تكوين ANC على ISE 3.3 و Stealthwatch 7.5.1

المحتويات

المقدمة

يصف هذا المستند تكوين إحتواء التهديدات السريعة (Adaptive Network Control) على Cisco ISE® الإصدار 3.3 و Stealthwatch.

المتطلبات الأساسية

توصي Cisco بالمعرفة في هذه الموضوعات:

- محرك خدمات كشف الهوية (ISE)
- شبكة تبادل الأنظمة الأساسية (PxGrid)
- تحليلات الشبكة الآمنة (Stealthwatch)
- إحتواء التهديد السريع (تحكم شبكة قابل للتكيف - ANC).

في هذا المستند يفترض أن محرك خدمات تعريف Cisco يتم دمجه مع تحليلات الشبكة الآمنة (Stealthwatch) باستخدام pxGrid التي تم تمكين ANC عليها.

المكونات المستخدمة

أسست المعلومة في هذا وثيقة على هذا برمجية وإصدارات:

- Cisco Identity Services Engine (ISE)، الإصدار 3.3
- تحليلات الشبكة الآمنة (Stealthwatch) 7.5.1
- Catalyst 9300

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 قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

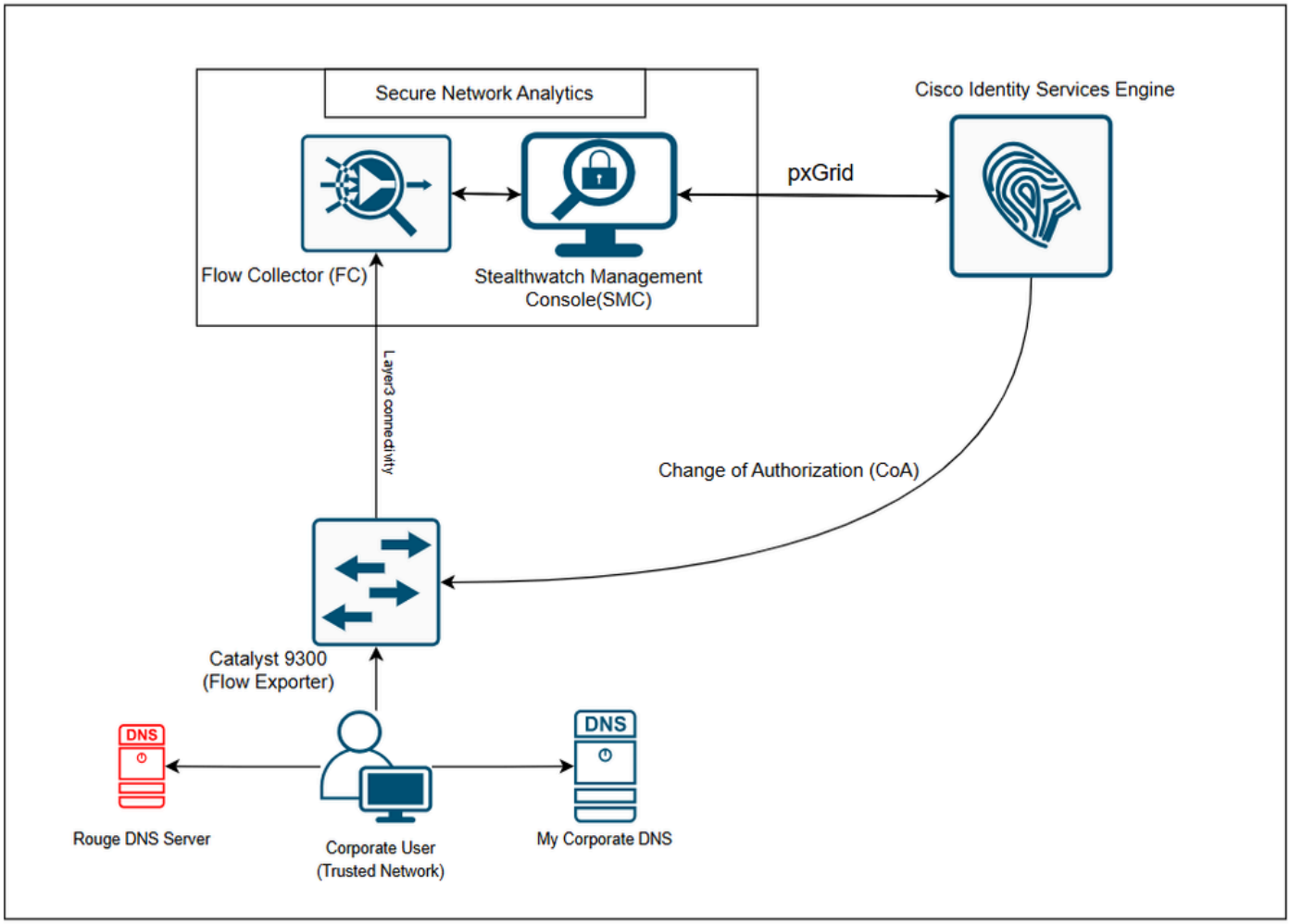
يمكن لتحليلات السحابة الآمنة من Cisco (الآن جزء من Cisco XDR) إستيراد بيانات مساهمة المستخدم من Cisco Identity Services Engine (ISE) باستخدام PxGrid. يتيح هذا التكامل إمكانية إعداد تقارير عن نشاط المستخدم في عارض أحداث تحليلات السحابة الآمنة.

تستعد مجموعة تحليلات الشبكة الآمنة (المعروفة سابقا باسم Stealthwatch) ومحرك خدمات الهوية (ISE) من Cisco شركة المؤسسات على الحصول على طريقة عرض بمقدار 360 درجة والاستجابة للتهديدات بشكل أسرع وتأمين رقمية متنامية. بمجرد أن تقوم "تحليلات الشبكة الآمنة" باكتشاف حركة المرور غير العادية، فإنها تصدر تنبيها، مما يعطي المستخدم. يتيح pxGrid تحليلات الشبكة الآمنة تسليم الأمر لعزل المستخدم المؤول خيار عزل المستخدم مباشرة إلى محرك خدمات الهوية.

يوضح هذا المثال الاستفادة من خادم DNS الخاص بالشركات للحماية من تهديدات الإنترنت. والهدف من ذلك هو إنشاء آلية تنبيه مخصصة تعمل عند اتصال المستخدمين الداخليين بخوادم DNS الخارجية. وقد صممت هذه المبادرة لمنع الاتصالات بخوادم DNS غير المعتمدة التي يمكن أن تعيد توجيه حركة المرور إلى المواقع الخارجية الضارة.

عند تشغيل تنبيه، تقوم تحليلات الشبكة الآمنة من Cisco بالتنسيق مع Cisco ISE لعزل المضيف الذي يصل إلى خوادم DNS غير المصرح بها، باستخدام سياسة التحكم في الشبكة القابلة للتكيف عبر PxGrid.

الرسم التخطيطي للشبكة



كما هو موضح في الرسم التخطيطي:

- يتم توصيل مستخدم الشركة بمحول C9300 switch تم تكوينه لتصدير تدفقات IP وإرسال البيانات إلى مجمع التدفق.
- تم تكوين نفس المستخدم الخاص بالشركة على خوادم DNS الخاصة بالمستخدم.
- يتم دمج مجمع التدفق مع وحدة تحكم إدارة Stealthwatch (SMC)
- وحدة تحكم إدارة Stealthwatch (SMC) مدمجة من خلال PxGrid مع ISE.

التكوين بالتفصيل

1. تجهيز المحول لمراقبة التدفقات وتصديرها باستخدام NetFlow.

