Configure ANC on ISE 3.3 and Stealthwatch 7.5.1

Contents

Introduction

Prerequisites

Components Used

Background Information

Network Diagram

Step-by-Step Configuration

Verify

Troubleshooting

Quarantined Endpoints do not Renew Authentication Post-policy Change

Problem

Possible Causes

Solution

ANCOperations Fail when IP Address or MAC Address is not Found

Introduction

This document describes Configuration of Rapid Threat Containment (Adaptive Network Control) on Cisco ISE® version 3.3 and Stealthwatch.

Prerequisites

Cisco recommends knowledge in these topics:

- Identity Services Engine (ISE)
- Platform Exchange Grid (PxGrid)
- Secure Network Analytics (Stealthwatch)
- Rapid Threat Containment (Adaptive Network Control - ANC).

In this document it is assumed that the Cisco Identity Services Engine is integrated with Secure Network Analytics (Stealthwatch) using pxGrid that is ANC-enabled.

Components Used

The information in this document is based on these software and versions:

- 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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

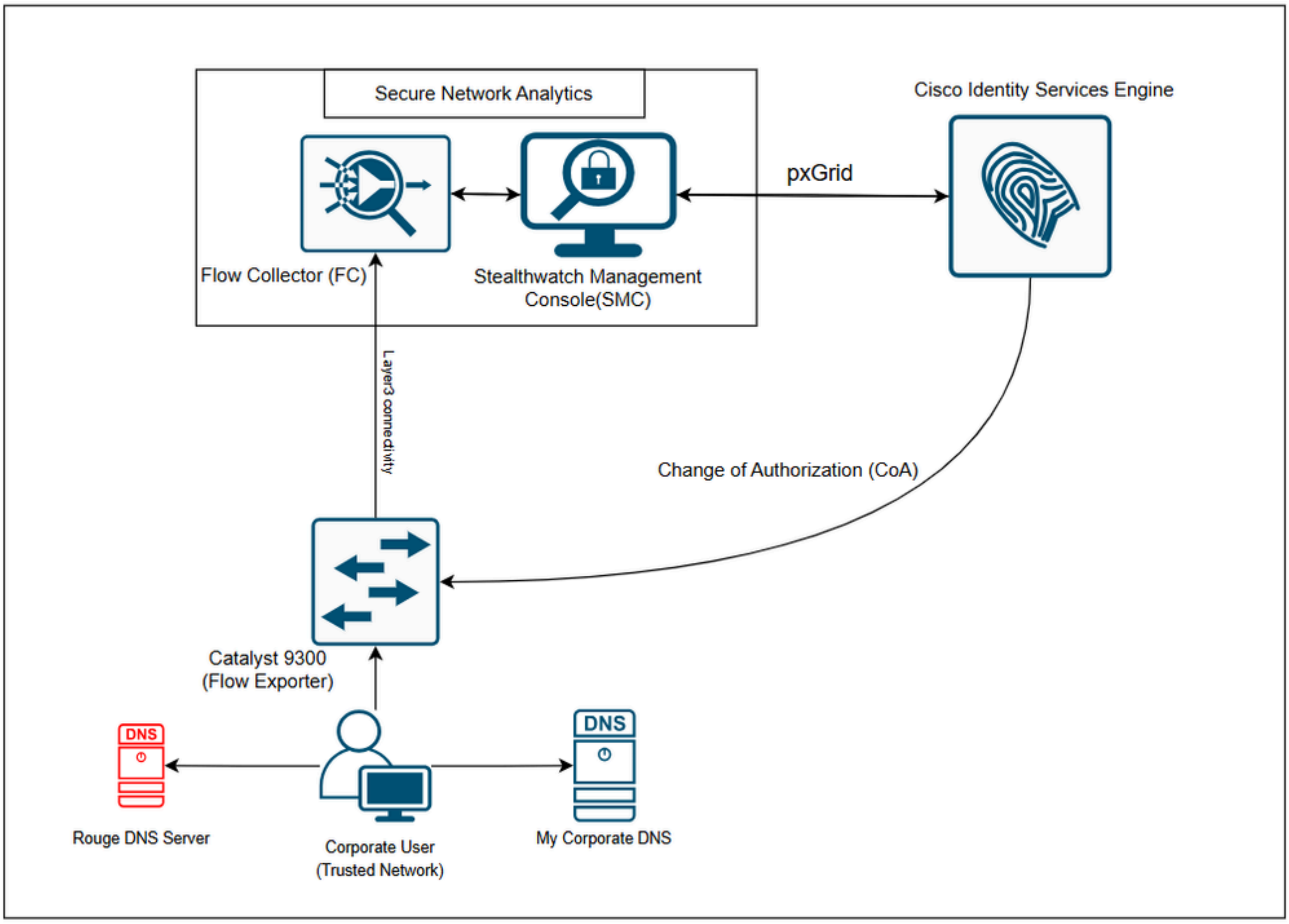
Cisco Secure Cloud Analytics (now part of Cisco XDR) can retrieve user attribution data from Cisco Identity Services Engine (ISE) using pxGrid. This integration enables user activity reporting in the Secure Cloud Analytics Event Viewer.

The combination of Secure Network Analytics (formerly Stealthwatch) and Cisco Identity Services Engine (ISE) helps organizations get a 360° view, respond to threats faster, and secure a growing digital business. Once Secure Network Analytics detects anomalous traffic, it issues an alert, giving the admin the option to quarantine the user. pxGrid enables Secure Network Analytics to hand off the quarantine command directly to Identity Services Engine.

This example describes leveraging Corporate DNS server to protect against Internet threats. The intention is to establish a customized alert mechanism that triggers when internal users connect to external DNS servers. This initiative is designed to block connections to unauthorized DNS servers that could redirect traffic to harmful external sites.

When an alert is triggered, Cisco Secure Network Analytics coordinates with Cisco ISE to quarantine the host accessing unauthorized DNS servers, using an Adaptive Network Control Policy via PxGrid.

Network Diagram


Secure Network Analytics
Cisco Identity Services Engine
pxGrid
Flow Collector (FC)
Stealthwatch Management Console(SMC)
Layer3 connectivity
Change of Authorization (CoA)
Catalyst 9300 (Flow Exporter)
DNS
Rouge DNS Server
Corporate User (Trusted Network)
DNS
My Corporate DNS

As shown in the diagram:

- A corporate user is connected to a C9300 switch which is configured to export the IP flows and send the data to the Flow collector.
- Same corporate user is configured to user corporate DNS servers.
- Flow Collector is integrated with Stealthwatch Management Console (SMC)
- Stealthwatch Management Console (SMC) integrated via Pxgrid with ISE.

