Configureer ANC op ISE 3.3 en Stealthwatch 7.5.1

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Netwerkdiagram](#)

[Stapsgewijze configuratie](#)

[Verifiëren](#)

[Probleemoplossing](#)

- [Quarantined Endpoints verlengen verificatie niet na beleidswijziging](#)
  - [Probleem](#)
  - [Mogelijke oorzaken](#)
  - [Oplossing](#)
  - [ANCO-bewerkingen mislukken wanneer IP-adres of MAC-adres niet wordt gevonden](#)

Inleiding

Dit document beschrijft Configuration of Rapid Threat Containment (Adaptive Network Control) op Cisco ISE® versie 3.3 en Stealthwatch.

Voorwaarden

Cisco raadt kennis over deze onderwerpen aan:

- Identity Services Engine (ISE)
- Platform Exchange Grid (PXGrid)
- Secure Network Analytics (Stealthwatch)
- Rapid Threat Containment (adaptieve netwerkcontrole - ANC).

In dit document wordt ervan uitgegaan dat de Cisco Identity Services Engine is geïntegreerd met Secure Network Analytics (Stealthwatch) met behulp van pxGrid dat ANC-ingeschakeld is.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze software en versies:

- Cisco Identity Services Engine (ISE) versie 3.3

- Secure Network Analytics (Stealthwatch) 7.5.1
- Catalyst 9300

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

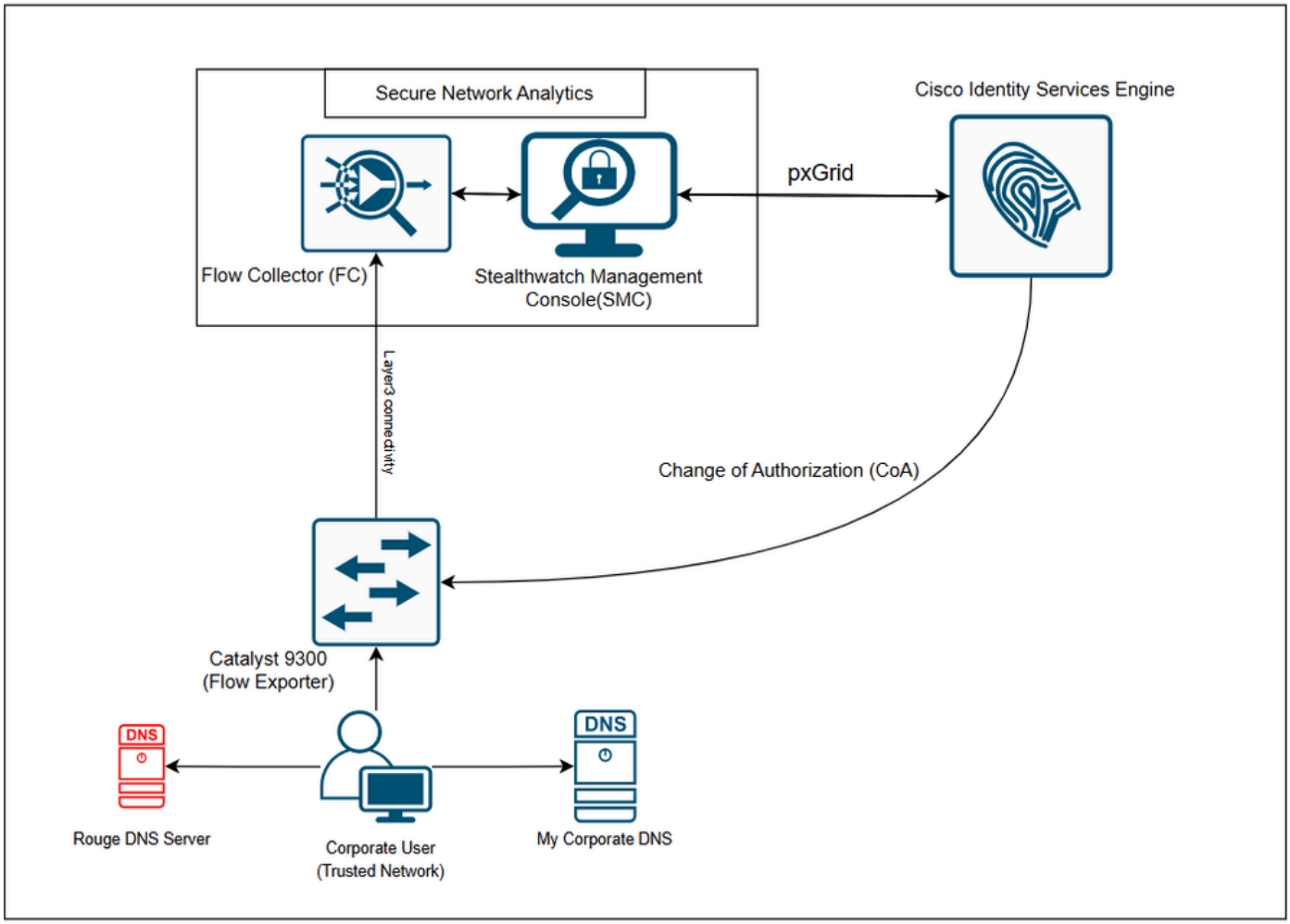
Cisco Secure Cloud-analyses (nu onderdeel van Cisco XDR) kunnen gebruikersattributiegegevens ophalen van Cisco Identity Services Engine (ISE) met behulp van pxGrid. Deze integratie maakt rapportage van gebruikersactiviteit in de Secure Cloud Analytics Event Viewer mogelijk.

De combinatie van Secure Network Analytics (voorheen Stealthwatch) en Cisco Identity Services Engine (ISE) helpt organisaties een 360°-weergave te krijgen, sneller te reageren op bedreigingen en een groeiende digitale business te beveiligen. Zodra Secure Network Analytics abnormaal verkeer detecteert, wordt een waarschuwing gegeven, waarbij de beheerder de optie krijgt om de gebruiker in quarantaine te plaatsen. pxGrid maakt het mogelijk dat Secure Network Analytics rechtstreeks aan Identity Services Engine wordt overgedragen.

In dit voorbeeld wordt beschreven hoe u uw bedrijfsDNS-server kunt gebruiken om u te beschermen tegen bedreigingen via internet. Het is de bedoeling om een aangepast waarschuwingsmechanisme in te stellen dat triggers activeert wanneer interne gebruikers verbinding maken met externe DNS servers. Dit initiatief is ontworpen om verbindingen met niet-geautoriseerde DNS-servers te blokkeren die verkeer kunnen omleiden naar schadelijke externe sites.

Wanneer een waarschuwing wordt geactiveerd, coördineert Cisco Secure Network Analytics met Cisco ISE om de host die toegang heeft tot onbevoegde DNS-servers in quarantaine te plaatsen met behulp van een Adaptive Network Control Policy via PxGrid.

Netwerkdiagram



Zoals afgebeeld in het diagram:

- Een zakelijke gebruiker is verbonden met een C9300-switch die is geconfigureerd voor het exporteren van de IP-stromen en het verzenden van de gegevens naar de Flow Collector.
- Dezelfde zakelijke gebruiker is ingesteld op zakelijke DNS-servers van de gebruiker.
- Flow Collector is geïntegreerd met Stealthwatch Management Console (SMC)
- Stealthwatch Management Console (SMC) geïntegreerd via PxGrid met ISE.

