在ISE 3.3和Stealthwatch 7.5.1上配置ANC

目录

简介

本文档介绍在Cisco ISE® 3.3版和Stealthwatch上配置快速威胁遏制（自适应网络控制）。

先决条件

思科建议了解以下主题：

- 身份服务引擎 (ISE)
- 平台交换网格(PxGrid)
- 安全网络分析(Stealthwatch)
- 快速遏制威胁（自适应网络控制 — ANC）。

在本文档中，假设思科身份服务引擎使用支持ANC的pxGrid与安全网络分析(Stealthwatch)集成。

使用的组件

本文档中的信息基于以下软件和版本：

- 思科身份服务引擎(ISE)版本3.3
- 安全网络分析(Stealthwatch)7.5.1
- Catalyst 9300

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

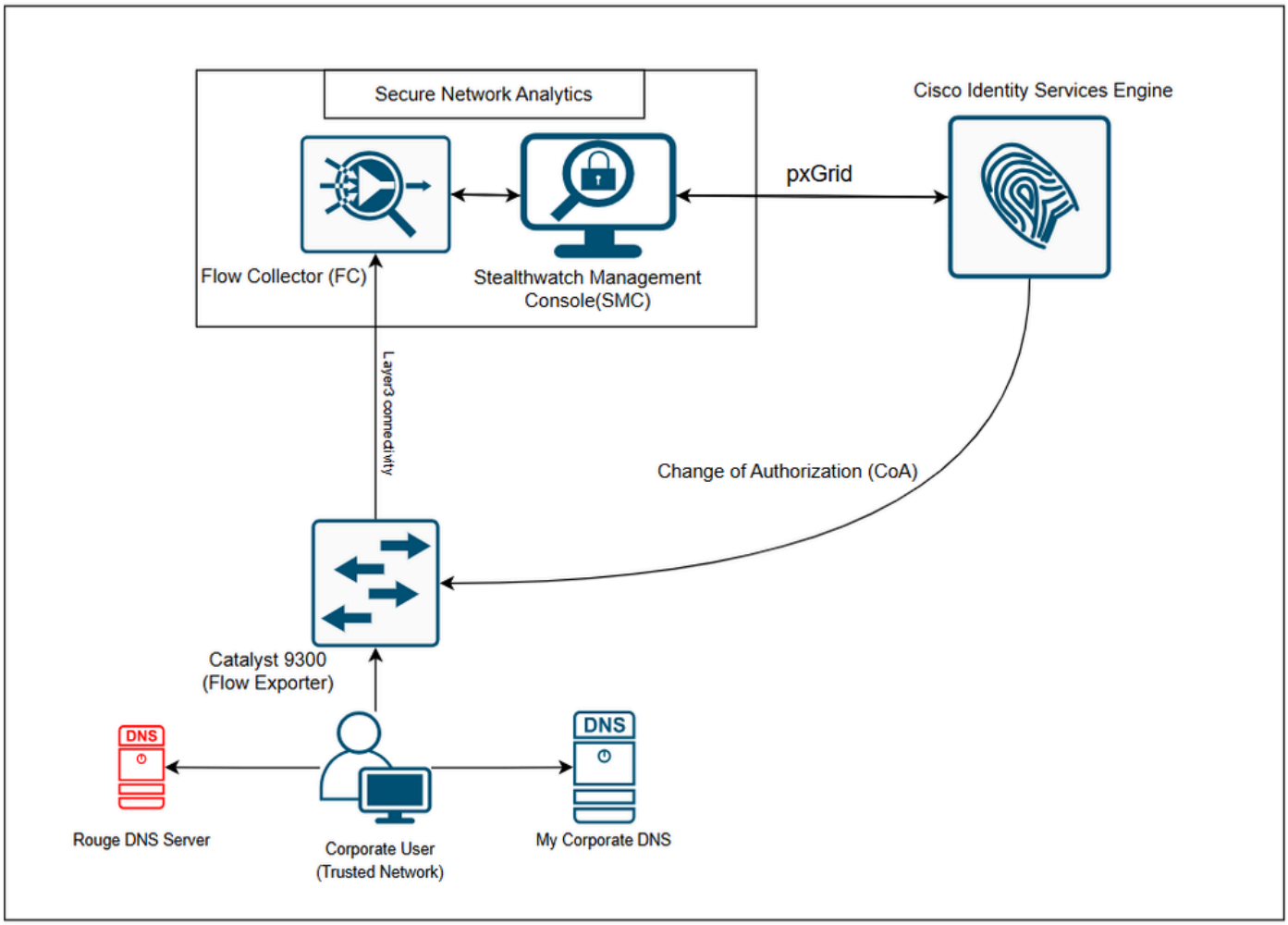
思科安全云分析（现已成为思科XDR的一部分）可以使用pxGrid从思科身份服务引擎(ISE)检索用户属性数据。此集成支持在Secure Cloud Analytics事件查看器中报告用户活动。

安全网络分析（以前称为Stealthwatch）和思科身份服务引擎(ISE)的组合可帮助组织获得360°的视野，更快地应对威胁，并保护不断增长的数字业务。安全网络分析检测到异常流量后，会发出警报，管理员可以选择隔离用户。pxGrid使安全网络分析能够将quarantine命令直接传递给身份服务引擎。

本示例介绍如何利用公司DNS服务器来防御互联网威胁。其目的是建立一个自定义警报机制，在内部用户连接到外部DNS服务器时触发该机制。此计划旨在阻止与未授权DNS服务器的连接，这些服务器可能会将流量重定向到有害的外部站点。

当触发警报时，思科安全网络分析与Cisco ISE协调，使用通过PxGrid的自适应网络控制策略隔离访问未授权DNS服务器的主机。

网络图



如图所示：

- 企业用户连接到C9300交换机，该交换机配置为导出IP流并将数据发送到流量收集器。
- 将同一企业用户配置为使用企业DNS服务器。
- 流量收集器与Stealthwatch管理控制台(SMC)集成
- Stealthwatch管理控制台(SMC)通过Pxgrid与ISE集成。

