Configurer ANC sur ISE 3.3 et StealthWatch 7.5.1

Table des matières

Introduction

Ce document décrit la configuration de Rapid Threat Containment (Adaptive Network Control) sur Cisco ISE® version 3.3 et StealthWatch.

Conditions préalables

Cisco recommande des connaissances sur les sujets suivants :

- Moteur du service de vérification des identités (ISE)
- Platform Exchange Grid (PxGrid)
- Secure Network Analytics (StealthWatch)
- Confinement rapide des menaces (Adaptive Network Control - ANC).

Dans ce document, nous supposons que Cisco Identity Services Engine est intégré à Secure Network Analytics (StealthWatch) à l'aide de pxGrid compatible ANC.

Composants utilisés

Les informations contenues dans ce document sont basées sur les logiciels et versions suivants :

- Cisco Identity Services Engine (ISE) version 3.3
- Secure Network Analytics (StealthWatch) 7.5.1
- Catalyst 9300

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

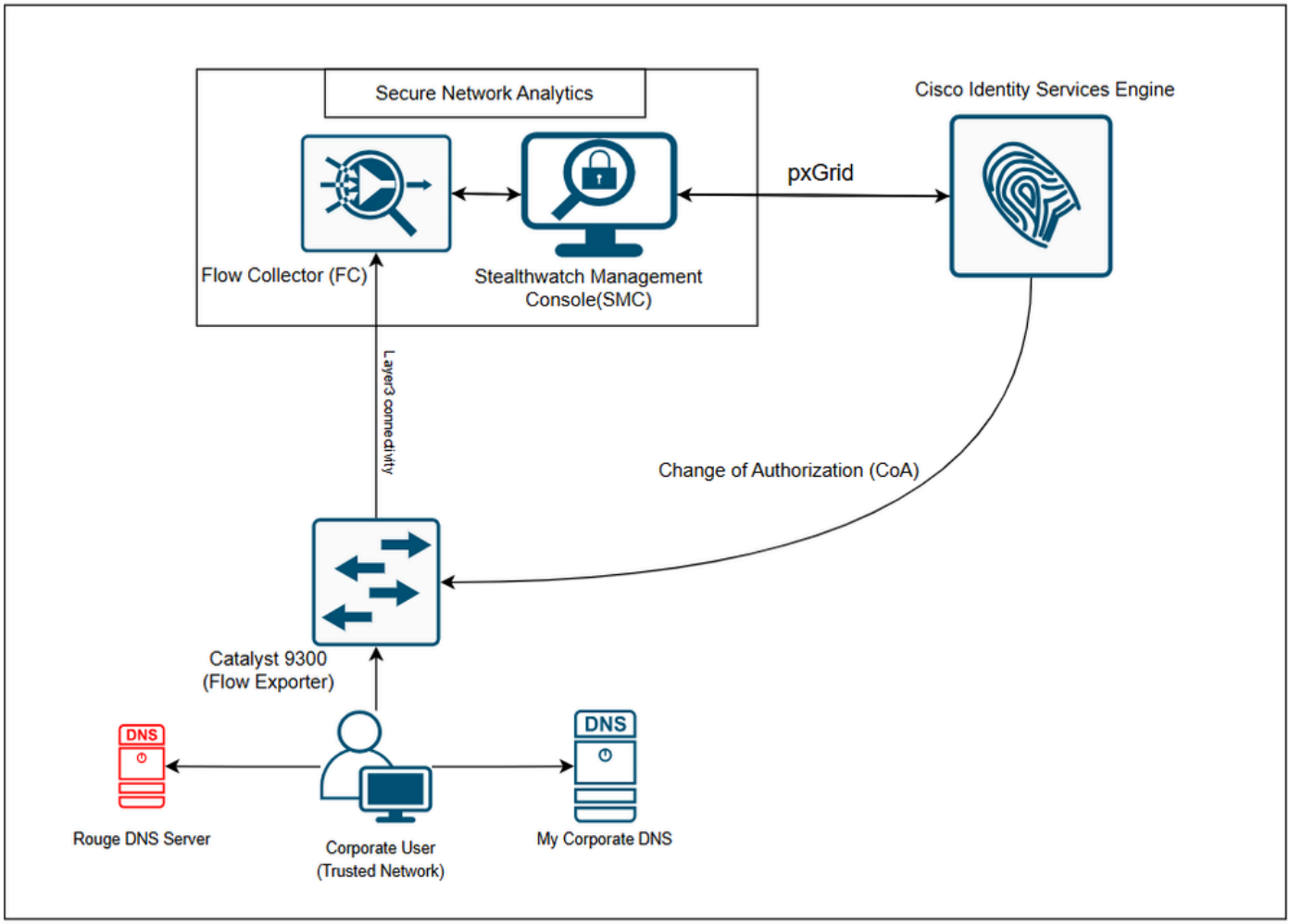
Cisco Secure Cloud Analytics (qui fait désormais partie de Cisco XDR) peut récupérer des données d'attribution d'utilisateur à partir de Cisco Identity Services Engine (ISE) à l'aide de pxGrid. Cette intégration permet de générer des rapports sur l'activité des utilisateurs dans l'Observateur d'événements Secure Cloud Analytics.

L'association de Secure Network Analytics (anciennement StealthWatch) et de Cisco Identity Services Engine (ISE) permet aux entreprises d'obtenir une vue à 360°, de répondre plus rapidement aux menaces et de sécuriser une entreprise numérique en pleine croissance. Une fois que Secure Network Analytics détecte un trafic anormal, il émet une alerte, donnant à l'administrateur la possibilité de mettre l'utilisateur en quarantaine. pxGrid permet à Secure Network Analytics de transférer la commande de quarantaine directement à Identity Services Engine.

Cet exemple décrit l'utilisation d'un serveur DNS d'entreprise pour se protéger contre les menaces Internet. L'objectif est d'établir un mécanisme d'alerte personnalisé qui se déclenche lorsque des utilisateurs internes se connectent à des serveurs DNS externes. Cette initiative est conçue pour bloquer les connexions aux serveurs DNS non autorisés qui pourraient rediriger le trafic vers des sites externes dangereux.

Lorsqu'une alerte est déclenchée, Cisco Secure Network Analytics se coordonne avec Cisco ISE pour mettre en quarantaine l'hôte accédant à des serveurs DNS non autorisés, à l'aide d'une politique de contrôle réseau adaptatif via PxGrid.

Diagramme du réseau



Comme le montre le schéma :

- Un utilisateur d'entreprise est connecté à un commutateur C9300 qui est configuré pour exporter les flux IP et envoyer les données au collecteur de flux.
- Le même utilisateur d'entreprise est configuré pour utiliser les serveurs DNS d'entreprise.
- Flow Collector est intégré à la console de gestion StealthWatch (SMC)
- Console de gestion StealthWatch (SMC) intégrée via Pxgrid avec ISE.