Step-by-Step Configuration

1. Prepare the switch to monitor and export flows using netflow.

The basic flow configuration on a C9300 switch running Cisco IOS® XE 17.15.01

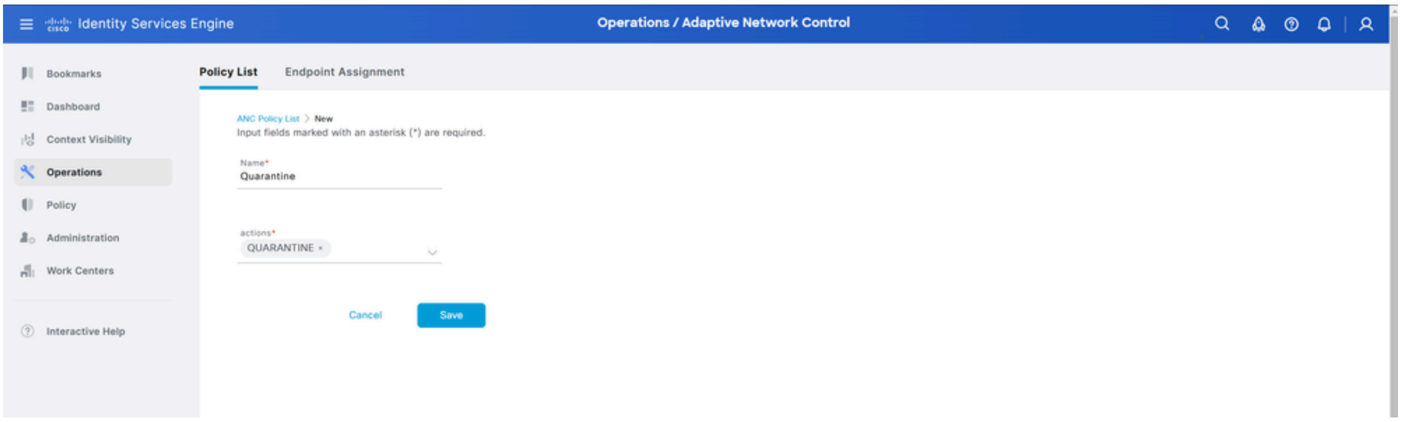
```
flow record SW_FLOW_RECORD
  description NetFlow record format to send to SW
  match ipv4 tos
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  match interface input
  collect transport tcp flags
  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
```

Upon completing the configuration, it enables the C9300 to export IP flow data to the Flow Collector. The Flow Collector then processes and transfers this data to the Stealthwatch Management Console (SMC) for analysis and monitoring.

2. EnableAdaptive Network Controlin Cisco ISE.

ANC is disabled by default. ANC gets enabled only when pxGrid is enabled, and it remains enabled until you manually disable the service in the Admin portal.

Select **Operations > Adaptive Network Control > Policy List > Add**, then enter **Quarantine for the Policy Name** and **Quarantine for the Action.**



Input fields marked with an asterisk (*) are required.

Name* Quarantine

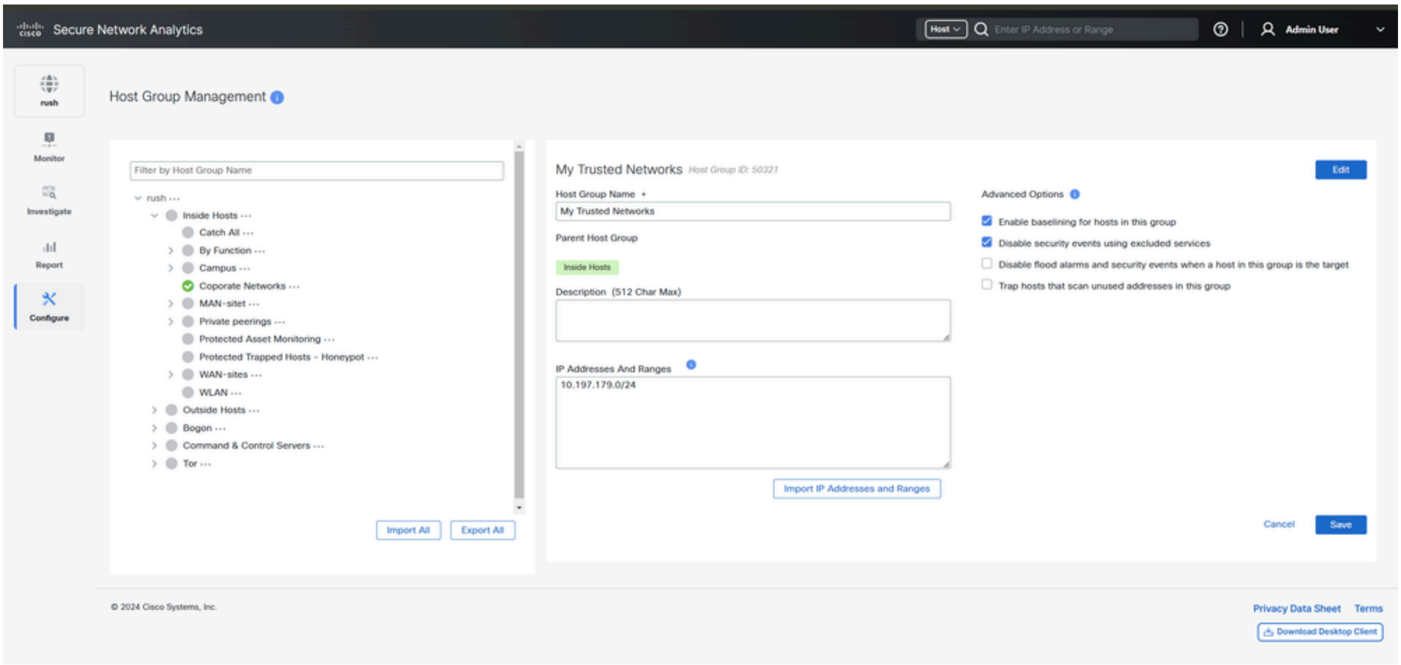
actions* QUARANTINE ×

3. Configure Secure Network Analytics for Event Trigger and Response Management for Rapid threat containment.

Step 1: Log in the SMC GUI and Navigate to **Configure > Detection > Host Group Management > Click on the (...) (ellipsis) icon** next to **Inside Hosts,** then select **Add Host Group**.

