在ISE 3.3和Stealthwatch 7.5.1上配置ANC

目錄

簡介

必要條件

採用元件

背景資訊

網路圖表

逐步配置

驗證

疑難排解

- 隔離的端點不會在策略更改後續訂身份驗證
  - 問題
  - 可能原因
  - 解決方案
  - 找不到IP地址或MAC地址時ANCO操作失敗

簡介

本文檔介紹在Cisco ISE® 3.3版和Stealthwatch上配置快速威脅遏制（自適應網路控制）。

必要條件

思科建議瞭解以下主題：

- 身分識別服務引擎 (ISE)
- 平台交換網格(PxGrid)
- 安全網路分析(Stealthwatch)
- 快速威脅遏制（自適應網路控制 — ANC）。

在本文檔中，假設思科身份服務引擎使用啟用ANC的pxGrid與安全網路分析(Stealthwatch)整合。

採用元件

本檔案中的資訊是根據以下軟體和版本：

- 思科身分識別服務引擎(ISE)版本3.3
- 安全網路分析(Stealthwatch)7.5.1
- Catalyst 9300

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

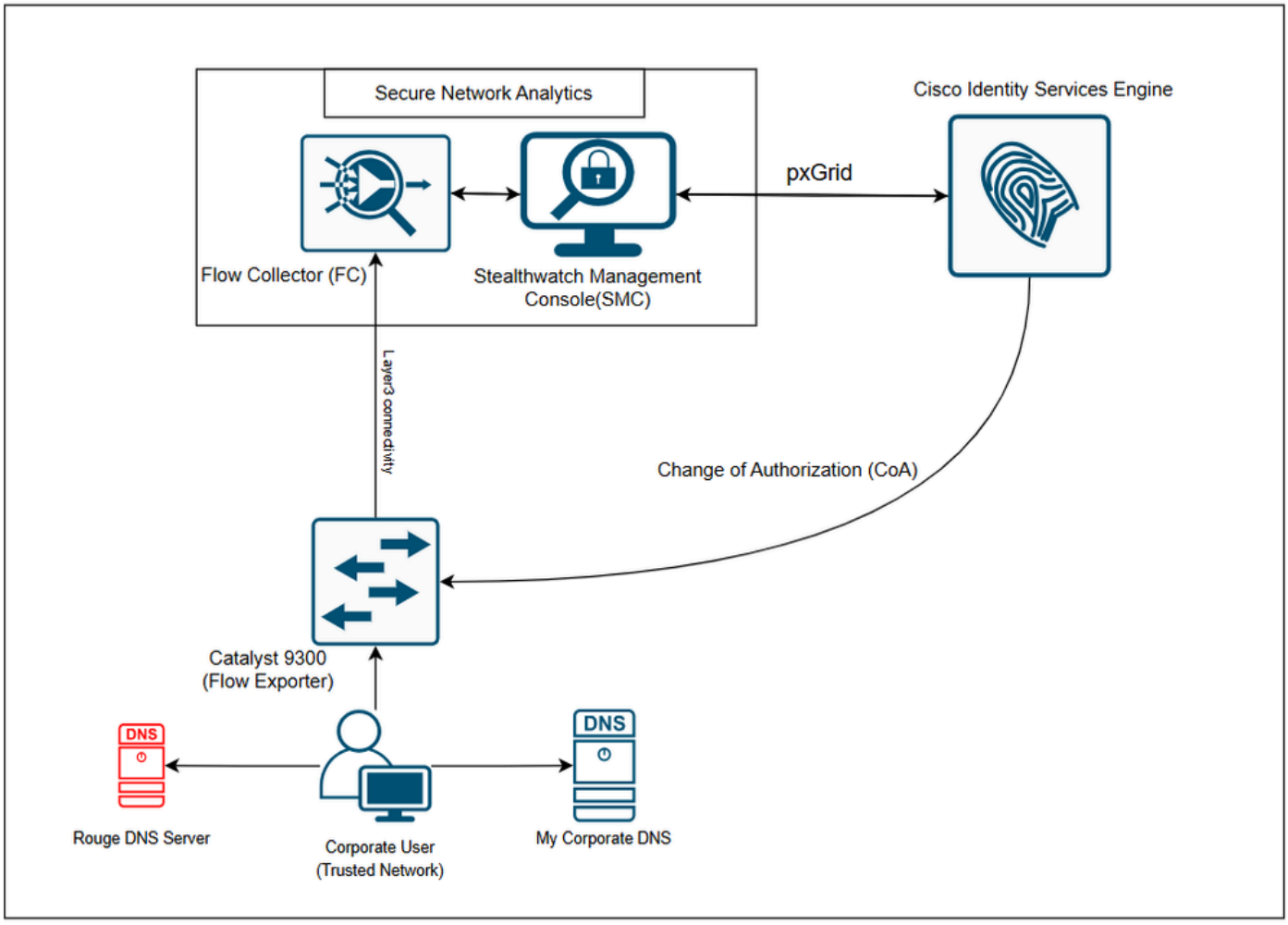
思科安全雲分析（現已成為思科XDR的一部分）可以使用pxGrid從思科身份服務引擎(ISE)檢索使用者屬性資料。此整合支援在Secure Cloud Analytics事件檢視器中報告使用者活動。

安全網路分析（前身為Stealthwatch）和思科身份服務引擎(ISE)的組合可幫助組織獲得360°的視野，更快地應對威脅，並保護不斷增長的數位業務。Secure Network Analytics檢測到異常流量後，會發出警報，為管理員提供隔離使用者的選項。pxGrid使Secure Network Analytics能夠將quarantine命令直接傳遞給身份服務引擎。

本示例介紹如何利用公司DNS伺服器來防禦Internet威脅。其目的是建立自定義警報機制，在內部使用者連線到外部DNS伺服器時觸發該機制。此計畫旨在阻止連線到未經授權的DNS伺服器，這些伺服器可能會將流量重定向到有害的外部站點。

觸發警報時，思科安全網路分析會與思科ISE協調，通過PxGrid使用自適應網路控制策略隔離訪問未授權DNS伺服器的主機。

網路圖表



如圖所示：

- 企業使用者連線到C9300交換機，該交換機配置為匯出IP流並將資料傳送到流量收集器。
- 將同一企業使用者配置為使用企業DNS伺服器。
- 流量收集器與Stealthwatch管理控制台(SMC)整合
- Stealthwatch管理控制檯(SMC)通過Pxgrid與ISE整合。