Configuration pas à pas

1. Préparez le commutateur à surveiller et à exporter des flux à l'aide de netflow.

Configuration de flux de base sur un commutateur C9300 exécutant 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
```

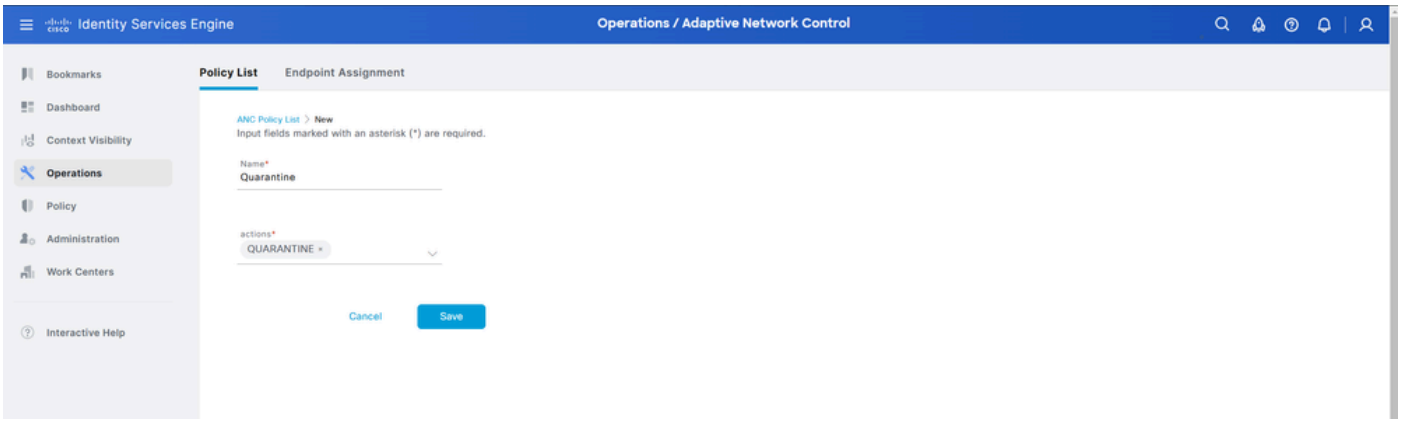
```
  collect transport tcp flags
  collect interface output
  collect counter bytes long
  collect counter packets long
  collect timestamp absolute first
  collect timestamp absolute last