In this example, a new host group is created with the name My Trusted Networks under the parent host group of Inside Hosts.

This network can be typically assigned to the enduser machine for monitoring DNS usage.



My Trusted Networks *Host Group ID: 50321*

Host Group Name * My Trusted Networks

Parent Host Group: Inside Hosts

Description (512 Char Max)

IP Addresses And Ranges: 10.197.179.0/24

Advanced Options

☑ Enable baselining for hosts in this group

☑ Disable security events using excluded services

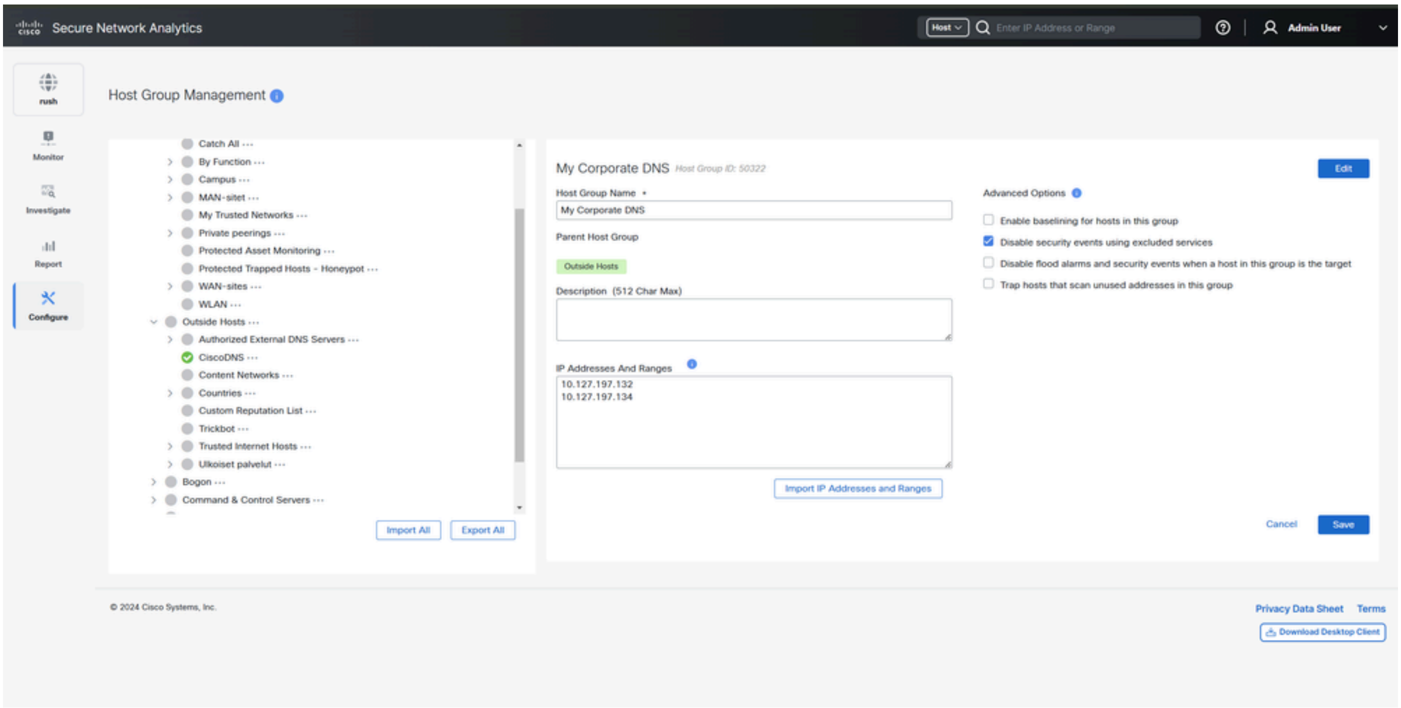
☐ Disable flood alarms and security events when a host in this group is the target

☐ Trap hosts that scan unused addresses in this group

Note: For this example, IP subnet 10.197.179.0/24 is used as a Local Area Network (LAN) subnet, This can differ in the actual network environment depending upon Network Architecture.

Step 2: Log in the SMC GUI and Navigate to **Configure > Detection > Host Group Management > Click on (...)** besides **Outside Hosts** and select **Add Host Group**.

In this example, a new host group is created with name My Corporate DNS under the parent host group of Outside Hosts.



Host Group Management

- Catch All ···
- By Function ···
- Campus ···
- MAN-sitet ···
- My Trusted Networks ···
- Private peerings ···
- Protected Asset Monitoring ···
- Protected Trapped Hosts - Honeypot ···
- WAN-sites ···
- WLAN ···
- Outside Hosts ···
  - Authorized External DNS Servers ···
  - ✓ CiscoDNS ···
  - Content Networks ···
  - Countries ···
  - Custom Reputation List ···
  - Trickbot ···
  - Trusted Internet Hosts ···
  - Ulkoiset palvelut ···
- Bogon ···
- Command & Control Servers ···

My Corporate DNS *Host Group ID: 50322*

Host Group Name *: My Corporate DNS

Parent Host Group: Outside Hosts

Description (512 Char Max)

