

# Vergelijk eerdere ISE-versies met ISE Posture Flow in ISE 2.2

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Posture Flow Pre ISE 2.2](#)

[Posture Flow in ISE 2.2](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Configuratie van clientprovisioning](#)

[Houdbaarheid beleid en voorwaarden](#)

[Het client-provisioningportal configureren](#)

[Autorisatieprofielen en -beleid configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Algemene informatie](#)

[Gemeenschappelijke problemen oplossen](#)

[Verwante problemen met betrekking tot SO](#)

[Selectie van beleid voor clientprovisioning voor probleemoplossing](#)

[Opdrachtproces voor probleemoplossing](#)

## Inleiding

Dit document beschrijft de vergelijking van de postuur in ISE 2.2 met de postuur in ISE-versies eerder dan 2.2.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Houdbaarheid op ISE
- Configuratie van postuur componenten op ISE
- Adaptieve security applicatie (ASA) configuratie voor postuur via Virtual Private Networks (VPN)

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ISE-versie 2.2
- Cisco ASA met software 9.6 (2)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

Dit document beschrijft een nieuwe functionaliteit in Identity Service Engine (ISE) 2.2 die ISE in staat stelt om een postenstroom te ondersteunen zonder enige omleidingsondersteuning op een Network Access Device (NAD) of ISE.

Positie is een kerncomponent van Cisco ISE. Positie als component kan worden weergegeven door drie hoofdelementen:

1. ISE als beleidsconfiguratie, distributie en beslissingspunt.  
Vanuit het beheerdersperspectief op ISE configureert u postuur-beleid (aan welke exacte voorwaarden moet worden voldaan om een apparaat te markeren als compatibel met de bedrijfsvoering), client provisioningbeleid (welke agent software moet worden geïnstalleerd op welk soort apparaten) en autorisatiebeleid (aan welk soort machtigingen moet worden toegewezen, hangt af van hun postuur-status).
2. Een netwerktoegangsapparaat als een beleidshandhavingpunt.  
Aan de NAD-zijde worden de werkelijke autorisatiebeperkingen toegepast op het moment van de gebruikersverificatie. ISE als beleidspunt biedt autorisatieparameters zoals gedownloade ACL (dACL)/VLAN/Redirect-URL/Redirect Access Control List (ACL). Traditioneel, om postuur te laten gebeuren, zijn NAD's vereist om omleiding te ondersteunen (om gebruikers of agent software te instrueren met welke ISE-knooppunt contact moet worden opgenomen) en wijziging van autorisatie (CoA) om de gebruiker opnieuw te authenticeren nadat de postuur status van het eindpunt is bepaald.
3. Software van de agent als punt van gegevensverzameling en interactie met de eindgebruiker.  
Cisco ISE maakt gebruik van drie typen agent-software: AnyConnect ISE-poortmodule, NAC-agent en Web Agent. De agent ontvangt informatie over de positievereisten van de ISE en geeft een rapport aan de ISE over de status van de vereisten.

**Opmerking:** dit document is gebaseerd op AnyConnect ISE-poortmodule, de enige die postuur volledig ondersteunt zonder omleiding.

In de pre-ISE 2.2 stroomhouding, worden NADs niet alleen gebruikt om gebruikers te verifiëren en toegang te beperken, maar ook om informatie aan agent software over een specifiek knooppunt van ISE te verstrekken dat moet worden gecontacteerd. Als onderdeel van het omleidingsproces wordt de informatie over de ISE-knooppunt teruggestuurd naar de agent-software.