逐步配置

1.准备交换机以使用netflow来监控和导出流。

运行Cisco IOS® XE 17.15.01的C9300交换机的基本流配置

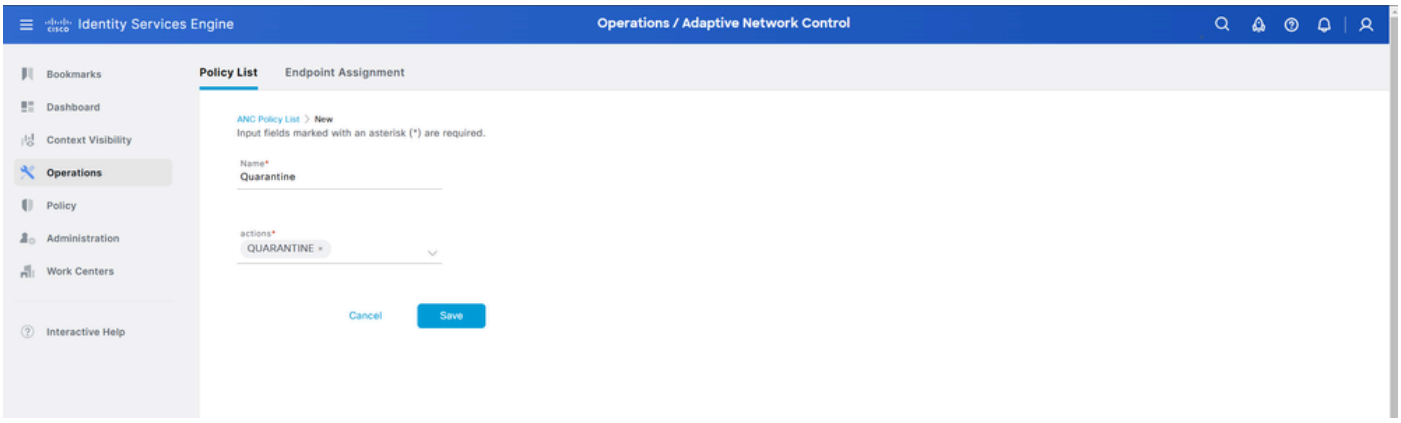
```
flow record SW_FLOW_RECORD
  description NetFlow record format to send to SW
  match ipv4 tos
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  match interface input
  collect transport tcp flags
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

完成配置后，它使C9300能够将IP流数据导出到流量收集器。然后，流量收集器处理此数据并将其传输到Stealthwatch管理控制台(SMC)，以进行分析和监控。

2. EnableAdaptive Network Control Cisco ISE。

默认情况下，ANC处于禁用状态。ANC仅在启用pxGrid时启用，并且保持启用状态，直到您在管理员门户中手动禁用该服务。

选择Operations > Adaptive Network Control > Policy List > Add，然后为Policy Name输入Quarantine，为Action输入Quarantine。