IP Addresses And Ranges
10.127.197.132
10.127.197.134

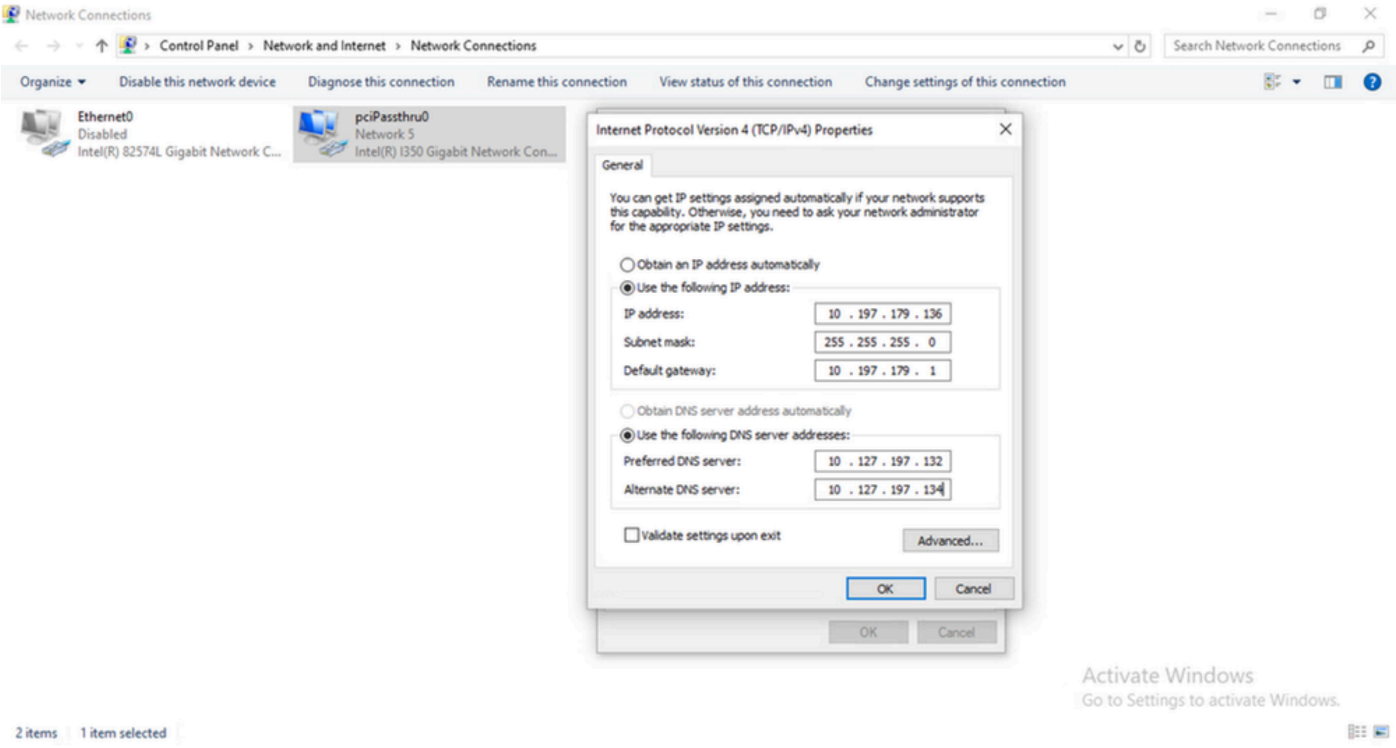
Advanced Options

☐ Enable baselining for hosts in this group
☑ Disable security events using excluded services
☐ Disable flood alarms and security events when a host in this group is the target
☐ Trap hosts that scan unused addresses in this group

© 2024 Cisco Systems, Inc.

Note: For this example, IPs 10.127.197.132 and 10.127.197.134 are used as the desired DNS servers to be used by the endusers, this can differ in the actual network environment depending upon Network Architecture.

The Test lab PC used for demonstration is configured with static IP 10.197.179.136 (belongs to My Trusted Networks host group created) and DNS 10.127.197.132 and 10.127.197.134 (belongs to My Corporate DNS host group created).


Network Connections
Control Panel > Network and Internet > Network Connections
Search Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this connection
View status of this connection
Change settings of this connection
Ethernet0
Disabled
Intel(R) 82574L Gigabit Network C...
pciPassthru0
Network 5
Intel(R) I350 Gigabit Network Con...
Activate Windows
Go to Settings to activate Windows.
2 items
1 item selected

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 197 . 179 . 136

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 197 . 179 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 10 . 127 . 197 . 132

Alternate DNS server: 10 . 127 . 197 . 134

□ Validate settings upon exit

Advanced... OK Cancel

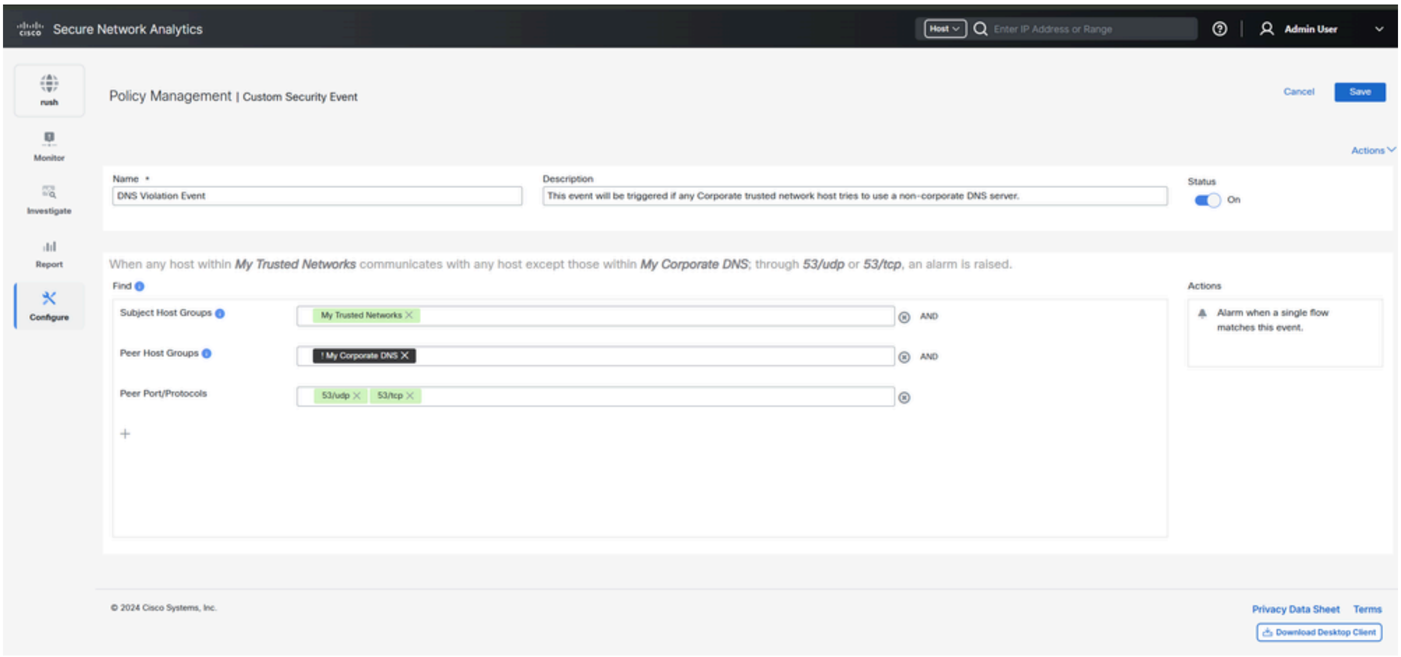
Step 3: Set up a tailored alert system to detect when internal users connect to external DNS servers, triggering an alarm to block connections to unauthorized DNS servers that could potentially redirect traffic to malicious external sites. Once an alarm is activated, Cisco Secure Network Analytics coordinates with Cisco ISE to isolate the host using these unauthorized DNS servers by employing an Adaptive Network Control Policy via PxGrid.

