# ISE 3.3 및 Stealthwatch 7.5.1에서 ANC 구성

## 목차



### 소개

이 문서에서는 Cisco ISE® 버전 3.3 및 Stealthwatch의 Rapid Threat Containment(Adaptive Network Control) 구성에 대해 설명합니다.

### 사전 요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- Identity Services Engine(ISE)
- 플랫폼 교환 그리드(PxGrid)
- 보안 네트워크 분석(Stealthwatch)
- 신속한 위협 억제(ANC(Adaptive Network Control)).

이 문서에서는 Cisco Identity Services Engine이 ANC가 활성화된 pxGrid를 사용하여 Secure Network Analytics(Stealthwatch)와 통합된다고 가정합니다.

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 버전을 기반으로 합니다.

- Cisco ISE(Identity Services Engine) 버전 3.3
- Secure Network Analytics(Stealthwatch) 7.5.1
- Catalyst 9300

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

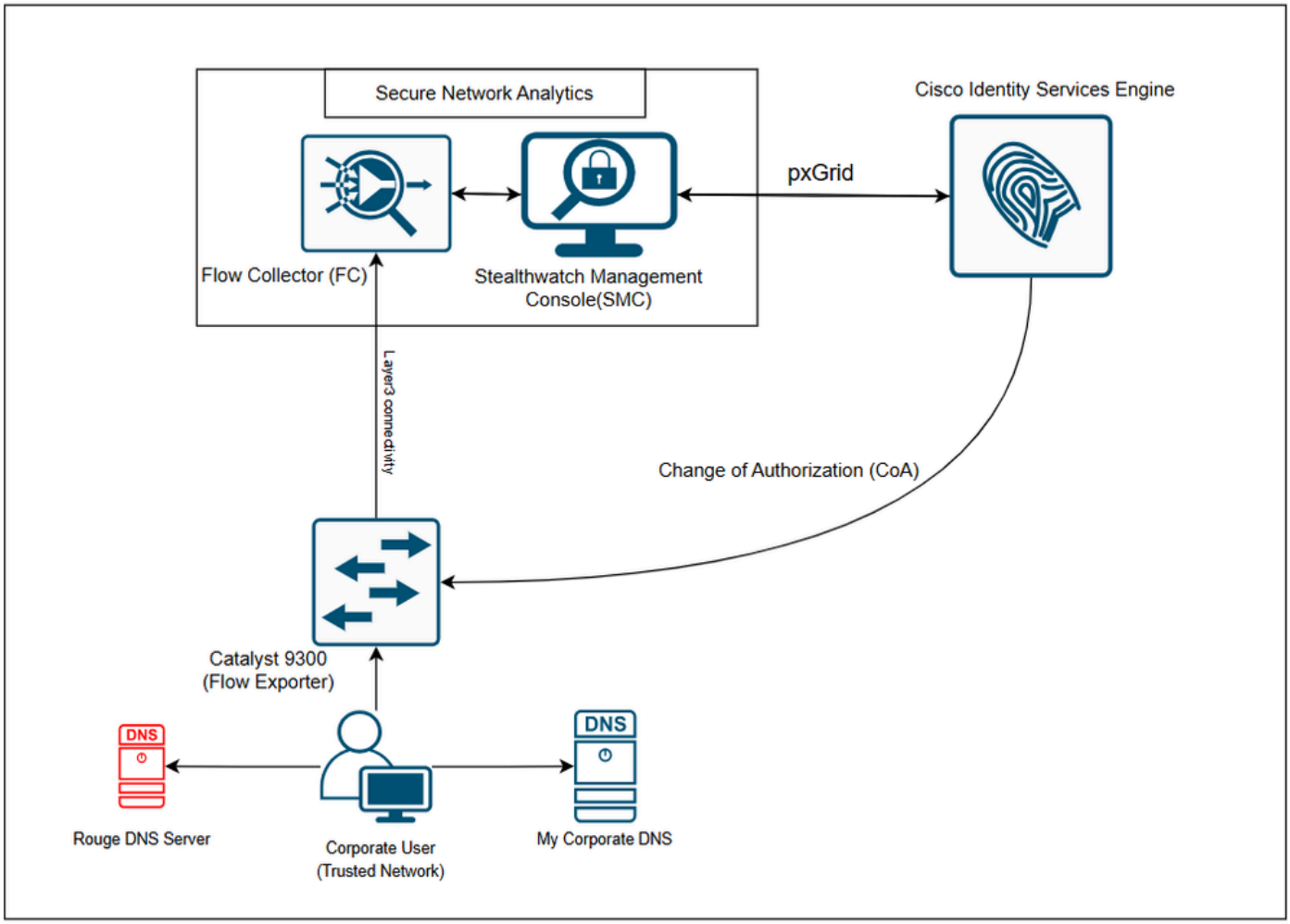
Cisco Secure Cloud Analytics(현재 Cisco XDR에 포함됨)는 pxGrid를 사용하여 Cisco ISE(Identity Services Engine)에서 사용자 속성 데이터를 검색할 수 있습니다. 이러한 통합을 통해 Secure Cloud Analytics Event Viewer에서 사용자 활동 보고를 수행할 수 있습니다.

Secure Network Analytics(이전의 Stealthwatch)와 Cisco ISE(Identity Services Engine)를 결합하면 360° 가시성을 확보하고 위협에 더 신속하게 대응하며 성장하는 디지털 비즈니스를 보호할 수 있습니다. Secure Network Analytics에서 이상 트래픽을 탐지하면 관리자에게 사용자를 격리할 수 있는 옵션을 제공하는 알림을 보냅니다. pxGrid를 사용하면 Secure Network Analytics에서 quarantine 명령을 Identity Services Engine으로 직접 전달할 수 있습니다.

이 예에서는 기업 DNS 서버를 활용하여 인터넷 위협으로부터 보호하는 방법을 설명합니다. 내부 사용자가 외부 DNS 서버에 연결할 때 트리거되는 사용자 지정 경고 메커니즘을 설정하기 위한 것입니다. 이 이니셔티브는 유해한 외부 사이트로 트래픽을 리디렉션할 수 있는 권한이 없는 DNS 서버에 대한 연결을 차단하도록 설계되었습니다.

경고가 트리거되면 Cisco Secure Network Analytics는 Cisco ISE와 조정하여 PxGrid를 통한 적응형 네트워크 제어 정책을 사용하여 무단 DNS 서버에 액세스하는 호스트를 격리합니다.

# 네트워크 다이어그램




다이어그램에 표시된 대로

- 기업 사용자가 IP 플로우를 내보내고 플로우 컬렉터로 데이터를 전송하도록 구성된 C9300 스위치에 연결되었습니다.
- 동일한 기업 사용자가 기업 DNS 서버를 사용하도록 구성되었습니다.
- Flow Collector가 SMC(Stealthwatch Management Console)와 통합
- SMC(Stealthwatch Management Console)는 Pxgrid를 통해 ISE와 통합됩니다.

단계별 구성

1. netflow를 사용하여 플로우를 모니터링하고 내보낼 스위치를 준비합니다.

