Configuración de ANC en ISE 3.3 y StealthWatch 7.5.1

Contenido

Introducción

Este documento describe la configuración de Rapid Threat Containment (Adaptive Network Control) en Cisco ISE® versión 3.3 y StealthWatch.

Prerequisites

Cisco recomienda conocimientos sobre los siguientes temas:

- Identity Services Engine (ISE)
- Platform Exchange Grid (PxGrid)
- Secure Network Analytics (StealthWatch)
- Contención rápida de amenazas (control de red adaptable - ANC).

En este documento se supone que Cisco Identity Services Engine está integrado con Secure Network Analytics (StealthWatch) mediante pxGrid habilitado para ANC.

Componentes Utilizados

La información de este documento se basa en estas versiones y software:

- Cisco Identity Services Engine (ISE) versión 3.3

- Secure Network Analytics (StealthWatch) 7.5.1
- Catalyst 9300

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

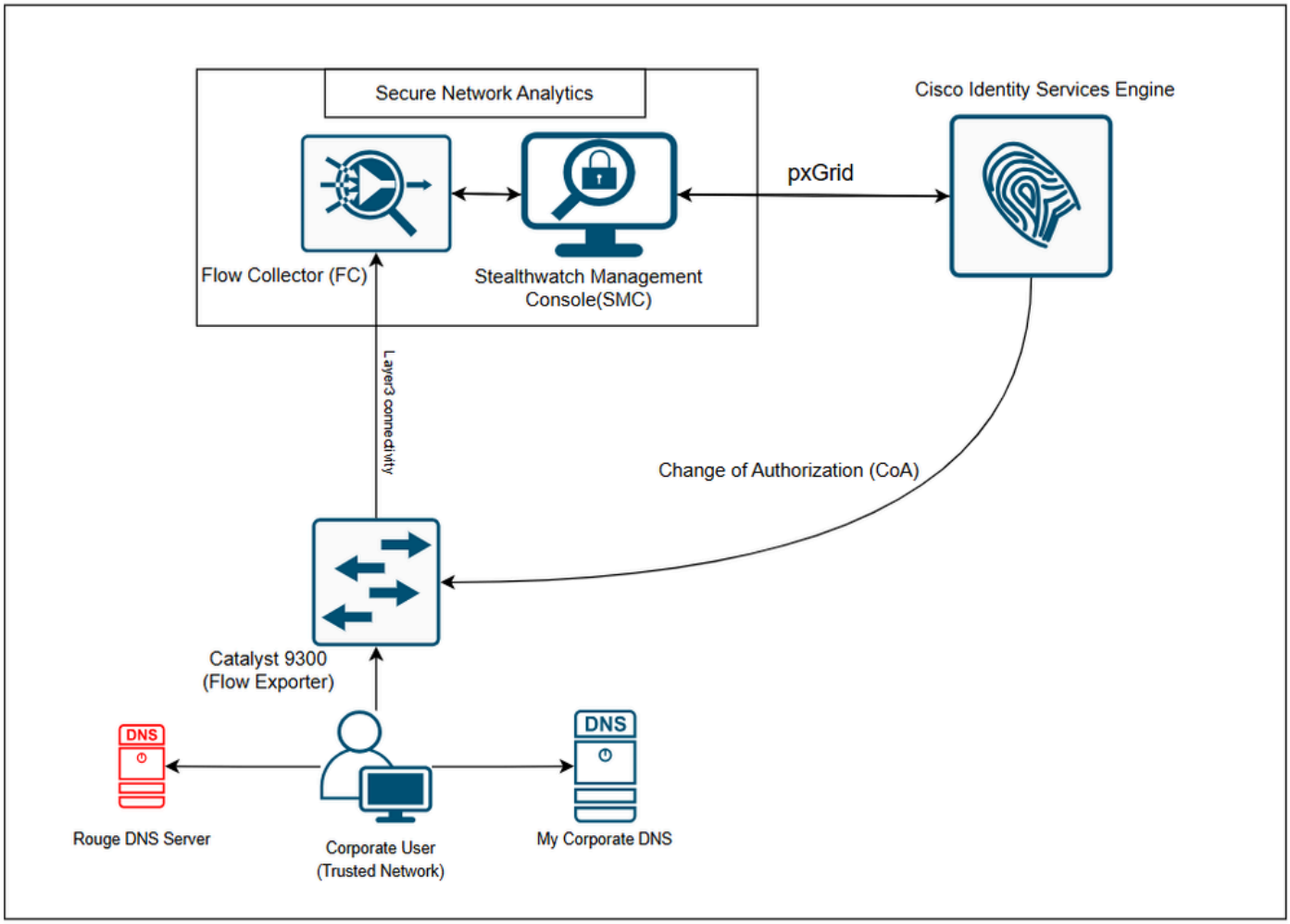
Cisco Secure Cloud Analytics (ahora parte de Cisco XDR) puede recuperar datos de atribución de usuarios de Cisco Identity Services Engine (ISE) mediante pxGrid. Esta integración permite la generación de informes de actividad del usuario en el visor de eventos de Secure Cloud Analytics.

La combinación de Secure Network Analytics (anteriormente Stealthwatch) y Cisco Identity Services Engine (ISE) ayuda a las organizaciones a obtener una vista de 360°, responder a las amenazas con mayor rapidez y proteger un negocio digital en crecimiento. Una vez que Secure Network Analytics detecta el tráfico anómalo, emite una alerta, que ofrece al administrador la opción de poner en cuarentena al usuario. pxGrid permite a Secure Network Analytics transferir el comando quarantine directamente a Identity Services Engine.

En este ejemplo se describe cómo aprovechar el servidor DNS corporativo para protegerlo frente a amenazas de Internet. La intención es establecer un mecanismo de alerta personalizado que se active cuando los usuarios internos se conecten a servidores DNS externos. Esta iniciativa está diseñada para bloquear las conexiones a servidores DNS no autorizados que podrían redirigir el tráfico a sitios externos dañinos.

Cuando se activa una alerta, Cisco Secure Network Analytics se coordina con Cisco ISE para poner en cuarentena al host que accede a los servidores DNS no autorizados, mediante una política de control de red adaptable a través de PxGrid.

Diagrama de la red



Como se muestra en el diagrama:

- Un usuario corporativo está conectado a un switch C9300 que está configurado para exportar los flujos IP y enviar los datos al recolector de flujos.
- El mismo usuario corporativo está configurado para usar servidores DNS corporativos.
- Flow Collector se integra con StealthWatch Management Console (SMC)
- StealthWatch Management Console (SMC) integrada mediante Pxgrid con ISE.