Navigate to **Configure > Policy Management.**

Create a Custom Events with the information:

- **Name :**DNS Violation Event.
- **Subject Host Groups :**My Trusted Networks.
- **Peer Host Groups** : (Not) My Corporate DNS.
- **Peer Port/Protocols** : 53/UDP 53/TCP

This means that when any host within My Trusted Networks (Host group) communicates with any host except those within My Corporate DNS (Host group) through 53/up or 53/tcp, an alarm is raised.



Policy Management | Custom Security Event

Name * DNS Violation Event

Description: This event will be triggered if any Corporate trusted network host tries to use a non-corporate DNS server.

Status: On

When any host within *My Trusted Networks* communicates with any host except those within *My Corporate DNS*; through *53/udp* or *53/tcp*, an alarm is raised.

Find

Subject Host Groups: My Trusted Networks — AND

Peer Host Groups: ! My Corporate DNS — AND

Peer Port/Protocols: 53/udp 53/tcp

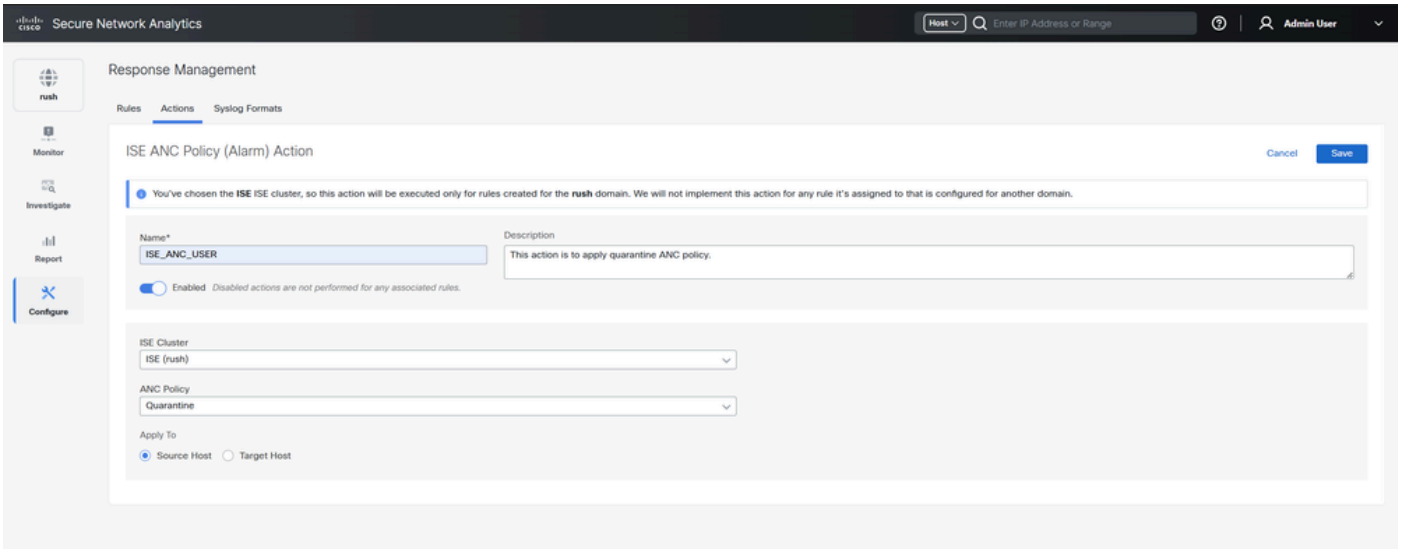
Actions: Alarm when a single flow matches this event.

© 2024 Cisco Systems, Inc.

Step 4: Configure a Response Management action to be performed, and which can later applied to the Response Management Rule once created.

Navigate to**Configure > Response Management** > **Actions, Click** on **Add New Action** and select **ISE ANC Policy (Alarm)**.

Assign a name and choose the specific Cisco ISE cluster to be notified in order to implement a quarantine policy for any violations or connections to unauthorized servers.



Response Management

ISE ANC Policy (Alarm) Action

You've chosen the **ISE** ISE cluster, so this action will be executed only for rules created for the **rush** domain. We will not implement this action for any rule it's assigned to that is configured for another domain.

Name* ISE_ANC_USER

Description: This action is to apply quarantine ANC policy.