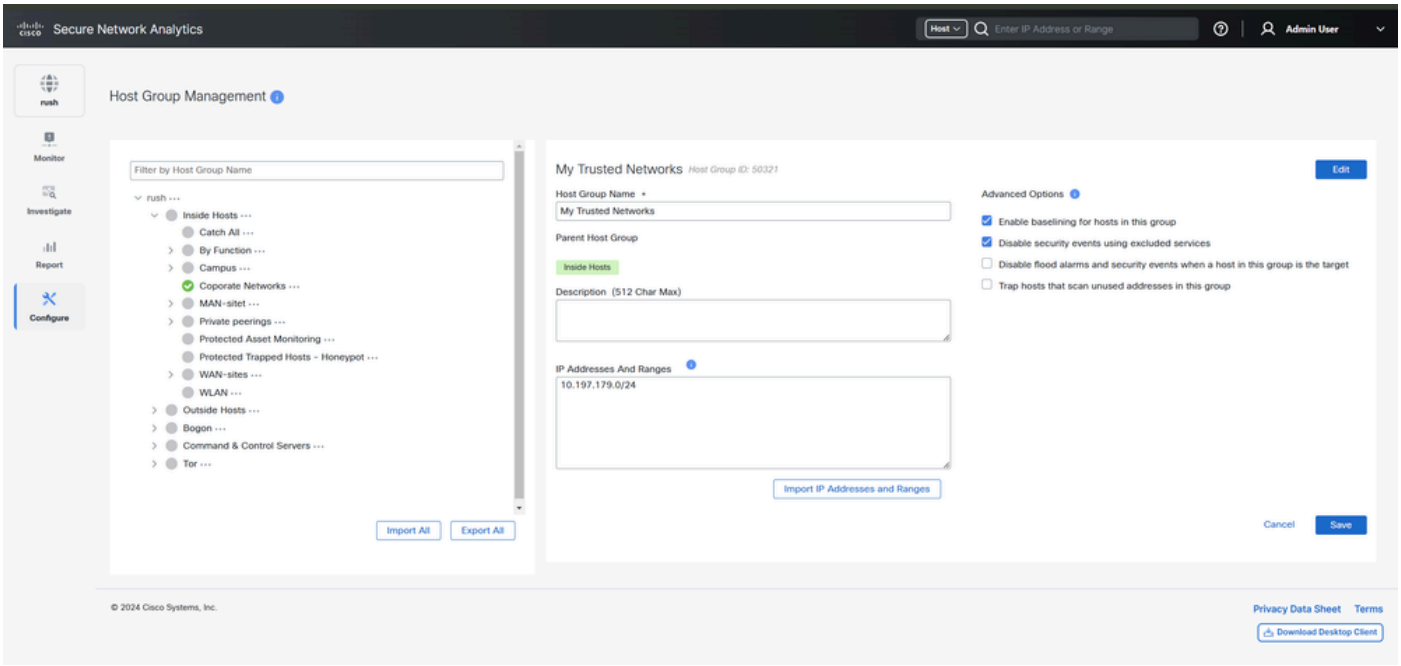


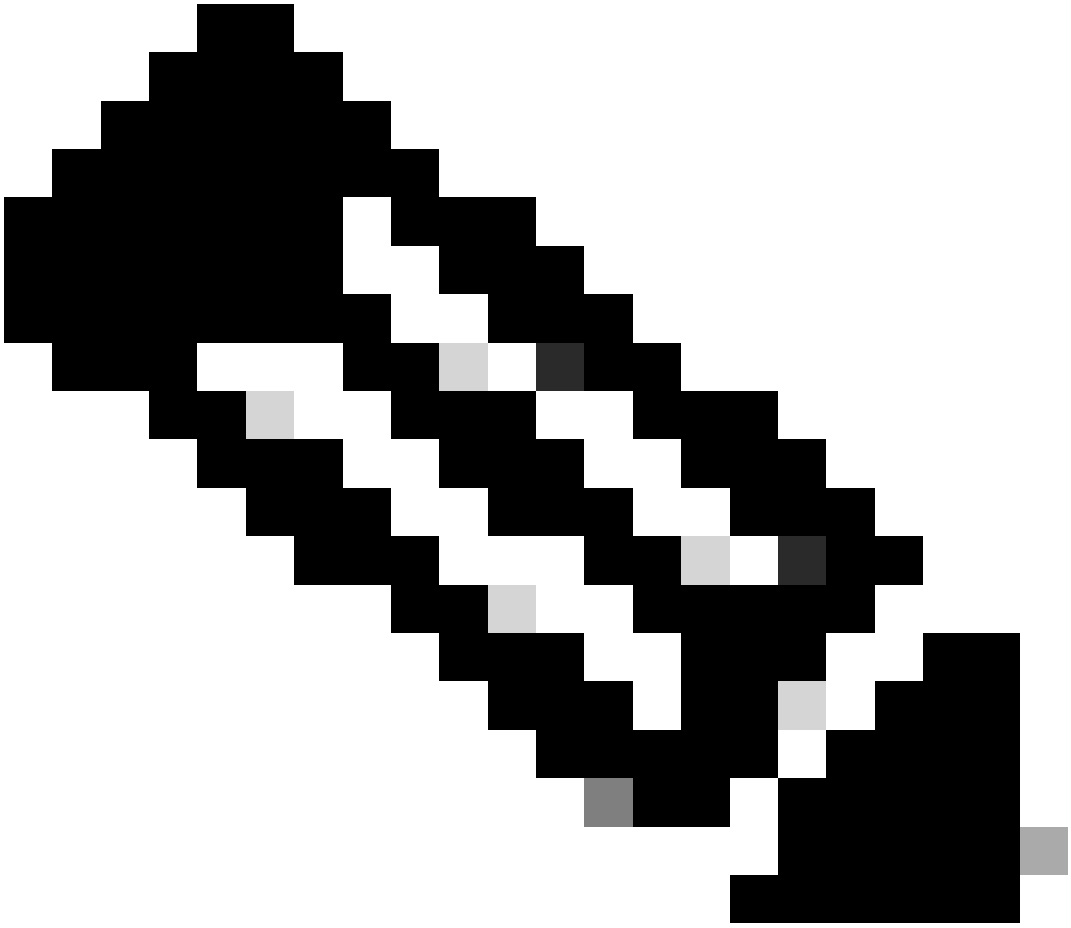
3.为事件触发和响应管理配置安全网络分析，以快速遏制威胁。

步骤 1：登录SMC GUI并导航至配置>检测>主机组管理>点击内部主机旁边的(...)（省略号）图标，然后选择添加主机组。

在本示例中，在Inside Hosts的父主机组下创建名为My Trusted Networks的新主机组。

通常可以将此网络分配给终端用户机器以监控DNS使用情况。

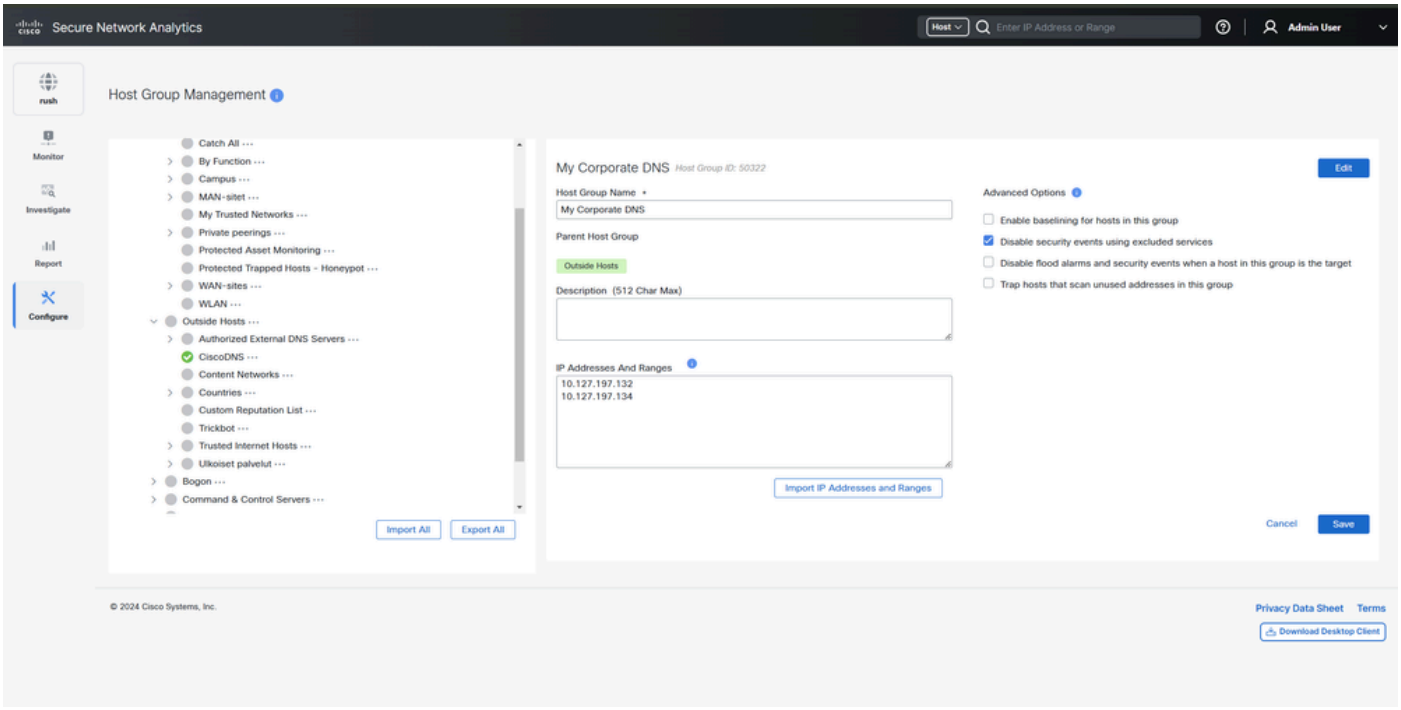


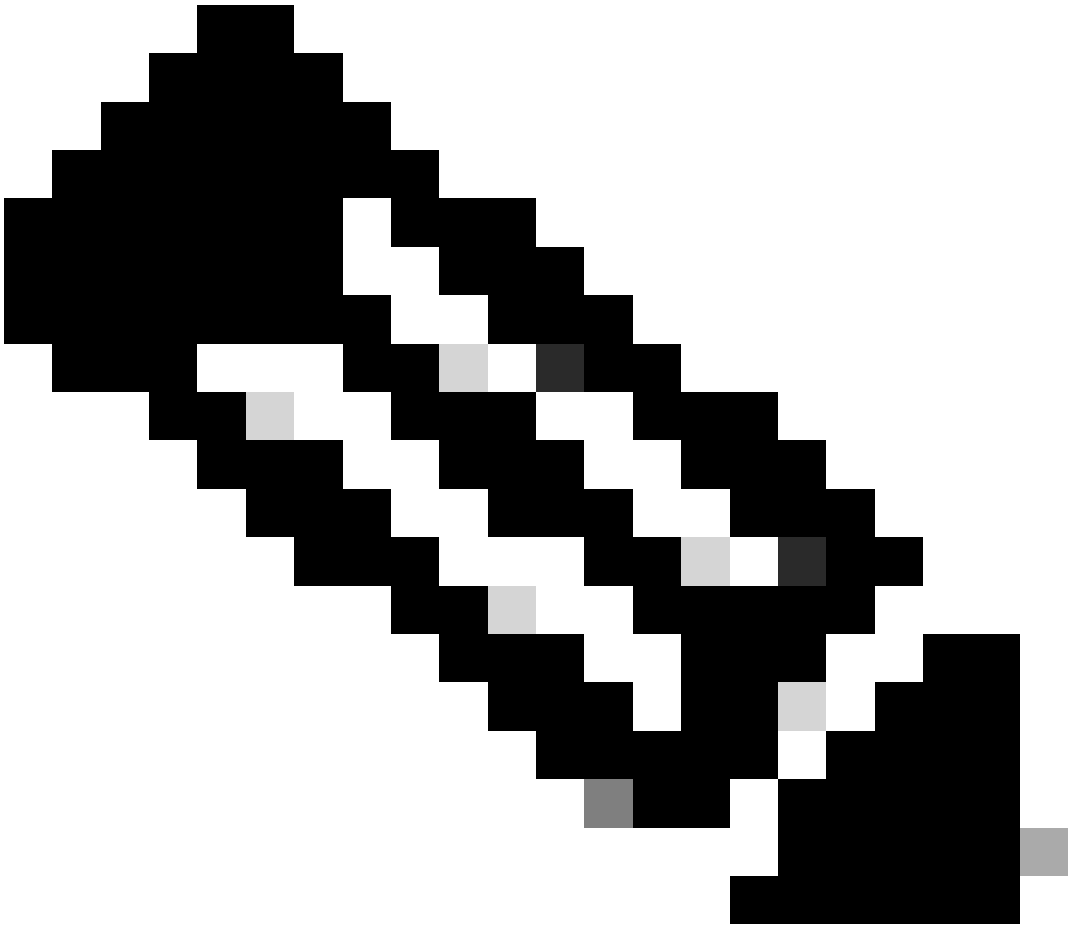


注意：在本例中，IP子网10.197.179.0/24用作局域网(LAN)子网。根据网络体系结构，这在实际网络环境中可能会有所不同。

步骤 2：登录SMC GUI并导航至配置>检测>主机组管理>点击(...)除外部主机外，然后选择添加主机组。

在本示例中，在Outside Hosts的父主机组下创建名为My Corporate DNS的新主机组。

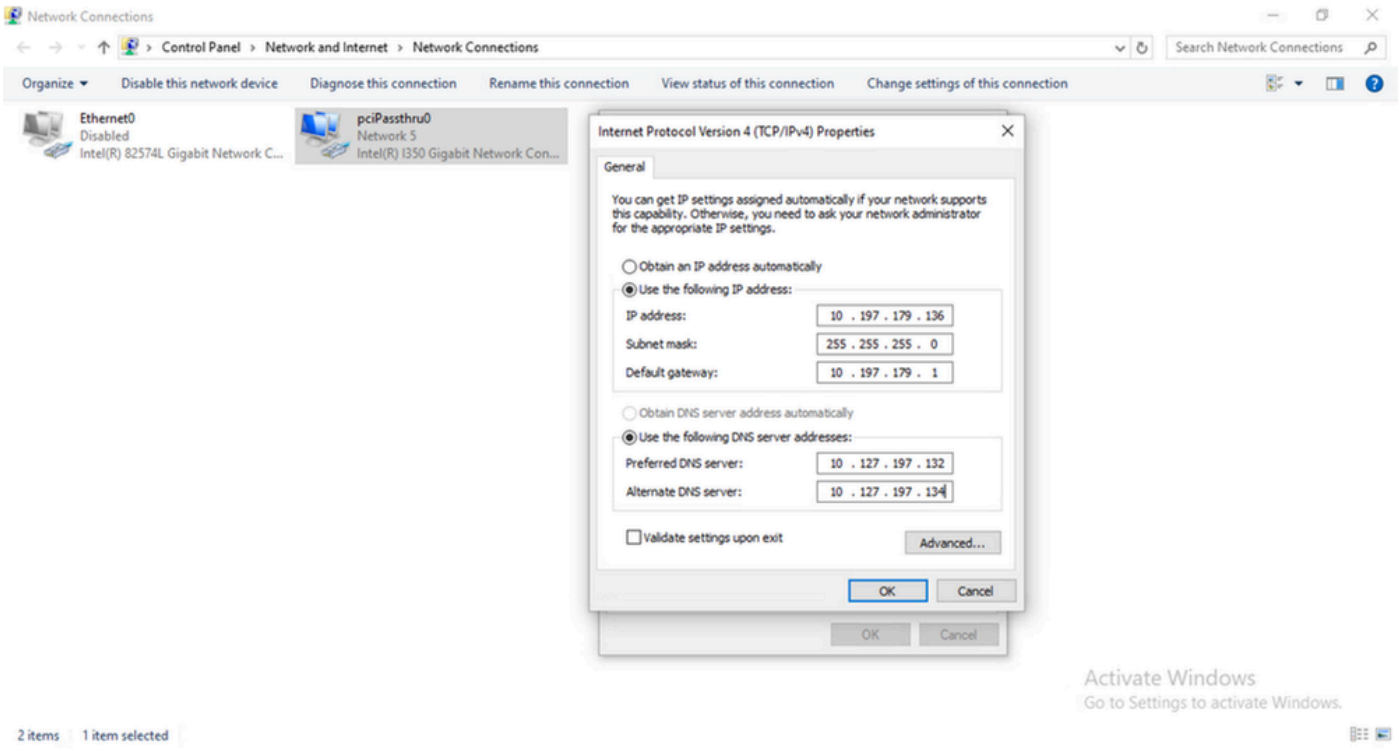




