Konfigurieren von ANC auf ISE 3.3 und StealthWatch 7.5.1

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration von Rapid Threat Containment (Adaptive Network Control) auf Cisco ISE® Version 3.3 und StealthWatch beschrieben.

Voraussetzungen

Cisco empfiehlt Fachwissen in folgenden Bereichen:

- Identity Services Engine (ISE)
- Platform Exchange Grid (PxGrid)
- Sichere Netzwerkanalysen (StealthWatch)
- Schnelle Eindämmung von Bedrohungen (Adaptive Network Control - ANC).

In diesem Dokument wird davon ausgegangen, dass die Cisco Identity Services Engine mit Secure Network Analytics (StealthWatch) integriert ist und dabei das ANC-fähige pxGrid verwendet.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der folgenden Software und Versionen:

- Cisco Identity Services Engine (ISE) Version 3.3

- Secure Network Analytics (StealthWatch) 7.5.1
- Catalyst 9300

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

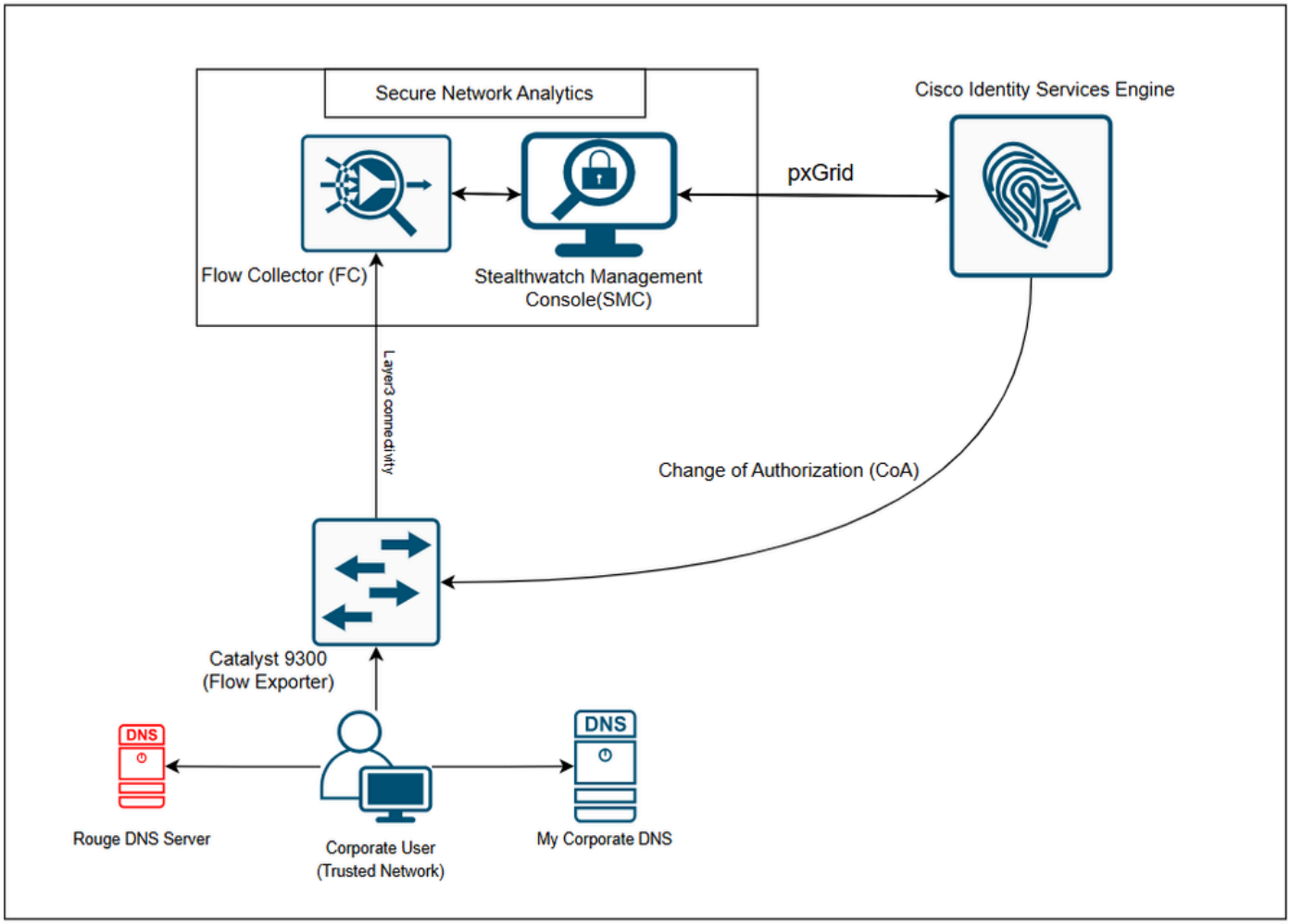
Cisco Secure Cloud Analytics (jetzt Teil von Cisco XDR) kann Benutzerzuordnungsdaten mithilfe von pxGrid von der Cisco Identity Services Engine (ISE) abrufen. Diese Integration ermöglicht das Erstellen von Berichten zu Benutzeraktivitäten in der Secure Cloud Analytics-Ereignisanzeige.

Die Kombination aus Secure Network Analytics (ehemals StealthWatch) und Cisco Identity Services Engine (ISE) bietet Unternehmen eine 360°-Ansicht, beschleunigt die Reaktion auf Bedrohungen und sichert ein wachsendes digitales Geschäft. Sobald Secure Network Analytics ungewöhnlichen Datenverkehr erkennt, gibt es eine Warnmeldung aus, sodass der Administrator den Benutzer in Quarantäne setzen kann. pxGrid ermöglicht Secure Network Analytics die direkte Übergabe des Quarantäne-Befehls an die Identity Services Engine.

In diesem Beispiel wird der Einsatz des DNS-Servers des Unternehmens zum Schutz vor Bedrohungen aus dem Internet beschrieben. Es soll ein benutzerdefinierter Warnmechanismus eingerichtet werden, der auslöst, wenn interne Benutzer eine Verbindung zu externen DNS-Servern herstellen. Ziel dieser Initiative ist es, Verbindungen zu nicht autorisierten DNS-Servern zu blockieren, die den Datenverkehr an schädliche externe Standorte umleiten könnten.

Wenn eine Warnung ausgelöst wird, stimmt sich Cisco Secure Network Analytics mit der Cisco ISE ab, um den Host, der auf nicht autorisierte DNS-Server zugreift, unter Verwendung einer Adaptive Network Control Policy über PxGrid unter Quarantäne zu stellen.

Netzwerkdiagramm



Wie im Diagramm gezeigt:

- Ein Benutzer des Unternehmens ist mit einem C9300-Switch verbunden, der so konfiguriert ist, dass er die IP-Datenflüsse exportiert und die Daten an den Flow Collector sendet.
- Derselbe Unternehmensbenutzer wird für den Benutzer von DNS-Servern des Unternehmens konfiguriert.
- Flow Collector ist in die StealthWatch Management Console (SMC) integriert
- StealthWatch Management Console (SMC) integriert über Pxgrid mit ISE.

