

# ISE 3.3およびStealthWatch 7.5.1でのANCの設定

## 内容

---

[はじめに](#)

[前提条件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ネットワーク図](#)

[段階的設定手順](#)

[確認](#)

[トラブルシューティング](#)

[隔離されたエンドポイントが認証を更新しないポリシー変更後](#)

[問題](#)

[考えられる原因](#)

[解決方法](#)

[IPアドレスまたはMACアドレスが見つからない場合にANCOperationsが失敗する](#)

---

## はじめに

このドキュメントでは、Cisco ISE®バージョン3.3およびStealthwatchでのRapid Threat Containment(Adaptive Network Control)の設定について説明します。

## 前提条件

次の項目に関する知識があることが推奨されます。

- Identity Services Engine ( ISE )
- Platform Exchange Grid(PxGrid)
- セキュアネットワーク分析(Stealthwatch)
- 迅速な脅威の抑制(Adaptive Network Control - ANC)

このドキュメントでは、ANC対応のpxGridを使用して、Cisco Identity Services Engine(ISE)がSecure Network Analytics(Stealthwatch)と統合されていることを前提としています。

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとバージョンに基づくものです。

- Cisco Identity Services Engine(ISE)バージョン3.3

- Secure Network Analytics(Stealthwatch)7.5.1
- Catalyst 9300

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

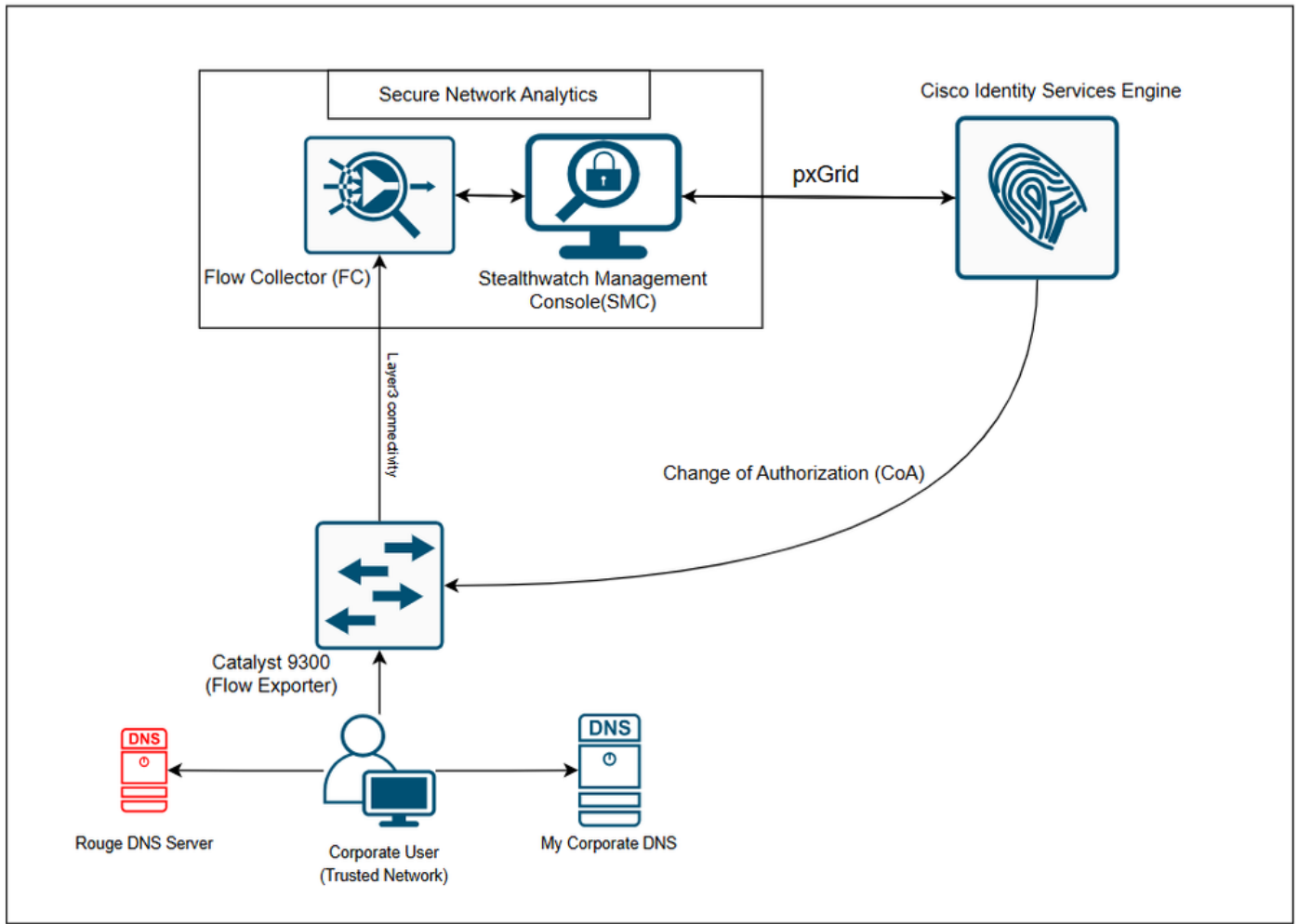
Cisco Secure Cloud Analytics（現在はCisco XDRの一部）は、pxGridを使用してCisco Identity Services Engine(ISE)からユーザ帰属データを取得できます。この統合により、Secure Cloud Analytics Event Viewerでユーザアクティビティレポートを作成できます。

Secure Network Analytics（以前のStealthwatch）とCisco Identity Services Engine(ISE)を組み合わせることで、組織は360°ビューを取得し、脅威に迅速に対応し、成長するデジタルビジネスを保護できます。Secure Network Analyticsが異常なトラフィックを検出すると、アラートを発行して、ユーザを検疫するオプションを管理者に提供します。pxGridにより、Secure Network Analyticsは検疫コマンドを直接Identity Services Engineに渡すことができます。

