Configurar o ANC no ISE 3.3 e no Stealthwatch 7.5.1

Contents

Introdução

Este documento descreve a configuração de contenção rápida de ameaças (Adaptive Network Control) no Cisco ISE® versão 3.3 e no Stealthwatch.

Pré-requisitos

A Cisco recomenda conhecimento sobre estes tópicos:

- Identity services engine (ISE)
- Grade de intercâmbio de plataforma (PxGrid)
- Análise de rede segura (Stealthwatch)
- Contenção rápida de ameaças (controle de rede adaptável - ANC).

Neste documento, presume-se que o Cisco Identity Services Engine esteja integrado ao Secure Network Analytics (Stealthwatch) usando pxGrid habilitado para ANC.

Componentes Utilizados

As informações neste documento são baseadas nestes softwares e versões:

- Cisco Identity Services Engine (ISE) versão 3.3

- Análise de rede segura (Stealthwatch) 7.5.1
- Catalyst 9300

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

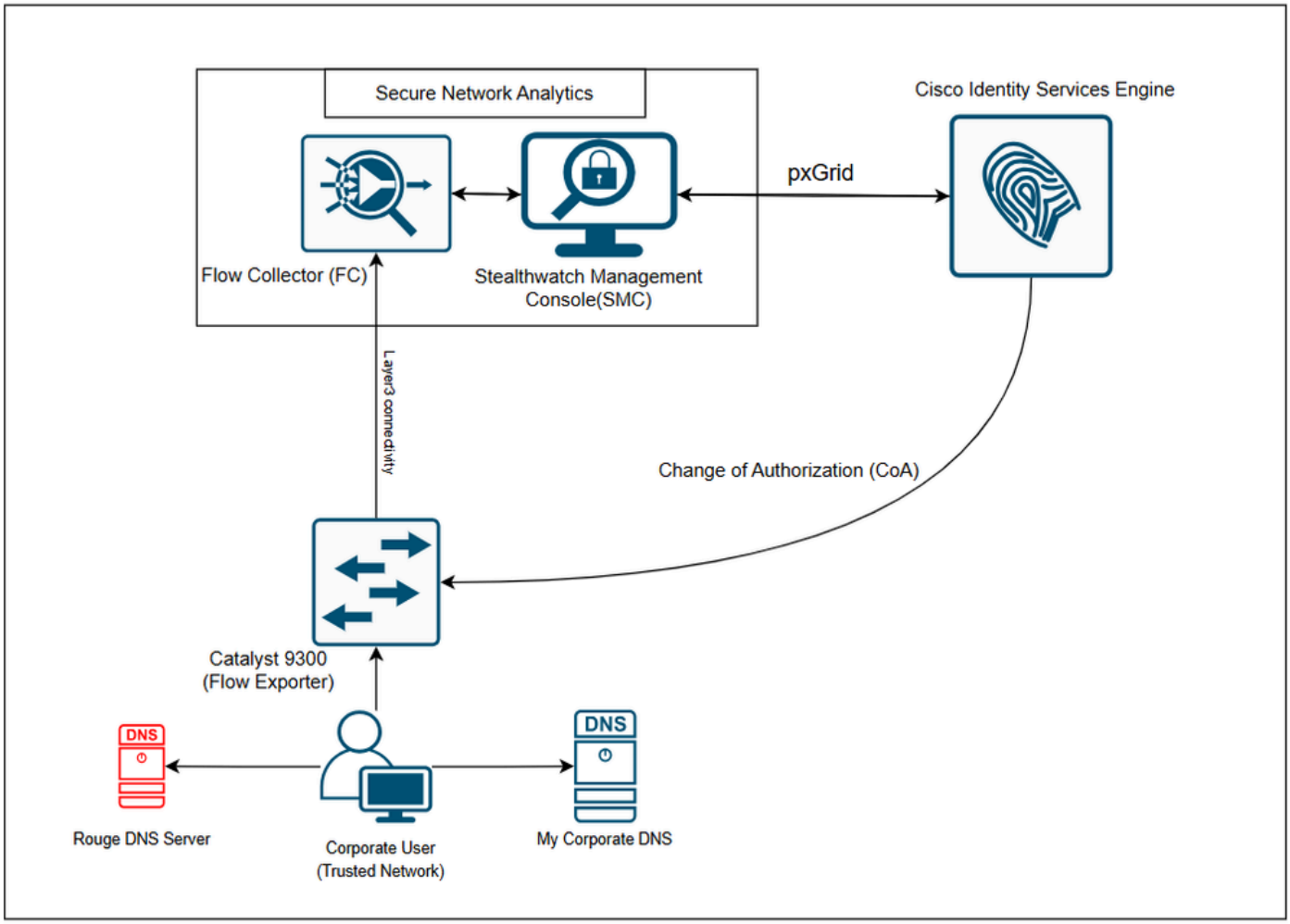
O Cisco Secure Cloud Analytics (agora parte do Cisco XDR) pode recuperar dados de atribuição do usuário do Cisco Identity Services Engine (ISE) usando o pxGrid. Essa integração permite o relatório de atividades do usuário no Visualizador de Eventos do Secure Cloud Analytics.

A combinação do Secure Network Analytics (antigo Stealthwatch) e do Cisco Identity Services Engine (ISE) ajuda as empresas a obter uma visão 360°, responder a ameaças com mais rapidez e proteger um negócio digital em crescimento. Depois que o Secure Network Analytics detecta tráfego suspeito, ele emite um alerta, dando ao administrador a opção de colocar o usuário em quarentena. O pxGrid permite que o Secure Network Analytics envie o comando de quarentena diretamente ao Identity Services Engine.

Este exemplo descreve o aproveitamento do servidor DNS corporativo para proteger contra ameaças da Internet. A intenção é estabelecer um mecanismo de alerta personalizado que seja acionado quando usuários internos se conectarem a servidores DNS externos. Essa iniciativa foi projetada para bloquear conexões com servidores DNS não autorizados que podem redirecionar o tráfego para sites externos prejudiciais.

Quando um alerta é disparado, o Cisco Secure Network Analytics se coordena com o Cisco ISE para colocar em quarentena o host que acessa servidores DNS não autorizados, usando uma Adaptive Network Control Policy via PxGrid.

Diagrama de Rede



Como mostrado no diagrama:

- Um usuário corporativo está conectado a um switch C9300 que está configurado para exportar os fluxos IP e enviar os dados para o coletor de fluxo.
- O mesmo usuário corporativo é configurado para usar servidores DNS corporativos.
- O Flow Collector é integrado ao Stealthwatch Management Console (SMC)
- Stealthwatch Management Console (SMC) integrado via Pxgrid com ISE.