Cisco IOS® XE 17.15.01을 실행하는 C9300 스위치의 기본 플로우 컨피그레이션

```
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
```

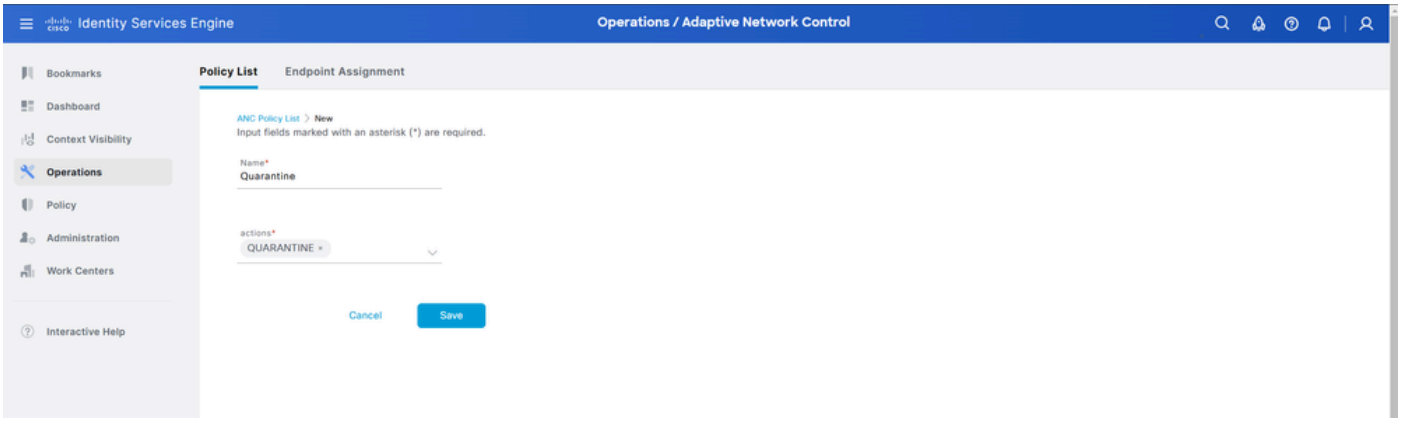
```
  collect transport tcp flags
  collect interface output
  collect counter bytes long
  collect counter packets long
  collect timestamp absolute first
  collect timestamp absolute last


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
```

컨피그레이션을 완료하면 C9300에서 IP 플로우 데이터를 Flow Collector로 내보낼 수 있습니다. 그런 다음 Flow Collector에서 이 데이터를 처리하고 분석 및 모니터링을 위해 SMC(Stealthwatch Management Console)로 전송합니다.

2. Cisco ISE에서 적응형 네트워크 제어 활성화

ANC는 기본적으로 비활성화되어 있습니다. ANC는 pxGrid가 활성화된 경우에만 활성화되며, 관리 포털에서 서비스를 수동으로 비활성화할 때까지 활성화된 상태로 유지됩니다.

Operations(운영) > Adaptive Network Control(적응형 네트워크 제어) > Policy List(정책 목록) > Add(추가)를 선택한 다음, Policy Name(정책 이름)에 Quarantine(격리)을 입력하고 Action(작업)에 Quarantine(격리)을 입력합니다.

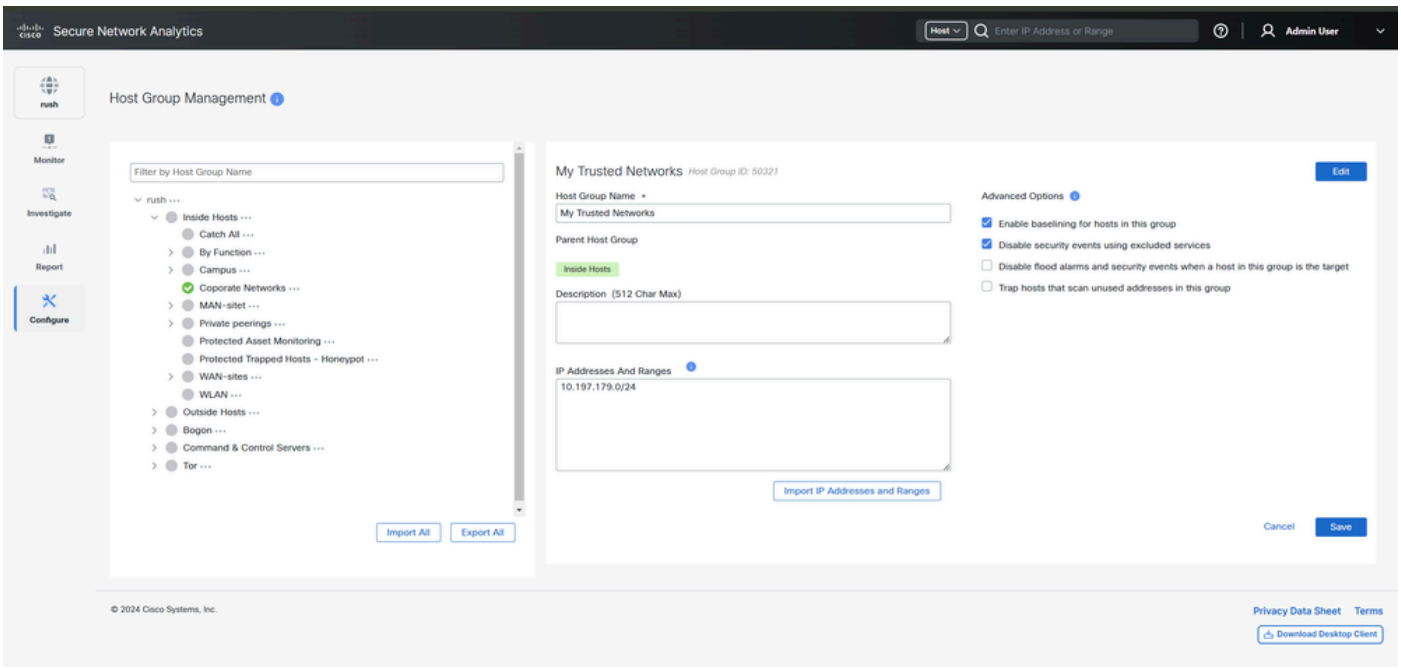


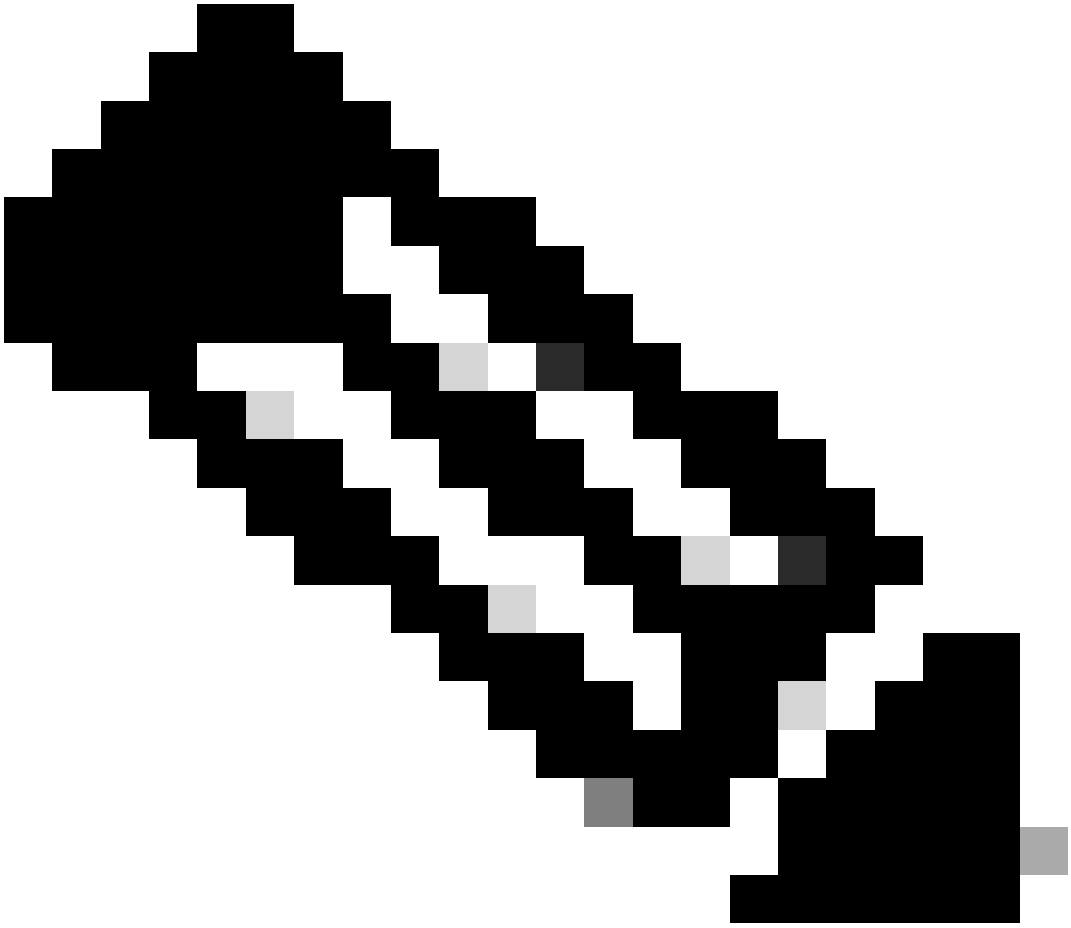
3. 신속한 위협 억제를 위해 이벤트 트리거 및 응답 관리를 위한 보안 네트워크 분석을 구성합니다.