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
```

Une fois la configuration terminée, le C9300 peut exporter les données de flux IP vers le collecteur de flux. Le collecteur de flux traite et transfère ensuite ces données vers la console de gestion StealthWatch (SMC) pour analyse et surveillance.

2. Activer le contrôle réseau adaptatif dans Cisco ISE.

ANC est désactivé par défaut. ANC n'est activé que lorsque pxGrid est activé, et il reste activé jusqu'à ce que vous désactiviez manuellement le service dans le portail Admin.

Sélectionnez Operations > Adaptive Network Control > Policy List > Add, puis entrez Quarantine pour le nom de la stratégie et Quarantine pour l'action.

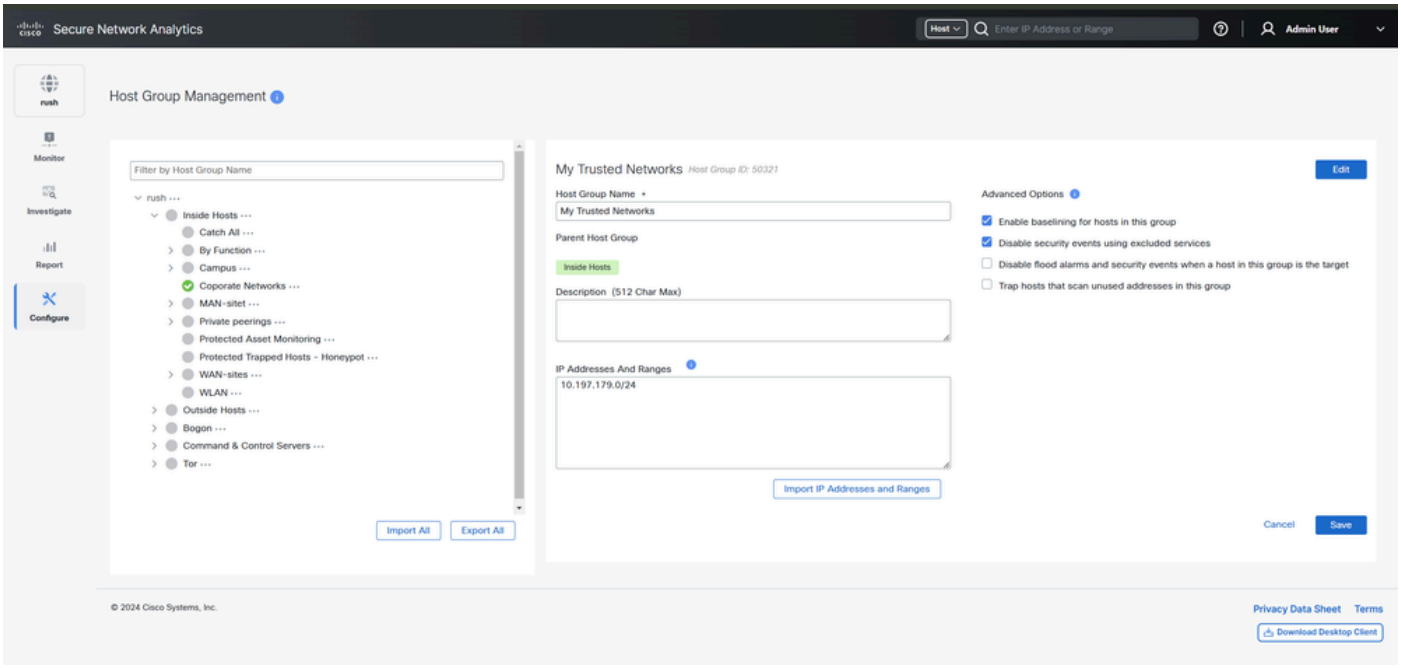


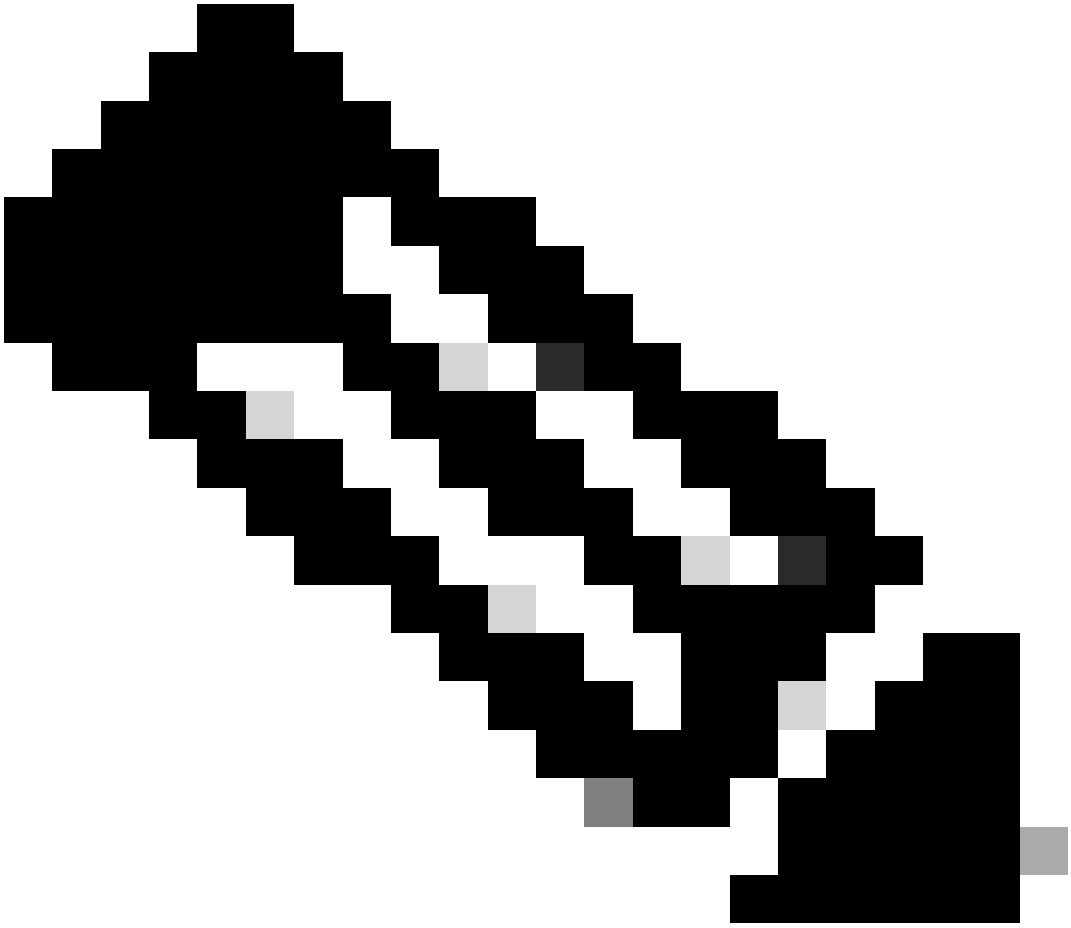
3. Configurez Secure Network Analytics pour Event Trigger et Response Management pour une maîtrise rapide des menaces.

Étape 1 : Connectez-vous à l'interface utilisateur graphique de SMC et accédez à Configure > Detection > Host Group Management > Cliquez sur l'icône (...) (points de suspension) en regard de Inside Hosts, puis sélectionnez Add Host Group.

Dans cet exemple, un nouveau groupe d'hôtes est créé sous le groupe d'hôtes parent d'hôtes internes sous le nom Mes réseaux de confiance.

Ce réseau peut généralement être attribué à l'ordinateur de l'utilisateur final pour surveiller l'utilisation du DNS.

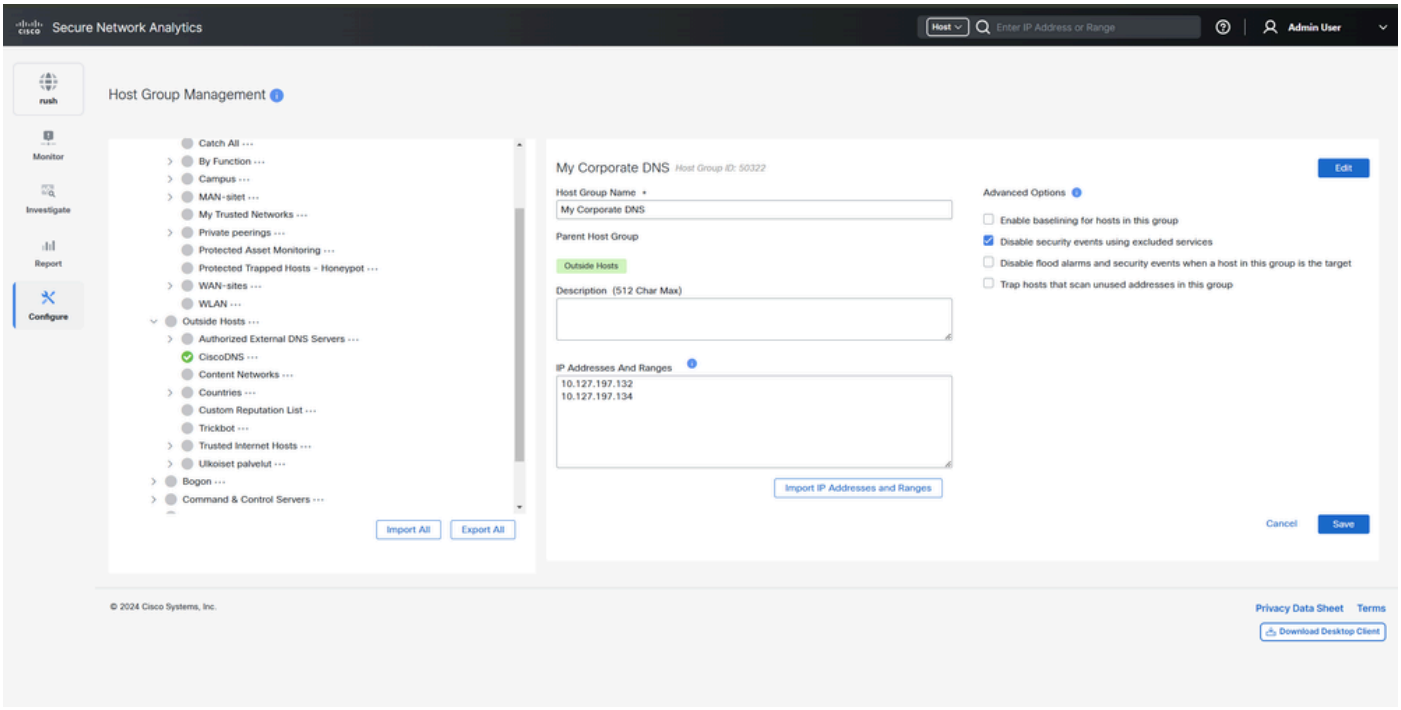


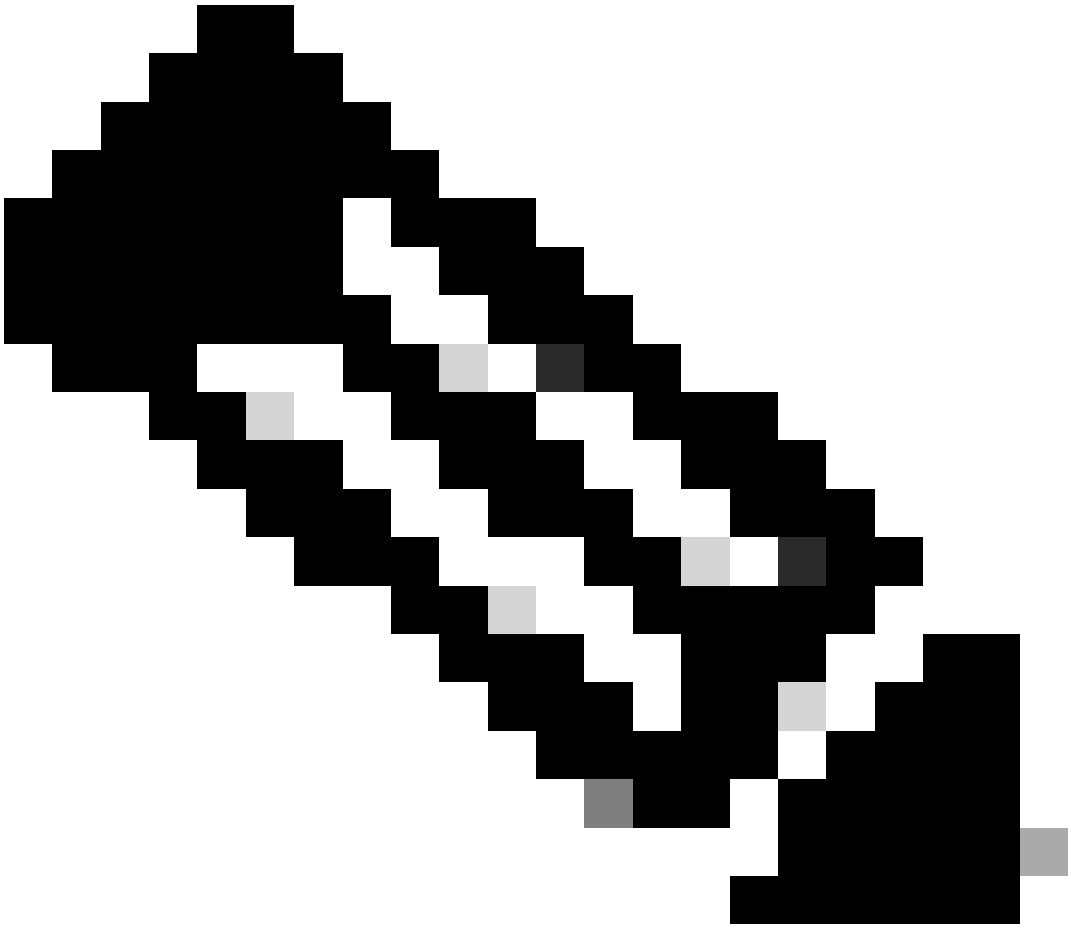


Remarque : Dans cet exemple, le sous-réseau IP 10.197.179.0/24 est utilisé comme sous-réseau de réseau local (LAN). Il peut varier dans l'environnement réseau réel en fonction de l'architecture réseau.