Configuração Passo a Passo

1. Prepare o switch para monitorar e exportar fluxos usando o netflow.

A configuração básica de fluxo em um switch C9300 executando o 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
```

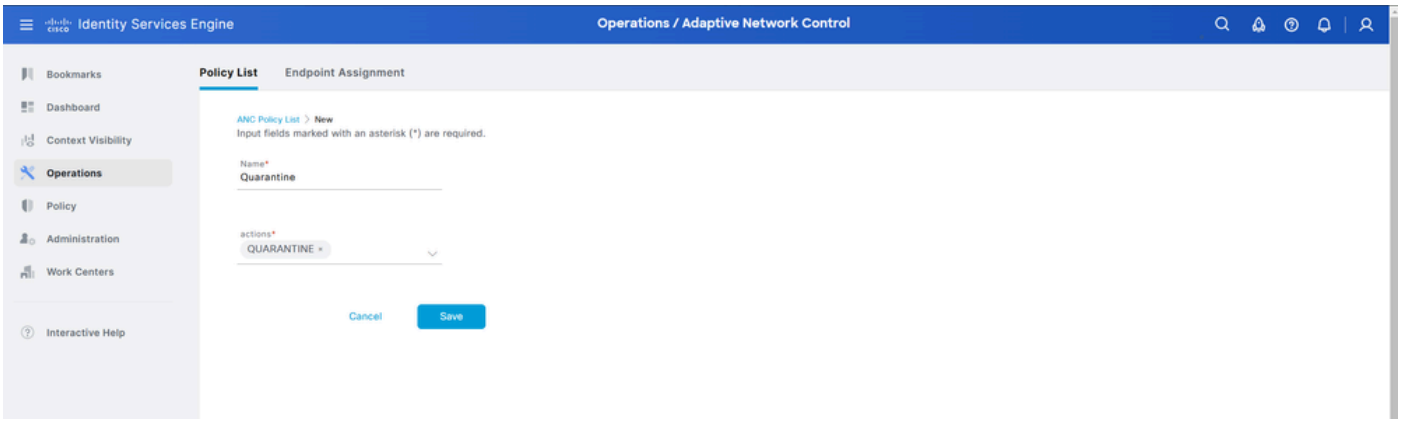
```
  collect transport tcp flags
  collect interface output
  collect counter bytes long
  collect counter packets long
  collect timestamp absolute first
  collect timestamp absolute last


