Confronta le versioni precedenti di ISE con ISE Posture Flow in ISE 2.2

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Flusso di postura prima di ISE 2.2](#)
[Posture Flow in ISE 2.2](#)
[Configurazione](#)
[Esempio di rete](#)
[Configurazioni](#)
[Configurazione provisioning client](#)
[Criteri e condizioni di postura](#)
[Configurazione del portale di provisioning client](#)
[Configura profili e criteri di autorizzazione](#)
[Verifica](#)
[Risoluzione dei problemi](#)
[Informazioni generali](#)
[Risoluzione dei problemi comuni](#)
[Problemi correlati a SSO](#)
[Risoluzione dei problemi relativi alla selezione dei criteri di provisioning client](#)
[Risoluzione dei problemi relativi al processo di postura](#)

Introduzione

Questo documento descrive il confronto tra il flusso di postura in ISE 2.2 e il flusso di postura nelle versioni ISE precedenti alla 2.2.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Flusso di postura su ISE
- Configurazione dei componenti di postura su ISE
- Configurazione ASA (Adaptive Security Appliance) per la postura sulle reti VPN (Virtual Private Network)

Componenti usati

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

- Cisco ISE versione 2.2
- Cisco ASAv con software 9.6 (2)

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

Questo documento descrive una nuova funzionalità di Identity Service Engine (ISE) 2.2 che consente ad ISE di supportare un flusso di postura senza alcun tipo di supporto di reindirizzamento su un dispositivo NAD (Network Access Device) o ISE.

La postura è un componente chiave di Cisco ISE. La postura come componente può essere rappresentata da tre elementi principali:

1. ISE come punto di distribuzione e di decisione per la configurazione delle policy.
   Dal punto di vista dell'amministratore di ISE, è possibile configurare le policy di postura (quali condizioni esatte devono essere soddisfatte per contrassegnare un dispositivo come conforme a livello aziendale), le policy di provisioning dei client (quale software agente deve essere installato su quale tipo di dispositivi) e le policy di autorizzazione (a quale tipo di autorizzazioni deve essere assegnato, a seconda dello stato della postura).
2. Un dispositivo di accesso alla rete come punto di imposizione dei criteri.
   Sul lato AND, le restrizioni effettive all'autorizzazione vengono applicate al momento dell'autenticazione dell'utente. ISE è un policy point che fornisce parametri di autorizzazione come ACL (dACL) scaricati/VLAN/Redirect-URL/Redirect Access Control List (ACL). In genere, affinché la postura venga eseguita, i servizi NAD devono supportare il reindirizzamento (per indicare all'utente o all'agente il software a cui deve essere contattato il nodo ISE) e la funzione di modifica dell'autorizzazione (CoA) per riautenticare l'utente dopo aver determinato lo stato di postura dell'endpoint.
3. Il software agente come punto di raccolta dei dati e di interazione con l'utente finale.
   Cisco ISE utilizza tre tipi di software agente: AnyConnect ISE Posture Module, NAC Agent e Web Agent. L'agente riceve informazioni sui requisiti di postura dall'ISE e fornisce all'ISE un report sullo stato dei requisiti.

> **Nota**: questo documento si basa sul modulo Anyconnect ISE Posture, l'unico che supporta completamente la postura senza reindirizzamento.

Nella postura di flusso precedente alla versione ISE 2.2, gli NAD vengono utilizzati non solo per autenticare gli utenti e limitare l'accesso, ma anche per fornire informazioni all'agente software su uno specifico nodo ISE che deve essere contattato. Come parte del processo di reindirizzamento, le informazioni sul nodo ISE vengono restituite al software dell'agente.

Storicamente, il supporto per il reindirizzamento su NAD o sul lato ISE era un requisito essenziale per l'implementazione della postura. In ISE 2.2 viene eliminato l'obbligo di supportare il reindirizzamento sia per il provisioning iniziale del client che per il processo di postura.

Provisioning dei client senza reindirizzamento: in ISE 2.2 è possibile accedere al Client Provisioning Portal (CPP) direttamente tramite il portale FQDN (Fully Qualified Domain Name). È simile alla modalità di accesso al portale degli sponsor o al portale MyDevice.

Processo di postura senza reindirizzamento - Durante l'installazione dell'agente dal portale CPP, le informazioni sui server ISE vengono salvate sul lato client, rendendo possibile la comunicazione diretta.

Flusso di postura prima di ISE 2.2

Nell'immagine viene mostrata una spiegazione dettagliata del flusso di Anyconnect ISE Posture Module prima di ISE 2.2:

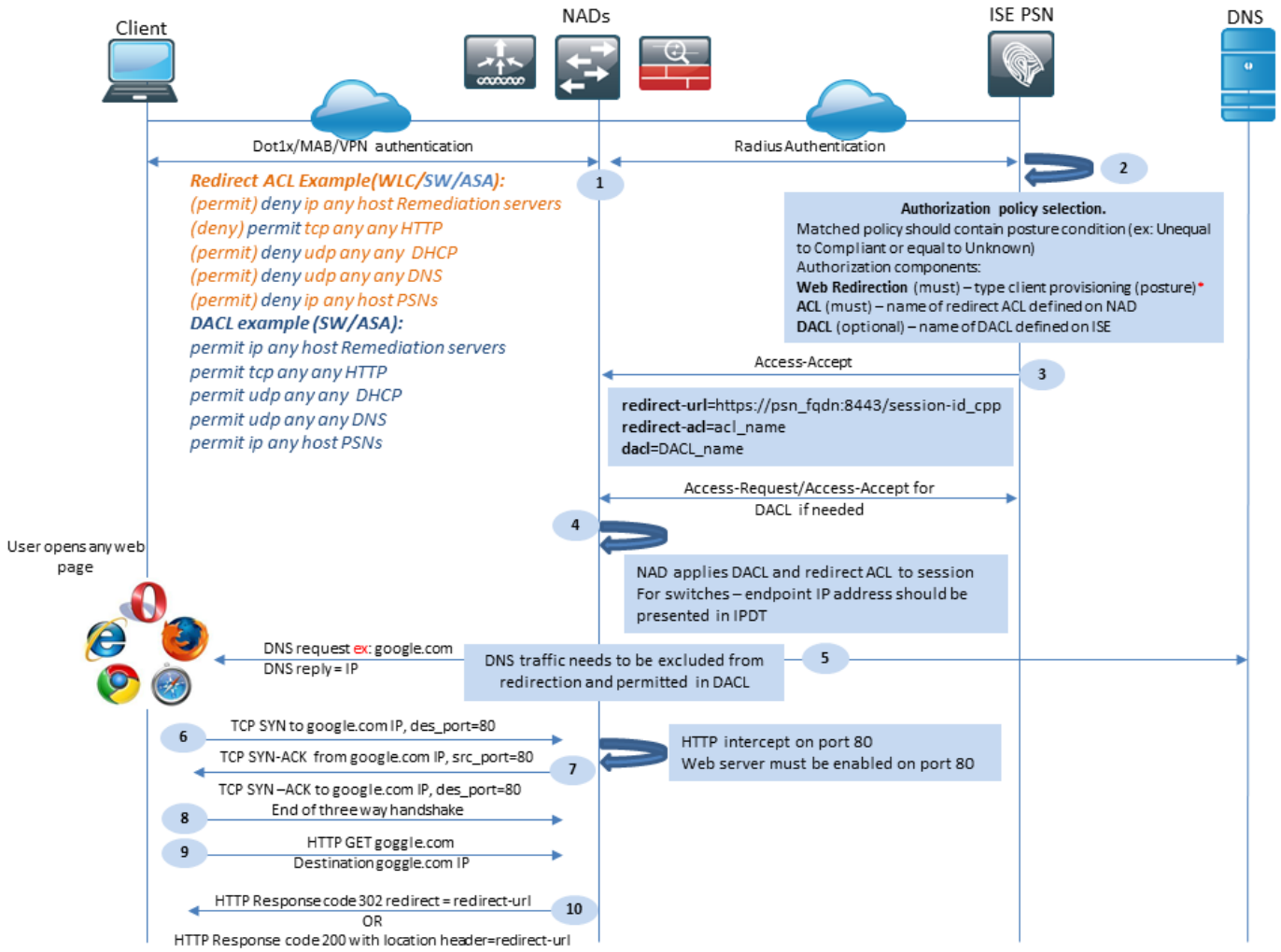

Figura 1-1

Passaggio 1. L'autenticazione è il primo passaggio del flusso e può essere dot1x, MAB o VPN.

Passaggio 2. ISE deve scegliere un criterio di autenticazione e autorizzazione per l'utente. Nello scenario di postura scelto il criterio di autorizzazione deve contenere un riferimento allo stato di

postura, che inizialmente deve essere sconosciuto o non applicabile. Per coprire entrambi i casi, è possibile utilizzare condizioni con stato di postura non conforme.

Il profilo di autorizzazione scelto deve contenere informazioni sul reindirizzamento:

- Reindirizzamento Web: per il case di postura, il tipo di reindirizzamento Web deve essere specificato come provisioning client (postura).
- ACL: questa sezione deve contenere il nome ACL configurato sul lato NAD. Questo ACL viene usato per indicare all'AD il traffico che deve ignorare il reindirizzamento e quale deve essere effettivamente reindirizzato.
- DACL: può essere utilizzato insieme all'elenco degli accessi reindirizzati, ma occorre tenere presente che piattaforme diverse elaborano gli ACL e gli ACL di reindirizzamento in un ordine diverso.

Ad esempio, ASA elabora sempre il DACL prima di reindirizzare l'ACL. Allo stesso tempo, alcune piattaforme di switch lo elaborano allo stesso modo dell'ASA e altre piattaforme di switch elaborano prima l'ACL di reindirizzamento e quindi controllano l'ACL/l'interfaccia se il traffico deve essere interrotto o autorizzato.

> **Nota**: dopo aver abilitato l'opzione di reindirizzamento Web nel profilo di autorizzazione, è necessario scegliere il portale di destinazione per il reindirizzamento.

Passaggio 3. ISE restituisce Access-Accept con attributi di autorizzazione. L'URL di reindirizzamento negli attributi di autorizzazione viene generato automaticamente da ISE. Contiene i seguenti componenti:

- FQDN del nodo ISE in cui è stata eseguita l'autenticazione. In alcuni casi, l'FQDN dinamico può essere sovrascritto dalla configurazione del profilo di autorizzazione (IP statico/nome host/FQDN) nella sezione Reindirizzamento Web. Se si utilizza il valore statico, questo deve puntare allo stesso nodo ISE in cui è stata elaborata l'autenticazione. Nel caso di Load Balancer (LB), questo FQDN può puntare a LB VIP, ma solo nel caso in cui LB è configurato per collegare connessioni Radius e SSL.
- Porta: il valore della porta viene ottenuto dalla configurazione del portale di destinazione.
- ID sessione: questo valore viene ricavato da ISE dall'ID della sessione di verifica della coppia Cisco AV presentato in Access-Request. Il valore stesso viene generato in modo dinamico da NAD.
- ID portale: identificativo del portale di destinazione sul lato ISE.

Passaggio 4. E applica un criterio di autorizzazione alla sessione. Inoltre, se DACL è configurato, il relativo contenuto viene richiesto prima dell'applicazione dei criteri di autorizzazione.

Considerazioni importanti:

- Tutti gli NAD - Il dispositivo deve avere ACL configurato localmente con lo stesso nome di quello ricevuto in Access-Accept come acl di reindirizzamento.
- Switch: l'indirizzo IP del client deve essere visualizzato nell'output di `show authentication session interface details` per applicare correttamente il reindirizzamento e gli ACL. L'indirizzo IP del client viene appreso dalla funzionalità di monitoraggio dei dispositivi IP (IPDT).

Passaggio 5. Il client invia una richiesta DNS per il nome di dominio completo immesso nel

browser Web. In questa fase, il traffico DNS deve ignorare il reindirizzamento e il server DNS deve restituire l'indirizzo IP corretto.

Passaggio 6. Il client invia TCP SYN all'indirizzo IP ricevuto nella risposta DNS. L'indirizzo IP di origine nel pacchetto è l'indirizzo IP del client e l'indirizzo IP di destinazione è l'indirizzo IP della risorsa richiesta. La porta di destinazione è uguale a 80, ad eccezione dei casi in cui nel browser Web del client è configurato un proxy HTTP diretto.

Passaggio 7.NAD intercetta le richieste dei client e prepara i pacchetti SYN-ACK con un IP di origine uguale all'IP della risorsa richiesta, un IP di destinazione uguale all'IP del client e una porta di origine uguale a 80.

Considerazioni importanti:

- I servizi NAD devono disporre di un server HTTP in esecuzione sulla porta su cui il client invia le richieste. Per impostazione predefinita, è la porta 80.
- Se il client utilizza un server Web proxy HTTP diretto, il server HTTP deve essere eseguito sulla porta proxy su NAS. Questo scenario non rientra nell'ambito del documento.
- Nei casi in cui NAD non dispone di un indirizzo IP locale nel client, la subnet SYN-ACK viene inviata con la tabella di routing NAD (in genere tramite l'interfaccia di gestione). In questo scenario, il pacchetto viene instradato sull'infrastruttura L3 e deve essere indirizzato nuovamente al client da un dispositivo upstream L3. Se il dispositivo L3 è un firewall con stato, è necessario specificare un'ulteriore eccezione per questo routing asimmetrico.

Passaggio 8. Il client completa l'handshake TCP a tre vie tramite ACK.

Passaggio 9. HTTP GET per la risorsa di destinazione viene inviato da un client.

Passaggio 10. NAD restituisce un URL di reindirizzamento al client con codice HTTP 302 (pagina spostata). In alcuni casi, il reindirizzamento NAD può essere restituito all'interno del messaggio HTTP 200 OK nell'intestazione del percorso.