Étape 2 : Connectez-vous à l'interface utilisateur graphique de SMC et accédez à Configure > Detection > Host Group Management > Cliquez sur (...) en regard de Outside Hosts et sélectionnez Add Host Group.

Dans cet exemple, un nouveau groupe d'hôtes est créé avec le nom My Corporate DNS sous le groupe d'hôtes parent Outside Hosts.

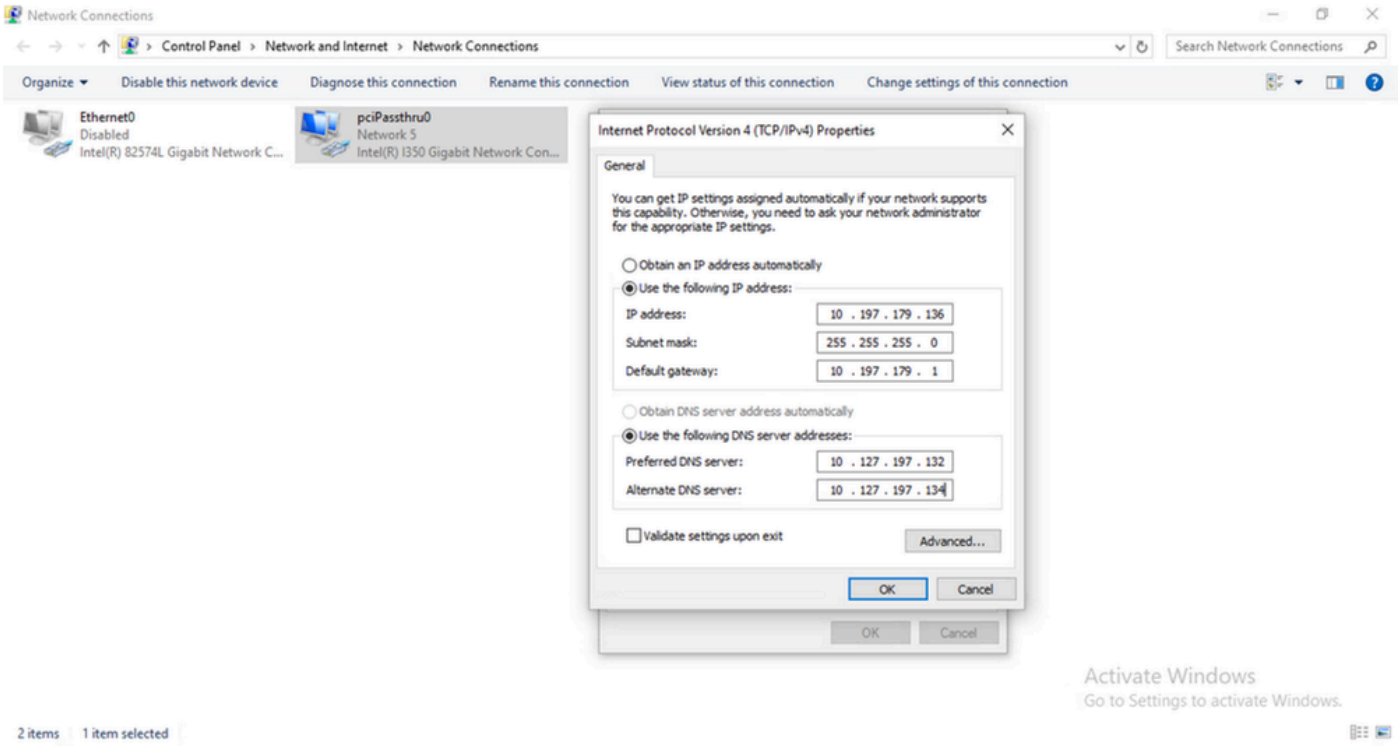




Remarque : Dans cet exemple, les adresses IP 10.127.197.132 et 10.127.197.134 sont

utilisées comme serveurs DNS à utiliser par les utilisateurs finaux. Cela peut varier dans l'environnement réseau réel en fonction de l'architecture réseau.

L'ordinateur de TP utilisé pour la démonstration est configuré avec l'adresse IP statique 10.197.179.136 (appartient au groupe d'hôtes Mes réseaux de confiance créé) et les adresses DNS 10.127.197.132 et 10.127.197.134 (appartient au groupe d'hôtes DNS de Mon entreprise créé).



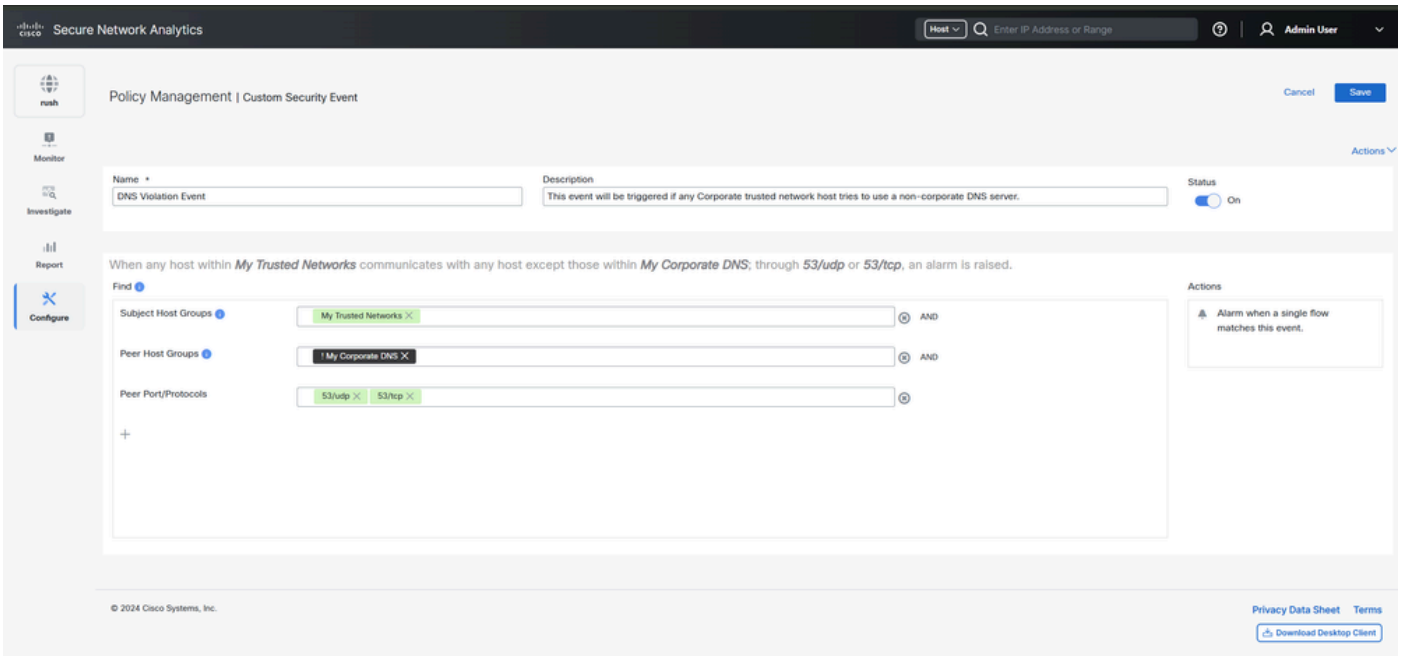
Étape 3 : Configurez un système d'alerte personnalisé pour détecter lorsque des utilisateurs internes se connectent à des serveurs DNS externes, déclenchant ainsi une alarme pour bloquer les connexions à des serveurs DNS non autorisés qui pourraient potentiellement rediriger le trafic vers des sites externes malveillants. Une fois l'alarme activée, Cisco Secure Network Analytics se coordonne avec Cisco ISE pour isoler l'hôte à l'aide de ces serveurs DNS non autorisés à l'aide d'une politique Adaptive Network Control Policy via PxGrid.

Naviguez jusqu'à Configure > Policy Management.

Créez un événement personnalisé avec les informations suivantes :