Enabled *Disabled actions are not performed for any associated rules.*

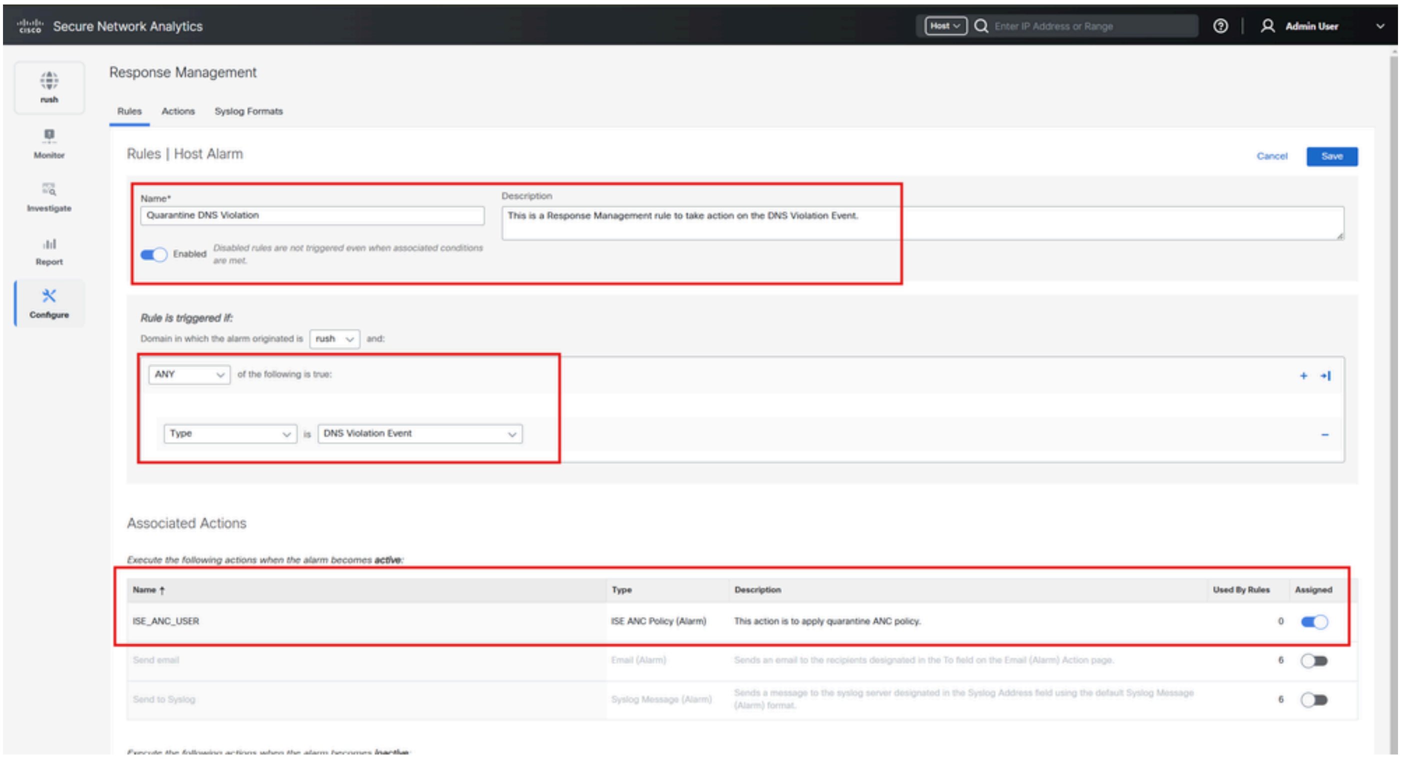
ISE Cluster: ISE (rush)

ANC Policy: Quarantine

Apply To: ● Source Host ○ Target Host

Step 5: Under the **Rules** section, **Create** a **new Rule**. This rule enforces the previously defined Action whenever a host within the internal network attempts to send DNS traffic to unauthorized DNS servers. In the **Rule is triggered if** section, choose **Type** and **select** the **custom event created** earlier.

Under **Associated Actions**, **select** the ISE **ANC Alarm action** that was previously configured.



Response Management

Rules | Actions | Syslog Formats

Rules | Host Alarm

Cancel | Save

Name*: Quarantine DNS Violation

Description: This is a Response Management rule to take action on the DNS Violation Event.

Enabled *Disabled rules are not triggered even when associated conditions are met.*

Rule is triggered if:

Domain in which the alarm originated is rush and:

ANY of the following is true:

Type is DNS Violation Event

Associated Actions

*Execute the following actions when the alarm becomes **active**:*

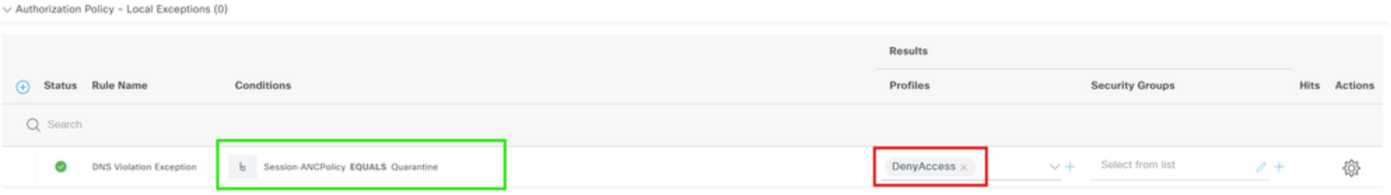
Name ↑	Type	Description	Used By Rules	Assigned
ISE_ANC_USER	ISE ANC Policy (Alarm)	This action is to apply quarantine ANC policy.	0	●
Send email	Email (Alarm)	Sends an email to the recipients designated in the To field on the Email (Alarm) Action page.	6	○
Send to Syslog	Syslog Message (Alarm)	Sends a message to the syslog server designated in the Syslog Address field using the default Syslog Message (Alarm) format.	6	○

*Execute the following actions when the alarm becomes **inactive**:*

4. Configure Cisco ISE to respond to actions initiated by Stealthwatch upon triggering the event.

Log in to Cisco ISE GUI and Navigate to **Policy > Policy Sets** > **Choose** the **Policy set** > under **Authorization Policy - Local Exceptions** > Create **new Policy.**

- **Name:** DNS Violation Exception
- **Conditions:** Session: ANCPolicy EQUALS Quarantine
- **Authorization Profiles**: DenyAccess



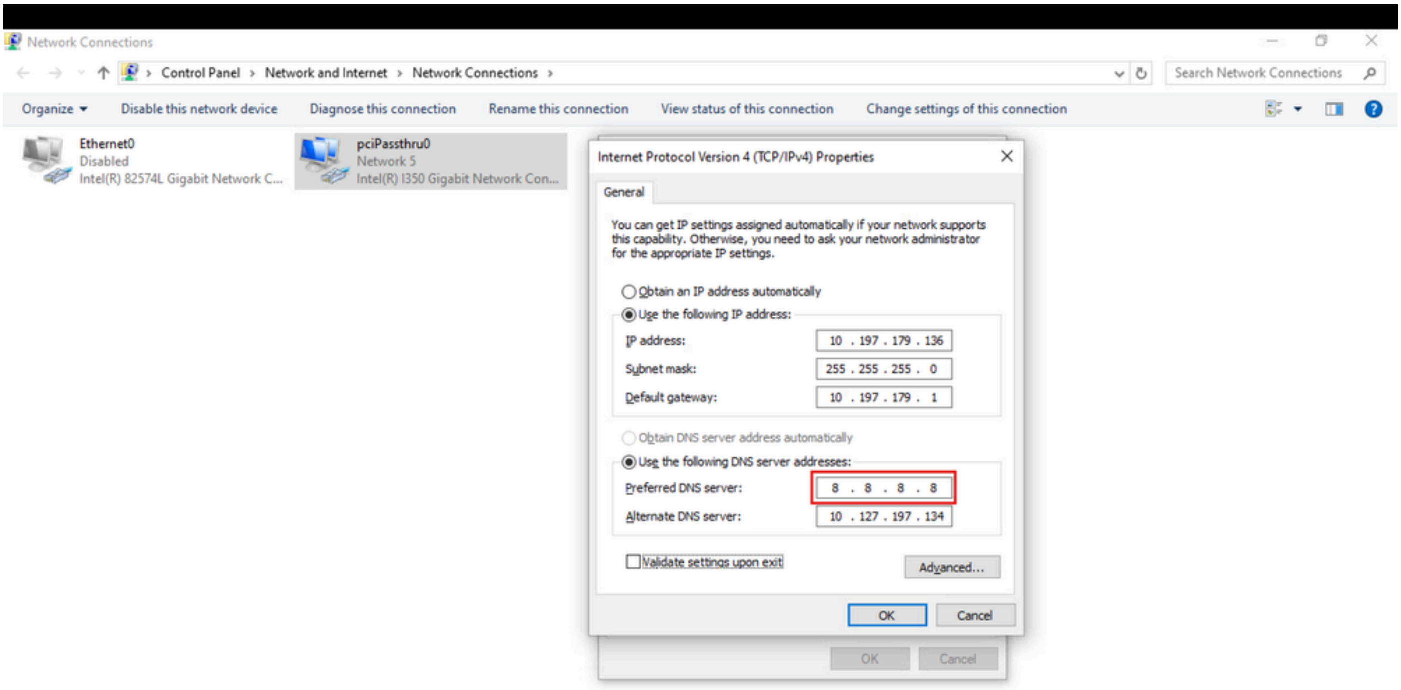
Authorization Policy - Local Exceptions (0)