この例では、企業のDNSサーバを利用してインターネットの脅威から保護する方法について説明します。目的は、内部ユーザが外部DNSサーバに接続したときにトリガーされる、カスタマイズされたアラートメカニズムを確立することです。この取り組みは、有害な外部サイトにトラフィックをリダイレクトする可能性のある不正なDNSサーバへの接続をブロックすることを目的としています。

アラートがトリガーされると、Cisco Secure Network AnalyticsはCisco ISEと連携し、PxGrid経由で適応型ネットワーク制御ポリシーを使用して、不正なDNSサーバにアクセスしているホストを検疫します。

## ネットワーク図



図に示すように：

- 企業ユーザは、IPフローをエクスポートし、フローコレクタにデータを送信するように設定されたC9300スイッチに接続されています。
- 同じ社内ユーザが、社内DNSサーバを使用するように設定されています。
- Flow CollectorはStealthWatch Management Console(SMC)と統合
- StealthWatch Management Console(SMC)は、PxgridとISEを介して統合されます。

## 段階的設定手順

1. NetFlowを使用してフローをモニタおよびエクスポートするようにスイッチを準備します。

Cisco IOS® XE 17.15.01を実行するC9300スイッチの基本フロー設定

```

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
```

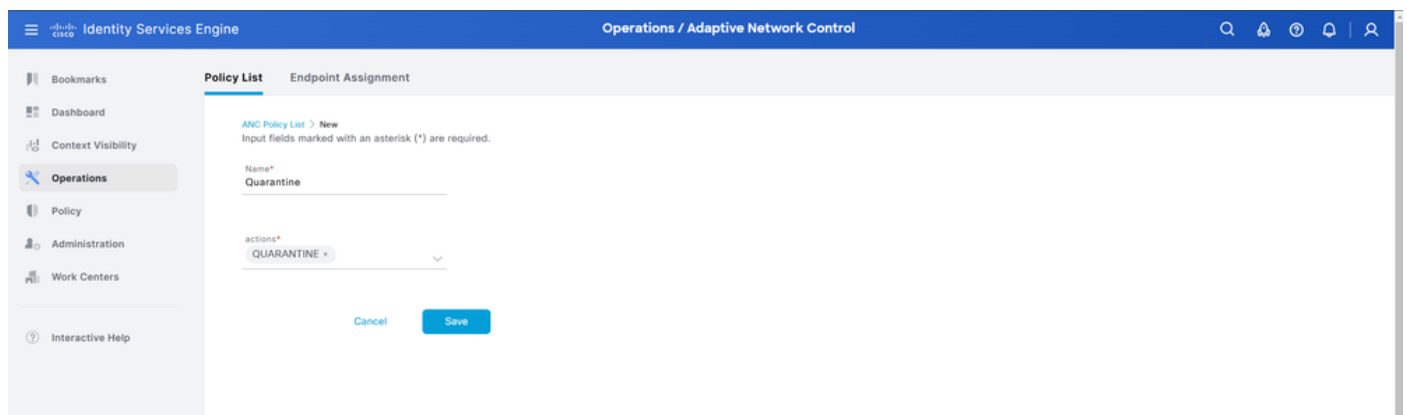
```
! VALIDATION COMMANDS
! show flow record SW_FLOW_RECORD
! show flow monitor IPv4_NETFLOW statistics
! show flow monitor IPv4_NETFLOW cache
```

設定が完了すると、C9300はフローコレクタにIPフローデータをエクスポートできるようになります。フローコレクタは、このデータを処理してStealthWatch Management Console(SMC)に転送し、分析とモニタリングを行います。

## 2. Cisco ISEのEnableAdaptive Networkコントロール

ANCはデフォルトで無効になっています。ANCはpxGridが有効になっている場合にのみ有効になり、管理者ポータルでサービスを手動で無効にするまで有効のままになります。

Operations > Adaptive Network Control > Policy List > Addの順に選択し、ポリシー名にQuarantine、アクションにQuarantineと入力します。