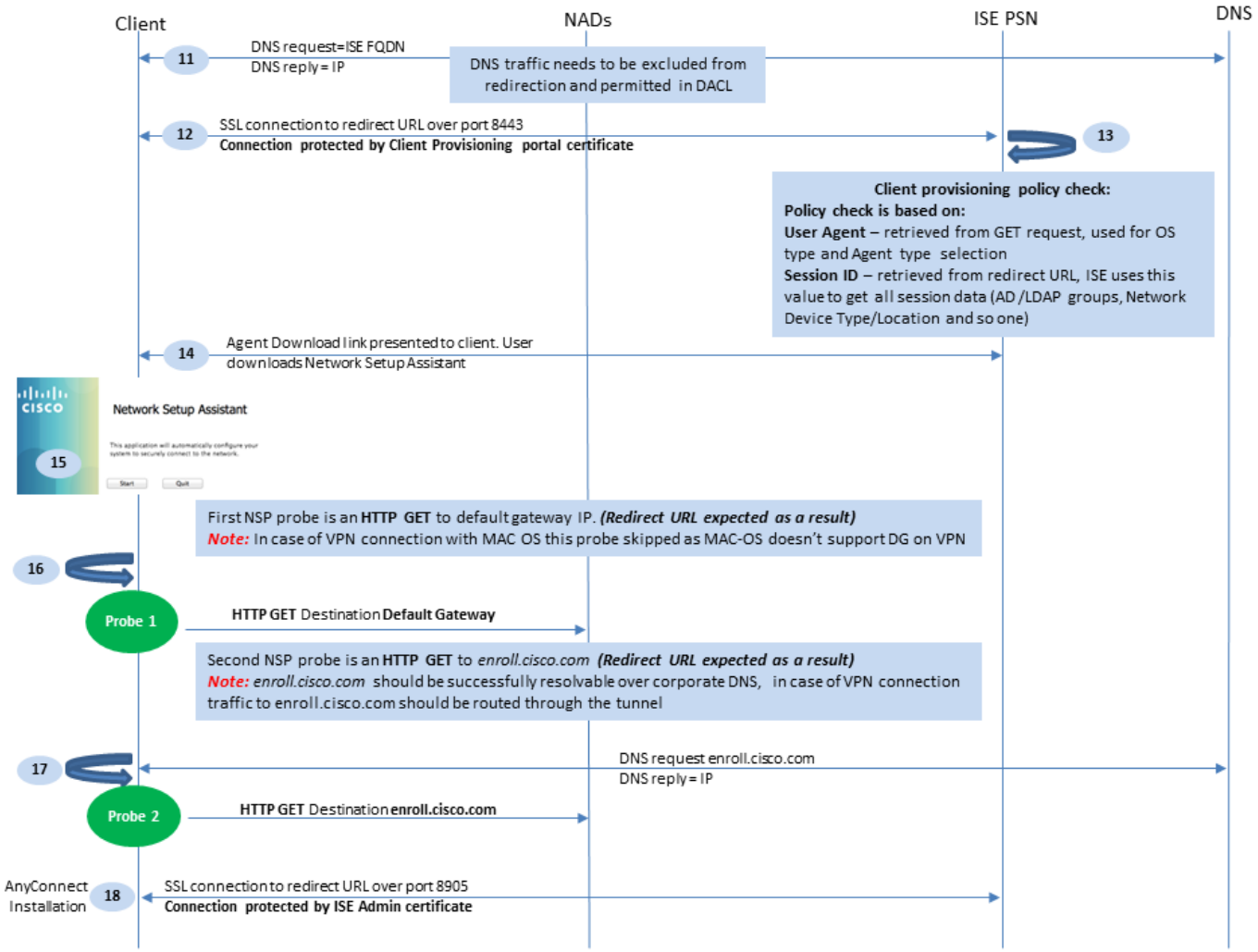

Figura 1-2

Passaggio 11. Il client invia una richiesta DNS per il nome di dominio completo dall'URL di reindirizzamento. Il nome di dominio completo deve essere risolvibile sul lato server DNS.

Passaggio 12. La connessione SSL sulla porta ricevuta nell'URL di reindirizzamento è stabilita (impostazione predefinita: 8443). Questa connessione è protetta da un certificato del portale dal lato ISE. Il portale di provisioning client (CPP) viene presentato all'utente.

Passaggio 13. Prima di fornire un'opzione di download al client, ISE deve scegliere la policy di provisioning del client di destinazione. Il sistema operativo (OS) del client rilevato dall'agente utente del browser e le altre informazioni necessarie per la selezione dei criteri CPP vengono recuperate dalla sessione di autenticazione (come i gruppi AD/LDAP e così via). ISE conosce la sessione di destinazione dall'ID sessione presentato nell'URL di reindirizzamento.

Passaggio 14. Il collegamento di download di Network Setup Assistant (NSA) viene restituito al client. Il client scarica l'applicazione.

> **Nota**: Normalmente, l'NSA fa parte del flusso BYOD per Windows e Android, ma questa applicazione può essere utilizzata anche per installare Anyconnect o i suoi componenti da ISE.

Passaggio 15. L'utente esegue l'applicazione NSA.

Passaggio 16. NSA invia la prima sonda di individuazione - HTTP /auth/discovery al gateway predefinito. L'NSA prevede quindi un URL di reindirizzamento.

> **Nota**: per le connessioni su VPN su dispositivi MAC OS, questa sonda viene ignorata perché MAC OS non ha un gateway predefinito sulla scheda VPN.

Passaggio 17. L'NSA invia una seconda sonda se la prima si guasta. La seconda sonda è HTTP GET /auth/discovery to `enroll.cisco.com`. Questo FQDN deve essere risolvibile correttamente dal server DNS. In uno scenario VPN con un tunnel suddiviso, il traffico verso `enroll.cisco.com` deve essere indirizzato attraverso il tunnel.

Passaggio 18. Se una delle richieste ha esito positivo, l'NSA stabilisce una connessione SSL sulla porta 8905 con le informazioni ottenute tramite il comando redirect-url. Questa connessione è protetta dal certificato di amministratore ISE. All'interno di questa connessione, NSA scarica Anyconnect.

Considerazioni importanti:

- Prima della versione ISE 2.2, la comunicazione SSL sulla porta 8905 è un requisito per la postura.
- Per evitare avvisi sui certificati, è necessario che i certificati del portale e dell'amministratore siano attendibili sul lato client.
- Nelle implementazioni ISE a più interfacce, le interfacce diverse da G0 possono essere associate a FQDN in modo diverso da FQDN di sistema (con l'utilizzo di `ip host` CLI). Ciò può causare problemi con la convalida del nome soggetto (SN)/nome alternativo soggetto (SAN). Se ad esempio il client viene reindirizzato all'FQDN dall'interfaccia G1, l'FQDN del sistema può essere diverso dall'FQDN nell'URL di reindirizzamento per il certificato di comunicazione 8905. Come soluzione per questo scenario, è possibile aggiungere FQDN di interfacce aggiuntive nei campi SAN del certificato di amministrazione oppure utilizzare un carattere jolly nel certificato di amministrazione.

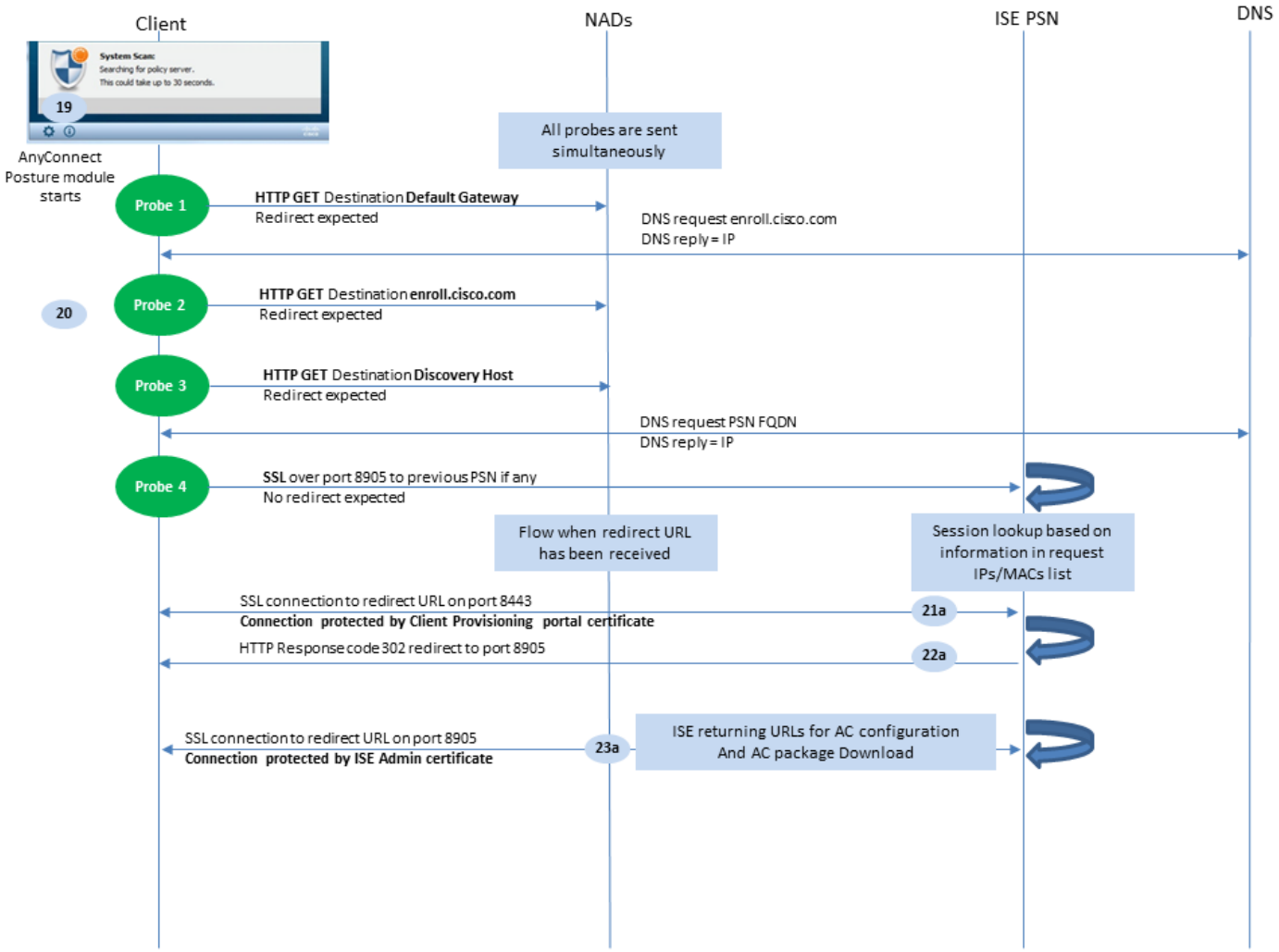

Figura 1-3

Passaggio 19. Viene avviato il processo di postura di Anyconnect ISE.

Il modulo Anyconnect ISE Posture inizia in una delle seguenti situazioni:

- Dopo l'installazione
- Dopo la modifica del valore predefinito del gateway
- Dopo l'evento di accesso dell'utente di sistema
- Dopo l'evento di alimentazione del sistema

Passaggio 20. In questa fase, il modulo Anyconnect ISE Posture avvia il rilevamento del server delle policy. A tale scopo, viene inviata una serie di richieste contemporaneamente dal modulo Anyconnect ISE Posture.

- Probe 1 - HTTP get /auth/discovery sull'IP gateway predefinito. È necessario ricordare che i dispositivi MAC OS non dispongono di un gateway predefinito sulla scheda VPN. Il risultato previsto per il probe è redirect-url.
- Sonda 2 - HTTP GET /auth/discovery su enroll.cisco.com. Questo FQDN deve essere risolvibile correttamente dal server DNS. In uno scenario VPN con un tunnel suddiviso, il traffico verso enroll.cisco.com deve essere indirizzato attraverso il tunnel. Il risultato previsto per il probe è redirect-url.
- Probe 3 - HTTP get /auth/discovery to discovery host. Il valore dell'host di rilevamento viene restituito da ISE durante l'installazione nel profilo di postura CA. Il risultato previsto per il

probe è redirect-url.

- Probe 4 - HTTP GET /auth/status su SSL sulla porta 8905 al PSN connesso in precedenza. Questa richiesta contiene informazioni sugli IP client e sugli elenchi MAC per la ricerca delle sessioni sul lato ISE. Questo problema non viene presentato durante il primo tentativo di postura. La connessione è protetta da un certificato di amministratore ISE. Come risultato di questa sonda, ISE può restituire l'ID sessione al client se il nodo in cui la sonda è atterrata è lo stesso nodo in cui l'utente è stato autenticato.

  Nota: come risultato di questa sonda, la postura può essere eseguita con successo anche senza il reindirizzamento di lavoro in alcune circostanze. Per una postura senza reindirizzamento riuscita è necessario che il PSN corrente che ha autenticato la sessione sia uguale al PSN connesso in precedenza. Tenere presente che prima di ISE 2.2, il successo della postura senza reindirizzamento è più un'eccezione che una regola.

I passaggi seguenti descrivono il processo di postura nel caso in cui l'URL di reindirizzamento venga ricevuto (flusso contrassegnato con la lettera a) come risultato di una delle richieste.

Passaggio 21. Il modulo Anyconnect ISE Posture stabilisce una connessione al portale di provisioning dei client con l'uso di un URL recuperato durante la fase di rilevamento. In questa fase, ISE esegue di nuovo la convalida della policy di provisioning dei client utilizzando le informazioni provenienti dalle sessioni autenticate.

Passaggio 2.Se viene rilevato un criterio di provisioning client, ISE restituisce il reindirizzamento alla porta 8905.

Passaggio 23. L'agente stabilisce una connessione con ISE sulla porta 8905. Durante questa connessione, ISE restituisce gli URL per il profilo della postura, il modulo di conformità e gli aggiornamenti di anyconnect.

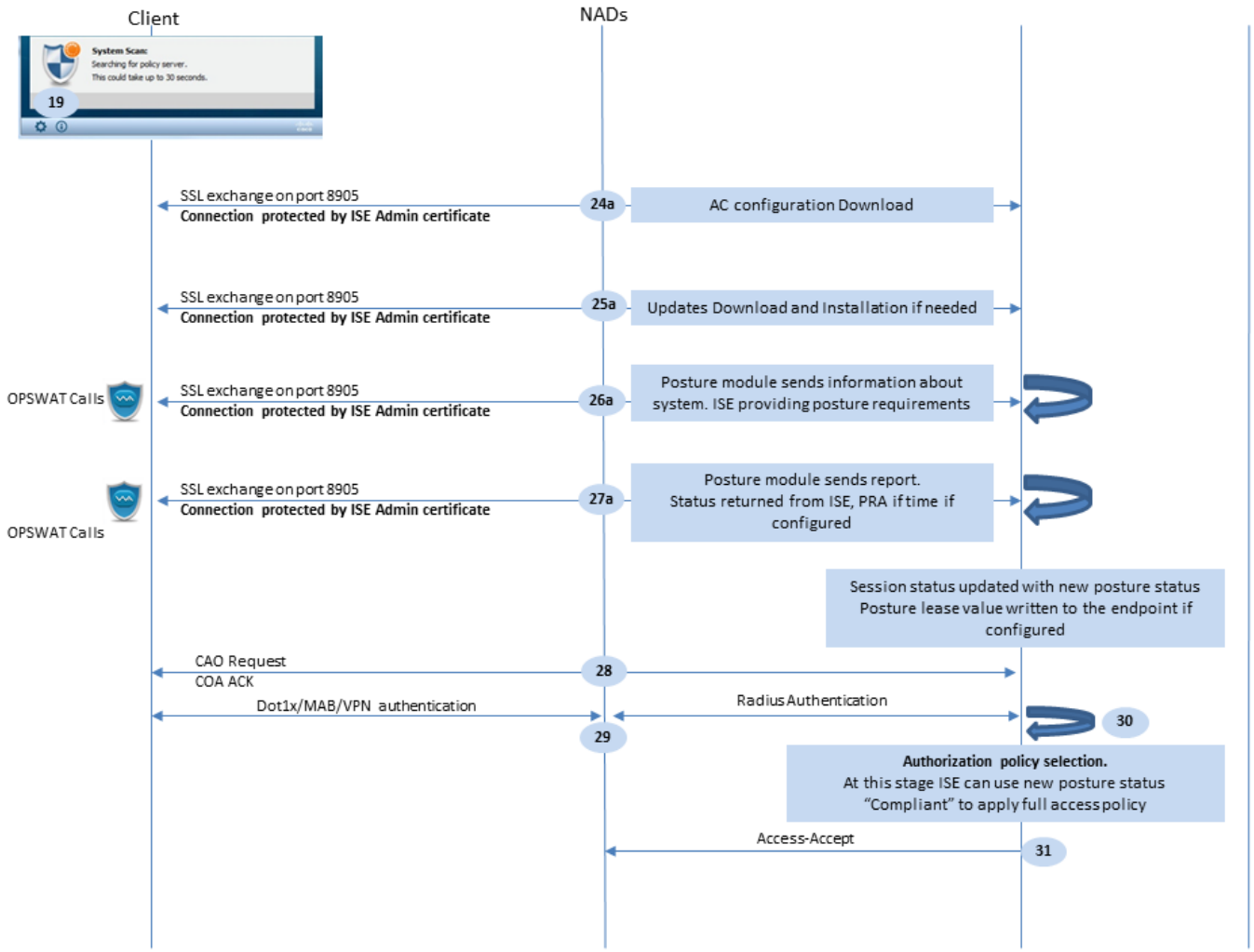

Figura 1-4

Fase 24. Download della configurazione del modulo AC ISE Posture da ISE.