1단계: SMC GUI에 로그인하고 Configure(구성) > Detection(탐지) > Host Group Management(호스트 그룹 관리)로 이동하고 Inside Hosts(내부 호스트) 옆의 (...) (생략 부호) 아이콘을 클릭한 다음 Add Host Group(호스트 그룹 추가)을 선택합니다.

이 예에서는 Inside Hosts의 상위 호스트 그룹 아래에 My Trusted Networks라는 이름으로 새 호스트 그룹이 생성됩니다.

일반적으로 이 네트워크는 DNS 사용을 모니터링하기 위해 엔드유저 시스템에 할당될 수 있습니다.



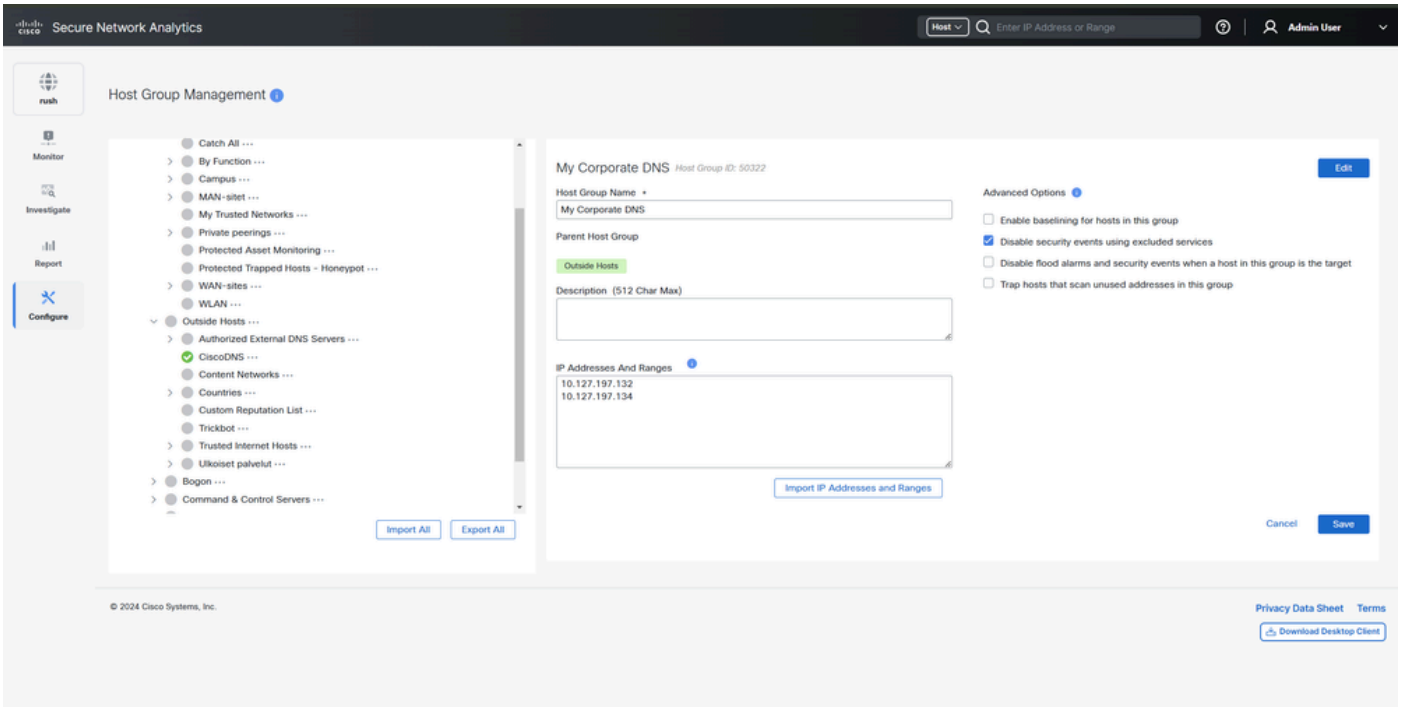


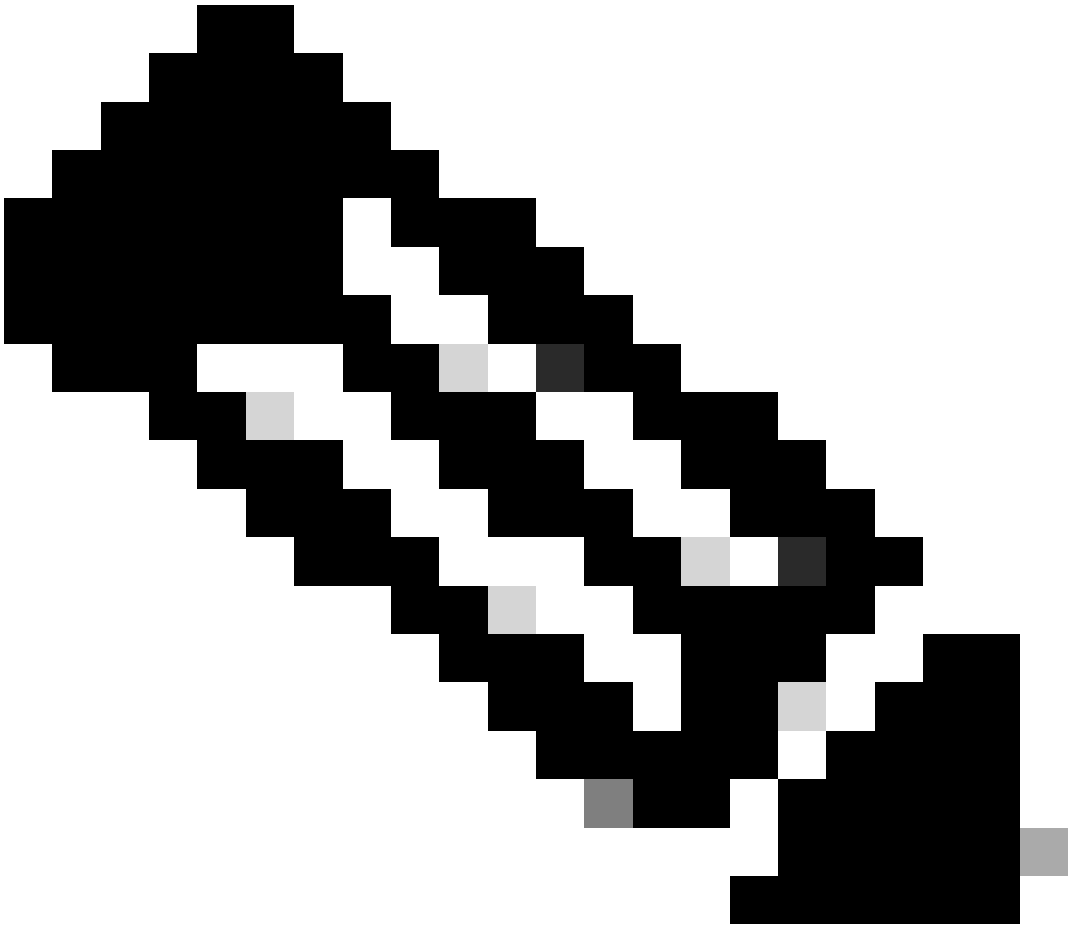
참고: 이 예에서 IP 서브넷 10.197.179.0/24은 LAN 서브넷으로 사용됩니다. 이는 네트워크 아키텍처에 따라 실제 네트워크 환경에서 다를 수 있습니다.