Stapsgewijze configuratie

1. Bereid de switch voor op het bewaken en exporteren van stromen met behulp van netflow.

De basis stroomconfiguratie op een C9300 switch met 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
```

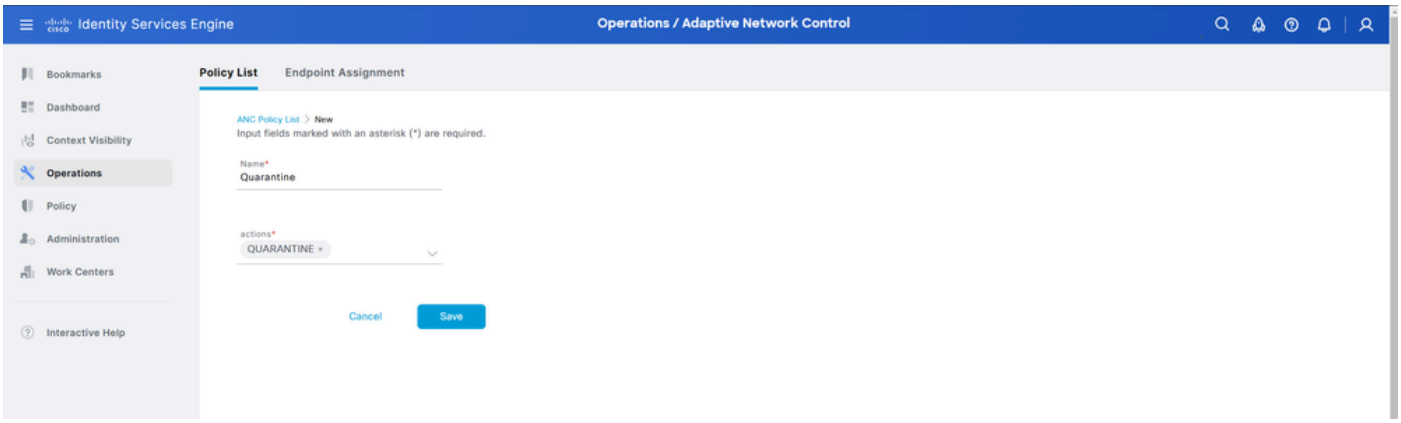
```
  collect transport tcp flags
  collect interface output
  collect counter bytes long
  collect counter packets long
  collect timestamp absolute first
  collect timestamp absolute last