逐步配置

1.準備交換機以使用netflow監控和匯出流。

運行Cisco IOS® XE 17.15.01的C9300交換器上的基本流配置

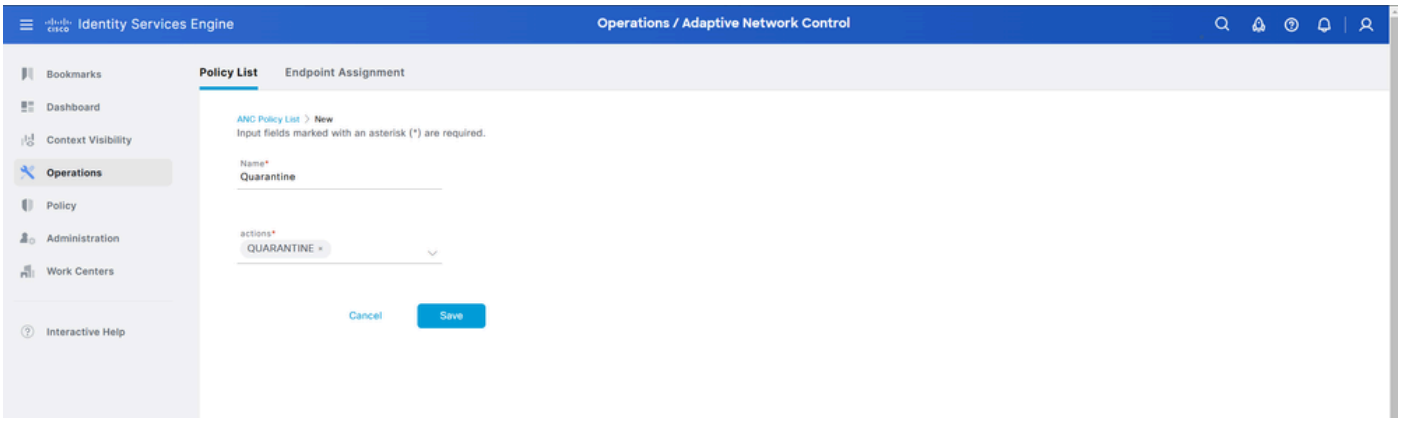
```
flow record SW_FLOW_RECORD
  description NetFlow record format to send to SW
  match ipv4 tos
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  match interface input
  collect transport tcp flags
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

完成配置後，C9300可以將IP流資料匯出到流量收集器。然後，流量收集器處理此資料，並將其傳輸到Stealthwatch管理控制檯(SMC)，以進行分析和監控。

2. EnableAdaptive Network Control Cisco ISE。

預設情況下，ANC處於禁用狀態。僅當啟用pxGrid時，才會啟用ANC，並且它保持啟用狀態，直到您在管理員門戶中手動禁用該服務。

選擇Operations > Adaptive Network Control > Policy List > Add，然後為Policy Name輸入Quarantine，為Action輸入Quarantine。

