
CN=EM ov TLS CA - G3B	eMudhra_OV_G3B
CN=EM ov TLS CA - G3C	eMudhra_OV_G3C

قم بإنشاء كائن DN ذو نطاق ضيق لكل كائن في الجدول أعلاه.

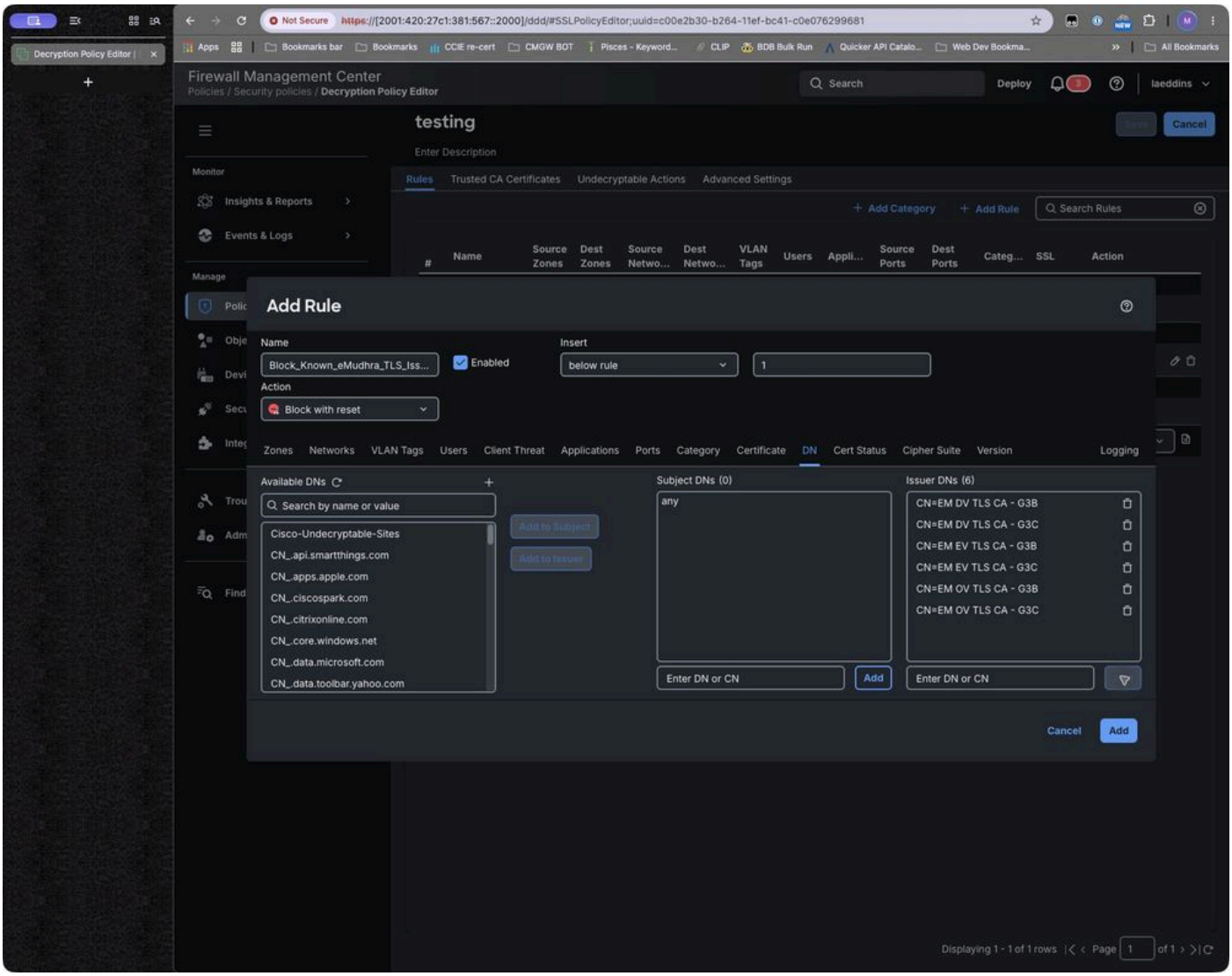
شكل 2. نموذج الاسم المميز الذي يظهر حقلي الاسم و DN. تم إدخال قيمة المثال للتوضيح؛ انقر فوق عنوان الانتهاء.