注意：在本例中，IP 10.127.197.132和10.127.197.134用作终端用户所需的DNS服务器

，这在实际网络环境中可能会有所不同，具体取决于网络体系结构。

用于演示的测试实验室PC配置了静态IP 10.197.179.136（属于创建的“我的受信任网络”主机组）和DNS 10.127.197.132和10.127.197.134（属于创建的“我的企业DNS”主机组）。



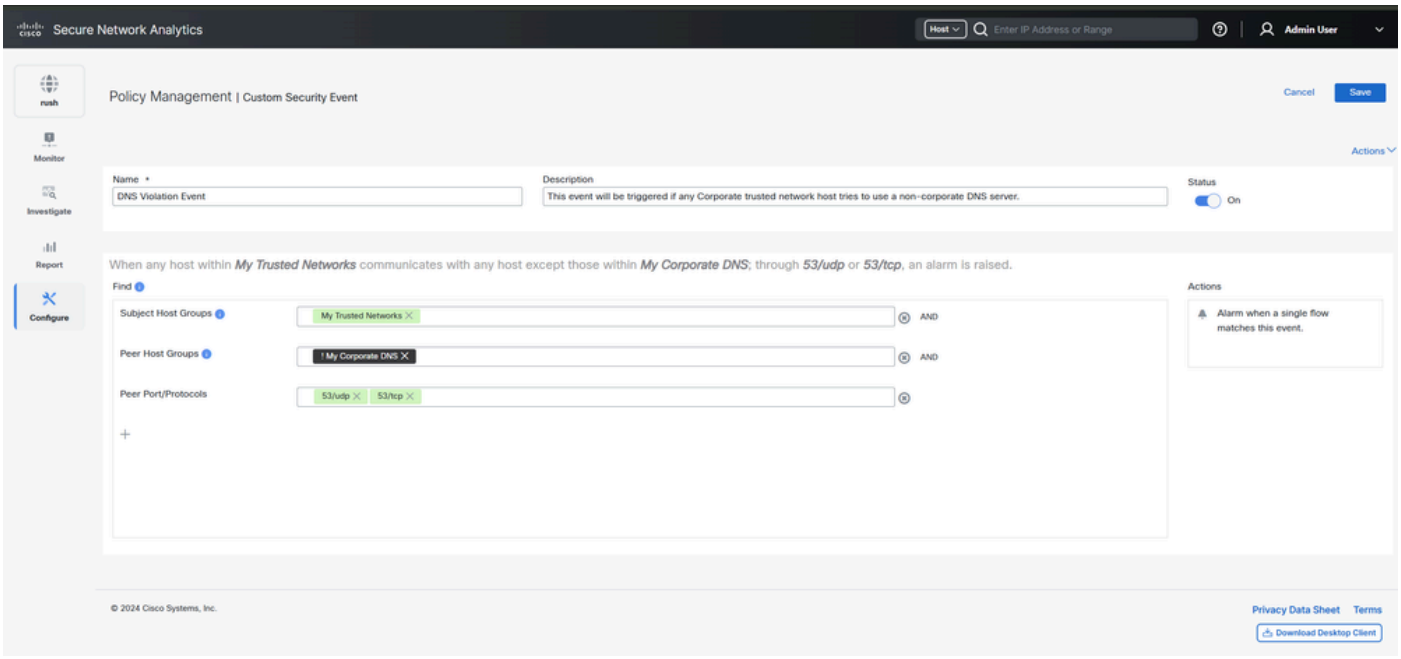
步骤 3：设置定制警报系统以检测内部用户何时连接到外部DNS服务器，触发警报以阻止与未授权DNS服务器的连接，这些服务器可能会将流量重定向到恶意外部站点。激活警报后，思科安全网络分析与Cisco ISE协调，通过PxGrid采用自适应网络控制策略，隔离使用这些未授权DNS服务器的主机。

导航到配置>策略管理。

使用以下信息创建自定义事件：

- 名称：DNS违规事件。
- Subject Host Groups:My Trusted Networks。
- 对等主机组:（非）我的公司DNS。
- 对等端口/协议:53/UDP 53/TCP

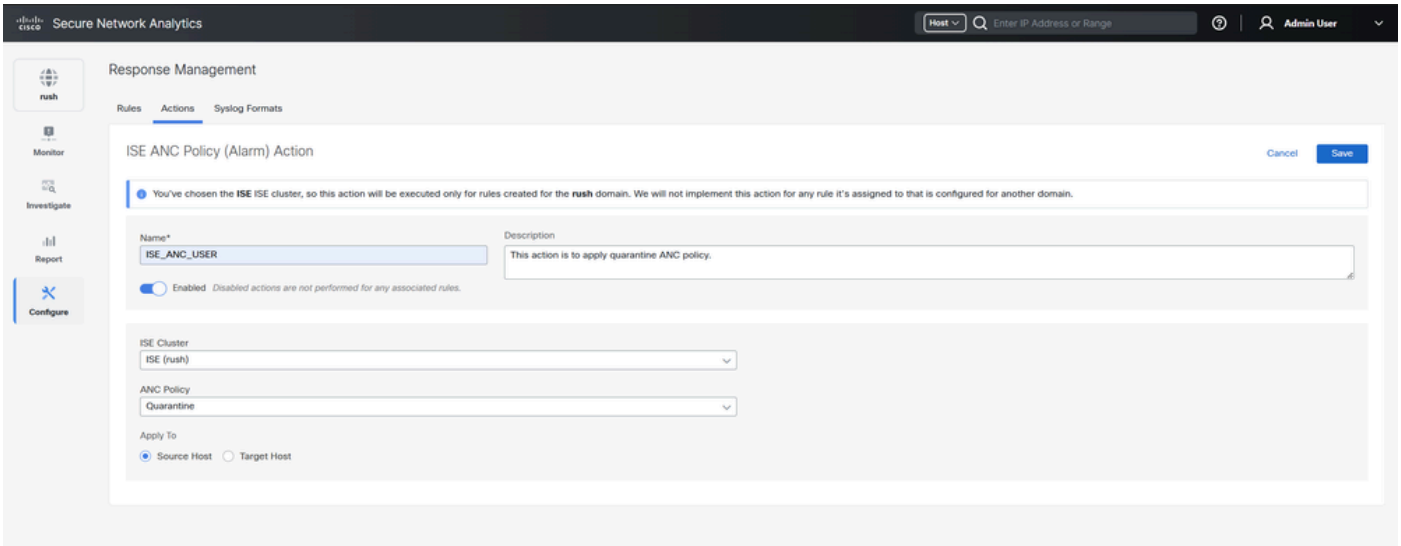
这意味着，当我的受信任网络（主机组）中的任何主机通过53/up或53/tcp与除我的公司DNS（主机组）中的主机外的任何主机通信时，将发出警报。