---

2단계: SMC GUI에 로그인하고 Configure(구성) > Detection(탐지) > Host Group Management(호스트 그룹 관리) > Outside Hosts(외부 호스트) 외에서 (...)를 클릭하고 Add Host Group(호스트 그룹 추가)을 선택합니다.

이 예에서는 Outside Hosts의 상위 호스트 그룹 아래에 My Corporate DNS라는 이름으로 새 호스트 그룹이 생성됩니다.



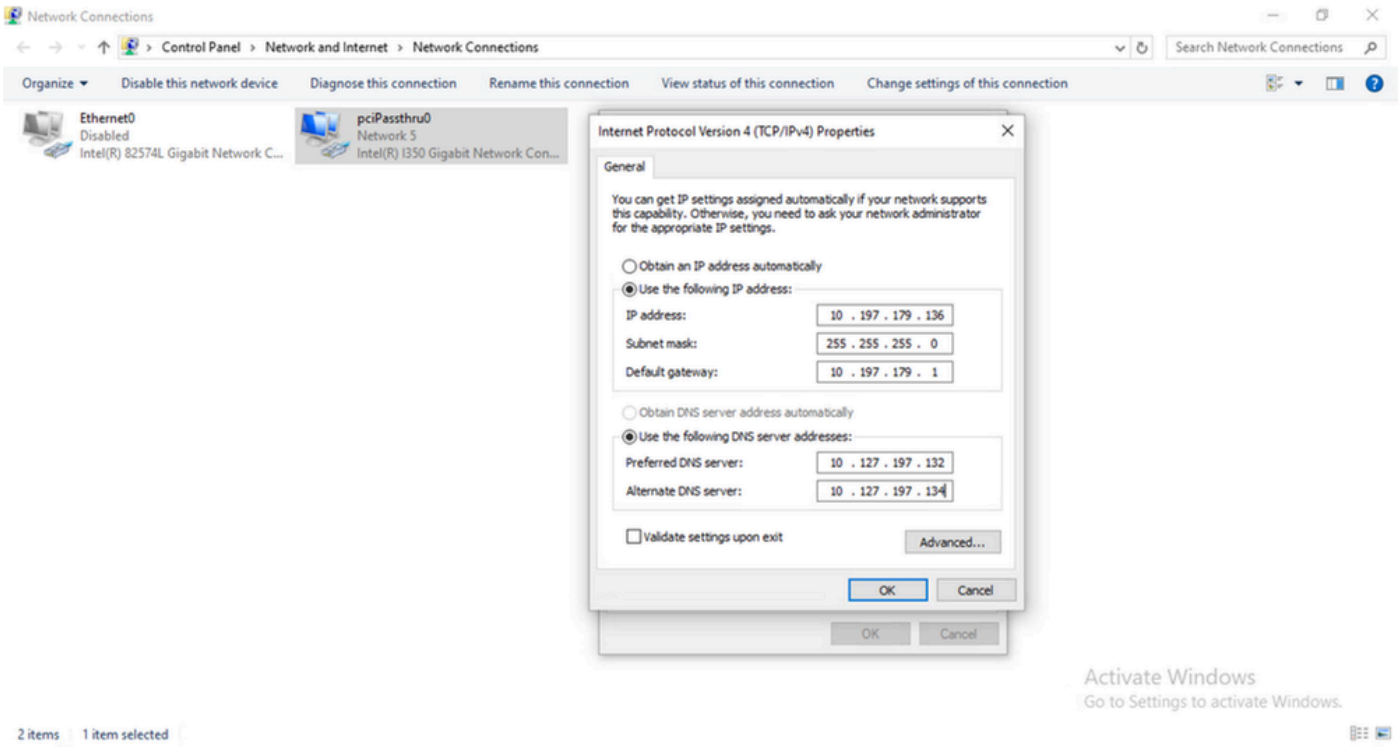



참고: 이 예에서 IP 10.127.197.132 및 10.127.197.134는 엔드유저가 사용할 DNS 서버로

사용되며, 이는 네트워크 아키텍처에 따라 실제 네트워크 환경에서 다를 수 있습니다.

---

데모에 사용되는 테스트 랩 PC는 정적 IP 10.197.179.136(만든 My Trusted Networks 호스트 그룹에 속함) 및 DNS 10.127.197.132 및 10.127.197.134(만든 My Corporate DNS 호스트 그룹에 속함)로 구성됩니다.



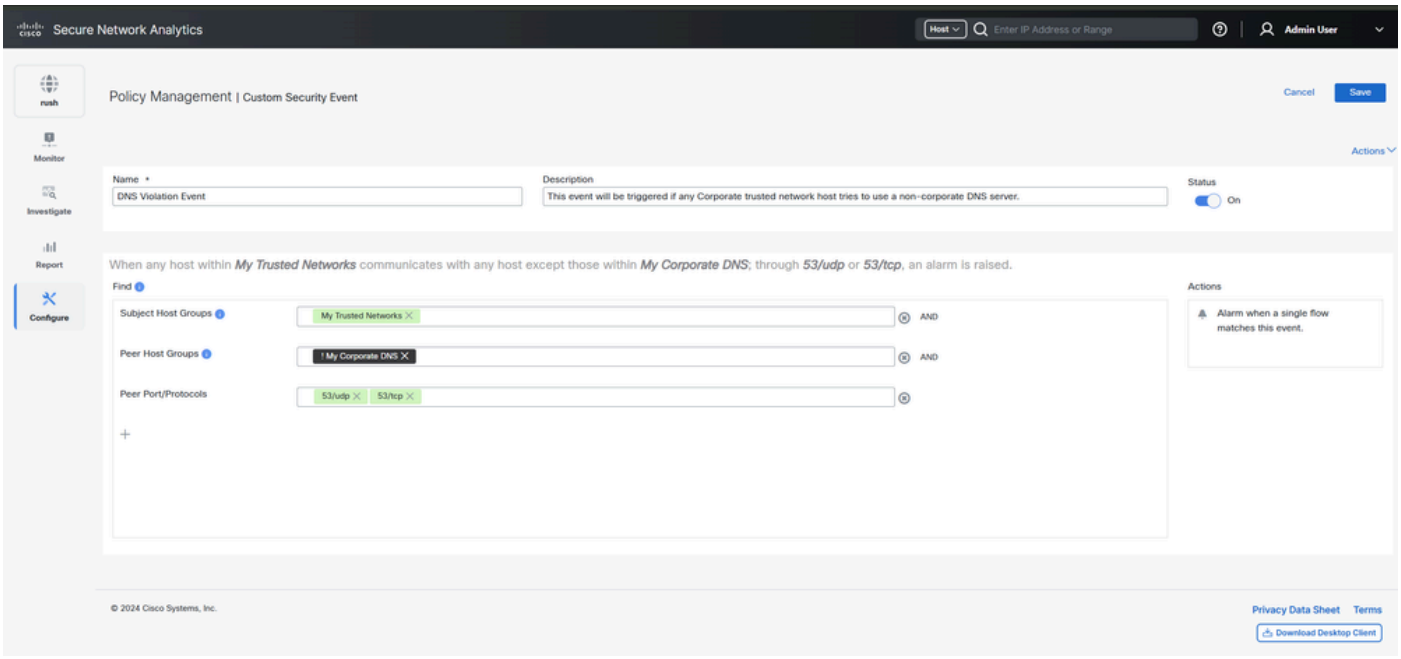

3단계: 내부 사용자가 외부 DNS 서버에 연결할 때 이를 탐지하도록 맞춤형 경고 시스템을 설정하여, 잠재적으로 트래픽을 악의적인 외부 사이트로 리디렉션할 수 있는 권한이 없는 DNS 서버에 대한 연결을 차단하는 경보를 트리거합니다. 경보가 활성화되면 Cisco Secure Network Analytics는 PxGrid를 통해 적응형 네트워크 제어 정책을 채택하여 Cisco ISE와 협력하여 이러한 무단 DNS 서버를 사용하여 호스트를 격리합니다.

Configure(구성) > Policy Management(정책 관리)로 이동합니다.

다음과 같은 정보를 사용하여 사용자 지정 이벤트를 생성합니다.