Schrittweise Konfiguration

1. Bereiten Sie den Switch mithilfe von NetFlow auf die Überwachung und den Export von Datenflüssen vor.

Die grundlegende Flusskonfiguration auf einem C9300-Switch mit 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
```

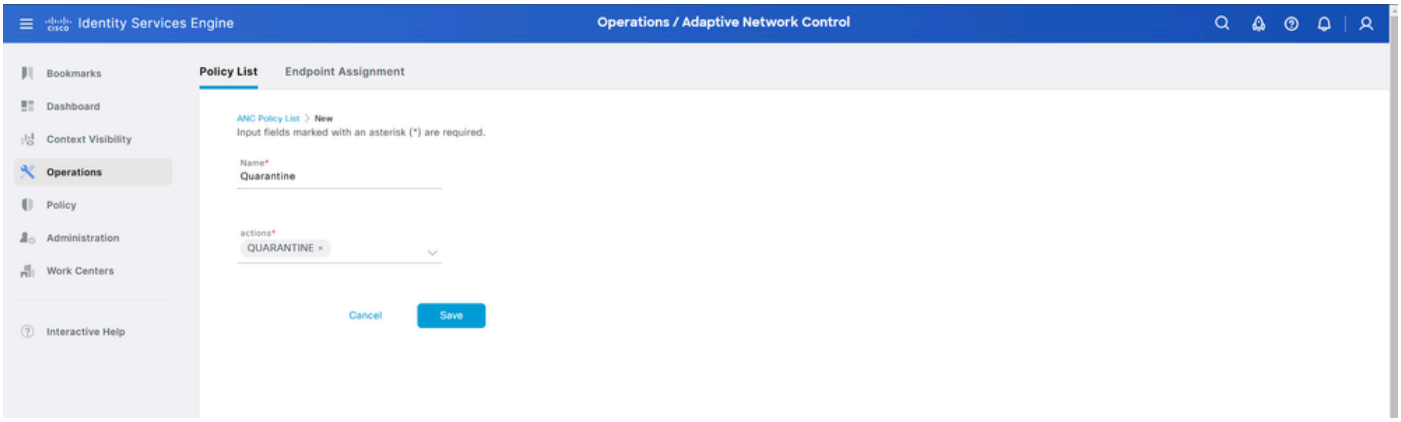
```
  match transport destination-port
  match interface input
  collect transport tcp flags
  collect interface output
  collect counter bytes long
  collect counter packets long
  collect timestamp absolute first
  collect timestamp absolute last