- Nom : Événement de violation DNS.
- Sujet Groupes d'hôtes : Mes réseaux de confiance.
- Groupes d'hôtes homologues : (Non) Mon DNS d'entreprise.
- Port/protocoles homologues : 53/UDP 53/TCP

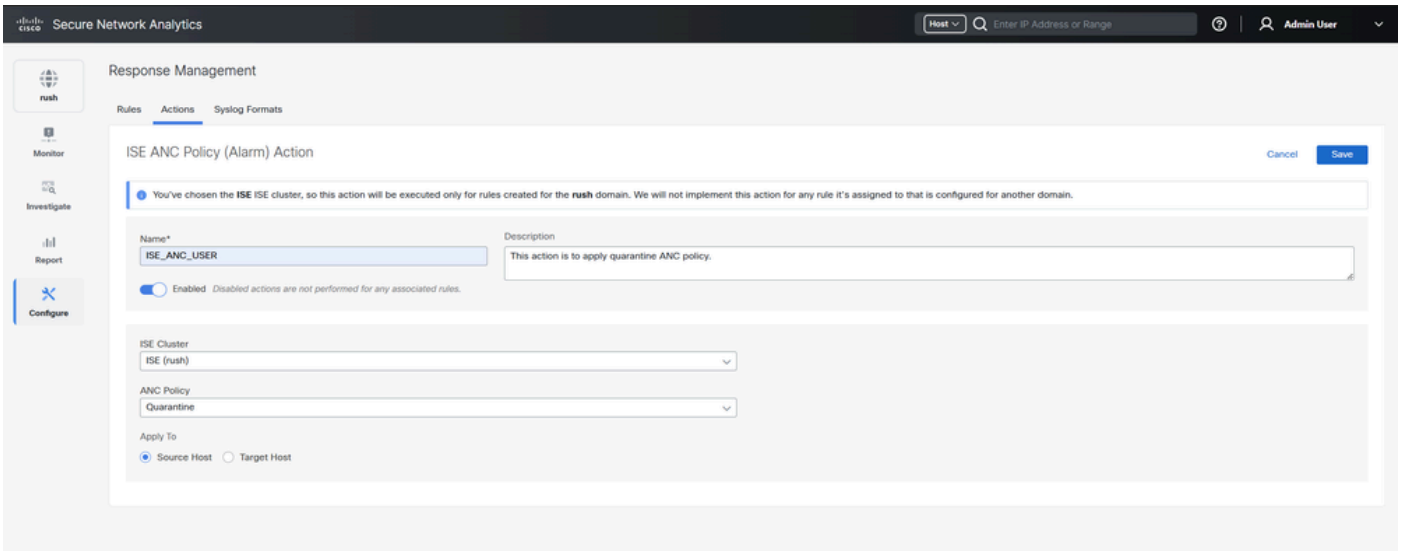
Cela signifie que lorsqu'un hôte de Mon réseau de confiance (groupe d'hôtes) communique avec un hôte autre que ceux de Mon DNS d'entreprise (groupe d'hôtes) via 53/up ou 53/tcp, une alarme est déclenchée.



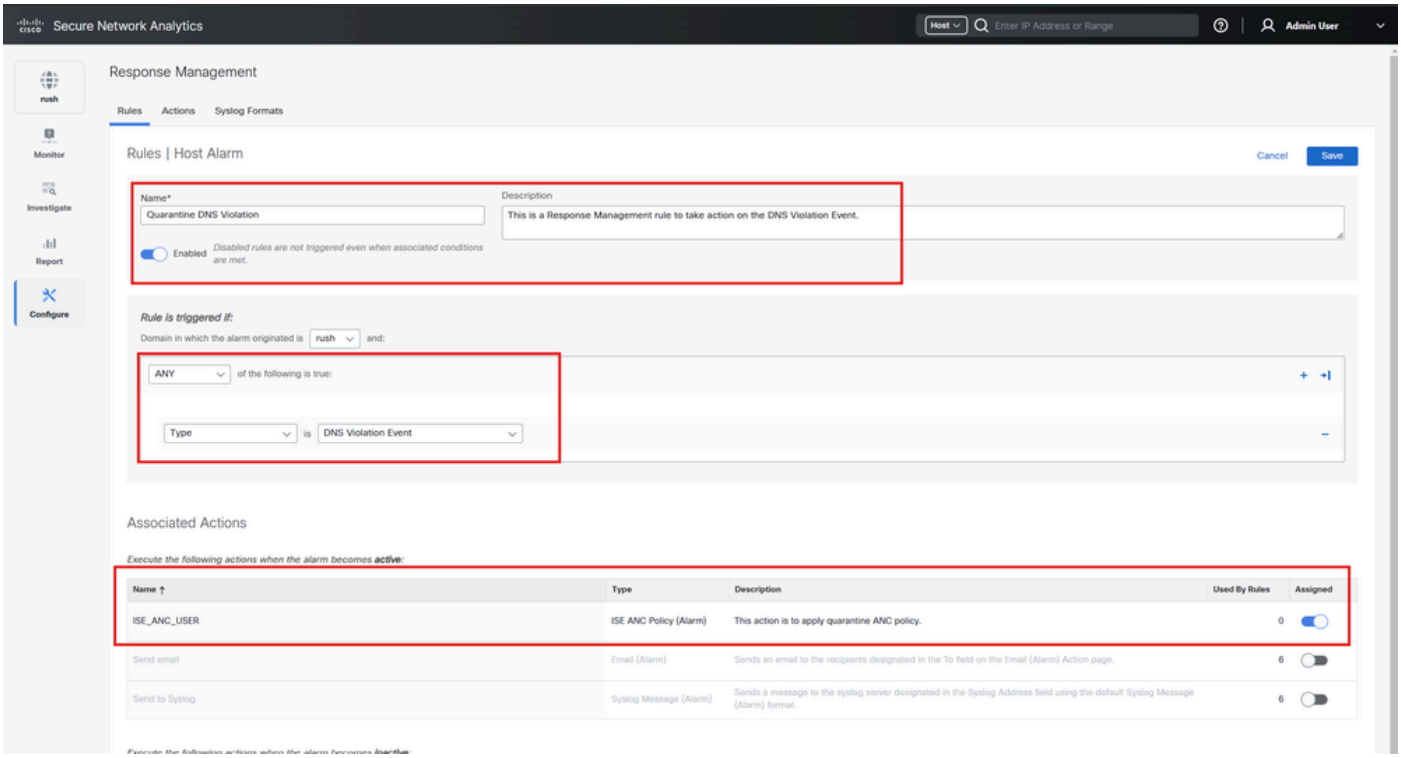
Étape 4 : Configurez une action de gestion des réponses à exécuter, qui pourra être appliquée ultérieurement à la règle de gestion des réponses une fois créée.

Accédez à Configure > Response Management > Actions, cliquez sur Add New Action et sélectionnez ISE ANC Policy (Alarm).

Attribuez un nom et choisissez le cluster Cisco ISE spécifique à notifier afin d'implémenter une stratégie de quarantaine pour toute violation ou connexion à des serveurs non autorisés.



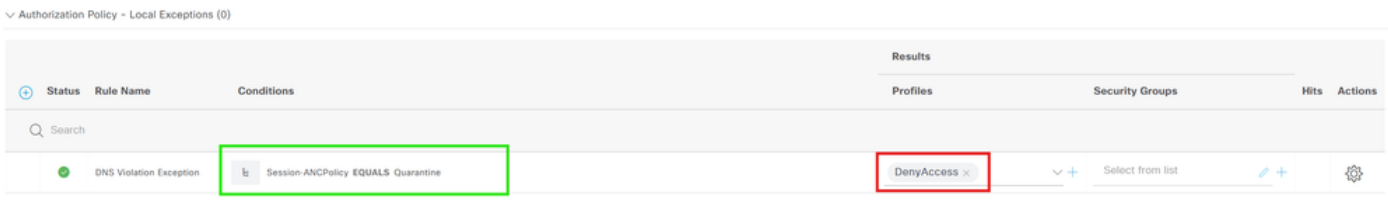
Étape 5 : Sous la section Règles, créez une nouvelle règle. Cette règle applique l'action précédemment définie chaque fois qu'un hôte du réseau interne tente d'envoyer du trafic DNS à des serveurs DNS non autorisés. Dans la section La règle est déclenchée si, choisissez Type et sélectionnez l'événement personnalisé créé précédemment.
Sous Associated Actions, sélectionnez l'action ISE ANC Alarm qui a été précédemment configurée.

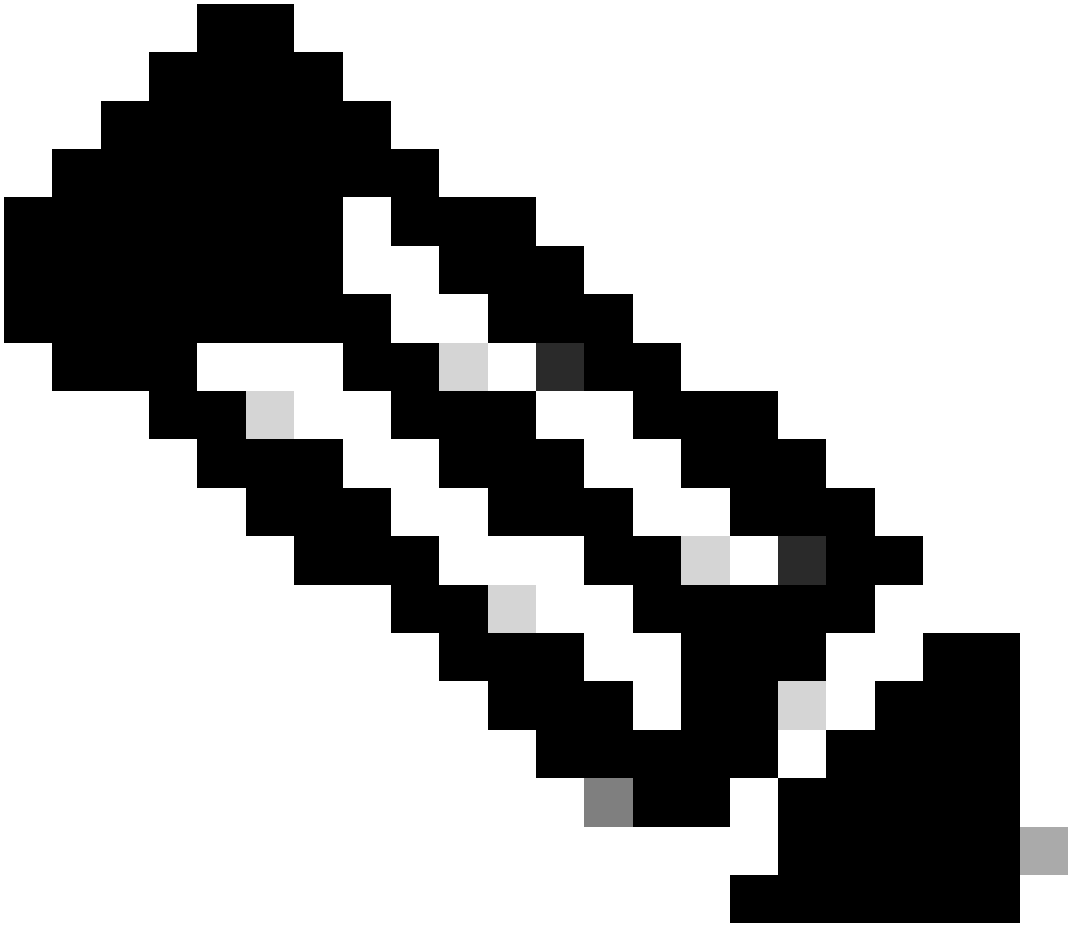


4. Configurez Cisco ISE pour répondre aux actions initiées par StealthWatch lors du déclenchement de l'événement.

