Configurazione di ANC su ISE 3.3 e Stealthwatch 7.5.1

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Componenti usati](#)

[Premesse](#)

[Esempio di rete](#)

[Configurazione dettagliata](#)

[Verifica](#)

[Risoluzione dei problemi](#)

- [Gli endpoint in quarantena non rinnovano l'autenticazione dopo la modifica dei criteri](#)
  - [Problema](#)
  - [Possibili cause](#)
  - [Soluzione](#)
  - [Operazioni ANCO non riuscite se non viene trovato l'indirizzo IP o MAC](#)

Introduzione

Questo documento descrive la configurazione di Rapid Threat Container (Adaptive Network Control) su Cisco ISE® versione 3.3 e Stealthwatch.

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Identity Services Engine (ISE)
- PxGrid (Platform Exchange Grid)
- Stealthwatch (Secure Network Analytics)
- Contenimento rapido delle minacce (Adaptive Network Control - ANC).

In questo documento si presume che Cisco Identity Services Engine sia integrato con Secure Network Analytics (Stealthwatch) utilizzando pxGrid abilitato per ANC.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Cisco Identity Services Engine (ISE) versione 3.3

- Secure Network Analytics (Stealthwatch) 7.5.1
- Catalyst 9300

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

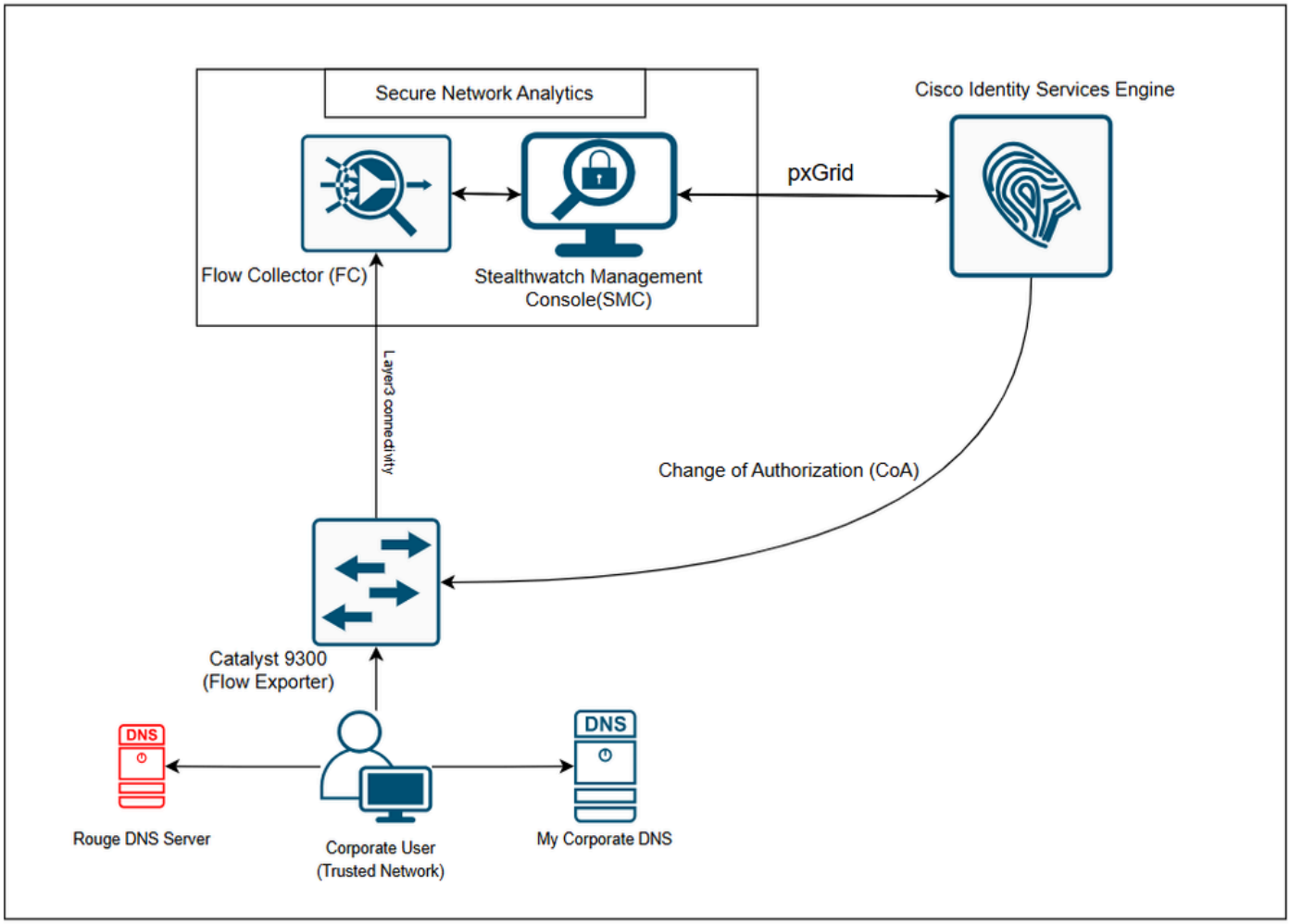
Cisco Secure Cloud Analytics (ora parte di Cisco XDR) può recuperare i dati di attribuzione degli utenti da Cisco Identity Services Engine (ISE) utilizzando pxGrid. Questa integrazione consente il reporting delle attività degli utenti nel Visualizzatore eventi di Secure Cloud Analytics.

La combinazione di Secure Network Analytics (in precedenza Stealthwatch) e Cisco Identity Services Engine (ISE) consente alle organizzazioni di avere una visione a 360°, rispondere più rapidamente alle minacce e proteggere un business digitale in crescita. Dopo che Secure Network Analytics ha rilevato un traffico anomalo, emette un avviso, offrendo all'amministratore la possibilità di mettere in quarantena l'utente. pxGrid consente a Secure Network Analytics di consegnare il comando di quarantena direttamente a Identity Services Engine.

In questo esempio viene descritto come utilizzare il server DNS aziendale per proteggersi dalle minacce provenienti da Internet. L'obiettivo è stabilire un meccanismo di avviso personalizzato che venga attivato quando gli utenti interni si connettono a server DNS esterni. Questa iniziativa è stata progettata per bloccare le connessioni a server DNS non autorizzati che potrebbero reindirizzare il traffico a siti esterni dannosi.

Quando viene attivato un avviso, Cisco Secure Network Analytics coordina con Cisco ISE la quarantena dell'host che accede ai server DNS non autorizzati, utilizzando un criterio di controllo di rete adattivo tramite PxGrid.

Esempio di rete



Come illustrato nel diagramma:

- Un utente aziendale è connesso a uno switch C9300 configurato per esportare i flussi IP e inviare i dati al Flow Collector.
- Lo stesso utente aziendale è configurato per i server DNS aziendali degli utenti.
- Flow Collector è integrato con Stealthwatch Management Console (SMC)
- Stealthwatch Management Console (SMC) integrata tramite Pxgrid con ISE.