- 이름:DNS 위반 이벤트
- 주체 호스트 그룹: 내 신뢰할 수 있는 네트워크
- 피어 호스트 그룹: (Not) 내 회사 DNS.
- 피어 포트/프로토콜: 53/UDP 53/TCP

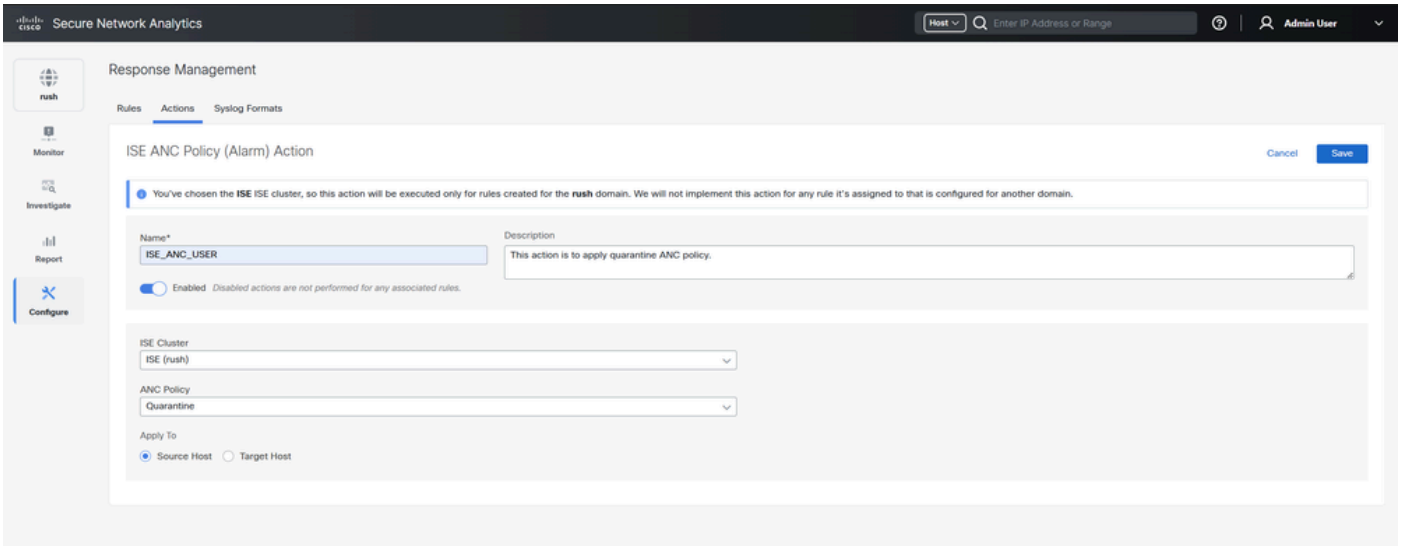
즉, My Trusted Networks(호스트 그룹) 내 호스트가 53/up 또는 53/tcp를 통해 My Corporate DNS(호스트 그룹) 내 호스트를 제외한 다른 호스트와 통신할 경우 경보가 발생합니다.



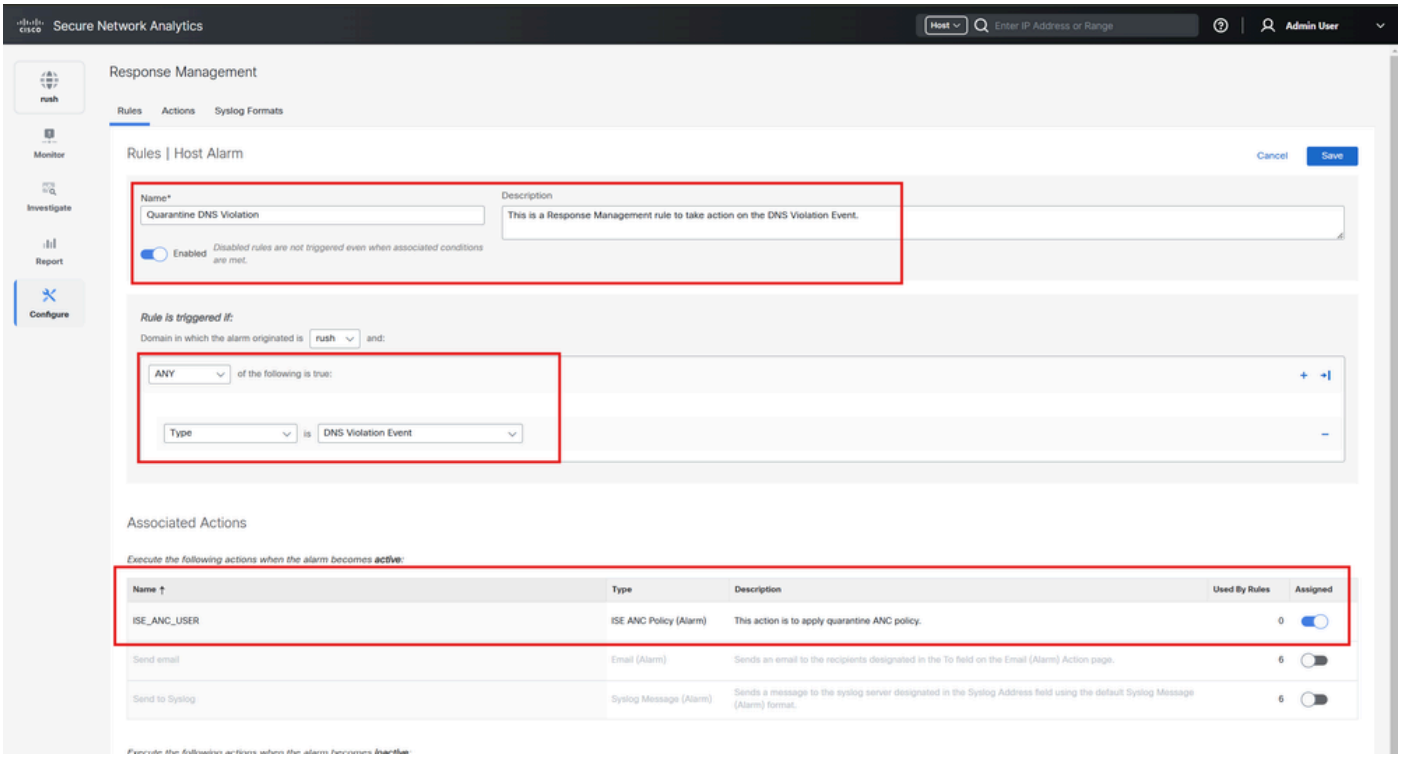

4단계: 수행할 응답 관리 작업을 구성하고 나중에 생성된 응답 관리 규칙에 적용할 수 있습니다.

Configure(구성) > Response Management(응답 관리) > Actions(작업)로 이동하고 Add New Action(새 작업 추가)을 클릭한 다음 ISE ANC Policy (Alarm)를 선택합니다.

위반에 대한 격리 정책 또는 무단 서버에 대한 연결을 구현하기 위해 이름을 지정하고 알림을 받을 특정 Cisco ISE 클러스터를 선택합니다.



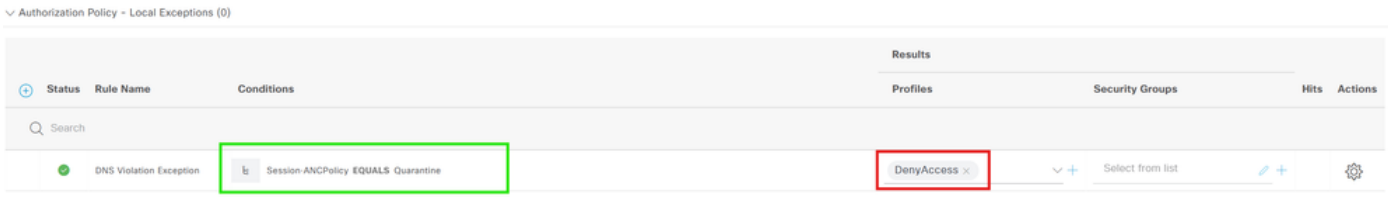

5단계: Rules(규칙) 섹션에서 새 규칙을 생성합니다. 이 규칙은 내부 네트워크 내의 호스트가 권한 없는 DNS 서버로 DNS 트래픽을 전송하려고 시도할 때마다 이전에 정의된 Action을 적용합니다. Rule is trigged if 섹션에서 Type을 선택하고 앞서 생성한 사용자 지정 이벤트를 선택합니다.
Associated Actions(연결된 작업)에서 이전에 구성된 ISE ANC Alarm(ISE ANC 경보) 작업을 선택합니다.