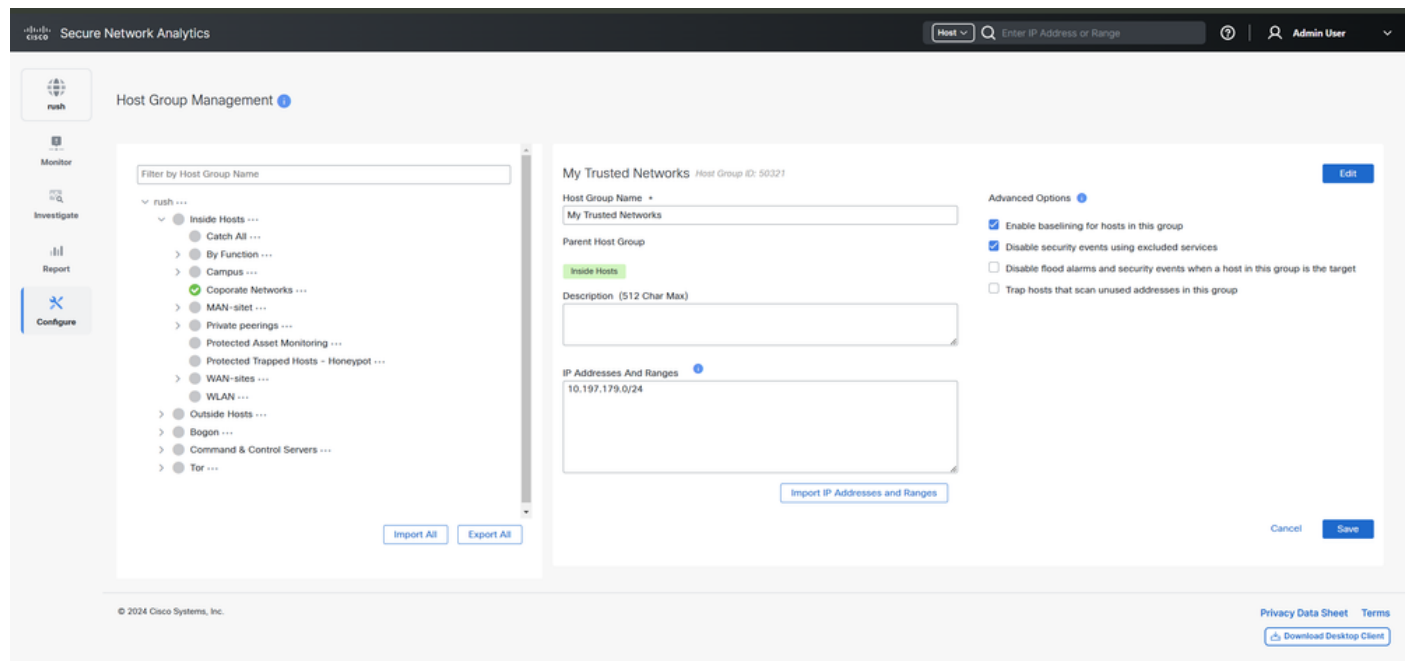


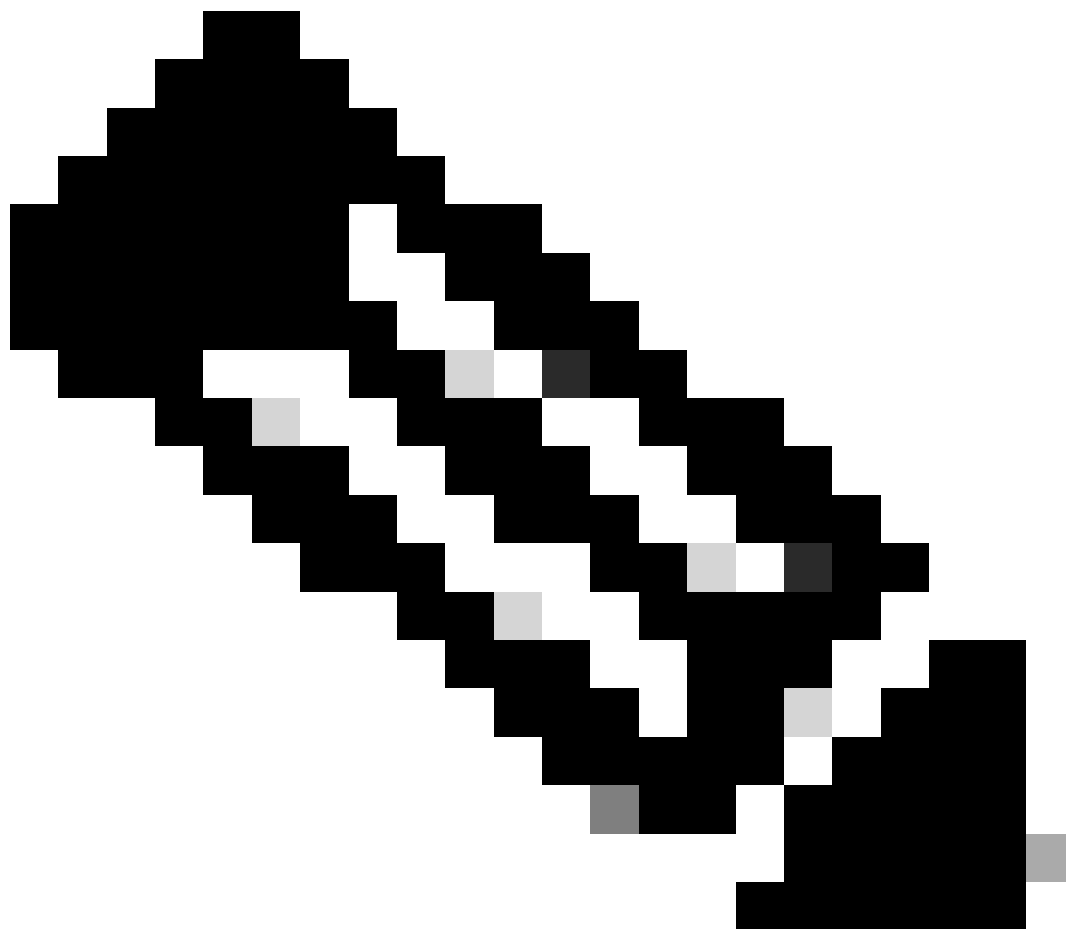
3. 迅速な脅威の封じ込めに備えて、イベントトリガーおよび応答管理のSecure Network Analyticsを設定します。

ステップ1: SMC GUIにログインし、設定>検出>ホストグループ管理に移動します。内部ホストの横にあるアイコン(...) (省略記号) をクリックし、ホストグループの追加を選択します。