Configurazione dettagliata

1. Preparare lo switch per monitorare ed esportare i flussi utilizzando netflow.

Configurazione del flusso di base su uno switch C9300 con 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
```

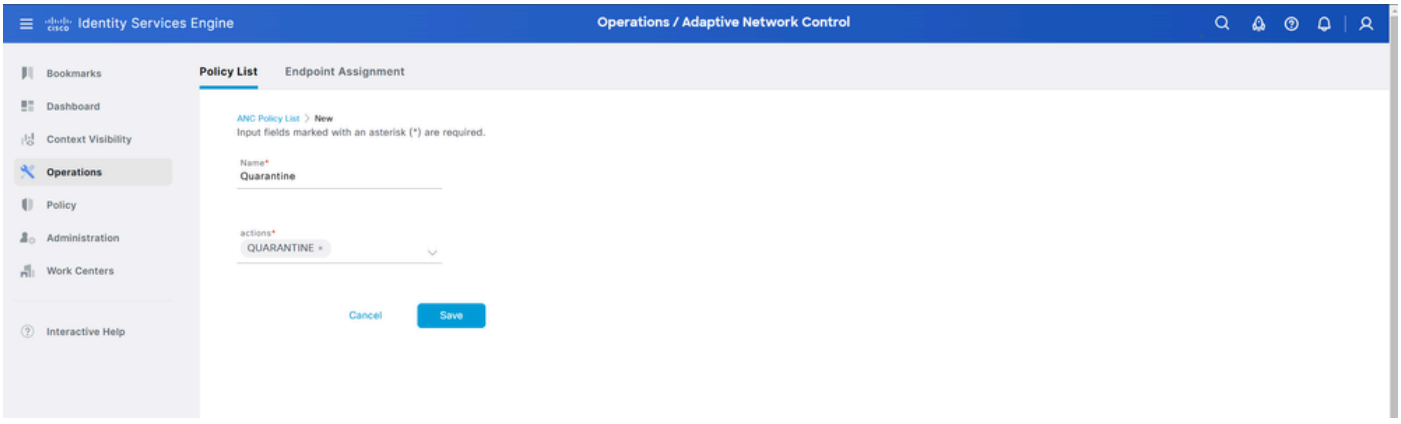
```
  collect transport tcp flags
  collect interface output
  collect counter bytes long
  collect counter packets long
  collect timestamp absolute first
  collect timestamp absolute last