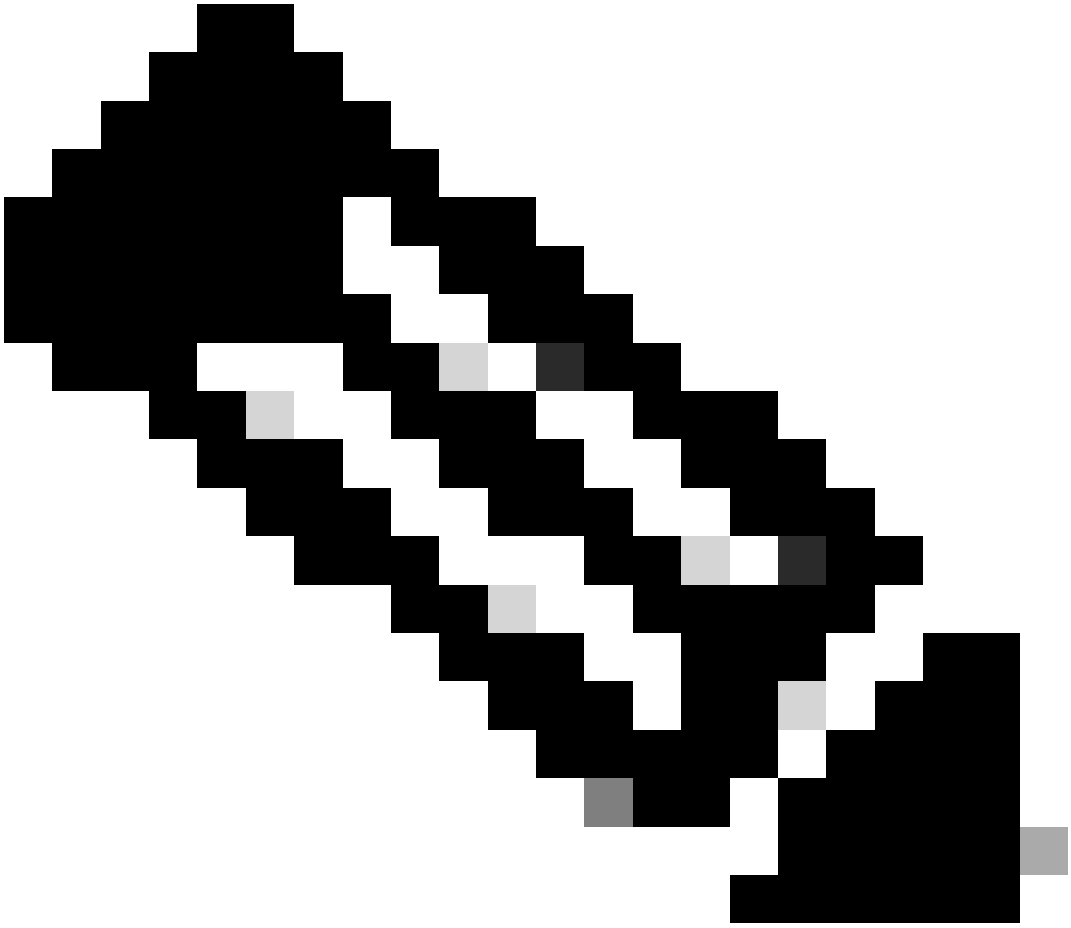



4. 이벤트를 트리거할 때 Stealthwatch에서 시작한 작업에 응답하도록 Cisco ISE를 구성합니다.

Cisco ISE GUI에 로그인하고 Policy(정책) > Policy Sets(정책 집합) > Authorization Policy(권한 부여 정책) - Local Exceptions(로컬 예외) > Create new Policy(새 정책 생성)에서 Policy set(정책 집합) > Create(선택)를 선택합니다.

- 이름: DNS 위반 예외
- 조건: 세션: ANCPolicy EQUALS 격리
- 권한 부여 프로파일: 액세스 거부



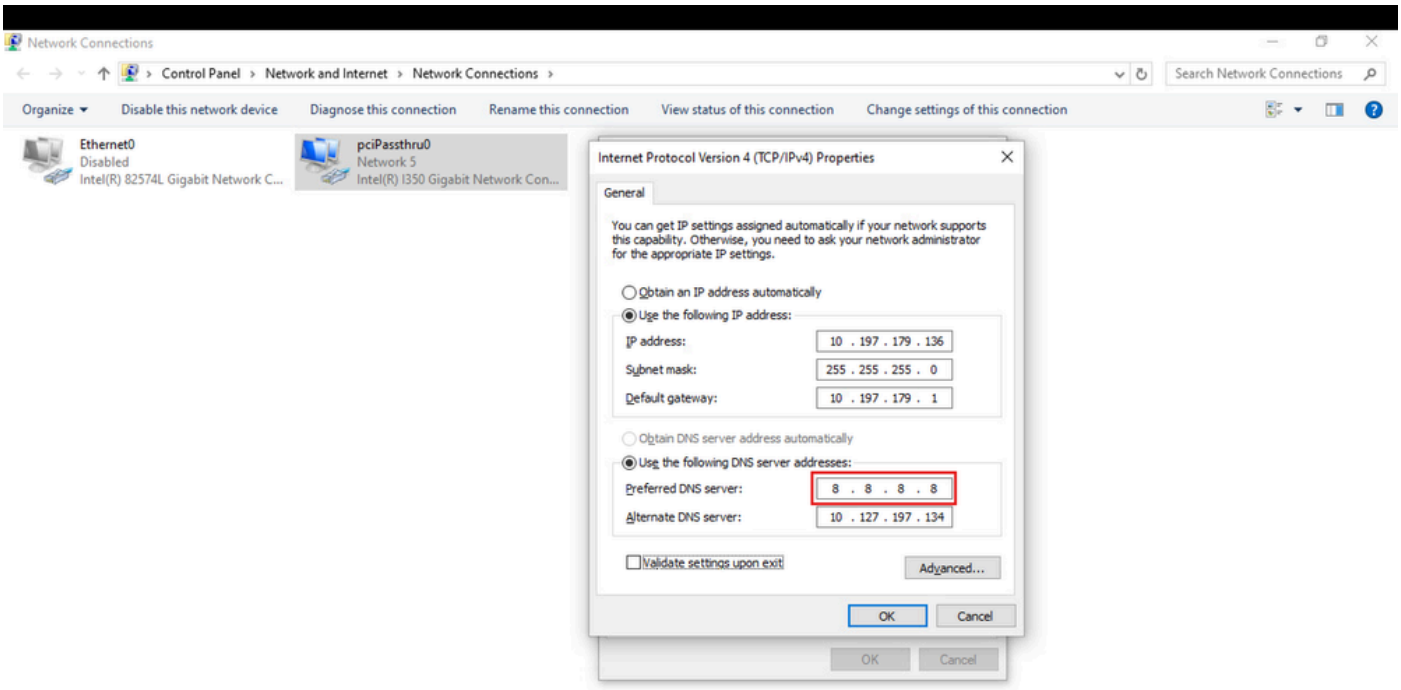


참고: 이 예에서는 DNS 위반 이벤트가 트리거되면 컨피그레이션에 따라 사용자에 대한 액세스가 거부됩니다

---

다음을 확인합니다.

활용 사례를 보여주기 위해 엔드포인트의 DNS 항목이 8.8.8.8로 변경되었으며, 이는 구성된 DNS 위반 이벤트를 트리거합니다. DNS 서버는 My Corporate DNS 서버의 호스트 그룹에 속하지 않으므로 이벤트를 트리거하여 엔드포인트에 대한 액세스를 거부합니다.