Configuración paso a paso

1. Prepare el switch para monitorear y exportar los flujos usando netflow.

La configuración básica de flujo en un switch C9300 que ejecuta 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
```

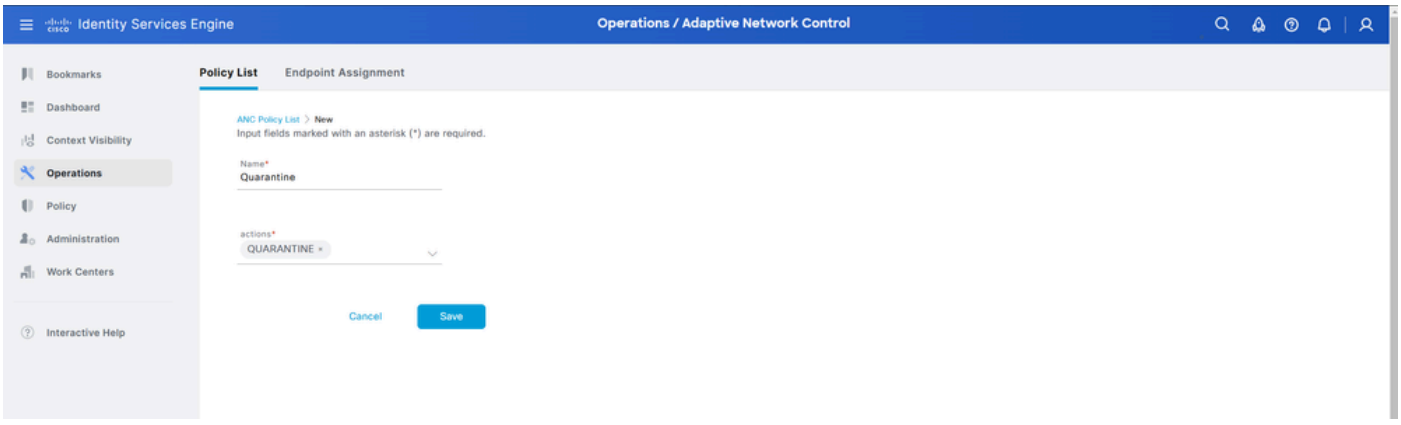
```
  collect transport tcp flags
  collect interface output
  collect counter bytes long
  collect counter packets long
  collect timestamp absolute first
  collect timestamp absolute last