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
```

Na voltooiing van de configuratie stelt het de C9300 in staat IP-stroomgegevens naar de Flow Collector te exporteren. De Flow Collector verwerkt en draagt deze gegevens vervolgens over naar de Stealthwatch Management Console (SMC) voor analyse en bewaking.

2. Schakel adaptieve netwerkbesturing in voor Cisco ISE.

ANC is standaard uitgeschakeld. ANC wordt alleen ingeschakeld wanneer pxGrid is ingeschakeld en blijft ingeschakeld tot u de service handmatig in het Admin-portal uitschakelt.

Selecteer Operations > Adaptieve netwerkcontrole > Beleidslijst > Toevoegen, en voer vervolgens Quarantaine in voor de beleidsnaam en quarantaine voor de actie.

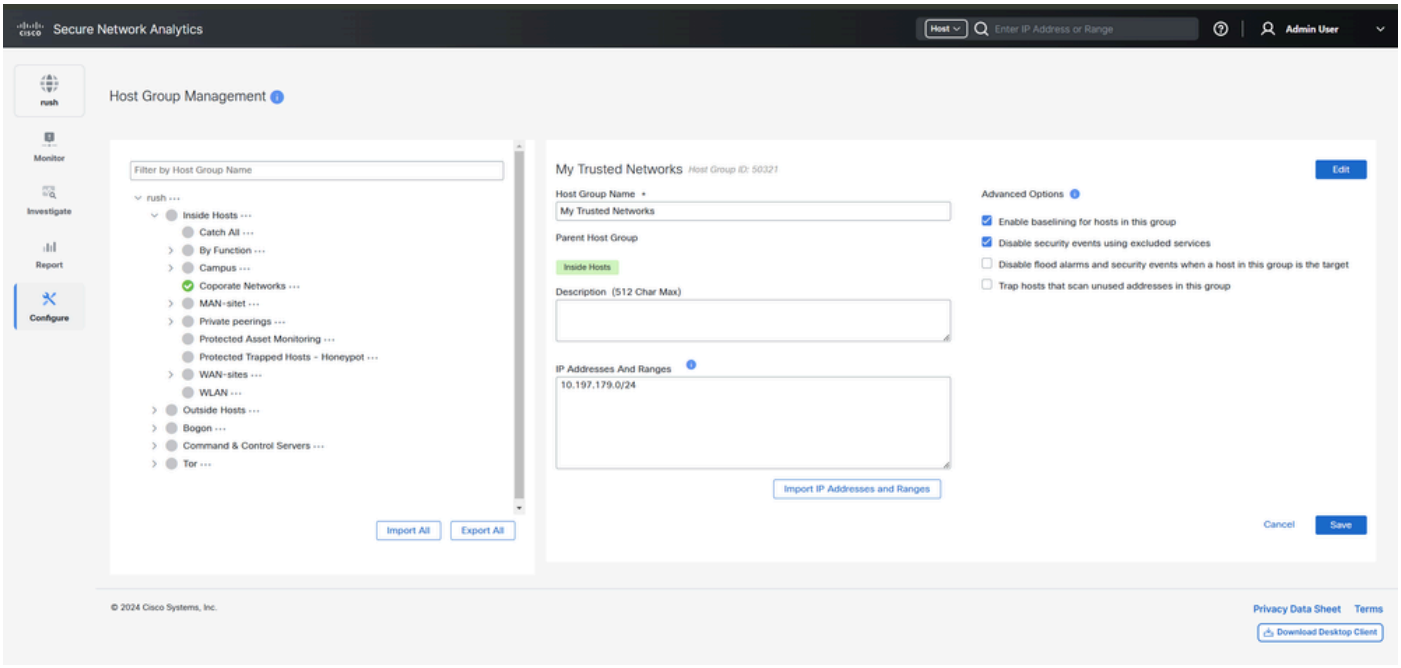


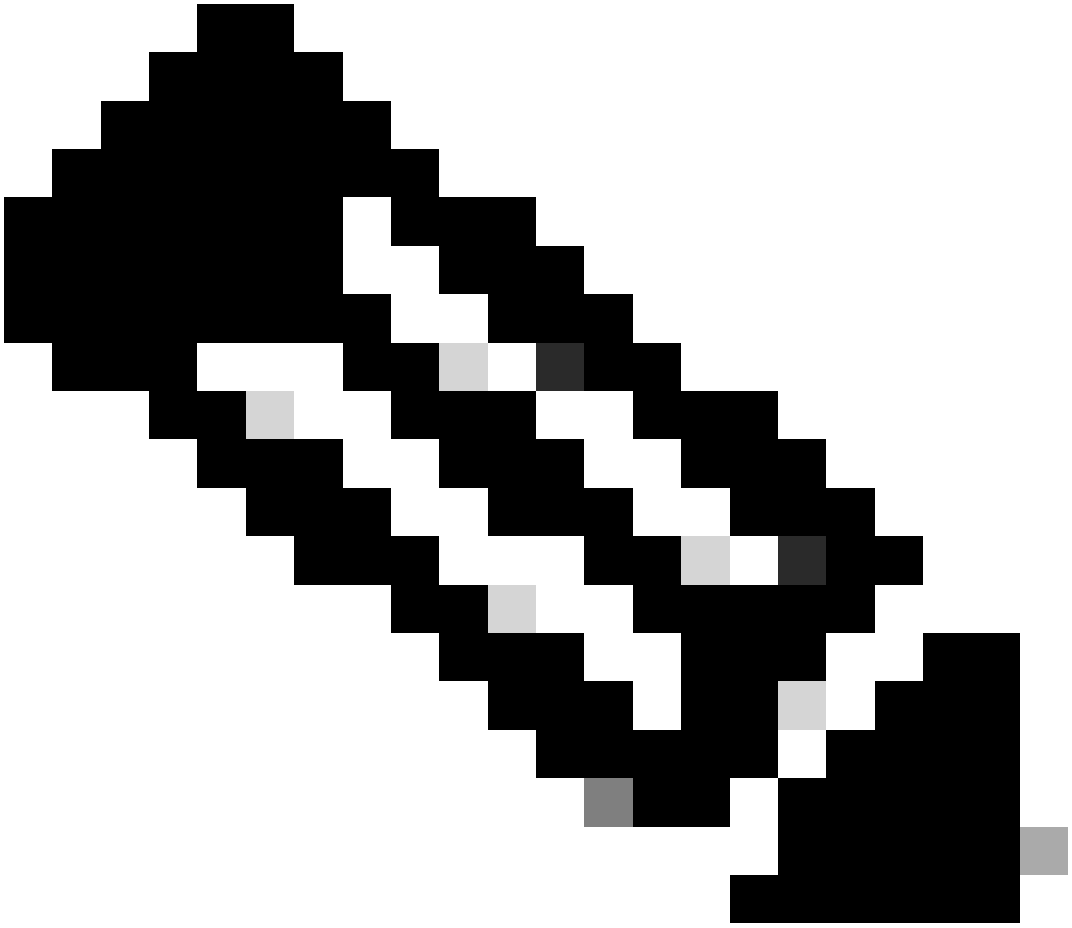
3. Configureer beveiligde netwerkanalyse voor gebeurtenistrigger- en responsbeheer voor snelle inperking van bedreigingen.

Stap 1: Log in de SMC GUI en navigeer om > Detectie > Beheer van hostgroep te configureren > Klik op het pictogram (...) (ellips) naast Inside Hosts en selecteer vervolgens Host Group toevoegen.

In dit voorbeeld wordt een nieuwe hostgroep gemaakt met de naam My Trusted Networks onder de moederhostgroep Inside Hosts.

Dit netwerk kan typisch aan de eindgebruikermachine worden toegewezen voor de controle van DNS gebruik.

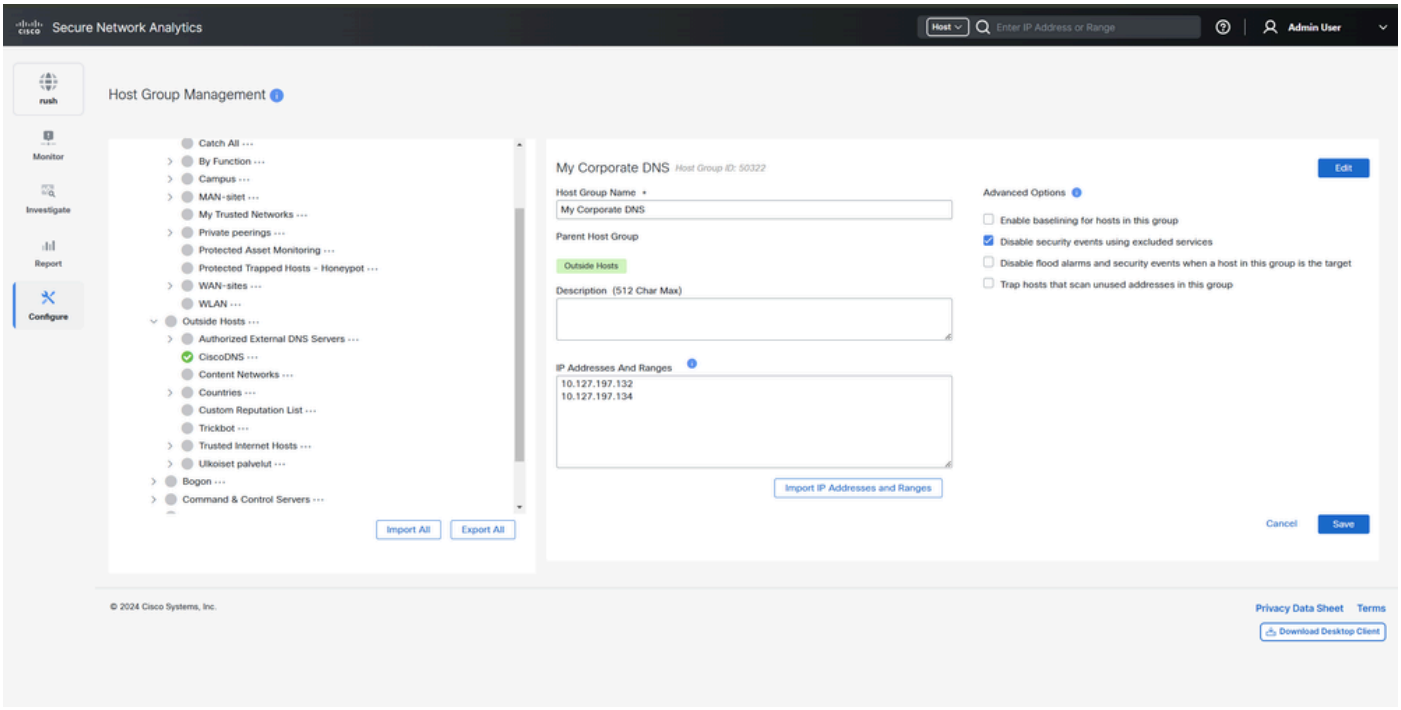


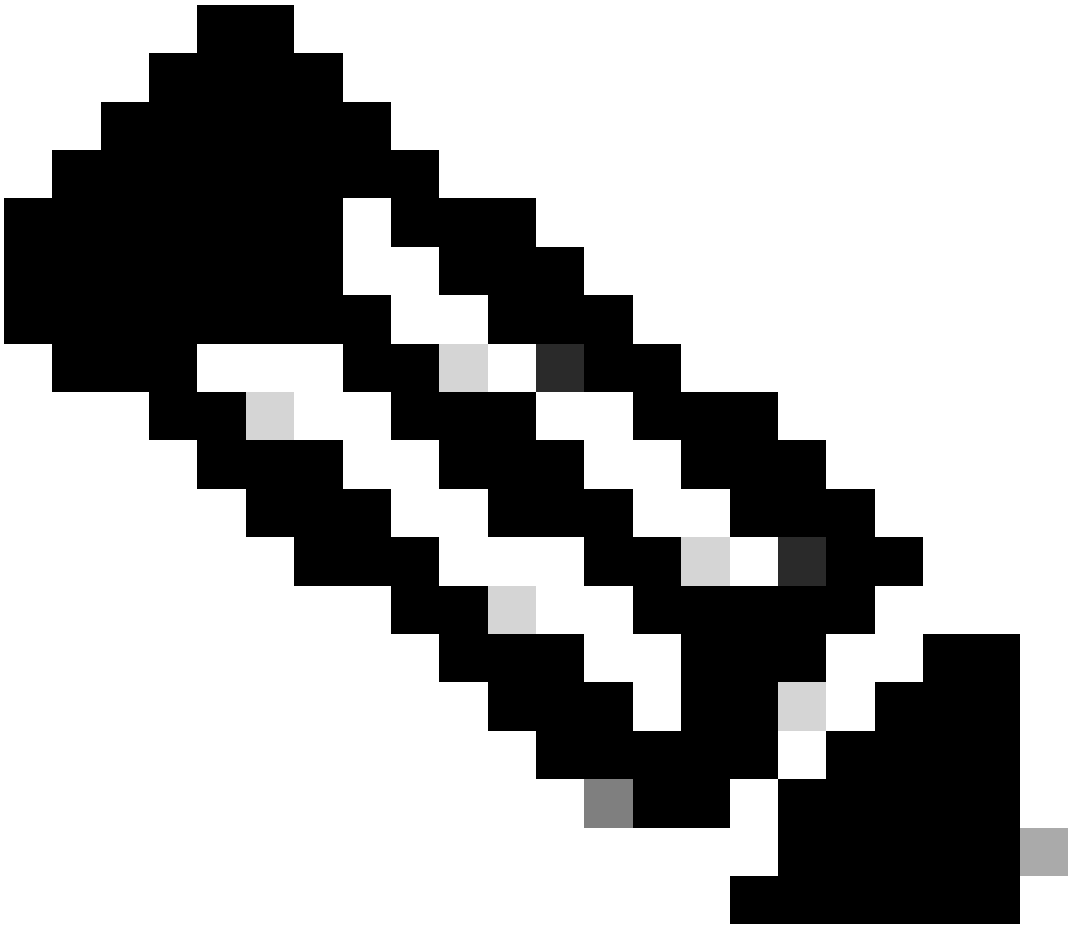


Opmerking: Bij dit voorbeeld wordt IP-subnetverbinding 10.197.179.0/24 gebruikt als LAN-subnetverbinding (Local Area Network). Dit kan per netwerkarchitectuur verschillen in de eigenlijke netwerkomgeving.