Passaggio 25. Se necessario, scaricare e installare gli aggiornamenti.

Passaggio 26. AC ISE Posture Module raccoglie le informazioni iniziali sul sistema (come la versione del sistema operativo, i prodotti di sicurezza installati e la loro versione di definizione). In questa fase, il modulo AC ISE posture coinvolge l'API OPSWAT per raccogliere informazioni sui prodotti di sicurezza. I dati raccolti vengono inviati ad ISE. In risposta a questa richiesta, ISE fornisce un elenco di requisiti di postura. L'elenco dei requisiti è selezionato come risultato dell'elaborazione dei criteri di postura. Per soddisfare la policy corretta, ISE utilizza la versione del sistema operativo del dispositivo (presente nella richiesta) e il valore dell'ID sessione per scegliere gli altri attributi richiesti (gruppi AD/LDAP). Il valore ID sessione viene inviato anche dal client.

Passaggio 27. In questa fase, il client utilizza chiamate OPSWAT e altri meccanismi per controllare i requisiti di postura. Il report finale con l'elenco dei requisiti e il loro stato viene inviato ad ISE. ISE deve prendere la decisione finale sullo stato di conformità dell'endpoint. Se in questa fase l'endpoint è contrassegnato come non conforme, verrà restituito un insieme di azioni di correzione. Per l'endpoint conforme, ISE scrive lo stato di conformità nella sessione e inserisce l'ultimo timestamp della postura negli attributi dell'endpoint se è configurato il lease della postura. Il risultato della postura viene inviato nuovamente all'endpoint. Nel caso della rivalutazione della postura (PRA), anche il tempo per PRA viene messo da ISE in questo pacchetto.

In uno scenario non conforme, tenere conto dei seguenti punti:

- Alcune azioni di correzione (come messaggi di testo visualizzati, correzione collegamento, correzione file e altre) vengono eseguite dall'agente di postura stesso.
- Altri tipi di correzione (come AV. AS, WSUS e SCCM) richiedono la comunicazione API OPSWAT tra l'agente di postura e il prodotto di destinazione. In questo scenario l'agente di postura invia una richiesta di correzione al prodotto. Il risanamento viene eseguito direttamente dai prodotti di sicurezza.

Nota: se il prodotto per la sicurezza deve comunicare con risorse esterne (server di aggiornamento interni/esterni), è necessario verificare che la comunicazione sia consentita in Redirect-ACL/DACL.

Passaggio 28. ISE invia una richiesta di certificato di autenticità al DNA che deve attivare una nuova autenticazione per l'utente. E deve confermare la richiesta da COA ACK. Tenere presente che per i casi VPN viene utilizzato il push COA, quindi non viene inviata alcuna nuova richiesta di autenticazione. L'ASA rimuove invece i parametri di autorizzazione precedenti (reindirizzamento dell'URL, reindirizzamento dell'ACL e DACL) dalla sessione e applica i nuovi parametri dalla richiesta COA.

Passaggio 29. Nuova richiesta di autenticazione per l'utente.

Considerazioni importanti:

- In genere, per Cisco e COA, ISE utilizza la riautenticazione, che indica a NAD di avviare una nuova richiesta di autenticazione con l'ID sessione precedente.
- Sul lato ISE, lo stesso valore di ID sessione indica che gli attributi della sessione raccolti in precedenza devono essere riutilizzati (stato del reclamo nel caso specifico) e che deve essere assegnato un nuovo profilo di autorizzazione basato su tali attributi.
- In caso di modifica dell'ID di sessione, questa connessione viene considerata come nuova e il processo di postura completo viene riavviato.
- Per evitare la ripostura ad ogni modifica dell'id della sessione, è possibile utilizzare un lease di postura. In questo scenario, le informazioni sullo stato della postura vengono memorizzate negli attributi dell'endpoint che rimangono sull'ISE anche se l'ID della sessione èè cambiata.

Passaggio 30. Sul lato ISE viene selezionato un nuovo criterio di autorizzazione basato sullo stato della postura.

Passaggio 31. Access-Accept con i nuovi attributi di autorizzazione viene inviato a NAD.

Il flusso successivo descrive lo scenario in cui l'URL di reindirizzamento non viene recuperato (contrassegnato con la lettera b) da alcuna sonda di postura e il PSN connesso in precedenza è stato interrogato dall'ultima sonda. Tutti i passaggi sono esattamente uguali a quelli relativi all'URL di reindirizzamento, ad eccezione della riproduzione restituita dal PSN come risultato della sonda 4. Se la sonda è arrivata sullo stesso PSN proprietario della sessione di autenticazione corrente, la ripetizione contiene il valore dell'ID della sessione che viene successivamente utilizzato dall'agente di postura per completare il processo. Nel caso in cui l'headend connesso in precedenza non sia lo stesso del proprietario della sessione corrente, la ricerca della sessione ha esito negativo e viene restituita una risposta vuota al modulo di postura ISE CA. Come risultato finale, la No Policy Server Detected all'utente finale.

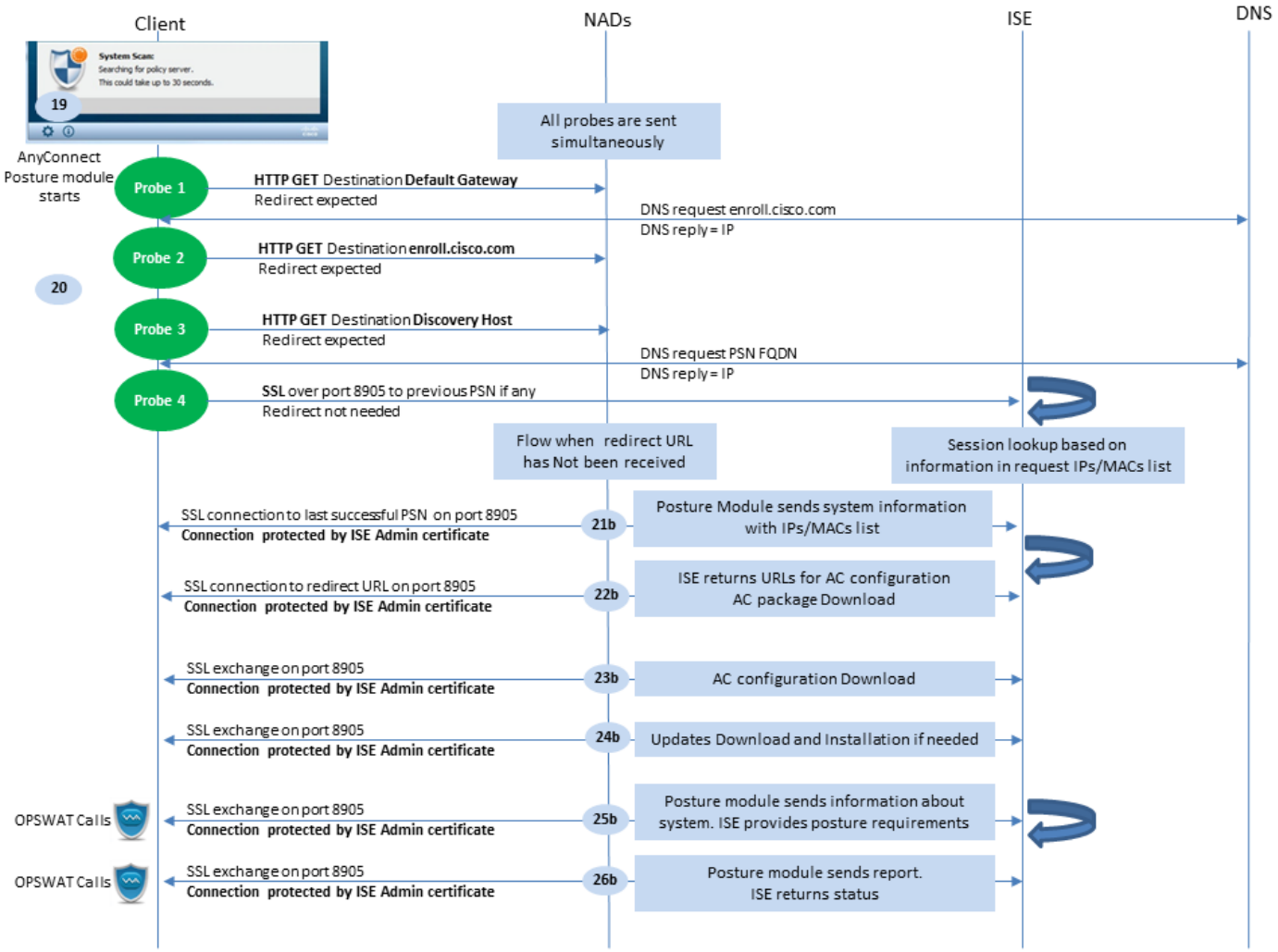

Figura 1-5

Posture Flow in ISE 2.2

ISE 2.2 supporta simultaneamente sia il vecchio che il nuovo stile. Questa è la spiegazione dettagliata del nuovo flusso:

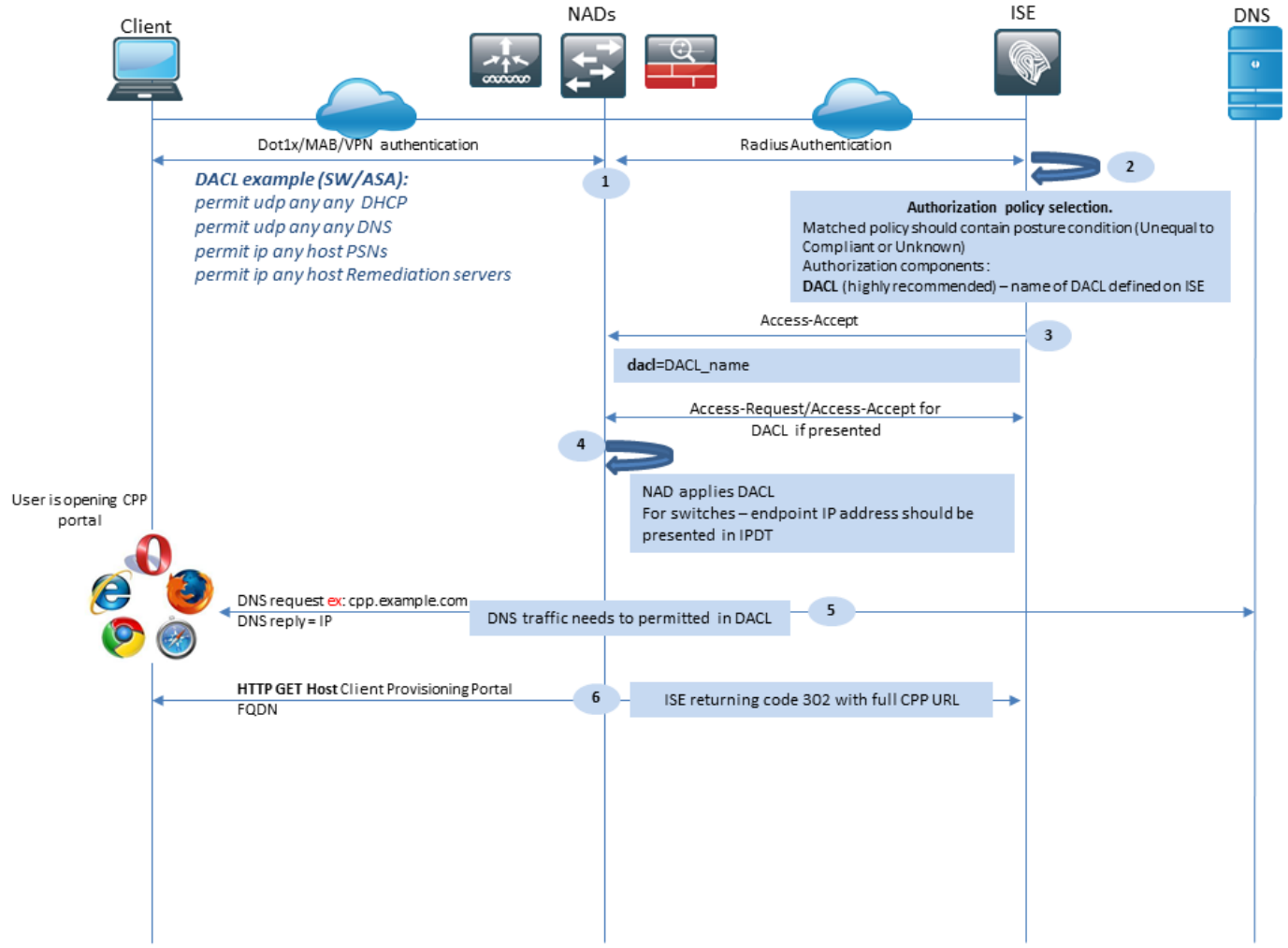

Figura 2-1

Passaggio 1. L'autenticazione è il primo passaggio del flusso. Può essere dot1x, MAB o VPN.

Fase 2. ISE deve scegliere i criteri di autenticazione e autorizzazione per l'utente. Nella postura, lo scenario scelto come criterio di autorizzazione deve contenere un riferimento allo stato della postura, che inizialmente deve essere sconosciuto o non applicabile. Per coprire entrambi i casi, è possibile utilizzare condizioni con stato di postura non conforme. Per una postura senza reindirizzamento, non è necessario utilizzare alcuna configurazione di reindirizzamento Web nel profilo di autorizzazione. È comunque possibile usare un ACL DACL o un ACL di spazio aereo per limitare l'accesso degli utenti in una fase in cui lo stato della postura non è disponibile.

Passaggio 3. ISE restituisce Access-Accept con attributi di autorizzazione.

Passaggio 4. Se il nome DACL viene restituito in Access-Accept, NAD avvia il download del contenuto DACL e applica il profilo di autorizzazione alla sessione dopo che è stato ottenuto.

Passaggio 5. Il nuovo approccio presuppone che il reindirizzamento non sia possibile, pertanto l'utente deve immettere manualmente l'FQDN del portale di provisioning client. L'FQDN del portale CPP deve essere definito nella configurazione del portale sul lato ISE. Dal punto di vista del server DNS, A-record deve puntare al server ISE con il ruolo PSN abilitato.

Passaggio 6. Il client invia il protocollo HTTP per raggiungere l'FQDN del portale di provisioning client. Questa richiesta viene analizzata sul lato ISE e l'URL completo del portale viene restituito al client.