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
```

Una vez finalizada la configuración, permite al C9300 exportar datos de flujo IP al Flow Collector. A continuación, el Flow Collector procesa y transfiere estos datos a la Stealthwatch Management Console (SMC) para su análisis y supervisión.

2. Habilite el control de red adaptable en Cisco ISE.

ANC está desactivado de forma predeterminada. ANC se habilita solo cuando pxGrid está habilitado y permanece habilitado hasta que inhabilita manualmente el servicio en el portal de administración.

Seleccione Operaciones > Control de red adaptable > Lista de políticas > Agregar, luego ingrese Cuarentena para el nombre de política y Cuarentena para la acción.

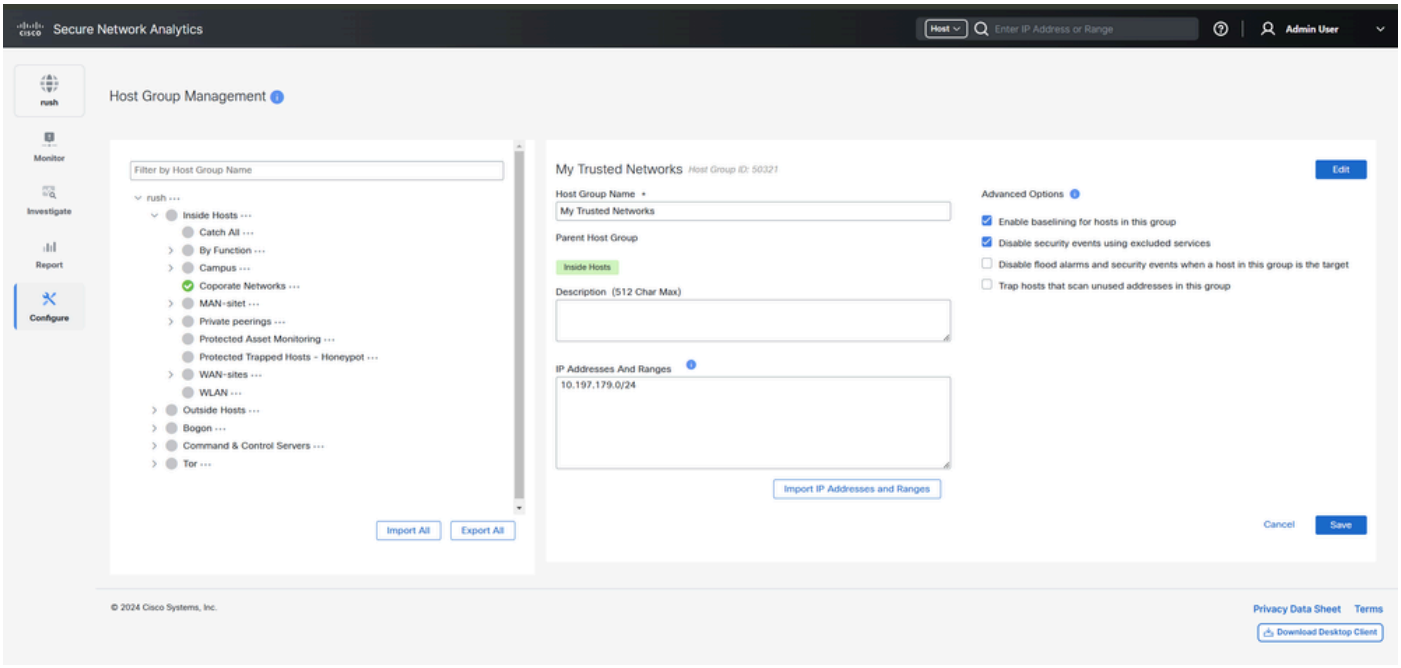


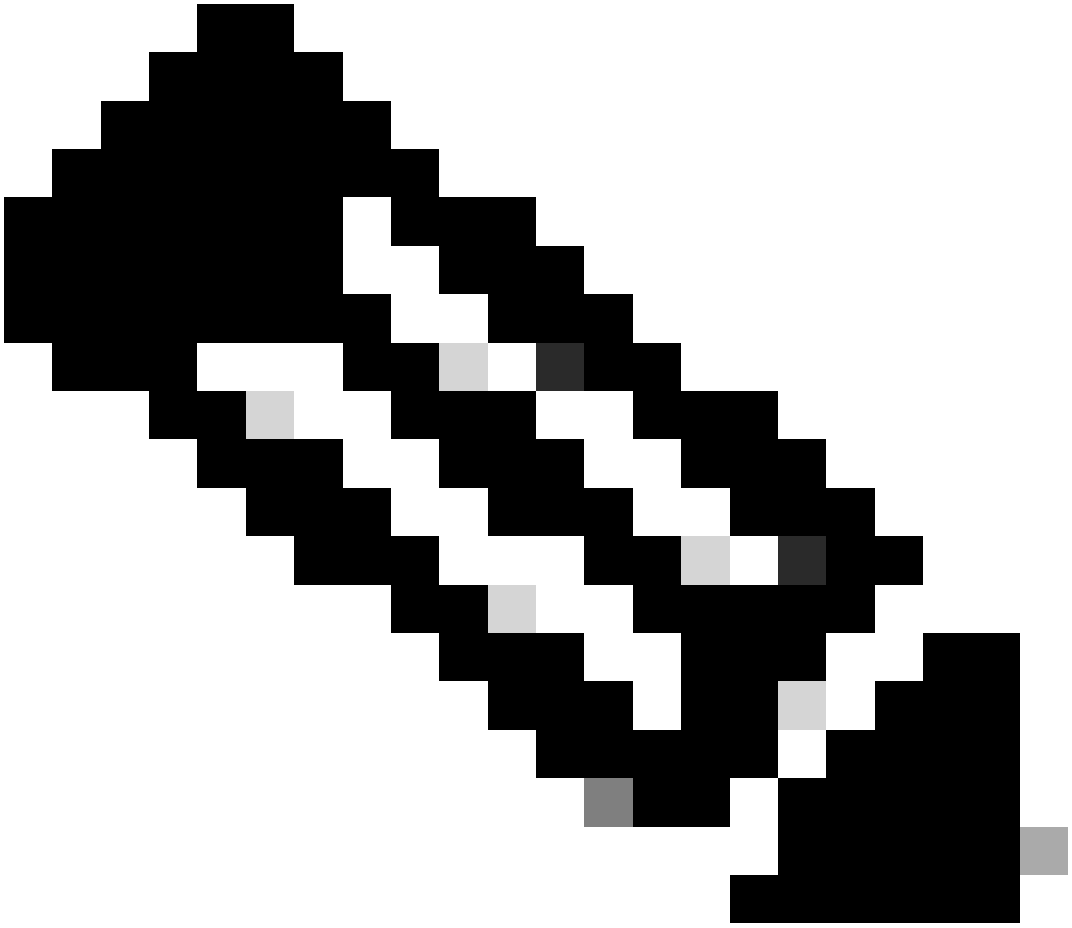
3. Configure Secure Network Analytics para Event Trigger and Response Management para una contención rápida de las amenazas.

Paso 1: Inicie sesión en la GUI de SMC y vaya a Configure > Detection > Host Group Management > Click on the (...) (ellipsis) icon junto a Inside Hosts, luego seleccione Add Host Group.

En este ejemplo, se crea un nuevo grupo de hosts con el nombre Mis redes de confianza bajo el grupo de hosts internos principal.

Esta red se puede asignar normalmente al equipo del usuario final para supervisar el uso de DNS.

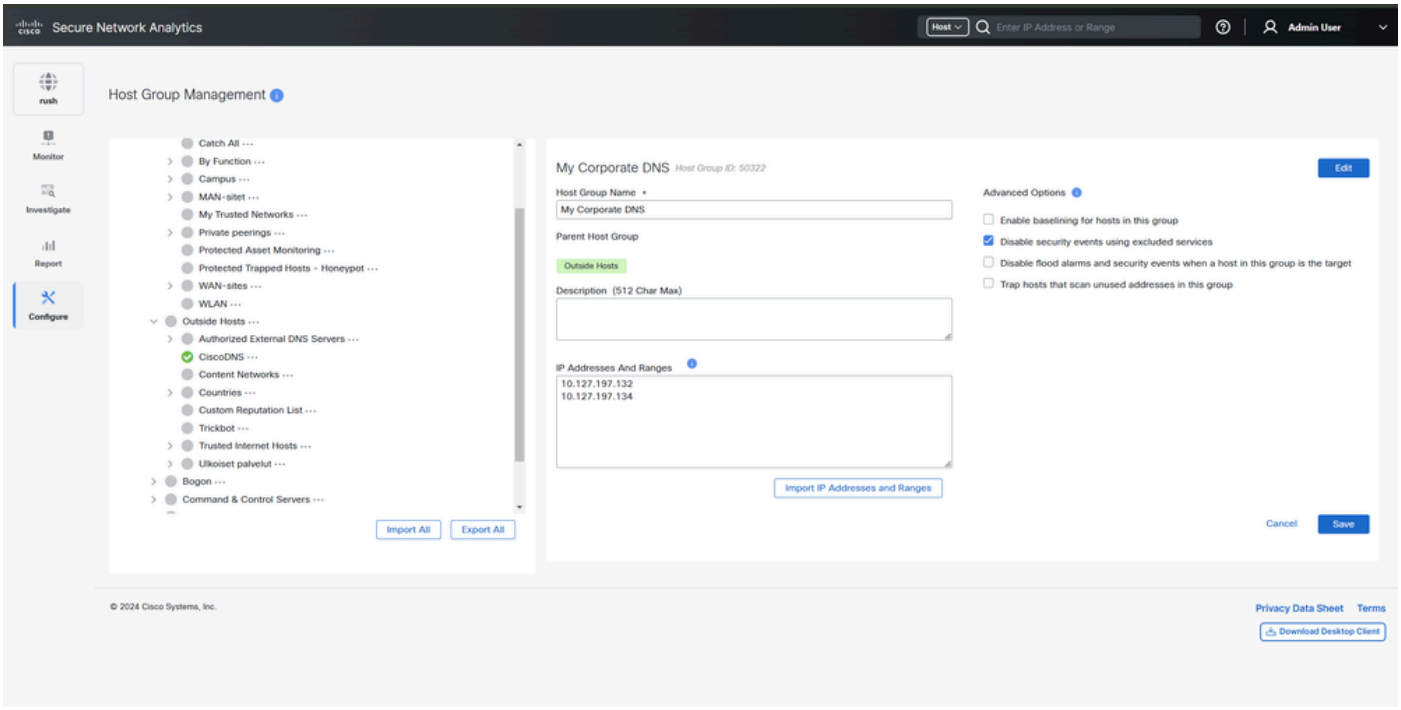


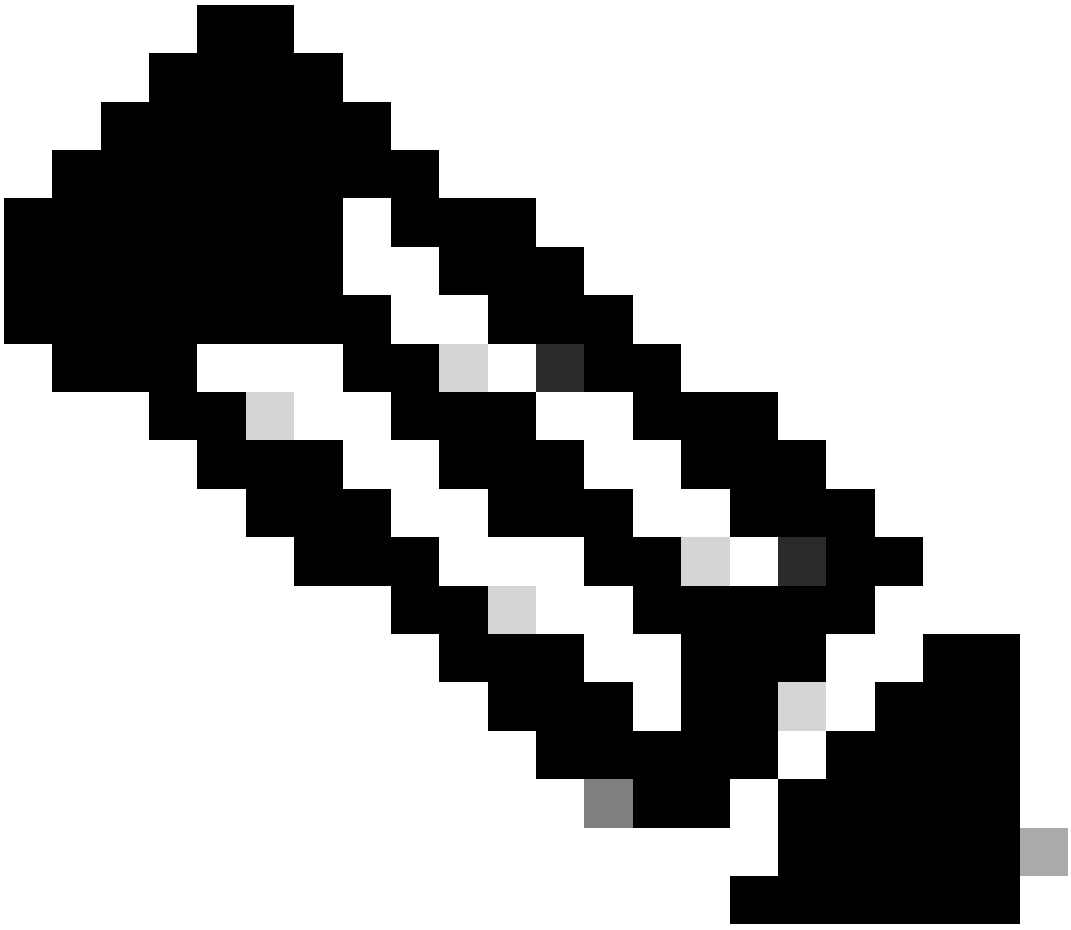