تكوين التدفق الأساسي على محول C9300 يشغل Cisco IOS® XE 17.15.01

```
flow record SW_FLOW_RECORD
  description NetFlow record format to send to SW
  match ipv4 tos
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  match interface input
```

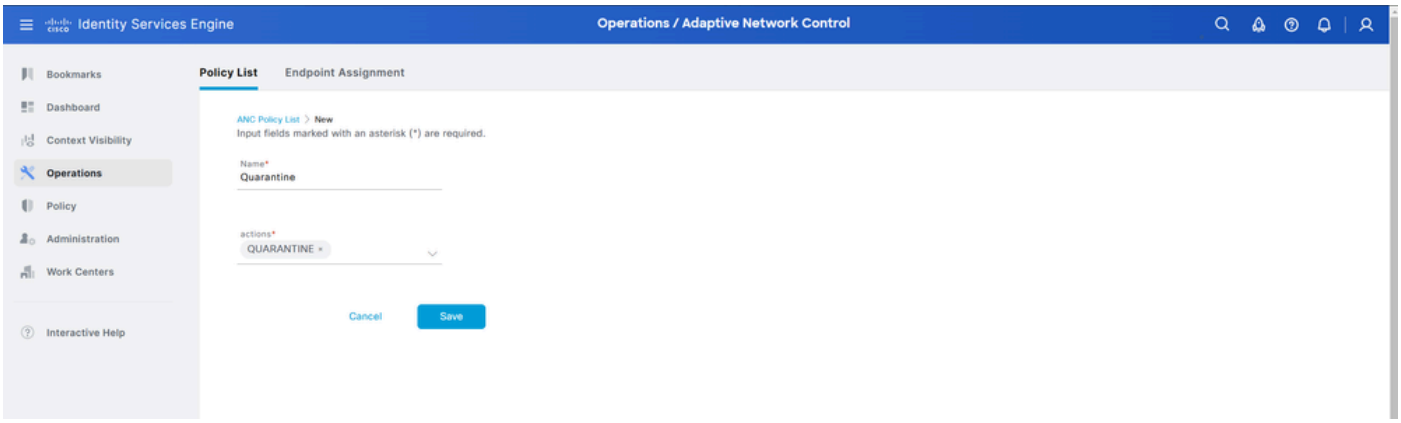
```
  collect transport tcp flags
  collect interface output
  collect counter bytes long
  collect counter packets long
  collect timestamp absolute first
  collect timestamp absolute last


flow exporter NETFLOW_TO_SW_FC
  description Export NetFlow to SW FC
  destination 10.106.127.51        ! Mention the IPv4 address for the Stealthwatch Flow Collector
  ! source Loopback0               ! OPTIONAL: Source Interface for sending Flow Telemetry (e.g. Loopba
  transport udp 2055
  template data timeout 30

flow monitor IPv4_NETFLOW
  record SW_FLOW_RECORD
  exporter NETFLOW_TO_SW_FC
  cache timeout active 60
  cache timeout inactive 15

vlan configuration Vlan992
  ip flow monitor IPv4_NETFLOW input   !Apply this to the VLAN/Interface that you want to monitor the f


! VALIDATION COMMANDS
!  show flow record SW_FLOW_RECORD
!  show flow monitor IPv4_NETFLOW statistics
!  show flow monitor IPv4_NETFLOW cache
```

عند إكمال التكوين، فإنه يمكن C9300 من تصدير بيانات تدفق IP إلى مجمع التدفق. ثم يقوم مجمع التدفق بمعالجة هذه البيانات ونقلها إلى وحدة تحكم إدارة Stealthwatch (SMC) للتحليل والمراقبة.

2. Enable Adaptive Network Controller في Cisco ISE.

يتم تعطيل ANC بشكل افتراضي. الا يتم تمكين ANC إلا عندما يتم تمكين pxGrid، وتظل ممكنة حتى تقوم بتعطيل الخدمة يدويا في مدخل الإدارة.

حدد عمليات > Adaptive Network Control (التحكم في الشبكة التكيفية) > Policy List (قائمة السياسات) > Add، ثم أدخل عزل الاسم النهج والحجر الزراعي للإجراء.

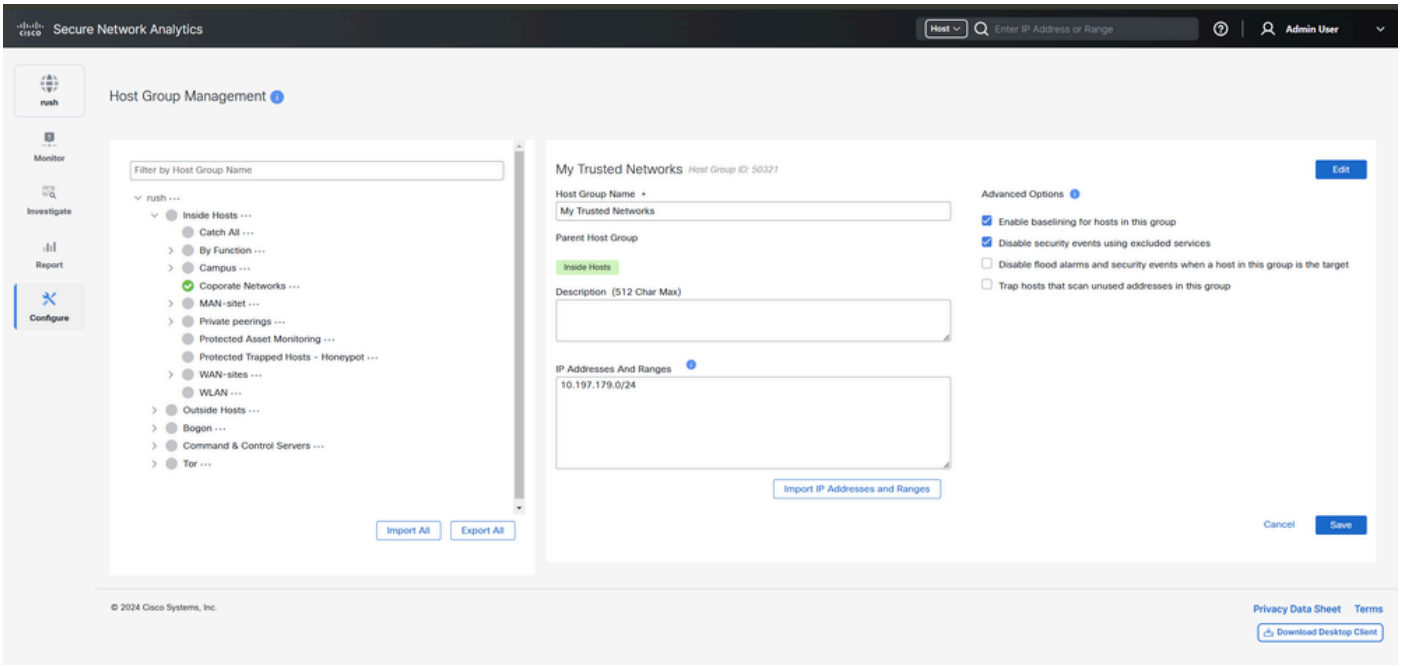


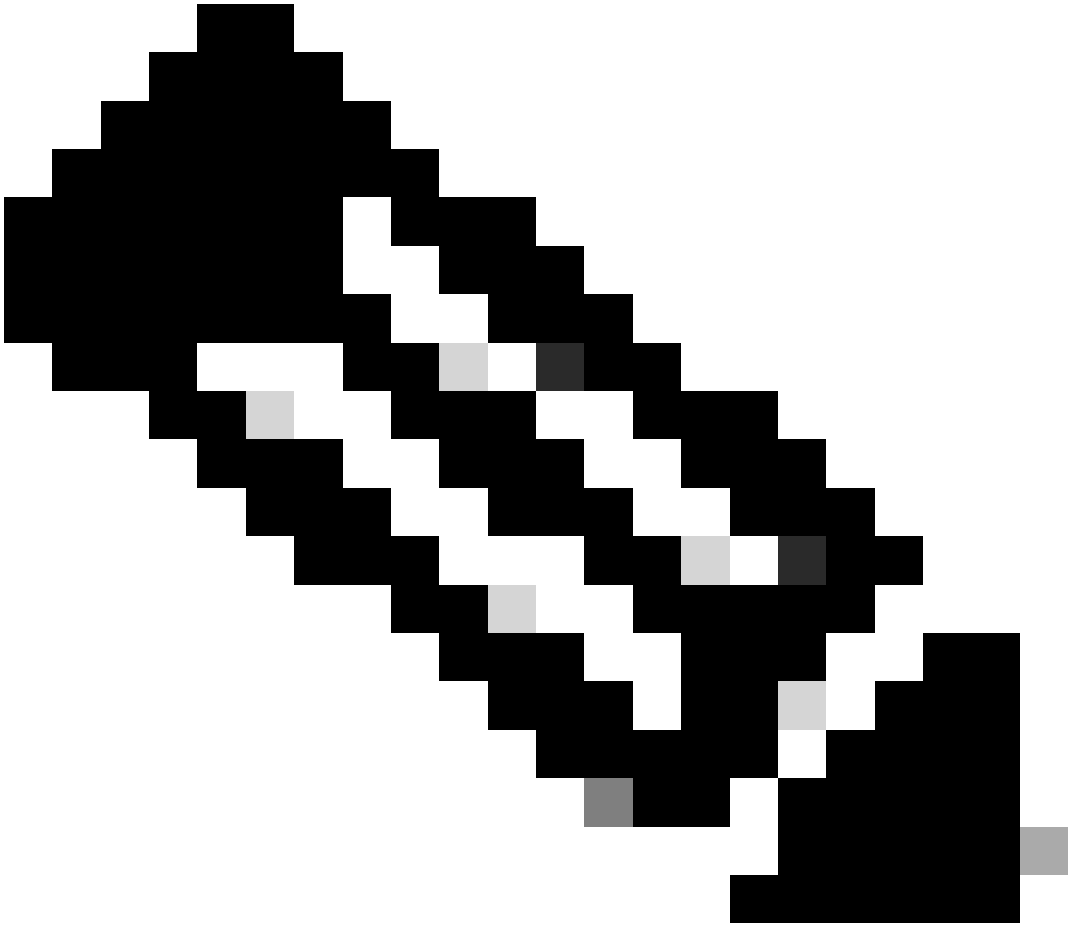
3. تكوين تحليلات الشبكة الآمنة لمشغل الحدث وإدارة الاستجابة لاحتواء التهديد السريع.