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
```

Al termine della configurazione, consente al C9300 di esportare i dati del flusso IP nel Flow Collector. Flow Collector elabora e trasferisce questi dati a Stealthwatch Management Console (SMC) per l'analisi e il monitoraggio.

2. EnableAdaptive Network Control in Cisco ISE.

ANC è disattivato per impostazione predefinita. ANC viene abilitato solo quando pxGrid è abilitato e rimane abilitato finché il servizio non viene disabilitato manualmente nel portale di amministrazione.

Selezionare Operazioni > Adaptive Network Control > Elenco criteri > Aggiungi, quindi immettere Quarantena per Nome criterio e Quarantena per Azione.

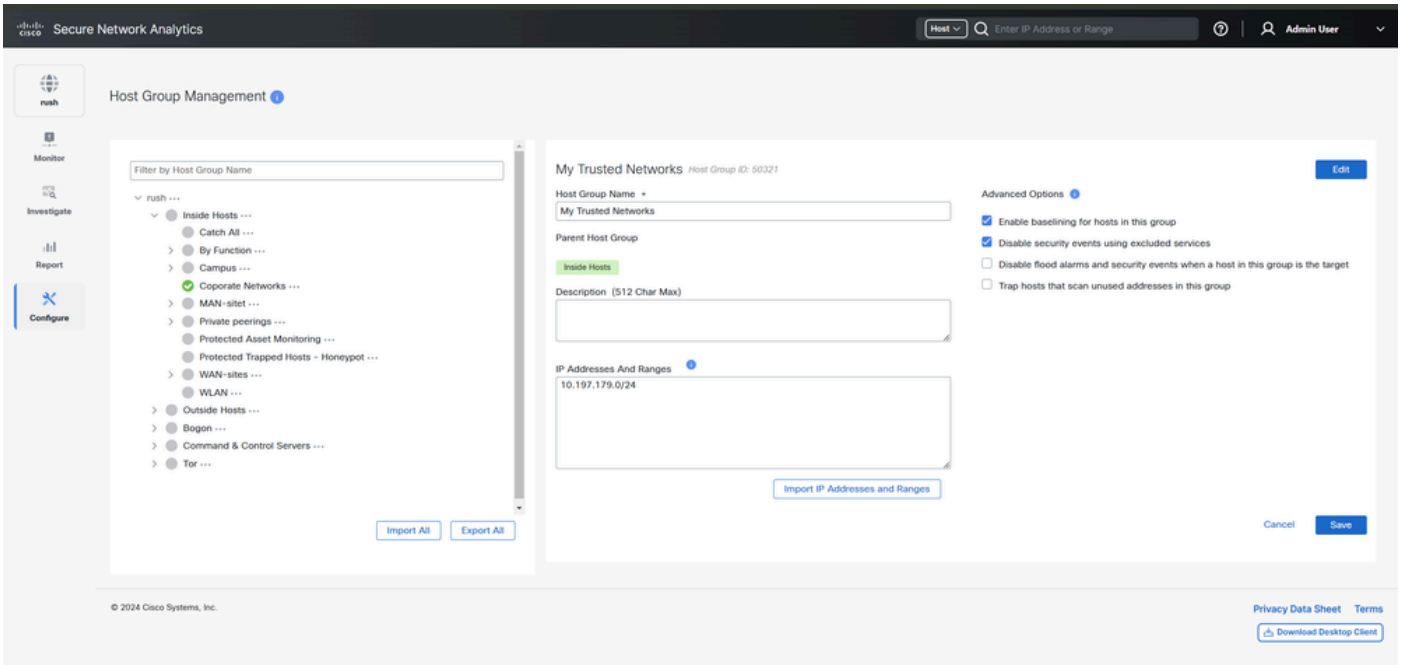


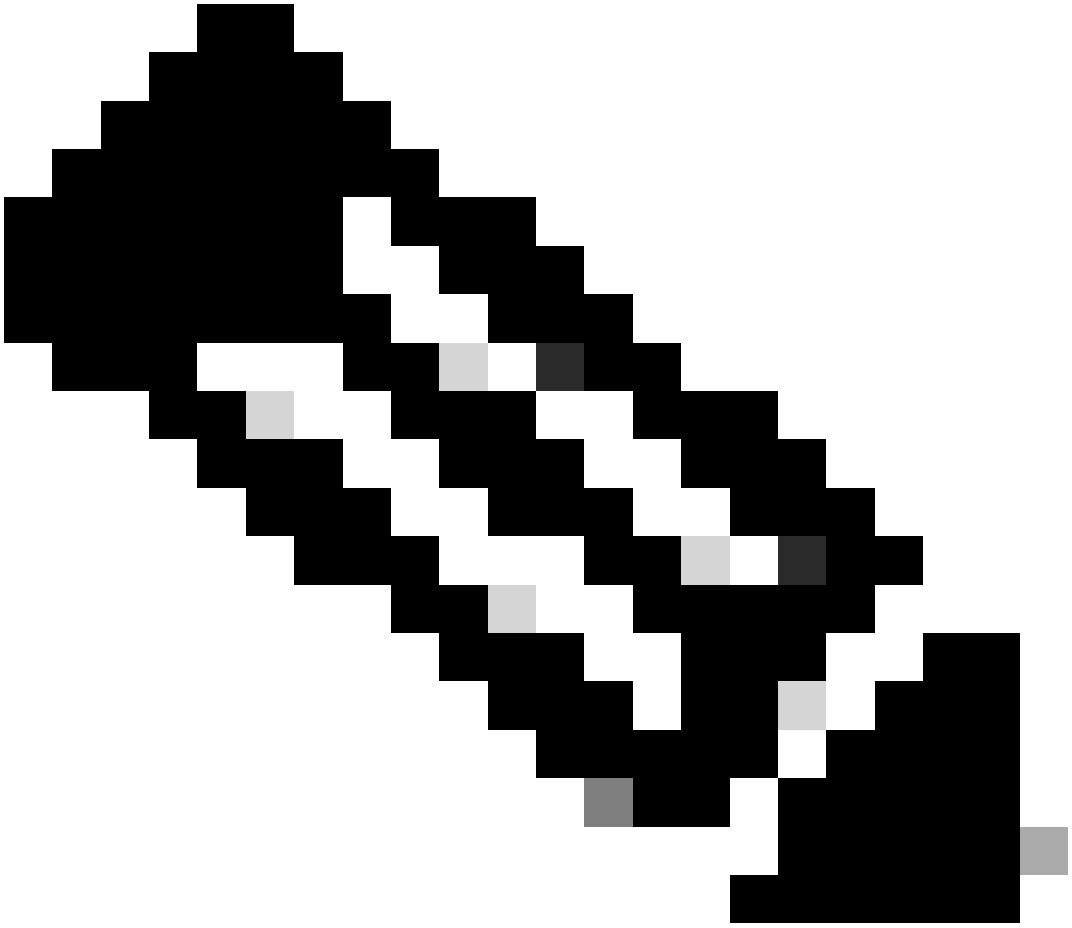
3. Configurare Secure Network Analytics per Event Trigger and Response Management per il contenimento rapido delle minacce.

Passaggio 1: Accedere alla GUI di SMC e selezionare Configura > Rilevamento > Gestione gruppo host > Fare clic sull'icona (...) (puntini di sospensione) accanto a Host interni, quindi selezionare Aggiungi gruppo host.

In questo esempio, viene creato un nuovo gruppo host denominato Reti attendibili (My Trusted Networks) nel gruppo host padre degli host interni.

Questa rete può essere in genere assegnata al computer dell'utente finale per il monitoraggio dell'utilizzo di DNS.

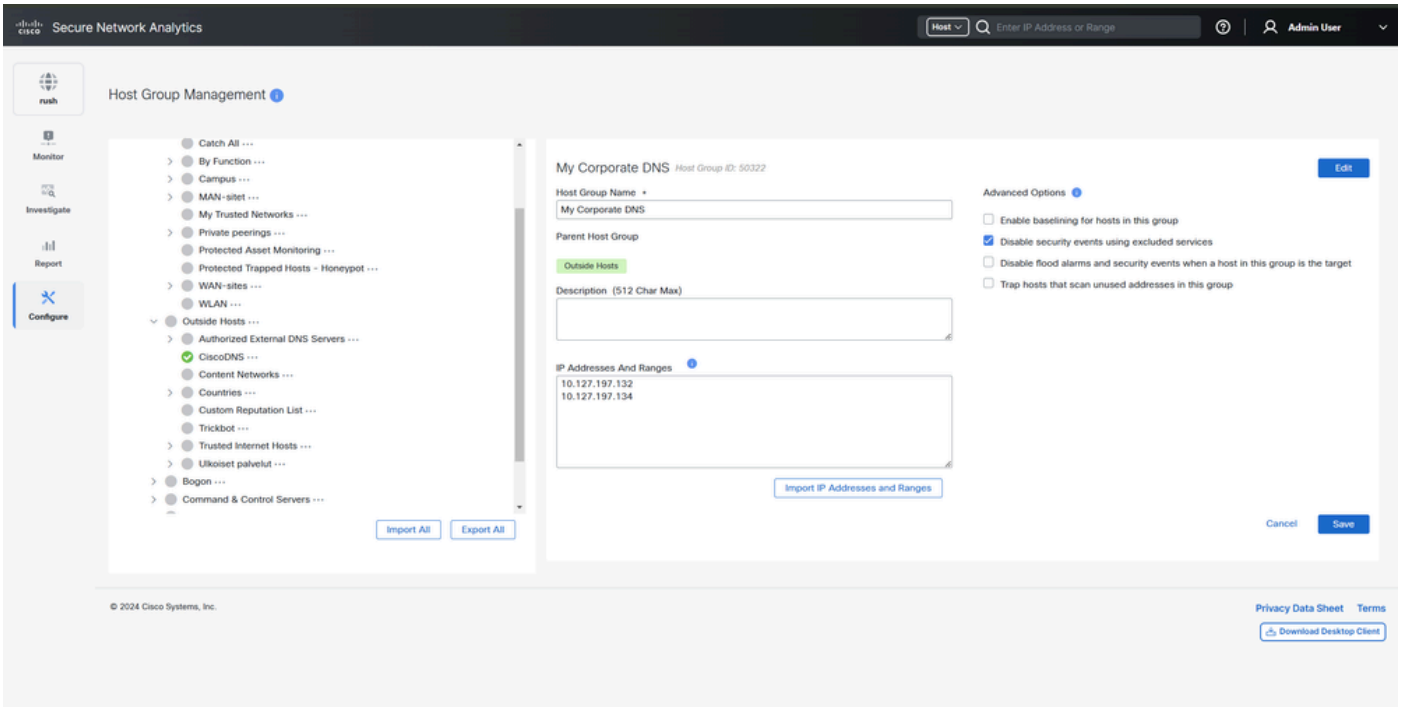


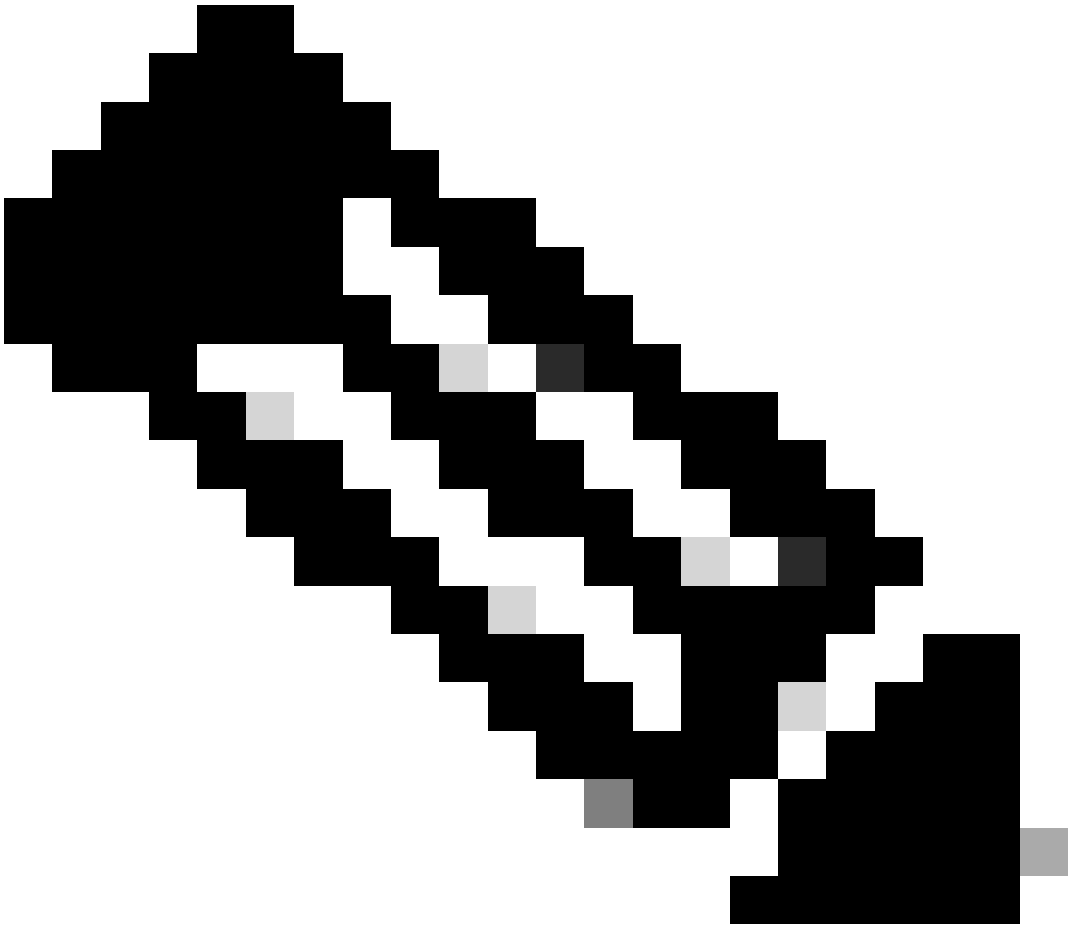


Nota: Nell'esempio, la subnet IP 10.197.179.0/24 viene usata come subnet LAN (Local Area Network). Può variare nell'ambiente di rete effettivo, a seconda dell'architettura di rete.