Nota: En este ejemplo, la subred IP 10.197.179.0/24 se utiliza como subred de la red de área local (LAN). Esta subred puede variar en el entorno de red real en función de la arquitectura de red.

Paso 2: Inicie sesión en la GUI de SMC y navegue hasta Configurar > Detección > Administración de grupos de hosts > Haga clic en (...) además de Hosts externos y seleccione Agregar grupo de hosts.

En este ejemplo, se crea un nuevo grupo de hosts con el nombre My Corporate DNS bajo el grupo de hosts externos principal.

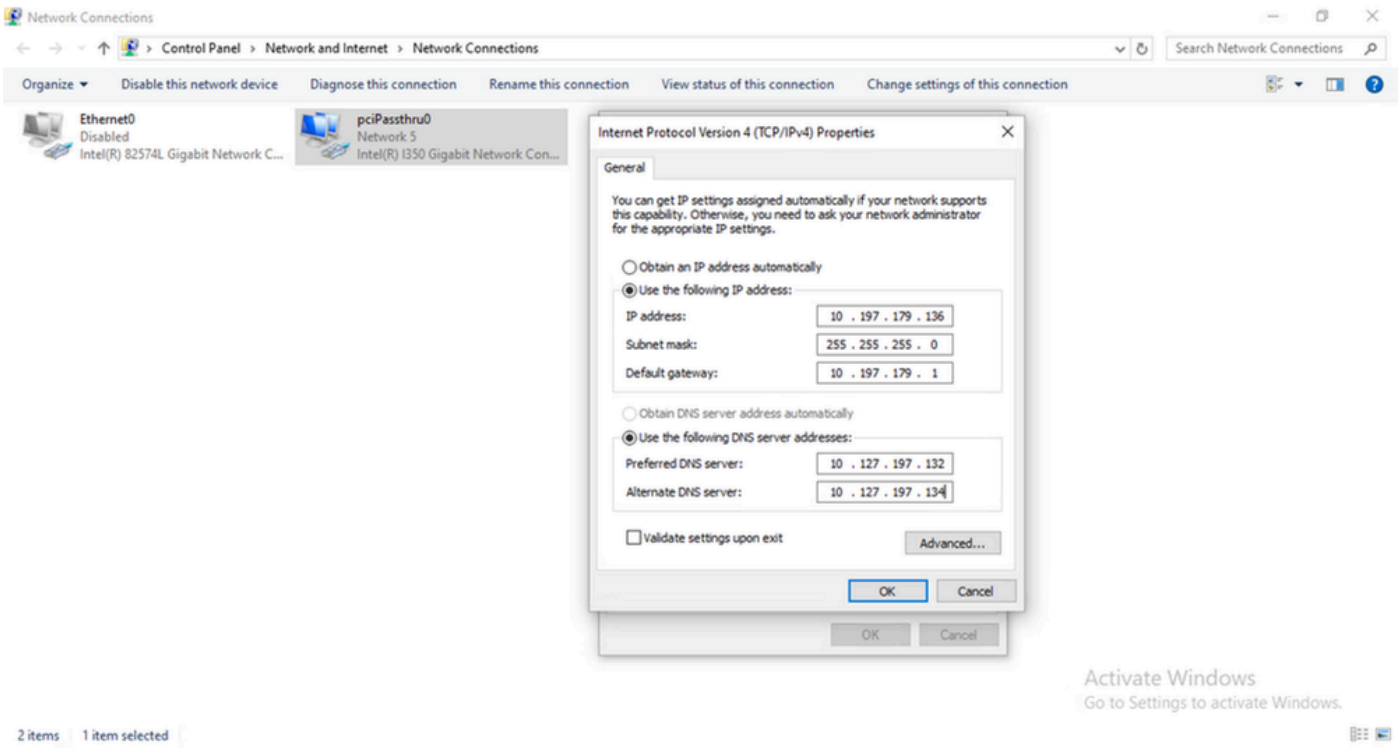




Nota: Para este ejemplo, las IP 10.127.197.132 y 10.127.197.134 se utilizan como los

servidores DNS deseados que deben utilizar los usuarios finales. Esto puede diferir en el entorno de red real dependiendo de la arquitectura de red.

El equipo del laboratorio de pruebas utilizado para la demostración está configurado con IP estática 10.197.179.136 (pertenece al grupo de hosts Mis redes de confianza creado) y DNS 10.127.197.132 y 10.127.197.134 (pertenece al grupo de hosts Mi DNS corporativo creado).



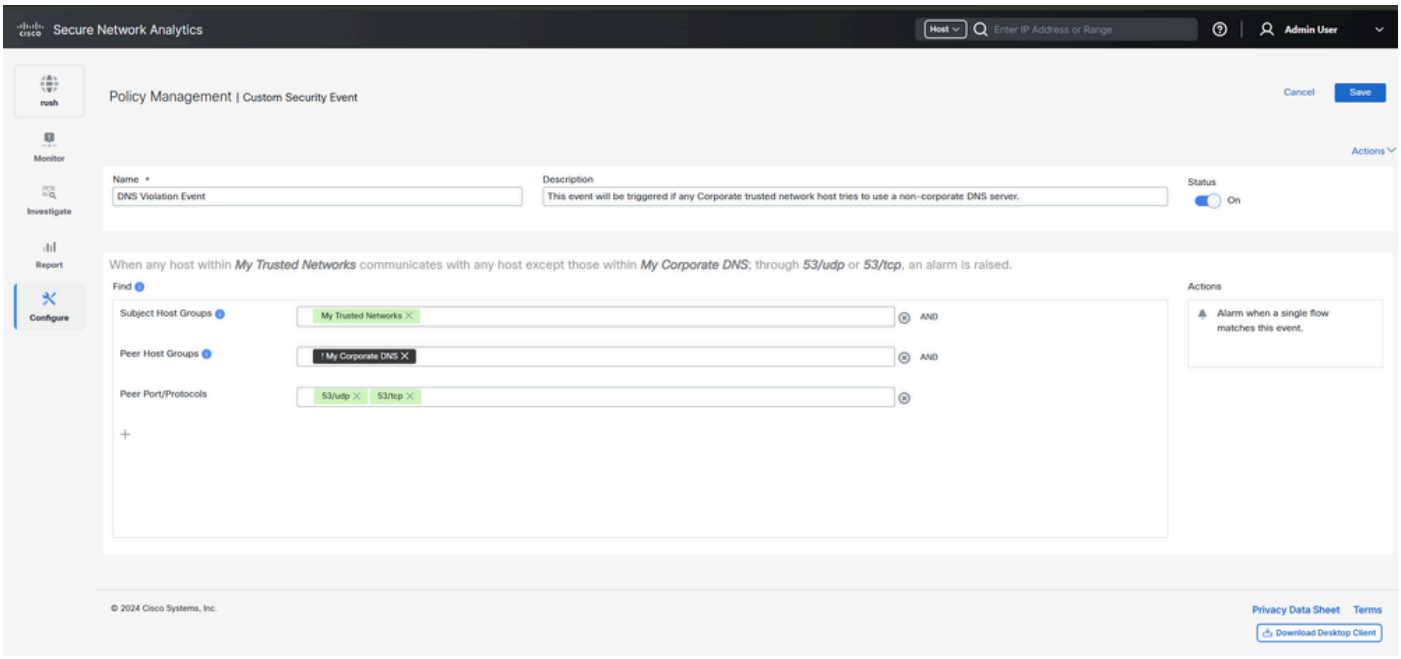
Paso 3: Configure un sistema de alerta personalizado para detectar cuándo los usuarios internos se conectan a servidores DNS externos, activando una alarma para bloquear las conexiones a servidores DNS no autorizados que podrían potencialmente redirigir el tráfico a sitios externos maliciosos. Una vez activada la alarma, Cisco Secure Network Analytics se coordina con Cisco ISE para aislar el host que utiliza estos servidores DNS no autorizados mediante una política de control de red adaptable a través de PxGrid.