この例では、Inside Hostsという親ホストグループの下に、My Trusted Networksという名前の新しいホストグループが作成されています。

通常、このネットワークは、DNS使用率を監視するためにエンドユーザマシンに割り当てることができます。



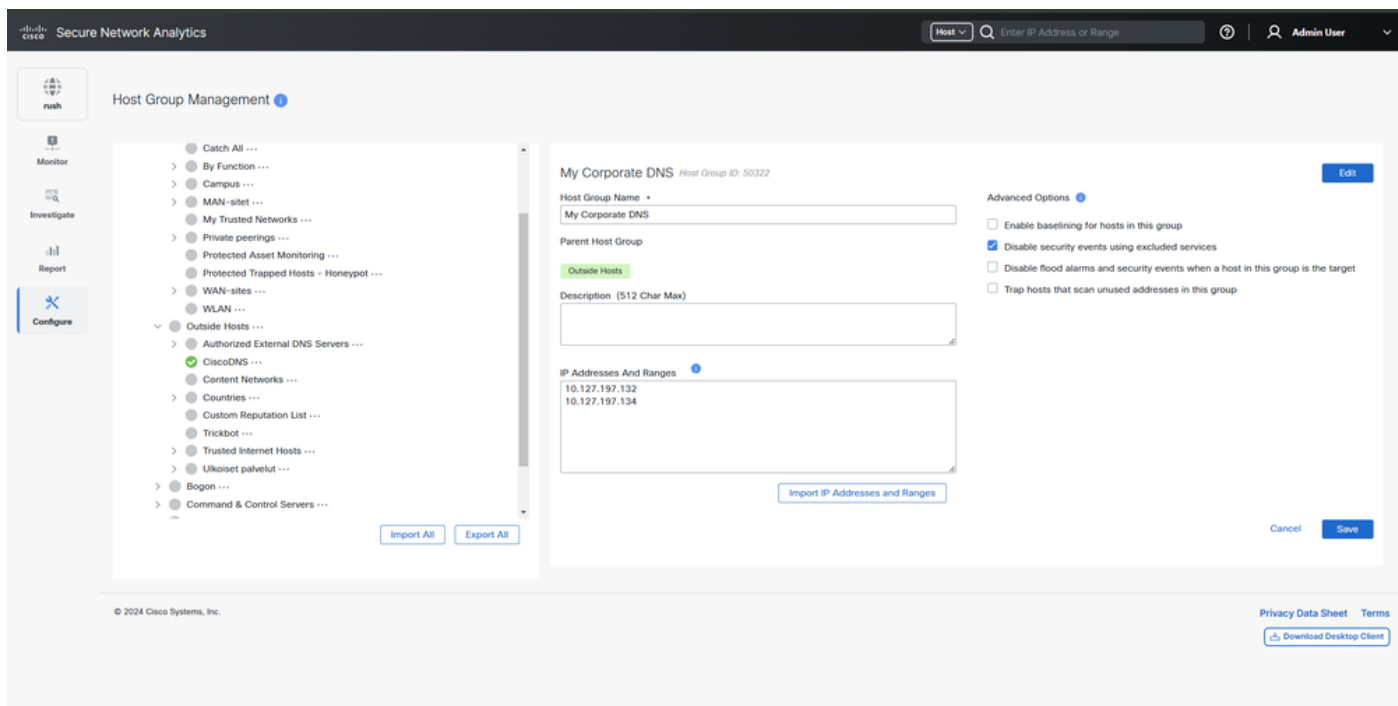


注：この例では、IPサブネット10.197.179.0/24がローカルエリアネットワーク(LAN)サブネットとして使用されています。これは、ネットワークアーキテクチャによって実際のネットワーク環境が異なる場合があります。

---

ステップ2:SMC GUIにログインし、Configure > Detection > Host Group Managementの順に選択します。Outside Hostsの横にある(...)をクリックし、Add Host Groupを選択します。

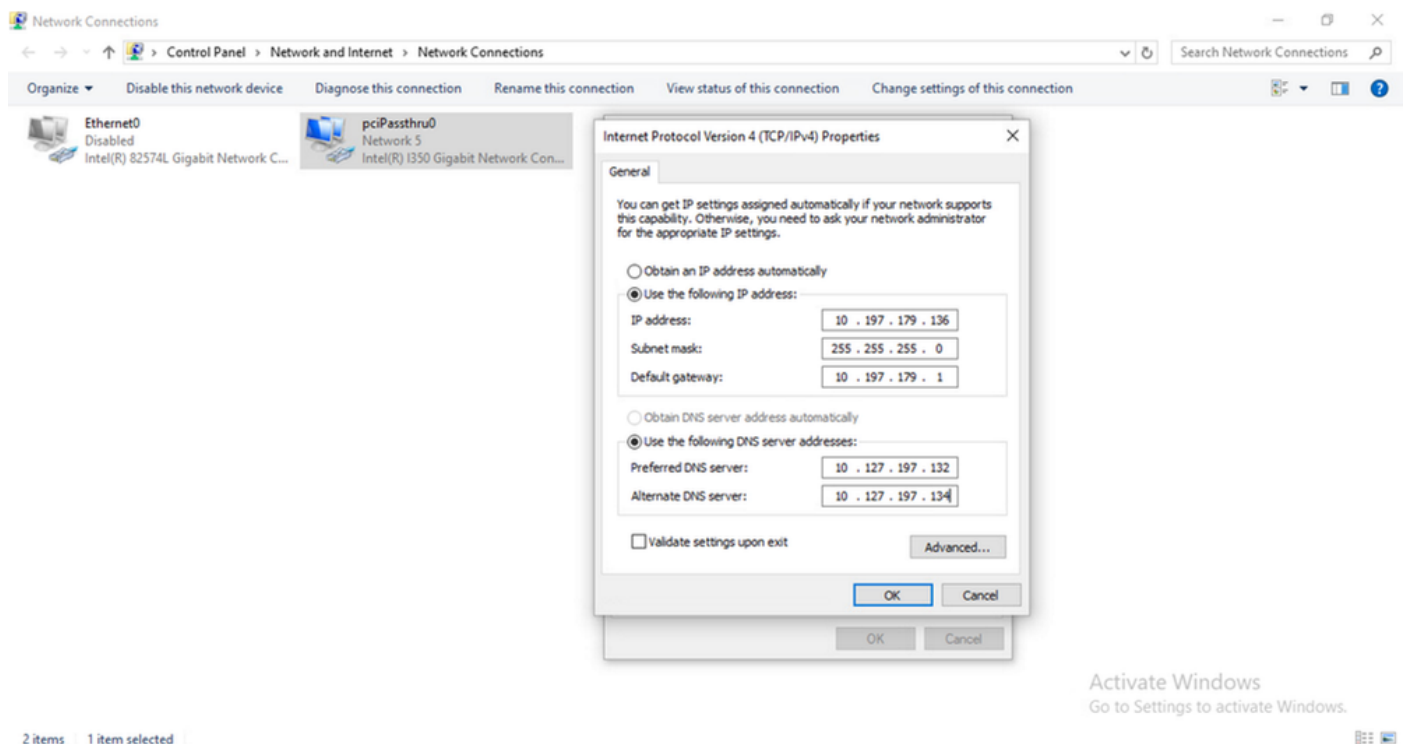
この例では、Outside Hostsという親ホストグループの下に、My Corporate DNSという名前の新しいホストグループが作成されます。