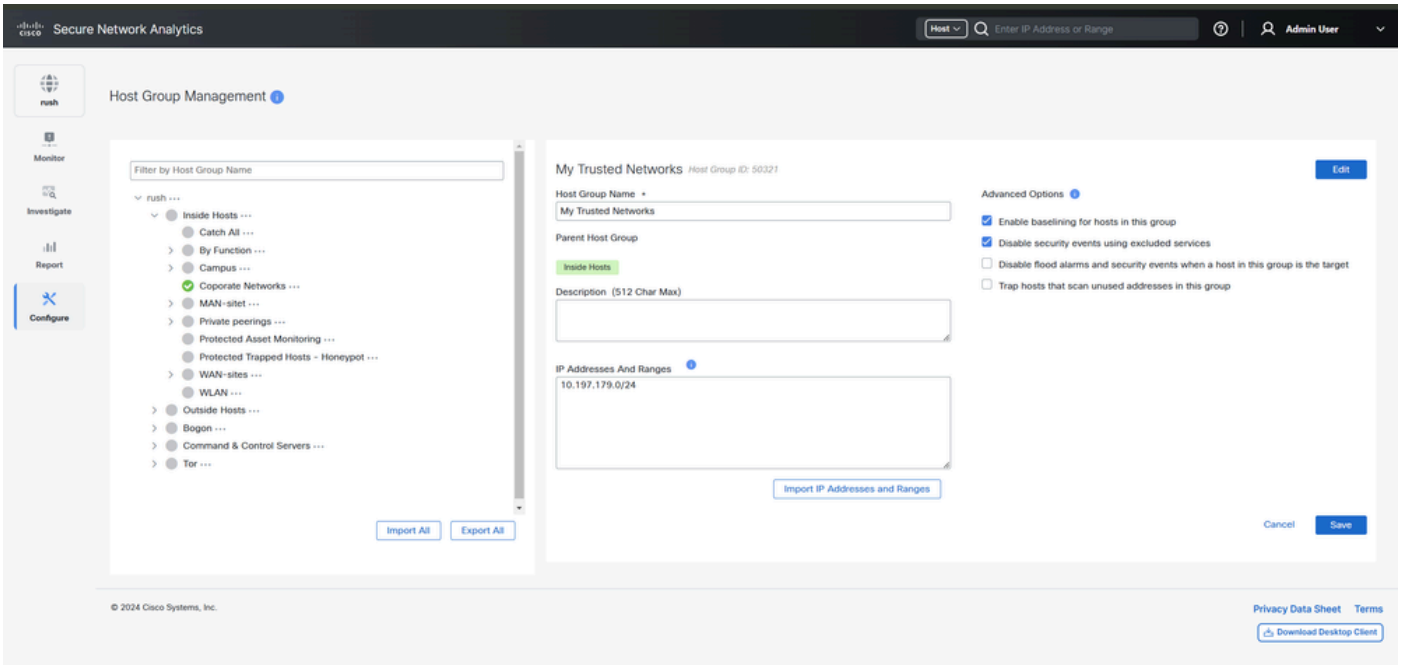


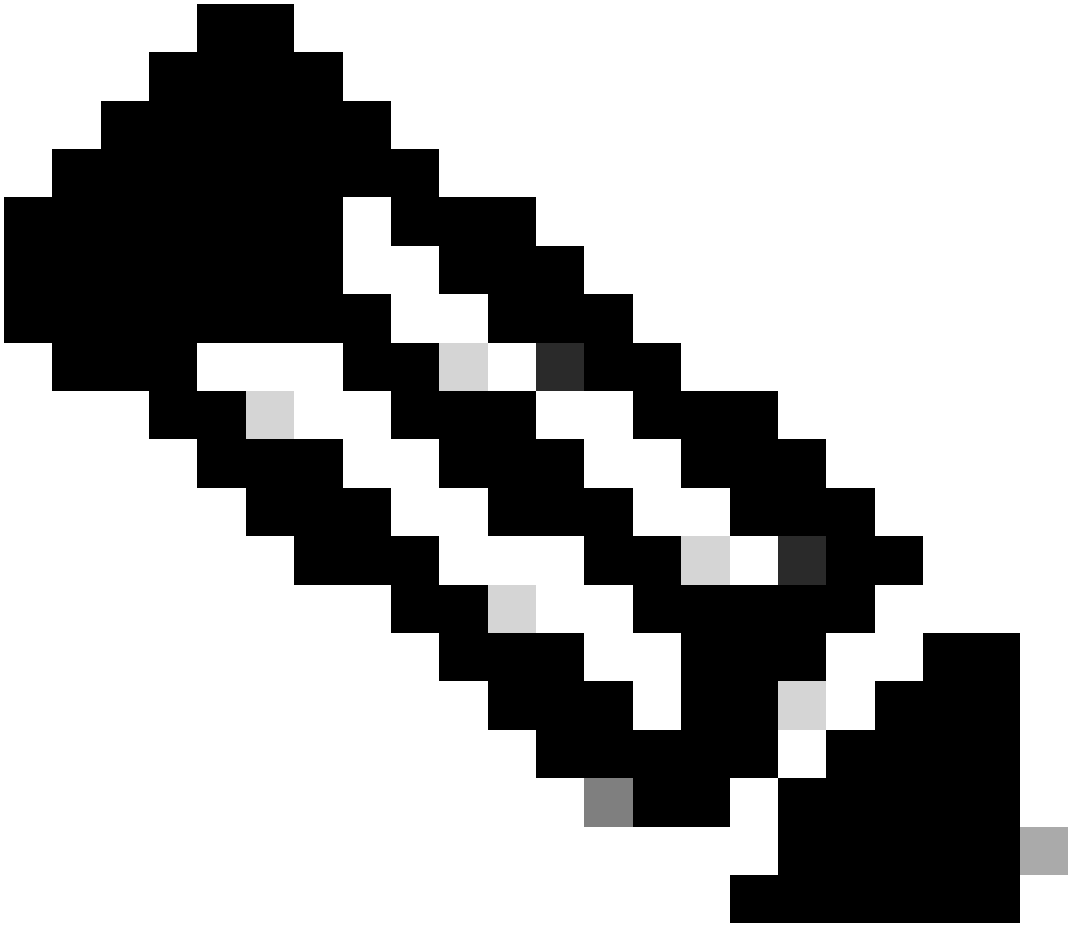
3.為事件觸發和響應管理配置安全網路分析，以便快速遏制威脅。

步驟 1:登入SMC GUI並導航至Configure > Detection > Host Group Management >按一下Inside Hosts旁邊的(...)（省略號）圖示，然後選擇Add Host Group。

在本示例中，在Inside Hosts的父主機組下建立名為My Trusted Networks的新主機組。

通常可以將此網路分配給終端使用者機器以監控DNS使用情況。

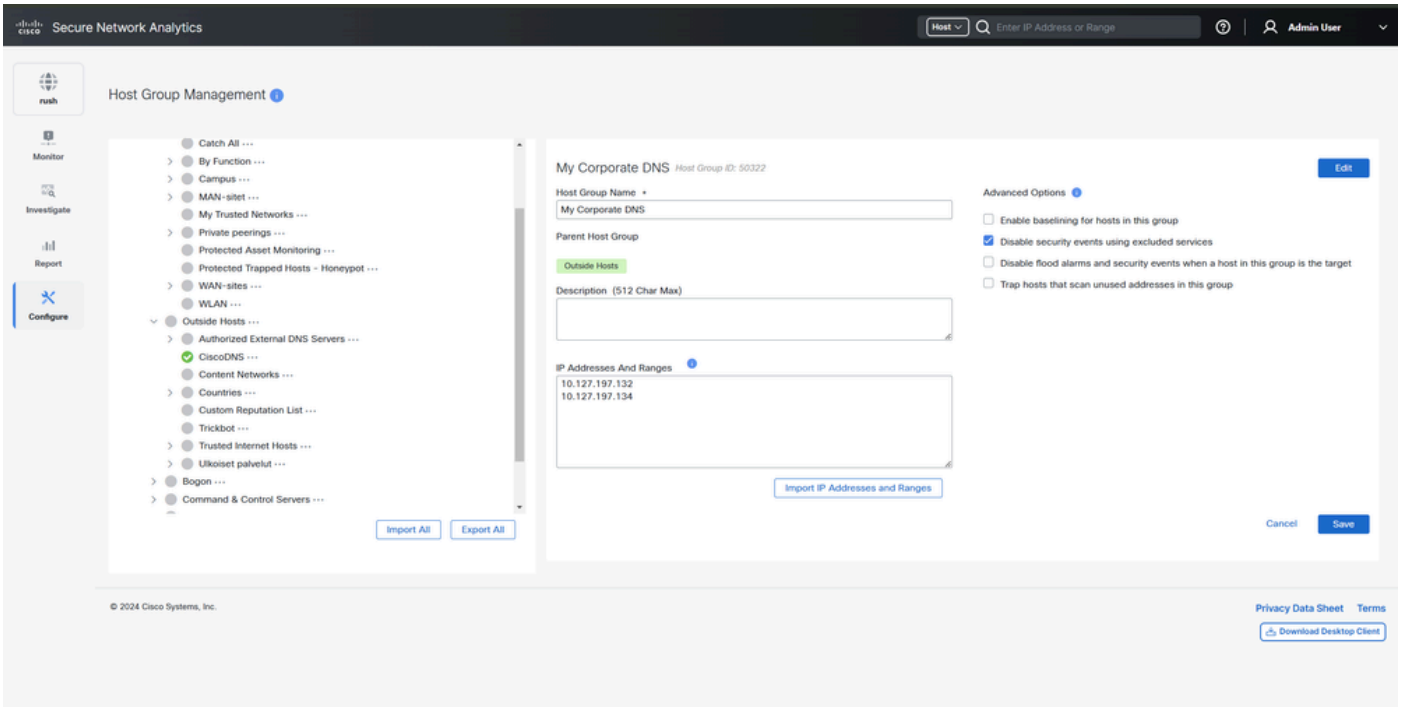


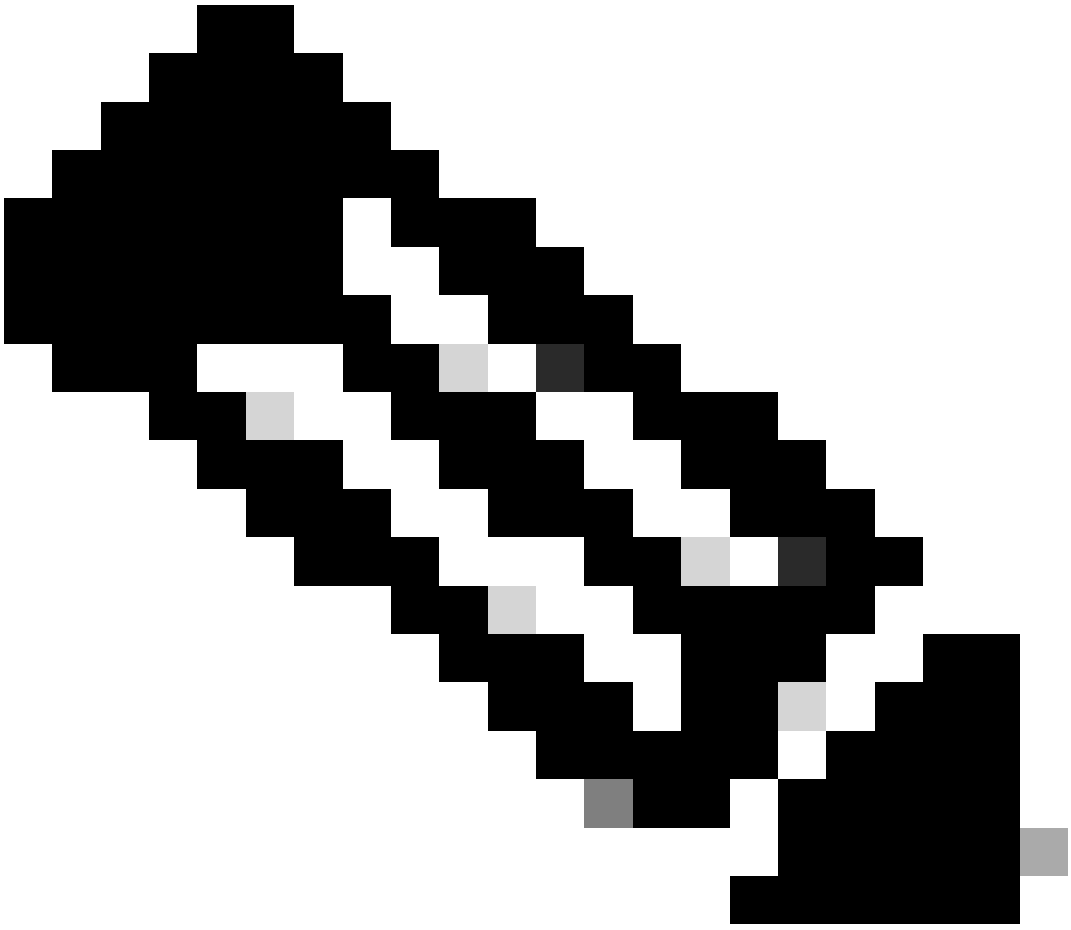


附註：在本例中，IP子網10.197.179.0/24用作區域網(LAN)子網。根據網路體系結構，這在實際網路環境中可能有所不同。

步驟 2:在SMC GUI中登入，導航至Configure > Detection > Host Group Management > Click on(...)(除Outside Hosts外)，然後選擇Add Host Group。

在本示例中，在Outside Hosts的父主機組下建立了一個名為My Corporate DNS的新主機組。