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
```

Nach Abschluss der Konfiguration kann der C9300 IP-Flussdaten in Flow Collector exportieren. Der Flow Collector verarbeitet und überträgt diese Daten dann zur Analyse und Überwachung an die StealthWatch Management Console (SMC).

2. Adaptive Netzwerksteuerung mit der Cisco ISE

ANC ist standardmäßig deaktiviert. ANC wird nur aktiviert, wenn pxGrid aktiviert ist, und es bleibt aktiviert, bis Sie den Dienst im Admin-Portal manuell deaktivieren.

Wählen Sie Operations > Adaptive Network Control > Policy List > Add aus, und geben Sie dann Quarantine für den Richtliniennamen und Quarantine für die Aktion ein.

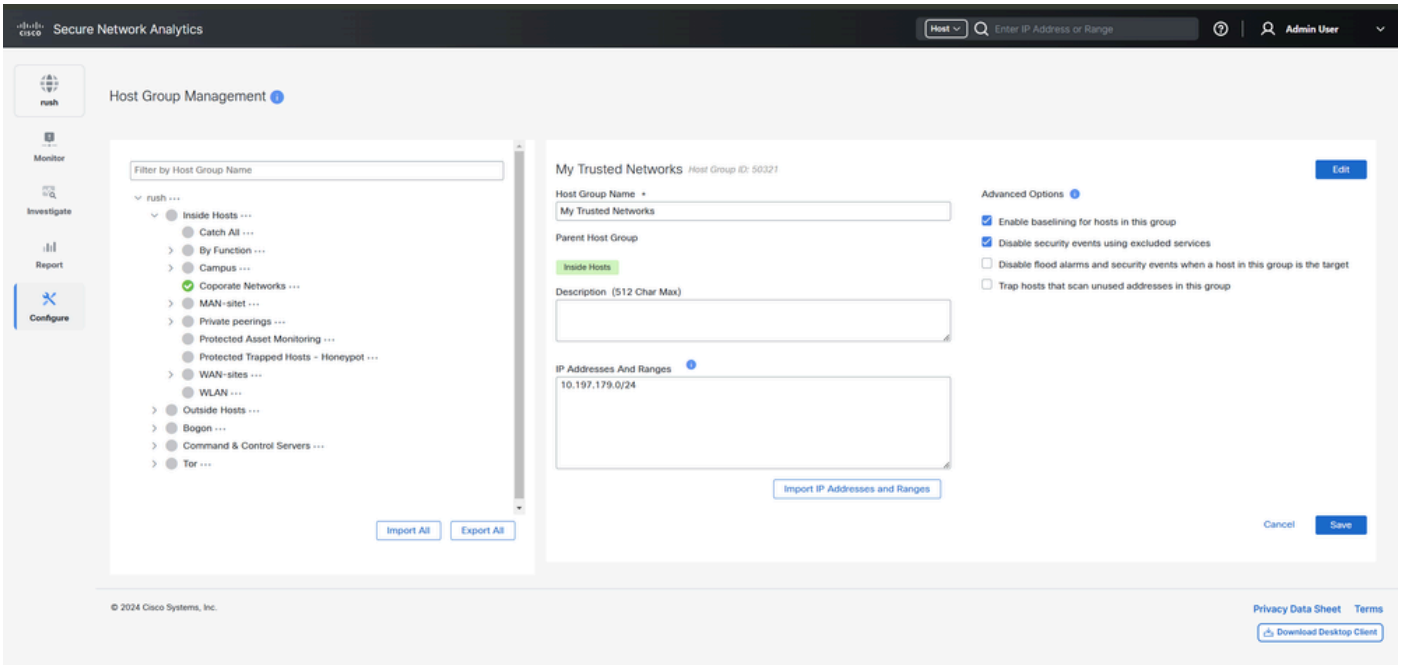


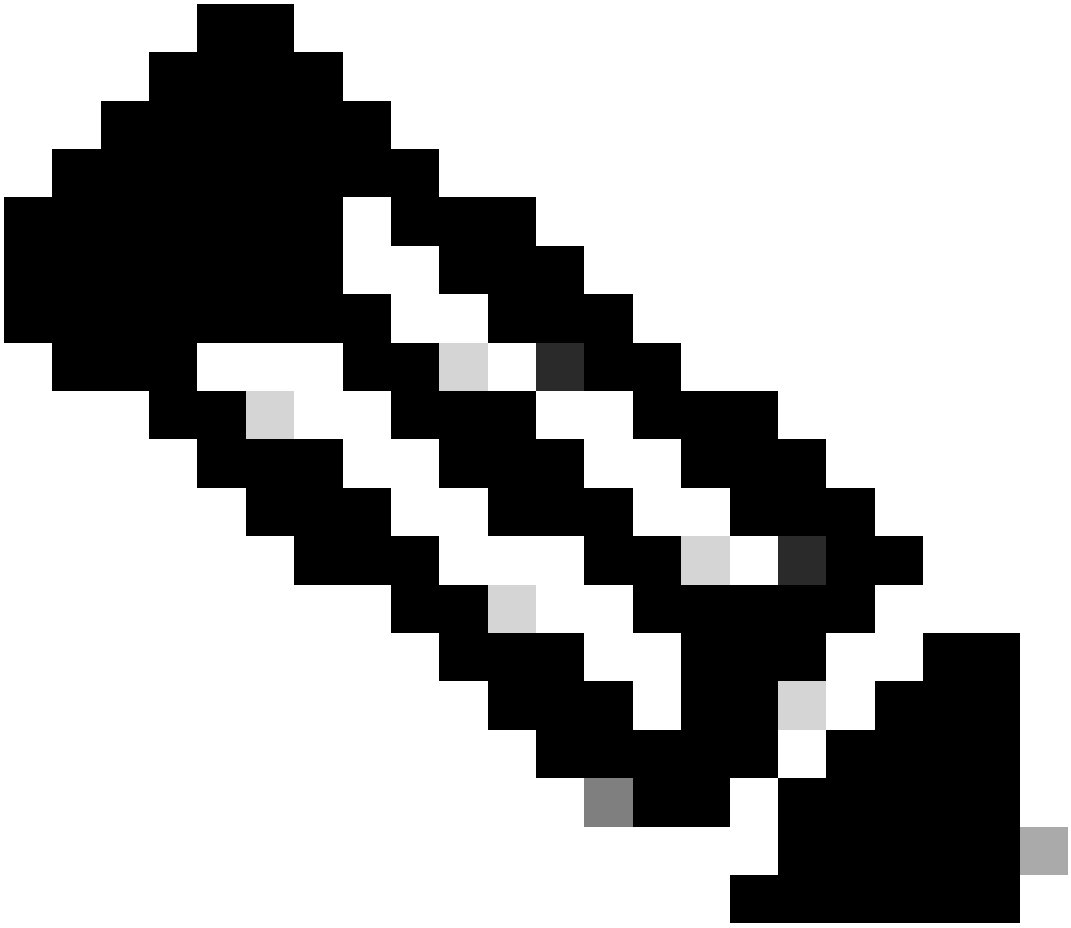
3. Konfigurieren Sie sichere Netzwerkanalysen für Ereignisauslöser und das Reaktionsmanagement, um Bedrohungen schnell einzudämmen.

Schritt 1: Melden Sie sich in der SMC-GUI an, und navigieren Sie zu Configure > Detection > Host Group Management > Klicken Sie auf das (...) (Auslassungszeichen) Symbol neben Inside Hosts, und wählen Sie Add Host Group.

In diesem Beispiel wird eine neue Hostgruppe mit dem Namen My Trusted Networks unter der übergeordneten Hostgruppe von Inside Hosts erstellt.

Dieses Netzwerk kann normalerweise dem Endbenutzercomputer zur Überwachung der DNS-Nutzung zugewiesen werden.

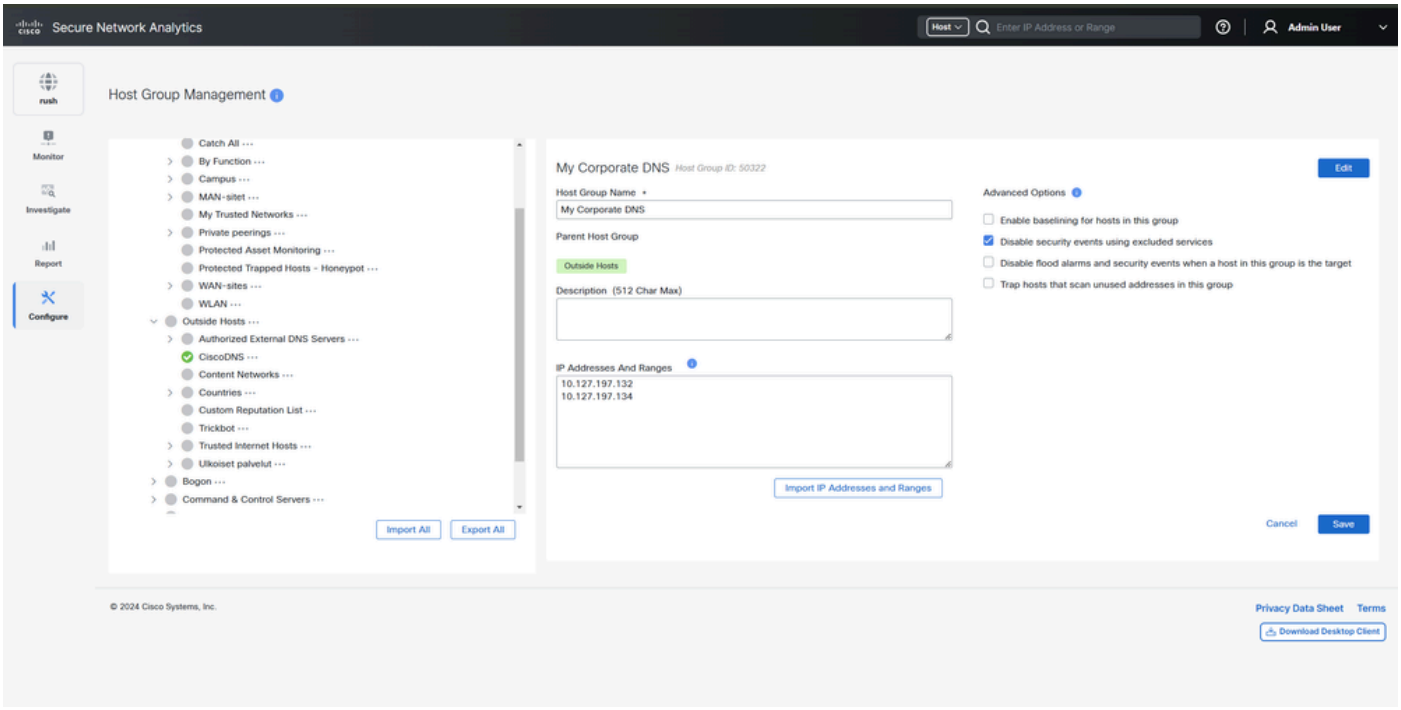


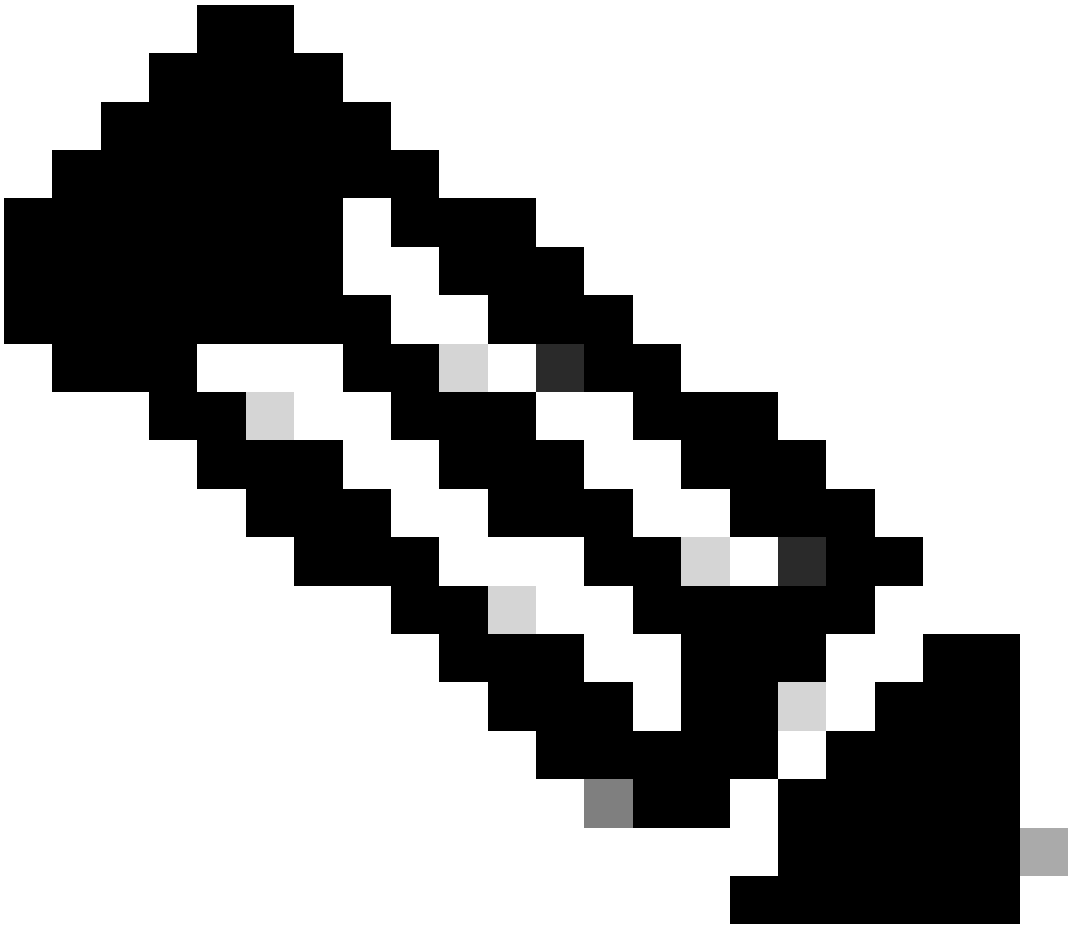


Anmerkung: In diesem Beispiel wird das IP-Subnetz 10.197.179.0/24 als LAN-Subnetz verwendet. Dies kann je nach Netzwerkarchitektur von der tatsächlichen Netzwerkumgebung abweichen.