Passaggio 2: Accedere alla GUI di SMC e selezionare Configura > Rilevamento > Gestione gruppo host > Fare clic su (...) oltre agli host esterni e selezionare Aggiungi gruppo host.

In questo esempio viene creato un nuovo gruppo host denominato My Corporate DNS nel gruppo host padre di host esterni.

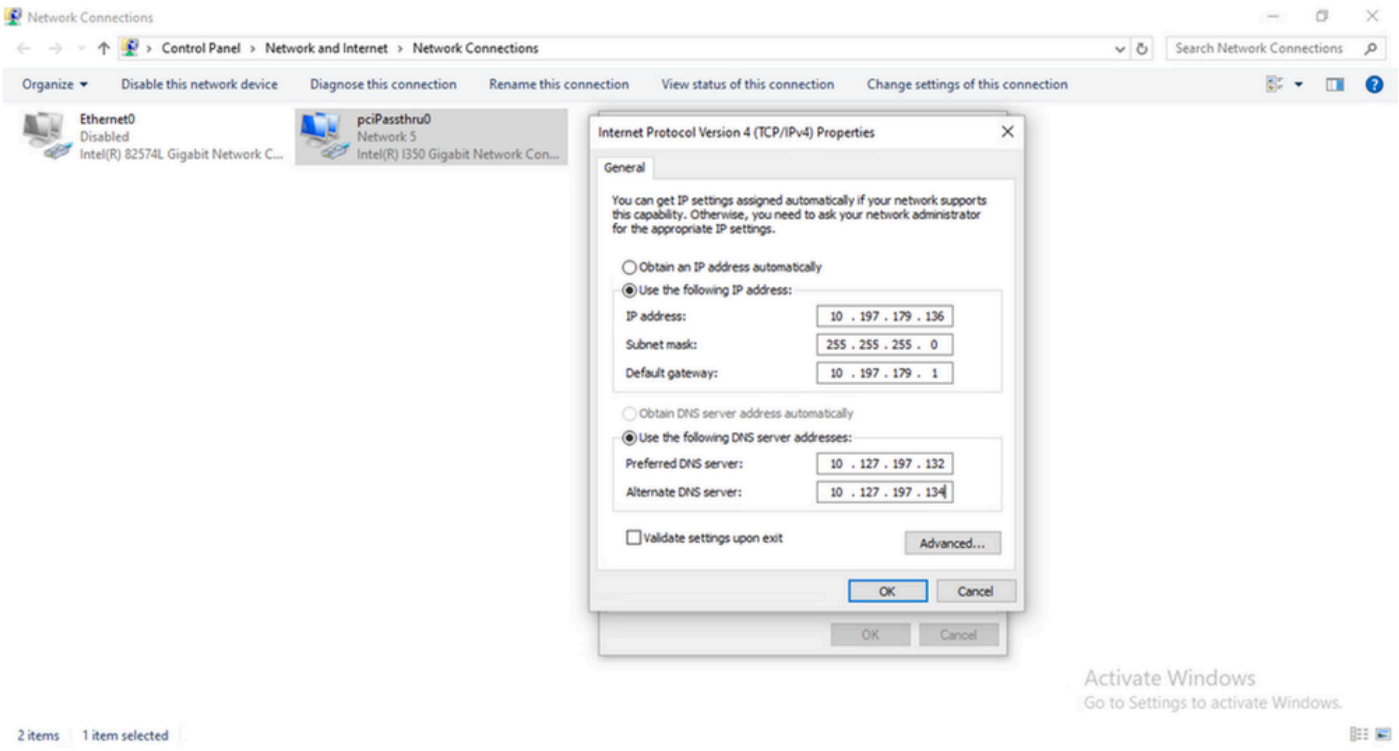




Nota: Nell'esempio, gli indirizzi IP 10.127.197.132 e 10.127.197.134 vengono utilizzati

come server DNS desiderati dagli utenti finali. Questa impostazione può variare nell'ambiente di rete effettivo, a seconda dell'architettura di rete.

Il PC del laboratorio di prova utilizzato per la dimostrazione è configurato con IP statico 10.197.179.136 (appartenente al gruppo host Reti trusted creato) e DNS 10.127.197.132 e 10.127.197.134 (appartenente al gruppo host DNS aziendale creato).



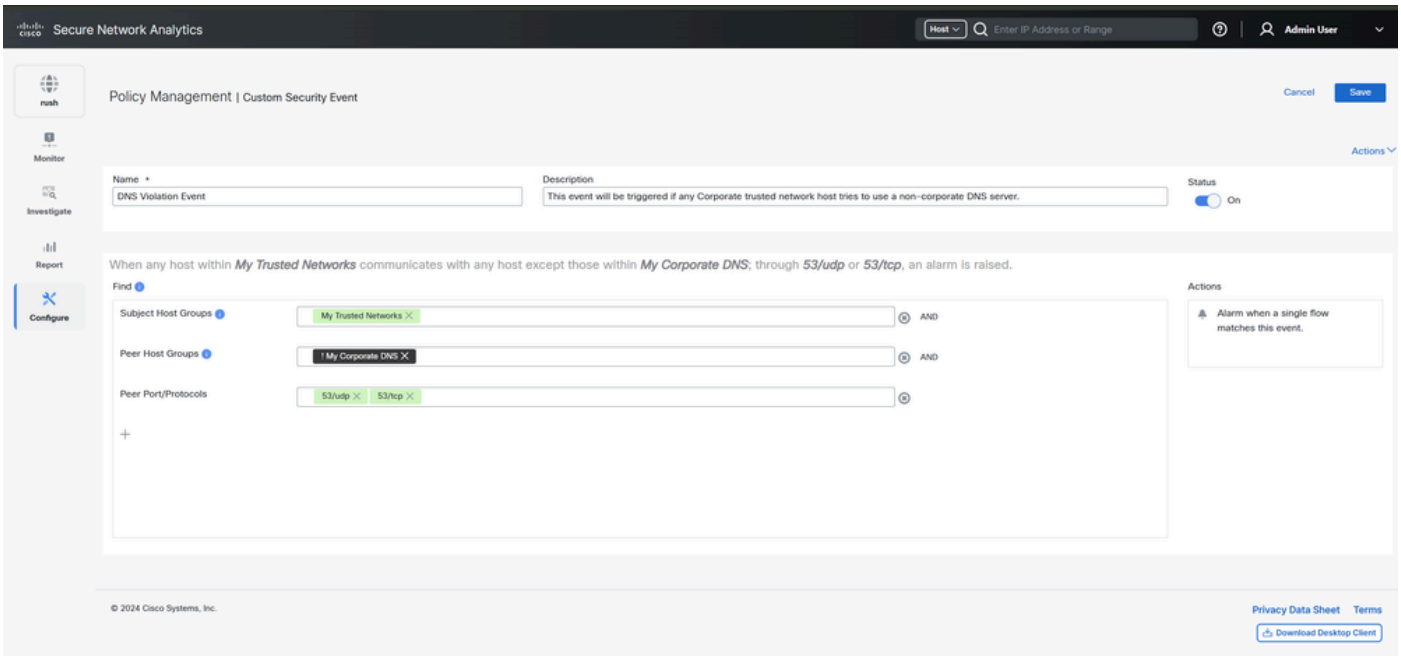
Passaggio 3: Configurare un sistema di avvisi personalizzato per rilevare quando gli utenti interni si connettono a server DNS esterni, attivando un allarme per bloccare le connessioni a server DNS non autorizzati che potrebbero reindirizzare il traffico a siti esterni dannosi. Dopo l'attivazione di un allarme, Cisco Secure Network Analytics si coordina con Cisco ISE per isolare l'host utilizzando questi server DNS non autorizzati, utilizzando Adaptive Network Control Policy tramite PxGrid.

Passare a Configura > Gestione delle policy.

Creare un evento personalizzato con le informazioni seguenti:

- Name :Evento di violazione DNS.
- Gruppi di host: Reti attendibili.
- Gruppi host peer: (No) Il mio DNS aziendale.
- Protocolli/porte peer: 53/UDP 53/TCP

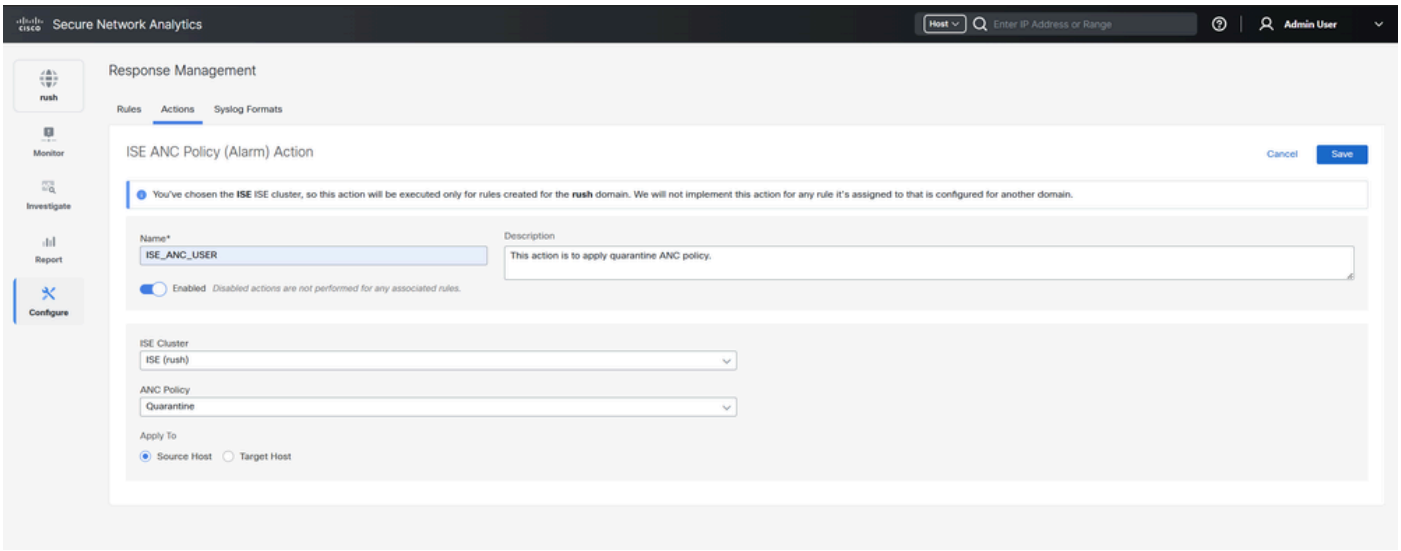
Ciò significa che quando un host all'interno di Reti attendibili (gruppo host) comunica con un host diverso da quelli all'interno di DNS aziendali (gruppo host) tramite 53/up o 53/tcp, viene generato un allarme.



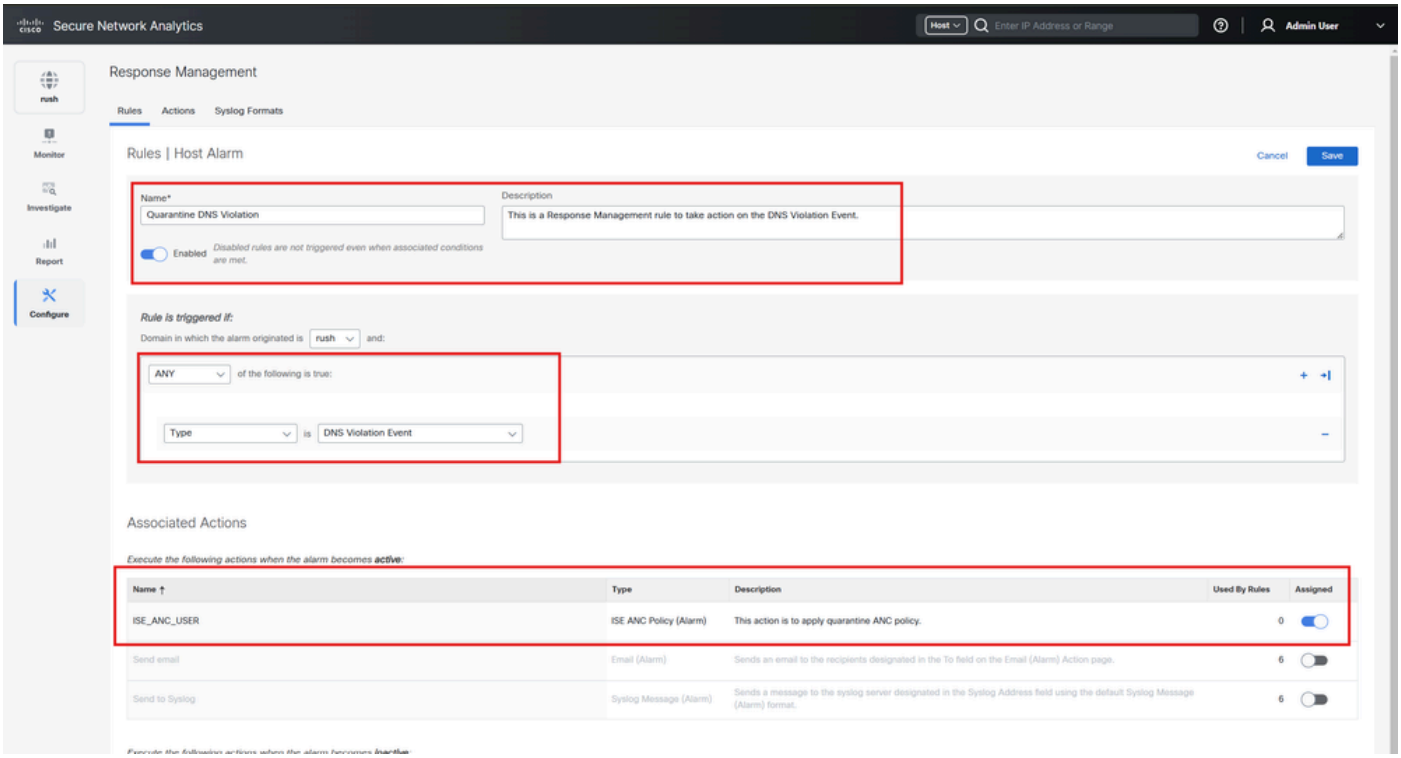
Passaggio 4: Configurare un'azione di Response Management da eseguire e che può essere successivamente applicata alla regola di Response Management dopo la creazione.

Selezionare Configure > Response Management > Actions, fare clic su Add New Action e selezionare ISE ANC Policy (Alarm).

Assegnare un nome e scegliere il cluster Cisco ISE specifico a cui inviare la notifica per implementare un criterio di quarantena per qualsiasi violazione o connessione a server non autorizzati.



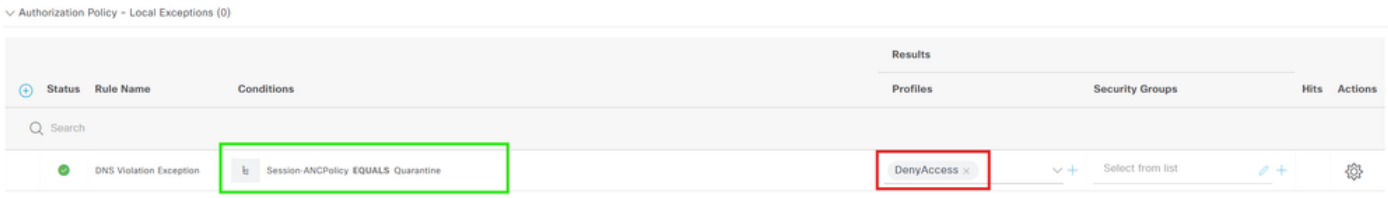
Passaggio 5: nella sezione Regole, Creare una nuova regola. Questa regola applica l'azione definita in precedenza ogni volta che un host della rete interna tenta di inviare traffico DNS a server DNS non autorizzati. Nella sezione Regola viene attivata se, scegliere Tipo e selezionare l'evento personalizzato creato in precedenza.
In Azioni associate, selezionare l'azione ISE ANC Alarm precedentemente configurata.

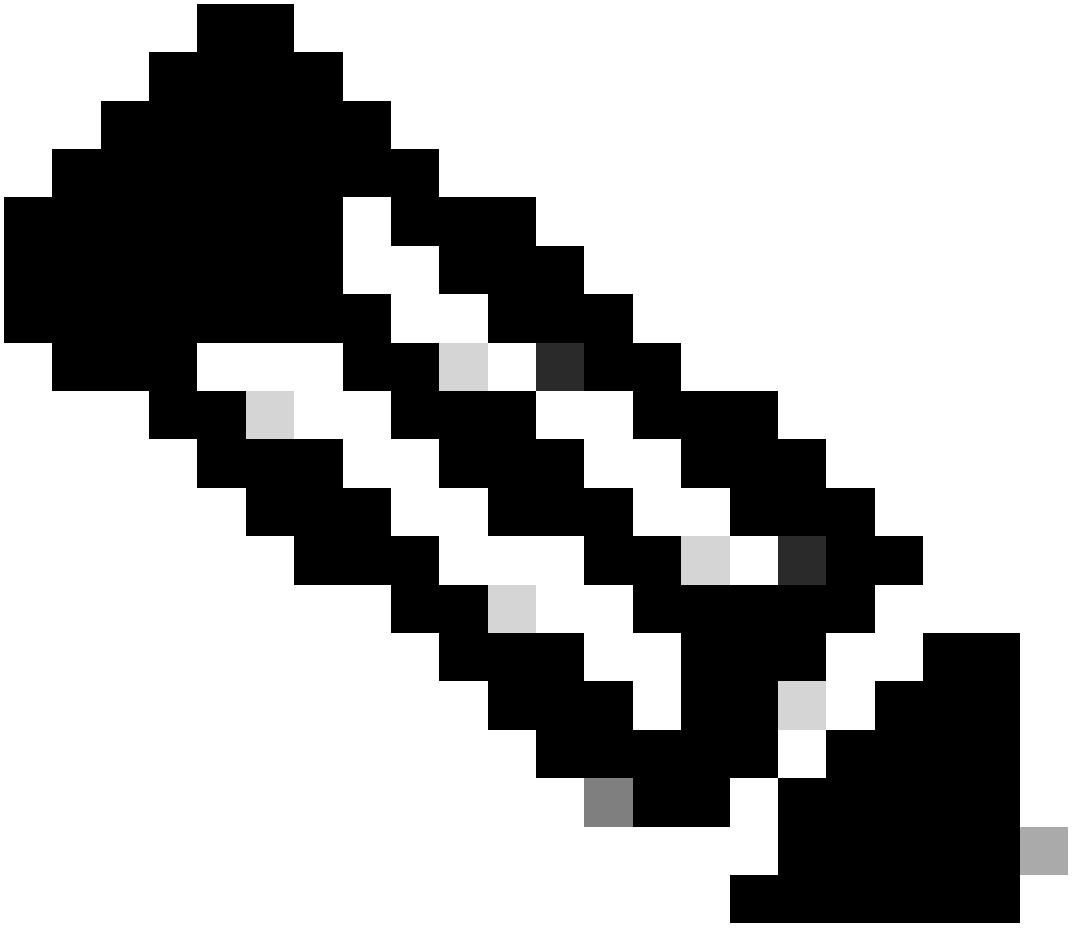


4. Configurare Cisco ISE in modo che risponda alle azioni avviate da Stealthwatch all'attivazione dell'evento.