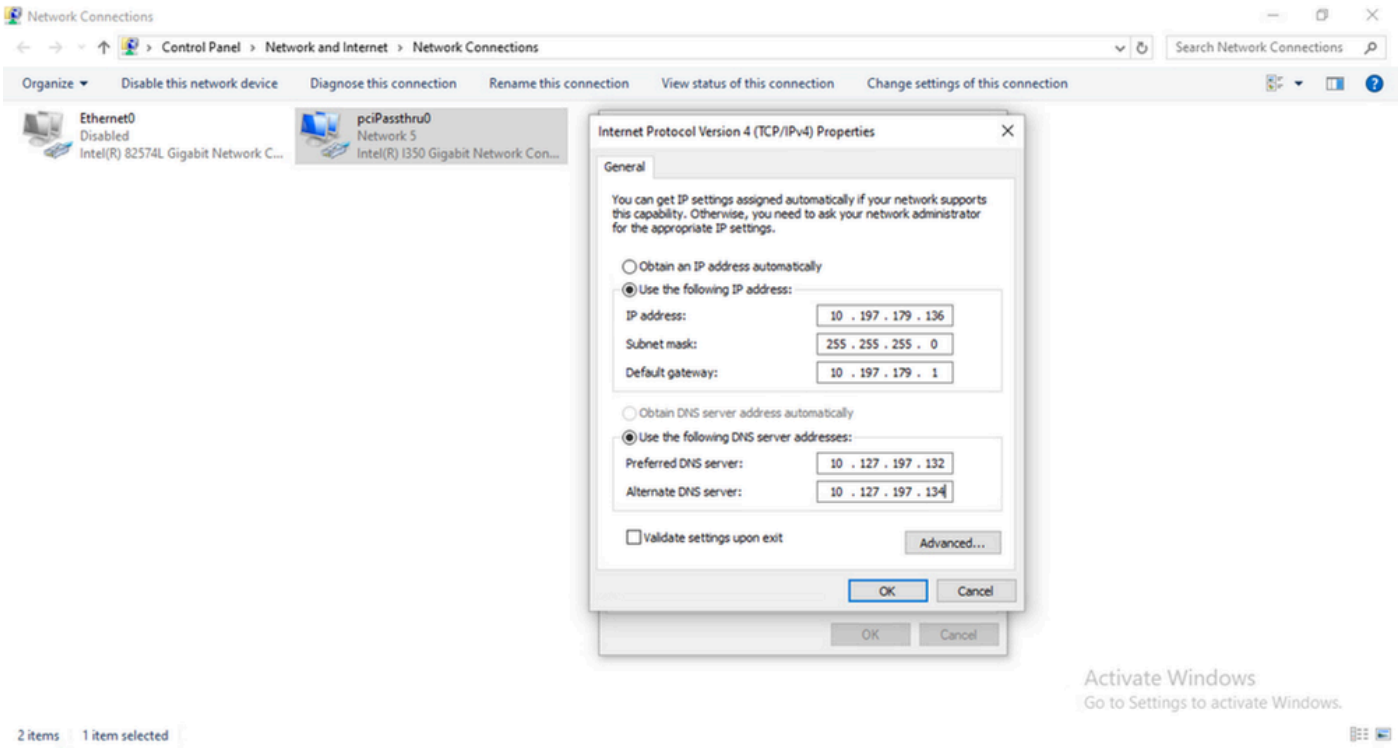




附註：在本例中，IP 10.127.197.132和10.127.197.134用作終端使用者使用的所需DNS伺

服器，這在實際網路環境中可能會有所不同，具體取決於網路體系結構。

用於演示的測試實驗室PC配置了靜態IP 10.197.179.136（屬於建立的我的受信任網路主機組）和DNS 10.127.197.132和10.127.197.134（屬於建立的我的公司DNS主機組）。



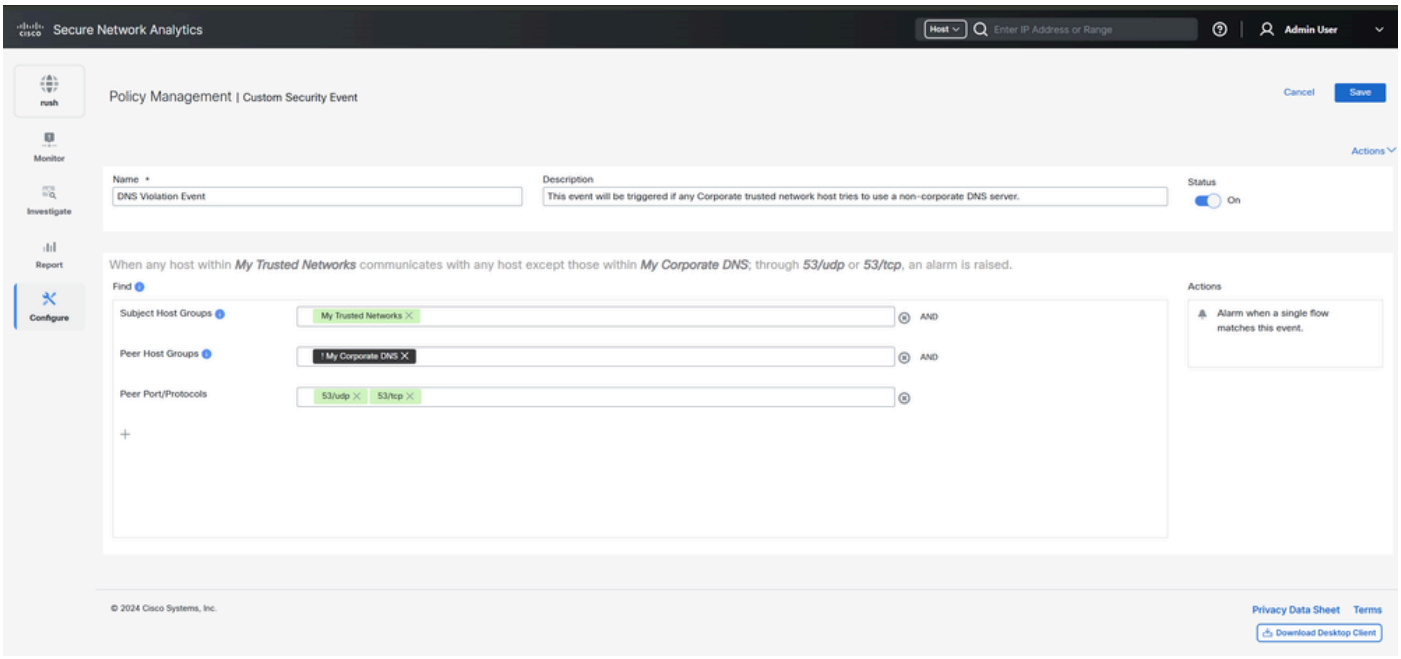
步驟 3:設定定製的警報系統以檢測內部使用者何時連線到外部DNS伺服器，觸發警報以阻止連線到未經授權的DNS伺服器，從而可能將流量重定向到惡意外部站點。啟用警報後，Cisco Secure Network Analytics會與Cisco ISE協調，通過PxGrid採用自適應網路控制策略，通過這些未經授權的DNS伺服器隔離主機。

導航到Configure > Policy Management。

使用下列資訊建立自定義事件：

- 名稱：DNS違規事件。
- Subject Host Groups：我的可信任網路。
- 對等主機組:（非）我的企業DNS。
- 對等連線埠/通訊協定：53/UDP 53/TCP

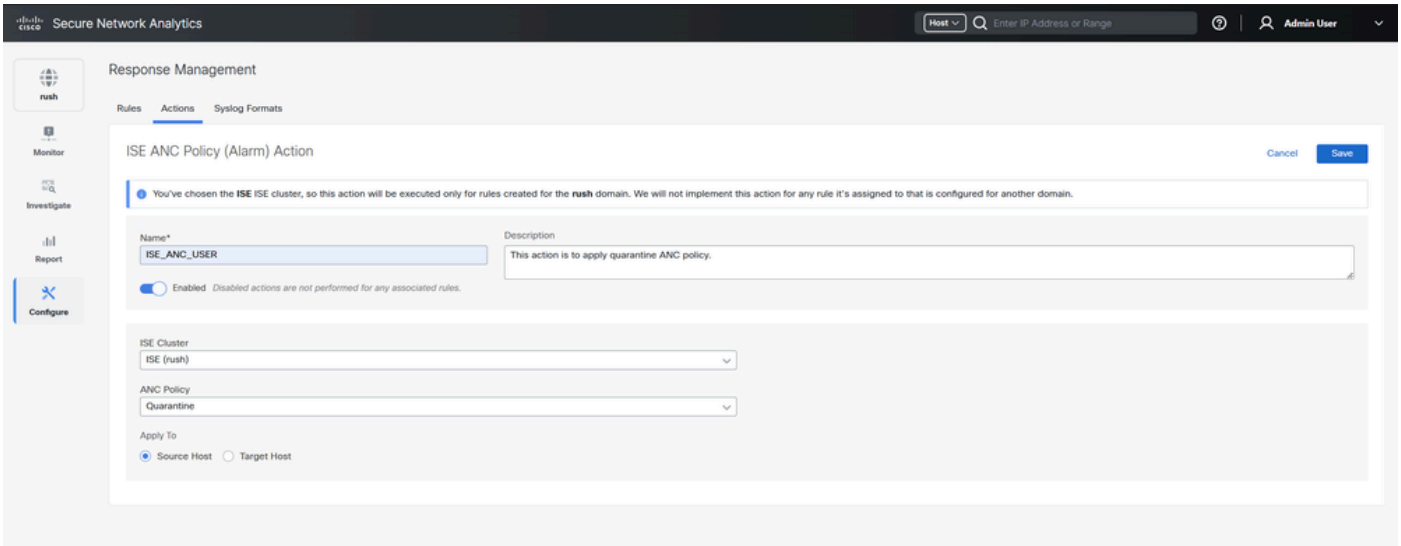