			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	DNS Violation Exception	Session·ANCPolicy EQUALS Quarantine	DenyAccess	Select from list		⚙

Note: In this example, once the DNS violation event is triggered access is denied to the user based on the configuration

Verify

To demonstrate the use case, the DNS entry on the endpoint has been changed to 8.8.8.8, which triggers the DNS violation event configured . Since the DNS server does not belong to the host group of My Corporate DNS servers, it triggers the event resulting a deny access to the endpoint.


Network Connections
Control Panel > Network and Internet > Network Connections >
Search Network Connections
Organize ▾
Disable this network device
Diagnose this connection
Rename this connection
View status of this connection
Change settings of this connection
Ethernet0
Disabled
Intel(R) 82574L Gigabit Network C...
pciPassthru0
Network 5
Intel(R) I350 Gigabit Network Con...
General
Advanced...
OK
Cancel

Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 197 . 179 . 136

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 197 . 179 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8

Alternate DNS server: 10 . 127 . 197 . 134

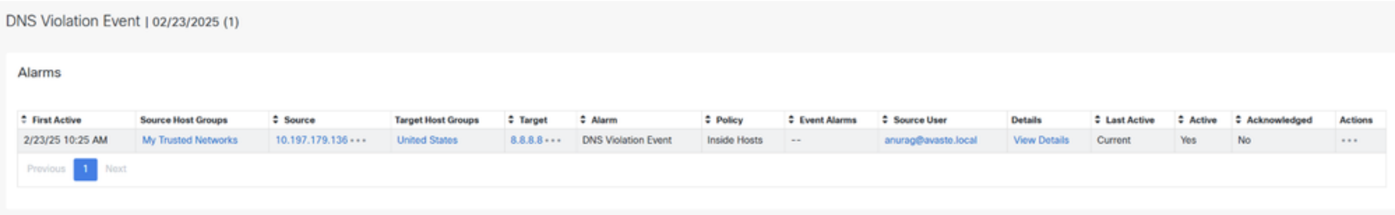
□ Validate settings upon exit

On the C9300 switch, verify using the **show flow monitor IPv4_NETFLOW cache | in 8.8.8.8** command with the output to see the flows are being captured and sent to the Flow Collector. The IPv4_NETFLOW is configured in the switch configuration.