الخطوة 1: قم بتسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) لـ SMC وانتقل إلى تكوين > اكتشاف > إدارة المجموعة المضيفة > انقر على أيقونة (...) (البيضاوي) بجوار الأجهزة المضيفة الداخلية، ثم حدد إضافة مجموعة مضيف.

في هذا المثال، يتم إنشاء مجموعة مضيف جديدة باسم الشبكات الموثوق بها الخاصة بي أسفل مجموعة المضيف الأصل من البيئات المضيفة الداخلية.

يمكن تعيين هذه الشبكة بشكل نموذجي إلى جهاز المستخدم النهائي لمراقبة إستخدام DNS.

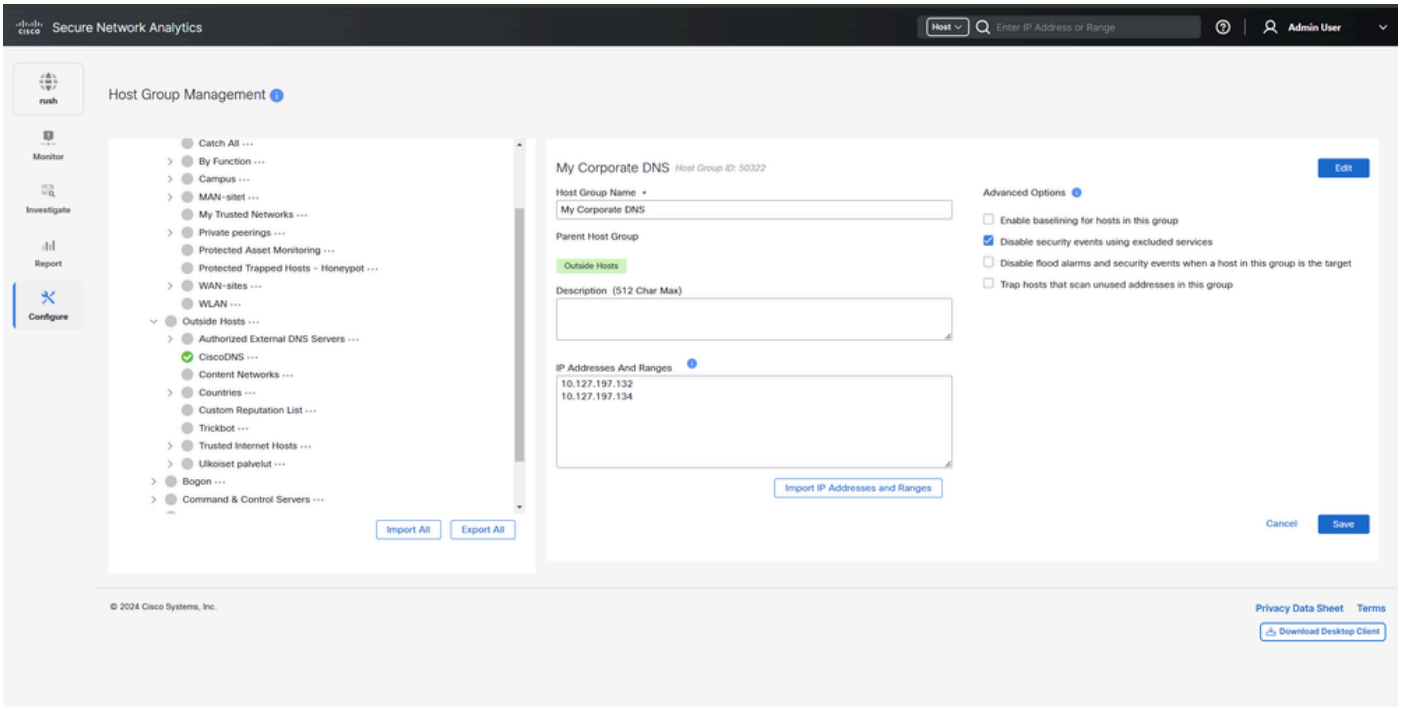


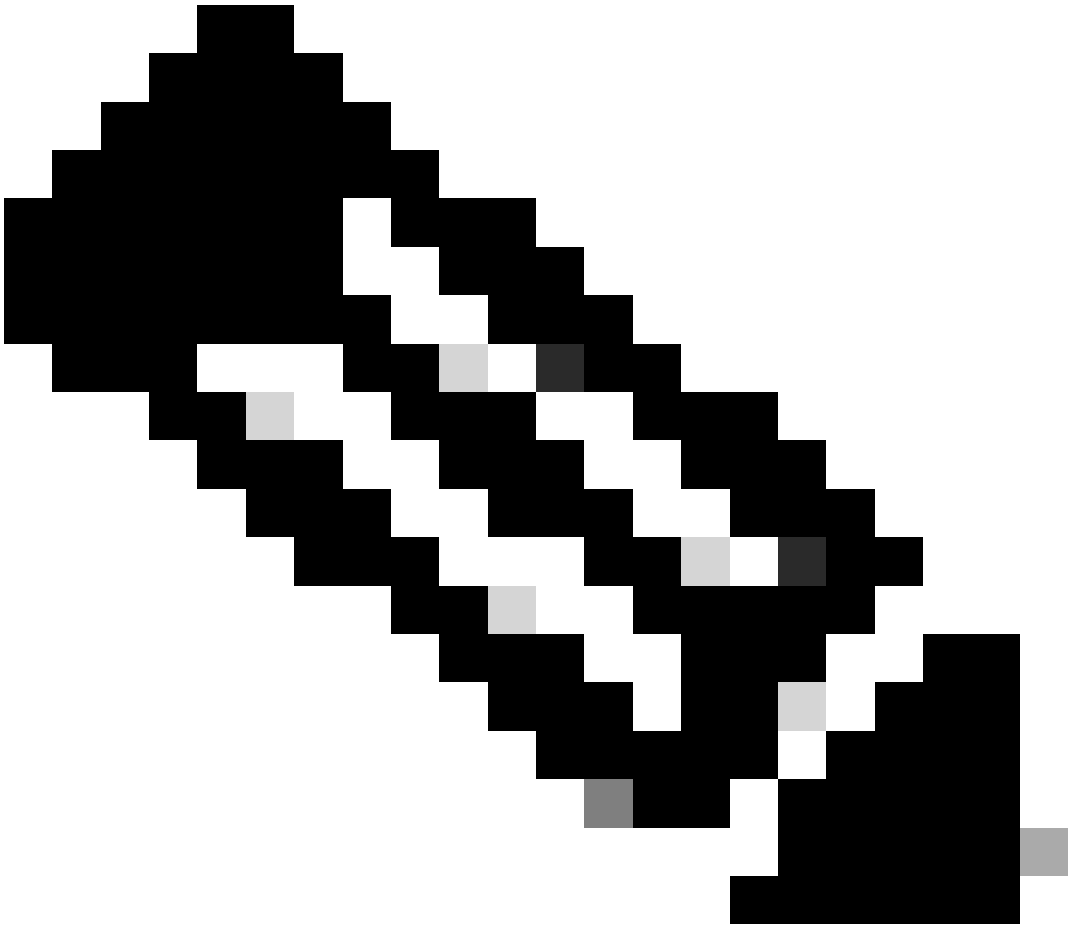


ملاحظة: على سبيل المثال، يتم إستخدام شبكة IP الفرعية 10.197.179.0/24 كشبكة فرعية لشبكة محلية (LAN)، ويمكن أن يختلف هذا في بيئة الشبكة الفعلية حسب بنية الشبكة.