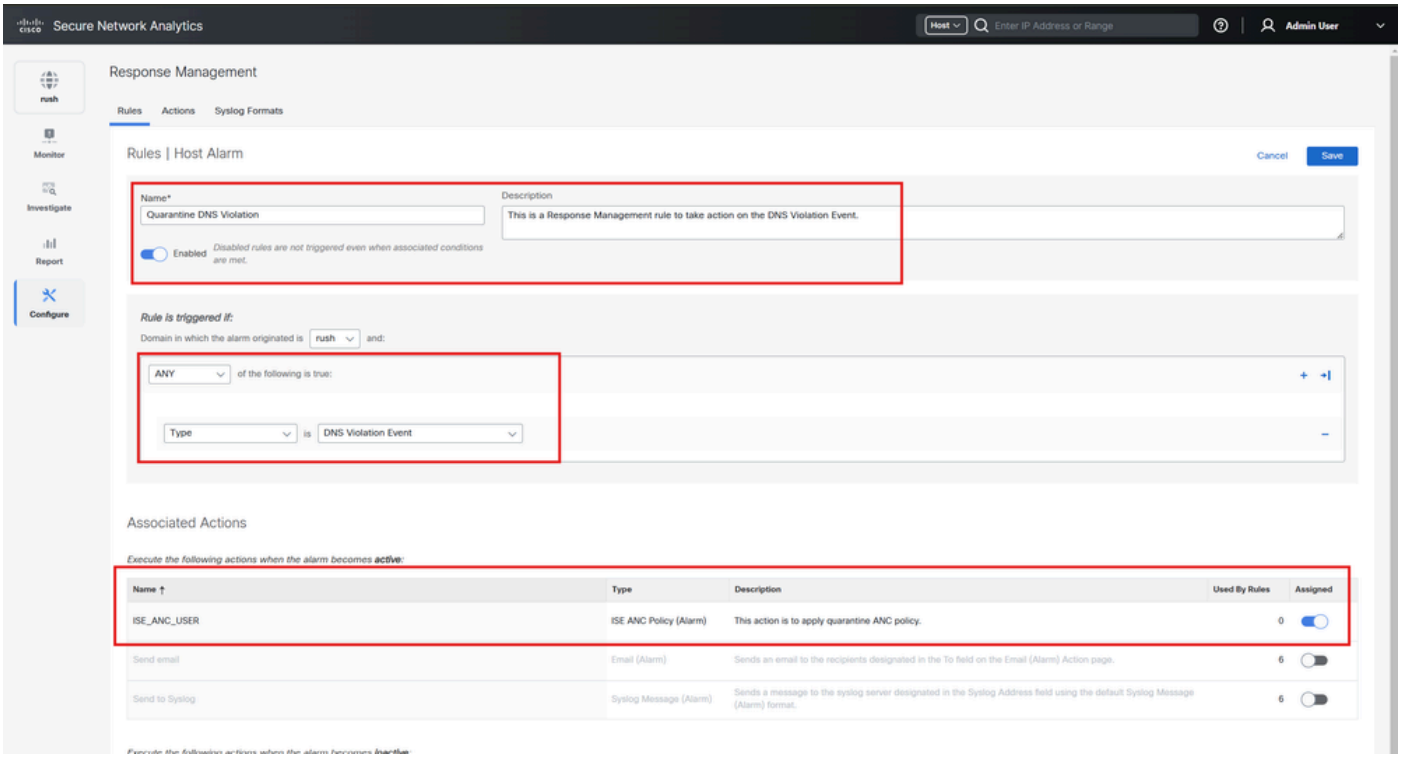
步骤 4：配置要执行的响应管理操作，该操作稍后可在创建后应用于响应管理规则。

依次导航到配置(Configure)>响应管理(Response Management)> 操作(Actions)，点击添加新操作(Add New Action)并选择ISE ANC策略（警报）(ISE ANC Policy(Alarm)。

分配名称并选择要通知的特定思科ISE集群，以便对任何违规或连接到未授权服务器实施隔离策略。



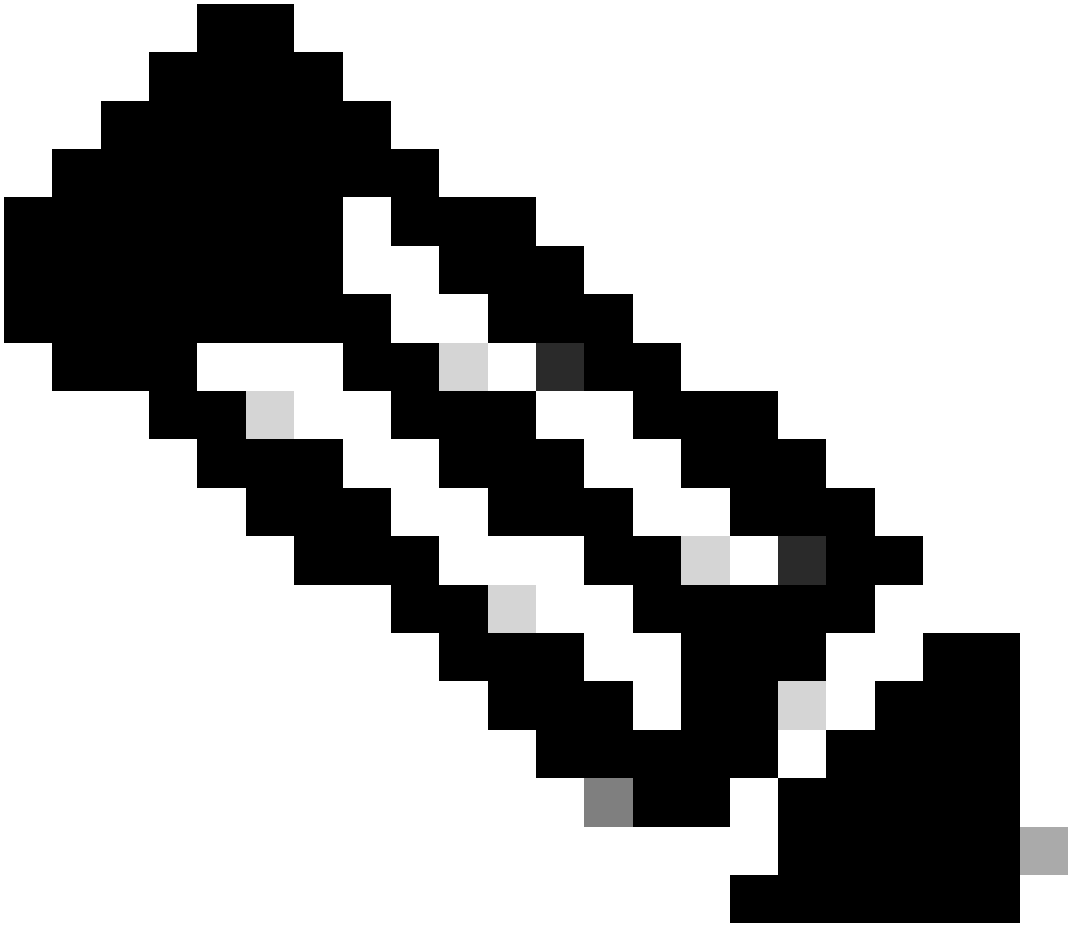
第5步：在Rules部分下，创建新规则。每当内部网络内的主机尝试向未授权的DNS服务器发送DNS流量时，此规则就会执行之前定义的操作。在Rule is triggered if部分中，选择Type，然后选择之前创建的自定义事件。
在Associated Actions下，选择之前配置的ISE ANC Alarm操作。



4.配置思科ISE以响应Stealthwatch在触发事件时启动的操作。

登录到Cisco ISE GUI并导航到Policy > Policy Sets > Choose the Policy set > under Authorization Policy - Local Exceptions > Create new Policy。