2 إنشاء قاعدة الحظر

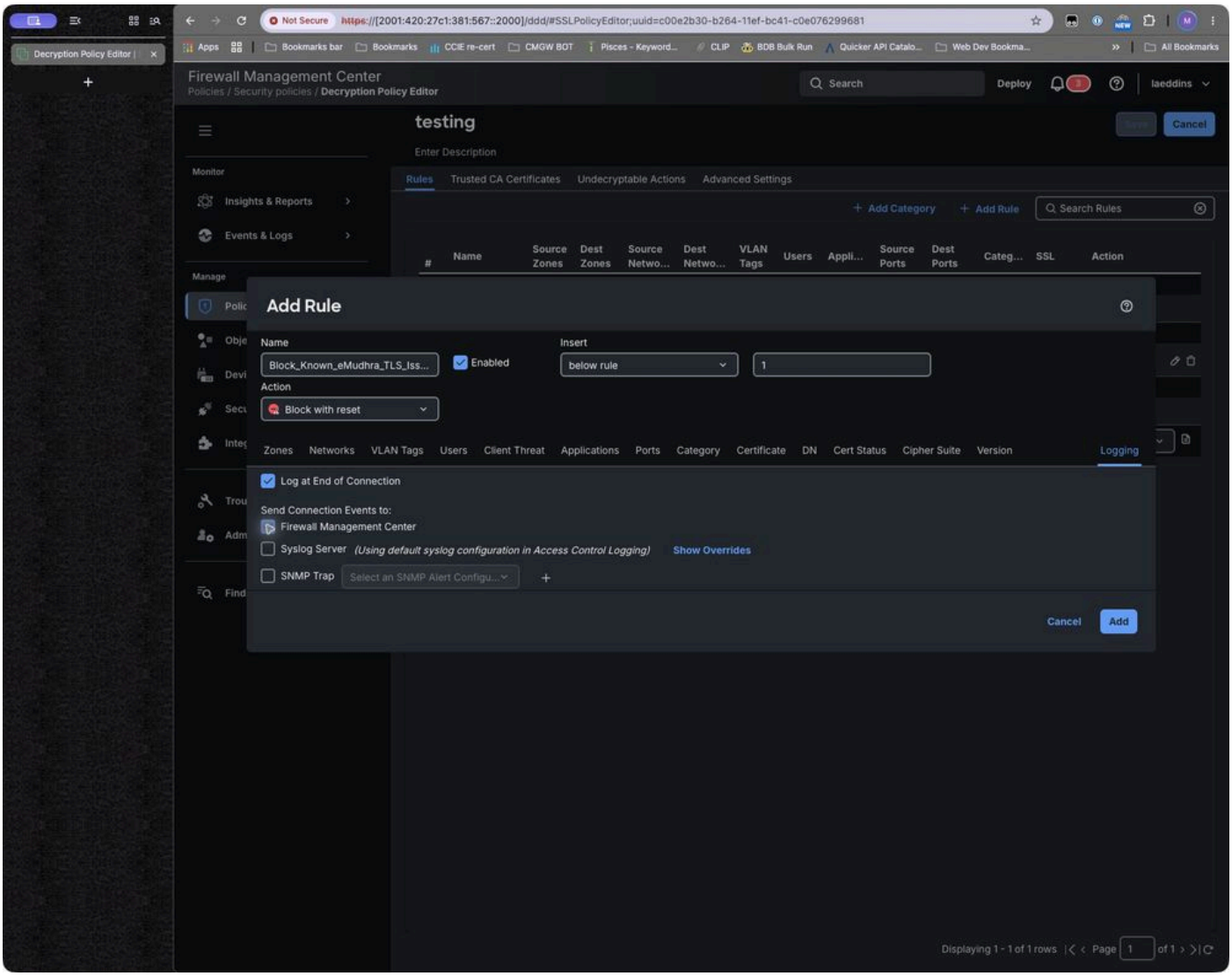
في FMC 10.1.0، حدد سياسات > سياسات التأمين > فك التشفير، افتح السياسة المطبقة، وانقر إضافة قاعدة. قم بتسمية القاعدة block_known_eMudhra_TLS_Issuers. افتح علامة التبويب DN. أضف كائنات تم التحقق منها مع إضافة إلى المصدر، أو أدخل DN في حقل Issuer DN المسمى أدخل DN أو CN وانقر فوق الزر "إضافة" الخاص به. تأكيد الأسماء التي تظهر في DNs المصدر وليس في SUBJECT DNs.

شكل 3. قاعدة تظهر الحظر مع إعادة التعيين، وعلامة التبويب DN، وست شبكات DN للإصدار، ولا يوجد قيد DN للموضوع. انقر إضافة عند الانتهاء.