الخطوة 2: قم بتسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) الخاصة ب SMC وانتقل إلى تكوين > اكتشاف > إدارة المجموعة المضيفة > انقر فوق (...) بجانب البيئات المضيفة الخارجية وحدد إضافة مجموعة مضيف.

في هذا المثال، يتم إنشاء مجموعة مضيف جديدة باسم DNS الخاص بشركتي ضمن مجموعة المضيف الأصل من البيئات المضيفة الخارجية.

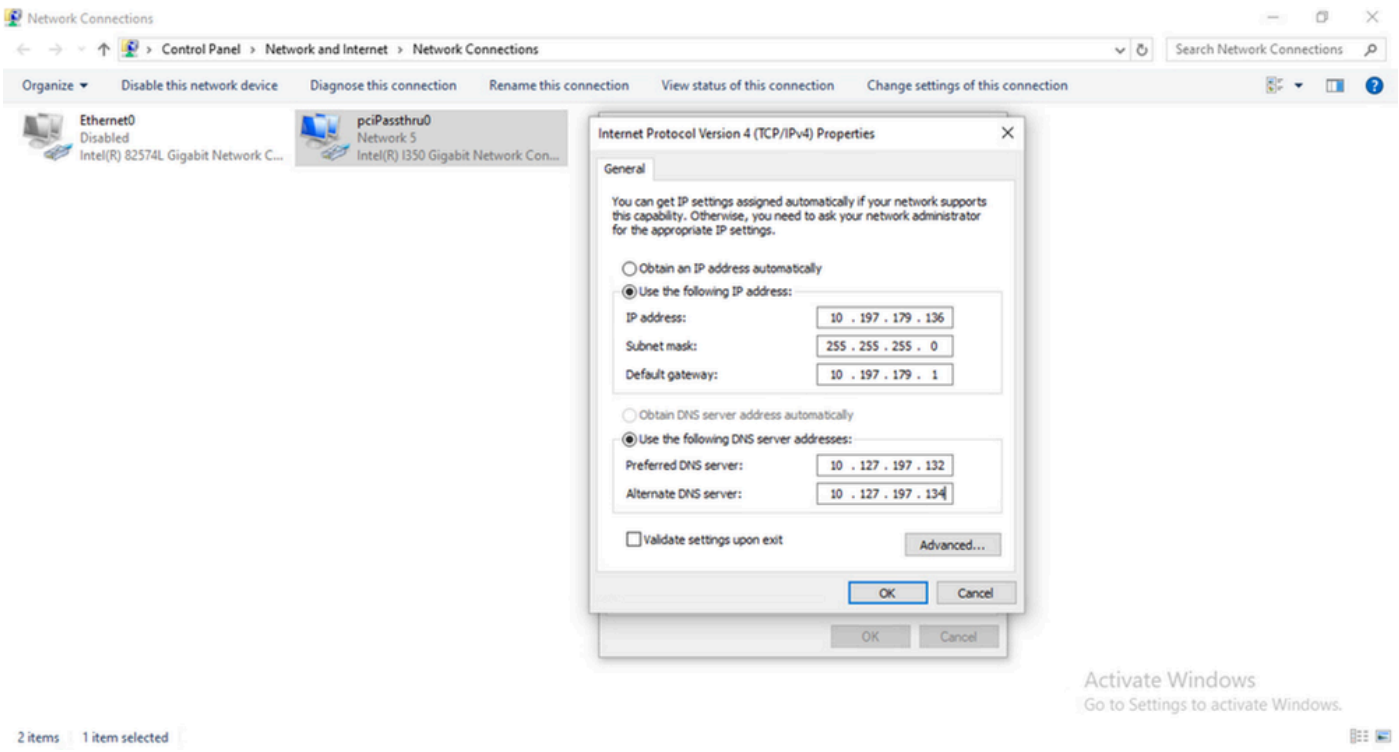




ملاحظة: على سبيل المثال، يتم إستخدام بروتوكولات IPs 10.127.197.132 و

10.127.197.134 كخوادم DNS المطلوبة التي يتم إستخدامها من قبل المستخدمين النهائيين، ويمكن أن يختلف هذا في بيئة الشبكة الفعلية حسب بنية الشبكة.

يتم تكوين كمبيوتر مختبر الاختبار المستخدم للعرض التوضيحي باستخدام IP الثابت و DNS (ينتمي إلى مجموعة مضيف الشبكات الموثوق بها التي تم إنشاؤها) 10.197.179.136 و 10.127.197.134 (ينتمي إلى مجموعة مضيف DNS الخاصة بي التي تم إنشاؤها).



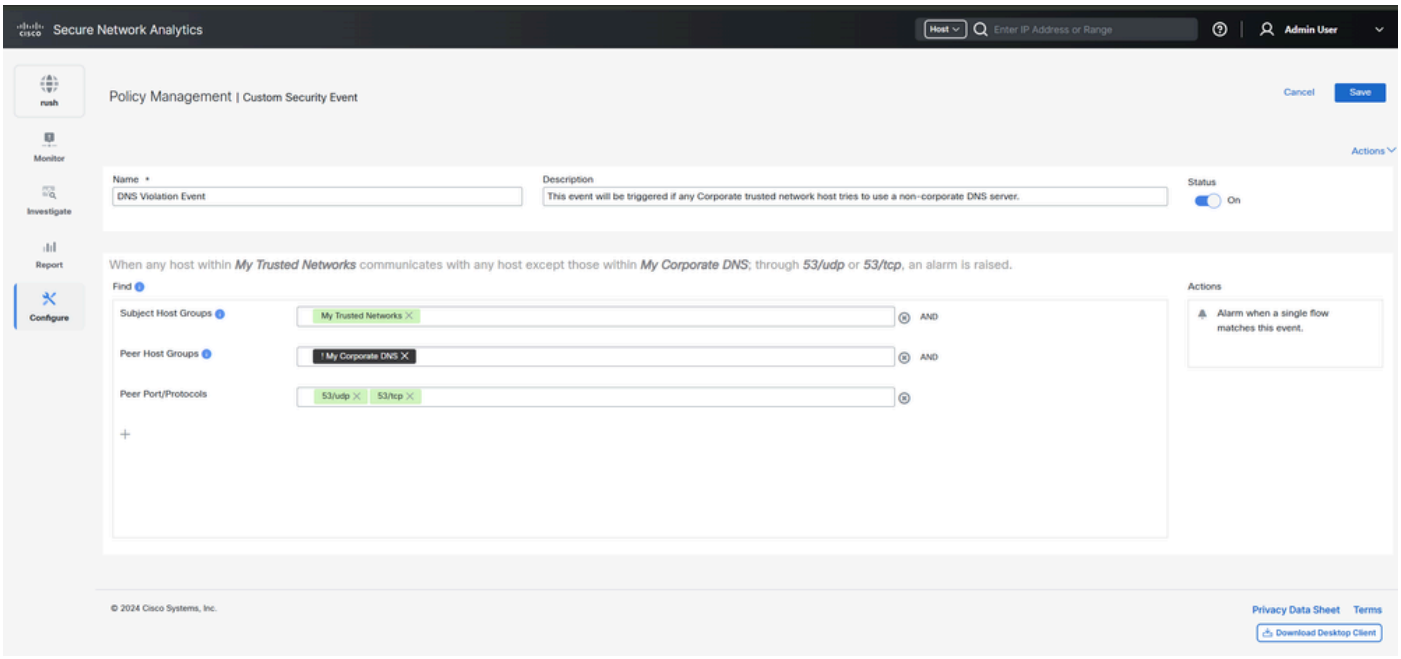
الخطوة 3: قم بإعداد نظام تنبيه مخصص لاكتشاف متى يتصل المستخدمون الداخليون بخوادم DNS الخارجية، مما يطلق إذا لحظر الاتصالات بخوادم DNS غير المعتمدة التي قد تعيد توجيه حركة مرور البيانات إلى مواقع خارجية ضارة. وبمجرد تنشيط تنبيه، تنسق تحليلات الشبكة الآمنة من Cisco مع Cisco ISE لعزل المضيف باستخدام خوادم DNS غير المصرح بها هذه باستخدام سياسة التحكم في الشبكة القابلة للتكيف عبر PxGrid.

انتقل إلى التكوين > إدارة السياسة.