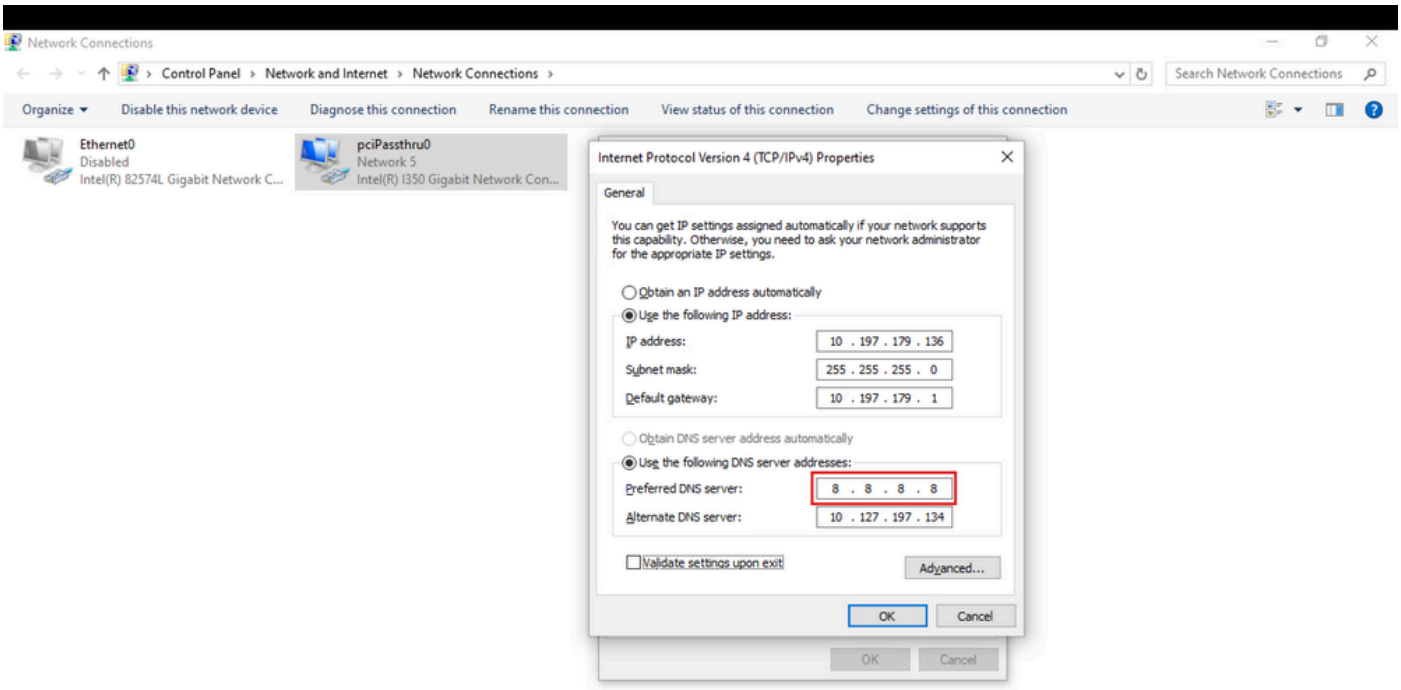
- 名称：DNS违规异常
- 条件:会话：ANCP策略等于隔离
- 授权配置文件：拒绝访问



注意：在本示例中，一旦触发了DNS违规事件，用户将根据配置拒绝访问

验证

为了演示使用案例，终端上的DNS条目已更改为8.8.8.8，这将触发配置的DNS违规事件。由于DNS服务器不属于我的公司DNS服务器的主机组，因此它会触发导致拒绝访问终端的事件。



在C9300交换机上，使用show flow monitor IPv4_NETFLOW cache进行验证 |在8.8.8.8命令中，输出用于查看流被捕获并发送到流量收集器。IPv4_NETFLOW在交换机配置中配置。

<#root>

IPV4 SOURCE ADDRESS:

10.197.179.136

IPV4 DESTINATION ADDRESS:

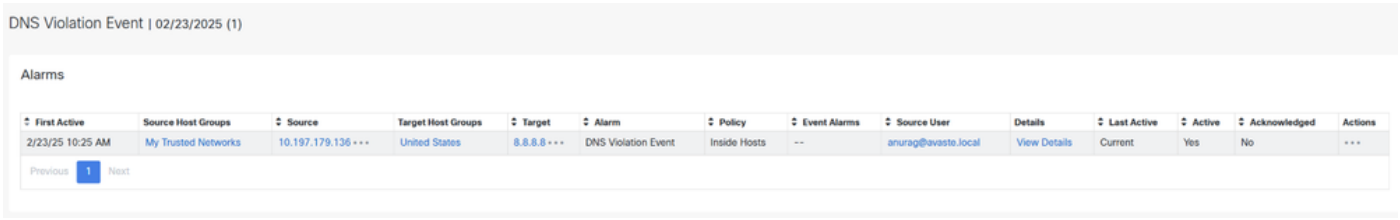
8.8.8.8

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

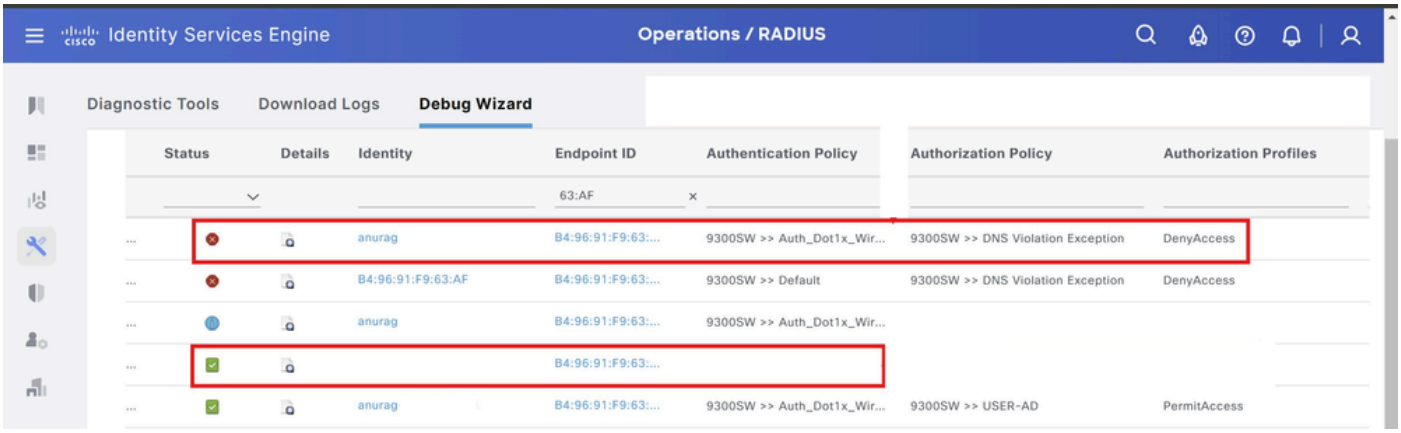
在Stealthwatch上触发事件后，请导航到Monitor > Security Insight Dashboard。



导航到监控>集成> ISE ANC策略分配。