Navegue hasta Configurar > Administración de políticas.

Cree un evento personalizado con la siguiente información:

- Nombre:Evento de violación de DNS.
- Grupos de hosts de asunto:Mis redes de confianza.
- Grupos host de peer: (No) Mi DNS corporativo.
- Puerto/Protocolos de Peer: 53/UDP 53/TCP

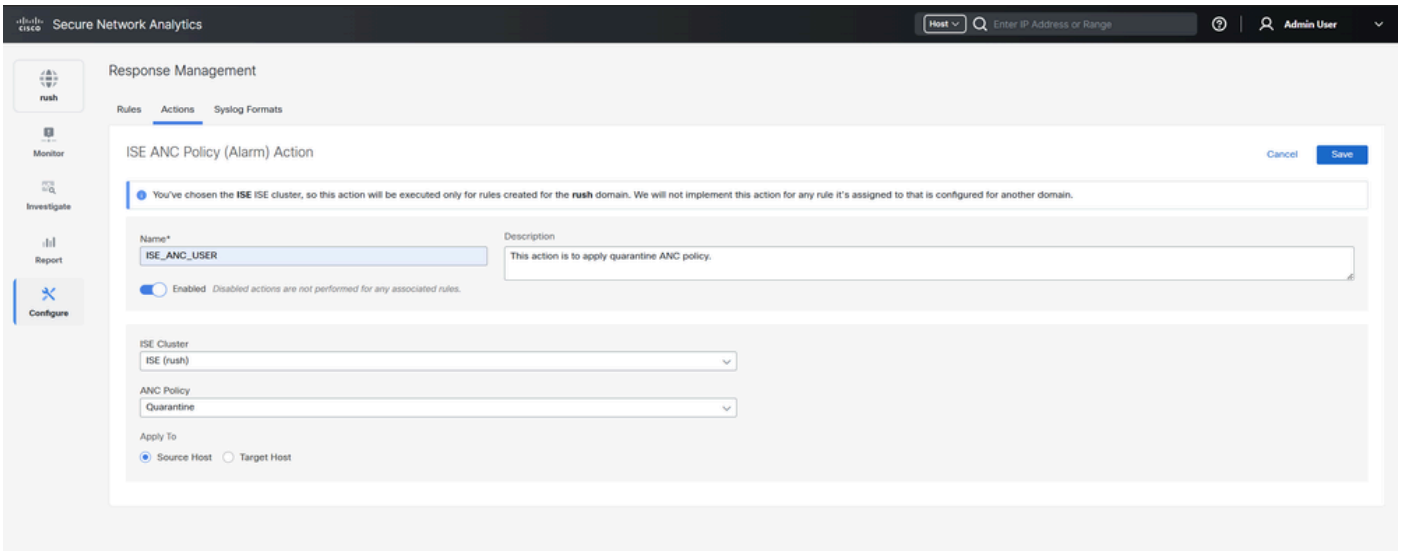
Esto significa que cuando cualquier host dentro de Mis redes de confianza (grupo de hosts) se comunica con cualquier host excepto aquellos dentro de Mi DNS corporativo (grupo de hosts) a través de 53/up o 53/tcp, se activa una alarma.



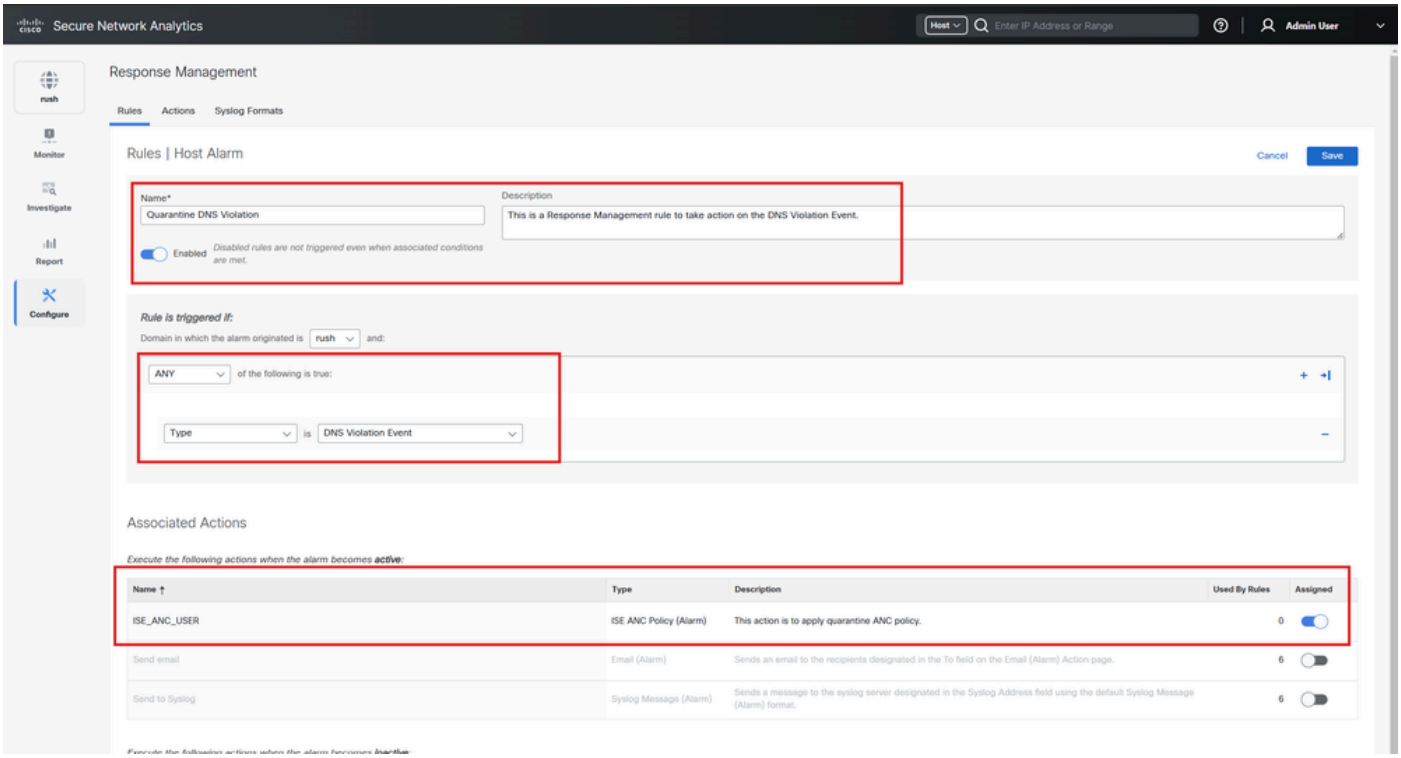
Paso 4: Configure la acción de administración de respuestas que se va a realizar y que se puede aplicar posteriormente a la regla de administración de respuestas una vez creada.

Vaya a Configure > Response Management > Actions, haga clic en Add New Action y seleccione ISE ANC Policy (Alarm).

Asigne un nombre y elija el clúster de Cisco ISE específico al que se notificará para implementar una política de cuarentena para cualquier infracción o conexión a servidores no autorizados.



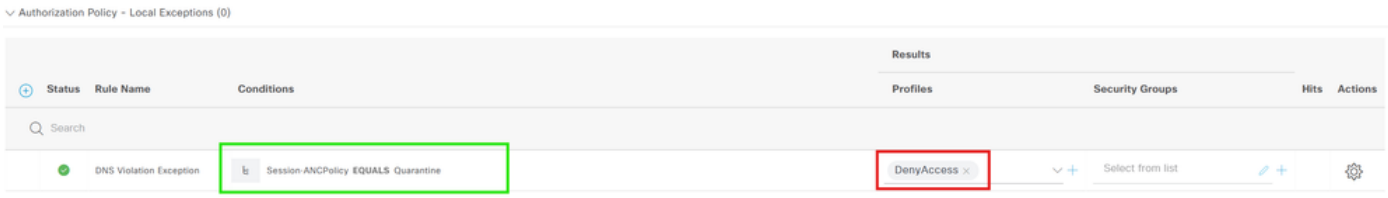