Stap 2: Log in de SMC GUI en navigeer om > Detectie > Beheer van hostgroep > Klik op (...) naast Outside Hosts en selecteer Add Host Group.

In dit voorbeeld wordt een nieuwe hostgroep gemaakt met de naam My Corporate DNS onder de moederhostgroep Outside Hosts.

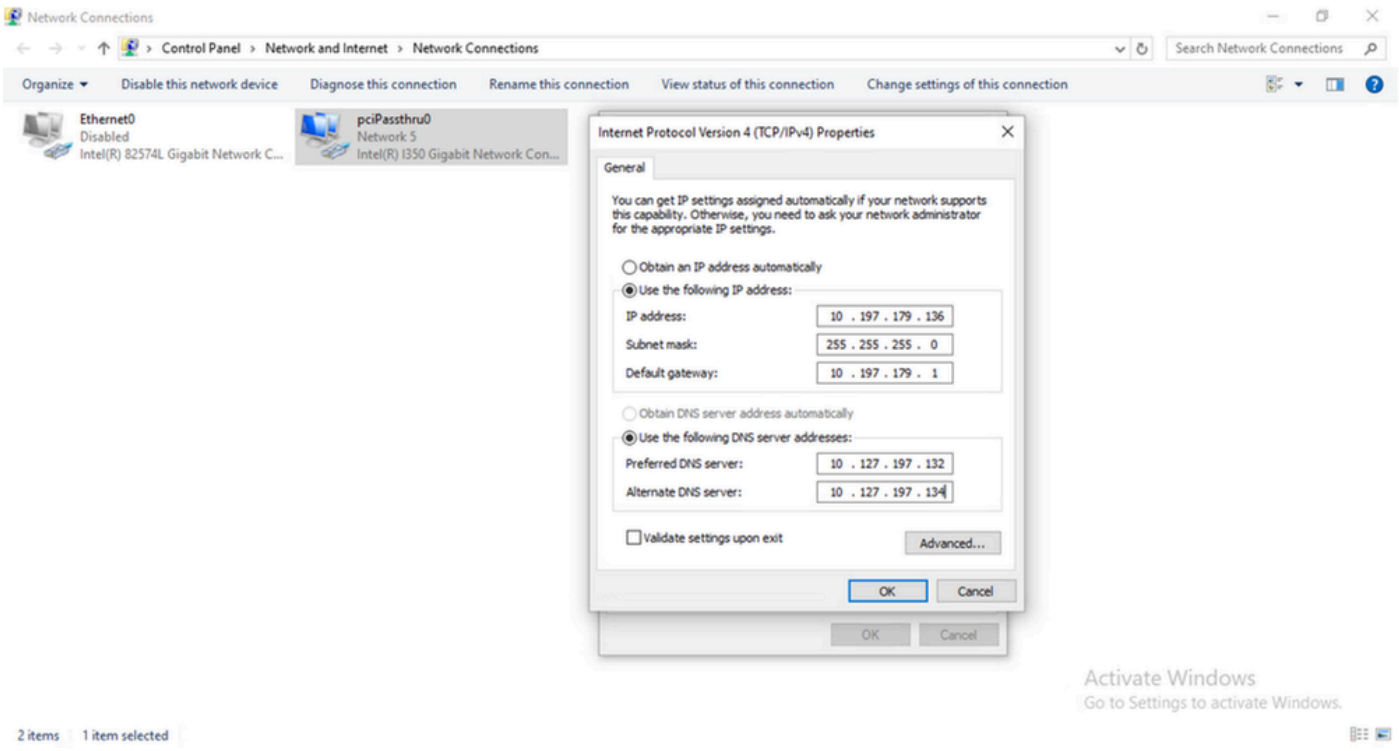




Opmerking: Bij dit voorbeeld worden IPs 10.127.197.132 en 10.127.197.134 gebruikt als

de gewenste DNS-servers die door de eindgebruikers moeten worden gebruikt. Dit kan in de werkelijke netwerkomgeving verschillen, afhankelijk van de netwerkarchitectuur.

De testlab-pc die voor demonstratie wordt gebruikt, is geconfigureerd met statische IP 10.197.179.136 (maakt deel uit van Mijn vertrouwde netwerkhostgroep gemaakt) en DNS 10.127.197.132 en 10.127.197.134 (maakt deel uit van Mijn zakelijke DNS-hostgroep gemaakt).



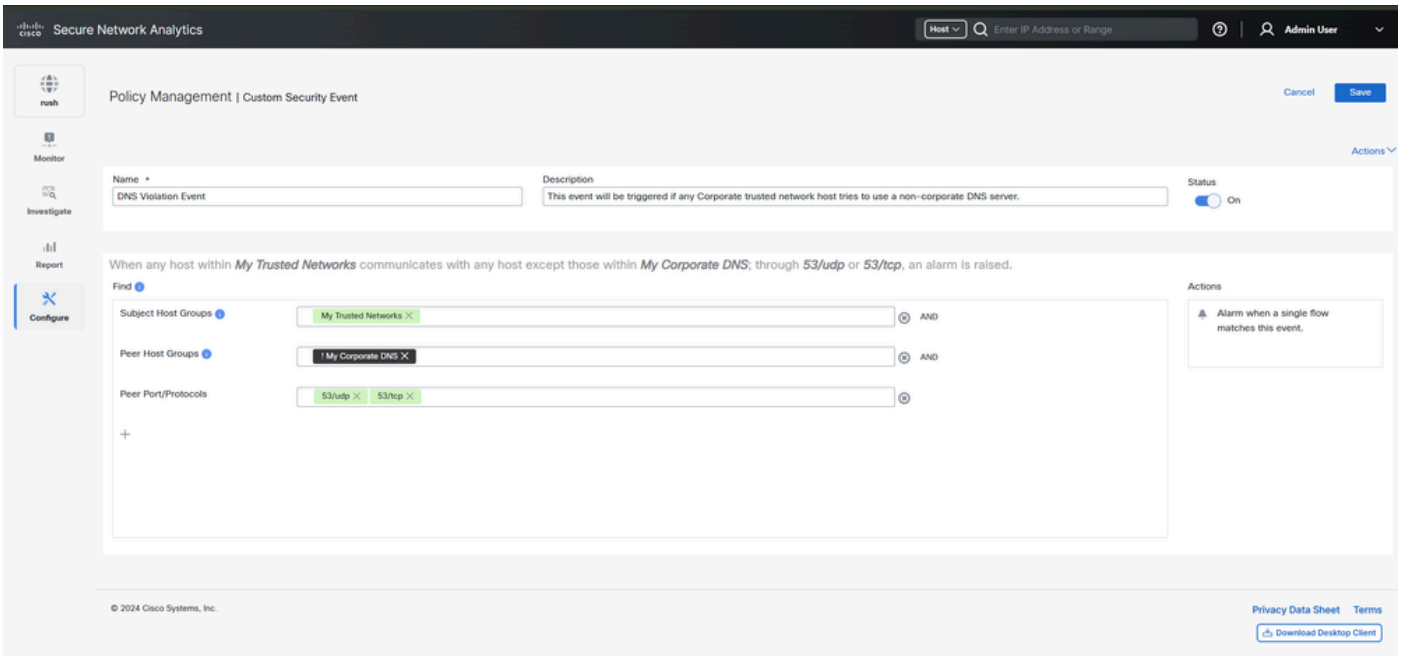
Stap 3: Stel een op maat gemaakt waarschuwingssysteem in om te detecteren wanneer interne gebruikers verbinding maken met externe DNS-servers, waarbij een alarm wordt geactiveerd om verbindingen met niet-geautoriseerde DNS-servers te blokkeren die mogelijk verkeer kunnen omleiden naar kwaadaardige externe sites. Zodra een alarm is geactiveerd, coördineert Cisco Secure Network Analytics met Cisco ISE om de host te isoleren met behulp van deze onbevoegde DNS-servers door gebruik te maken van een Adaptive Network Control Policy via PxGrid.

Blader naar Configureren > Beleidsbeheer.

Maak een Aangepaste Gebeurtenissen met de informatie:

- Naam:Gebeurtenis DNS-schending.