إنشاء أحداث مخصصة باستخدام المعلومات:

- الاسم: حدث انتهاك DNS.
- مجموعات مضيف الموضوع: الشبكات الموثوق بها الخاصة بي.
- مجموعات الأجهزة المضيفة النظيرة : (لا) DNS الخاص بشركتي.
- منفذ/بروتوكولات النظير : 53/UDP 53/TCP

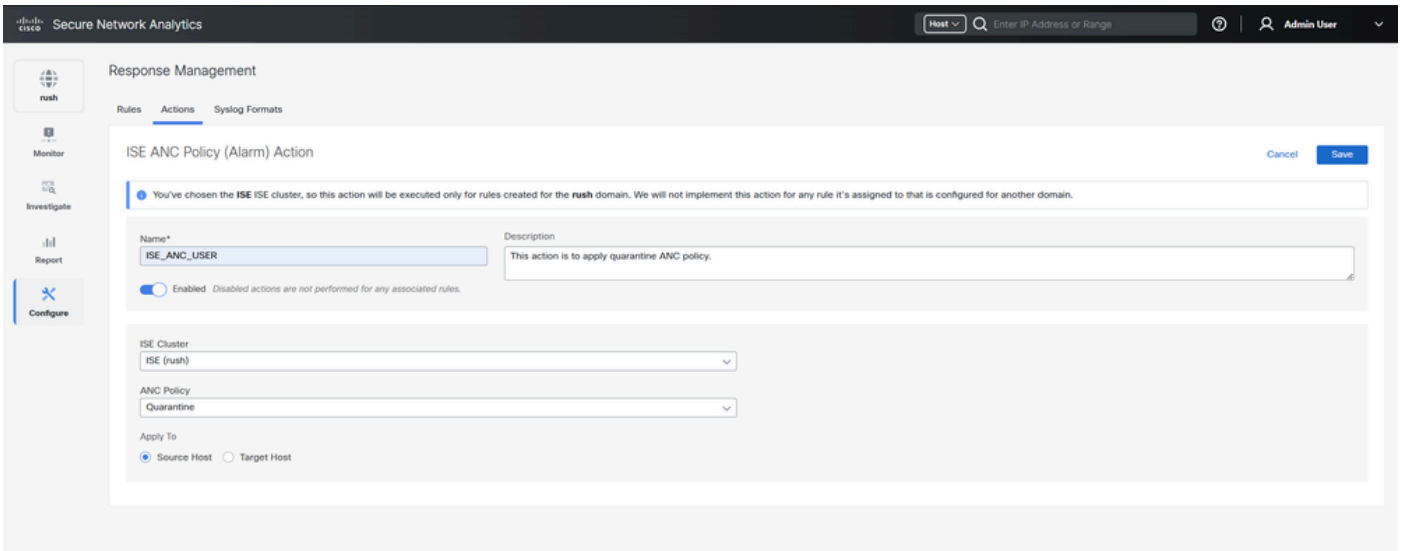
وهذا يعني أنه عندما يتصل أي مضيف ضمن شبكاتي الموثوقة (المجموعة المضيفة) بأي مضيف باستثناء الموجود ضمن DNS الخاص بمؤسستي (المجموعة المضيفة) من خلال 53/up أو 53/tcp، ينشأ تنبيه.



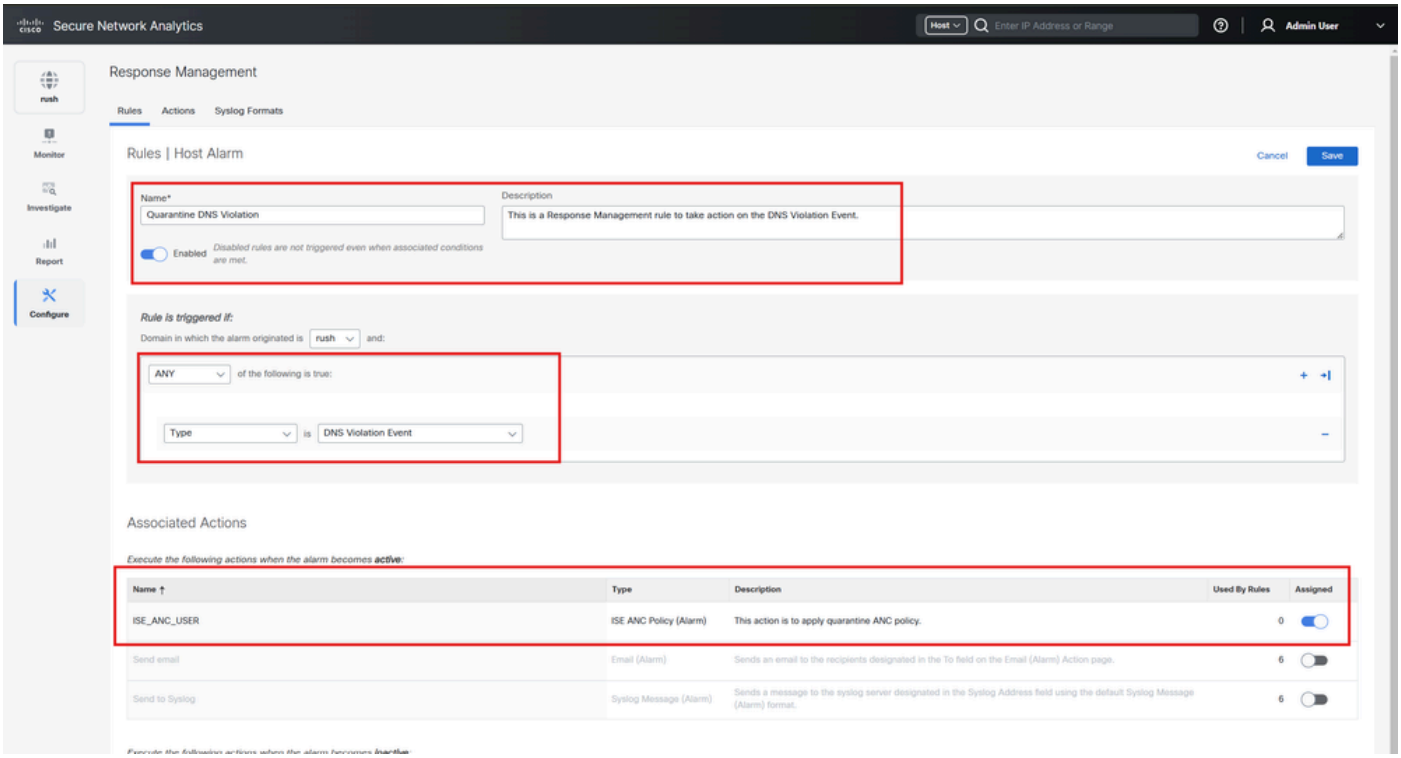
الخطوة 4: قم بتكوين إجراء إدارة إستجابة ليتم تنفيذه، والذي يمكن تطبيقه لاحقا على قاعدة إدارة الاستجابة بمجرد إنشائها.

انتقل إلى تكوين > إدارة الاستجابة>الإجراءات، وانقر على إضافة إجراء جديد وحدد ISE ANC Policy (Alarm).

قم بتعيين اسم واختر مجموعة Cisco ISE المحددة التي سيتم إخطارها من أجل تنفيذ سياسة عزل لأي انتهاكات أو إتصالات بالخوادم غير المعتمدة.



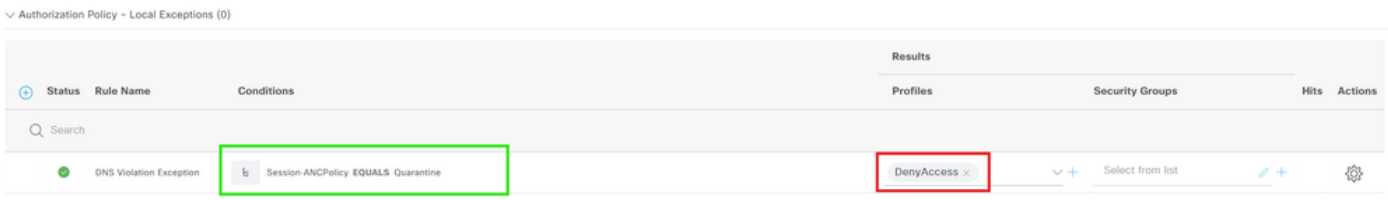
الخطوة 5: ضمن قسم القواعد، قم بإنشاء قاعدة جديدة. تفرض هذه القاعدة الإجراء المحدد مسبقا عندما يحاول مضيف ضمن الشبكة الداخلية إرسال حركة مرور DNS إلى خوادم DNS غير المعتمدة. في القاعدة يتم تشغيلها إذا كان المقطع، أختر النوع وحدد الحدث المخصص الذي تم إنشاؤه سابقا.
تحت الإجراءات المرتبطة، حدد إجراء تنبيه ISE ANC الذي تم تكوينه مسبقا.