Paso 5: en la sección Reglas, Crear una nueva regla. Esta regla aplica la acción definida anteriormente cada vez que un host de la red interna intenta enviar tráfico DNS a servidores DNS no autorizados. En la sección La regla se desencadena si, elija Tipo y seleccione el evento personalizado creado anteriormente.
En Acciones asociadas, seleccione la acción de alarma ANC de ISE que se configuró anteriormente.

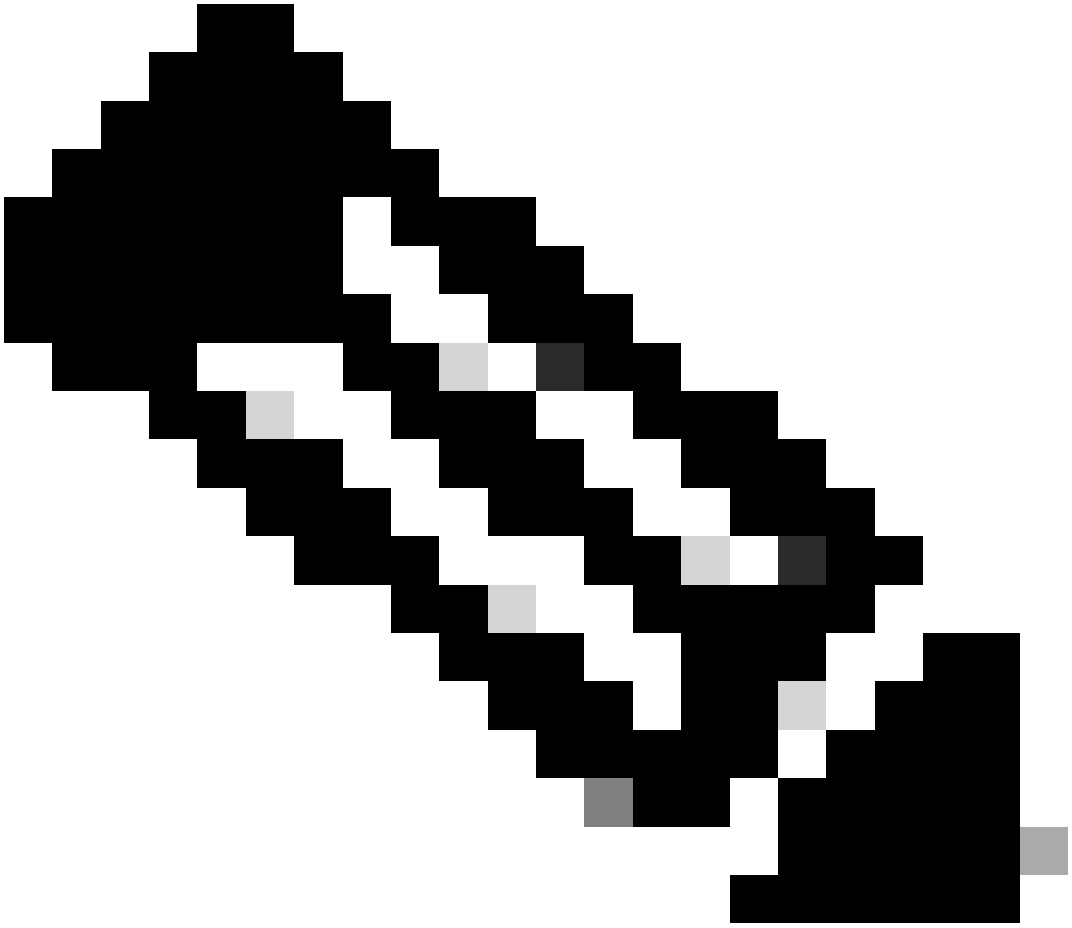


4. Configure Cisco ISE para que responda a las acciones iniciadas por StealthWatch al desencadenar el evento.

Inicie sesión en la GUI de Cisco ISE y vaya a Policy > Policy Sets > Choose the Policy set > under Authorization Policy - Local Exceptions > Create new Policy.

- Nombre: Excepción de violación de DNS
- Condiciones: Sesión: ANCPolicy EQUALS Quarantine
- Perfiles de autorización: DenegarAcceso

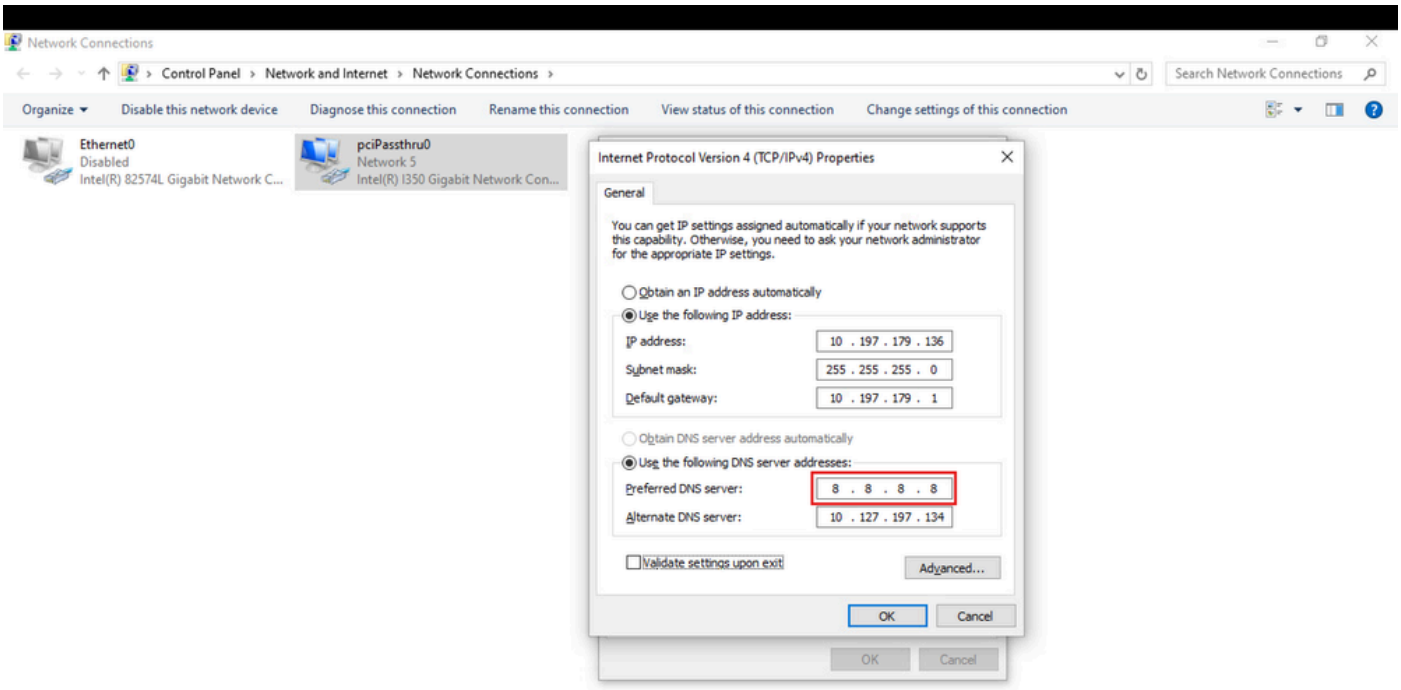




Nota: En este ejemplo, una vez que se desencadena el evento de violación de DNS, se deniega el acceso al usuario en función de la configuración

Verificación

Para demostrar el caso práctico, la entrada DNS en el punto final se ha cambiado a 8.8.8.8, que activa el evento de violación de DNS configurado . Dado que el servidor DNS no pertenece al grupo host de Mis servidores DNS corporativos, desencadena el evento que da lugar a una denegación de acceso al extremo.



En el switch C9300, verifique usando la memoria caché show flow monitor IPv4_NETFLOW | en el comando 8.8.8.8 con el resultado para ver que los flujos se capturan y se envían al Flow Collector. IPv4_NETFLOW se configura en la configuración del switch.