C9300 스위치에서 show flow monitor IPv4_NETFLOW 캐시를 사용하여 확인합니다 | 8.8.8.8 명령에서 흐름을 캡처하여 Flow Collector로 전송하는 것을 확인할 수 있습니다. IPv4_NETFLOW는 스위치 컨피그레이션에 구성됩니다.

<#root>

IPV4 SOURCE ADDRESS:

**10.197.179.136**

IPV4 DESTINATION ADDRESS:

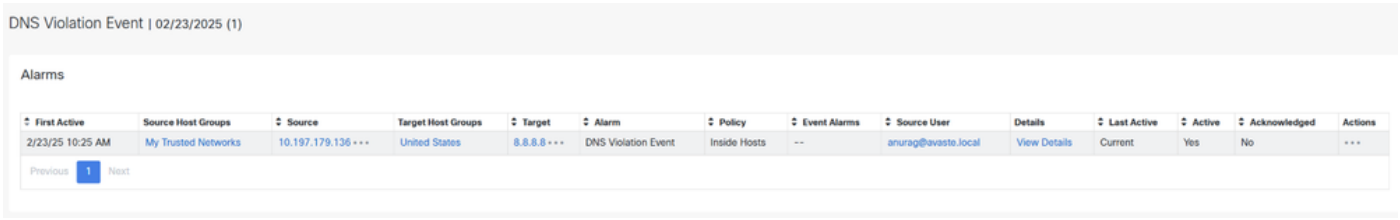
**8.8.8.8**

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

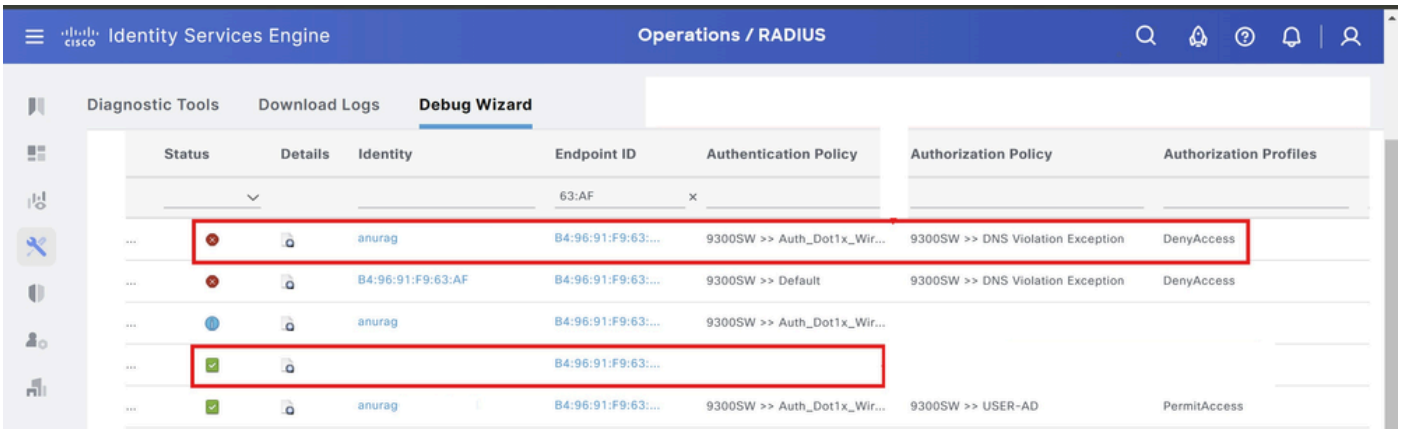
Stealthwatch에서 이벤트가 트리거되면 Monitor(모니터링) > Security Insight Dashboard(보안 인사이트 대시보드)로 이동합니다.




Monitor(모니터링) > Integration(통합) > ISE ANC Policy Assignments(ISE ANC 정책 할당)로 이동합니다.

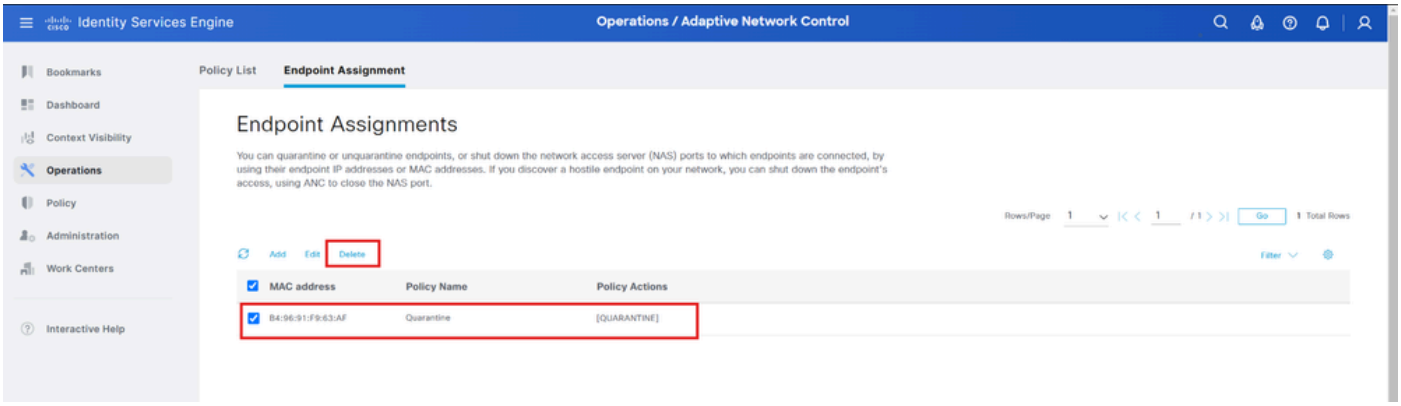
Cisco Secure Network Analytics에서 PxGrid 및 Cisco ISE를 통해 적응형 네트워크 제어 정책을 성공적으로 구현하여 호스트를 격리했는지 확인합니다.


마찬가지로 Cisco ISE에서 Operations(운영) > RADIUS > Livelogs(라이브 로그)로 이동하고 엔드포인트에 대해 필터를 적용합니다.




로컬 예외 정책 DNS 위반 예외에 따라, CoA(Change of Authorization)는 ISE에 의해 실행되며 액세스 ISE는 엔드포인트에 거부됩니다.

엔드포인트에서 교정 작업이 수행된 후 엔드포인트의 MAC 주소를 제거하려면 Operations(운영) > Adaptive Network Control(적응형 네트워크 제어) > Endpoint Assignments(엔드포인트 할당) > Delete(삭제)에서 MAC을 제거합니다.



Cisco ISE에 대한 참조를 기록합니다.

Cisco ISE의 pxgrid(pxgrid-server.log) 구성 요소에 대해 TRACE 레벨로 설정된 특성은 pxgrid-server.log 파일에 표시됩니다.

<#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**

"}

# 문제 해결

## 격리된 엔드포인트는 정책 변경 후 인증을 갱신하지 않습니다.

문제

정책 변경 또는 추가 ID로 인해 인증에 실패했으며 재인증이 수행되지 않습니다. 인증이 실패하거

나 문제의 엔드포인트가 네트워크에 연결할 수 없는 상태로 남아 있습니다. 이 문제는 사용자 역할에 할당 된 상태 정책에 따라 상태 평가에 실패 한 클라이언트 컴퓨터에서 종종 발생 합니다.