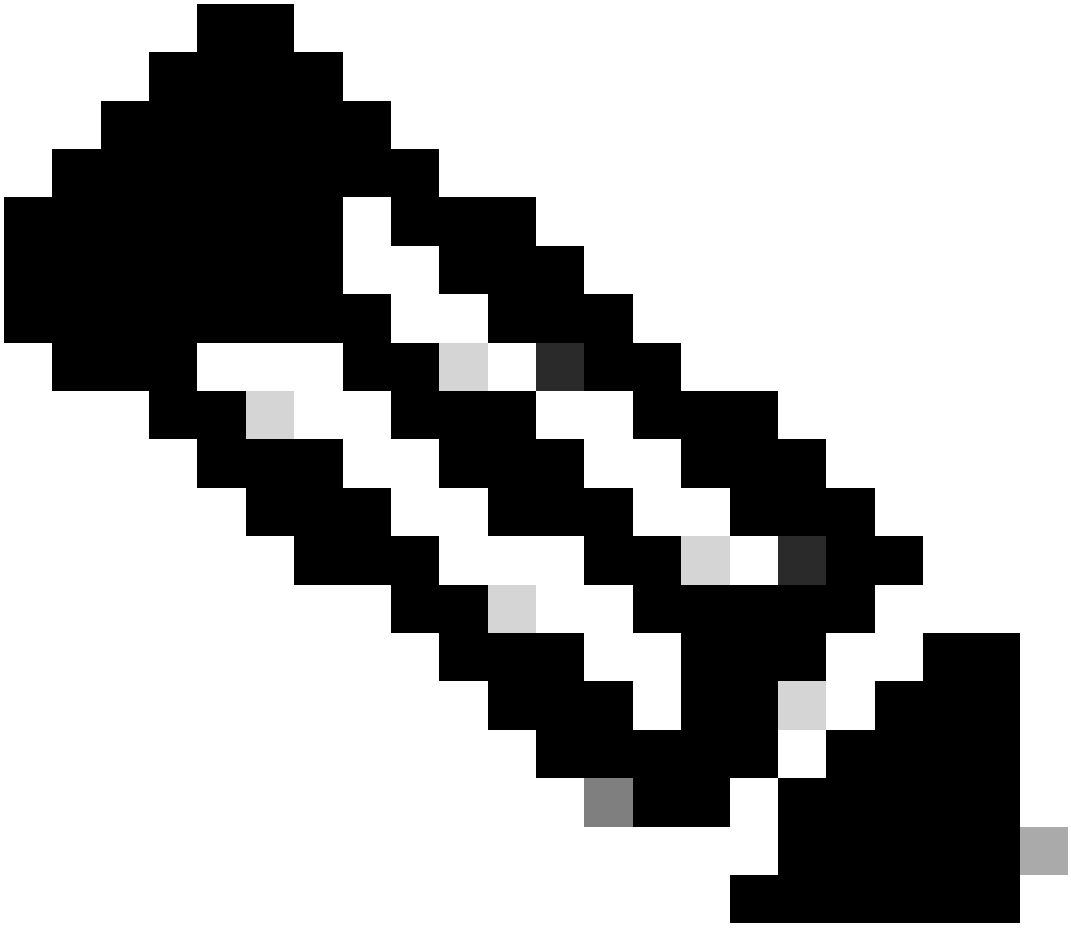


4. قم بتكوين Cisco ISE للاستجابة للإجراءات التي بدأها Stealthwatch عند إطلاق الحدث.

سجل الدخول إلى واجهة المستخدم الرسومية Cisco ISE وانتقل إلى السياسة > مجموعات السياسات > أختر مجموعة السياسات > ضمن سياسة التخويل - الاستثناءات المحلية > إنشاء سياسة جديدة.

- الاسم: إستثناء انتهاك DNS
- المعايير: جلسة العمل: ANCPolicy يساوي عزل
- ملفات تعريف التخويل: DenyAccess

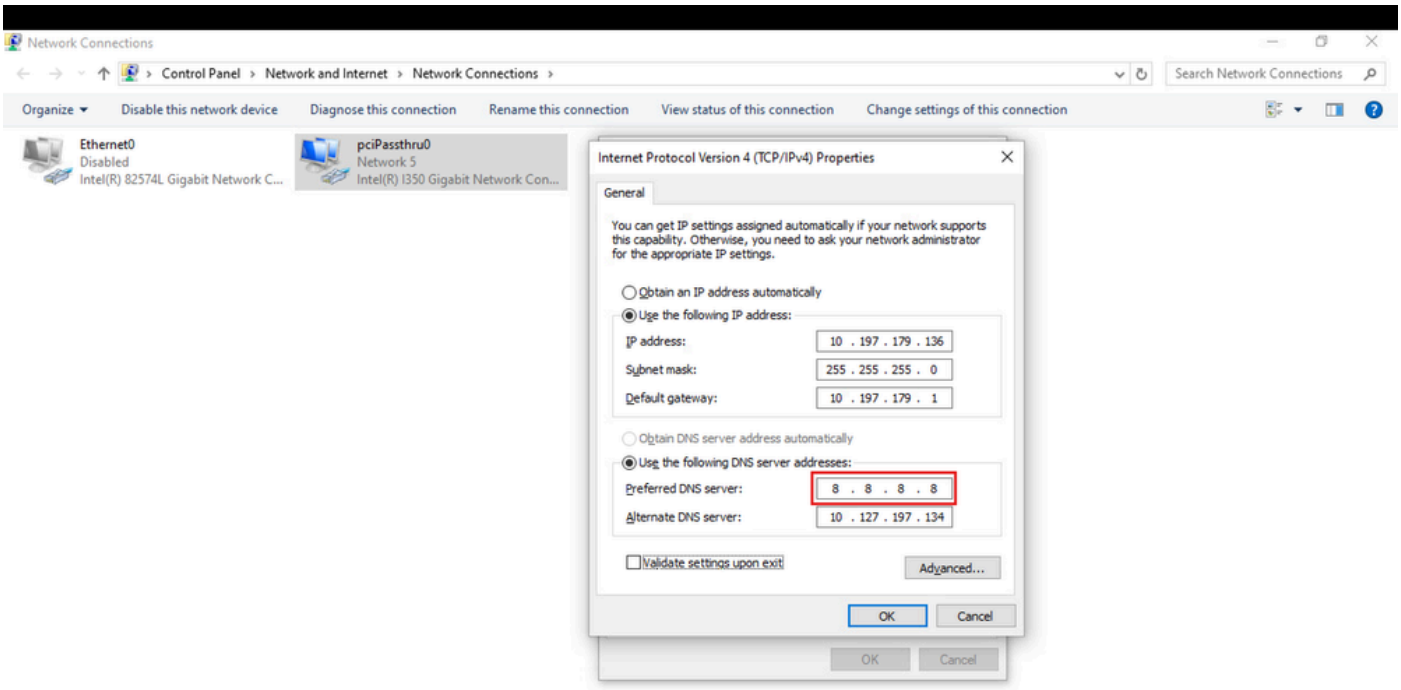




ملاحظة: في هذا المثال، بمجرد تشغيل حدث انتهاك DNS، يتم رفض الوصول إلى المستخدم استنادا إلى التكوين

التحقق من الصحة

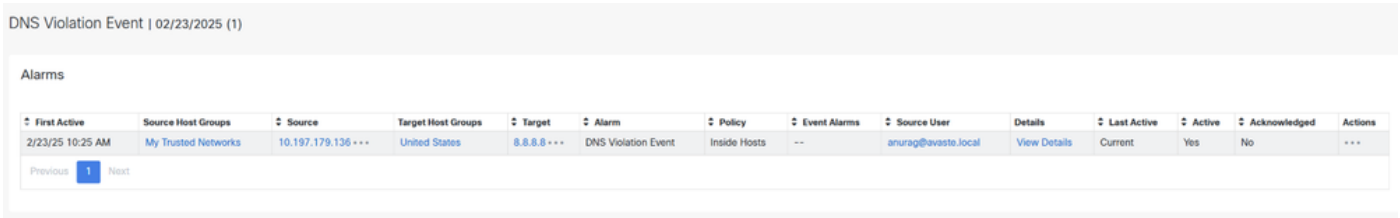
لتوضيح حالة الاستخدام، تم تغيير إدخال DNS على نقطة النهاية إلى 8.8.8.8، والذي يؤدي إلى تشغيل حدث انتهاك DNS الذي تم تكوينه . نظرا لأن خادم DNS ال ينتمي إلى المجموعة المضيفة لخوادم DNS الخاصة بالشركة، فإنه يشغل الحدث مما يؤدي إلى رفض الوصول إلى نقطة النهاية.