حدد "كتلة" أو "كتلة" مع إعادة التعيين. تحديد مناطق المصدر أو الشبكات للنطاق المتفق عليه. إذا رغبت، في علامة التبويب تسجيل، حدد تسجيل في نهاية التوصيل وتحقق من تحديد مركز إدارة جدار الحماية. عدم إضافة متطلب = نعم صالح: يجب ألا تعتمد كتلة المصدر المقصودة على التحقق من صحة الثقة العابرة للشهادة.

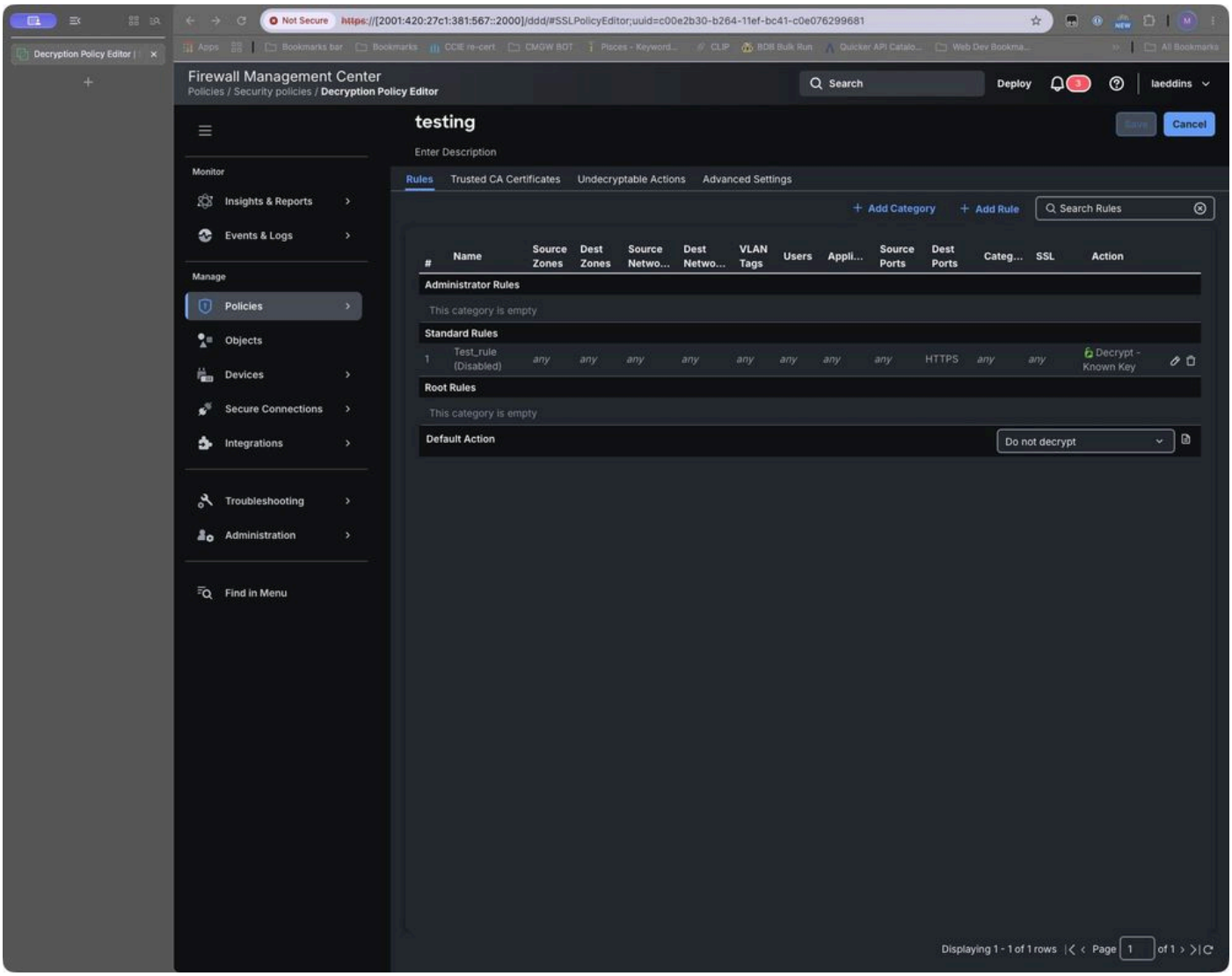
الشكل 4. تم تحديد قاعدة ظهر السجل في نهاية الاتصال ومركز إدارة جدار الحماية. انقر إضافة عند الانتهاء