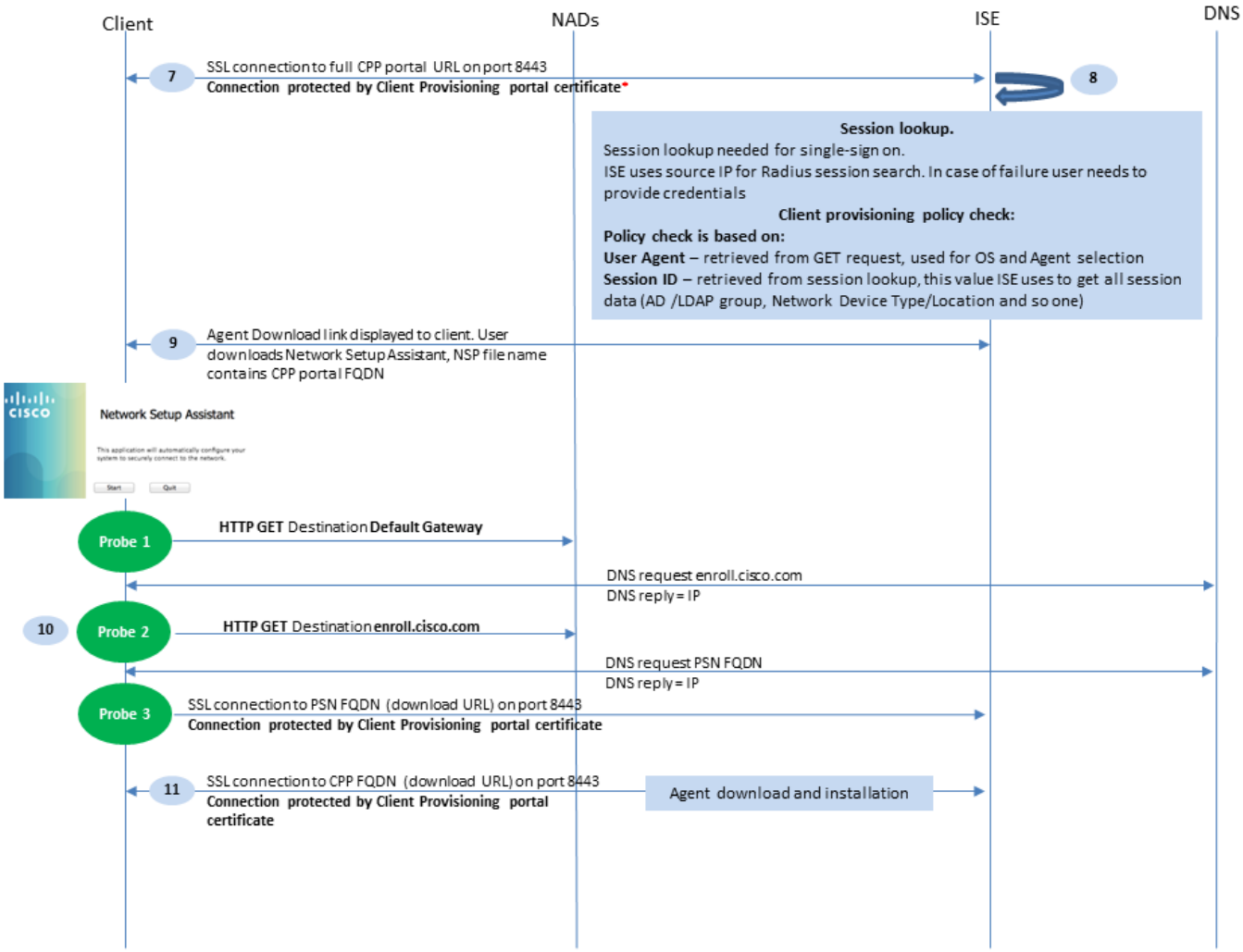

Figura 2-2

Passaggio 7. Viene stabilita la connessione SSL sulla porta ricevuta nell'URL di reindirizzamento (impostazione predefinita: 8443). Questa connessione è protetta da un certificato del portale dal lato ISE. All'utente viene presentato il Client Provisioning Portal (CPP).

Passaggio 8. In questa fase, ISE genera due eventi:

- Single Sign On (SSO) - ISE tenta di cercare l'autenticazione riuscita precedente. ISE utilizza l'indirizzo IP di origine del pacchetto come filtro di ricerca per le sessioni radius attive.

  Nota: la sessione viene recuperata in base a una corrispondenza tra l'IP di origine nel pacchetto e l'indirizzo IP con frame nella sessione. L'indirizzo IP con frame viene in genere recuperato da ISE dagli aggiornamenti della contabilità provvisori, quindi è necessario che l'accounting sia abilitato sul lato NAD. È inoltre necessario ricordare che l'SSO è possibile solo sul nodo proprietario della sessione. Se, ad esempio, la sessione viene autenticata sul PSN 1, ma il nome FQDN stesso punta a PSN2, il meccanismo SSO non riesce.

- Ricerca dei criteri di provisioning del client: se l'SSO ha esito positivo, ISE può utilizzare i dati di sessioni autenticate e User-Agent dal browser del client. In caso di un SSO non riuscito, l'utente deve fornire le credenziali e, dopo il recupero delle informazioni di autenticazione utente dagli archivi identità interna ed esterna (gruppi AD/LDAP/interni), può essere utilizzato per il controllo dei criteri di provisioning client.

Nota: a causa dell'ID bug Cisco CSCvd11574, è possibile visualizzare un errore al momento della selezione dei criteri di provisioning del client per i casi non SSO quando l'utente esterno è membro di più gruppi AD/LDAP aggiunti nella configurazione dell'archivio identità esterno. Il difetto indicato è stato risolto a partire da ISE 2.3 FCS e la correzione richiede l'utilizzo di CONTAINS in condizione con il gruppo AD invece di EQUAL.

Passaggio 9. Dopo aver selezionato la policy di provisioning del client, ISE visualizza l'URL di download dell'agente per l'utente. Dopo aver fatto clic su scarica NSA, l'applicazione viene indirizzata all'utente. Il nome file NSA contiene l'FQDN del portale CPP.

Passaggio 10. In questa fase, l'NSA esegue delle richieste per stabilire una connessione all'ISE. Due sonde sono classiche e la terza è stata progettata per consentire il rilevamento da parte di ISE in ambienti senza reindirizzamento dell'URL.

- NSA invia la prima sonda di individuazione - HTTP /auth/discovery al gateway predefinito. L'NSA prevede quindi un URL di reindirizzamento.
- L'NSA invia una seconda sonda se la prima non riesce. La seconda sonda è HTTP GET /auth/discovery to enroll.cisco.com. Questo FQDN deve essere risolvibile correttamente dal server DNS. In uno scenario VPN con un tunnel suddiviso, il traffico verso enroll.cisco.com deve essere indirizzato attraverso il tunnel.
- L'NSA invia la terza sonda attraverso la porta del portale CPP all'FQDN del portale di provisioning del client. Questa richiesta contiene informazioni sull'ID sessione del portale che consente ad ISE di identificare le risorse da fornire.

Passaggio 11. NSA scarica Anyconnect e/o moduli specifici. Il processo di download viene eseguito sulla porta del portale di provisioning del client.

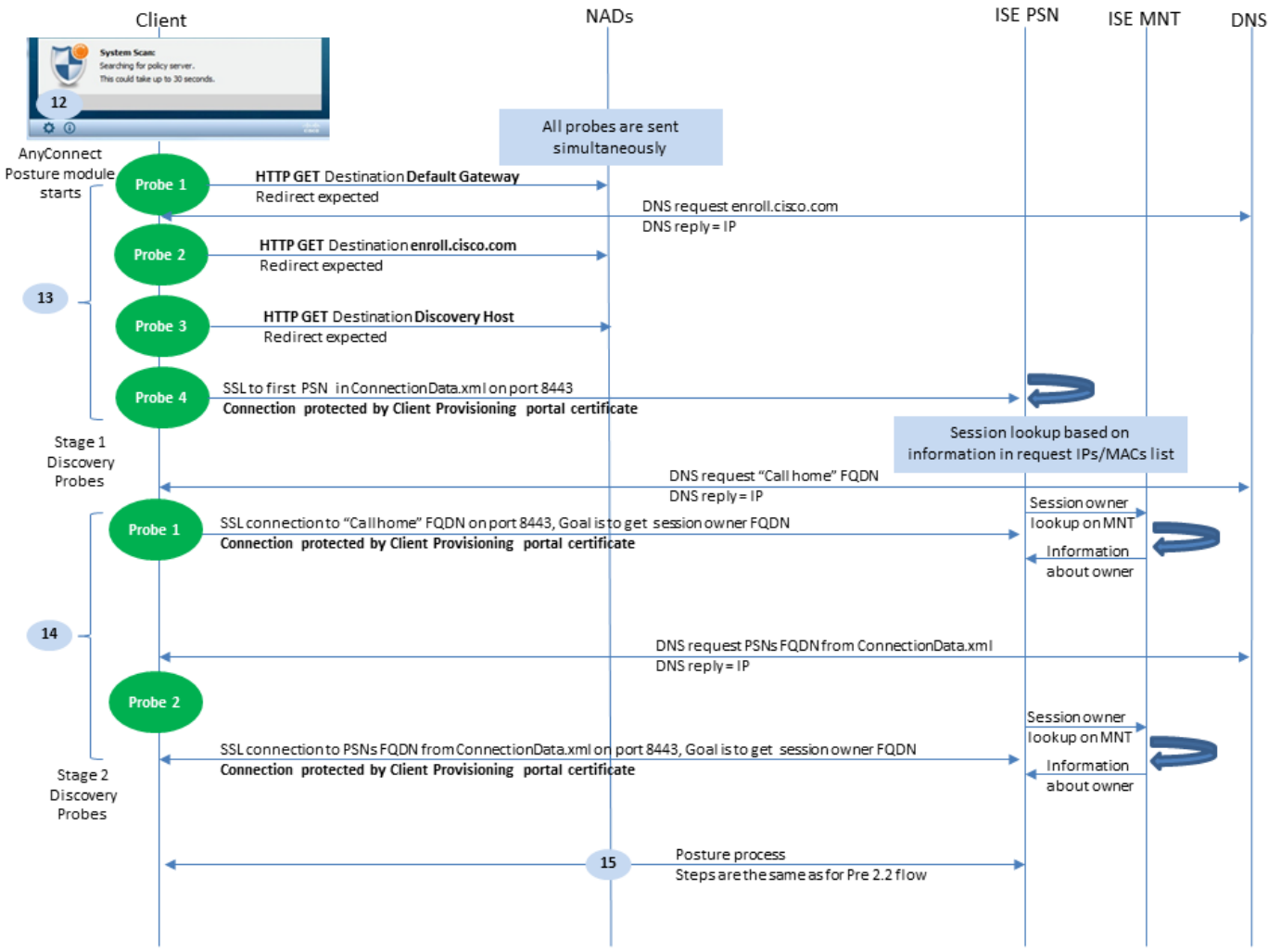

Figura 2-3

Passaggio 12. Ad ISE 2.2, il processo di postura è diviso in due fasi. La prima fase contiene una serie di sonde tradizionali per il rilevamento della postura che supportano la compatibilità con le installazioni che si basano sul reindirizzamento dell'URL.

Passaggio 13. La prima fase contiene tutte le sonde tradizionali per la scoperta della postura. Per ulteriori dettagli sulle sonde, rivedere il Passaggio 20. nel flusso di postura precedente a ISE 2.2.

Passaggio 14. La seconda fase contiene due sonde di rilevamento che consentono al modulo di postura ISE AC di stabilire una connessione al PSN in cui la sessione viene autenticata in ambienti in cui il reindirizzamento non è supportato. Durante la seconda fase, tutte le sonde sono sequenziali.

- Probe 1 - Durante la prima sonda, il modulo di postura ISE CA cerca di stabilire una connessione con IP/FQDN dall'elenco "Call Home". È necessario configurare un elenco di destinazioni per la sonda nel profilo della postura CA sul lato ISE. È possibile definire indirizzi IP/FQDN separati da virgole e con i due punti è possibile definire il numero di porta per ogni destinazione di chiamata a domicilio. Questa porta deve essere uguale alla porta su cui viene eseguito il portale di provisioning client. Sul lato client, le informazioni sui server di call home si trovano in ISEPostureCFG.xml, il file si trova nella cartella - C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture\.
  Nel caso in cui la destinazione non sia proprietaria della sessione, in questa fase è necessaria una ricerca del proprietario. Il modulo AC ISE Posture indica ad ISE di avviare la ricerca del

proprietario con l'uso di un URL di destinazione speciale - /auth/ng-discovery richiesta. Contiene inoltre l'elenco degli IP e degli MAC dei client. Dopo che il messaggio è stato ricevuto dalla sessione PSN, viene eseguita prima una ricerca localmente (questa ricerca utilizza sia IP che MAC dalla richiesta inviata dal modulo di postura ISE AC). Se la sessione non viene trovata, PSN avvia una query del nodo MNT. Questa richiesta contiene solo l'elenco degli indirizzi MAC, di conseguenza, l'FQDN del proprietario deve essere ottenuto dal MNT. In seguito, PSN restituisce l'FQDN dei proprietari al client. La richiesta successiva del client viene inviata all'FQDN del proprietario della sessione con autenticazione/stato in URL e elenco di IP e MAC.

- Probe 2 - In questa fase, il modulo di postura ISE CA prova con i nomi FQDN PSN situati in ConnectionData.xml. Questo file è disponibile in C:\Users\ . Il modulo AC ISE Posture crea questo file dopo il primo tentativo di postura. Il file contiene un elenco di FQDN di ISE PSN. Il contenuto dell'elenco può essere aggiornato in modo dinamico durante i successivi tentativi di connessione. L'obiettivo finale di questa sonda è ottenere il nome di dominio completo (FQDN) del proprietario della sessione corrente. L'implementazione è identica alla sonda 1. con l'unica differenza nella selezione della destinazione della sonda.
  Se il dispositivo è utilizzato da più utenti, il file si trova nella cartella dell'utente corrente. Un altro utente non è in grado di utilizzare le informazioni di questo file. Questo può portare gli utenti al problema di galline e uova in ambienti senza reindirizzamento quando le destinazioni Call Home non sono specificate.

Passaggio 15. Dopo aver ottenuto le informazioni sul proprietario della sessione, tutti i passaggi successivi sono identici al flusso precedente a ISE 2.2.

Configurazione

Per questo documento, ASAv è usato come dispositivo di accesso alla rete. Tutti i test sono condotti con postura su VPN. La configurazione ASA per il supporto della postura su VPN non è inclusa nell'ambito del documento. Per ulteriori informazioni, fare riferimento all'esempio di configurazione ASA VPN versione 9.2.1 con ISE.

> **Nota**: per la distribuzione con utenti VPN, l'impostazione consigliata è la postura basata sul reindirizzamento. Non è consigliabile configurare callhomelist. Per tutti gli utenti non basati sulla vpn, verificare che l'ACL sia applicato in modo che non parlino con il PSN in cui è configurata la postura.

Esempio di rete

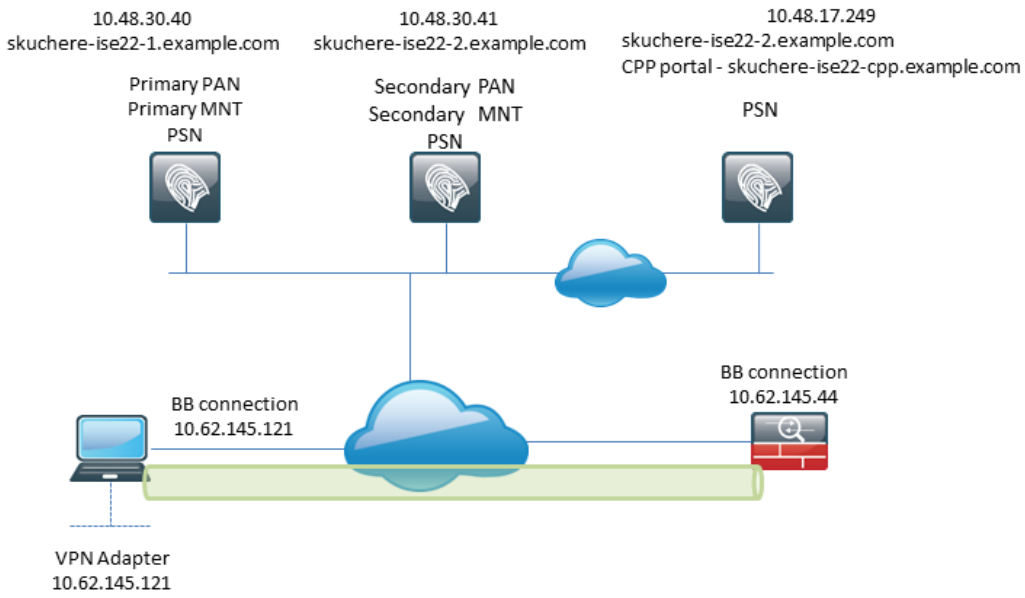

Figura 3-1

Questa topologia viene utilizzata nei test. Con l'ASA, è possibile simulare facilmente lo scenario quando il meccanismo SSO per il portale di provisioning del client ha esito negativo sul lato PSN, a causa della funzione NAT. Nel caso di un flusso di postura regolare su VPN, l'SSO deve funzionare correttamente poiché di norma NAT non viene applicato agli IP VPN quando gli utenti entrano nella rete aziendale.