注：この例では、IP 10.127.197.132と10.127.197.134がエンドユーザが使用する目的の

DNSサーバとして使用されます。これは、ネットワークアーキテクチャによって実際のネットワーク環境が異なる場合があります。

デモンストレーションに使用するテストラボPCは、スタティックIP 10.197.179.136 ( 作成したMy Trusted Networksホストグループに属する ) とDNS 10.127.197.132および10.127.197.134 ( 作成したMy Corporate DNSホストグループに属する ) で設定されています。



ステップ3:内部ユーザが外部DNSサーバに接続したときに検出するようにカスタマイズされたアラートシステムを設定し、悪意のある外部サイトにトラフィックをリダイレクトする可能性のある不正なDNSサーバへの接続をブロックするアラームをトリガーします。アラームがアクティブになると、Cisco Secure Network AnalyticsはCisco ISEと連携し、PxGrid経由でAdaptive Network Control Policy(ACP)を採用することで、不正なDNSサーバを使用しているホストを分離します。

Configure > Policy Managementの順に移動します。

次の情報を使用してカスタムイベントを作成します。

- 名前 : DNS違反イベント。
- Subject Host Groups :My Trusted Networks ( 信頼できるネットワーク )。
- ピアホストグループ ( Pホストグループ ) : ( 社内DNSではありません )。
- ピアポート/プロトコル:53/UDP 53/TCP

これは、My Trusted Networks ( ホストグループ ) 内のホストがMy Corporate DNS ( ホストグループ ) 内のホスト以外のホストと53/upまたは53/tcp経由で通信するときにアラームが発生することを意味します。

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

Peer Host Groups: My Corporate DNS

Peer Port/Protocols: 53/udp, 53/tcp

Actions

Alarm when a single flow matches this event.

© 2024 Cisco Systems, Inc. Privacy Data Sheet Terms Download Desktop Client

ステップ4：実行する応答管理アクションを設定します。このアクションは、作成後に応答管理ルールに適用できます。

Configure > Response Management > Actionsの順に移動し、Add New Actionをクリックして、ISE ANC Policy (Alarm)を選択します。

名前を割り当て、通知する特定のCisco ISEクラスタを選択して、不正なサーバへの違反または接続に対する検疫ポリシーを実装します。

Response Management

ISE ANC Policy (Alarm) Action

Name: ISE\_ANC\_USER

Description: This action is to apply quarantine ANC policy.

Status: Enabled

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.

ISE Cluster: ISE (rush)

ANC Policy: Quarantine

Apply To: Source Host

© 2024 Cisco Systems, Inc. Privacy Data Sheet Terms Download Desktop Client

ステップ5:Rulesセクションの下で、Create a new Ruleを入力します。このルールは、内部ネットワーク内のホストが許可されていないDNSサーバにDNSトラフィックを送信しようとするたびに、以前に定義したアクションを適用します。Rule is triggered ifセクションで、Typeを選択し、前述のcustom event createdを選択します。Associated Actionsの下で、以前に設定されたISE ANC Alarm actionを選択します。

Secure Network Analytics

Host Enter IP Address or Range

Admin User

### 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 ruth 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             | <input checked="" type="checkbox"/> |
| Send email     | Email (Alarm)          | Sends an email to the recipients designated in the To field on the Email (Alarm) Action page.                                | 6             | <input type="checkbox"/>            |
| 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             | <input type="checkbox"/>            |

Execute the following actions when the alarm becomes inactive:

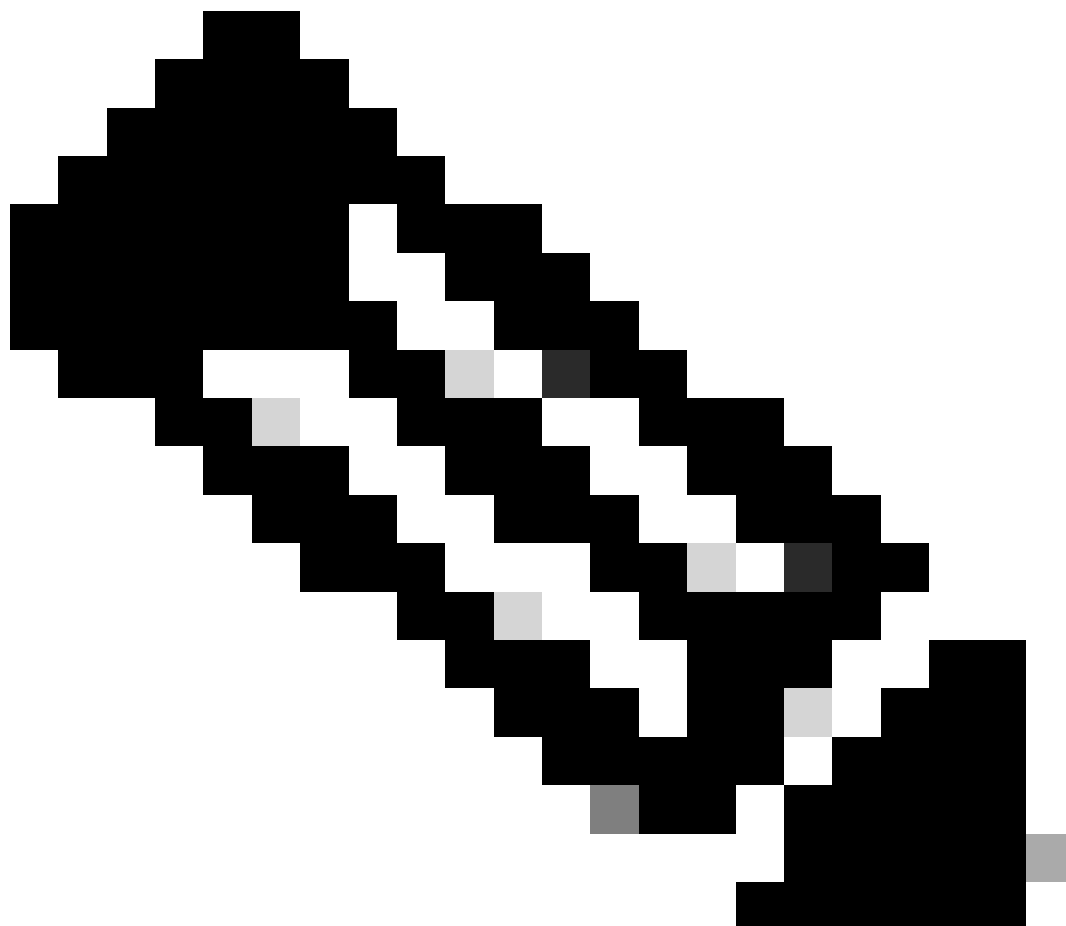
4. イベントのトリガー時にStealthwatchが開始したアクションに応答するようにCisco ISEを設定します。