Phase 2: Melden Sie sich in der SMC-GUI an, und navigieren Sie zu Configure > Detection > Host Group Management > Click on (...) side Outside Hosts, und wählen Sie Add Host Group.

In diesem Beispiel wird eine neue Hostgruppe mit dem Namen My Corporate DNS unter der übergeordneten Hostgruppe von Outside Hosts erstellt.

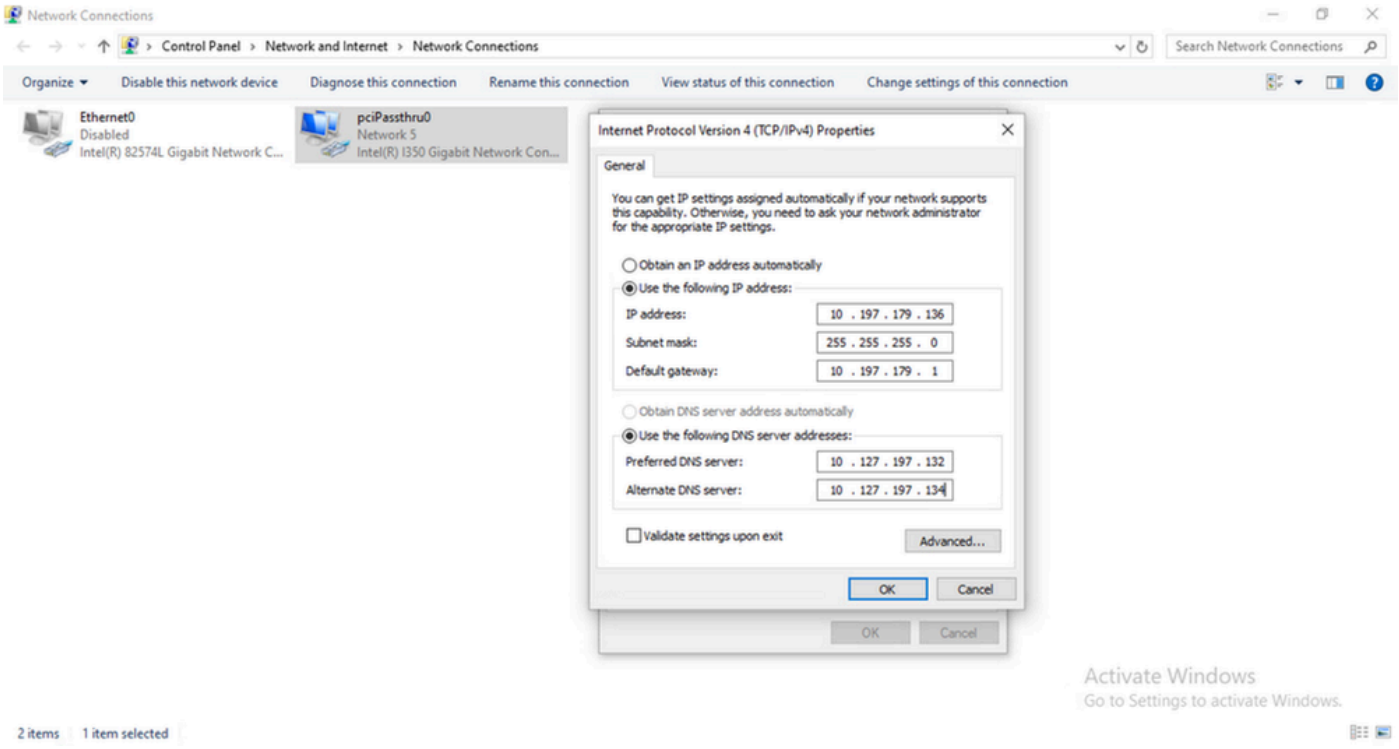




Anmerkung: Für dieses Beispiel werden die IPs 10.127.197.132 und 10.127.197.134 als

gewünschte, von den Endbenutzern zu verwendende DNS-Server verwendet. Dies kann sich in der tatsächlichen Netzwerkumgebung je nach Netzwerkarchitektur unterscheiden.

Der für die Demonstration verwendete Test Lab-PC ist mit der statischen IP-Adresse 10.197.179.136 (gehört zur erstellten Hostgruppe "Meine vertrauenswürdigen Netzwerke") und DNS 10.127.197.132 und 10.127.197.134 (gehört zur erstellten Hostgruppe "Mein firmeneigener DNS") konfiguriert.).



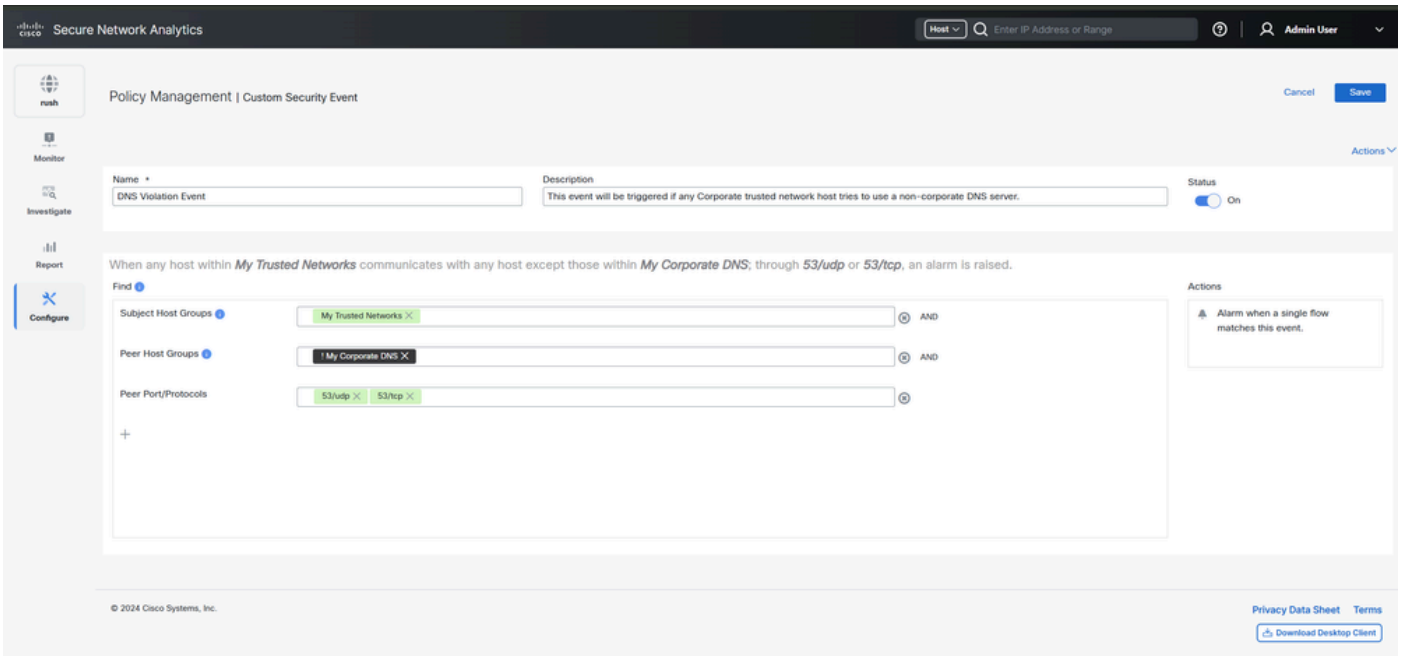
Schritt 3: Richten Sie ein maßgeschneidertes Warnsystem ein, um zu erkennen, wenn interne Benutzer eine Verbindung zu externen DNS-Servern herstellen. Dies löst einen Alarm aus, um Verbindungen zu nicht autorisierten DNS-Servern zu blockieren, die potenziell Datenverkehr an schädliche externe Websites weiterleiten könnten. Sobald ein Alarm aktiviert wurde, stimmt sich Cisco Secure Network Analytics mit der Cisco ISE ab, um den Host mithilfe dieser nicht autorisierten DNS-Server mithilfe einer Adaptive Network Control Policy über PxGrid zu isolieren.

Navigieren Sie zu Konfigurieren > Richtlinienverwaltung.

Erstellen Sie benutzerdefinierte Ereignisse mit den folgenden Informationen:

- Name: DNS-Verletzungsereignis.
- Betreff-Hostgruppen: Meine vertrauenswürdigen Netzwerke.
- Peer-Host-Gruppen: (Not) Mein Unternehmens-DNS.