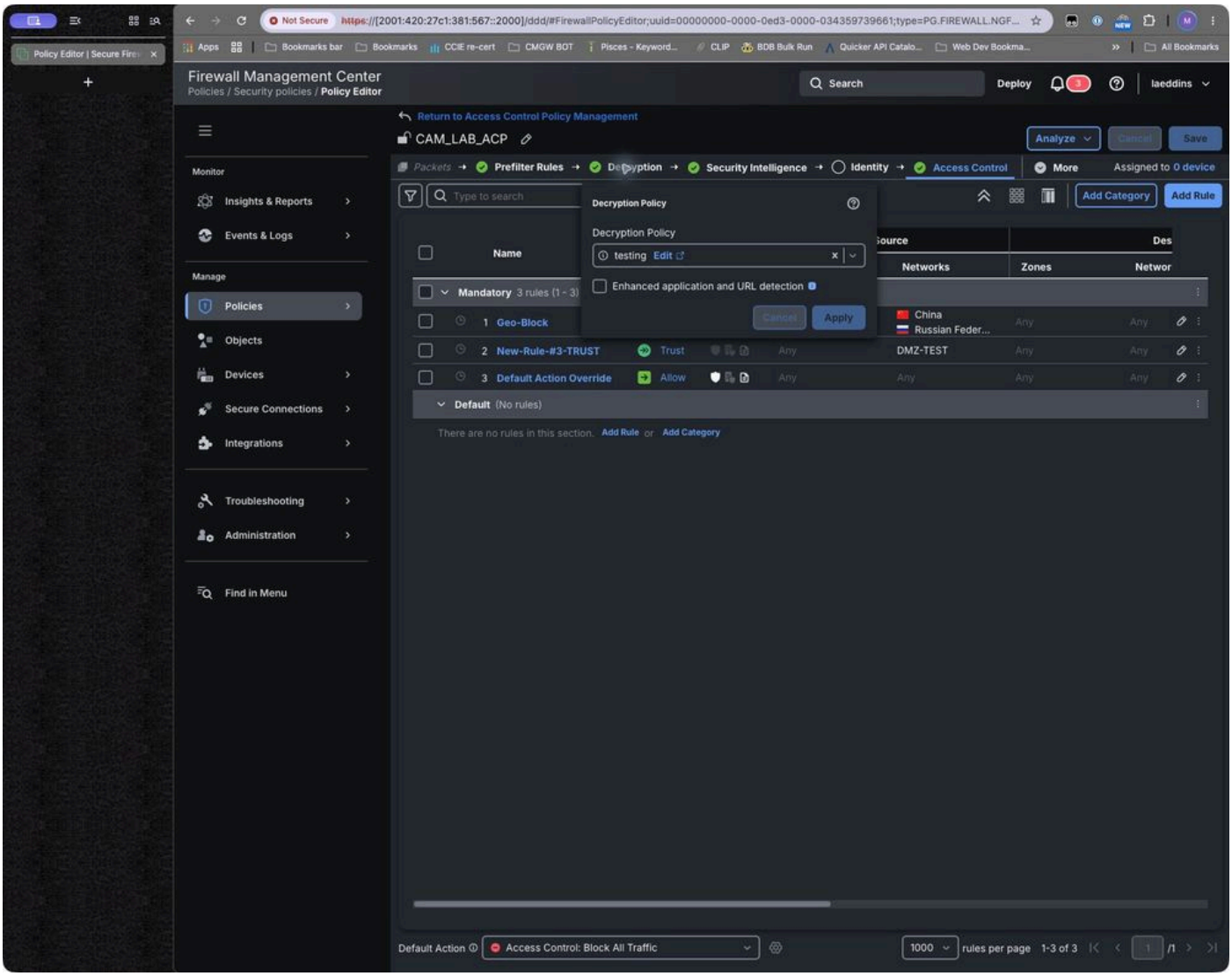
3 مراجعة اقتران نظام القاعدة والسياسة

ضع القاعدة قبل القواعد الأوسع التي يمكنها التعامل مع حركة المرور نفسها أولا. تأكيد اقتران نهج TLS بنهج التحكم بالوصول المعين للأجهزة الهدف. راجع مرشح مسبق ومسارات تجاوز أخرى قبل الاختبار.