Cisco ISE GUIにログインし、Policy > Policy Sets > Choose the Policy set > under Authorization Policy - Local Exceptions > Create new Policyの順に選択します。

- 名前：DNS違反の例外
- 条件：セッション：ANCPolicy EQUALS Quarantine
- 許可プロファイル:DenyAccess

Authorization Policy - Local Exceptions (0)

| Status                              | Rule Name               | Conditions                          | Results    |                  |              |
|-------------------------------------|-------------------------|-------------------------------------|------------|------------------|--------------|
|                                     |                         |                                     | Profiles   | Security Groups  | Hits Actions |
| <input checked="" type="checkbox"/> | DNS Violation Exception | Session-ANCPolicy EQUALS Quarantine | DenyAccess | Select from list |              |

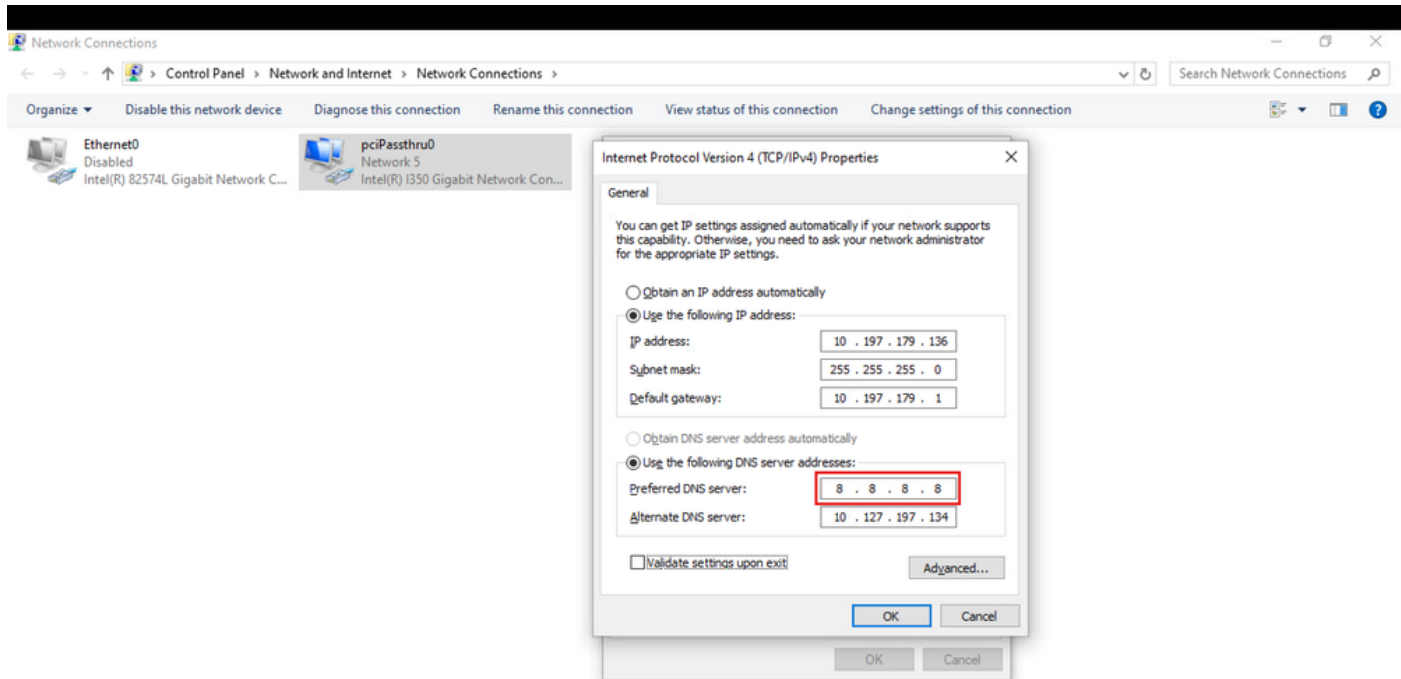


注：この例では、DNS違反イベントがトリガーされると、設定に基づいてユーザへのアクセスが拒否されます

---

## 確認

使用例を示すために、エンドポイントのDNSエントリは8.8.8.8に変更され、設定されたDNS違反イベントがトリガーされます ( DNS違反イベントはトリガーされません )。DNSサーバがMy Corporate DNSサーバのホストグループに属していないため、エンドポイントへのアクセスを拒否するイベントが発生します。