Configurazioni

Configurazione provisioning client

Di seguito viene riportata la procedura per preparare la configurazione di Anyconnect.

Passaggio 1. Download del pacchetto Anyconnect. Il pacchetto Anyconnect non è disponibile per il download diretto da ISE, quindi prima di iniziare, verificare che l'alimentazione sia disponibile sul PC. Questo collegamento può essere utilizzato per il download dell'AC - https://www.cisco.com/site/us/en/products/security/secure-client/index.html. Nel presente documento, anyconnect-win-4.4.00243-webdeploy-k9.pkg pacchetto.

Passaggio 2. Per caricare il pacchetto di corrente alternata in ISE, passare a Policy > Policy Elements > Results > Client Provisioning > Resourcese fare clic su Add. Scegliere Risorse agente dal disco locale. Nella nuova finestra, scegliere Cisco Provided Packages, fare clic su browse e scegliere il pacchetto di corrente alternata sul PC.

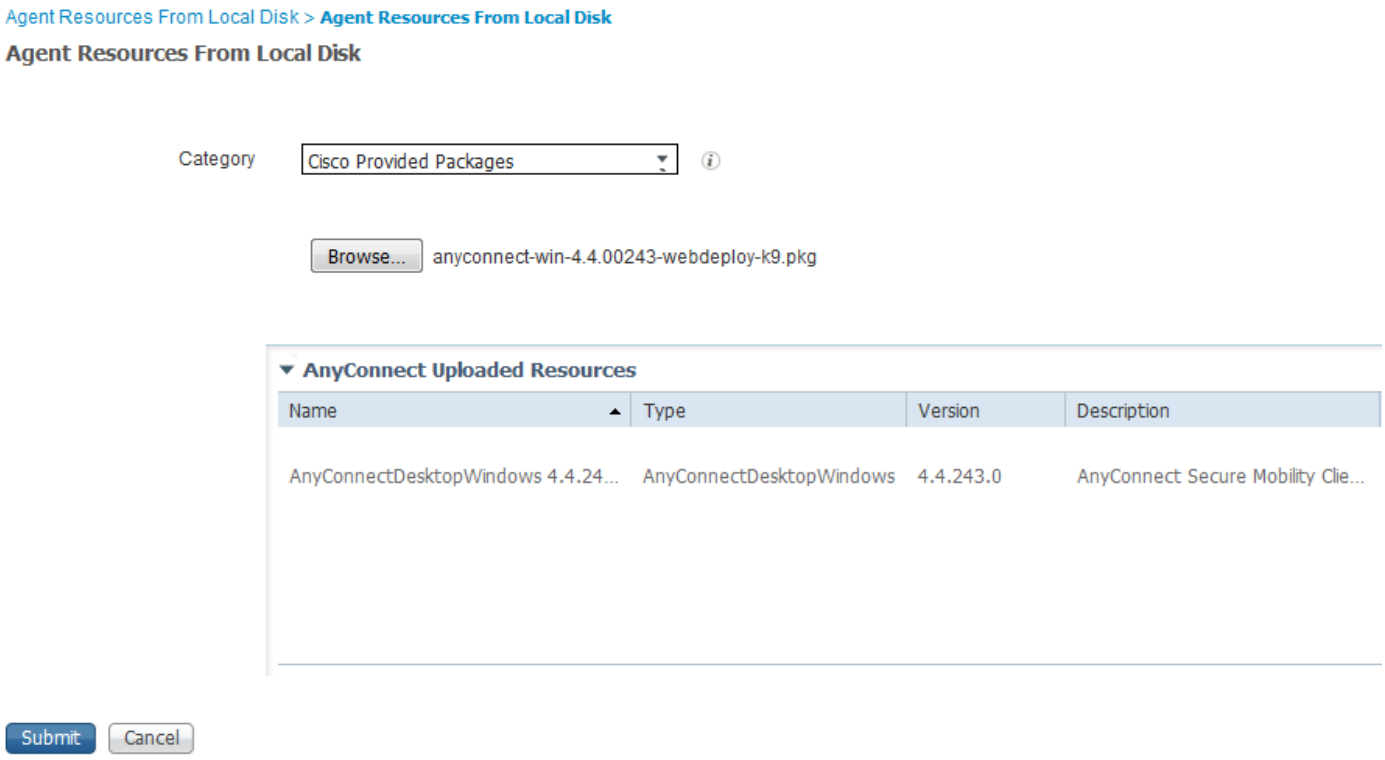

Figura 3-2

Clic Submit per completare l'importazione.

Passaggio 3. Il modulo sulla conformità deve essere caricato su ISE. Nella stessa pagina fare clic su Add e scegliere il Agent resources from Cisco site. Nell'elenco delle risorse è necessario controllare un modulo di conformità. Per questo documento, AnyConnectComplianceModuleWindows 4.2.508.0 viene utilizzato il modulo di conformità.

Passaggio 4. Ora è necessario creare il profilo di postura CA. Clic Add e scegliere il NAC agent or Anyconnect posture profile.

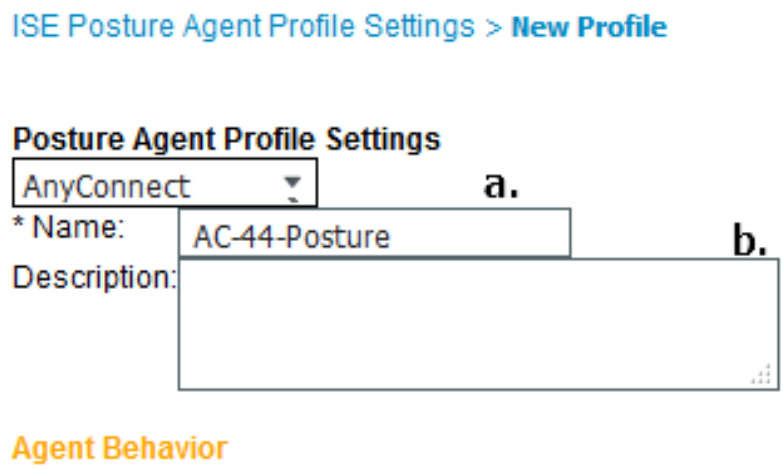

Figura 3-3

- Scegliere il tipo di profilo. Per questo scenario, è necessario usare AnyConnect.
- Specificare il nome del profilo. Passare alla Posture Protocol sezione del profilo.

Posture Protocol

Parameter	Value	Notes
PRA retransmission time	120 secs	
Discovery host		
* Server name rules	* a.	need to be blank by default to force admin to enter a value. "*" means agent will connect to all
Call Home List	skuchere-ise22-2.examp b.	List of IP addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.

Figura 3-4

- Specificare il Server Name Rules, questo campo non può essere vuoto. Il campo può contenere FQDN con caratteri jolly che limita la connessione del modulo di postura ISE AC ai PSN dello spazio dei nomi appropriato. Inserire un asterisco se è necessario consentire FQDN.
- I nomi e gli IP specificati qui sono in uso durante la fase 2 del rilevamento della postura. È possibile separare i nomi tramite virgola, nonché aggiungere numeri di porta dopo FQDN/IP utilizzando i due punti. Nel caso in cui la CA sia stata distribuita fuori banda (non dal portale di provisioning del client ISE) con l'uso dell'oggetto Criteri di gruppo o di un altro sistema di provisioning software, la presenza degli indirizzi di Call Home diventa essenziale, poiché questa è solo una sonda in grado di raggiungere il numero di serie del servizio (PSN) ISE con successo. Ciò significa che, in caso di provisioning CA fuori banda, l'amministratore deve creare un profilo di postura ISE CA con l'uso dell'editor di profili CA ed effettuare il provisioning di questo file insieme all'installazione CA.

Nota: tenere presente che la presenza di Call Home Address è fondamentale per i PC multiutente. Passaggio 14. nel flusso della postura dopo ISE 2.2.

Passaggio 5. Creare la configurazione CA. Passa a Policy > Policy Elements > Results > Client Provisioning > Resources, fare clic Add, quindi scegliere AnyConnect Configuration.

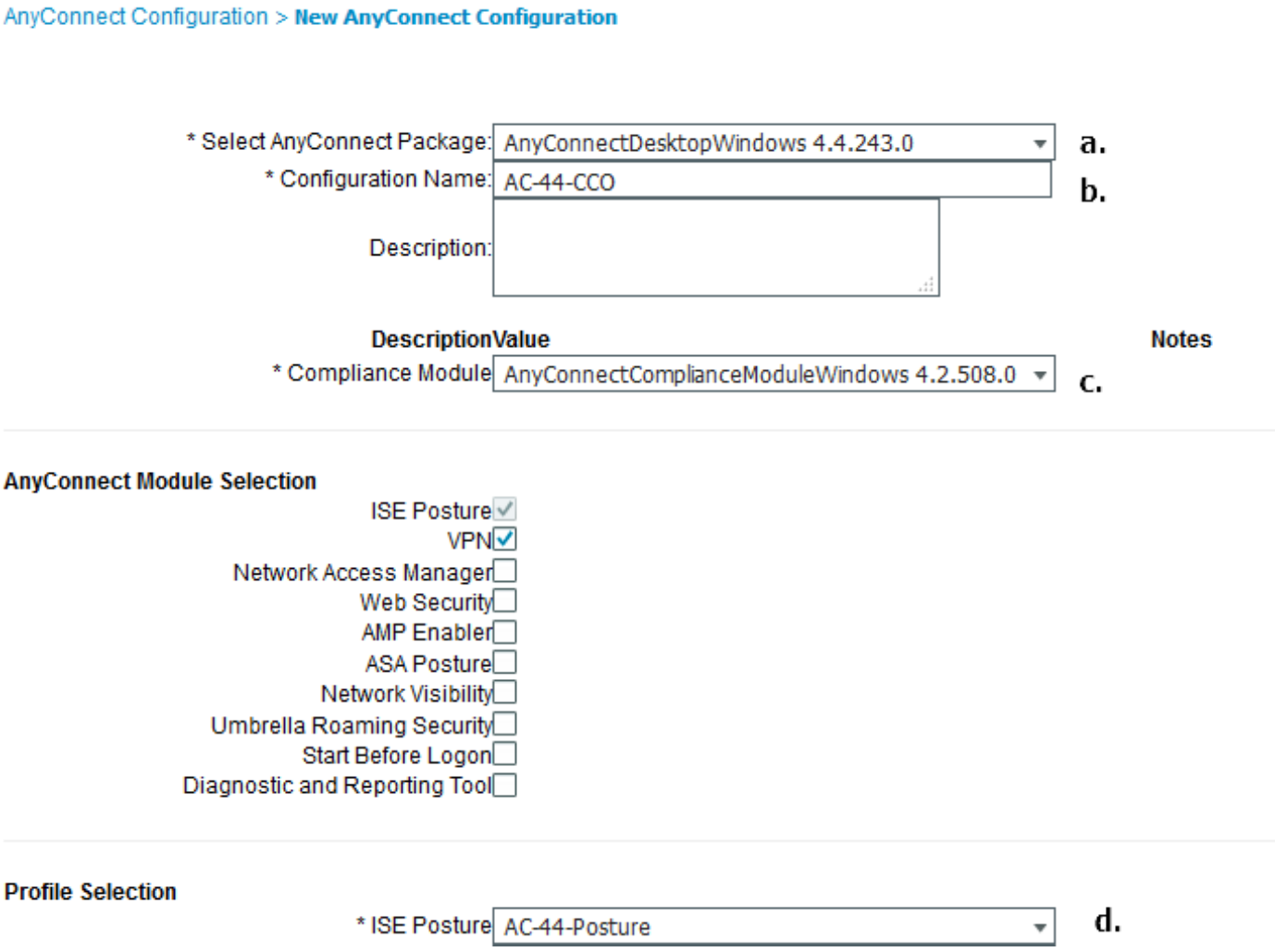

Figura 3-5

- Scegliere il pacchetto CA.
- Fornire il nome della configurazione CA.
- Scegliere la versione del modulo di conformità.
- Selezionare il profilo di configurazione della postura CA dall'elenco a discesa.

Passaggio 6. Configurare i criteri di provisioning client. Passa a Policy > Client Provisioning. Nel caso della configurazione iniziale, è possibile inserire valori vuoti nel criterio presentato con i valori predefiniti. Se è necessario aggiungere un criterio alla configurazione di postura esistente, passare al criterio che può essere riutilizzato e scegliere Duplicate Above o Duplicate Below . Si può anche creare una politica nuova di zecca.

Questo è un esempio del criterio utilizzato nel documento.

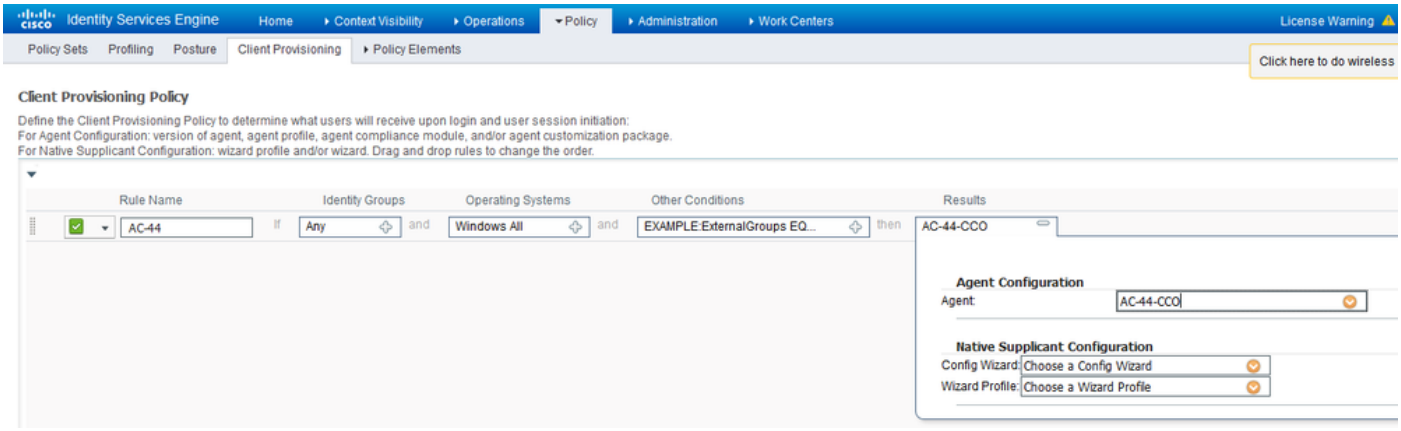

Figura 3-6

Scegliere la configurazione CA nella sezione dei risultati. Tenere presente che in caso di errore SSO ISE può avere solo attributi da login a portale. Questi attributi sono limitati alle informazioni che possono essere recuperate sugli utenti da archivi identità interni ed esterni. In questo documento, il gruppo AD viene utilizzato come condizione nei criteri di provisioning client.