<#root>

IPV4 SOURCE ADDRESS:

10.197.179.136

IPV4 DESTINATION ADDRESS:

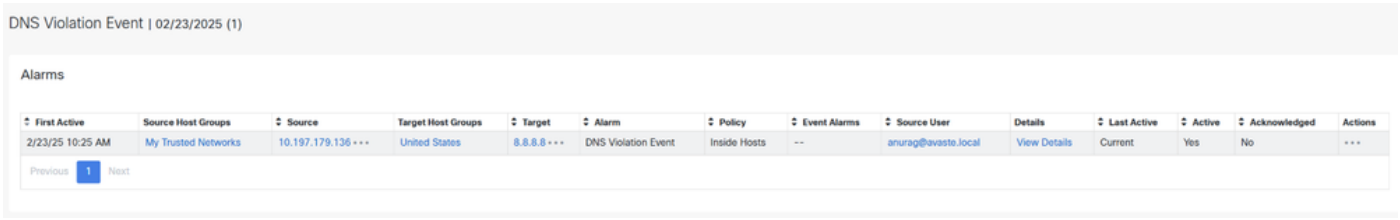
8.8.8.8

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

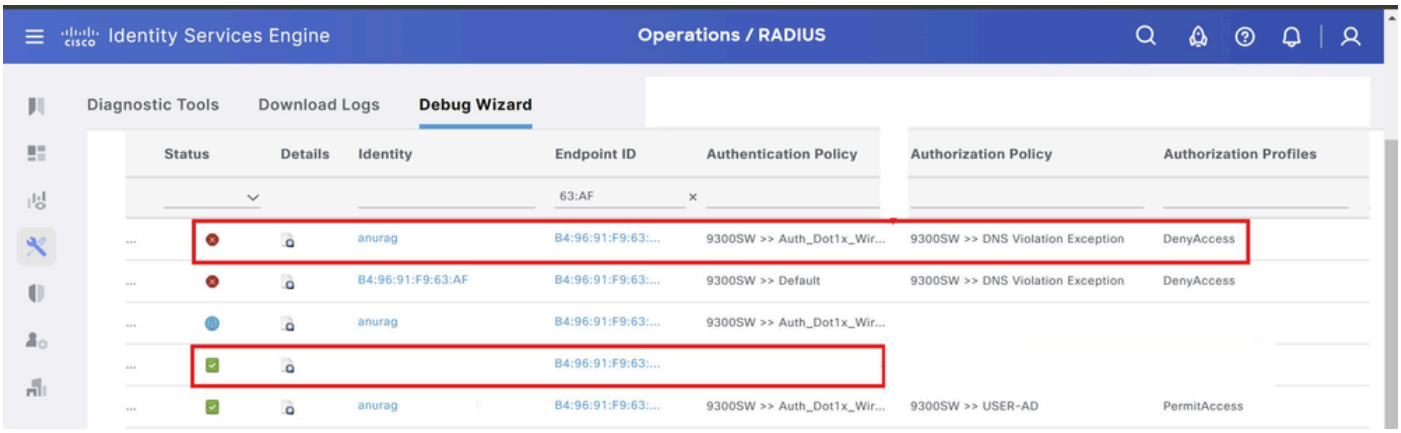
Una vez que el evento se active en StealthWatch, navegue hasta Monitor > Security Insight Dashboard,.



Vaya a Monitor > Integration > ISE ANC Policy Assignments (Supervisión > Integración > Asignaciones de políticas ISE ANC).

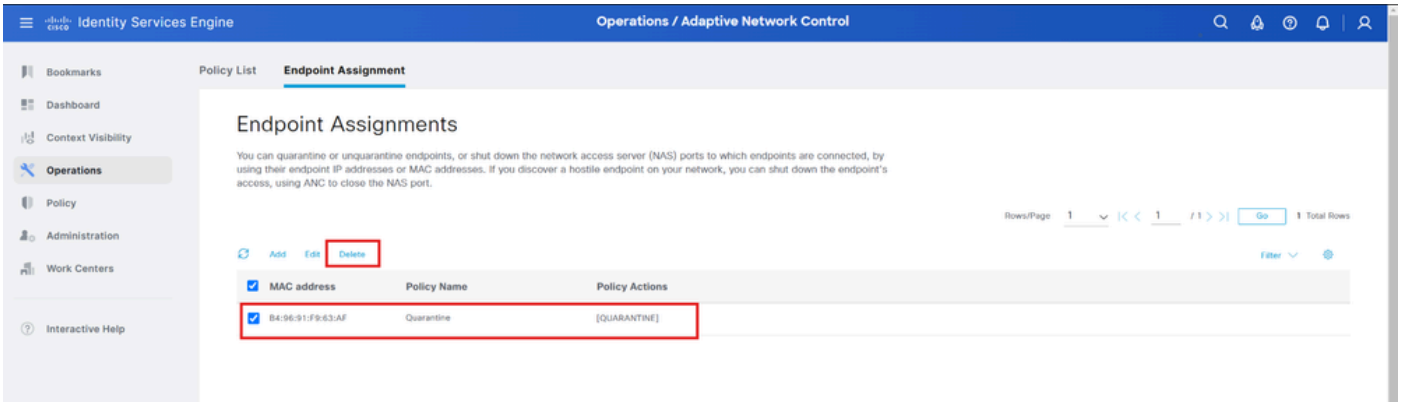
Asegúrese de que Cisco Secure Network Analytics haya implementado correctamente la política de control de red adaptable a través de PxGrid y Cisco ISE para poner en cuarentena el host.

Del mismo modo, en Cisco ISE, navegue hasta Operaciones > RADIUS > Livelogs y aplique un filtro para el terminal.



Según la política de excepciones local Excepción de violación de DNS, ISE emite el cambio de autorización (CoA) y se deniega el acceso a ISE al terminal.

Una vez realizadas las acciones de remediación en el terminal, elimine el MAC de Operations > Adaptive Network Control > Endpoint Assignments > Delete para quitar la dirección MAC del terminal.



Referencia de registro en Cisco ISE.

Los atributos establecidos en el nivel TRACE para el componente pxgrid (pxgrid-server.log) en Cisco ISE, los registros se ven en el archivo 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