على المحول C9300، تحقق باستخدام ذاكرة التخزين المؤقت show flow monitor ipV4_NETFLOW | في الأمر 8.8.8.8 مع الإخراج للاطلاع على التدفقات التي يتم التقاطها وإرسالها إلى مجمع التدفق. يتم تكوين IPv4_NETFLOW في تكوين المحول.

```
<#root>

IPV4 SOURCE ADDRESS:

10.197.179.136


IPV4 DESTINATION ADDRESS:

8.8.8.8


TRNS SOURCE PORT:          62734
TRNS DESTINATION PORT:

53


INTERFACE INPUT:           Te1/0/46
IP TOS:                    0x00
IP PROTOCOL:               17
tcp flags:                 0x00
interface output:          Null
counter bytes long:        55
counter packets long:      1
timestamp abs first:       10:21:41.000
timestamp abs last:        10:21:41.000
```

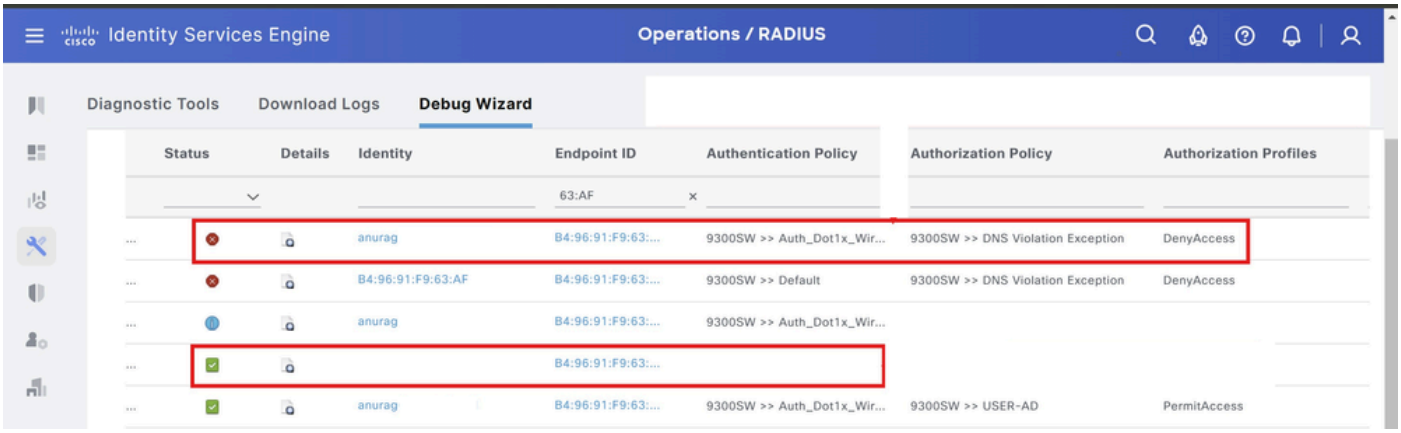
بمجرد تشغيل الحدث على Stealthwatch، انتقل إلى الشاشة > لوحة معلومات رؤية الأمان.



انتقل إلى الشاشة > التكامل > تعيينات سياسة ISE ANC.

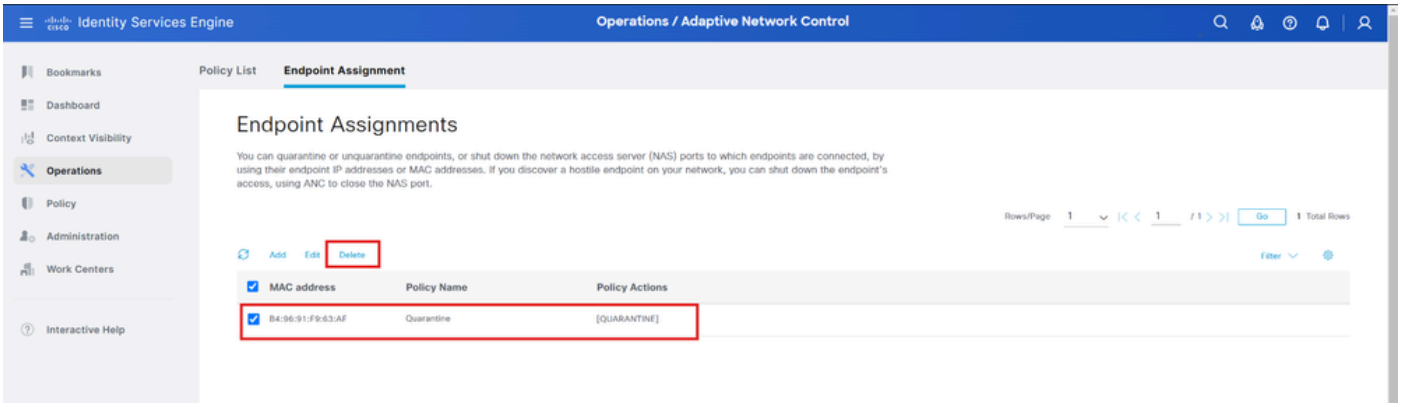
تأكد من أن تحليلات الشبكة الآمنة من Cisco نفذت بنجاح سياسة التحكم في الشبكة الفاصلة للتكيف عبر PxGrid و Cisco ISE لعزل المضيف.

بالمثل على Cisco ISE، انتقل إلى عمليات > RADIUS > أحياء وطبق مرشح لنقطة النهاية.



وفقا لإستثناء انتهاك DNS لنهج الاستثناء المحلي، يتم إصدار تغيير التفويض(CoA) من قبل ISE و Access ISE المرفوض إلى نقطة النهاية.

بمجرد تنفيذ إجراءات المعالجة على نقطة النهاية، قم بإزالة MAC من العمليات > التحكم في الشبكة المتكيفة > تعيينات نقطة النهاية > حذف لإزالة عنوان MAC الخاص بنقطة النهاية.



سجل مرجع على Cisco ISE.

السمات المضبوطة على مستوى TRACE لمكون (pxgrid-server.log) في Cisco ISE، راجع السجلات في ملف pxgrid-server.log.

<#root>

DEBUG [pxgrid-http-pool5][[]] cpm.pxgrid.ws.client.WsIseClientConnection -::::::617fffb27858402d9ff9658

RUNNING

","policyName":"

Quarantine

"}
TRACE [WsIseClientConnection-1162][[]] cpm.pxgrid.ws.client.WsEndpoint -::::::617fffb27858402d9ff9658b8

command=SEND

,headers=[content-length=123, trace-id=617fffb27858402d9ff9658b89a29f23, destination=/topic/com.cisco.i
TRACE [pxgrid-http-pool2][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -::::::617fffb27858402d9ff
TRACE [pxgrid-http-pool2][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -::::::617fffb2785840
TRACE [sub-sender-0][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -::::::617fffb27858402d9ff9658b8
DEBUG [RMI TCP Connection(1440)-10.127.197.128][[]] cpm.pxgrid.ws.client.WsIseClientConnection -::::::e

SUCCESS

","policyName":"

Quarantine

"}
TRACE [WsIseClientConnection-1162][[]] cpm.pxgrid.ws.client.WsEndpoint -::::::ef9ad261537846ae906d637d6

command=SEND

,headers=[content-length=123, trace-id=ef9ad261537846ae906d637d6dc1e597, destination=/topic/com.cisco.i
TRACE [pxgrid-http-pool5][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -::::::ef9ad261537846ae906
TRACE [pxgrid-http-pool5][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -::::::ef9ad261537846a
TRACE [sub-sender-0][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -::::::ef9ad261537846ae906d637d6

SUCCESS

","policyName":"

Quarantine

"}

استكشاف الأخطاء وإصلاحها

نقاط النهاية المعزولة لا تجدد تغيير ما بعد النهج للمصادقة

المشكلة

فشلت المصادقة نتيجة لتغيير النهج أو الهوية الإضافية ولم تتم إعادة المصادقة. تفشل المصادقة أو تظل نقطة النهاية المعنية غير قادرة على الاتصال بالشبكة. غالبا ما تحدث هذه المشكلة على أجهزة العميل التي تفشل في تقييم الوضع وفقا لسياسة

الوضع التي تم تعيينها لدور المستخدم.