Criteri e condizioni di postura

Viene utilizzato un semplice controllo della postura. ISE è configurato per controllare lo stato del servizio Windows Defender dal lato del dispositivo terminale. Gli scenari reali possono essere molto più complicati, ma i passi di configurazione generali sono gli stessi.

Passaggio 1. Creare una condizione di postura. Le condizioni di postura si trovano in Policy > Policy Elements > Conditions > Posture. Scegliete il tipo di condizione di postura. Di seguito è riportato un esempio di una condizione del servizio che deve verificare se il servizio Windows Defender è in esecuzione.

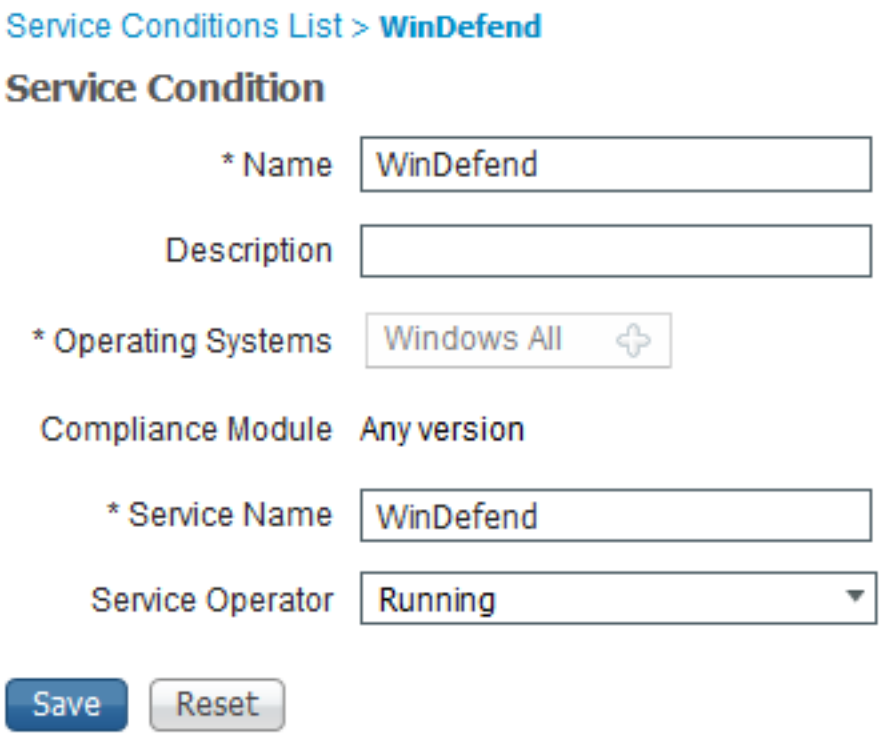

Figura 3-7

Passaggio 2. Configurazione dei requisiti di postura. Passa a Policy > Policy Elements > Results > Posture > Requirements. Questo è un esempio di un controllo di Windows Defender:

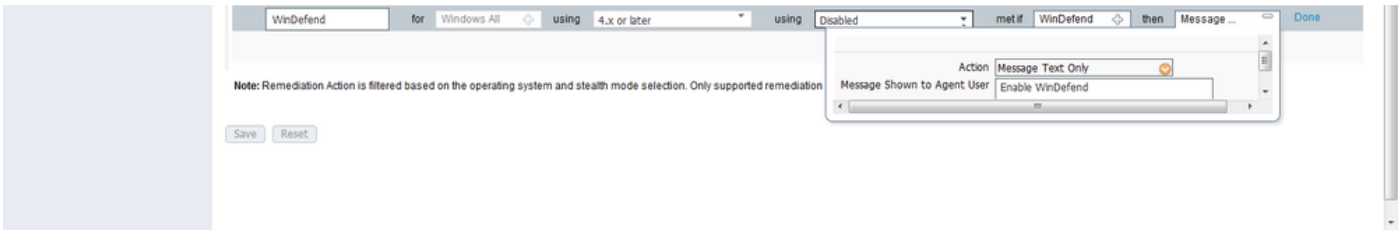

Figura 3-8

Scegliere la condizione di postura nel nuovo requisito e specificare l'azione correttiva.

Passaggio 3. Configurazione dei criteri di postura. Passa a Policy > Posture. Di seguito è riportato un esempio del criterio utilizzato per questo documento. Per il criterio è stato assegnato il requisito di Windows Defender come obbligatorio e come condizione è contenuto solo il nome del gruppo AD esterno.

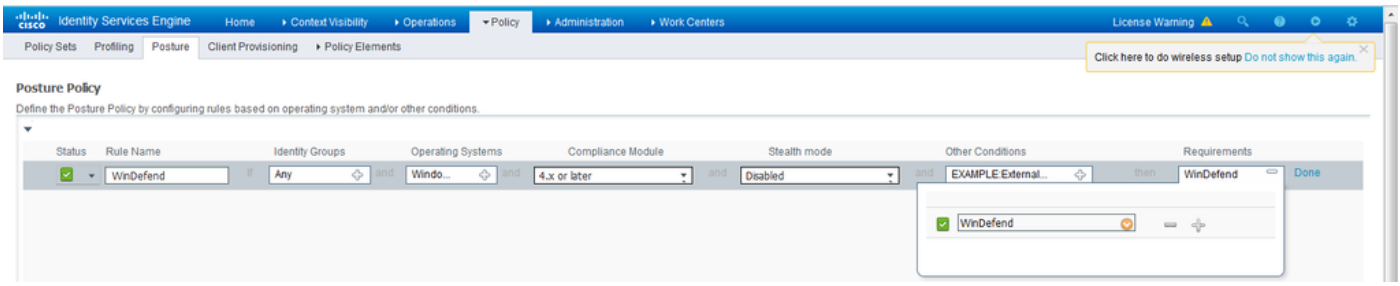

Figura 3-9

Configurazione del portale di provisioning client

Per la postura senza reindirizzamento, è necessario modificare la configurazione del portale di provisioning client. Passa a Administration > Device Portal Management > Client ProvisioningÈ possibile utilizzare il portale predefinito o crearne uno personalizzato. Lo stesso portale può essere utilizzato per entrambe le posture con e senza reindirizzamento.

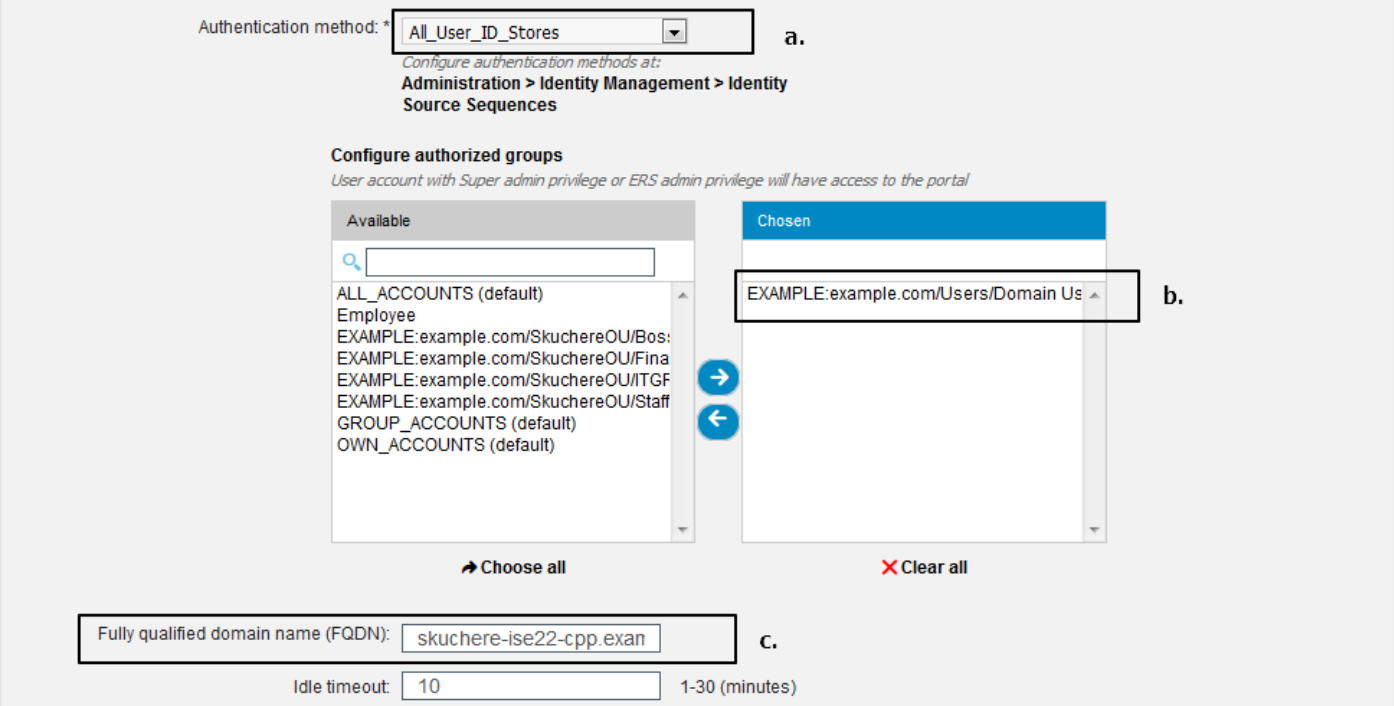

Figura 3-10

Queste impostazioni devono essere modificate nella configurazione del portale per lo scenario di non reindirizzamento:

- In Autenticazione specificare la sequenza di origine dell'identità da utilizzare se SSO non è in grado di individuare una sessione per l'utente.
- In base all'elenco di gruppi disponibili della sequenza di origine identità selezionata, è compilato. A questo punto è necessario selezionare i gruppi autorizzati per l'accesso al portale.
- Ènecessario specificare il nome di dominio completo (FQDN) del portale di provisioning client per gli scenari in cui è necessario distribuire CA dal portale di provisioning client. Questo FQDN deve essere risolvibile in IP PSN ISE. Agli utenti deve essere indicato di specificare il nome FQDN nel browser Web durante il primo tentativo di connessione.

Configura profili e criteri di autorizzazione

L'accesso iniziale per i client quando lo stato di postura non è disponibile deve essere limitato. Questo obiettivo può essere raggiunto in diversi modi:

- Assegnazione DACL: durante la fase di accesso limitato, è possibile assegnare DACL all'utente per limitare l'accesso. Questo approccio può essere utilizzato per i dispositivi di accesso alla rete Cisco.
- Assegnazione VLAN: prima che gli utenti con postura corretta possano essere inseriti in una VLAN limitata, questo approccio deve funzionare correttamente per quasi tutti i fornitori NAD.
- Radius Filter-Id: con questo attributo, è possibile assegnare all'utente con stato di postura sconosciuto un ACL definito localmente su NAD. Poiché si tratta di un attributo RFC standard, questo approccio deve funzionare correttamente per tutti i fornitori di servizi di supporto all'installazione e alla distribuzione.

Passaggio 1. Configurare DACL. Poiché questo esempio è basato su ASA, è possibile utilizzare

un NAD DACL. Per scenari reali, è necessario considerare VLAN o Filter-ID come opzioni possibili.

Per creare un DACL, passare a Policy > Policy Elements > Results > Authorization > Downloadable ACLse fare clic su Add.

Durante lo stato di postura sconosciuto, è necessario fornire almeno le seguenti autorizzazioni:

- traffico DNS
- traffico DHCP
- Traffico verso i VPN ISE (porte 80 e 443) per una possibilità di aprire un FQDN descrittivo del portale. La porta su cui è in esecuzione il portale CP è 8443 (per impostazione predefinita e la porta 8905 per la compatibilità con le versioni precedenti)
- Traffico verso i server di monitoraggio e aggiornamento, se necessario

Questo è un esempio di DACL senza server di monitoraggio e aggiornamento:

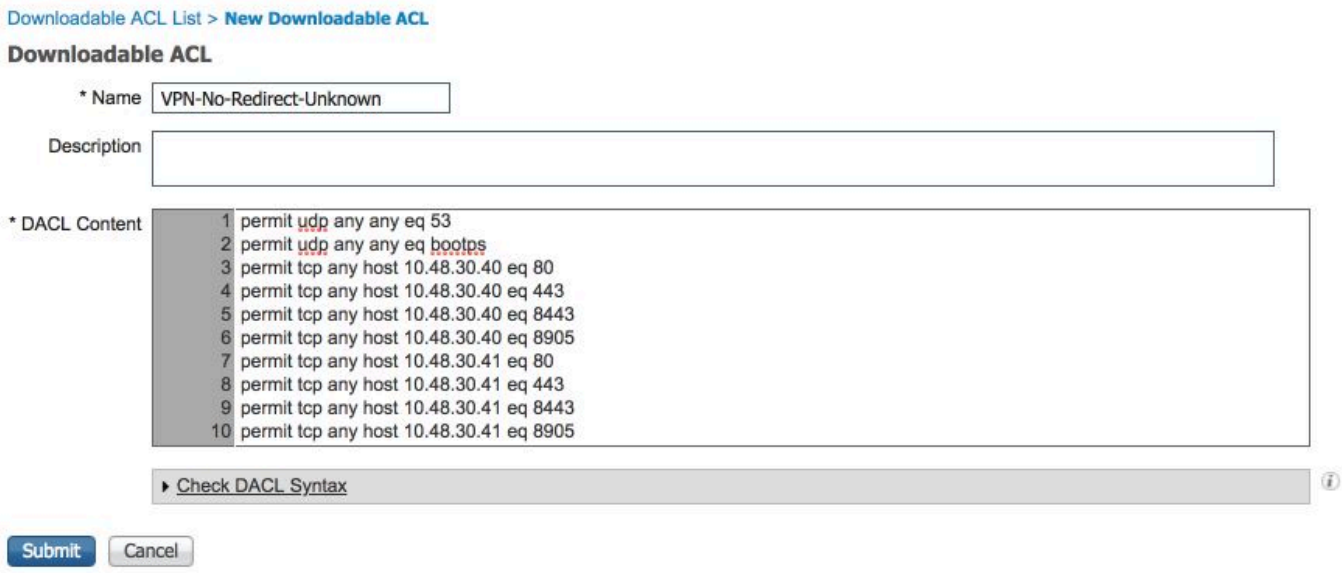

Figura 3-1

Passaggio 2. Configurare il profilo di autorizzazione.

Come al solito per la postura sono richiesti due profili di autorizzazione. La prima deve contenere qualsiasi tipo di restrizione di accesso alla rete (profilo con DACL utilizzato in questo esempio). Questo profilo può essere applicato alle autenticazioni il cui stato di postura è diverso da conforme. Il secondo profilo di autorizzazione può contenere solo l'autorizzazione di accesso e può essere applicato per le sessioni con stato di postura uguale a conformità.

Per creare un profilo di autorizzazione, passare a Policy > Policy Elements > Results > Authorization > Authorization Profiles.