- Onderwerp hostgroepen: Mijn vertrouwde netwerken.
- Peer host-groepen : (Niet) My Corporate DNS.
- Peer poort/protocollen: 53/UDP 53/TCP-module

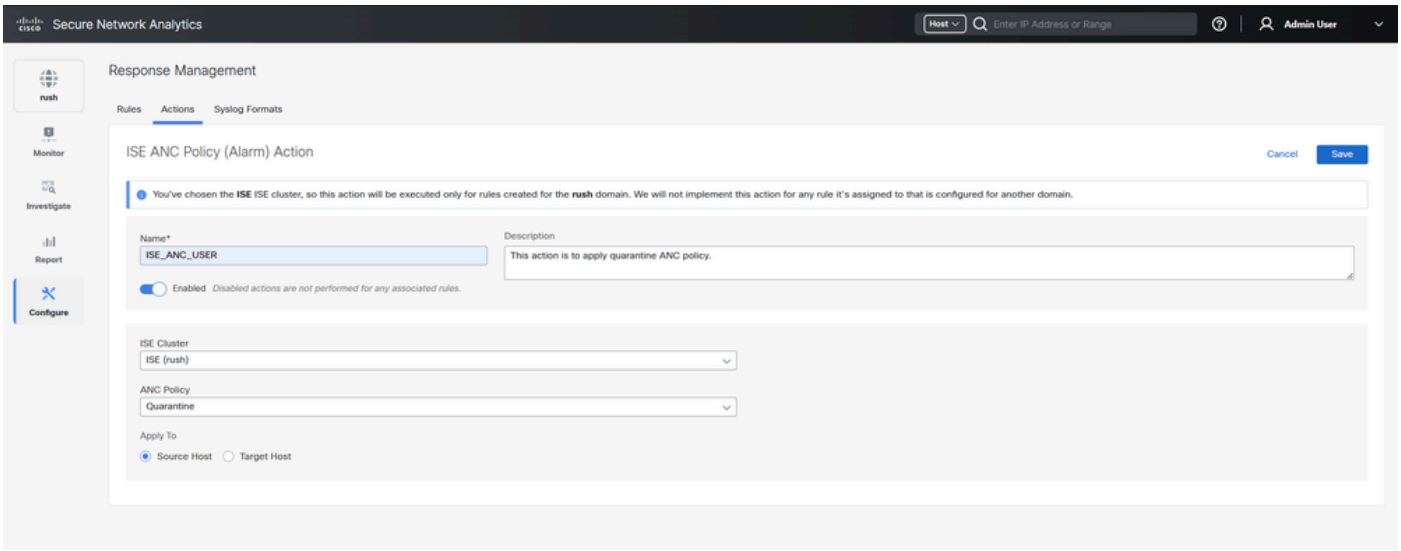
Dit betekent dat wanneer een host binnen My Trusted Networks (hostgroep) communiceert met een andere host dan die binnen My Corporate DNS (hostgroep) via 53/up of 53/tcp, een alarm wordt gegeven.



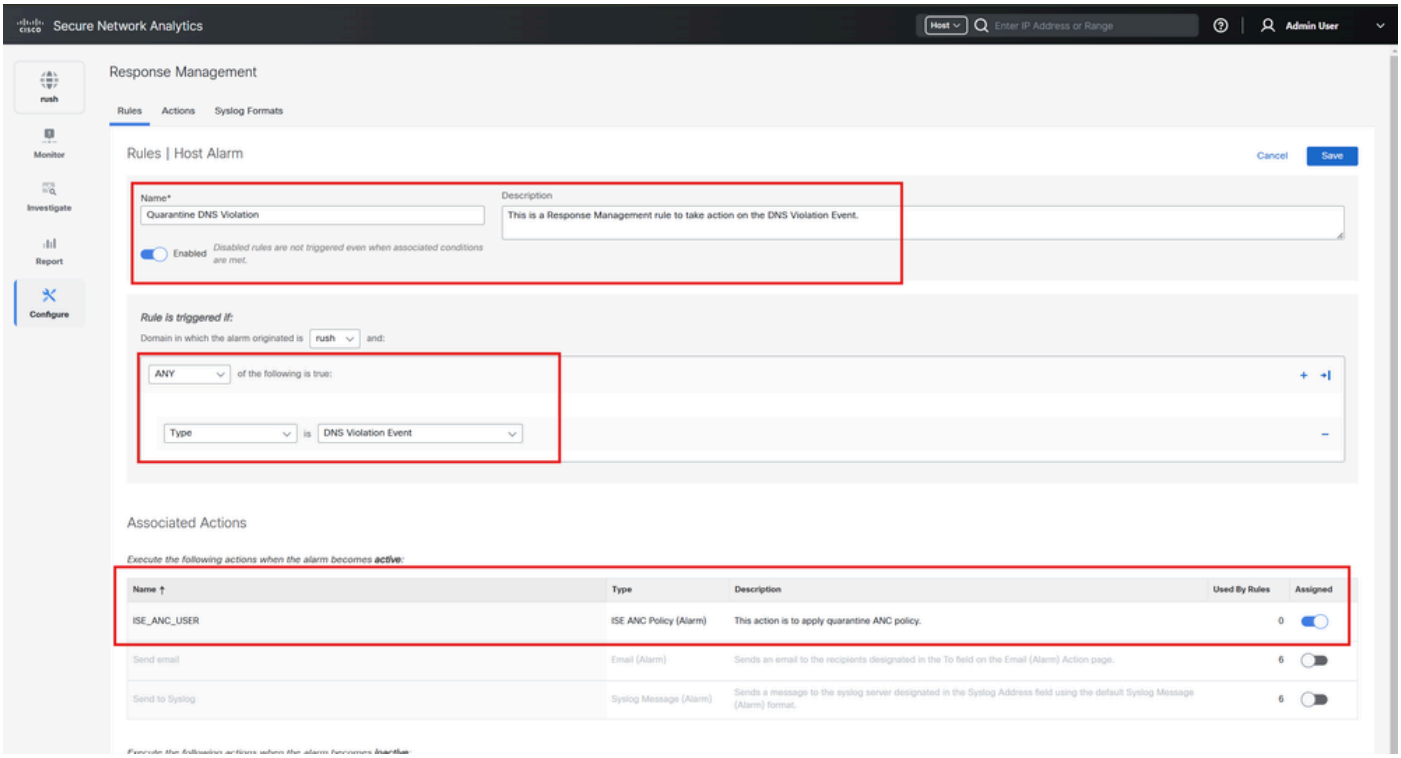
Stap 4: Configureer een actie voor responsbeheer die moet worden uitgevoerd en die later kan worden toegepast op de responsbeheerregel zodra deze is gemaakt.

Navigeer om te configureren > Response Management > Actions, klik op Add New Action en selecteer ISE ANC Policy (Alarm).

Wijs een naam toe en kies het specifieke Cisco ISE-cluster dat moet worden aangemeld om een quarantainebeleid voor eventuele schendingen of verbindingen met onbevoegde servers te implementeren.



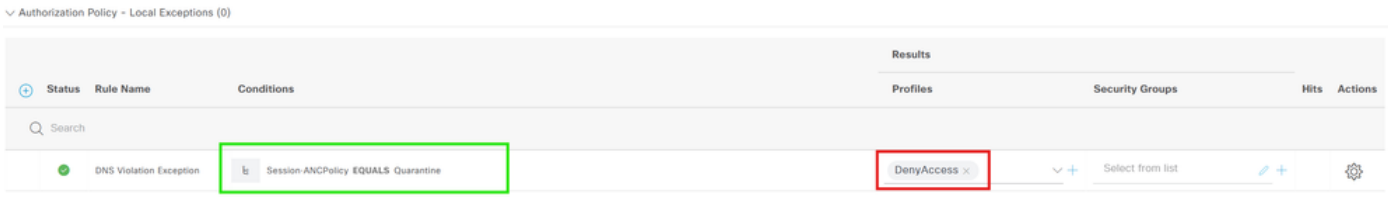
Stap 5: Maak een nieuwe regel onder het gedeelte Regels. Deze regel dwingt de eerder gedefinieerde actie af wanneer een host binnen het interne netwerk probeert DNS-verkeer naar onbevoegde DNS-servers te verzenden. In de Regel wordt geactiveerd als sectie, kies Type en selecteer de aangepaste gebeurtenis die eerder gemaakt is.
Selecteer onder Associated Actions de ISE ANC Alarmactie die eerder is geconfigureerd.

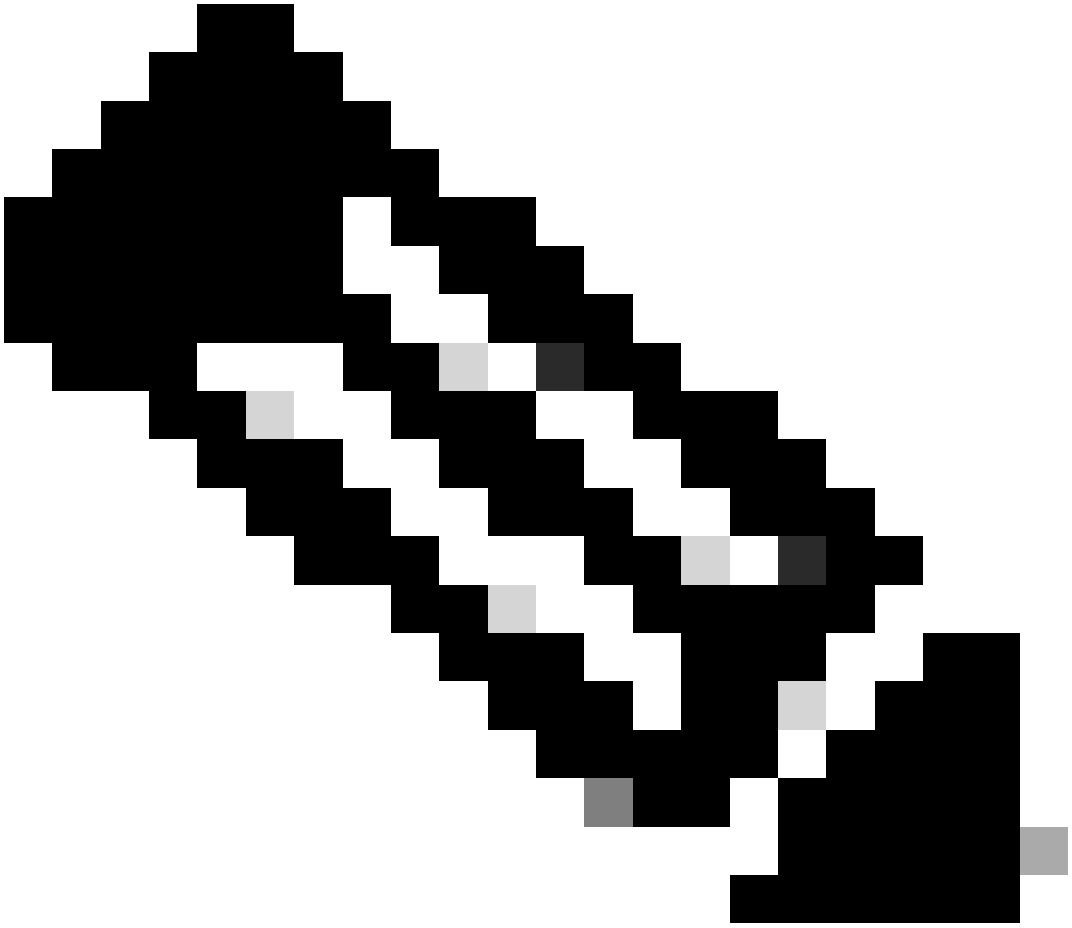


4. Configureer Cisco ISE om te reageren op acties die door Stealthwatch zijn geïnitieerd na het activeren van de gebeurtenis.