Accedere alla GUI di Cisco ISE e selezionare Policy > Policy Sets > Choose the Policy set > in Authorization Policy - Local Exceptions > Create new Policy.

- Nome: Eccezione di violazione DNS
- Condizioni: Sessione: ANCPolicy è uguale a quarantena
- Profili di autorizzazione: NegaAccesso

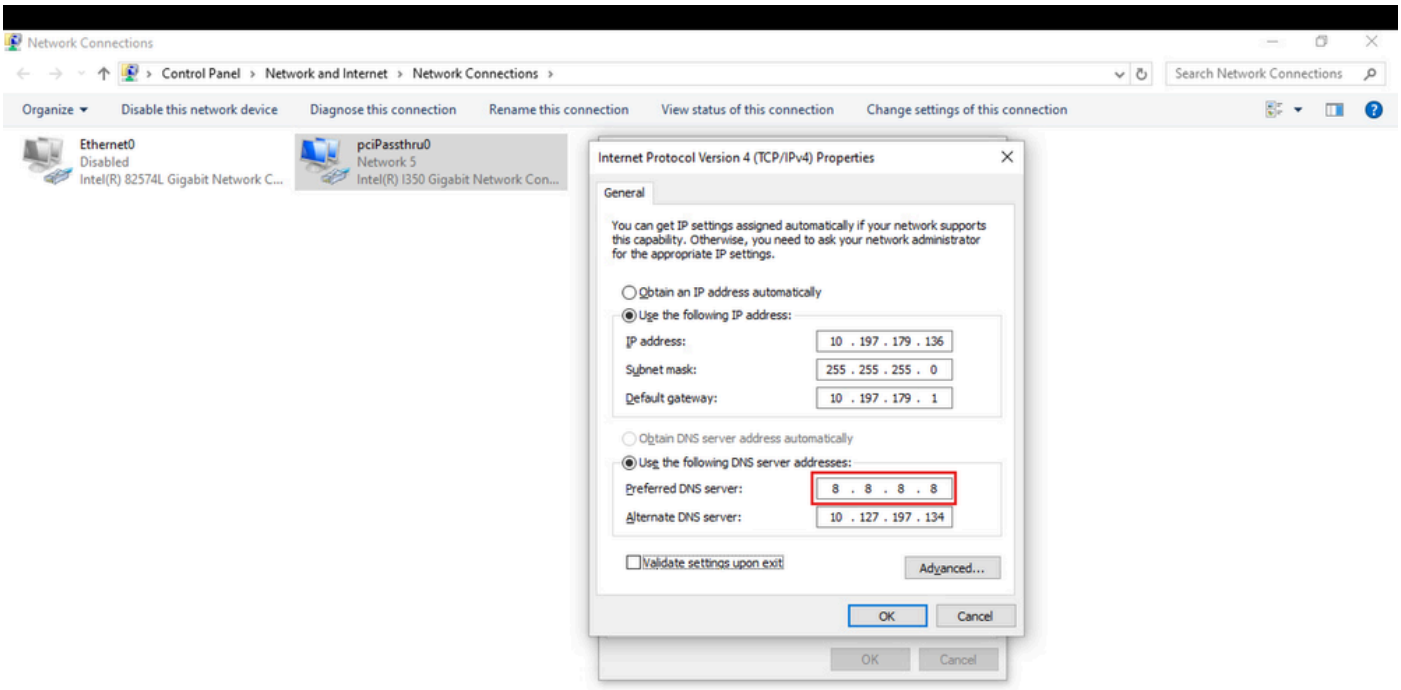




Nota: In questo esempio, quando viene attivato l'evento di violazione DNS, l'accesso viene negato all'utente in base alla configurazione

Verifica

Per dimostrare lo Use Case, la voce DNS sull'endpoint è stata modificata in 8.8.8.8, attivando l'evento di violazione DNS configurato. Poiché il server DNS non appartiene al gruppo host dei server DNS aziendali, viene attivato l'evento che genera un accesso negato all'endpoint.



Sullo switch C9300, verificare l'utilizzo della cache IPv4_NETFLOW di show flow monitor | nel comando 8.8.8 con l'output per verificare che i flussi vengano acquisiti e inviati al Flow Collector. IPv4_NETFLOW è configurato nella configurazione dello switch.

<#root>

IPV4 SOURCE ADDRESS:

10.197.179.136

IPV4 DESTINATION ADDRESS:

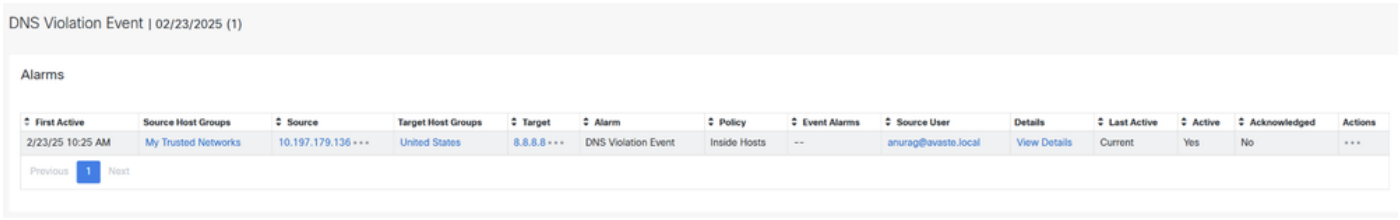
8.8.8.8

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

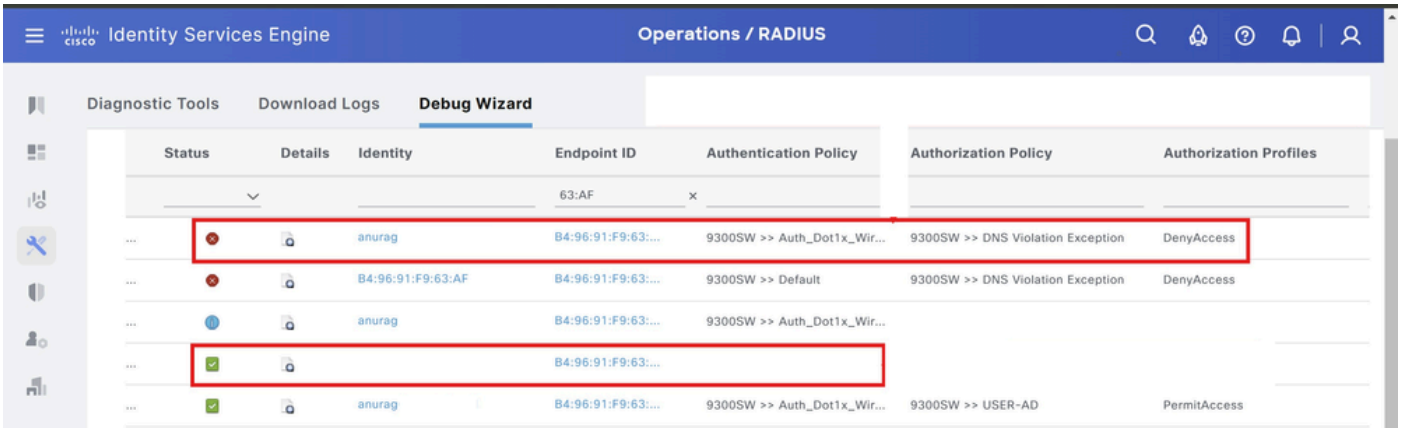
Una volta che l'evento è stato attivato su Stealthwatch, passare a Monitor > Security Insight Dashboard,.



Selezionare Monitor > Integrazione > Assegnazioni criteri ISE ANC.

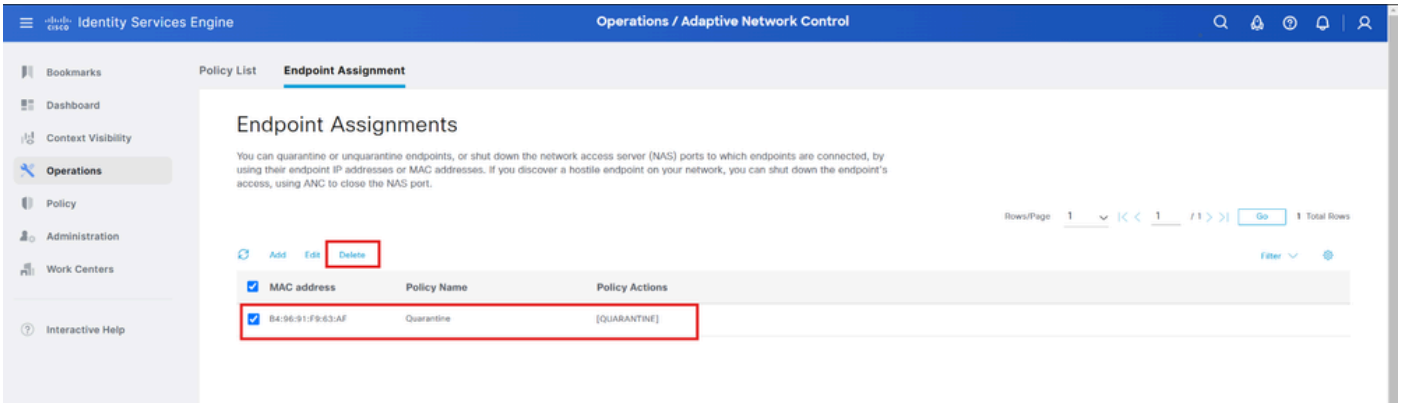
Verificare che Cisco Secure Network Analytics abbia implementato correttamente la policy di controllo di rete adattiva tramite PxGrid e Cisco ISE per mettere in quarantena l'host.