Esempio di profilo ad accesso limitato:

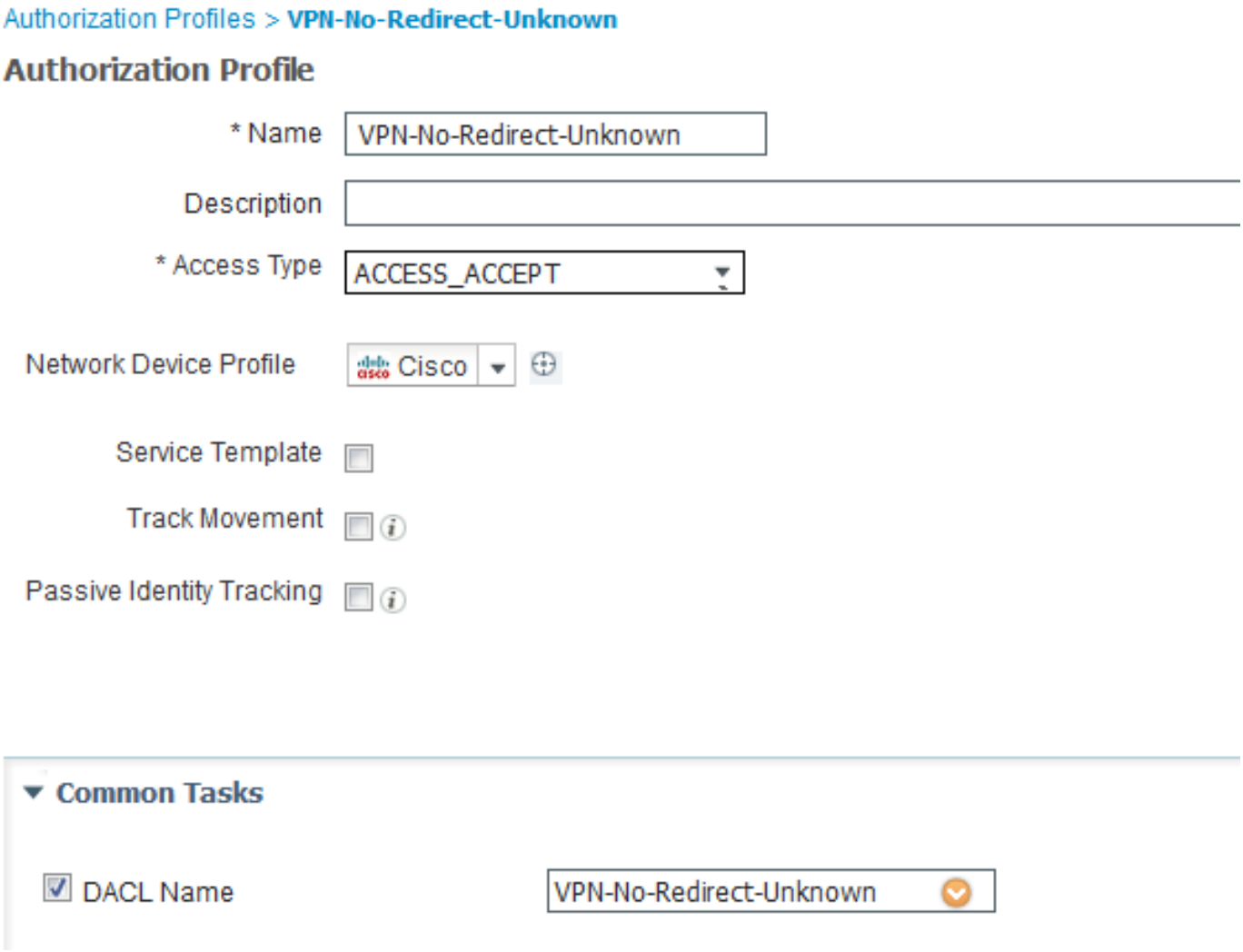

Figura 3-12

Nell'esempio, il profilo ISE predefinito PermitAccess viene usato per la sessione dopo un controllo riuscito dello stato della postura.

Passaggio 3. Configurare i criteri di autorizzazione. In questa fase è necessario creare due criteri di autorizzazione. Una consiste nel far corrispondere la richiesta di autenticazione iniziale con uno stato di postura sconosciuto, l'altra consiste nell'assegnare l'accesso completo dopo un processo di postura riuscito.

Questo è un esempio di criteri di autorizzazione semplici per il caso:

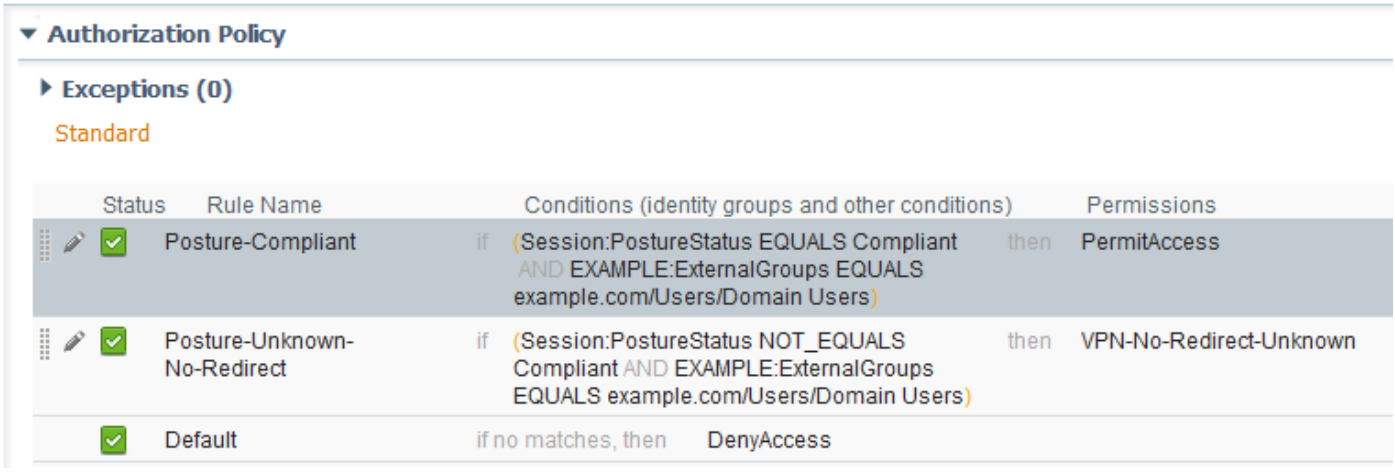

Figura 3-13

La configurazione dei criteri di autenticazione non fa parte di questo documento, ma è necessario tenere presente che prima di elaborare correttamente i criteri di autorizzazione è necessario eseguire l'autenticazione.

Verifica

La verifica di base del flusso può consistere in tre fasi principali:

Passaggio 1. Verifica del flusso di autenticazione.

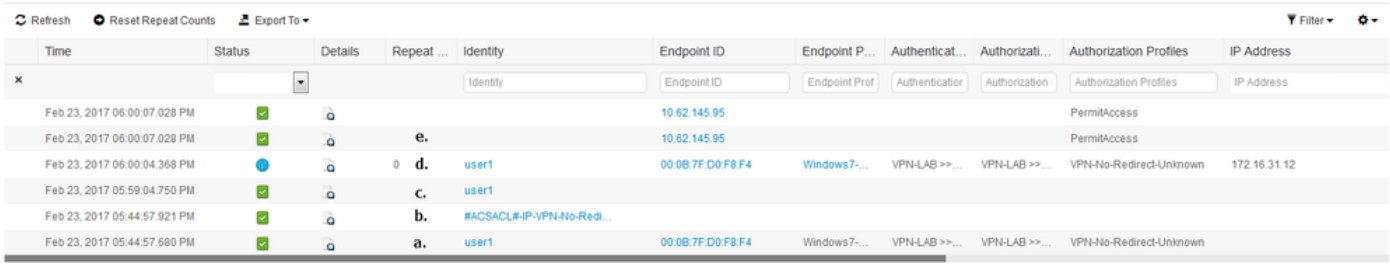

Figura 4-1

1. Autenticazione iniziale Per questo passaggio è possibile essere interessati alla convalida di cui è stato applicato il profilo di autorizzazione. Se è stato applicato un profilo di autorizzazione imprevisto, esaminare un report di autenticazione dettagliato. È possibile aprire questo report facendo clic sulla lente di ingrandimento nella colonna Dettagli. È possibile confrontare gli attributi dei report di autenticazione dettagliati con le condizioni dei criteri di autorizzazione che si prevede soddisfino.

2. Evento di download DACL. Questa stringa viene visualizzata solo se il profilo di autorizzazione selezionato per l'autenticazione iniziale contiene un nome DACL.

3. Autenticazione del portale: questo passaggio nel flusso indica che il meccanismo SSO non è riuscito a individuare la sessione utente. Questo problema può essere dovuto a più motivi: NAD non è configurato per l'invio di messaggi di accounting oppure l'indirizzo IP con frame

non è presente nei messaggiL'FQDN del portale CPP è stato risolto nell'IP del nodo ISE diverso dal nodo in cui è stata elaborata l'autenticazione inizialeIl client si trova dietro il NAT

4. Modifica dati sessione. In questo particolare esempio, lo stato della sessione è passato da Sconosciuto a Conforme.

5. il certificato di autenticità (COA) al dispositivo di accesso alla rete. Il certificato di autenticità deve avere esito positivo per eseguire il push della nuova autenticazione dal lato AND e delle nuove assegnazioni dei criteri di autorizzazione dal lato ISE. In caso di errore del Certificato di autenticità (COA), è possibile aprire un report dettagliato per verificarne la causa. I problemi più comuni relativi al certificato di autenticità possono essere i seguenti: Timeout COA: in questo caso, il PSN che ha inviato la richiesta non è configurato come client COA sul lato NAD oppure la richiesta COA è stata eliminata da qualche parte.ACK negativi COA: indica che il COA è stato ricevuto da NAD ma per qualche motivo non è possibile confermare l'operazione. Per questo scenario, una relazione dettagliata deve contenere una spiegazione più dettagliata.

Poiché nell'esempio l'appliance ASA viene usata come protocollo NAD, non è possibile visualizzare alcuna richiesta di autenticazione successiva per l'utente. Ciò si verifica perché ISE utilizza il push COA per ASA, che evita l'interruzione del servizio VPN. In uno scenario di questo tipo, il certificato di autenticità contiene nuovi parametri di autorizzazione, pertanto non è necessaria la riautenticazione.

Passaggio 2.Verifica della selezione dei criteri di provisioning del client: a tale scopo, è possibile eseguire un report su ISE che consente di identificare i criteri di provisioning del client applicati all'utente.

Passa a Operations > Reports Endpoint and Users > Client Provisioning ed eseguire il rapporto per la data desiderata.

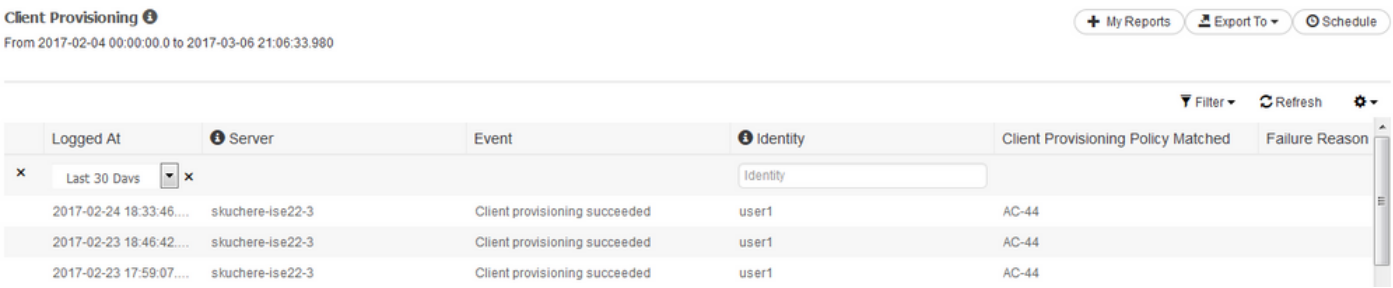

Figura 4-2

Con questo report è possibile verificare quale criterio di provisioning client è stato selezionato. Inoltre, in caso di inadempienza, i motivi devono essere indicati nella Failure Reason colonna.

Passaggio 3. Verifica report postura - Passa a Operations > Reports Endpoint and Users > Posture Assessment by Endpoint.

Figura 4-3

Da qui è possibile aprire un report dettagliato per ogni evento specifico per verificare, ad esempio, a quale ID sessione appartiene il report, quali requisiti di postura esatti sono stati selezionati da ISE per l'endpoint e lo stato per ogni requisito.

Risoluzione dei problemi

Informazioni generali

Per la risoluzione dei problemi del processo di postura, questi componenti ISE devono essere abilitati per il debug sui nodi ISE in cui può avvenire il processo di postura:

- client-webapp - Il componente responsabile del provisioning dell'agente. File di log di destinazione guest.log e ise-psc.log.
- guestacess - Il componente responsabile della ricerca del componente del portale di provisioning client e del proprietario della sessione (quando la richiesta arriva al numero PSN errato). File di log di destinazione - guest.log.
- provisioning - Il componente responsabile dell'elaborazione dei criteri di provisioning del client. File di log di destinazione - guest.log.
- posture - Tutti gli eventi correlati alla postura. File di log di destinazione - ise-psc.log.

Per la risoluzione dei problemi sul lato client, è possibile utilizzare quanto segue:

- acisensa.log -In caso di errore di provisioning client sul lato client, questo file viene creato nella stessa cartella in cui è stato scaricato NSA (la directory di download per Windows viene scaricata normalmente).
- AnyConnect_ISEPosture.txt - Questo file si trova nel bundle DART nella directory Cisco AnyConnect ISE Posture Module. Tutte le informazioni su ISE PSN discovery e le fasi generali del flusso di postura sono registrate in questo file.

Risoluzione dei problemi comuni

Problemi correlati a SSO

Se l'SSO ha esito positivo, è possibile visualizzare questi messaggi nel ise-psc.log, questo insieme di messaggi indica che la ricerca della sessione è stata completata e che l'autenticazione sul portale può essere ignorata.

```
2016-11-09 15:07:35,951 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for Radius session with input
values : sessionId: null, MacAddr: null, ipAddr: 10.62.145.121
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for session using session ID:
null, IP addrs: [10.62.145.121], mac Addrs [null]
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for session using IP
10.62.145.121
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- nasPortType = 5
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- nasPortType equal to 5 ( 5 is virtual
NAS_PORT_TYPE for VPN ). Found a VPN session null using ip address 10.62.145.121
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- Found session c0a801010002600058232bb8
using ipAddr 10.62.145.121
```

Finestra Testo 5-1

Èpossibile utilizzare l'indirizzo IP dell'endpoint come chiave di ricerca per trovare queste informazioni.

Poco dopo, nel registro guest, si noterà che l'autenticazione è stata ignorata:

```
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
guestaccess.flowmanager.step.cp.CPInitStepExecutor -::- SessionInfo is not null and session
AUTH_STATUS = 1
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
com.cisco.ise.portalSessionManager.PortalSession -::- Putting data in PortalSession with key and
value: Radius.Session c0a801010002600058232bb8
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
com.cisco.ise.portalSessionManager.PortalSession -::- Putting data in PortalSession with key :
Radius.Session
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
guestaccess.flowmanager.step.cp.CPInitStepExecutor -::- Login step will be skipped, as the
session =c0a801010002600058232bb8 already established for mac address null , clientIPAddress
10.62.145.121
2016-11-09 15:07:36,066 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
cpm.guestaccess.flowmanager.processor.PortalFlowProcessor -::- After executeStepAction(INIT),
returned Enum: SKIP_LOGIN_PROCEED
```

Finestra Testo 5-2

Se l'SSO non funziona, il ise-psc log il file contiene informazioni sull'errore di ricerca della sessione:

```
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for Radius session with input
values : sessionId: null, MacAddr: null, ipAddr: 10.62.145.44
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for session using session ID:
null, IP addrs: [10.62.145.44], mac Addrs [null]
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for session using IP 10.62.145.44
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- nasPortType = null
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
```

```
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- nasPortType == null or is not a virtual
NAS_PORT_TYPE ( 5 ).
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- No Radius session found
```

Finestra Testo 5-3

Nella scheda guest.log in questo caso, è necessario visualizzare l'autenticazione utente completa sul portale:

```
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
cpm.guestaccess.flowmanager.step.StepExecutor -::- Find Next Step=LOGIN
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
cpm.guestaccess.flowmanager.step.StepExecutor -::- Step : LOGIN will be visible!
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
cpm.guestaccess.flowmanager.step.StepExecutor -::- Returning next step =LOGIN
2017-02-23 17:59:00,780 INFO [http-bio-10.48.17.249-8443-exec-2][]
cpm.guestaccess.flowmanager.step.StepExecutor -::- Radius Session ID is not set, assuming in
dry-run mode
```

Finestra Testo 5-4

In caso di errori di autenticazione sul portale, è necessario concentrarsi sulla verifica della configurazione del portale. Quale archivio identità è in uso? Quali gruppi sono autorizzati per l'accesso?