C9300スイッチで、`show flow monitor IPv4_NETFLOW cache | in 8.8.8.8`コマンドと出力を使用して、フローがキャプチャされ、フローコレクタに送信されていることを確認します。IPv4\_NETFLOWは、スイッチ設定で設定されます。

<#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

Stealthwatchでイベントがトリガーされたら、Monitor > Security Insight Dashboardの順に移動します。

## 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@avast.local | <a href="#">View Details</a> | Current     | Yes    | No           | ...     |

Previous 1 Next

Monitor > Integration > ISE ANC Policy Assignmentsの順に移動します。

Cisco Secure Network Analyticsが、ホストを検疫するためにPxGridおよびCisco ISEを介してAdaptive Network Control Policyを正常に実装していることを確認します。

## 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         | ...               |

同様にCisco ISEで、Operations > RADIUS > Livelogsの順に移動し、エンドポイントにフィルタを適用します。

ローカル例外ポリシーDNS Violation Exceptionに従い、認可変更(CoA)がISEによって発行され、エンドポイントに対するアクセスがISEによって拒否されます。

エンドポイントで修復操作が実行されたら、Operations > Adaptive Network Control > Endpoint Assignments > Delete の順に選択し、MACを削除してエンドポイントのMACアドレスを削除します。

| Identity Services Engine |  |  |  |  |  |  |  | Operations / Adaptive Network Control                                                                                                                                                                                                                                                                                   |  |
|--------------------------|--|--|--|--|--|--|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| Bookmarks                |  |  |  |  |  |  |  | Policy List                                                                                                                                                                                                                                                                                                             |  |
| Dashboard                |  |  |  |  |  |  |  | Endpoint Assignment                                                                                                                                                                                                                                                                                                     |  |
| Context Visibility       |  |  |  |  |  |  |  | Endpoint Assignments                                                                                                                                                                                                                                                                                                    |  |
| Operations               |  |  |  |  |  |  |  | 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. |  |
| Policy                   |  |  |  |  |  |  |  | Rows/Page 1 < 1 / 1 > Go 1 Total Rows                                                                                                                                                                                                                                                                                   |  |
| Administration           |  |  |  |  |  |  |  | Add Edit Delete Filter                                                                                                                                                                                                                                                                                                  |  |
| Work Centers             |  |  |  |  |  |  |  | MAC address Policy Name Policy Actions                                                                                                                                                                                                                                                                                  |  |
| Interactive Help         |  |  |  |  |  |  |  | B4:96:91:F9:63:AF Quarantine [QUARANTINE]                                                                                                                                                                                                                                                                               |  |

Cisco ISEのログ参照。

Cisco ISEのpxgrid(pxgrid-server.log)コンポーネントの属性がTRACEレベルに設定されている場合、ログはpxgrid-server.logファイルに表示されます。

<#root>

DEBUG [pxgrid-http-pool5][[]] cpm.pxgrid.ws.client.WsIseClientConnection -:::617fffb27858402d9ff9658b8

**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**

"}

## トラブルシューティング

隔離されたエンドポイントが認証を更新しないポリシー変更後

問題

ポリシーの変更または追加のIDが原因で認証に失敗し、再認証は行われません。認証が失敗する

か、または問題のエンドポイントが引き続きネットワークに接続できない。この問題は、ユーザロールに割り当てられたポスチャポリシーに従ったポスチャ評価に失敗したクライアントマシンで頻繁に発生します。