- Peer-Port/Protokolle: 53/UDP 53/TCP

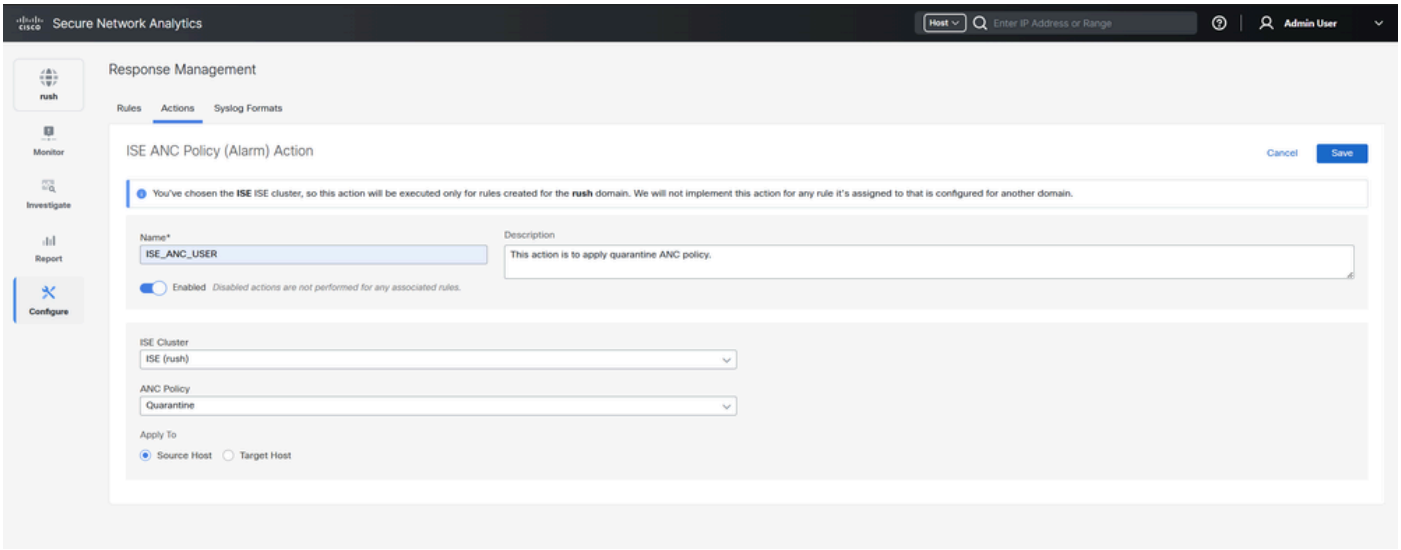
Das bedeutet, dass ein Alarm ausgelöst wird, wenn ein Host in My Trusted Networks (Hostgruppe) mit einem anderen Host als dem in My Corporate DNS (Hostgruppe) über 53/up oder 53/tcp kommuniziert.



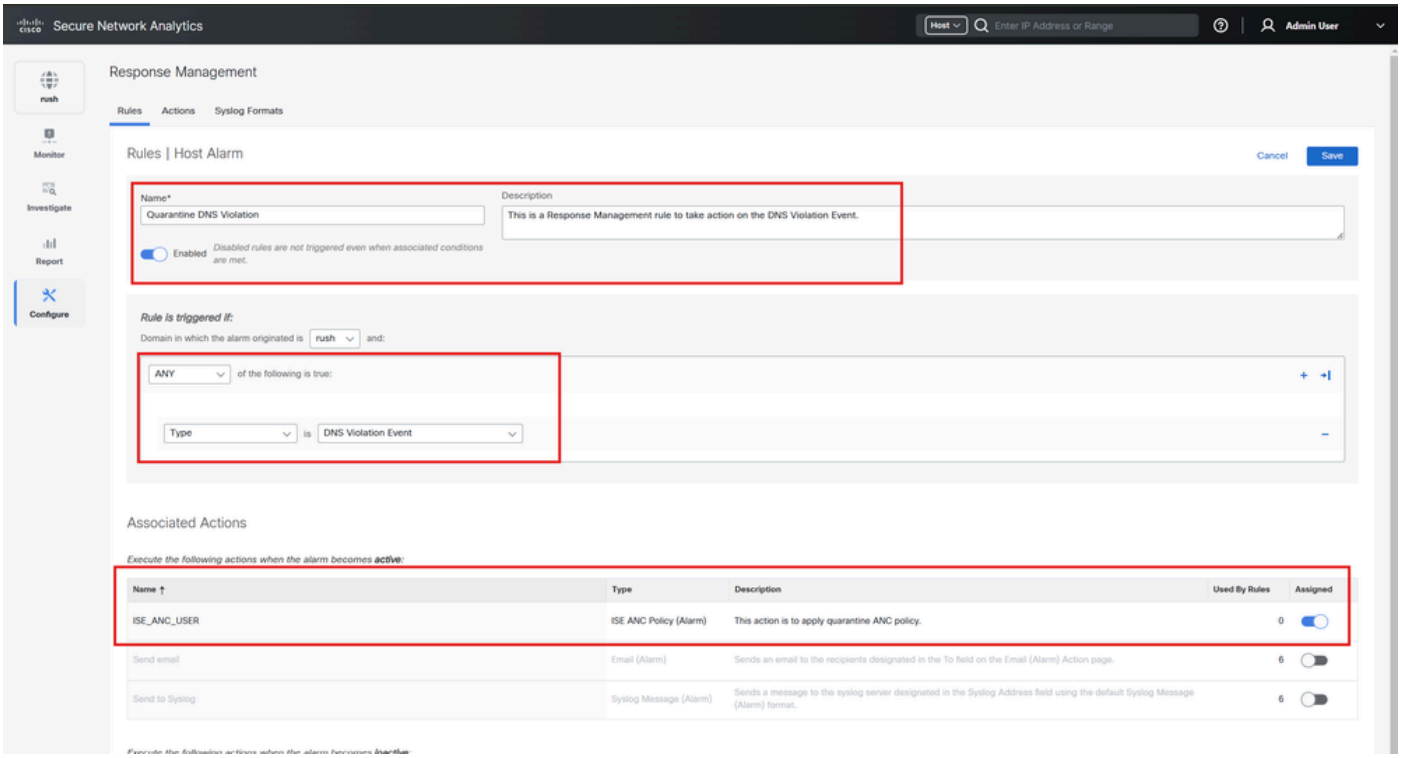
Schritt 4: Konfigurieren Sie eine auszuführende Aktion für die Antwortverwaltung, die später nach dem Erstellen auf die Antwortverwaltungsregel angewendet werden kann.

Navigieren Sie zu Configure > Response Management > Actions, klicken Sie auf Add New Action und wählen Sie ISE ANC Policy (Alarm) aus.

Weisen Sie einen Namen zu, und wählen Sie den entsprechenden Cisco ISE-Cluster aus, der benachrichtigt werden soll, um eine Quarantänerichtlinie für Verstöße oder Verbindungen mit nicht autorisierten Servern zu implementieren.



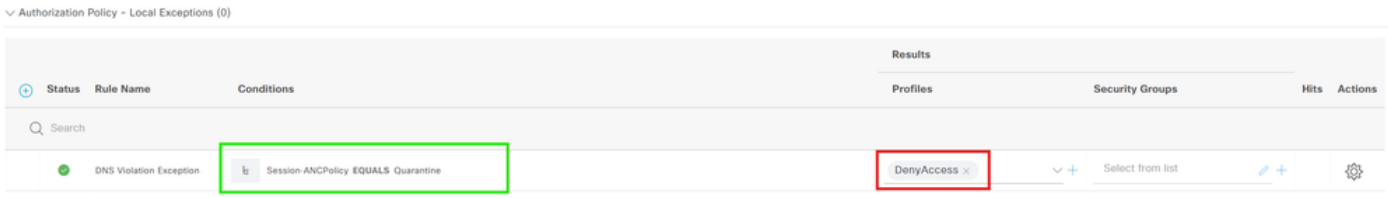
Schritt 5: Erstellen Sie im Abschnitt Regeln eine neue Regel. Diese Regel erzwingt die zuvor definierte Aktion jedes Mal, wenn ein Host innerhalb des internen Netzwerks versucht, DNS-Datenverkehr an nicht autorisierte DNS-Server zu senden. Wählen Sie im Abschnitt Regel wird ausgelöst, wenn die Option Typ und wählen Sie das zuvor erstellte benutzerdefinierte Ereignis aus.
Wählen Sie unter Associated Actions (Zugeordnete Aktionen) die zuvor konfigurierte ISE ANC Alarm-Aktion aus.

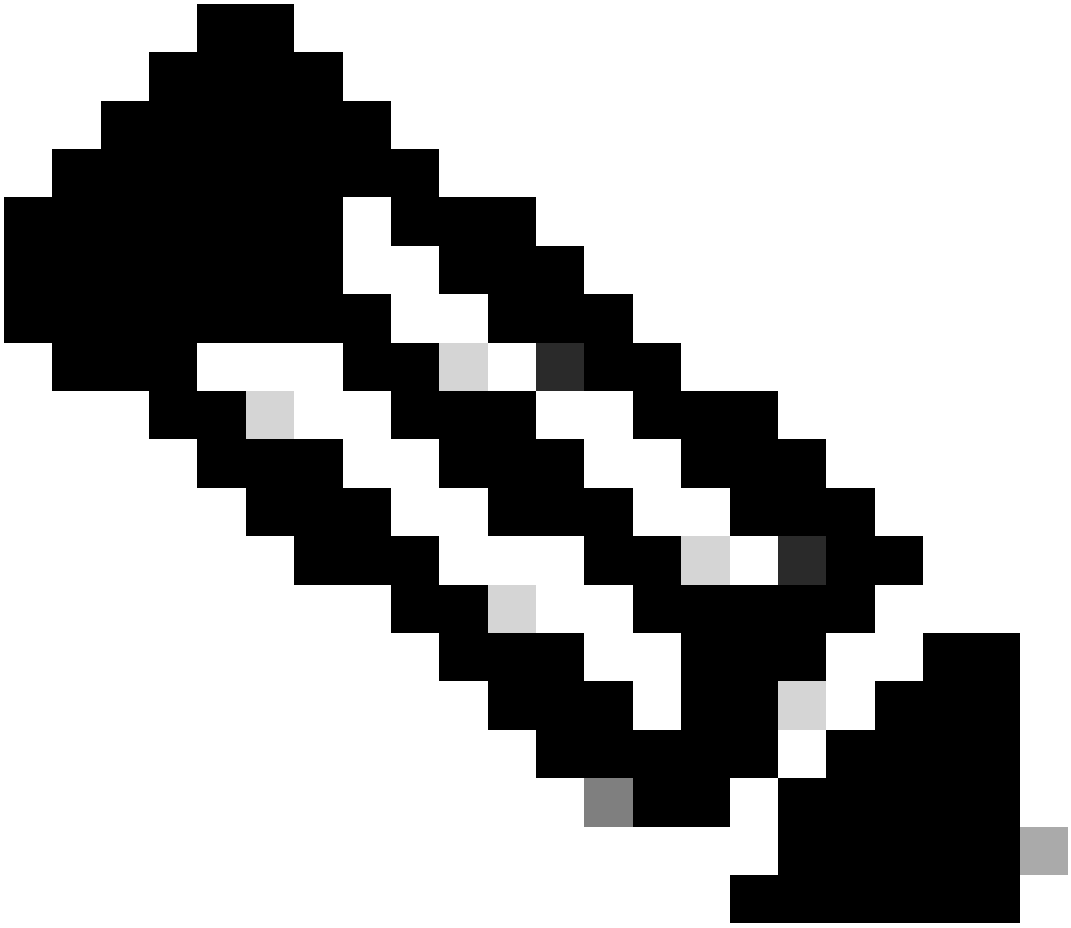


4. Konfigurieren Sie die Cisco ISE so, dass sie auf Aktionen reagiert, die von Stealthwatch beim Auslösen des Ereignisses initiiert wurden.

Melden Sie sich bei der Cisco ISE-GUI an, und navigieren Sie zu Policy > Policy Sets > Choose the Policy set > under Authorization Policy - Local Exceptions > Create New Policy (Richtlinie > Lokale Ausnahmen > Neue Richtlinie erstellen).