這表示當我的受信任網路（主機組）內的任何主機通過53/up或53/tcp與除我的公司DNS（主機組）內的任何主機以外的任何主機通訊時，將發出警報。



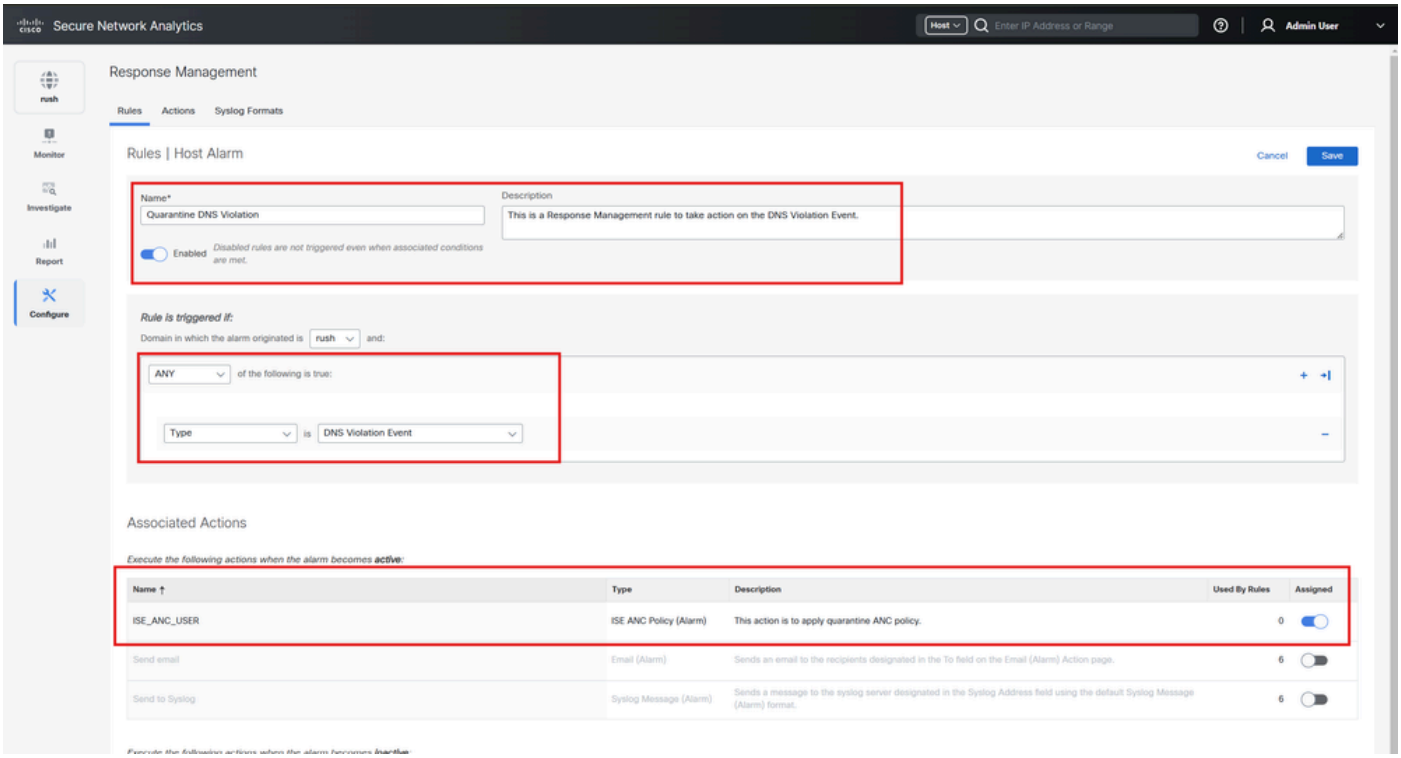
步驟 4:配置要執行的響應管理操作，該操作可在建立後應用於響應管理規則。

導覽至Configure > Response Management > Actions，點選Add New Action，然後選擇ISE ANC Policy(Alarm)。

分配名稱並選擇要通知的特定思科ISE集群，以便對任何違規或連線到未經授權的伺服器實施隔離策略。



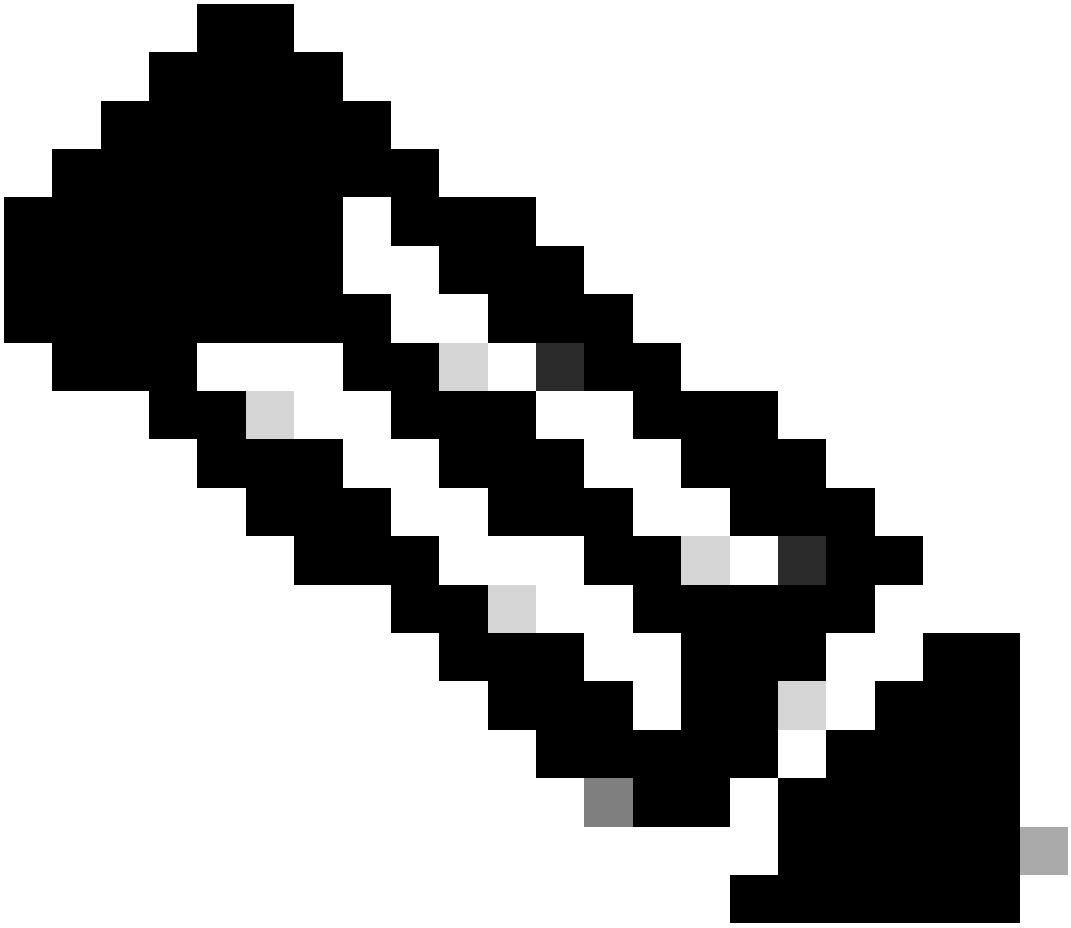
步驟5：在Rules部分下創建新規則。只要內部網路中的主機嘗試將DNS流量傳送到未授權的DNS伺服器，此規則就會實施以前定義的操作。在Rule is triggered if部分，選擇Type，然後選擇先前建立的自定義事件。
在Associated Actions下，選擇之前配置的ISE ANC警報操作。



4.配置Cisco ISE以在觸發事件時響應Stealthwatch發起的操作。

登入到Cisco ISE GUI並導航到Policy > Policy Sets > Choose the Policy set > under Authorization Policy - Local Exceptions > Createnew Policy。