Risoluzione dei problemi relativi alla selezione dei criteri di provisioning client

In caso di errori dei criteri di provisioning client o di elaborazione dei criteri non corretta, è possibile controllare guest.log per ulteriori dettagli:

```
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
guestaccess.flowmanager.step.guest.ClientProvStepExecutor -:user1:- In Client Prov : userAgent
=Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0, radiusSessionID=null,
idGroupName=S-1-5-21-70538695-790656579-4293929702-513, userName=user1, isInUnitTestMode=false
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
cpm.guestaccess.common.utils.OSMapper -:user1:- UserAgent : Mozilla/5.0 (Windows NT 6.1; WOW64;
rv:51.0) Gecko/20100101 Firefox/51.0
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
cpm.guestaccess.common.utils.OSMapper -:user1:- Client OS: Windows 7 (All)
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
guestaccess.flowmanager.step.guest.ClientProvStepExecutor -:user1:- Retrieved OS=Windows 7 (All)
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
guestaccess.flowmanager.step.guest.ClientProvStepExecutor -:user1:- Updating the idGroupName to
NAC Group:NAC:IdentityGroups:S-1-5-21-70538695-790656579-4293929702-513
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
guestaccess.flowmanager.step.guest.ClientProvStepExecutor -:user1:- User Agent/Radius Session is
empty or in UnitTestMode
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
guestaccess.flowmanager.step.guest.ClientProvStepExecutor -:user1:- Calling
getMatchedPolicyWithNoRedirection for user=user1
2017-02-23 17:59:07,505 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
guestaccess.flowmanager.step.guest.ClientProvStepExecutor -:user1:- CP Policy Status =SUCCESS,
needToDoVlan=false, CoaAction=NO_COA
```

Finestra Testo 5-5

Nella prima stringa è possibile vedere in che modo le informazioni sulla sessione vengono inserite nel motore di selezione dei criteri. In caso di mancata corrispondenza dei criteri o di mancata corrispondenza dei criteri, è possibile confrontare gli attributi da questa stringa con la configurazione dei criteri di provisioning del client. L'ultima stringa indica lo stato di selezione dei criteri.

Risoluzione dei problemi relativi al processo di postura

Dal lato client, bisogna essere interessati nell'investigazione delle sonde e dei loro risultati. Questo è un esempio di sonda della fase 1 riuscita:

```
*************************************

Date : 02/23/2017
Time : 17:59:57
Type : Unknown
Source : acise

Description : Function: Target::Probe
Thread Id: 0x4F8
File: SwiftHttpRunner.cpp
Line: 1415
Level: debug

PSN probe skuchere-ise22-cpp.example.com with path /auth/status, status is -1..

*************************************
```

Finestra Testo 5-6

In questa fase, PSN torna alle informazioni sull'AC relative al proprietario della sessione. Questi due messaggi possono essere visualizzati in un secondo momento:

```
*************************************

Date : 02/23/2017
Time : 17:59:58
Type : Unknown
Source : acise

Description : Function: Target::probeRecentConnectedHeadEnd
Thread Id: 0xBE4
File: SwiftHttpRunner.cpp
Line: 1674
Level: debug

Target skuchere-ise22-2.example.com, posture status is Unknown..

*************************************
```

Finestra Testo 5-7

I proprietari della sessione restituiscono all'agente tutte le informazioni necessarie:

```
****************************************

Date : 02/23/2017
Time : 17:59:58
Type : Unknown
Source : acise

Description : Function: SwiftHttpRunner::invokePosture
Thread Id: 0xFCC
File: SwiftHttpRunner.cpp
Line: 1339
Level: debug

MSG_NS_SWISS_NEW_SESSION, <?xml version="1.0" ?>
<root>
<IP></IP>
<FQDN>skuchere-ise22-2.example.com</FQDN>
<PostureDomain>posture_domain</PostureDomain>
<sessionId>c0a801010009e00058af0f7b</sessionId>
<configUri>/auth/anyconnect?uuid=106a93c0-9f71-471c-ac6c-a2f935d51a36</configUri>
<AcPackUri>/auth/provisioning/download/81d12d4b-ff58-41a3-84db-5d7c73d08304</AcPackUri>
<AcPackPort>8443</AcPackPort>
<AcPackVer>4.4.243.0</AcPackVer>
<PostureStatus>Unknown</PostureStatus>
<PosturePort>8443</PosturePort>
<PosturePath>/auth/perfigo_validate.jsp</PosturePath>
<PRAConfig>0</PRAConfig>
<StatusPath>/auth/status</StatusPath>
<BackupServers>skuchere-ise22-1.example.com,skuchere-ise22-3.example.com</BackupServers>
</root>
.

****************************************
```

Finestra Testo 5-8

Dal lato PSN, è possibile concentrarsi su questi messaggi nel guest.log quando si prevede che la richiesta iniziale inviata al nodo non sia proprietaria della sessione:

```
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- Got http request from 10.62.145.44 user
agent is: Mozilla/4.0 (compatible; WINDOWS; 1.2.1.6.1.48; AnyConnect Posture Agent v.4.4.00243)
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- mac_list from http request ==>
00:0B:7F:D0:F8:F4,00:0B:7F:D0:F8:F4
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- iplist from http request ==>
172.16.31.12,10.62.145.95
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- Session id from http request -
req.getParameter(sessionId) ==> null
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cpm.client.provisioning.utils.ProvisioningUtil -::- the input ipAddress from the list currently
being processed in the for loop ==> 172.16.31.12
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cpm.client.provisioning.utils.ProvisioningUtil -::- the input ipAddress from the list currently
being processed in the for loop ==> 10.62.145.95
2017-02-23 17:59:56,368 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- Found Client IP null and corresponding mac
address null
```

```
2017-02-23 17:59:56,369 ERROR [http-bio-10.48.17.249-8443-exec-10][]
cpm.client.provisioning.utils.ProvisioningUtil -::- Session Info is null
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- Not able to find a session for input
values - sessionId : null, Mac addresses : [00:0B:7F:D0:F8:F4, 00:0B:7F:D0:F8:F4], client Ip :
[172.16.31.12, 10.62.145.95]
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- clientMac is null/ empty, will go over the
mac list to query MNT for active session
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- Performing MNT look up for macAddress ==>
00-0B-7F-D0-F8-F4
2017-02-23 17:59:56,539 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- Performed MNT lookup, found session 0 with
session id c0a801010009e00058af0f7b
2017-02-23 17:59:56,539 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cpm.client.provisioning.utils.ProvisioningUtil -::- getting NIC name for skuchere-ise22-
cpp.example.com
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cpm.client.provisioning.utils.ProvisioningUtil -::- local interface 0 addr 10.48.17.249 name
eth0
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cpm.client.provisioning.utils.ProvisioningUtil -::- Nic name for local host: skuchere-ise22-
cpp.example.com is: eth0
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cpm.client.provisioning.utils.ProvisioningUtil -::- getting host FQDN or IP for host skuchere-
ise22-2 NIC name eth0
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cpm.client.provisioning.utils.ProvisioningUtil -::- hostFQDNOrIP for host skuchere-ise22-2 nic
eth0 is skuchere-ise22-2.example.com
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- PDP with session of 00-0B-7F-D0-F8-F4 is
skuchere-ise22-2, FQDN/IP is: skuchere-ise22-2.example.com
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- Redirecting the request to new URL:
https://skuchere-ise22-2.example.com:8443/auth/status
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- Session info is null. Sent an http
response to 10.62.145.44.
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-PDP-WITH-SESSION value is
skuchere-ise22-2.example.com
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cpm.client.provisioning.utils.ProvisioningUtil -::- header Location value is https://skuchere-
ise22-2.example.com:8443/auth/status
```

Finestra Testo 5-9

Qui potete vedere che il PSN tenta prima di trovare una sessione localmente e, dopo un errore, avvia una richiesta al MNT utilizzando l'elenco IP e MAC per individuare il proprietario della sessione.

Poco dopo è necessario visualizzare una richiesta del client sul PSN corretto:

```
2017-02-23 17:59:56,790 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for session using session ID:
null, IP addrs: [172.16.31.12, 10.62.145.95], mac Addrs [00:0B:7F:D0:F8:F4, 00:0B:7F:D0:F8:F4]
2017-02-23 17:59:56,790 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for session using IP 172.16.31.12
2017-02-23 17:59:56,791 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- nasPortType = 5
```

```
2017-02-23 17:59:56,792 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -:::::- nasPortType equal to 5 ( 5 is virtual
NAS_PORT_TYPE for VPN ). Found a VPN session null using ip address 172.16.31.12
2017-02-23 17:59:56,792 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -:::::- Found session c0a801010009e00058af0f7b
using ipAddr 172.16.31.12
```

Finestra Testo 5-10

Nel passaggio successivo, il PSN esegue la ricerca dei criteri di provisioning client per questa sessione:

```
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
com.cisco.cpm.swiss.SwissServer -:::::- null or empty value for hostport obtained from
SwissServer : getHostNameBySession()
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -:::::- looking for Radius session with input
values : sessionId: c0a801010009e00058af0f7b, MacAddr: 00-0b-7f-d0-f8-f4, ipAddr: 172.16.31.12
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -:::::- looking for session using session ID:
c0a801010009e00058af0f7b, IP addrs: [172.16.31.12], mac Addrs [00-0b-7f-d0-f8-f4]
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -:::::- Found session using sessionId
c0a801010009e00058af0f7b
2017-02-23 17:59:56,795 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:::::- User user1 belongs to groups NAC
Group:NAC:IdentityGroups:Endpoint Identity Groups:Profiled:Workstation,NAC
Group:NAC:IdentityGroups:Any
2017-02-23 17:59:58,203 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
com.cisco.cpm.swiss.SwissServer -:::::- null or empty value for hostport obtained from
SwissServer : getHPortNumberBySession()
2017-02-23 17:59:58,907 DEBUG [http-bio-10.48.30.41-8443-exec-10][]
cisco.cpm.posture.util.AgentUtil -:::::- Increase MnT counter at
CP:ClientProvisioning.ProvisionedResource.AC-44-Posture
```

Finestra Testo 5-11

Nel passo successivo, potete vedere il processo di selezione dei requisiti di postura. Al termine della fase, viene preparato un elenco di requisiti che viene restituito all'agente:

```
2017-02-23 18:00:00,372 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:user1:::- About to query posture policy for user
user1 with endpoint mac 00-0b-7f-d0-f8-f4
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureManager -:user1:::- agentCMVersion=4.2.508.0,
agentType=AnyConnect Posture Agent, groupName=OESIS_V4_Agents -> found agent group with
displayName=4.x or later
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- User user1 belongs to groups NAC
Group:NAC:IdentityGroups:Endpoint Identity Groups:Profiled:Workstation,NAC
Group:NAC:IdentityGroups:Any
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- About to retrieve posture policy
resources for os 7 Professional, agent group 4.x or later and identity groups [NAC
Group:NAC:IdentityGroups:Endpoint Identity Groups:Profiled:Workstation, NAC
Group:NAC:IdentityGroups:Any]
2017-02-23 18:00:00,432 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- Evaluate resourceId NAC
Group:NAC:Posture:PosturePolicies:WinDefend by agent group with FQN NAC
```

Group:NAC:AgentGroupRoot:ALL:OESIS_V4_Agents
2017-02-23 18:00:00,433 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- The evaluation result by agent group for resourceId NAC Group:NAC:Posture:PosturePolicies:WinDefend is Permit
2017-02-23 18:00:00,433 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- Evaluate resourceId NAC Group:NAC:Posture:PosturePolicies:WinDefend by OS group with FQN NAC Group:NAC:OsGroupRoot:ALL:WINDOWS_ALL:WINDOWS_7_ALL:WINDOWS_7_PROFESSIONAL_ALL
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- stealth mode is 0
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- The evaluation result by os group for resourceId NAC Group:NAC:Posture:PosturePolicies:WinDefend is Permit
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- Evaluate resourceId NAC Group:NAC:Posture:PosturePolicies:WinDefend by Stealth mode NSF group with FQN NAC Group:NAC:StealthModeStandard
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- Procesing obligation with posture policy resource with id NAC Group:NAC:Posture:PosturePolicies:WinDefend
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- Found obligation id urn:cisco:cepm:3.3:xacml:response-qualifier for posture policy resource with id NAC Group:NAC:Posture:PosturePolicies:WinDefend
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- Found obligation id PostureReqs for posture policy resource with id NAC Group:NAC:Posture:PosturePolicies:WinDefend
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- Posture policy resource id WinDefend has following associated requirements []
2017-02-23 18:00:03,884 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cpm.posture.runtime.agent.AgentXmlGenerator -:user1:::- policy enforcemnt is 0
2017-02-23 18:00:03,904 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cpm.posture.runtime.agent.AgentXmlGenerator -:user1:::- simple condition: [Name=WinDefend, Descriptionnull, Service Name=WinDefend, Service Operator=Running, Operating Systems=[Windows All], Service Type=Daemon, Exit code=0]
2017-02-23 18:00:03,904 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cpm.posture.runtime.agent.AgentXmlGenerator -:user1:::- check type is Service
2017-02-23 18:00:04,069 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:user1:::- NAC agent xml <?xml version="1.0" encoding="UTF-8"?><cleanmachines>
<version>ISE: 2.2.0.470</version>
<encryption>0</encryption>
<package>
<id>10</id>

WinDefend

```
</package>
</cleanmachines>
```

Finestra Testo 5-12

In seguito, è possibile vedere che il report sulla postura è stato ricevuto dal PSN:

```
2017-02-23 18:00:04,231 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:::::- UDID is
8afb76ad11e60531de1d3e7d2345dbba5f11a96d for end point 00-0b-7f-d0-f8-f4
2017-02-23 18:00:04,231 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:::::- Received posture request [parameters:
reqtype=report, userip=10.62.145.44, clientmac=00-0b-7f-d0-f8-f4, os=WINDOWS,
osVerison=1.2.1.6.1.48, architecture=9, provider=Device Filter, state=, userAgent=Mozilla/4.0
(compatible; WINDOWS; 1.2.1.6.1.48; AnyConnect Posture Agent v.4.4.00243),
session_id=c0a801010009e00058af0f7b
```

Finestra Testo 5-13

Alla fine del flusso, ISE contrassegna l'endpoint come conforme e avvia il processo COA:

```
2017-02-23 18:00:04,272 INFO [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureManager -:user1:::- Posture state is compliant for endpoint
with mac 00-0b-7f-d0-f8-f4
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureCoA -:user1:::- entering triggerPostureCoA for session
c0a801010009e00058af0f7b
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureCoA -:user1:::- Posture CoA is scheduled for session id
[c0a801010009e00058af0f7b]
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureCoA -:user1:::- Posture status for session id
c0a801010009e00058af0f7b is Compliant
2017-02-23 18:00:04,273 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureCoA -:user1:::- Issue CoA on active session with sessionID
c0a801010009e00058af0f7b
2017-02-23 18:00:04,273 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureCoA -:user1:::- Posture CoA is scheduled for session id
[c0a801010009e00058af0f7b]
```

Finestra Testo 5-14

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).