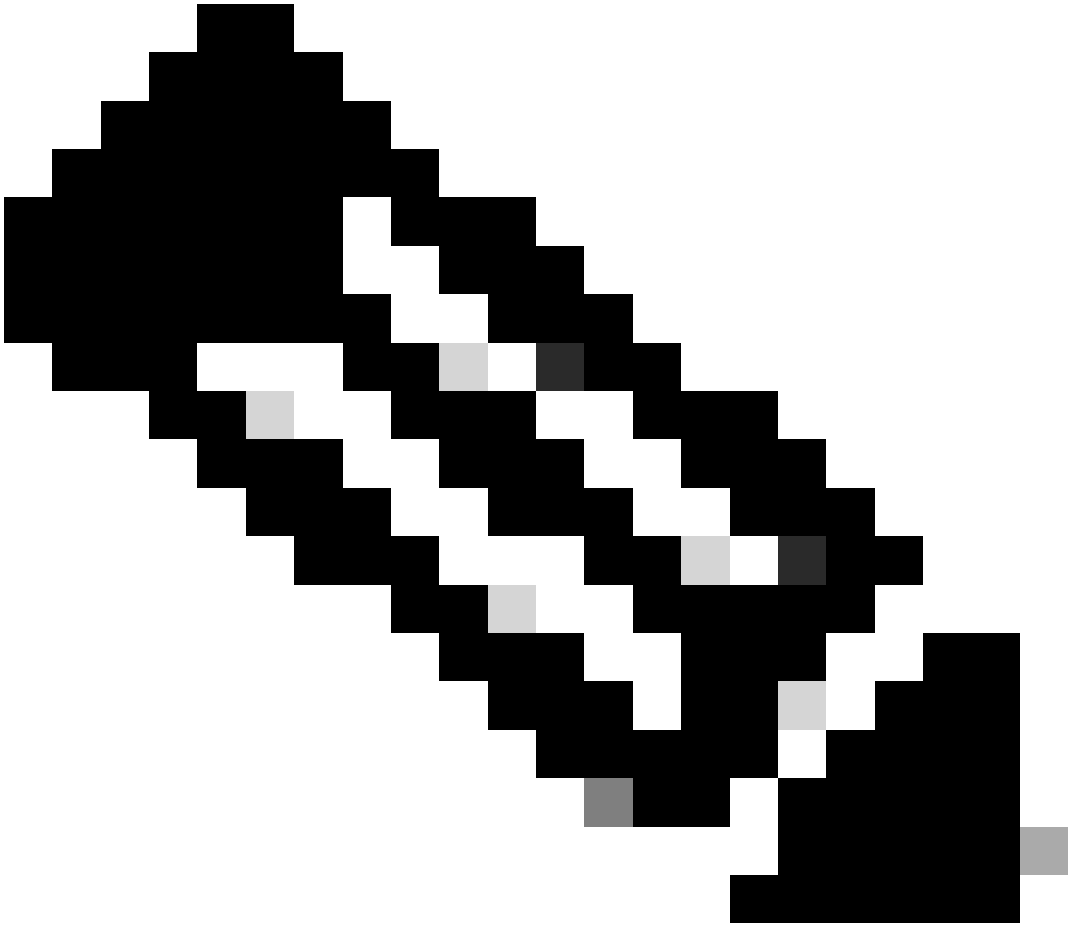
الأسباب المحتملة

لم يتم تعيين إعداد مؤقت المصادقة بشكل صحيح على جهاز العميل، أو لم يتم تعيين الفاصل الزمني للمصادقة بشكل صحيح على المحول.

الحل

وهناك العديد من القرارات المحتملة لهذه القضية:

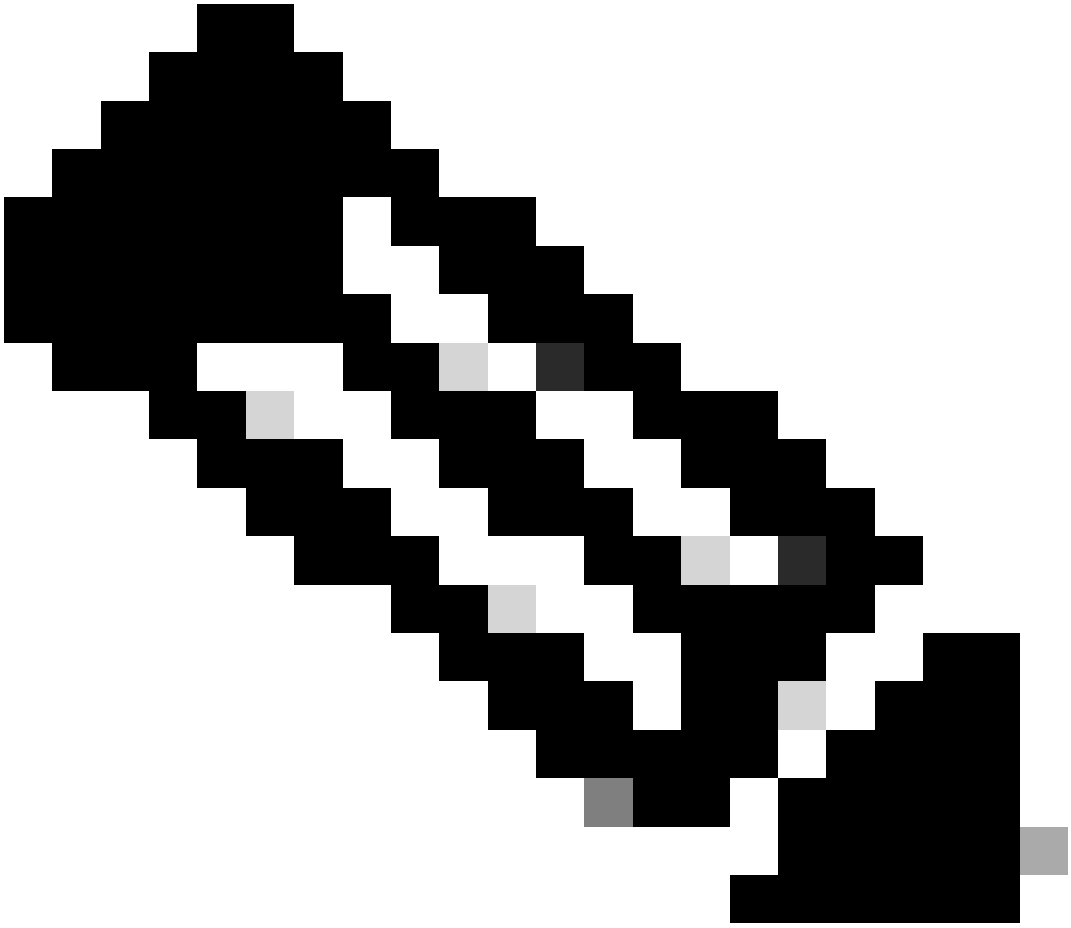
1. تحقق من Session Status SummaryReport في Cisco ISE لـ NAD المحدد أو مفتاح، وتأكد أن القارن يتلقى فترة المصادقة المناسبة لشكل.
2. أدخل show running configuration على NAD/switch وتأكد من تكوين الواجهة باستخدام إعداد إعادة تشغيل مؤقت المصادقة المناسب. (على سبيل المثال، إعادة تشغيل مؤقت المصادقة 15، وإعادة مصادقة مؤقت المصادقة 15).
3. دخلت قارن إيقاف عمل وما من إيقاف عمل أن يثبت المينا على NAD/مفتاح ويفرض إعادة مصادقة واحتمال تشكيل تغيير في cisco ISE.



ملاحظة: لأن CoA يتطلب عنوان MAC أو معرف جلسة، فمن المستحسن ألا ترتد المنفذ الذي يتم عرضه في تقرير SNMP لجهاز الشبكة.

تفشل عمليات ANC عند عدم العثور على عنوان IP أو عنوان MAC

يفشل ANCoperation التي تقوم بتنفيذها على نقطة نهاية عندما لا تحتوي جلسة نشطة لنقطة النهاية تلك على معلومات حول عنوان IP. ينطبق هذا أيضا على عنوان MAC ومعرف الجلسة لنقطة النهاية تلك.



ملاحظة: عندما تريد تغيير حالة التخويل لنقطة نهاية من خلال ANC، يجب عليك توفير عنوان IP أو عنوان MAC لنقطة النهاية. إذا لم يتم العثور على عنوان IP أو عنوان MAC في الجلسة النشطة لنقطة النهاية، يمكنك رؤية رسالة الخطأ: "لم يتم العثور على جلسة عمل نشطة لعنوان MAC هذا أو عنوان IP أو معرف جلسة العمل".

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).