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
```

Após concluir a configuração, ele permite que o C9300 exporte dados de fluxo IP para o Flow Collector. Em seguida, o coletor de fluxo processa e transfere esses dados para o Stealthwatch Management Console (SMC) para análise e monitoramento.

2. HabilitarControle de Rede Adaptável no Cisco ISE.

O ANC é desativado por padrão. O ANC é habilitado somente quando o pxGrid está habilitado e permanece habilitado até que você desabilite manualmente o serviço no portal do Administrador.

Selecione Operations > Adaptive Network Control > Policy List > Add, depois insira Quarantine for the Policy Name e Quarantine for the Action.

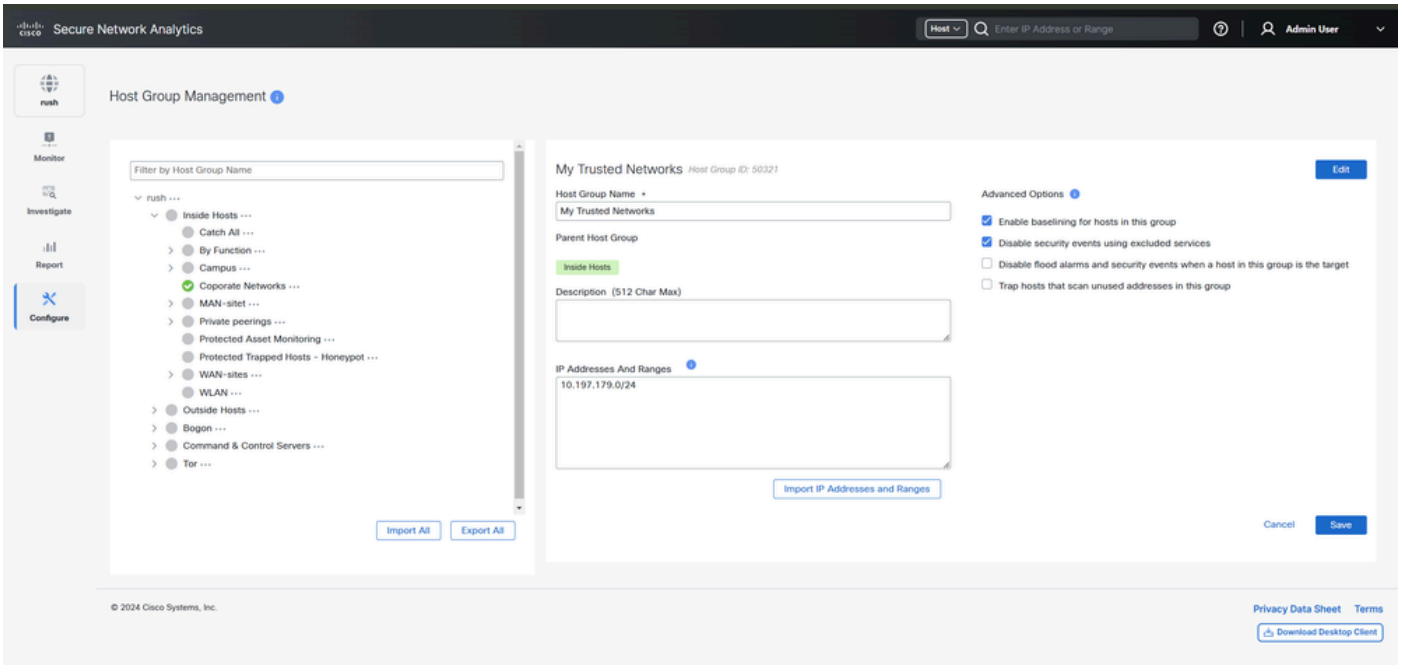


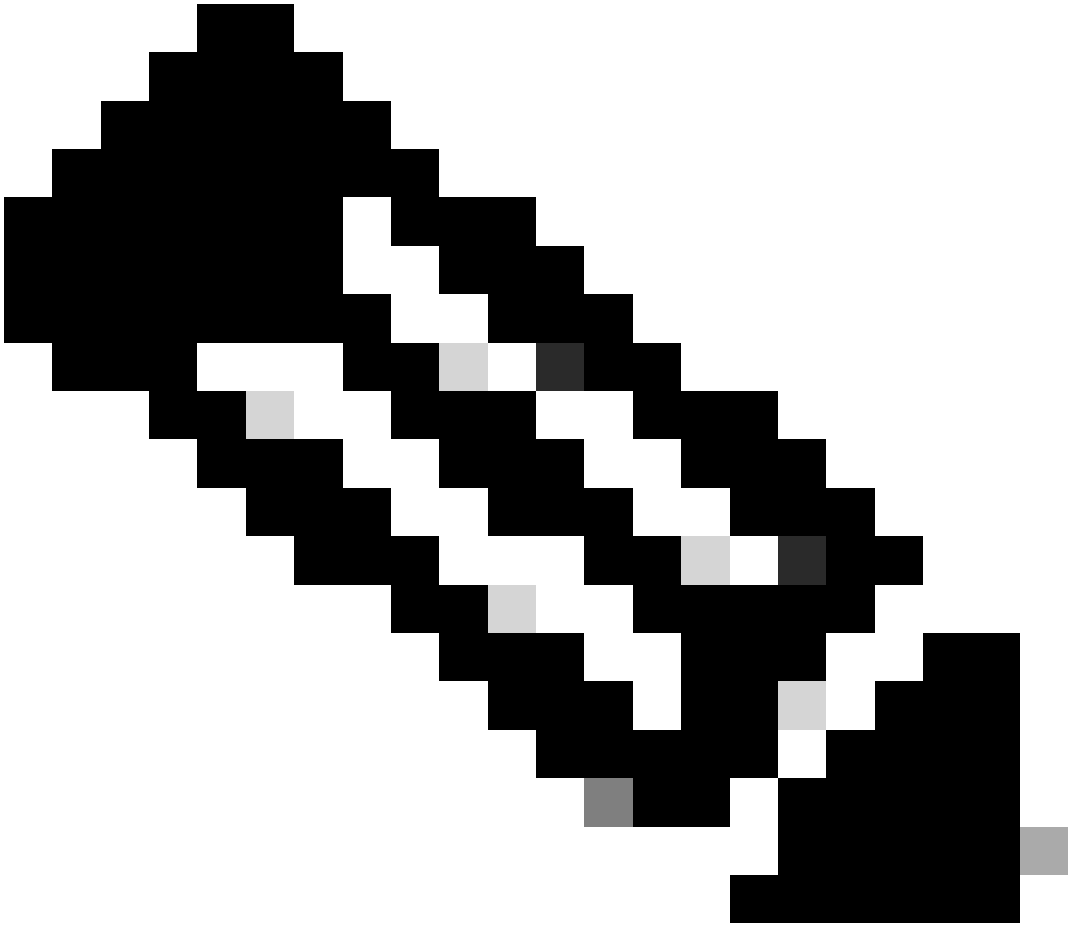
3. Configure o Secure Network Analytics para Disparo de Eventos e Gerenciamento de Resposta para contenção rápida de ameaças.

Passo 1: Faça login na GUI do SMC e navegue até Configure > Detection > Host Group Management > Clique no ícone (...) (reticências) ao lado de Inside Hosts e selecione Add Host Group.

Neste exemplo, um novo grupo de hosts é criado com o nome Minhas redes confiáveis sob o grupo de hosts pai de Hosts internos.

Essa rede pode ser normalmente atribuída à máquina do usuário final para monitorar o uso do DNS.

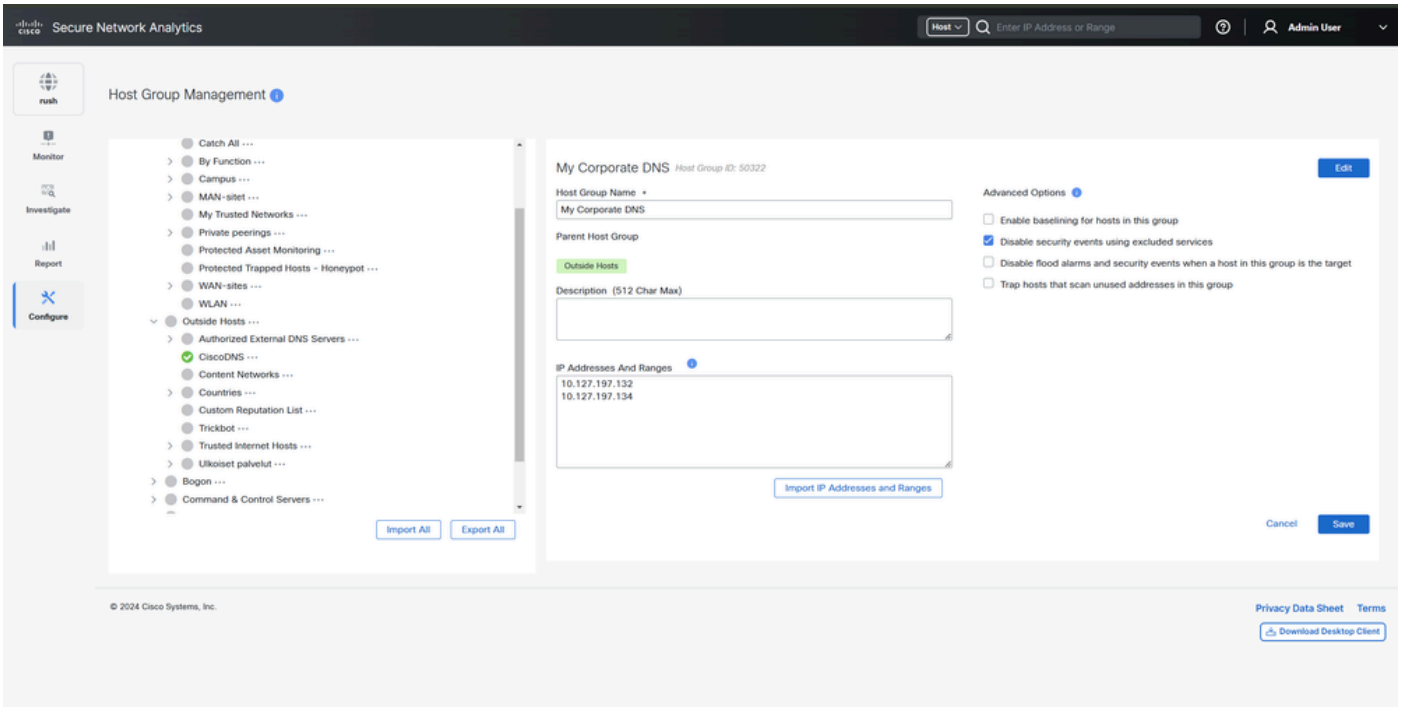


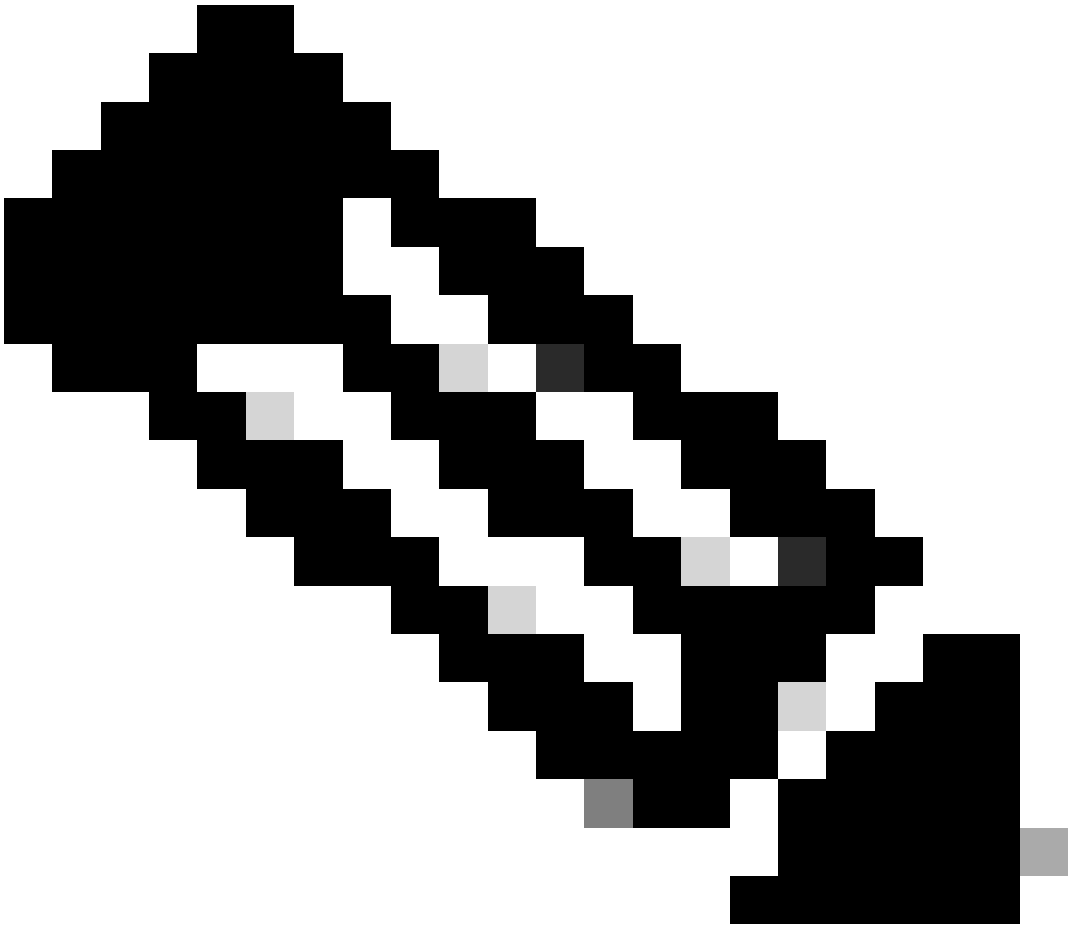