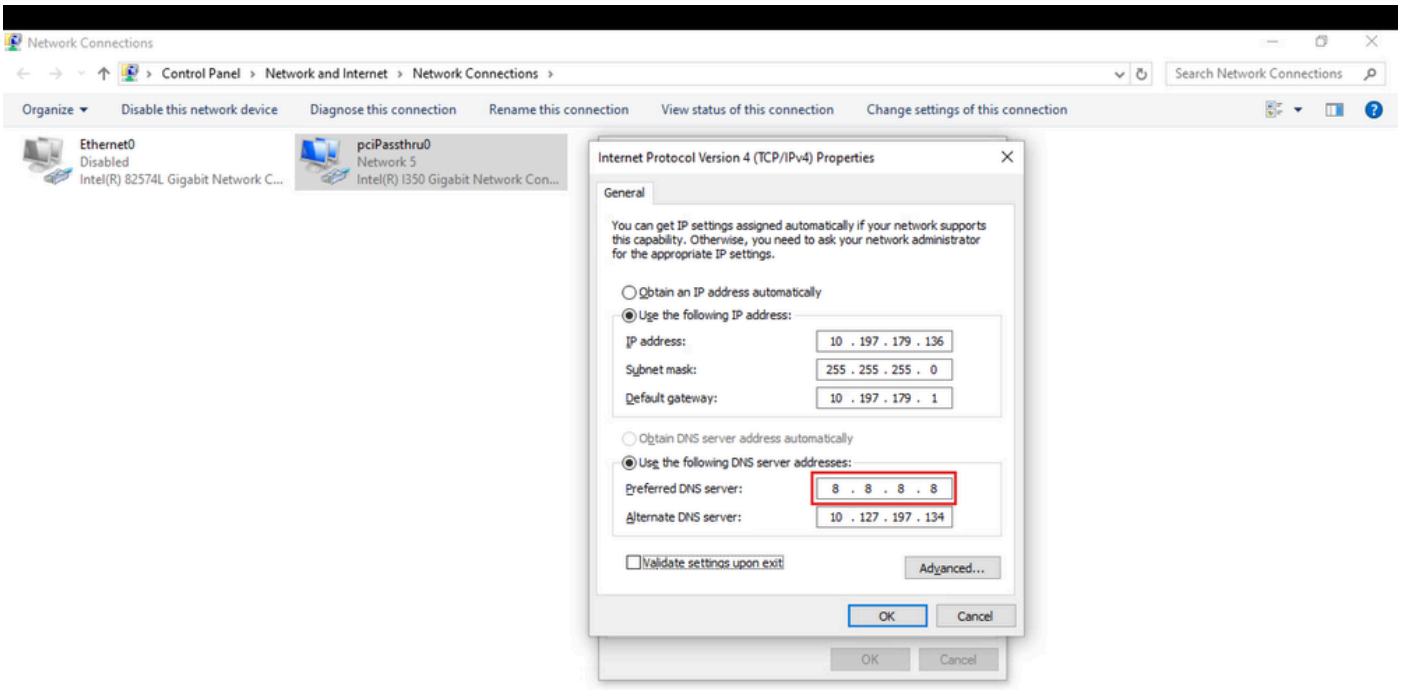
- 名稱:DNS違例異常
- 狀況:會話：ANCPolicy EQUALS QUARANTINE（ANCPolicy等於隔離）
- 授權配置檔案:DenyAccess



附註：在此範例中，一旦觸發DNS違例事件，就會根據組態拒絕使用者存取

驗證

為了演示使用案例，終端上的DNS條目已更改為8.8.8.8，這將觸發配置的DNS違規事件。由於DNS伺服器不屬於我的公司DNS伺服器的主機組，因此它會觸發導致拒絕訪問終端的事件。



在C9300交換機上，使用show flow monitor IPv4_NETFLOW cache進行驗證 |在8.8.8.8命令中，輸出用於檢視正在捕獲流並將其傳送到流量收集器。IPv4_NETFLOW是在交換器設定中設定的。

<#root>

IPV4 SOURCE ADDRESS:

10.197.179.136

IPV4 DESTINATION ADDRESS:

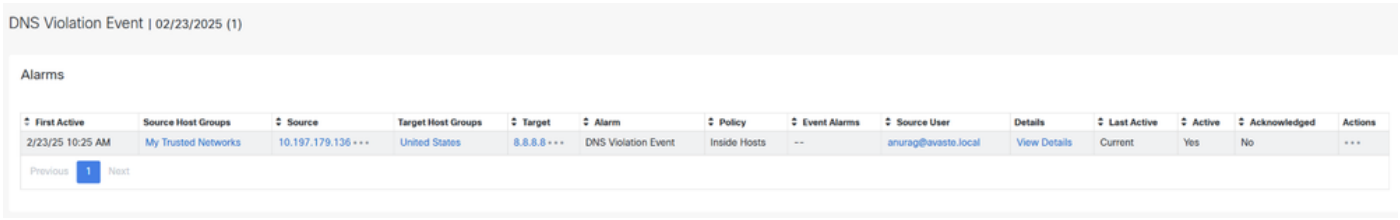
8.8.8.8

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

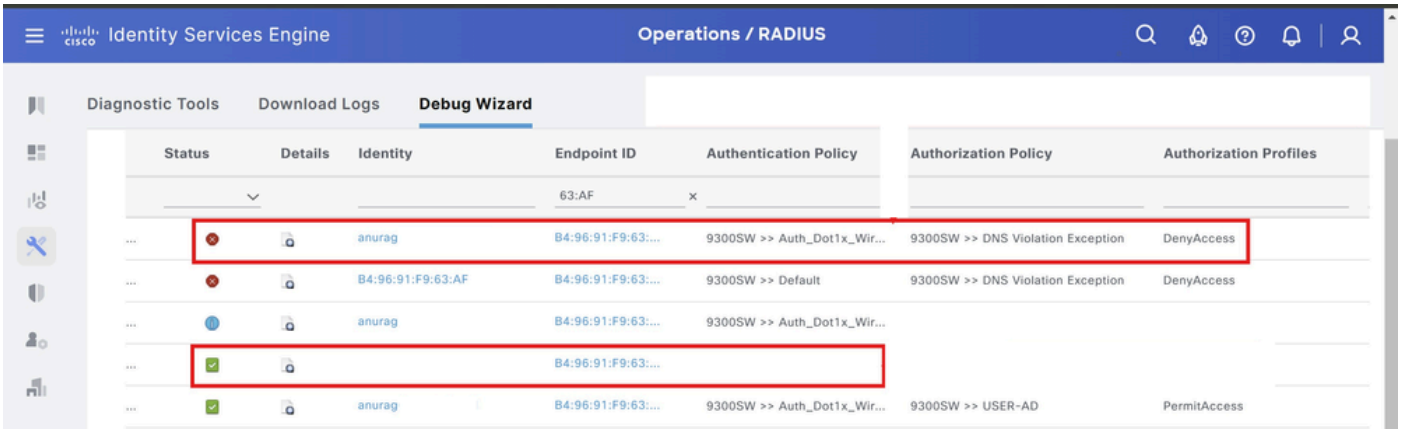
在Stealthwatch上觸發事件後，請導航到Monitor > Security Insight Dashboard。