- Name: DNS-Verletzungsausnahme
- Bedingungen: Sitzung: ANCPolicy ENTSPRICHT Quarantäne
- Autorisierungsprofile: Zugriff verweigern

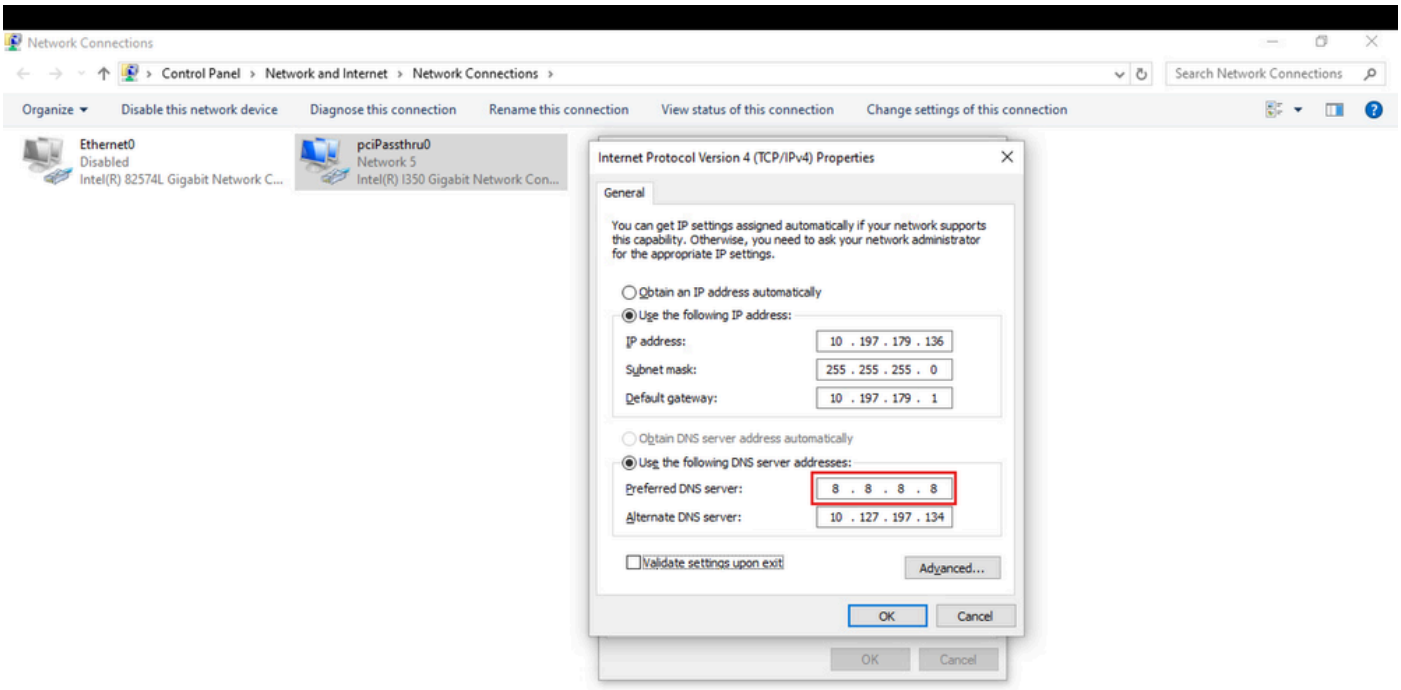




Anmerkung: Wenn in diesem Beispiel das DNS-Verletzungsereignis ausgelöst wurde, wird dem Benutzer der Zugriff auf Basis der Konfiguration verweigert.

Überprüfung

Um den Anwendungsfall zu veranschaulichen, wurde der DNS-Eintrag auf dem Endpunkt in 8.8.8.8 geändert, wodurch das konfigurierte DNS-Verletzungsereignis ausgelöst wird. Da der DNS-Server nicht zur Hostgruppe der DNS-Server in "Mein Unternehmen" gehört, löst er das Ereignis aus, das zu einer Ablehnung des Zugriffs auf den Endpunkt führt.



Überprüfen Sie auf dem C9300-Switch mithilfe des Caches show flow monitor IPv4_NETFLOW. | in 8.8.8.8 ein, um zu sehen, dass die Flows erfasst und an den Flow Collector gesendet werden. IPv4_NETFLOW wird in der Switch-Konfiguration konfiguriert.

<#root>

IPV4 SOURCE ADDRESS:

10.197.179.136

IPV4 DESTINATION ADDRESS:

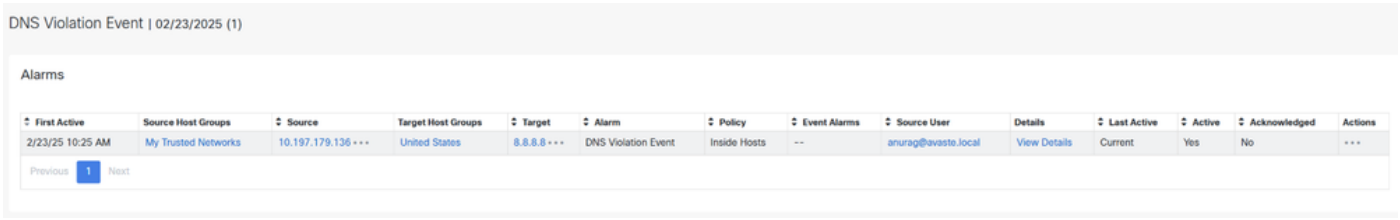
8.8.8.8

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

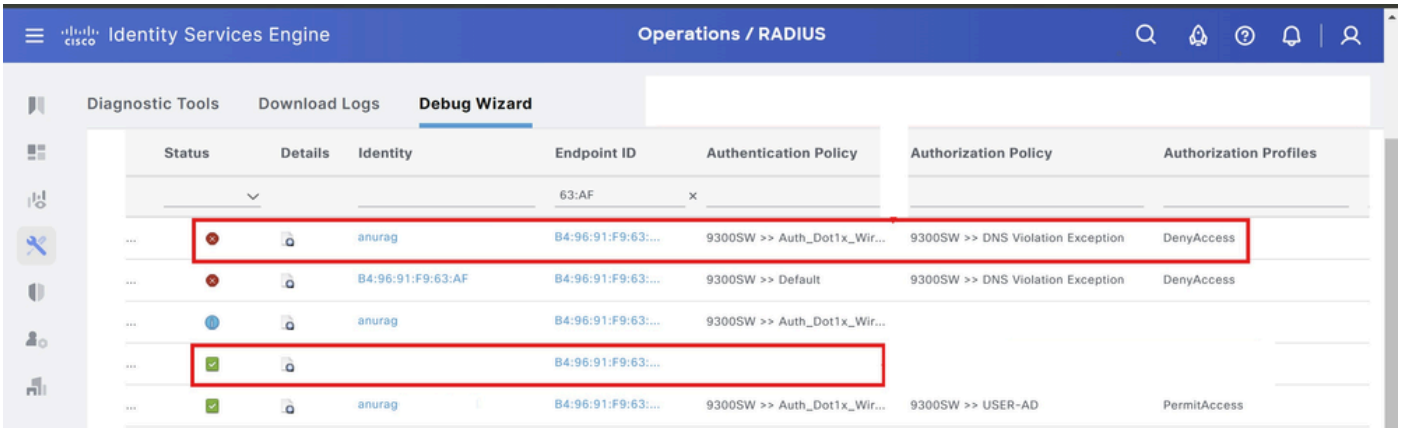
Sobald das Ereignis in StealthWatch ausgelöst wurde, navigieren Sie zu Überwachen > Security Insight Dashboard.



Navigieren Sie zu Monitor > Integration > ISE ANC Policy Assignments.

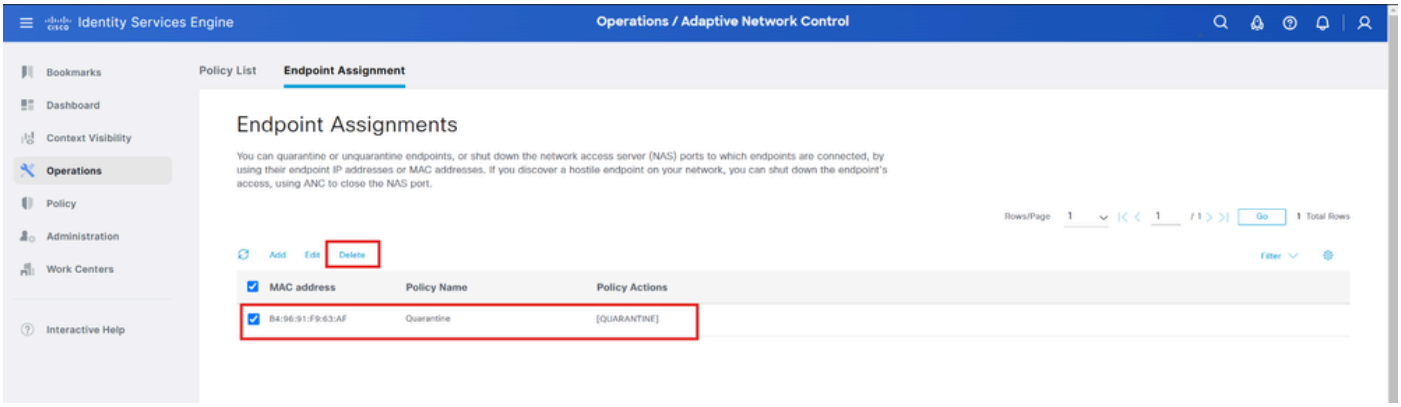
Sicherstellen, dass Cisco Secure Network Analytics die Adaptive Network Control Policy über PxGrid und Cisco ISE erfolgreich implementiert hat, um den Host unter Quarantäne zu stellen