Note: Para este exemplo, a sub-rede IP 10.197.179.0/24 é usada como uma sub-rede de rede local (LAN). Isso pode diferir no ambiente de rede real, dependendo da arquitetura de rede.

Passo 2: Faça login na GUI do SMC e navegue até Configure > Detection > Host Group Management > Clique em (...) além de Outside Hosts e selecione Add Host Group.

Neste exemplo, um novo grupo de hosts é criado com o nome My Corporate DNS no grupo de hosts pai de hosts externos.

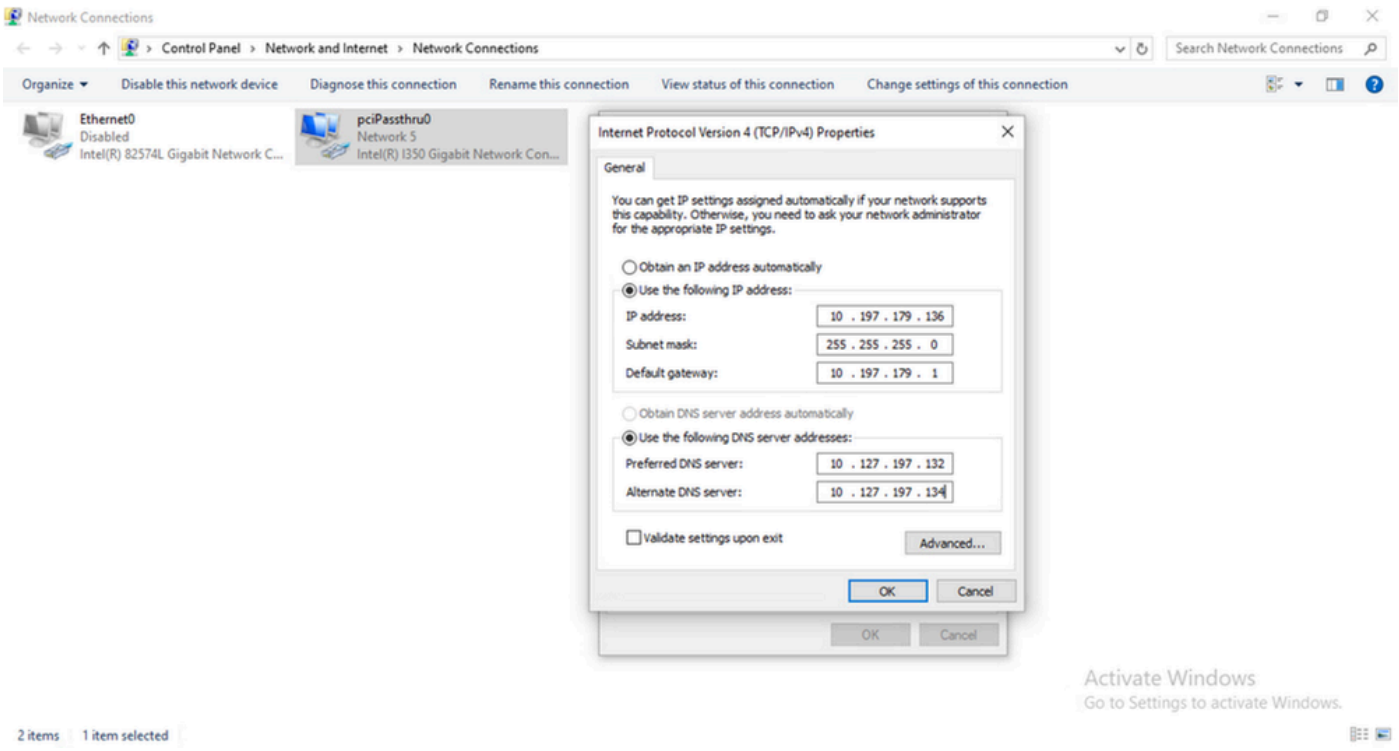




Note: Para este exemplo, os IPs 10.127.197.132 e 10.127.197.134 são usados como os

servidores DNS desejados a serem usados pelos usuários finais, isso pode diferir no ambiente de rede real, dependendo da arquitetura de rede.

O PC do laboratório de testes usado para demonstração é configurado com IP estático 10.197.179.136 (pertence ao grupo de hosts criado em Minhas redes confiáveis) e DNS 10.127.197.132 e 10.127.197.134 (pertence ao grupo de hosts criado em Minha empresa DNS).



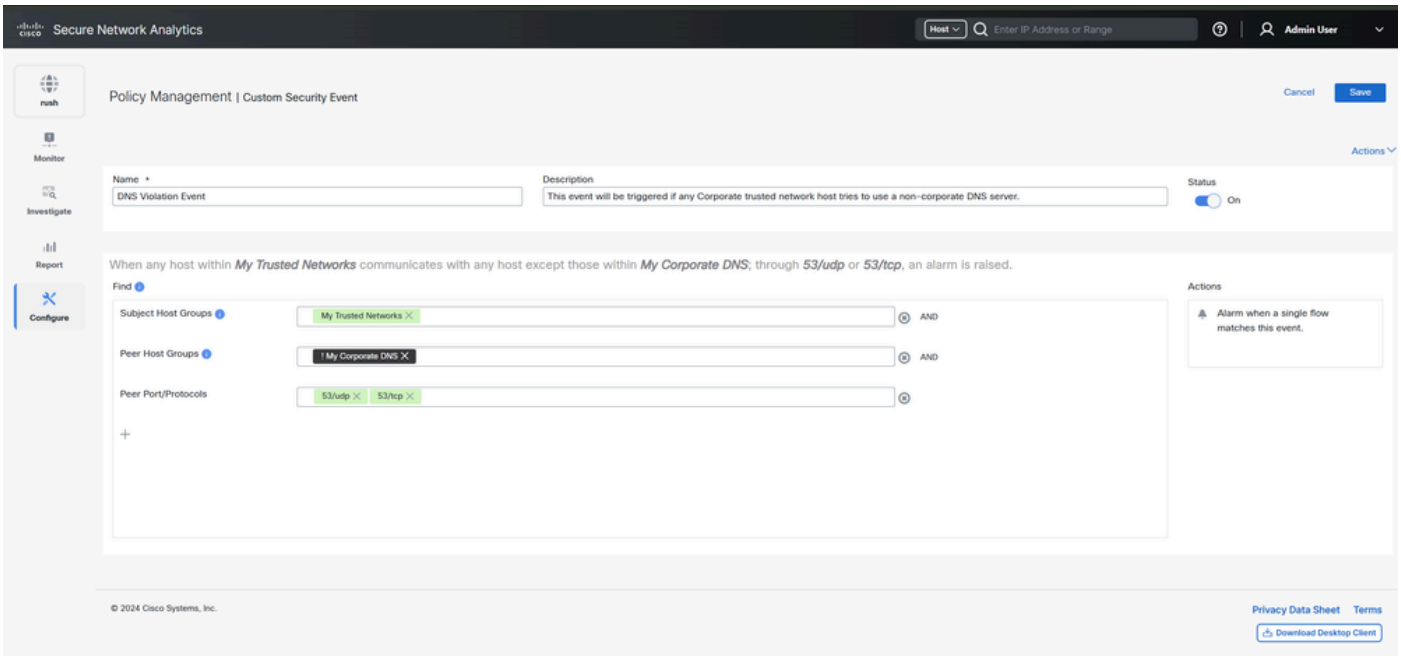
Passo 3: Configure um sistema de alerta personalizado para detectar quando usuários internos se conectam a servidores DNS externos, acionando um alarme para bloquear conexões a servidores DNS não autorizados que possam redirecionar o tráfego para sites externos mal-intencionados. Quando um alarme é ativado, o Cisco Secure Network Analytics se coordena com o Cisco ISE para isolar o host que usa esses servidores DNS não autorizados, empregando uma Adaptive Network Control Policy via PxGrid.