導航到監控(Monitor)>整合(Integration)> ISE ANC策略分配(ISE ANC Policy Assignments)。

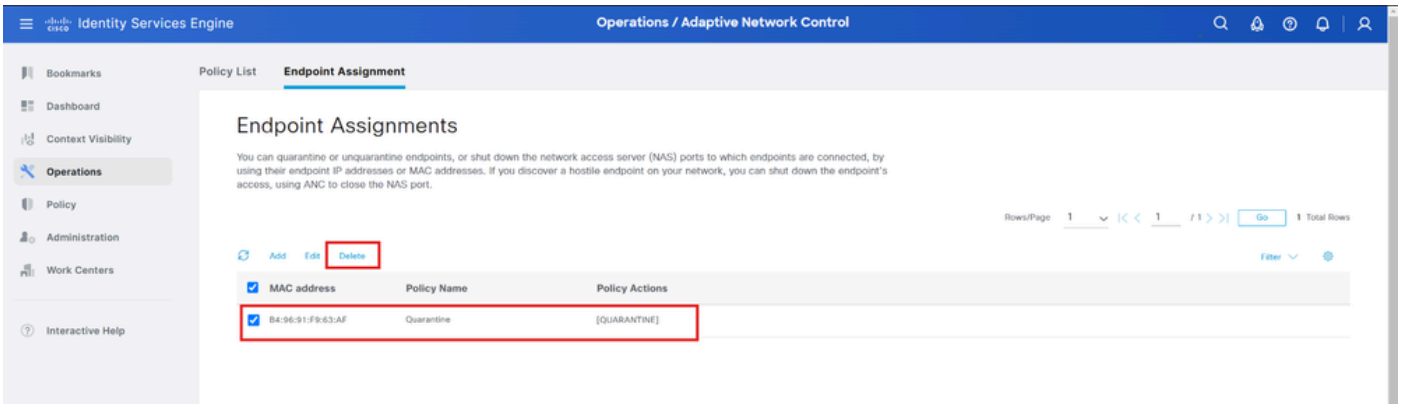
確保思科安全網路分析已成功通過PxGrid和思科ISE實施自適應網路控制策略以隔離主機。

類似地，在Cisco ISE上，導航到Operations > RADIUS > Livelogs，並對端點應用過濾器。



根據本地異常策略DNS違例異常，授權更改(CoA)由ISE頒發，訪問ISE被拒絕到終端。

在端點上執行補救操作後，從操作>自適應網路控制>端點分配>刪除中刪除MAC以刪除端點的MAC地址。



思科ISE上的日誌參考。

思科ISE上的pxgrid(pxgrid-server.log)元件的屬性設定為TRACE級別，可在pxgrid-server.log檔案中看到日誌。

<#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

"}

疑難排解

隔離的端點不會在策略更改後續訂身份驗證

問題

由於策略或其他標識的更改，身份驗證失敗，並且未進行重新身份驗證。身份驗證失敗，或者有問題的終端仍然無法連線到網路。此問題通常發生在根據分配給使用者角色的終端安全評估失敗的客戶端電腦上。

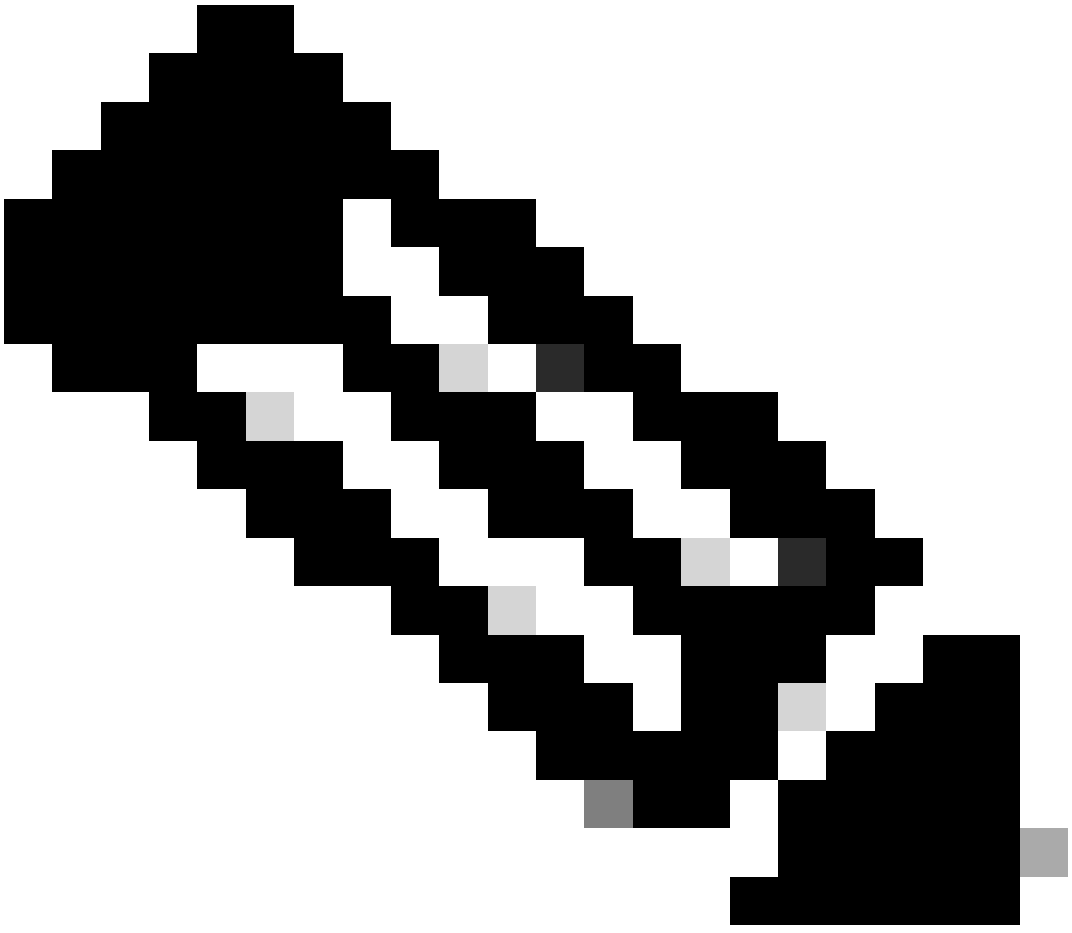
可能原因