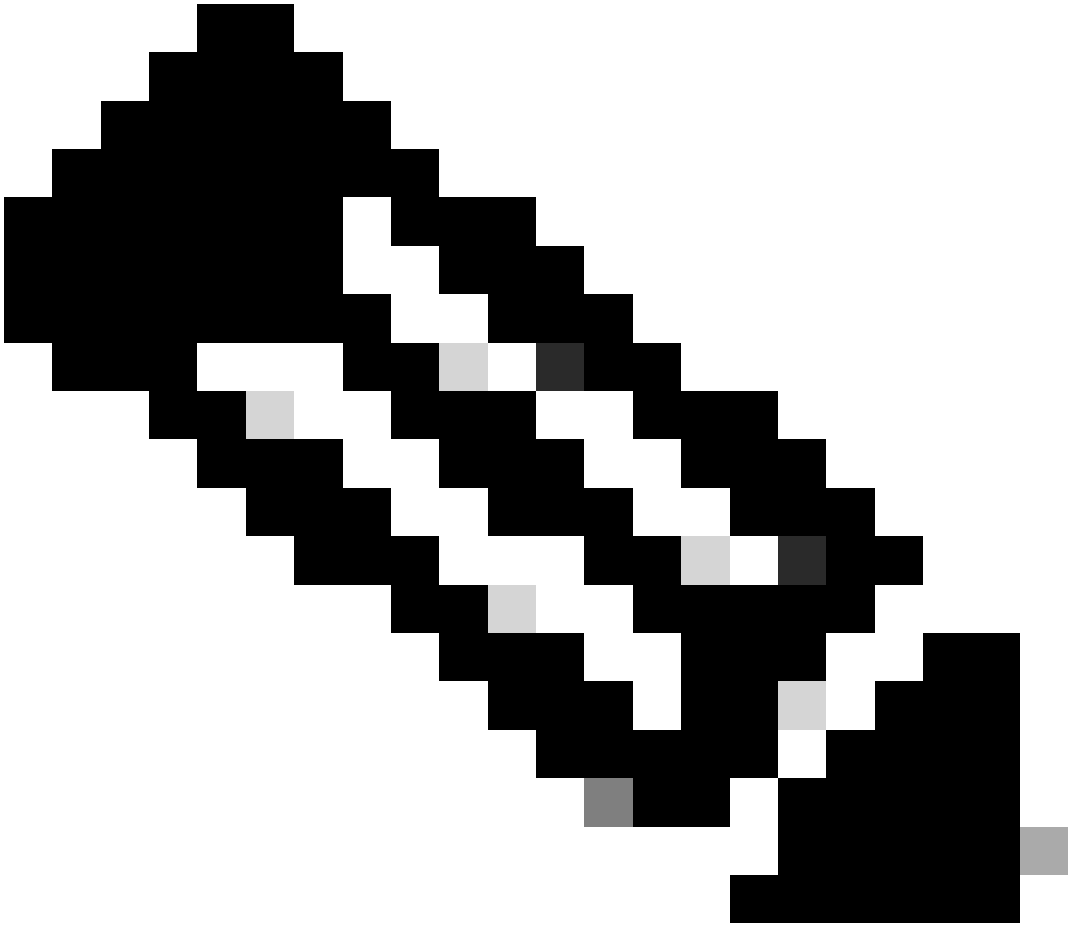
가능한 원인

클라이언트 컴퓨터에서 인증 타이머 설정이 올바르게 설정되지 않았거나 스위치에서 인증 간격이 올바르게 설정되지 않았습니다.

솔루션

이 문제에 대한 몇 가지 해결 방법이 있습니다.

1. 지정된 NAD 또는 스위치에 대한 Cisco ISE의 Session Status Summaryreport(세션 상태 요약 보고서)를 확인하고 인터페이스에 적절한 인증 간격이 구성되어 있는지 확인합니다.
2. NAD/switch에서 show running configuration을 입력하고 인터페이스가 적절한 인증 타이머 재시작 설정으로 구성되었는지 확인합니다. (예: 인증 타이머는 15를 다시 시작하고, 인증 타이머는 15를 다시 인증합니다).
3. 인터페이스 종료 및 no shutdown을 입력하여 NAD/스위치의 포트를 바운스하고 Cisco ISE에서 재인증 및 잠재적 컨피그레이션 변경을 적용합니다.

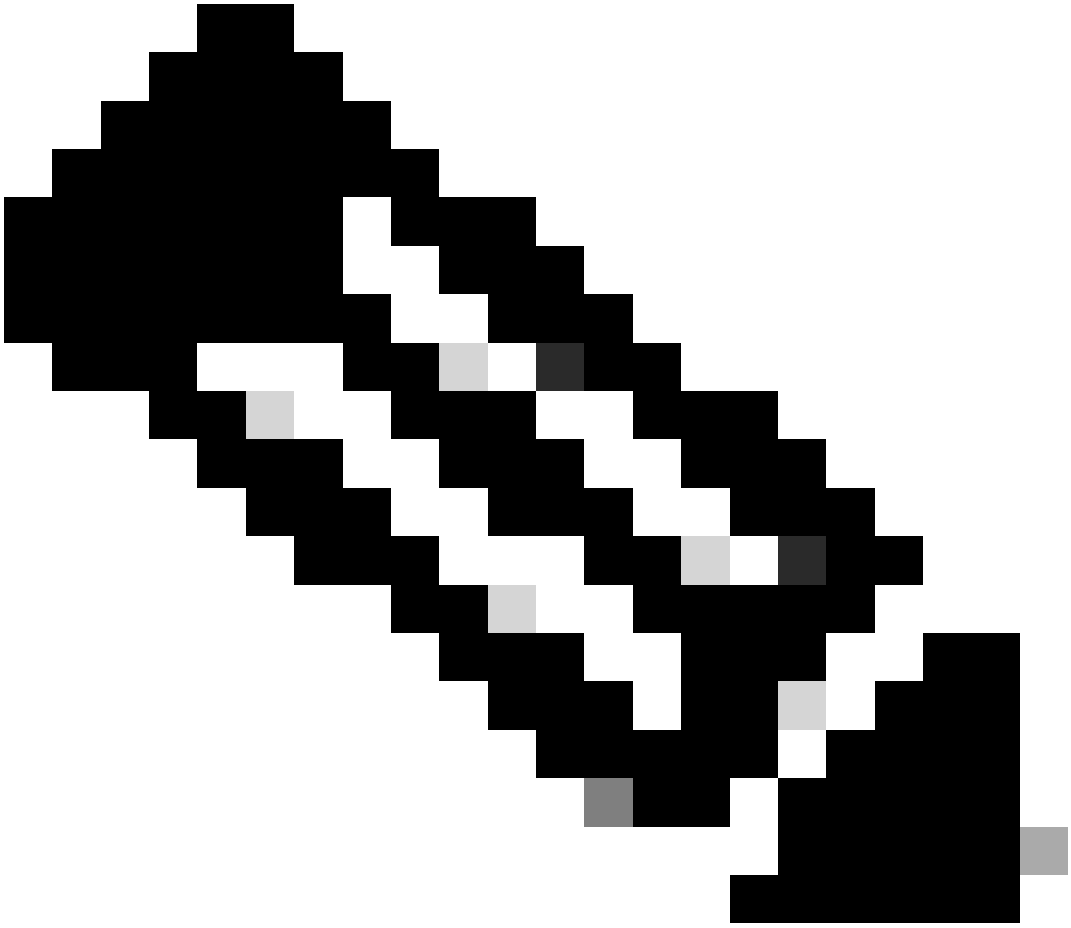


참고: CoA에는 MAC 주소 또는 세션 ID가 필요하므로 네트워크 디바이스 SNMP 보고서에 표시된 포트를 반송하지 않는 것이 좋습니다.

---

IP 주소 또는 MAC 주소를 찾을 수 없을 때 ANC 작업 실패

엔드포인트에 대한 활성 세션에 IP 주소에 대한 정보가 포함되어 있지 않으면 엔드포인트에서 수행하는 ANC작업이 실패합니다. 이는 해당 엔드포인트의 MAC 주소 및 세션 ID에도 적용됩니다.



참고: ANC를 통해 엔드포인트의 권한 부여 상태를 변경하려면 엔드포인트의 IP 주소 또는 MAC 주소를 제공해야 합니다. 엔드포인트의 활성 세션에서 IP 주소 또는 MAC 주소를 찾을 수 없는 경우 다음과 같은 오류 메시지가 표시됩니다. "이 MAC 주소, IP 주소 또는 세션 ID에 대한 활성 세션을 찾을 수 없습니다."

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.