Navegue até Configurar > Gerenciamento de políticas.

Crie eventos personalizados com as seguintes informações:

- Nome :Evento de violação de DNS.
- Grupos de host do assunto:Minhas redes confiáveis.
- Grupos de host de mesmo nível: (Não) Meu DNS corporativo.
- Porta/Protocolos de Par: 53/UDP 53/TCP

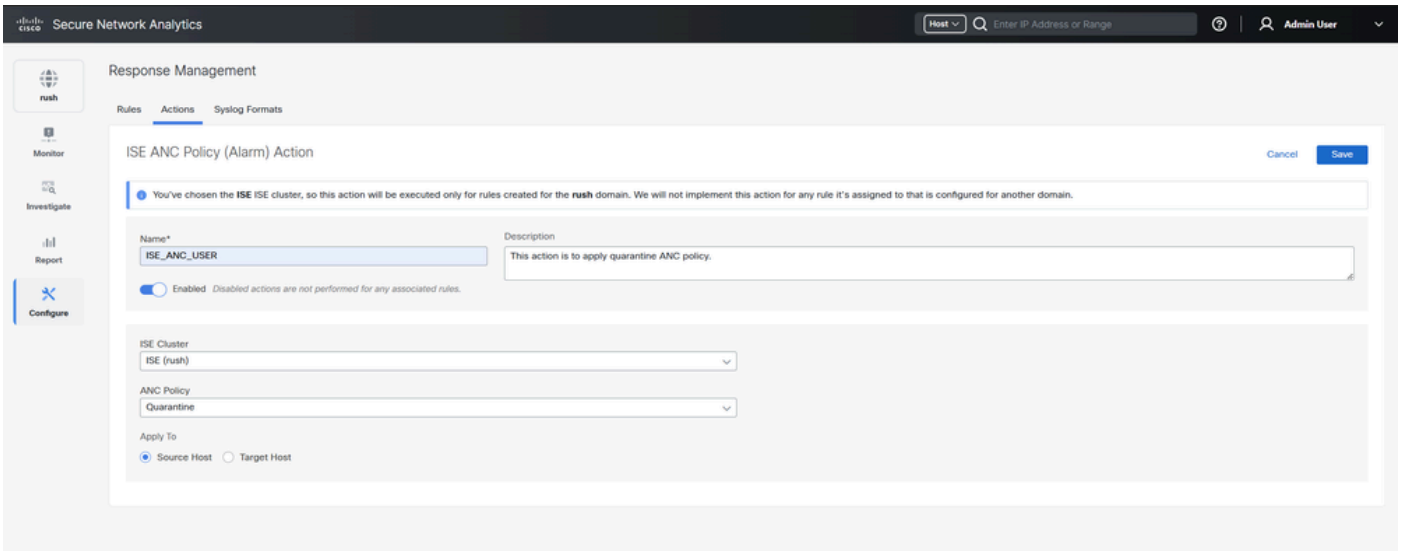
Isso significa que quando qualquer host em Minhas redes confiáveis (Grupo de hosts) se comunica com qualquer host, exceto aqueles dentro de Meu DNS corporativo (Grupo de hosts) por meio de 53/up ou 53/tcp, um alarme é acionado.



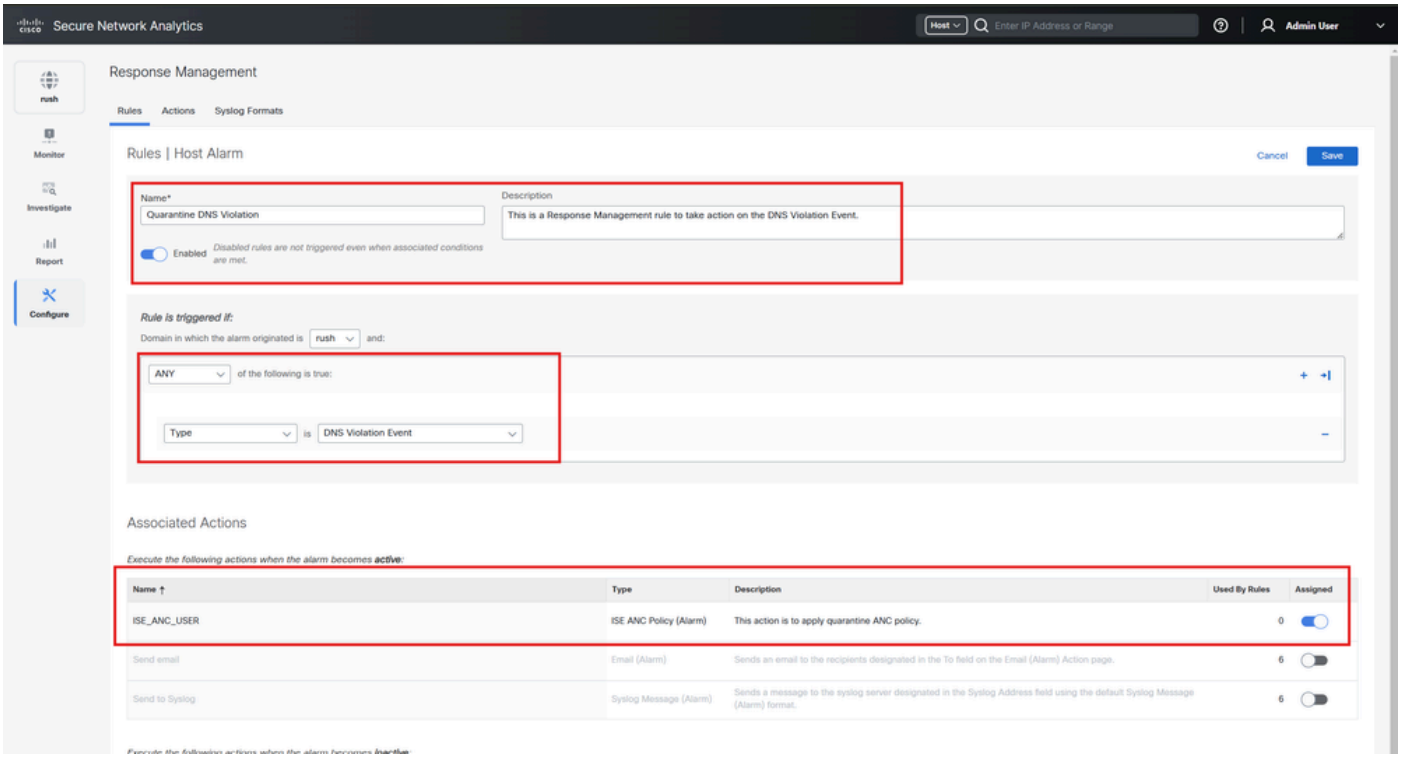
Passo 4: Configure uma ação de Gerenciamento de Resposta a ser executada e que possa ser aplicada posteriormente à Regra de Gerenciamento de Resposta depois de criada.

Navegue para Configurar > Gerenciamento de resposta > Ações, clique em Adicionar nova ação e selecione Política ISE ANC (Alarme).

Atribua um nome e escolha o cluster do Cisco ISE específico a ser notificado para implementar uma política de quarentena para quaisquer violações ou conexões a servidores não autorizados.



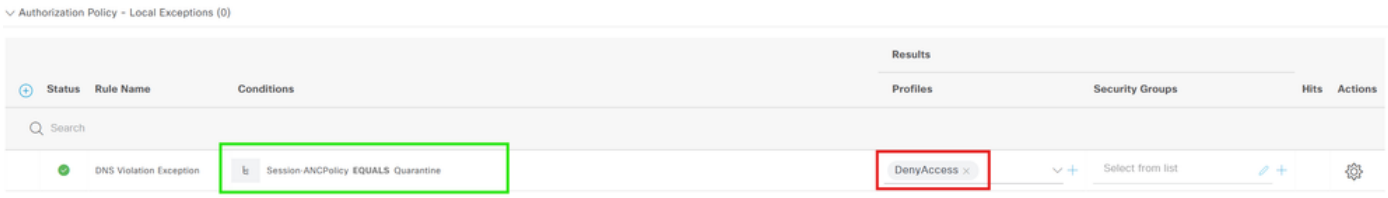