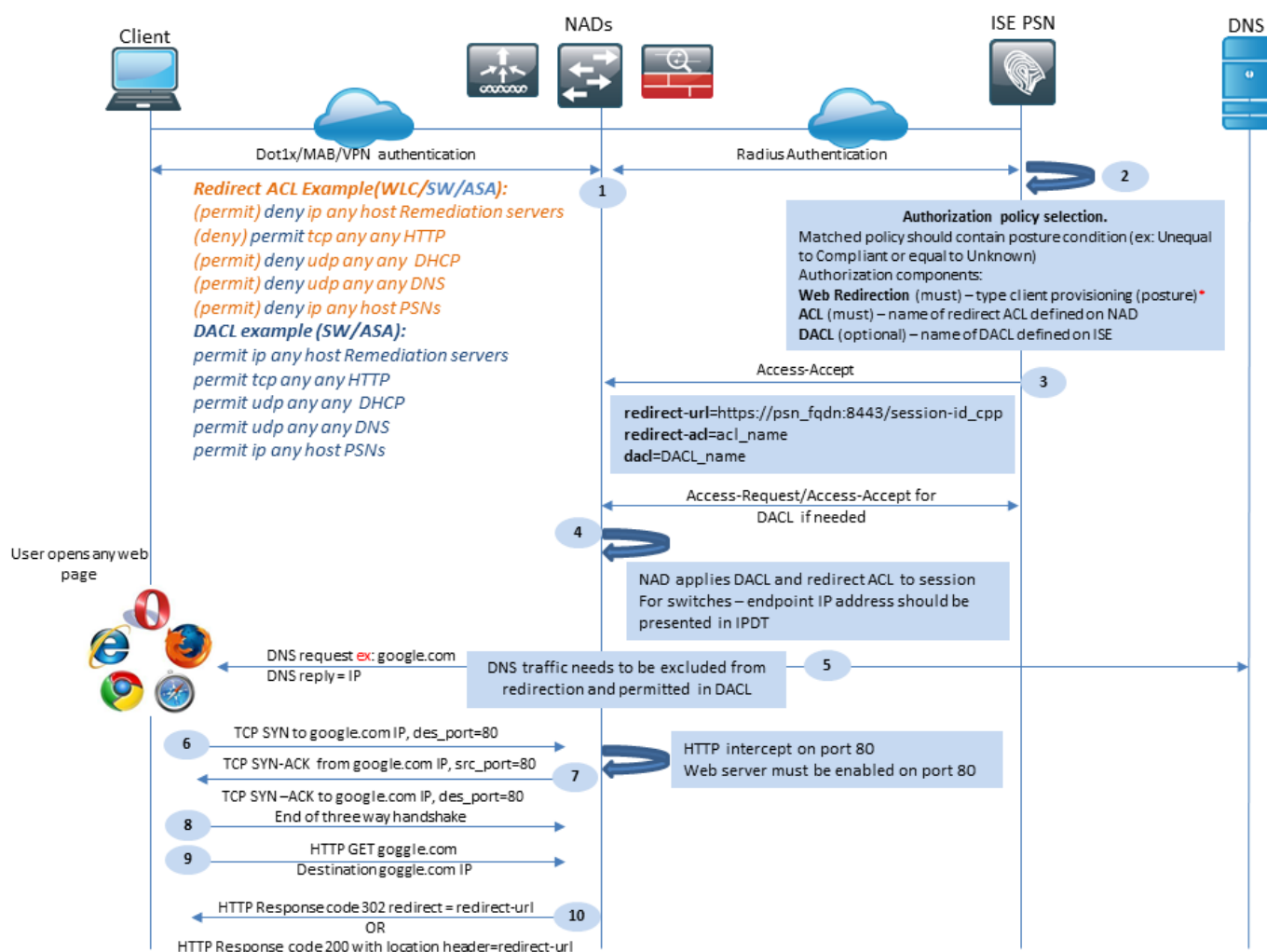
Van oudsher was de omleidingsteun aan NAD of aan ISE-zijde een essentiële voorwaarde voor de uitvoering van de houding. In ISE 2.2 wordt de eis om omleiding te ondersteunen geëlimineerd voor zowel de initiële client provisioning en postuur proces.