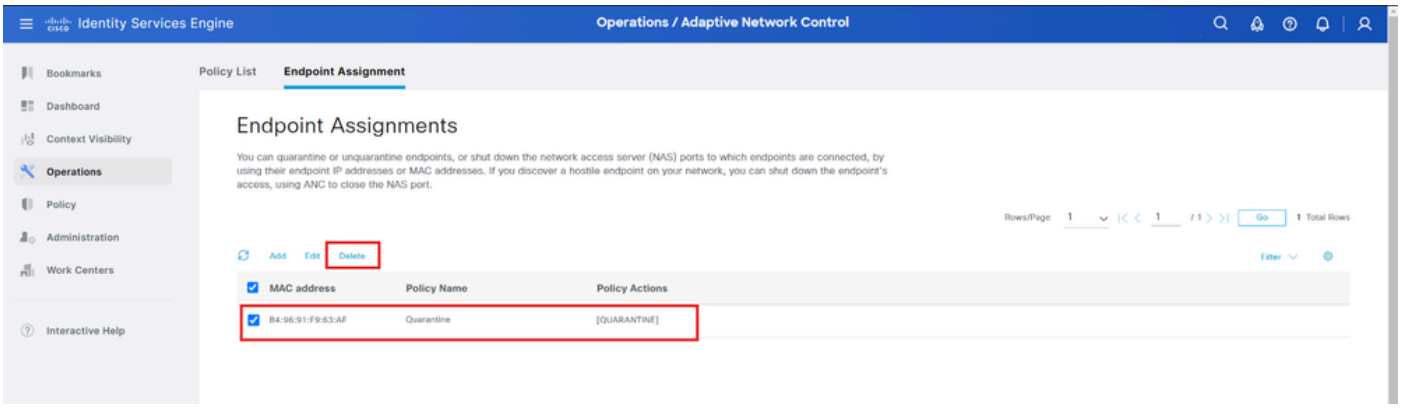
确保思科安全网络分析已成功通过PxGrid和思科ISE实施自适应网络控制策略以隔离主机。

类似地，在Cisco ISE上，导航到Operations > RADIUS > Livelogs并为终端应用过滤器。



根据本地例外策略DNS违规例外，授权更改(CoA)由ISE颁发，访问ISE被拒绝到终端。

对终端执行补救操作后，请从操作>自适应网络控制>终端分配>删除中删除MAC以删除终端的MAC地址。



思科ISE上的日志参考。

Cisco ISE上的pxgrid(pxgrid-server.log)组件的属性设置为TRACE级别，可在pxgrid-server.log文件中看到日志。

<#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

"}

故障排除

隔离的终端在策略更改后不更新身份验证

问题

身份验证失败，因为策略或其他身份发生了更改，并且未进行重新身份验证。身份验证失败，或者有问题的终端仍然无法连接到网络。此问题通常发生在根据分配给用户角色的终端安全评估策略未通过终端安全评估的客户计算机上。

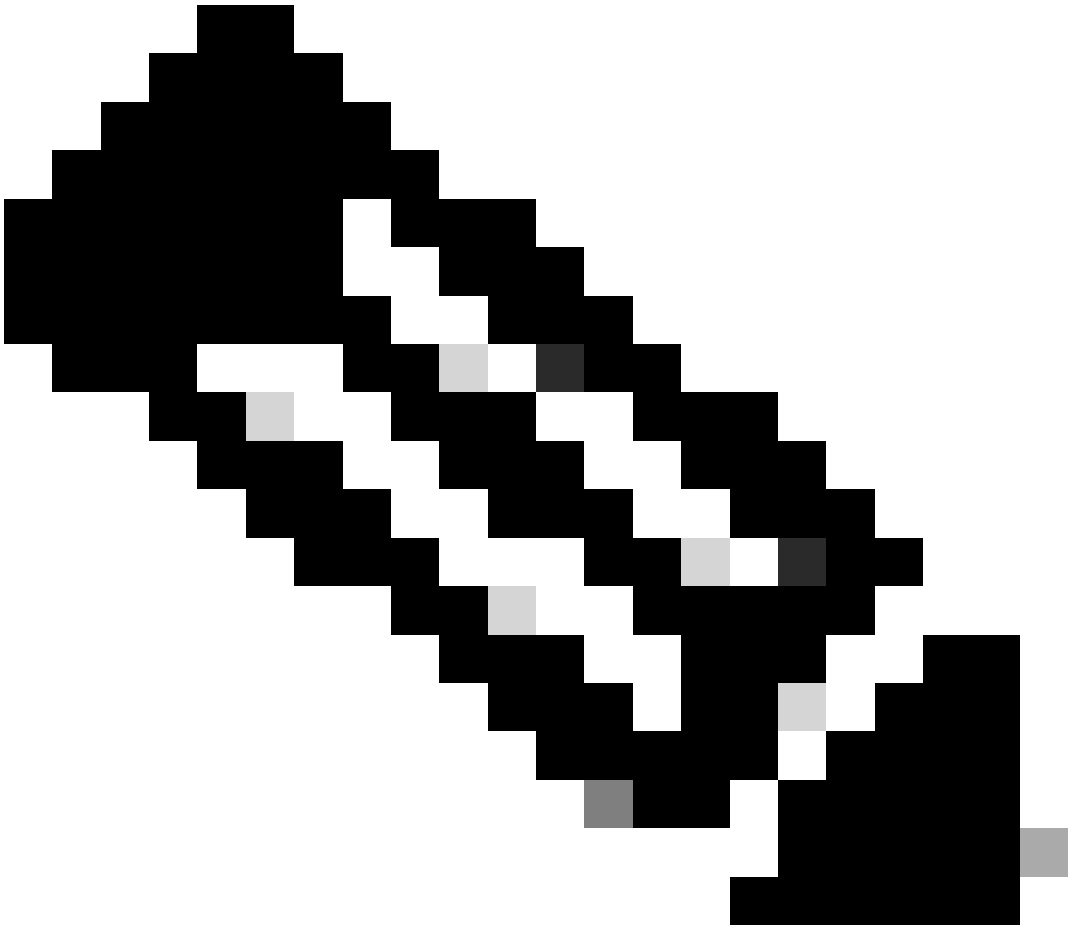
可能的原因

客户端计算机上身份验证计时器设置不正确，或者交换机上的身份验证间隔设置不正确。

解决方案