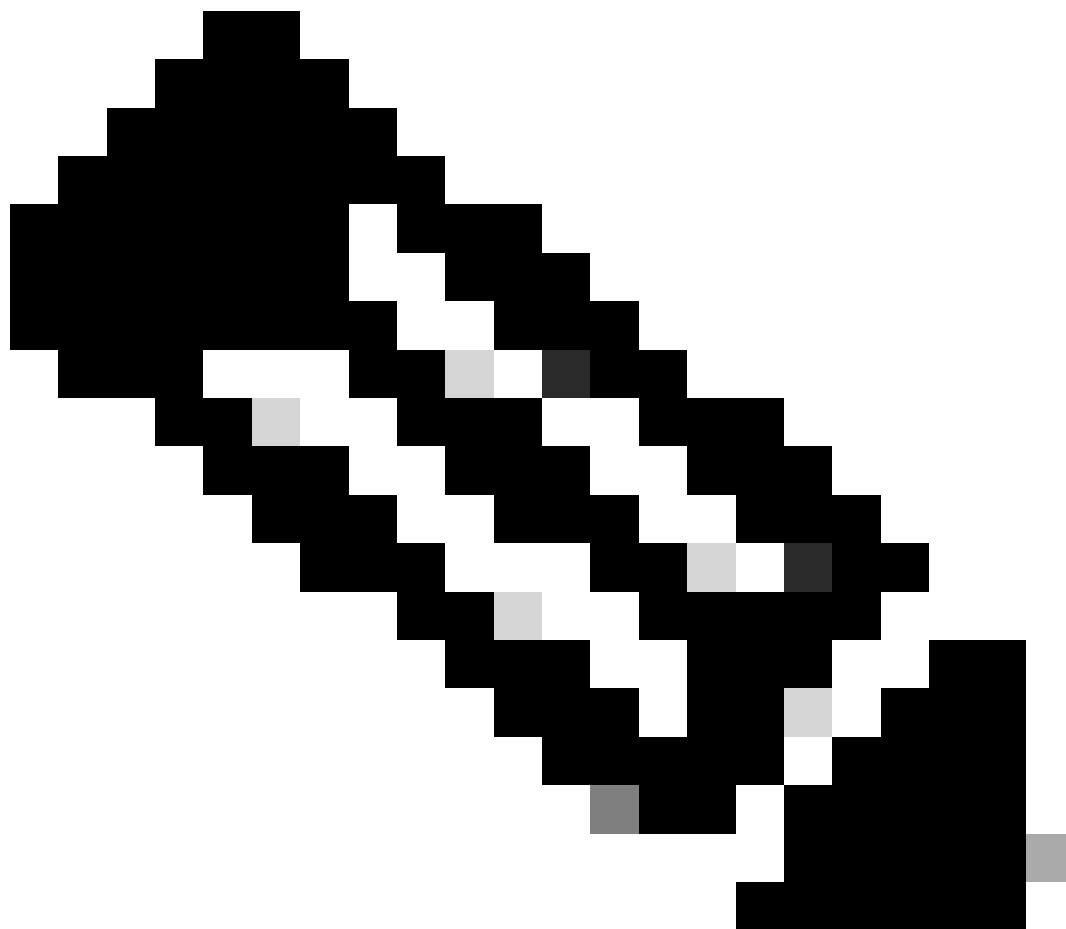
### 考えられる原因

認証タイマー設定がクライアントマシンで正しく設定されていないか、または認証間隔がスイッチで正しく設定されていません。

### 解決方法

この問題には、次のようないくつかの解決策があります。

1. Cisco ISEで指定したNADまたはスイッチのセッションステータス要約レポートを確認し、インターフェイスに適切な認証間隔が設定されていることを確認します。
2. NAD/スイッチでshow running configurationを入力し、インターフェイスに適切な authentication timer restart設定が設定されていることを確認します。(たとえば、 authentication timer restart 15、 authentication timer reauthenticate 15)。
3. interface shutdownおよびno shutdownを入力して、NAD/スイッチ上のポートをバウンスし、再認証とCisco ISEでの設定変更を強制します。

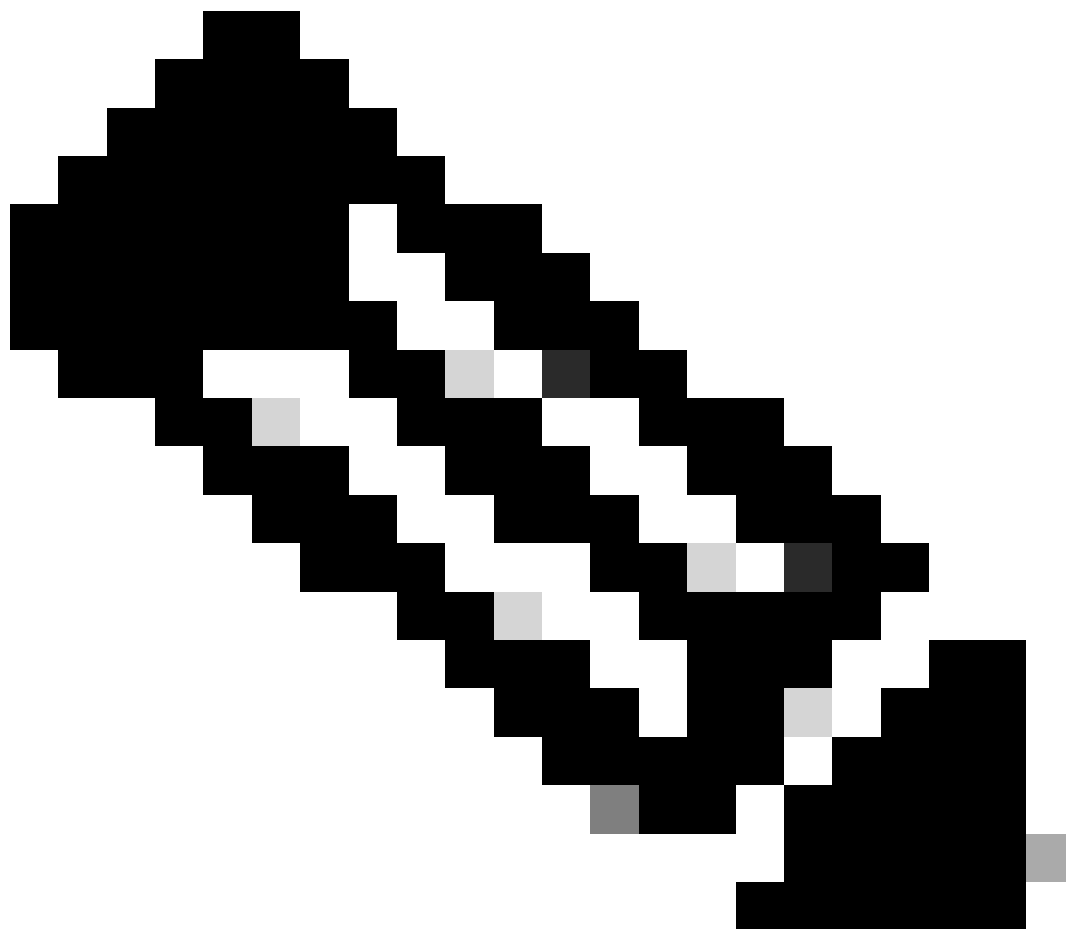


注:CoAにはMACアドレスまたはセッションIDが必要なので、ネットワークデバイスのSNMPレポートに表示されるポートをバウンスしないことを推奨します。

---

IPアドレスまたはMACアドレスが見つからないとANC操作が失敗する

エンドポイントに対して実行するANCoperationは、そのエンドポイントのアクティブセッションにIPアドレスに関する情報が含まれていないと失敗します。これは、そのエンドポイントのMACアドレスとセッションIDにも適用されます。



注:ANCを使用してエンドポイントの承認状態を変更する場合は、エンドポイントのIPアドレスまたはMACアドレスを指定する必要があります。エンドポイントのアクティブセッションでIPアドレスまたはMACアドレスが見つからない場合は、「No active session found for this MAC address, IP Address or Session ID」というエラーメッセージが表示されます。

---

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。