Log in op Cisco ISE GUI en navigeer naar beleid > Beleidssets > Kies de Beleidsset > onder Autorisatiebeleid - Lokale uitzonderingen > Nieuw beleid maken.

- Naam: Uitzondering voor DNS-schending
- Voorwaarden: Sessie: ANCP-beleid = quarantaine
- Autorisatieprofielen: Toegang weigeren

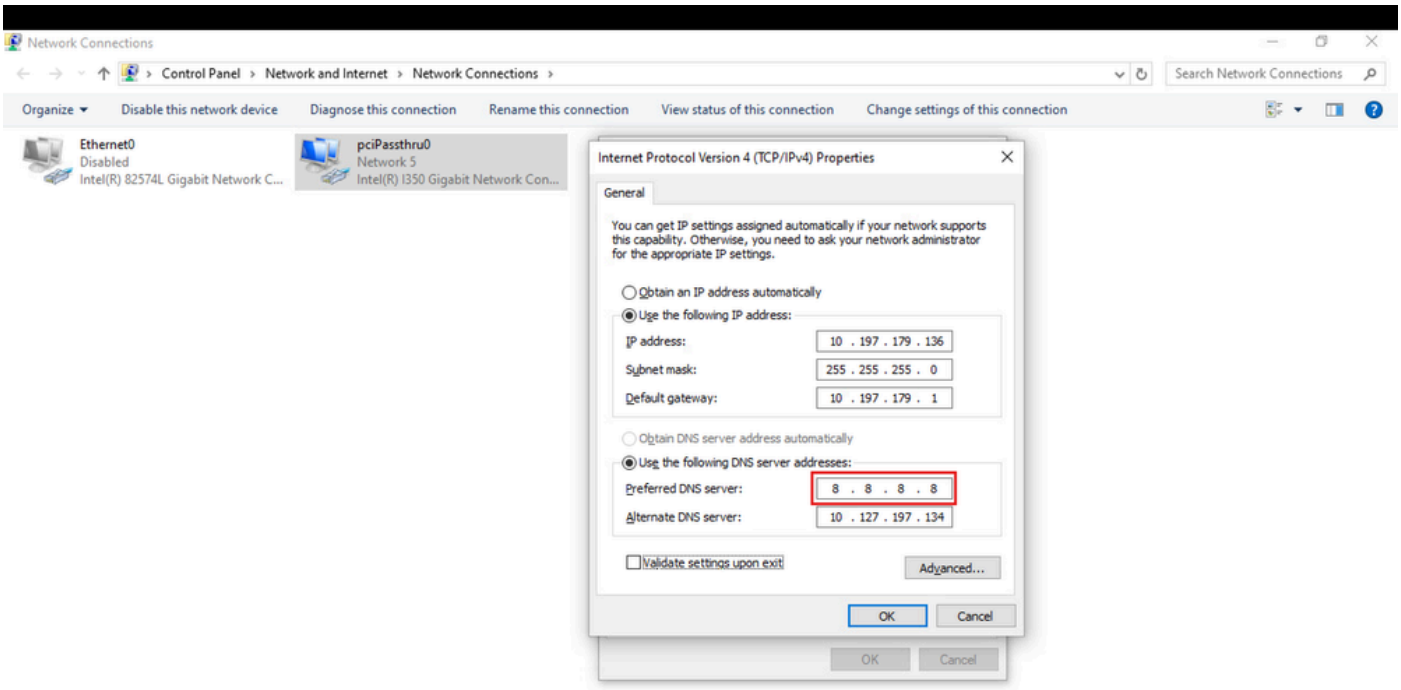




Opmerking: In dit voorbeeld, zodra de DNS-overschrijdingsgebeurtenis is geactiveerd, wordt toegang geweigerd aan de gebruiker op basis van de configuratie

Verifiëren

Om het gebruiksgeval aan te tonen, is de DNS-ingang op het eindpunt veranderd in 8.8.8.8, wat de geconfigureerde DNS-schendingsgebeurtenis activeert. Aangezien de DNS-server niet tot de hostgroep van Mijn Corporate DNS-servers behoort, wordt de gebeurtenis die resulteert in een ontzegging van de toegang tot het eindpunt geactiveerd.



Controleer in de C9300-switch met de Show Flow Monitor IPv4_NETFLOW cache | in 8.8.8.8 opdracht met de uitvoer om de stromen te zien worden opgenomen en naar de Flow Collector verzonden. IPv4_NETFLOW wordt geconfigureerd in de switch-configuratie.

<#root>

IPV4 SOURCE ADDRESS:

10.197.179.136

IPV4 DESTINATION ADDRESS:

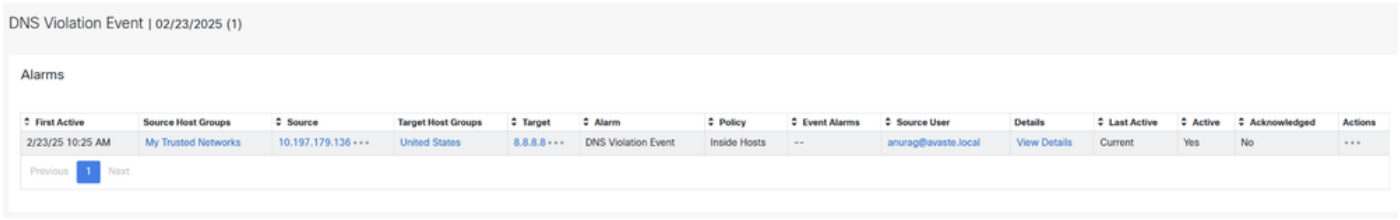
8.8.8.8

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

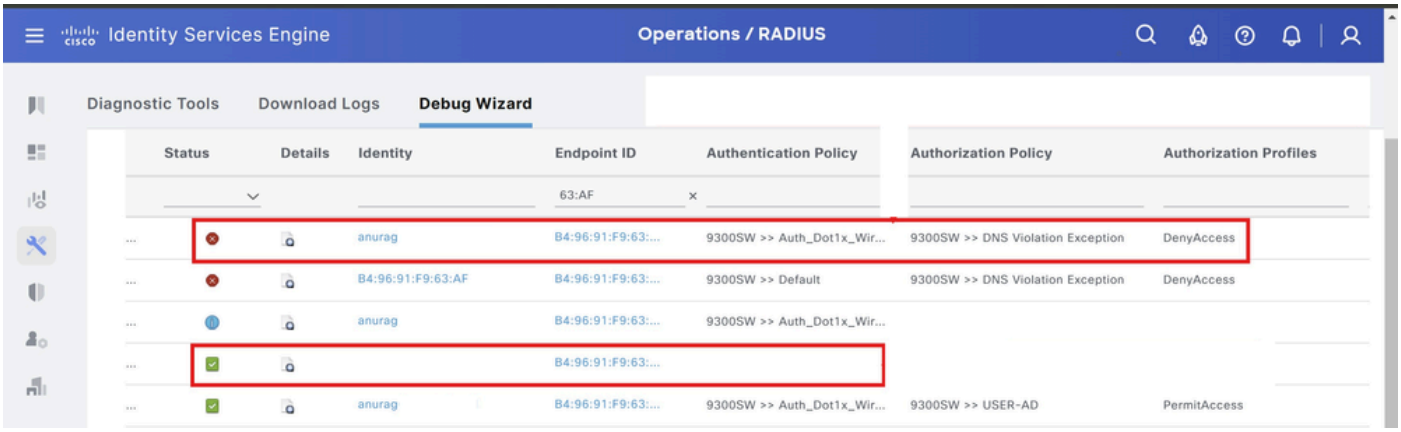
Zodra de Gebeurtenis op Stealthwatch wordt geactiveerd, navigeer naar Monitor > Security Insight Dashboard,.



Blader naar Monitor > Integratie > ISE ANC Policy Assignments.

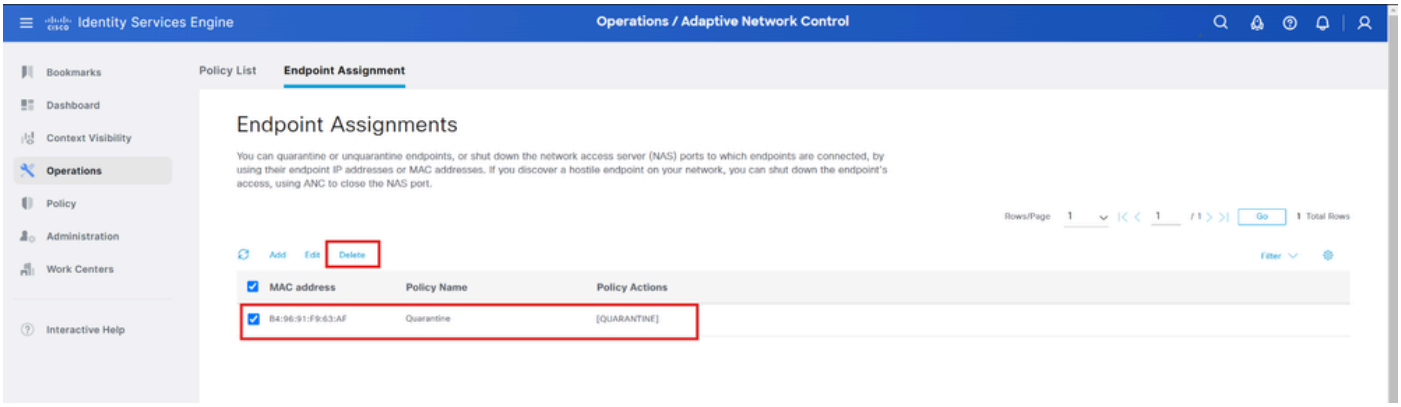
Zorg ervoor dat Cisco Secure Network Analytics met succes het Adaptive Network Control Policy via PxGrid en Cisco ISE heeft geïmplementeerd om de host in quarantaine te plaatsen.