Clientprovisioning zonder omleiding - In ISE 2.2 hebt u rechtstreeks toegang tot de Client Provisioning Portal (CPP) via de portal Fully Qualified Domain Name (FQDN). Dit is vergelijkbaar met de manier waarop u toegang hebt tot Sponsor Portal of MyDevice Portal.

Posture proces zonder omleiding - Tijdens agent installatie van de CPP portal informatie over ISE servers wordt opgeslagen aan de kant van de klant, waardoor directe communicatie mogelijk wordt.

## Posture Flow Pre ISE 2.2

Dit beeld toont een stapsgewijze uitleg van de AnyConnect ISE-poortmodule voorafgaand aan ISE 2.2:



Figuur 1-1

Stap 1. Verificatie is de eerste stap van de stroom, het kan dot1x, MAB of VPN zijn.

Stap 2. ISE moet een authenticatie- en autorisatiebeleid voor de gebruiker kiezen. In het posturescenario moet het gekozen toelatingsbeleid een verwijzing bevatten naar de postuur

status, die aanvankelijk onbekend of niet van toepassing moet zijn. Om beide gevallen te dekken, kunnen voorwaarden met postuur status ongelijke naleving worden gebruikt.

Het gekozen autorisatieprofiel moet informatie bevatten over omleiding:

- Web Redirection- Voor het postuur geval, moet het web redirectie type worden gespecificeerd als client provisioning (postuur).
- ACL - Deze sectie moet de ACL-naam bevatten die aan de NAD-kant is geconfigureerd. Deze ACL wordt gebruikt om instructies te geven en te bepalen welk verkeer de omleiding moet omzeilen en welke daadwerkelijk omgeleid moet worden.
- DACL - Het kan samen met redirect access-list worden gebruikt, maar u moet in gedachten houden dat verschillende platforms DACL verwerken en ACL's in een andere volgorde omleiden.

ASA verwerkt bijvoorbeeld altijd DACL voordat ACL wordt omgeleid. Tegelijkertijd verwerken sommige switch-platforms het op dezelfde manier als ASA, en andere switch-platforms verwerken eerst Redirect ACL en controleren vervolgens DACL/Interface ACL als het verkeer moet worden verboden of toegestaan.

**Opmerking:** nadat u de optie voor webomleiding in het autorisatieprofiel hebt ingeschakeld, moet het doelportal voor omleiding worden gekozen.

Stap 3. ISE retourneert access-Accept met autorisatiekenmerken. Redirect URL in autorisatiekenmerken wordt automatisch gegenereerd door ISE. Het bevat de volgende onderdelen:

- FQDN van ISE-knooppunt waarop verificatie heeft plaatsgevonden. In bepaalde gevallen kan dynamische FQDN worden overschreven door de configuratie van het autorisatieprofiel (statische IP/Hostnaam/FQDN) in de sectie Webomleiding. Als de statische waarde wordt gebruikt, moet deze naar hetzelfde ISE-knooppunt wijzen waar de verificatie is verwerkt. In het geval van Load Balancer (LB) kan dit FQDN naar LB VIP wijzen, maar alleen als LB is geconfigureerd om RADIUS- en SSL-verbindingen te koppelen.
- Port - De poortwaarde wordt verkregen uit de doelpoortconfiguratie.
- Session ID - Deze waarde wordt door ISE overgenomen van de Cisco AV-controlesessie-id die in Access-request is gepresenteerd. De waarde zelf wordt dynamisch gegenereerd door NAD.
- Portal ID-identificatiecode van een doelportal aan de kant van de ISE.

Stap 4. En past een autorisatiebeleid toe op de sessie. Bovendien, als DACL wordt geconfigureerd, wordt de inhoud ervan gevraagd voordat het autorisatiebeleid wordt toegepast.