未在客戶端電腦上正確設定身份驗證計時器設定，或者未在交換機上正確設定身份驗證間隔。

解決方案

此問題有幾種可能的解決方案：

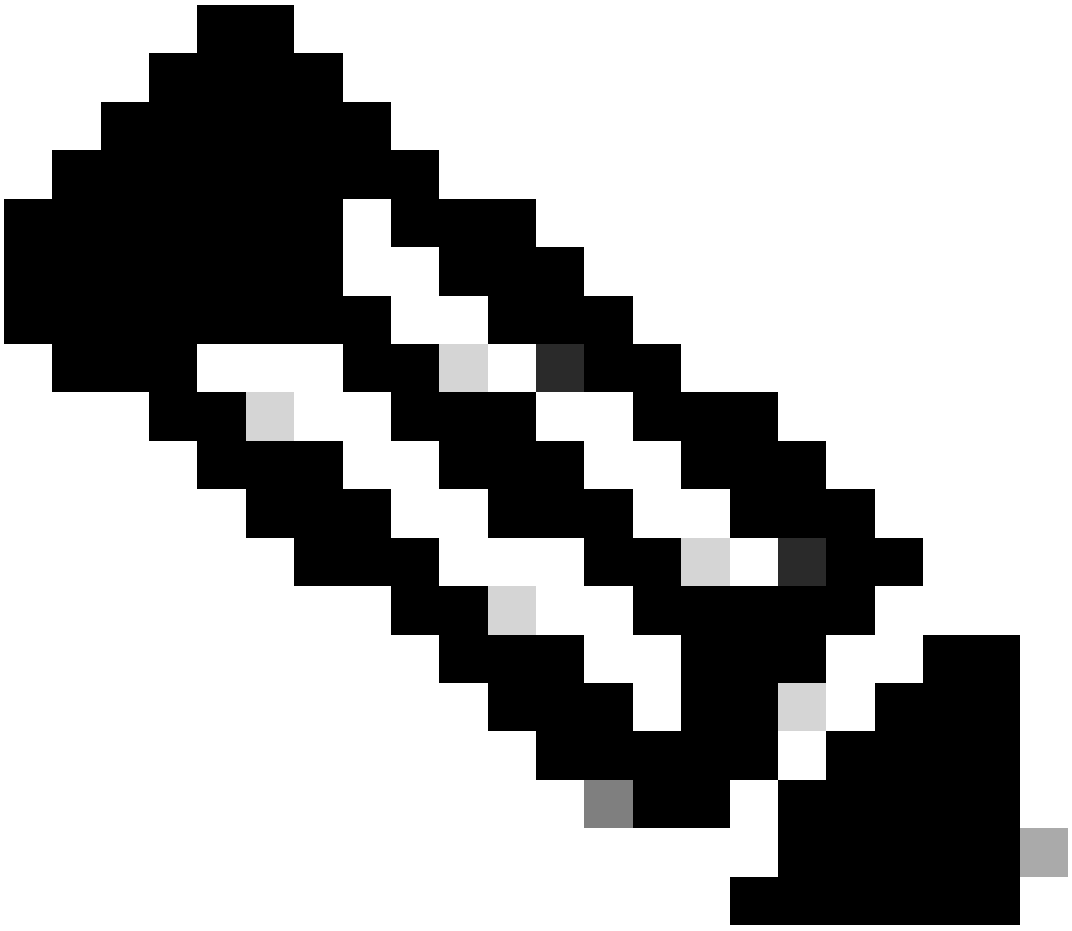
1. 檢查思科ISE中指定的NAD或交換機的Session Status摘要報告，並確保介面配置了適當的身份驗證間隔。
2. 在NAD/交換機上輸入show running configuration，並確保使用適當的身份驗證計時器重新啟動設定配置介面。(例如，authentication timer restart 15,authentication timer reauthenticate 15)。
3. 輸入interface shutdown和no shutdown以彈出NAD/交換機上的埠，並在Cisco ISE中強制重新身份驗證和可能的配置更改。



附註：由於CoA需要MAC地址或會話ID，因此建議您不要退回網路裝置SNMP報告中顯示的埠。

未找到IP地址或MAC地址時，ANC操作失敗

當終結點的活動會話不包含有關IP地址的資訊時，在終結點上執行的ANC操作失敗。這也適用於該終端的MAC地址和會話ID。



附註：如果要通過ANC更改終端的授權狀態，必須提供終端的IP地址或MAC地址。如果在終端的活動會話中找不到IP地址或MAC地址，您可以看到錯誤消息："找不到此MAC地址、IP地址或會話ID的活動會話"。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。