الشكل 5 - الجدول الحالي لقاعدة قواعد سياسة الاختبار. يعرض هذا واجهة طلب الشراء فقط.



شكل 5 ب. يشير نهج CAM_LAB_ACP الموجود إلى نهج فك تشفير الاختبار.



النشر والتحقق

قم بنشر التغييرات على الأجهزة المعنية. إذا كانت متاحة، قم بالاختبار باستخدام موقع ويب تعرف أنه يستخدم شهادة صادرة عن أحد المراجع المصدقة المعنية.

أستكشاف النتائج غير المتوقعة وإصلاحها

إذا تم تمرير حركة المرور، فتحقق من حالة النشر، ونطاق حركة المرور، واقتران السياسة، وترتيب القاعدة، وتصحيح أخطاء المصدر والترميز الميداني، وما إذا كان الجهاز يحتوي على معلومات شهادة. حدد ما إذا كانت هناك قاعدة أخرى أو مسار جانبي آخر يعالج التدفق. راجع إمكانية رؤية TLS 1.3 على الإصدار الذي تم إختباره قبل المطالبة بتغطية مكافئة.

إعداد متقدم TLS 1. 3: في FMC 7. 6، يعد فك تشفير TLS 1. 3 التحقق الإضافي من صحة مستقل لسياسة فك التشفير؛ في حالة تعطيله، يتم تطبيق قواعد فك التشفير

مداخ ةيوه نم ققحتلا TLS 1.3 ريفشت كف نيكمت هجيتي. قفطل قلأ وأ TLS 1.2 على
ةداهشلا نيزختم تي ال دنعم قيقحت لغشيت DN رصدم طرش موقي نأ نكمي وه،ةيكيتاملا
ةيولوألا دادعإ ةيوه كافشتسا TLS 1.3 مداخ صاخلا بنهج لتحكم بالوصول
.تكون مزلتقملا. تقول Cisco نأب تيم هذه تادادعإلا ةمدقتملا على ةزهجألا مدقألا نم 7.1 وأ
ةيوهلا قباطلل للتكيف ريغ موعدم على FTDv ذيلا تم
ةيساسألا ةمظنألا/جمارب ةيؤر ةيناكمإ نم ققحت .AWS ىلإ رشنه
ةيطغتلا بتكملا TLS 1.3. ةمدختسملا TLS 1.2 ىتح؛ ةيامحلا ةدعاقلا ىلع هذه ةدحملا ل TLS 1.3. [7]

ةمزح .رداصملا ةيلعفلا ةقباطملا ةدعاق ،ةطبترملا ريغ رورملا ةكرح تلشف اذإ
ةمزحلا ىوتسم ىلع ةيامحلا ةدعاق ريغيت ،ةمزحلا ىوتسم ىلع ةيامحلا ةدعاق ريغيت
.ةمزحلا ىوتسم ىلع ةيامحلا ةدعاق ريغيت ،ةمزحلا ىوتسم ىلع ةيامحلا ةدعاق ريغيت

ةيلغشتلا دودحلاو ةيطغتلا

.ةيامحلا ةدعاق ريغيت ،ةمزحلا ىوتسم ىلع ةيامحلا ةدعاق ريغيت

ةدعاقلا لازنإو عجارتلا

ةدعاقلا ريغيت ،ةمزحلا ىوتسم ىلع ةيامحلا ةدعاق ريغيت ،ةمزحلا ىوتسم ىلع ةيامحلا ةدعاق ريغيت
.ةمزحلا ىوتسم ىلع ةيامحلا ةدعاق ريغيت ،ةمزحلا ىوتسم ىلع ةيامحلا ةدعاق ريغيت

عجارملا

[1] FMC 7.2 ريفشتلا فك دعاوق

[2] FMC 10.x ةدعاق ىلإ ةدنتسملا زيمرتلا فك دعاوق

[3] رادصإلا نم ةديدجلا تازيملا نم ةيامحلا رادج ةرادإ زكرم

[4] FDM و FMC ل CA تاعومجمل يئاقلتلا ثيدحتلا نيوكت قم

[5] FMC 7.6 تاداهش

[6] تاداهش FDM 7.6

[7] سياسات فك الترميز FMC 7.6 وإدارة شهادات TLS 1.3

[8] دليل تكوين واجهة سطر الأوامر للعمليات العامة Cisco Secure Firewall ASA 9.22 — تاداهش الرقمية

[9] مرجع أوامر سلسلة ASA لجدار الحماية الآمن من Cisco — سياسة Crypto CA TrustPool

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).