Connectez-vous à l'interface utilisateur graphique de Cisco ISE et accédez à Policy > Policy Sets > Choisissez the Policy set > sous Authorization Policy - Local Exceptions > Create new Policy.

- Name : Exception de violation DNS
- Modalités: Session : Stratégie ANC ÉGALE Quarantaine
- Profils d'autorisation : RefuserAccès

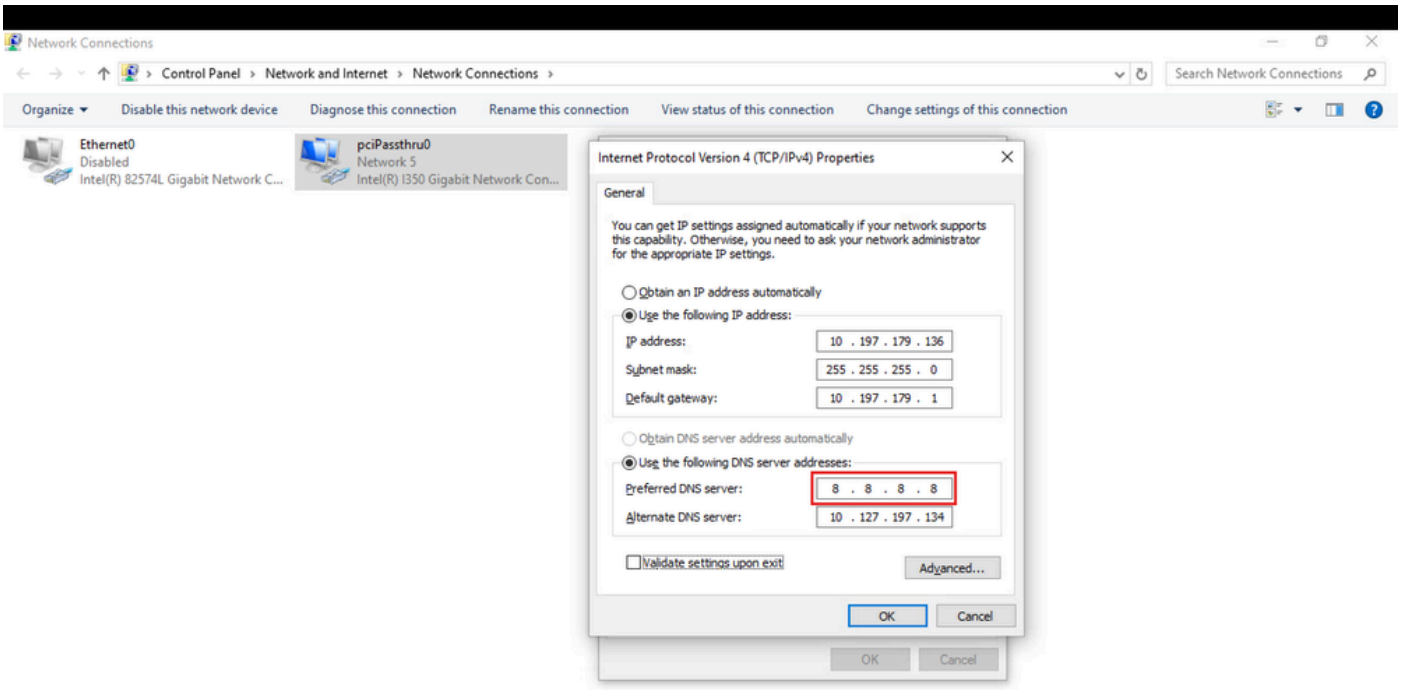




Remarque : Dans cet exemple, une fois l'événement de violation DNS déclenché, l'accès est refusé à l'utilisateur en fonction de la configuration

Vérifier

Pour illustrer l'exemple d'utilisation, l'entrée DNS sur le point d'extrémité a été remplacée par 8.8.8.8, ce qui déclenche l'événement de violation DNS configuré . Comme le serveur DNS n'appartient pas au groupe d'hôtes des serveurs DNS My Corporate, il déclenche l'événement qui entraîne un refus d'accès au point d'extrémité.



Sur le commutateur C9300, vérifiez à l'aide du cache show flow monitor IPv4_NETFLOW | dans la commande 8.8.8.8 avec le résultat pour voir les flux sont capturés et envoyés au collecteur de flux. IPv4_NETFLOW est configuré dans la configuration du commutateur.

<#root>

IPV4 SOURCE ADDRESS:

10.197.179.136

IPV4 DESTINATION ADDRESS:

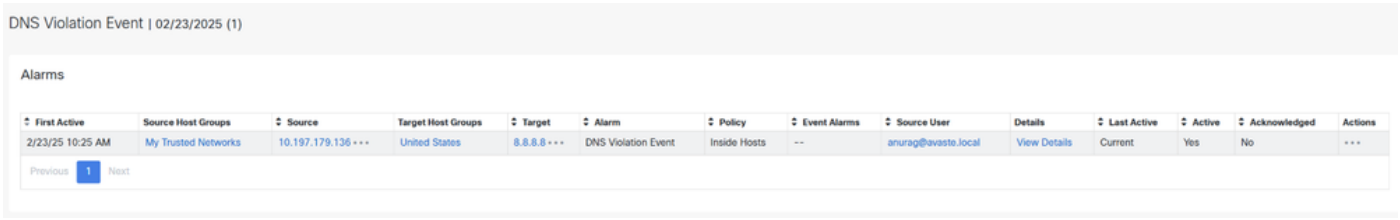
8.8.8.8

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

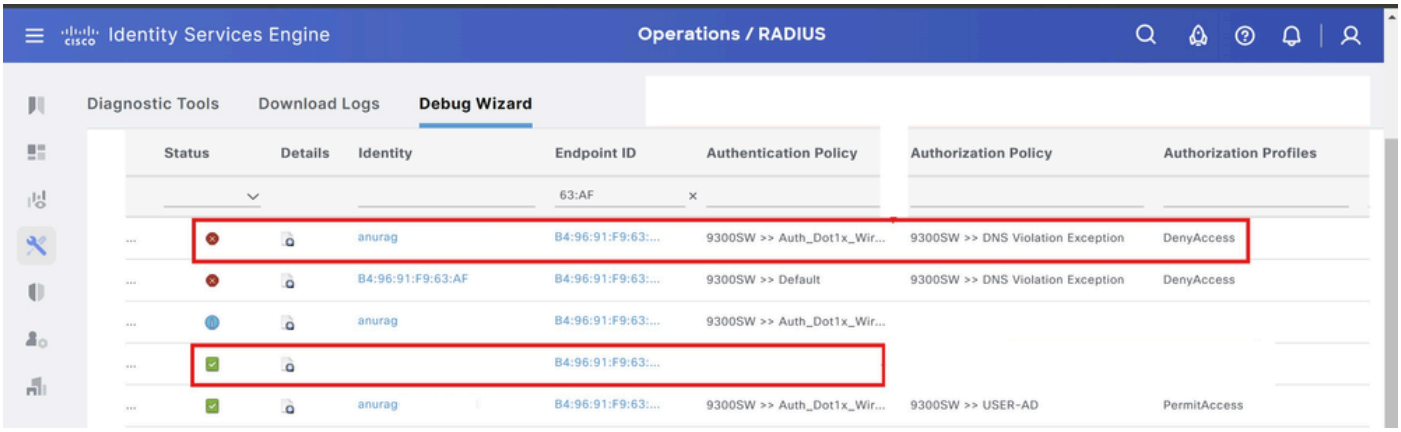
Une fois que l'événement est déclenché sur StealthWatch, naviguez vers Monitor > Security Insight Dashboard,.



Accédez à Monitor > Integration > ISE ANC Policy Assignments.

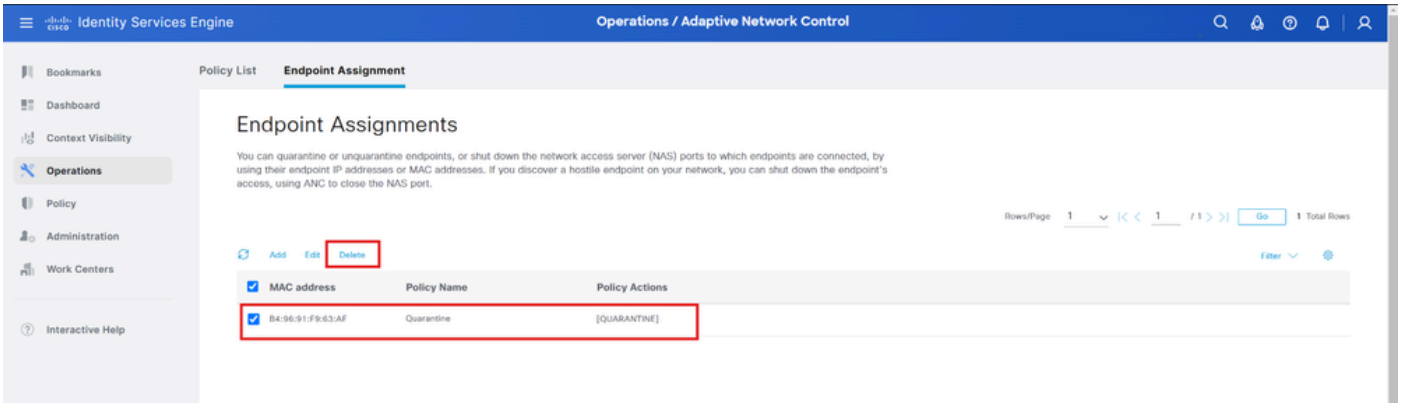
Assurez-vous que Cisco Secure Network Analytics a correctement mis en oeuvre la stratégie Adaptive Network Control Policy via PxGrid et Cisco ISE pour mettre l'hôte en quarantaine.