Etapa 5: na seção Regras, Criar uma nova regra. Essa regra aplica a Ação definida anteriormente sempre que um host dentro da rede interna tenta enviar o tráfego DNS para servidores DNS não autorizados. Na seção A regra é acionada se, escolha Tipo e selecione o evento personalizado criado.
Em Associated Actions, selecione a ação do alarme do ISE ANC que foi configurada anteriormente.

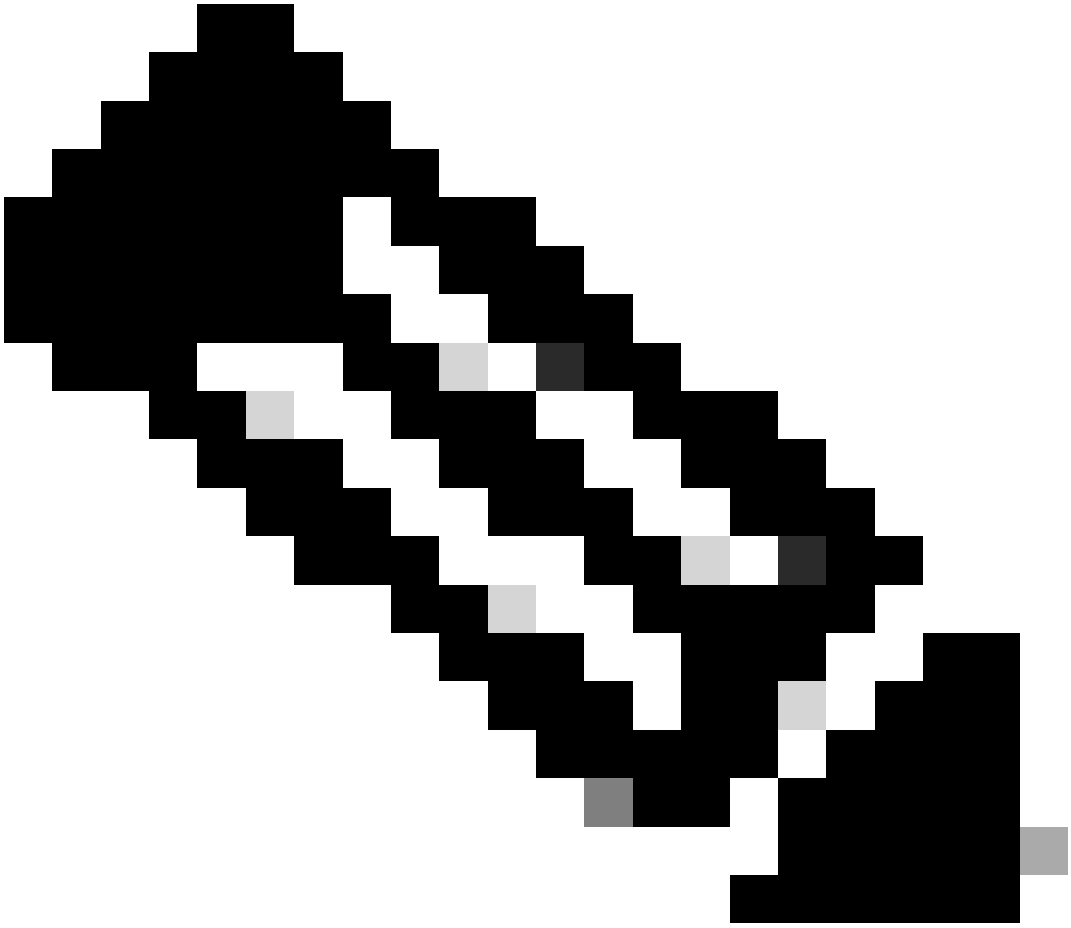


4. Configure o Cisco ISE para responder às ações iniciadas pelo Stealthwatch ao disparar o evento.

Faça login na GUI do Cisco ISE e navegue até Policy > Policy Sets > Choose the Policy set > em Authorization Policy - Local Exceptions > Create new Policy.

- Nome: Exceção de violação de DNS
- Condições: Sessão: ANCPolicy É IGUAL a Quarentena
- Perfis de autorização: NegarAcesso

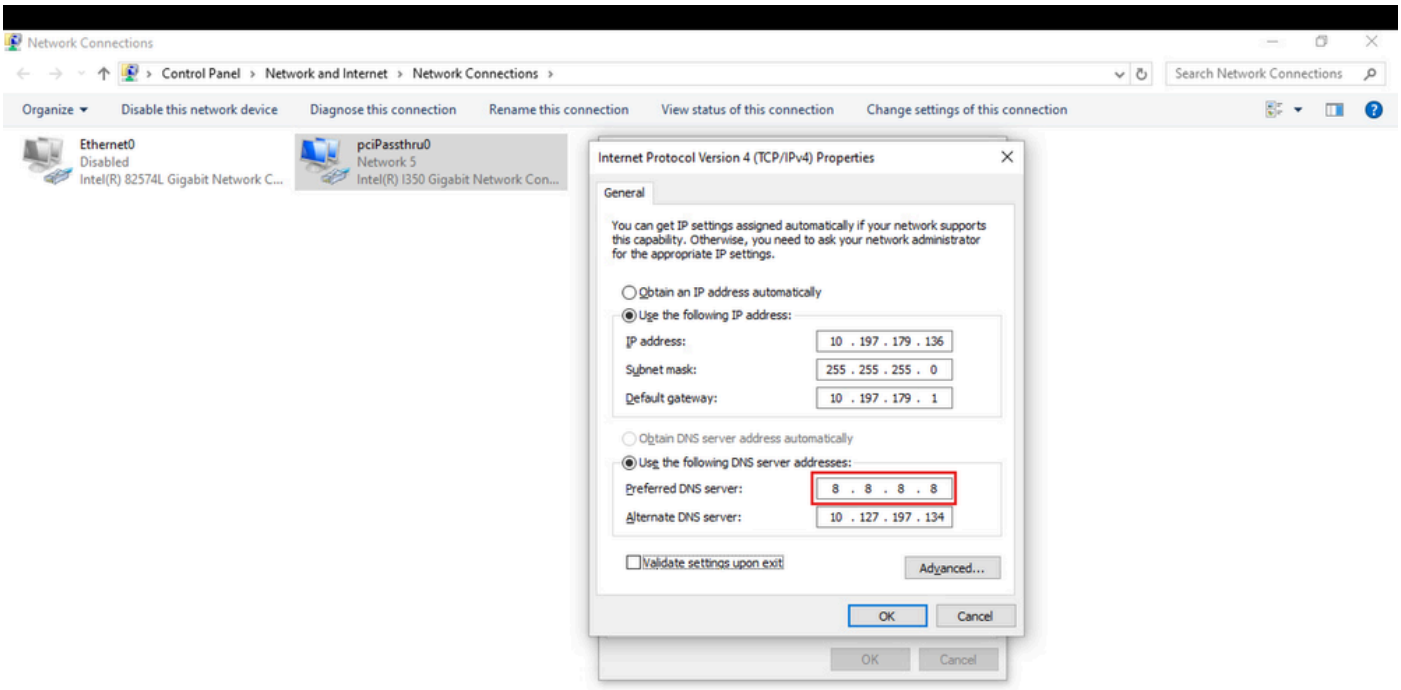




Note: Neste exemplo, quando o evento de violação de DNS é disparado, o acesso é negado ao usuário com base na configuração

Verificar

Para demonstrar o caso de uso, a entrada DNS no endpoint foi alterada para 8.8.8.8, o que aciona o evento de violação de DNS configurado . Como o servidor DNS não pertence ao grupo de hosts dos servidores DNS corporativos, ele aciona o evento que resulta em uma negação de acesso ao endpoint.



No switch C9300, verifique usando o cache show flow monitor IPv4_NETFLOW | no comando 8.8.8.8 com a saída para ver se os fluxos estão sendo capturados e enviados ao coletor de fluxo. O IPv4_NETFLOW é configurado na configuração do switch.