Navigieren Sie auf der Cisco ISE ähnlich zu Operations > RADIUS > Livelogs (Betrieb > RADIUS > Protokolle), und wenden Sie Filter auf das Endgerät an.



Gemäß der lokalen Ausnahmerichtlinie "DNS Violation Exception" (DNS-Verletzungsausnahme) wird die Autorisierungsänderung (Change of Authorization, CoA) von der ISE ausgegeben, und der Zugriff auf die ISE wird dem Endpunkt verweigert.

Sobald die Korrekturmaßnahmen am Endpunkt durchgeführt wurden, entfernen Sie die MAC aus Operations > Adaptive Network Control > Endpoint Assignments > Delete (Betrieb > Adaptive Netzwerksteuerung > Endpunktzuweisungen > Löschen), um die MAC-Adresse des Endpunkts zu entfernen.



Protokollreferenz auf der Cisco ISE.

Attribute, die für die pxgrid-Komponente (pxgrid-server.log) auf der Cisco ISE auf die TRACE-Ebene festgelegt wurden, werden in der Datei pxgrid-server.log angezeigt.

<#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

"}

Fehlerbehebung

Endgeräte in Quarantäne verlängern Authentifizierungs-Postrichtlinienänderung nicht

Problem

Fehler bei der Authentifizierung aufgrund einer Änderung der Richtlinie oder einer zusätzlichen Identität. Es findet keine erneute Authentifizierung statt. Die Authentifizierung schlägt fehl, oder der betreffende Endpunkt kann keine Verbindung zum Netzwerk herstellen. Dieses Problem tritt häufig auf Client-Computern auf, die die Statusüberprüfung gemäß der Statusrichtlinie, die der Benutzerrolle zugewiesen ist, nicht durchführen.

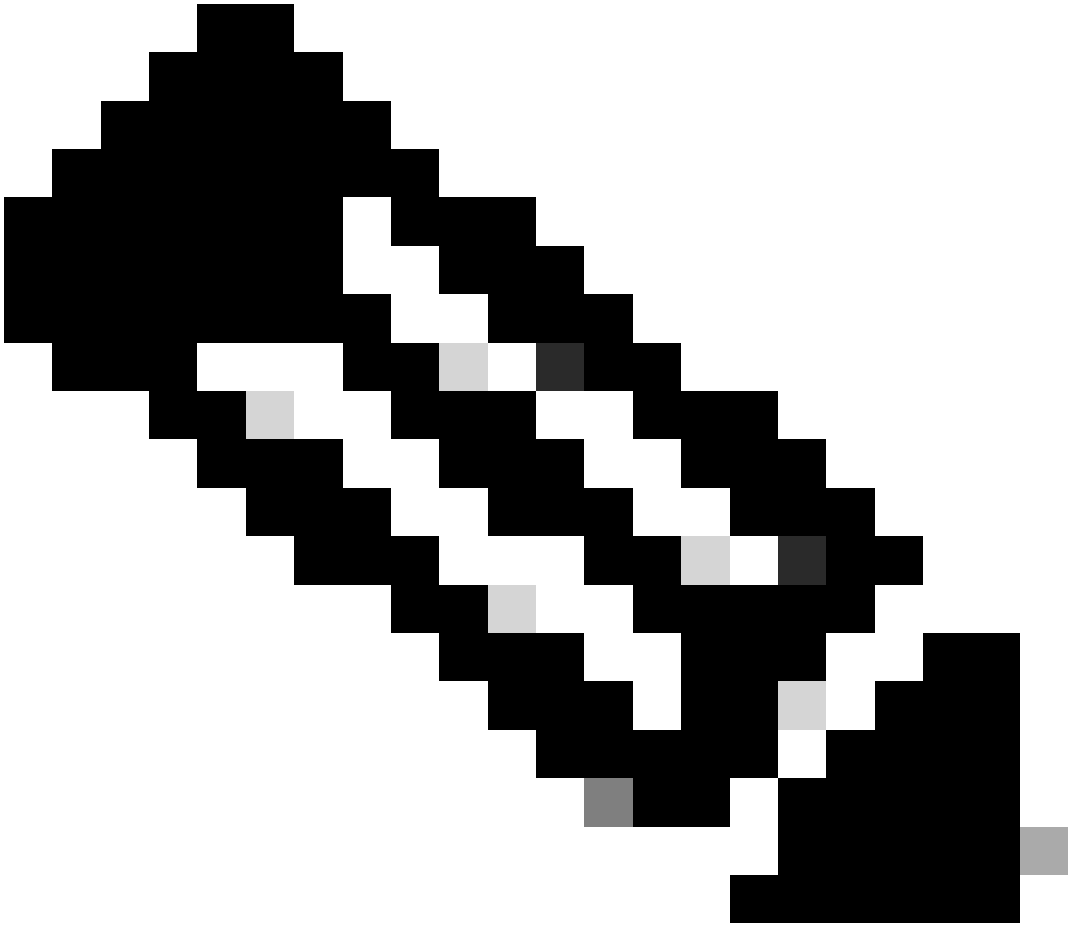
Mögliche Ursachen

Die Einstellung für den Authentifizierungs-Timer ist auf dem Client-Computer oder das Authentifizierungsintervall auf dem Switch nicht richtig festgelegt.

Lösung

Es gibt mehrere mögliche Lösungen für dieses Problem:

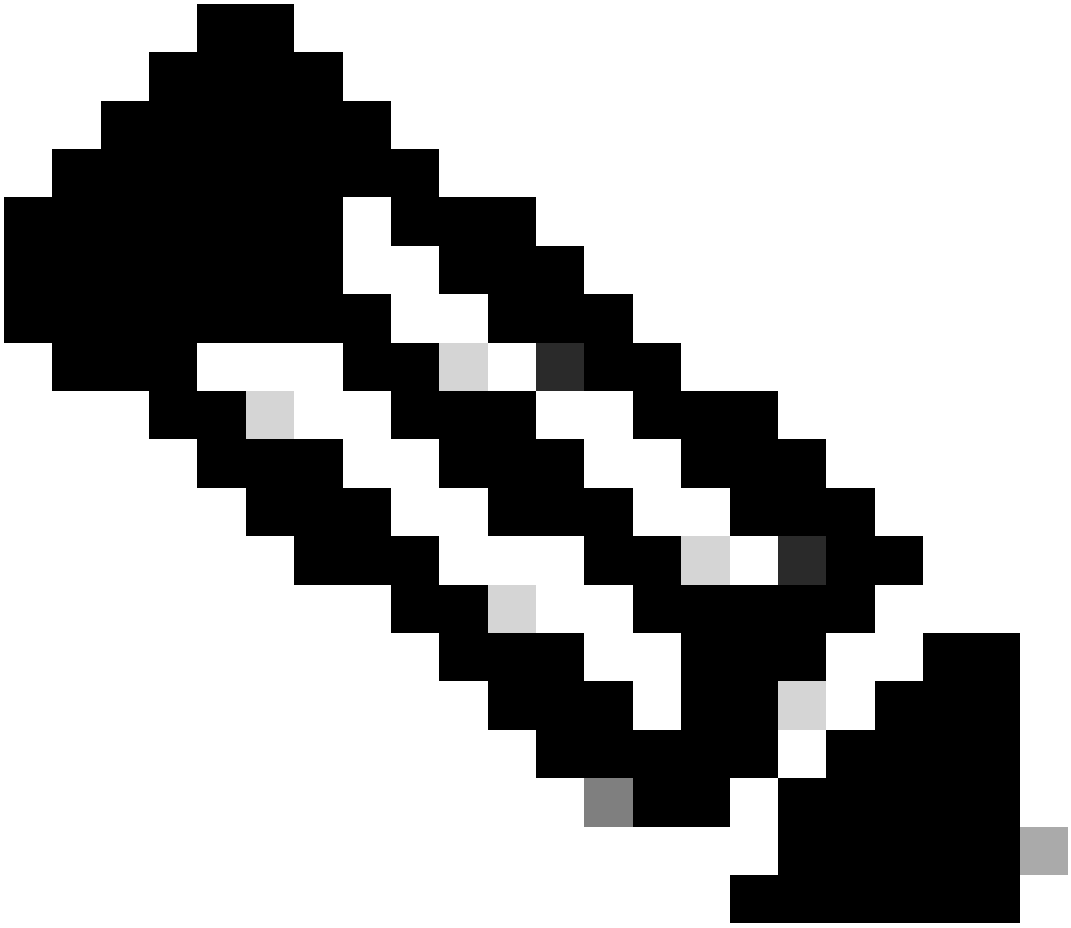
1. Überprüfen Sie den Sitzungsstatus-Zusammenfassungsbericht in der Cisco ISE für die angegebene NAD oder den angegebenen Switch, und stellen Sie sicher, dass für die Schnittstelle das entsprechende Authentifizierungsintervall konfiguriert ist.
2. Geben Sie show running configuration auf dem NAD/Switch ein, und stellen Sie sicher, dass die Schnittstelle mit einer entsprechenden Einstellung für den Neustart des Authentifizierungs-Timers konfiguriert ist. (Beispiel: Authentifizierungs-Timer restart 15 und Authentifizierungs-Timer reauthentifizieren 15).
3. Geben Sie interface shutdown und no shutdown ein, um den Port auf dem NAD/Switch zurückzusetzen und eine erneute Authentifizierung und potenzielle Konfigurationsänderung in der Cisco ISE zu erzwingen.



Anmerkung: Da für CoA eine MAC-Adresse oder eine Sitzungs-ID erforderlich ist, wird empfohlen, den im SNMP-Bericht für Netzwerkgeräte angezeigten Port nicht per Bounce zurückzusetzen.

ANC-Vorgänge schlagen fehl, wenn keine IP- oder MAC-Adresse gefunden wird

Eine ANC-Operation, die Sie an einem Endpunkt ausführen, schlägt fehl, wenn eine aktive Sitzung für diesen Endpunkt keine Informationen über die IP-Adresse enthält. Dies gilt auch für die MAC-Adresse und die Sitzungs-ID für den Endpunkt.



Anmerkung: Wenn Sie den Autorisierungsstatus eines Endpunkts über ANC ändern möchten, müssen Sie die IP- oder MAC-Adresse für den Endpunkt angeben. Wenn die IP- oder MAC-Adresse in der aktiven Sitzung für den Endpunkt nicht gefunden wird, wird die folgende Fehlermeldung angezeigt: "Keine aktive Sitzung für diese MAC-Adresse, IP-Adresse oder Sitzungs-ID gefunden".

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.