De même, sur Cisco ISE, accédez à Operations > RADIUS > Livelogs et appliquez un filtre pour le terminal.



Conformément à l'exception de violation DNS de la stratégie d'exception locale, le changement d'autorisation (CoA) est émis par ISE et l'accès ISE est refusé au point d'extrémité.

Une fois que les actions de correction sont effectuées sur le terminal, supprimez l'adresse MAC de Operations > Adaptive Network Control > Endpoint Assignments > Delete pour supprimer l'adresse MAC du terminal.



Log Reference sur Cisco ISE.

Les attributs définis sur le niveau TRACE pour le composant pxgrid (pxgrid-server.log) sur Cisco ISE, les journaux sont affichés dans le fichier 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

"}

Dépannage

Les terminaux mis en quarantaine ne renouvellent pas l'authentification après la modification de la stratégie

Problème

L'authentification a échoué en raison d'une modification de la stratégie ou d'une identité supplémentaire et aucune nouvelle authentification n'est en cours. L'authentification échoue ou le point d'extrémité en question ne parvient toujours pas à se connecter au réseau. Ce problème se produit souvent sur les ordinateurs clients qui échouent à l'évaluation de la position conformément à la stratégie de position qui est attribuée au rôle d'utilisateur.

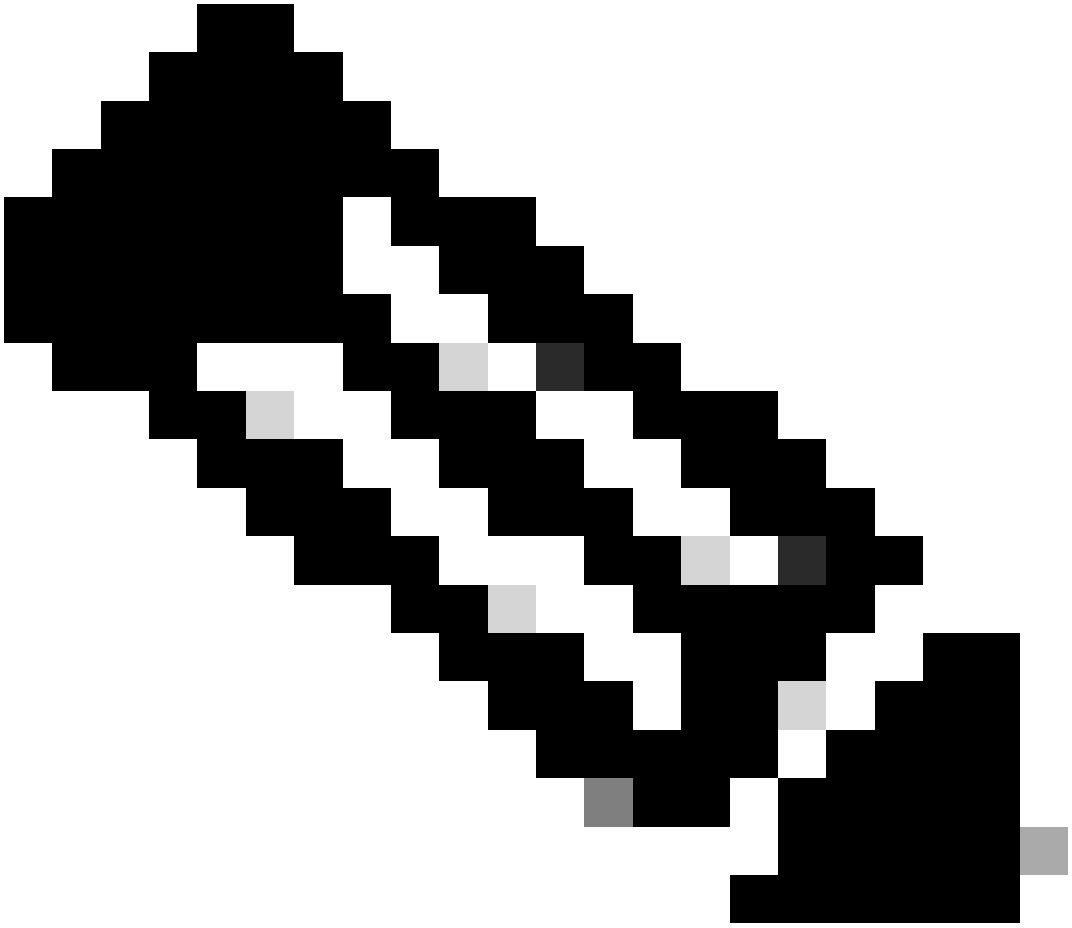
Causes possibles

Le paramètre du minuteur d'authentification n'est pas correctement défini sur l'ordinateur client ou l'intervalle d'authentification n'est pas correctement défini sur le commutateur.

Solution

Il existe plusieurs solutions possibles à ce problème :