<#root>

IPV4 SOURCE ADDRESS:

10.197.179.136

IPV4 DESTINATION ADDRESS:

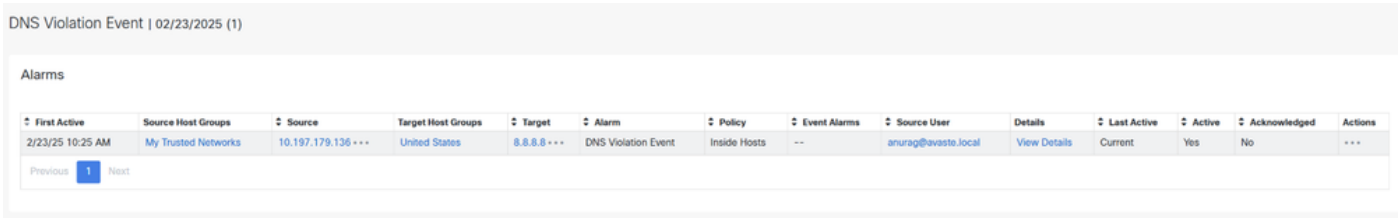
8.8.8.8

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

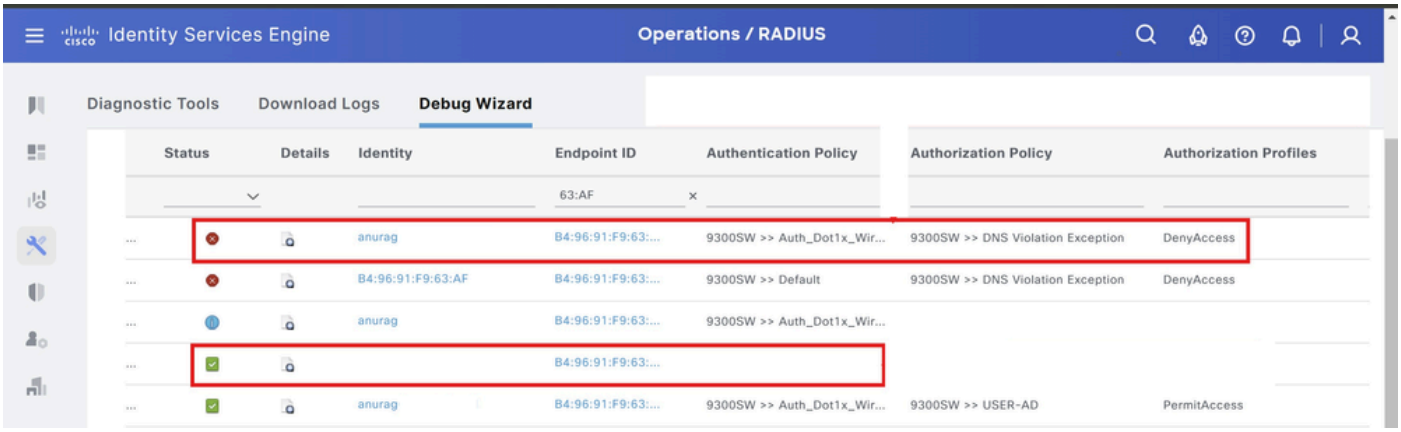
Quando o evento for acionado no Stealthwatch, navegue para Monitor > Security Insight Dashboard,.



Navegue até Monitor > Integration > ISE ANC Policy Assignments.

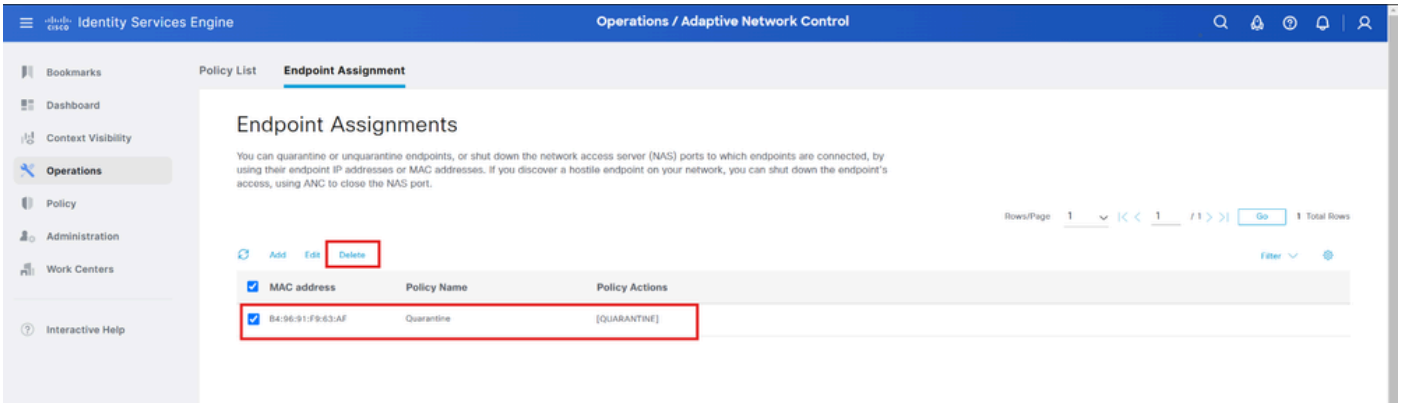
Certifique-se de que o Cisco Secure Network Analytics tenha implementado com êxito a Adaptive Network Control Policy via PxGrid e Cisco ISE para colocar o host em quarentena.

Da mesma forma, no Cisco ISE, navegue para Operations > RADIUS > Livelogs e aplique o filtro para o endpoint.



De acordo com a exceção de violação de DNS da política local, a alteração de autorização (CoA) é emitida pelo ISE e o acesso ao ISE é negado ao ponto final.

Depois que as ações de correção forem executadas no endpoint, remova o MAC de Operations > Adaptive Network Control > Endpoint Assignments > Delete para remover o endereço MAC do endpoint.



Referência de registro no Cisco ISE.

Atributos definidos no nível TRACE para o componente pxgrid (pxgrid-server.log) no Cisco ISE, os logs são vistos no arquivo 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