Analogamente, in Cisco ISE, selezionare Operations > RADIUS > Livelogs e applicare il filtro per l'endpoint.



In base al criterio di eccezione locale Eccezione violazione DNS, la modifica dell'autorizzazione (CoA) viene emessa da ISE e l'accesso a ISE viene negato all'endpoint.

Una volta eseguite le azioni di correzione sull'endpoint, rimuovere l'indirizzo MAC da Operazioni > Adaptive Network Control > Assegnazioni endpoint > Elimina per rimuovere l'indirizzo MAC dell'endpoint.



Log Reference su Cisco ISE.

Attributi impostati su TRACE level per il componente pxgrid (pxgrid-server.log) in Cisco ISE, i log sono visualizzati nel file 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

"}

Risoluzione dei problemi

Gli endpoint in quarantena non rinnovano l'autenticazione dopo la modifica dei criteri

Problema

Autenticazione non riuscita a causa della modifica dei criteri o di un'identità aggiuntiva e non è in corso alcuna riautenticazione. L'autenticazione non riesce o l'endpoint in questione non riesce a connettersi alla rete. Questo problema si verifica spesso nei computer client che non riescono a valutare la postura in base ai criteri di postura assegnati al ruolo utente.

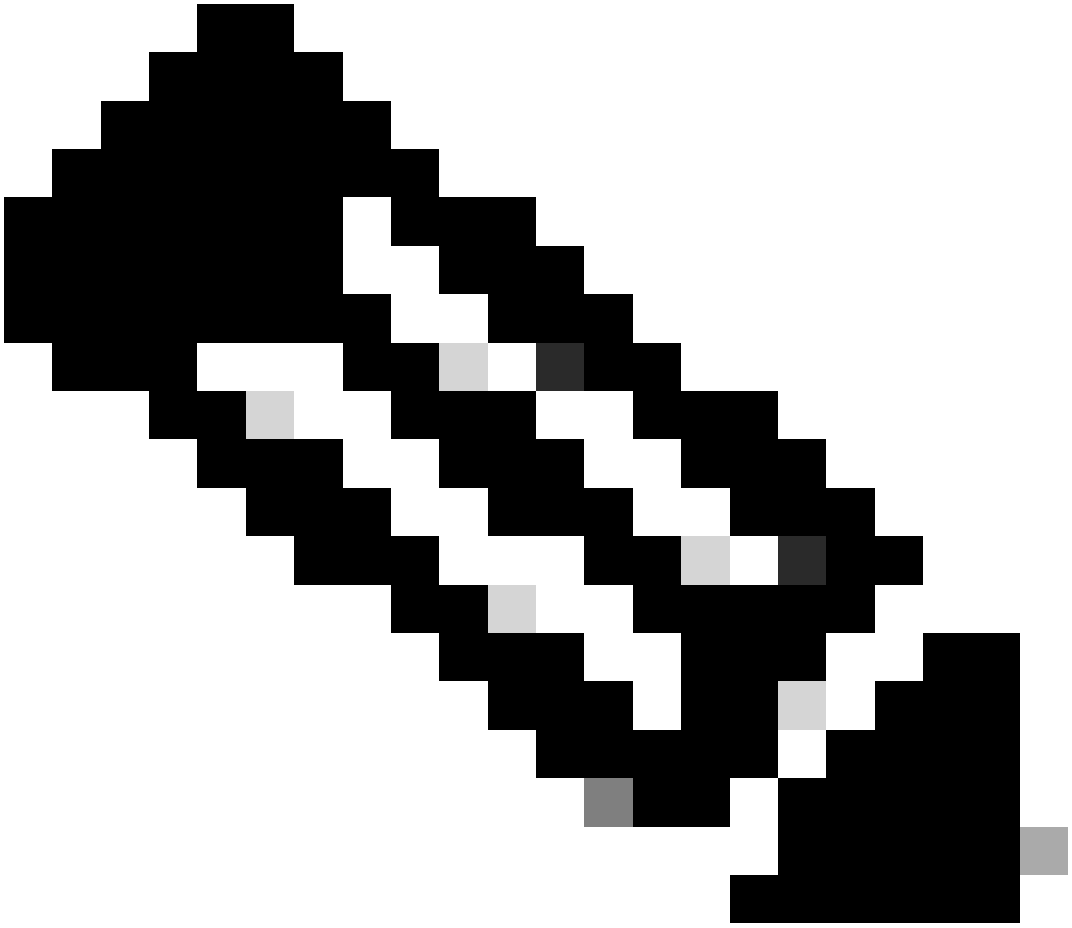
Possibili cause

L'impostazione del timer di autenticazione non è impostata correttamente sul computer client oppure l'intervallo di autenticazione sullo switch non è impostato correttamente.

Soluzione

Per questo problema esistono diverse soluzioni possibili:

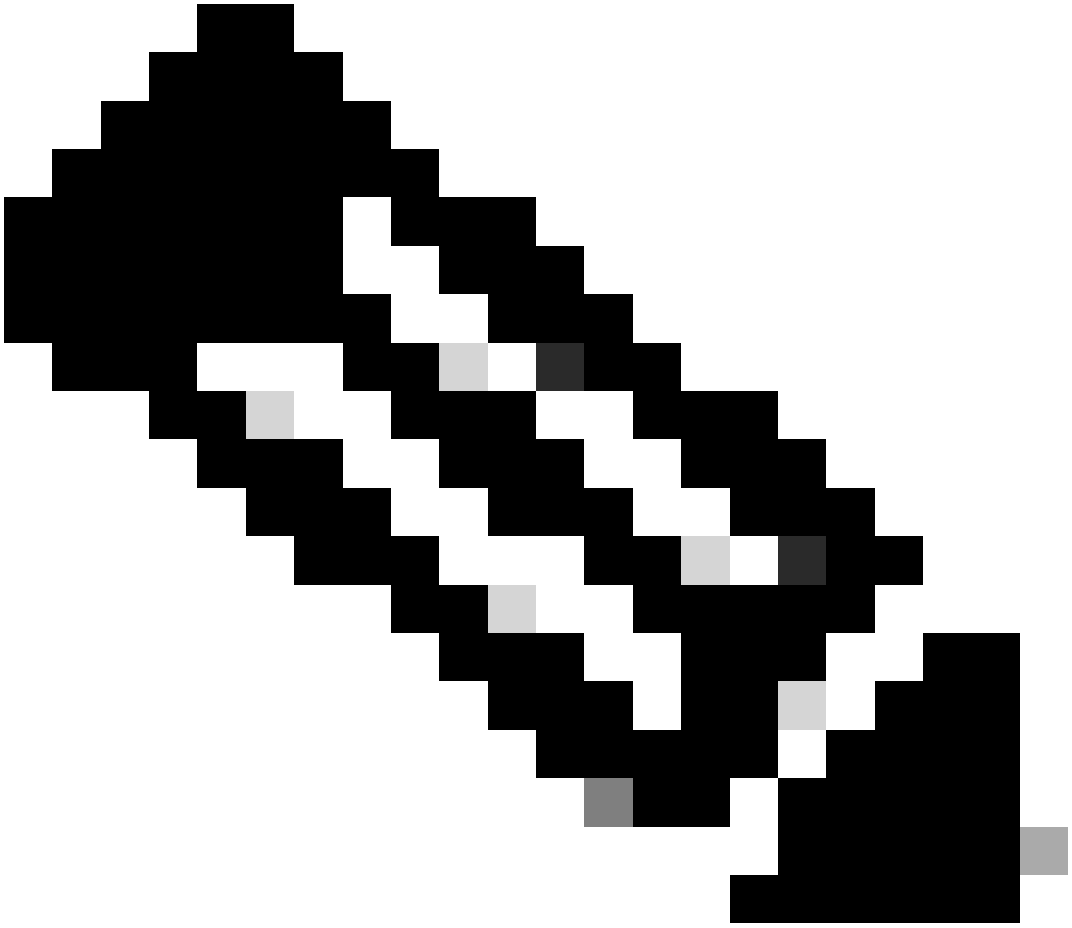