Op dezelfde manier navigeer je op Cisco ISE naar Operations > RADIUS > Livelogs en pas je filter toe op het eindpunt.



In overeenstemming met het lokale uitzonderingsbeleid wordt DNS-schending-uitzondering, wijziging van autorisatie (CoA) afgegeven door ISE en toegang tot ISE geweigerd tot het eindpunt.

Nadat de herstelacties op het eindpunt zijn uitgevoerd, verwijdert u de MAC uit Operations > Adaptive Network Control > Endpoint Assignments > Delete om het MAC-adres van het eindpunt te verwijderen.



Log in op Cisco ISE.

Attributen die op TRACE-niveau zijn ingesteld voor de component pxgrid (pxgrid-server.log) op Cisco ISE, worden logbestanden weergegeven in het bestand 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 -::::::617fffb27858402
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

"}

Probleemoplossing

Quarantined Endpoints verlengen verificatie niet na beleidswijziging

Probleem

Verificatie is mislukt vanwege wijzigingen in beleid of aanvullende identiteit en er vindt geen

herverificatie plaats. Verificatie mislukt of het betreffende eindpunt blijft niet in staat om verbinding te maken met het netwerk. Deze kwestie komt vaak op cliëntmachines voor die de beoordeling van de houding per het houdingsbeleid ontbreekt dat aan de gebruikersrol wordt toegewezen.

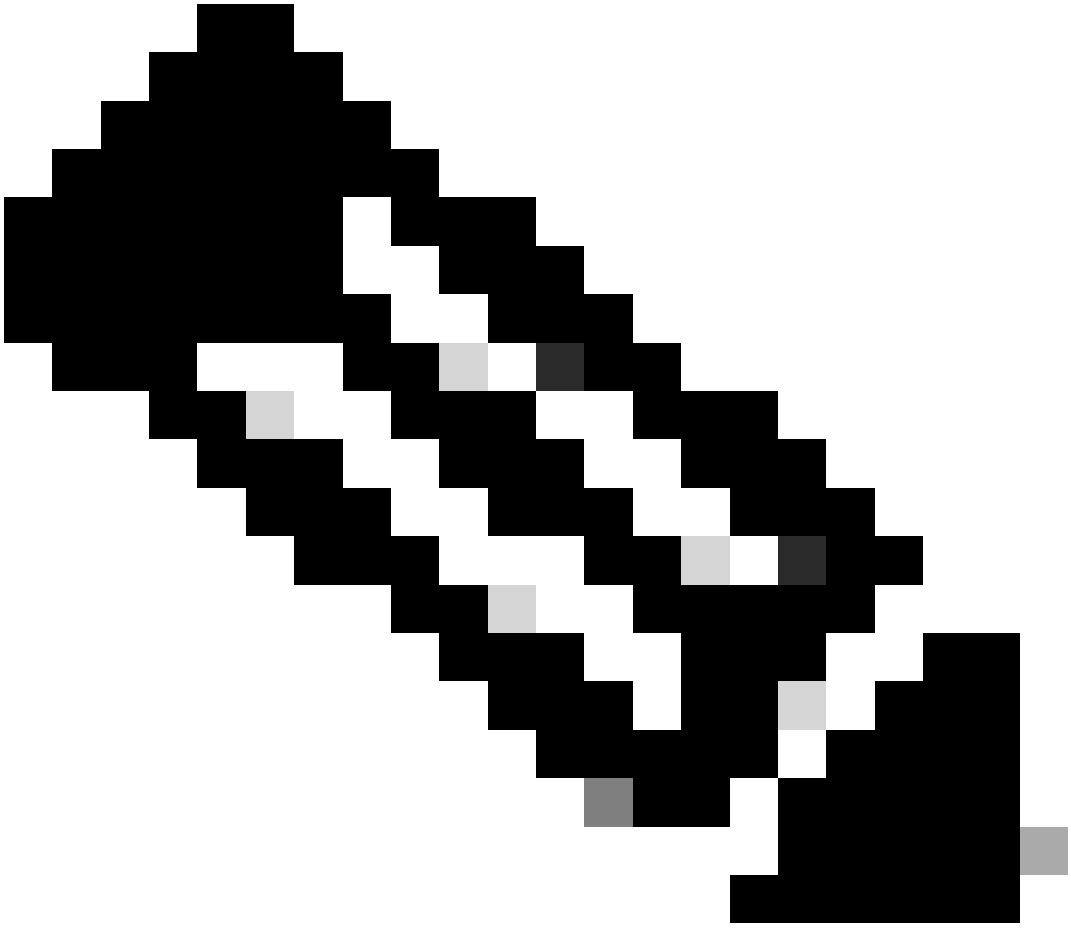
Mogelijke oorzaken

De instelling van de verificatietimer is niet juist ingesteld op de clientmachine of het verificatieinterval is niet juist ingesteld op de switch.

Oplossing