此问题有几种可能的解决方案：

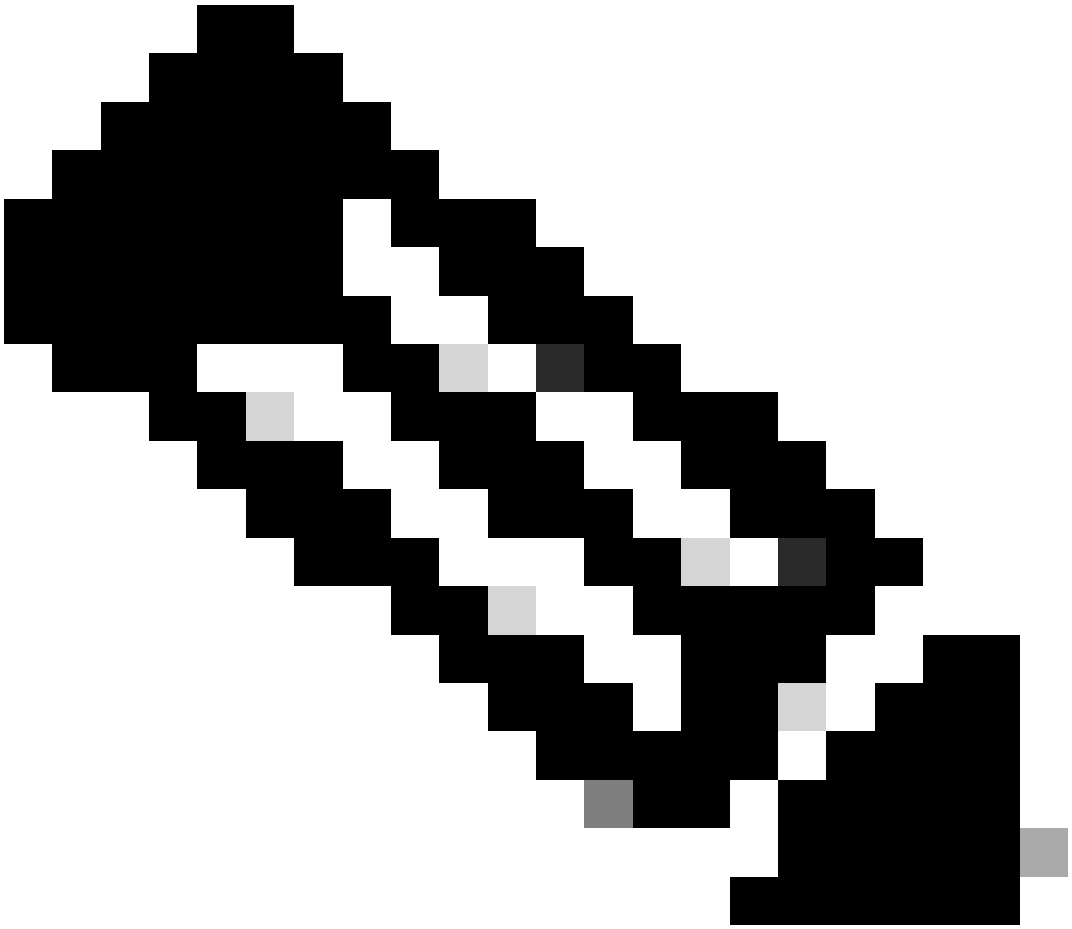
1. 检查Cisco ISE中指定的NAD或交换机的Session Status报告，并确保接口配置了适当的身份验证间隔。
2. 在NAD/交换机上输入show running configuration，并确保接口配置了适当的身份验证计时器重新启动设置。(例如，authentication timer restart 15,authentication timer reauthenticate 15)。
3. 输入interface shutdown和no shutdown以弹回NAD/交换机上的端口，并强制重新验证和思科ISE中的潜在配置更改。



注意：由于CoA需要MAC地址或会话ID，因此建议您不要退回网络设备SNMP报告中显示的端口。

未找到IP地址或MAC地址时，ANC操作失败

当终端的活动会话不包含有关IP地址的信息时，您在终端上执行的ANC操作失败。这也适用于该终端的MAC地址和会话ID。



注意：当您希望通过ANC更改终端的授权状态时，必须提供终端的IP地址或MAC地址。如果在终端的活动会话中找不到IP地址或MAC地址，则可能会看到错误消息："找不到此MAC地址、IP地址或会话ID的活动会话"。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。