1. Controllare il report di riepilogo sullo stato della sessione in Cisco ISE per lo switch o l'NAD specificato e verificare che per l'interfaccia sia configurato l'intervallo di autenticazione appropriato.
2. Immettere show running configuration sul server NAD/switch e verificare che l'interfaccia sia configurata con un'impostazione di riavvio del timer di autenticazione appropriata. (ad esempio, il timer di autenticazione riavvia il sistema 15 e il timer di autenticazione riautentica il sistema 15).
3. Accedere a interface shutdown e no shutdown per riavviare la porta sull'NAD/switch e forzare la riautenticazione e la potenziale modifica della configurazione in Cisco ISE.



Nota: Poiché CoA richiede un indirizzo MAC o un ID sessione, si consiglia di non riavviare la porta mostrata nel report SNMP del dispositivo di rete.

Operazioni ANC non riuscite quando non viene trovato l'indirizzo IP o MAC

Un'operazione ANCoperation eseguita su un endpoint non riesce quando una sessione attiva per l'endpoint non contiene informazioni sull'indirizzo IP. Ciò è valido anche per l'indirizzo MAC e l'ID sessione per l'endpoint.



Nota: Per modificare lo stato di autorizzazione di un endpoint tramite ANC, è necessario specificare l'indirizzo IP o l'indirizzo MAC dell'endpoint. Se l'indirizzo IP o l'indirizzo MAC non viene trovato nella sessione attiva per l'endpoint, viene visualizzato il messaggio di errore: "Nessuna sessione attiva trovata per questo indirizzo MAC, indirizzo IP o ID sessione".

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).