Er zijn verschillende mogelijke resoluties voor dit probleem:

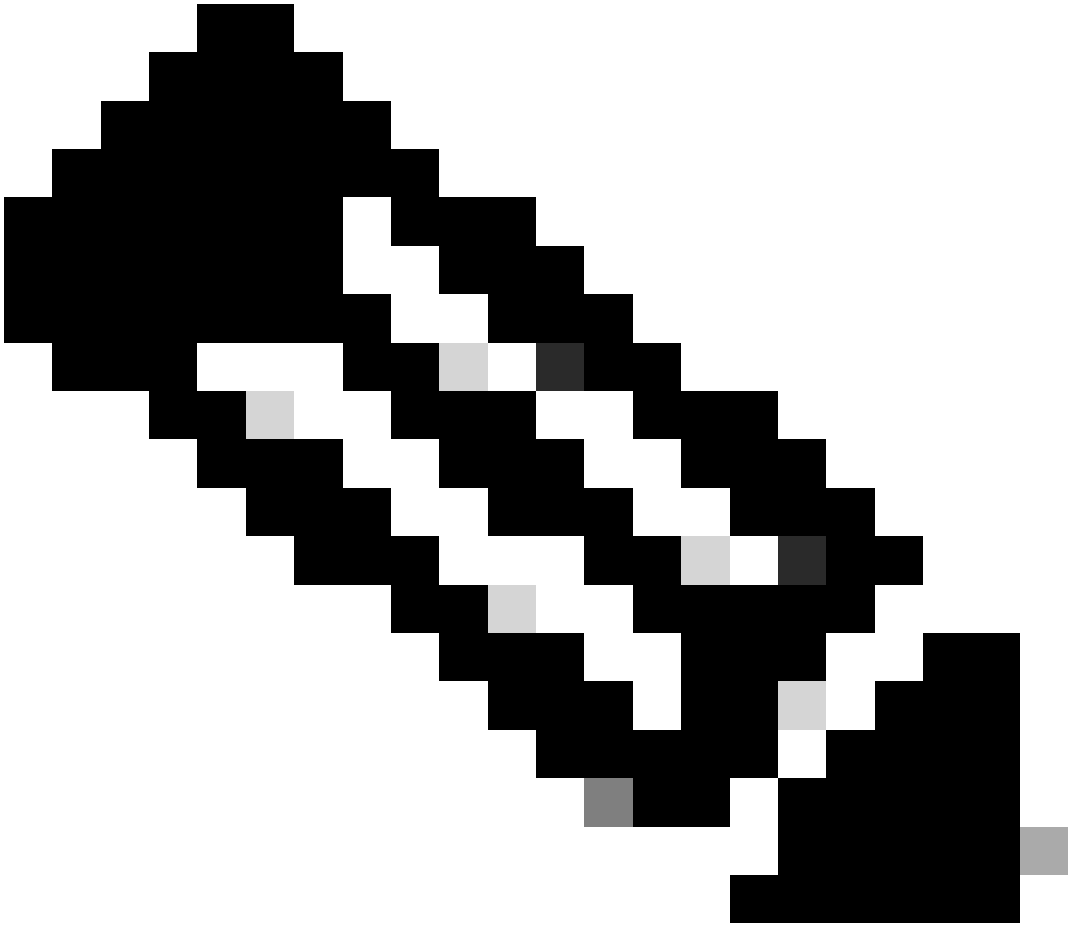
1. Controleer het rapport Session Status Summier in Cisco ISE voor de opgegeven NAD of switch en zorg ervoor dat de interface het juiste verificatieinterval heeft ingesteld.
2. Geef de actieve configuratie op de NAD/switch op en zorg ervoor dat de interface is geconfigureerd met de juiste instelling voor het opnieuw opstarten van de verificatietimer. (Verificatietimer start bijvoorbeeld opnieuw 15 en verificatietimer opnieuw 15).
3. Voer sluitingen van interfaces en geen sluitingen in om de poort op de NAD/switch te laten stuiteren en forceer opnieuw verificatie en potentiële configuratiewijzigingen in Cisco ISE.



Opmerking: Omdat CoA een MAC-adres of sessie-id vereist, wordt aanbevolen om de poort die in het SNMP-rapport van het netwerkapparaat wordt weergegeven, niet te laten stuiteren.

ANC-bewerkingen mislukken wanneer IP-adres of MAC-adres niet wordt gevonden

Een ANC-bewerking die u op een eindpunt uitvoert, mislukt wanneer een actieve sessie voor dat eindpunt geen informatie bevat over het IP-adres. Dit geldt ook voor het MAC-adres en de sessie-ID voor dat eindpunt.



Opmerking: Wanneer u de autorisatiestatus van een eindpunt wilt wijzigen via ANC, moet u het IP-adres of het MAC-adres voor het eindpunt opgeven. Als het IP-adres of het MAC-adres niet wordt gevonden in de actieve sessie voor het eindpunt, kunt u de foutmelding zien: "Geen actieve sessie gevonden voor dit MAC-adres, IP-adres of sessie-id".

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.