```
"}
```

Resolución de problemas

Los extremos en cuarentena no renuevan la autenticación Cambio de política posterior

Problema

La autenticación ha fallado debido a un cambio en la política o a una identidad adicional y no se está llevando a cabo ninguna reautenticación. La autenticación falla o el terminal en cuestión sigue sin poder conectarse a la red. Este problema suele ocurrir en equipos cliente que no superan la evaluación de estado según la política de estado asignada a la función de usuario.

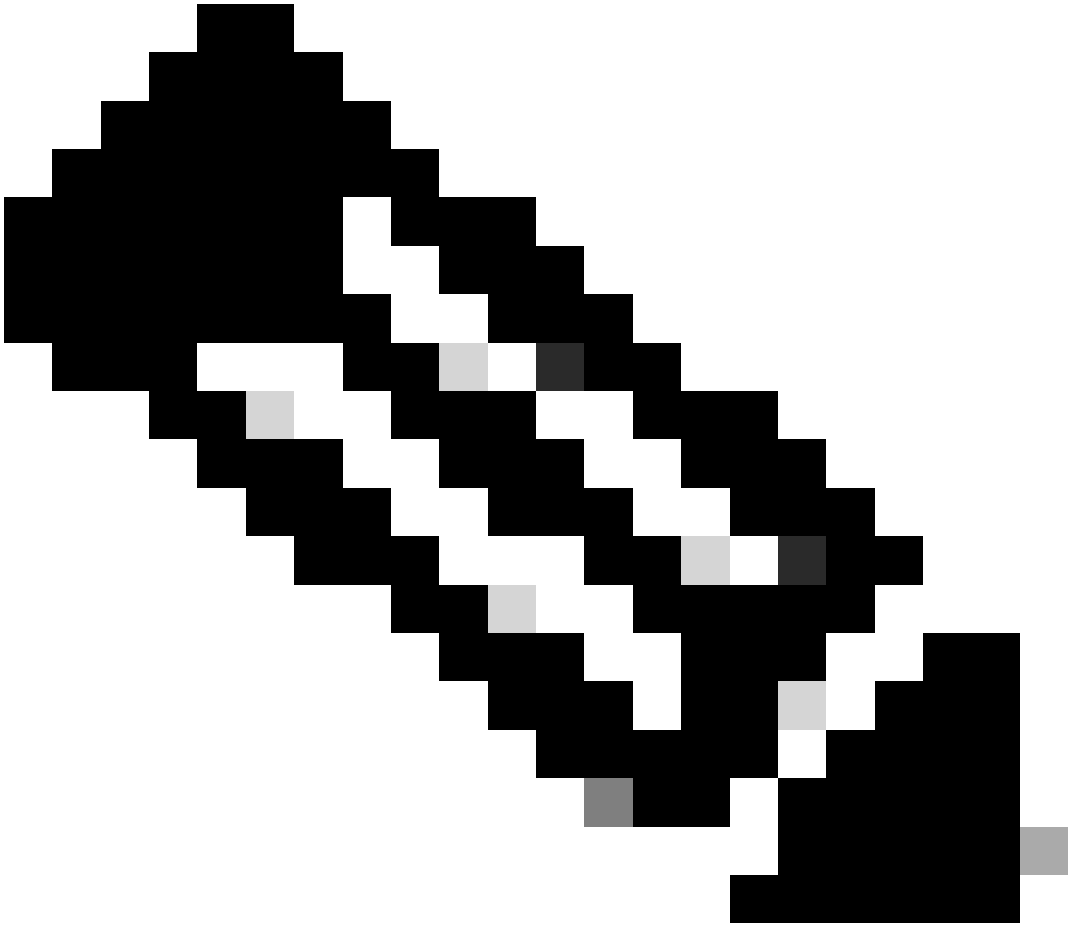
Posibles Causas

La configuración del temporizador de autenticación no está establecida correctamente en el equipo cliente o el intervalo de autenticación no está establecido correctamente en el switch.

Solución

Hay varias posibles soluciones para este problema:

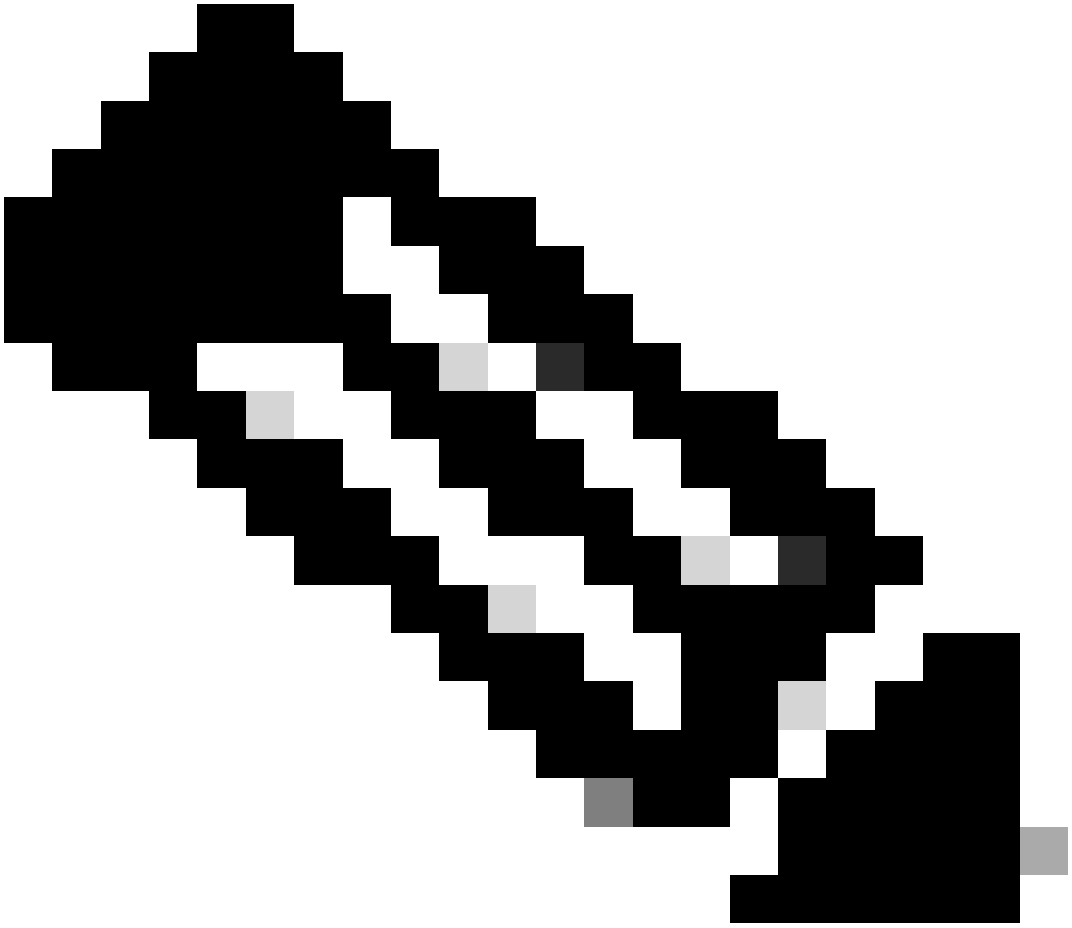
1. Verifique el informe de resumen de estado de sesión en Cisco ISE para el NAD o el switch especificado y asegúrese de que la interfaz tenga configurado el intervalo de autenticación apropiado.
2. Ingrese show running configuration en el switch/NAD y asegúrese de que la interfaz esté configurada con una configuración adecuada de reinicio del temporizador de autenticación. (Por ejemplo, el temporizador de autenticación reinicia 15, y el temporizador de autenticación reautentica 15).
3. Ingrese interface shutdown y no shutdown para hacer rebotar el puerto en el switch/NAD y forzar la reautenticación y el posible cambio de configuración en Cisco ISE.



Nota: Debido a que CoA requiere una dirección MAC o un ID de sesión, se recomienda que no rechace el puerto que se muestra en el informe SNMP del dispositivo de red.

Las operaciones ANC fallan cuando no se encuentra la dirección IP o MAC

Una operación ANC que se realiza en un extremo falla cuando una sesión activa para ese extremo no contiene información sobre la dirección IP. Esto también se aplica a la dirección MAC y al ID de sesión de ese terminal.



Nota: Cuando desee cambiar el estado de autorización de un terminal a través de ANC, debe proporcionar la dirección IP o la dirección MAC para el terminal. Si la dirección IP o la dirección MAC no se encuentra en la sesión activa para el terminal, puede ver el mensaje de error: "No se ha encontrado ninguna sesión activa para esta dirección MAC, dirección IP o ID de sesión".

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).