```
"}
```

Troubleshooting

Endpoints em quarentena não renovam a autenticação após a alteração da política

Problema

A autenticação falhou devido a uma alteração na política ou identidade adicional e nenhuma

reautenticação está ocorrendo. A autenticação falha ou o endpoint em questão permanece incapaz de se conectar à rede. Esse problema geralmente ocorre em computadores cliente que não passam na avaliação de postura de acordo com a política de postura atribuída à função de usuário.

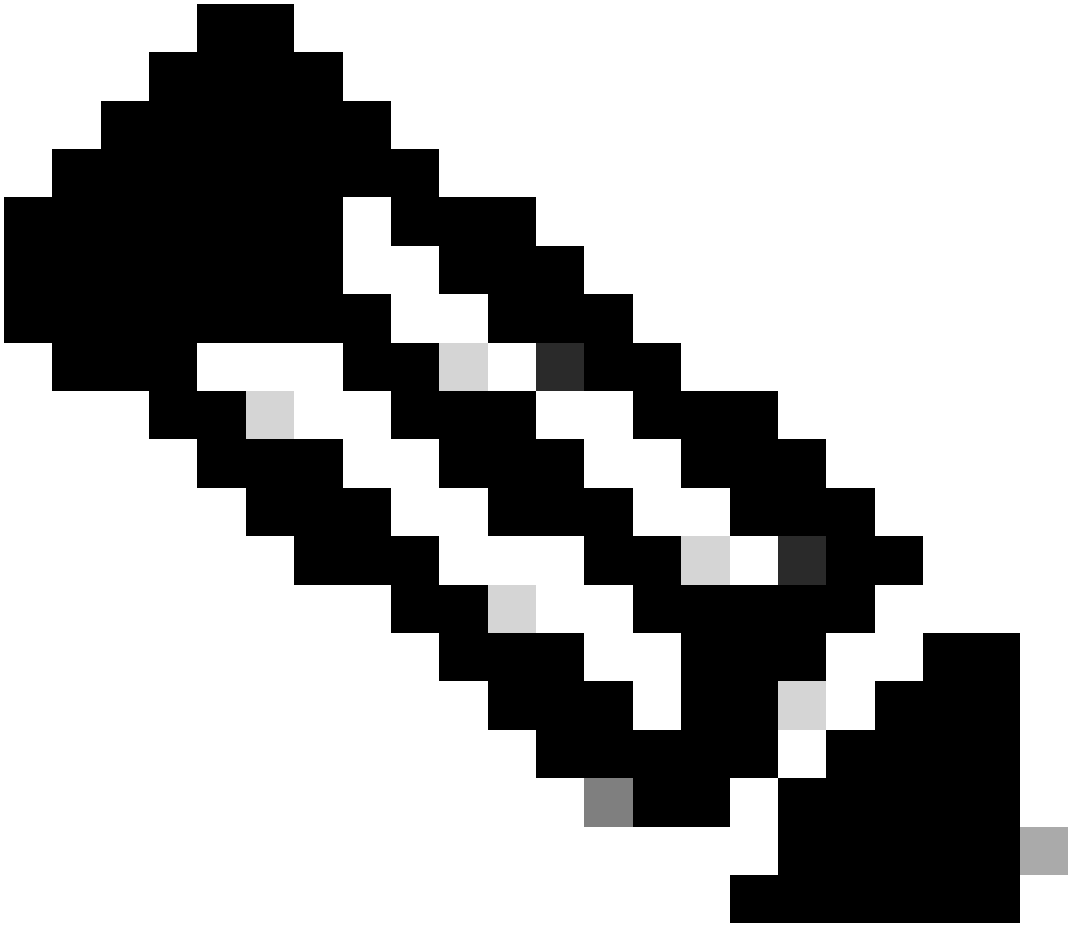
Possíveis causas

A configuração do timer de autenticação não está definida corretamente na máquina cliente ou o intervalo de autenticação não está definido corretamente no switch.

Solução

Há várias soluções possíveis para esse problema:

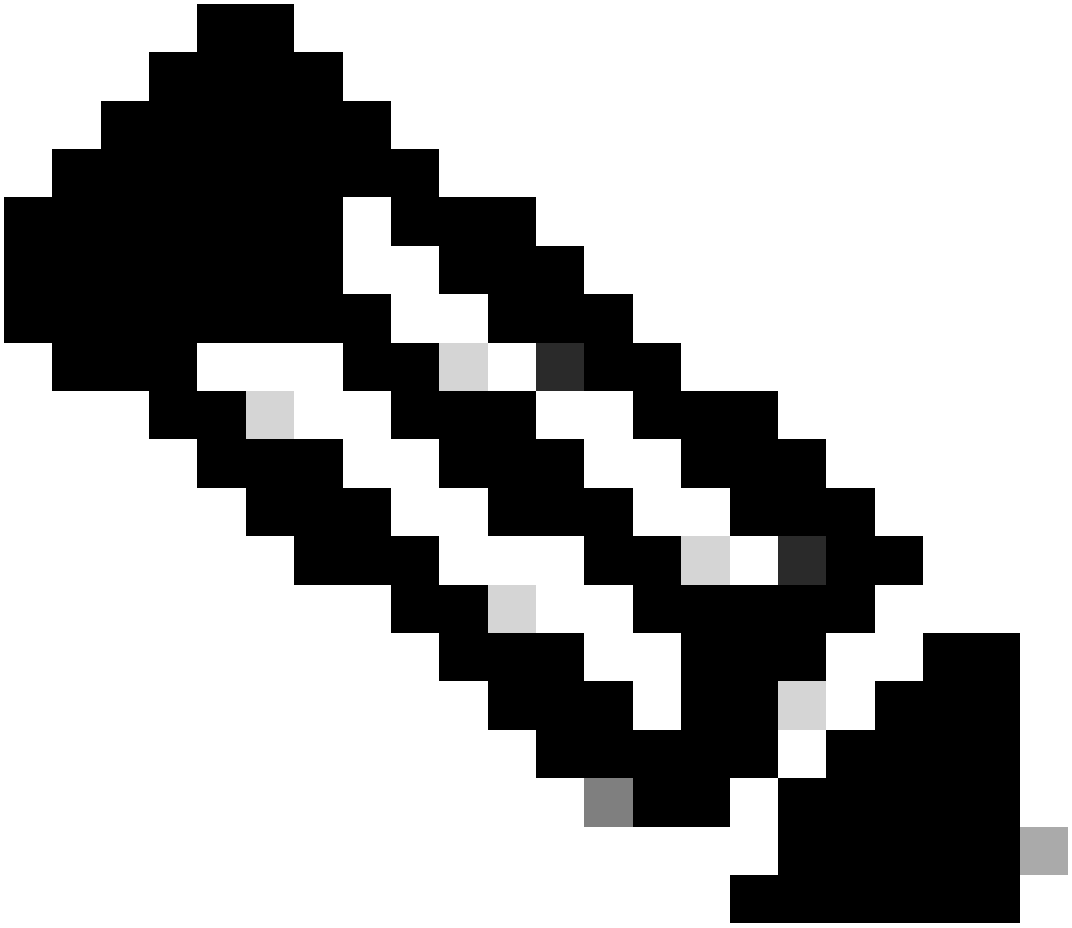
1. Verifique o relatório Session Status Summaryno Cisco ISE para o NAD ou switch especificado e certifique-se de que a interface tenha o intervalo de autenticação apropriado configurado.
2. Insira show running configuration no NAD/switch e verifique se a interface está configurada com uma configuração apropriada de reinicialização do temporizador de autenticação. (Por exemplo, reinicialização do temporizador de autenticação 15 e reautenticação do temporizador de autenticação 15).
3. Insira interface shutdown e no shutdown para devolver a porta no NAD/switch e forçar uma nova autenticação e uma possível alteração de configuração no Cisco ISE.



Note: Como CoA requer um endereço MAC ou ID de sessão, é recomendável não devolver a porta exibida no relatório SNMP do dispositivo de rede.

Falha nas operações ANC quando o endereço IP ou o endereço MAC não é encontrado

Uma operação ANC executada em um endpoint falha quando uma sessão ativa desse endpoint não contém informações sobre o endereço IP. Isso também se aplica ao endereço MAC e à ID de sessão desse ponto final.



Note: Quando quiser alterar o estado de autorização de um endpoint por meio do ANC, você deve fornecer o endereço IP ou o endereço MAC do endpoint. Se o endereço IP ou o endereço MAC não for encontrado na sessão ativa para o endpoint, você poderá ver a mensagem de erro: "Nenhuma sessão ativa encontrada para este endereço MAC, endereço IP ou ID de sessão".

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.