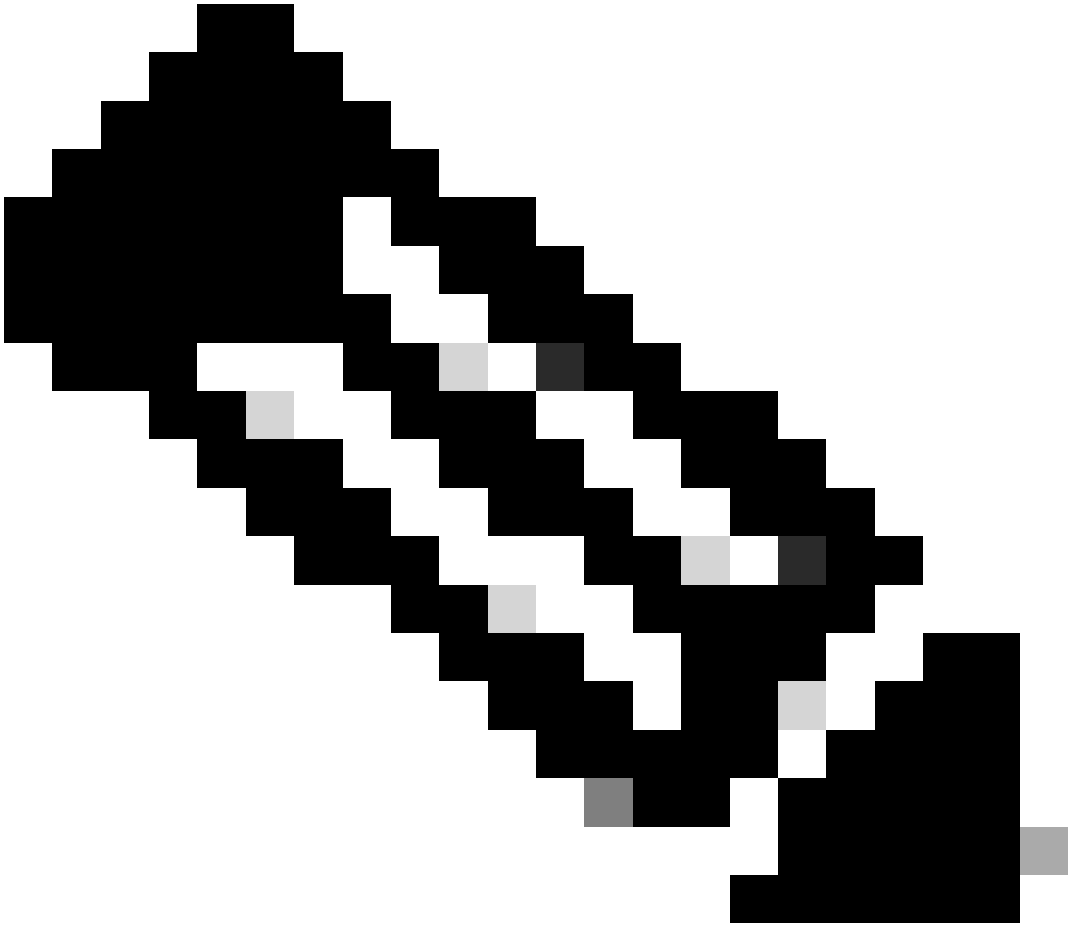
1. Vérifiez le rapport Session Status Summary dans Cisco ISE pour le NAD ou le commutateur spécifié, et assurez-vous que l'interface a l'intervalle d'authentification approprié configuré.
2. Entrez show running configuration sur le NAD/commutateur et assurez-vous que l'interface est configurée avec un paramètre de redémarrage du minuteur d'authentification approprié. (Par exemple, le minuteur d'authentification redémarre 15 et le minuteur d'authentification réauthentifie 15).
3. Entrez interface shutdown et no shutdown pour renvoyer le port sur le NAD/commutateur et forcer la ré-authentification et la modification potentielle de la configuration dans Cisco ISE.



Remarque : Étant donné que CoA nécessite une adresse MAC ou un ID de session, il est recommandé de ne pas renvoyer le port qui est affiché dans le rapport SNMP du périphérique réseau.

Les opérations ANC échouent lorsque l'adresse IP ou MAC est introuvable

Une opération ANC que vous effectuez sur un point de terminaison échoue lorsqu'une session active pour ce point de terminaison ne contient pas d'informations sur l'adresse IP. Cela s'applique également à l'adresse MAC et à l'ID de session de ce terminal.



Remarque : Lorsque vous souhaitez modifier l'état d'autorisation d'un terminal via ANC, vous devez fournir l'adresse IP ou l'adresse MAC du terminal. Si l'adresse IP ou l'adresse MAC est introuvable dans la session active du point d'extrémité, le message d'erreur suivant s'affiche : "Aucune session active trouvée pour cette adresse MAC, adresse IP ou ID de session".

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.