<#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
```

Once the Event is triggered on the Stealthwatch, **navigate** to **Monitor** > **Security Insight Dashboard**,.



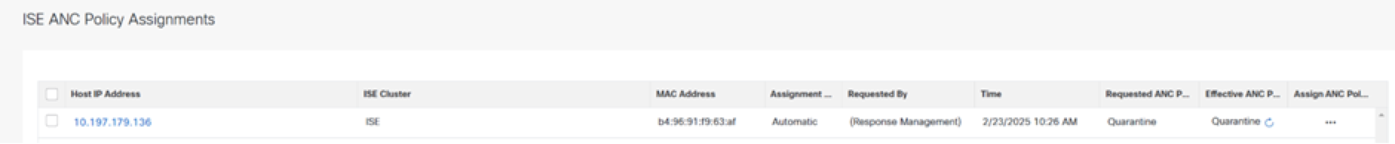
DNS Violation Event | 02/23/2025 (1)

Alarms

⇕ First Active	Source Host Groups	⇕ Source	Target Host Groups	⇕ Target	⇕ Alarm	⇕ Policy	⇕ Event Alarms	⇕ Source User	Details	⇕ Last Active	⇕ Active	⇕ Acknowledged	Actions
2/23/25 10:25 AM	My Trusted Networks	10.197.179.136 •••	United States	8.8.8.8 •••	DNS Violation Event	Inside Hosts	--	anurag@avaste.local	View Details	Current	Yes	No	•••

Navigate to **Monitor > Integration > ISE ANC Policy Assignments.**

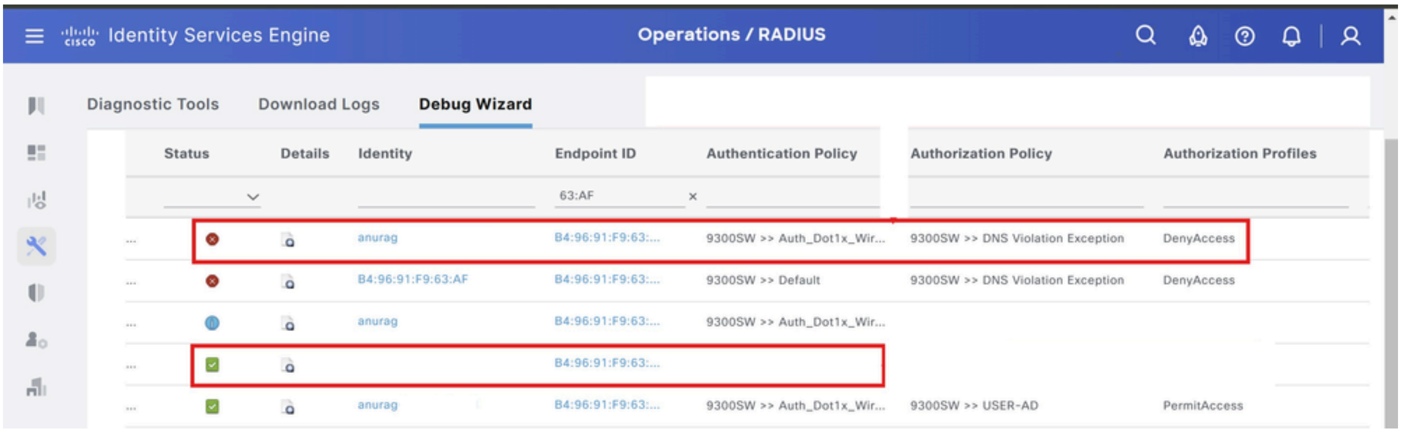
Ensure that Cisco Secure Network Analytics has successfully implemented the Adaptive Network Control Policy via PxGrid and Cisco ISE to quarantine the host.



ISE ANC Policy Assignments

□	Host IP Address	ISE Cluster	MAC Address	Assignment ...	Requested By	Time	Requested ANC P...	Effective ANC P...	Assign ANC Pol...
□	10.197.179.136	ISE	b4:96:91:f9:63:af	Automatic	(Response Management)	2/23/2025 10:26 AM	Quarantine	Quarantine	•••

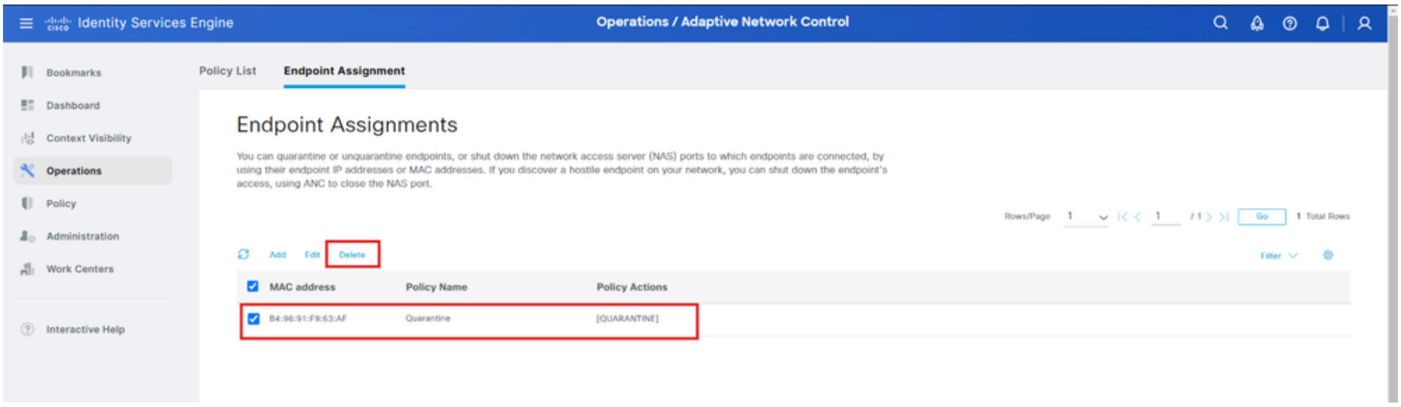
Similarly on Cisco ISE, navigate to **Operations > RADIUS > Livelogs** and apply filter for the endpoint.



	Status	Details	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles
				63:AF			
...	⊗	🔍	anurag	B4:96:91:F9:63:...	9300SW >> Auth_Dot1x_Wir...	9300SW >> DNS Violation Exception	DenyAccess
...	⊗	🔍	B4:96:91:F9:63:AF	B4:96:91:F9:63:...	9300SW >> Default	9300SW >> DNS Violation Exception	DenyAccess
...	●	🔍	anurag	B4:96:91:F9:63:...	9300SW >> Auth_Dot1x_Wir...		
...	✓	🔍		B4:96:91:F9:63:...			
...	✓	🔍	anurag	B4:96:91:F9:63:...	9300SW >> Auth_Dot1x_Wir...	9300SW >> USER-AD	PermitAccess

Per the local exception policy DNS Violation Exception, Change of Authorization(CoA) is issued by ISE and access ISE denied to the endpoint.

Once the remediation actions are performed on the endpoint, remove the MAC from **Operations > Adaptive Network Control > Endpoint Assignments > Delete** to remove the MAC address of the endpoint.



Endpoint Assignments

You can quarantine or unquarantine endpoints, or shut down the network access server (NAS) ports to which endpoints are connected, by using their endpoint IP addresses or MAC addresses. If you discover a hostile endpoint on your network, you can shut down the endpoint's access, using ANC to close the NAS port.

☑	MAC address	Policy Name	Policy Actions
☑	B4:96:91:F9:63:AF	Quarantine	[QUARANTINE]

Log Reference on Cisco ISE.

Attributes set to TRACE level for pxgrid (pxgrid-server.log) component on Cisco ISE, logs are seen in the pxgrid-server.log file.

<#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

Quarantined Endpoints do not Renew Authentication Post-policy Change

Problem

Authentication has failed due to change in policy or additional identity and no re-authentication is taking place. Authentication fails or the endpoint in question remains unable to connect to the network. This issue often occurs on client machines that fails posture assessment per the posture policy that is assigned to the user role.

Possible Causes

The authentication timer setting is not correctly set on the client machine, or the authentication interval is not correctly set on the switch.

Solution

There are several possible resolutions for this issue:

1. Check theSession Status Summaryreport in Cisco ISE for the specified NAD or switch, and ensure that the interface has the appropriate authentication interval configured.

2. Enter **show running configuration** on the NAD/switch and ensure that the interface is configured with an appropriate **authentication timer restart** setting. (For example, **authentication timer restart 15**, and **authentication timer reauthenticate 15)**.

3. Enter **interface shutdown** and **no shutdown** to bounce the port on the NAD/switch and force re-authentication and potential configuration change in Cisco ISE.

Note: Because CoA requires a MAC address or session ID, it is recommended that you do not bounce the port that is shown in the Network Device SNMP report.

ANC Operations Fail when IP Address or MAC Address is not Found

AnANCoperation that you perform on an endpoint fails when an active session for that endpoint does not contain information about the IP address. This also applies to the MAC address and session ID for that endpoint.

Note: When you want to change the authorization state of an endpoint through ANC, you must provide the IP address or the MAC address for the endpoint. If the IP address or the MAC address is not found in the active session for the endpoint, you can see the error message: "No active session found for this MAC address, IP Address or Session ID".