Belangrijke overwegingen:

- Al NADs - het Apparaat moet lokaal gevormde ACL met de zelfde naam hebben die in toegang-Accepteer zoals redirect-acl wordt ontvangen.
- Switches- Het IP-adres van de client moet worden weergegeven in de uitvoer van `show authentication session interface details` opdracht om omleiding en ACL's toe te passen. Het IP-adres van de client wordt geleerd door de IPDT (IP Device Tracking Feature).

Stap 5. De client stuurt een DNS-verzoek voor de FQDN die in de webbrowser is ingevoerd. In

deze fase moet DNS-verkeer omleiding omzeilen en moet het juiste IP-adres door de DNS-server worden geretourneerd.

Stap 6. De client stuurt TCP SYN naar het IP-adres dat in het DNS-antwoord wordt ontvangen. Het IP-bronadres in het pakket is de client-IP en het IP-adres van de bestemming is het IP-adres van de gevraagde bron. De bestemmingshaven is gelijk aan 80, behalve in gevallen waarin een directe HTTP proxy is geconfigureerd in de client web browser.

Stap 7. NAD onderschept clientverzoeken en bereidt SYN-ACK-pakketten voor met een IP-bron gelijk aan de gevraagde IP-bron, een IP-bestemming gelijk aan de IP-client en een IP-bronpoort gelijk aan 80.

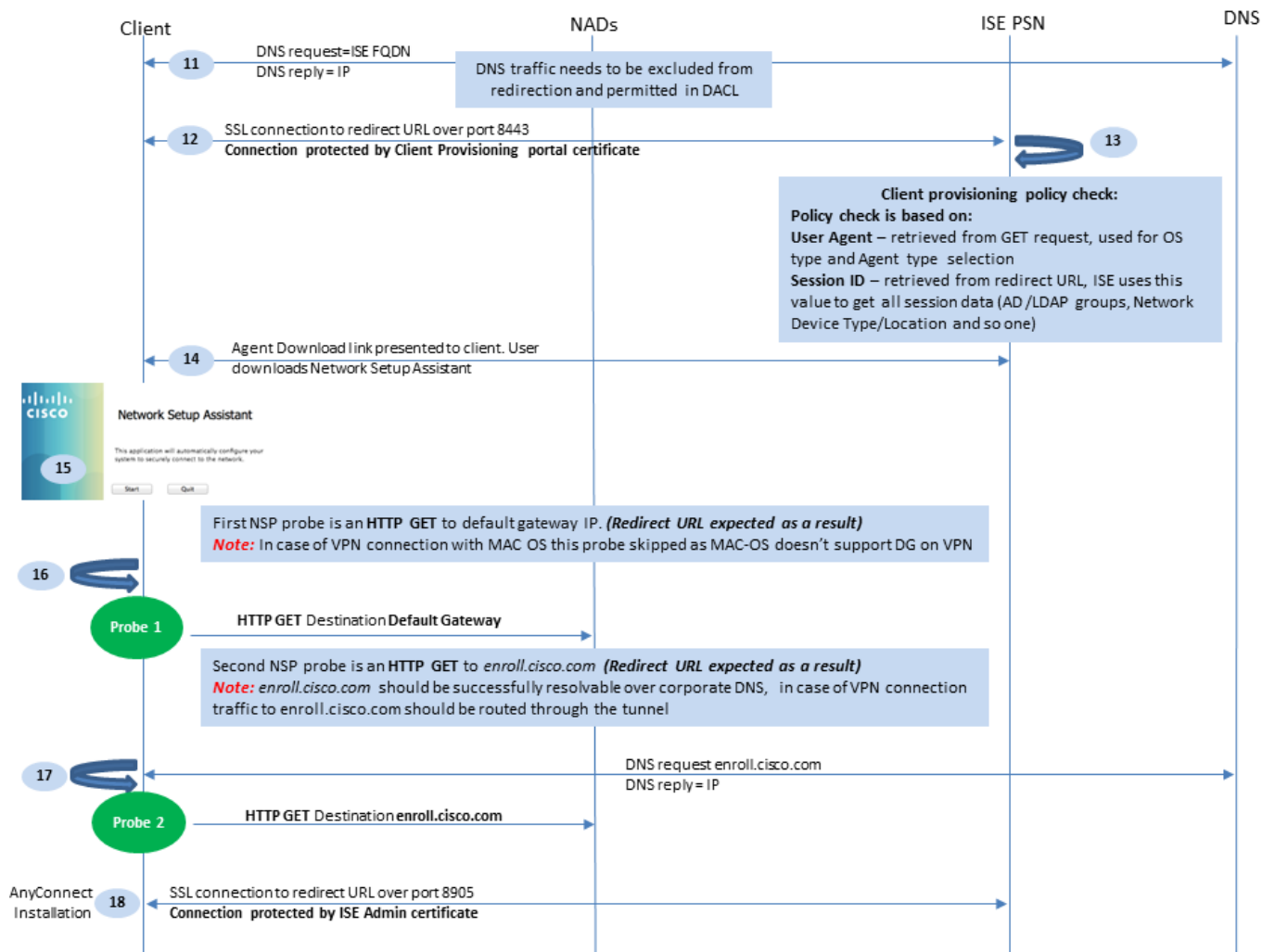
Belangrijke overwegingen:

- NAD's moeten een HTTP-server hebben die actief is op de poort waarop de client aanvragen verstuurt. Standaard is het poort 80.
- Als de client een directe HTTP proxy webserver gebruikt, moet de HTTP-server op de proxy-poort op NAS draaien. Dit scenario valt buiten het bereik van dit document.
- In de gevallen waarin NAD geen lokaal IP-adres in de client heeft, wordt subnetvoeding SYN-ACK verzonden met NAD Routing-tabel (meestal via beheerinterface). In dit scenario wordt het pakket via L3-infrastructuur gerouteerd en moet het door een L3 upstream-apparaat naar de client worden teruggeleid. Als het L3-apparaat een stateful firewall is, moet er een extra uitzondering worden gemaakt voor een dergelijke asymmetrische routing.

Stap 8. De client voltooit de drieweg-handdruk TCP door ACK.

Stap 9. HTTP GET voor de target resource wordt verzonden door een client.

Stap 10. NAD retourneert een omleiding URL naar de client met HTTP code 302 (pagina verplaatst), op sommige NADs redirect kan worden teruggestuurd binnen het HTTP 200 OK bericht in de locatie header.



Figuur 1-2

Stap 11. De client stuurt een DNS-verzoek voor de FQDN via de doorverwijzing naar URL. FQDN moet oplosbaar zijn aan de DNS-serverkant.

Stap 12. SSL-verbinding via poort ontvangen in omleiding URL is ingesteld (standaard 8443). Deze verbinding wordt beschermd door een portaalcertificaat van de kant van de ISE. Client Provisioning Portal (CPP) wordt aan de gebruiker gepresenteerd.

Stap 13. Voordat u een downloadoptie aan de client biedt, moet ISE het beleid voor doelclientprovisioning (CP) kiezen. Het bewerkingsysteem (OS) van de client die is gedetecteerd vanuit de browser-user-agent en andere informatie die vereist is voor CPP-beleidsselectie worden opgehaald uit de verificatiesessie (zoals AD/LDAP-groepen enzovoort). ISE kent de doelsessie van de sessie-id in de omleiding-URL.

Stap 14. Network Setup Assistant (NSA) downloadlink wordt naar de client teruggestuurd. De client downloadt de toepassing.

**Opmerking:** normaal kunt u NSA zien als onderdeel van BYOD flow voor Windows en Android, maar ook deze toepassing kan worden gebruikt om AnyConnect of zijn componenten van ISE te installeren.

Stap 15. De gebruiker voert de NSA-toepassing uit.

Stap 16. NSA verstuurt de eerste detectiesonde - HTTP /auth/discovery naar de Default gateway. De NSA verwacht dat dit zal resulteren in een herverwijzende url.

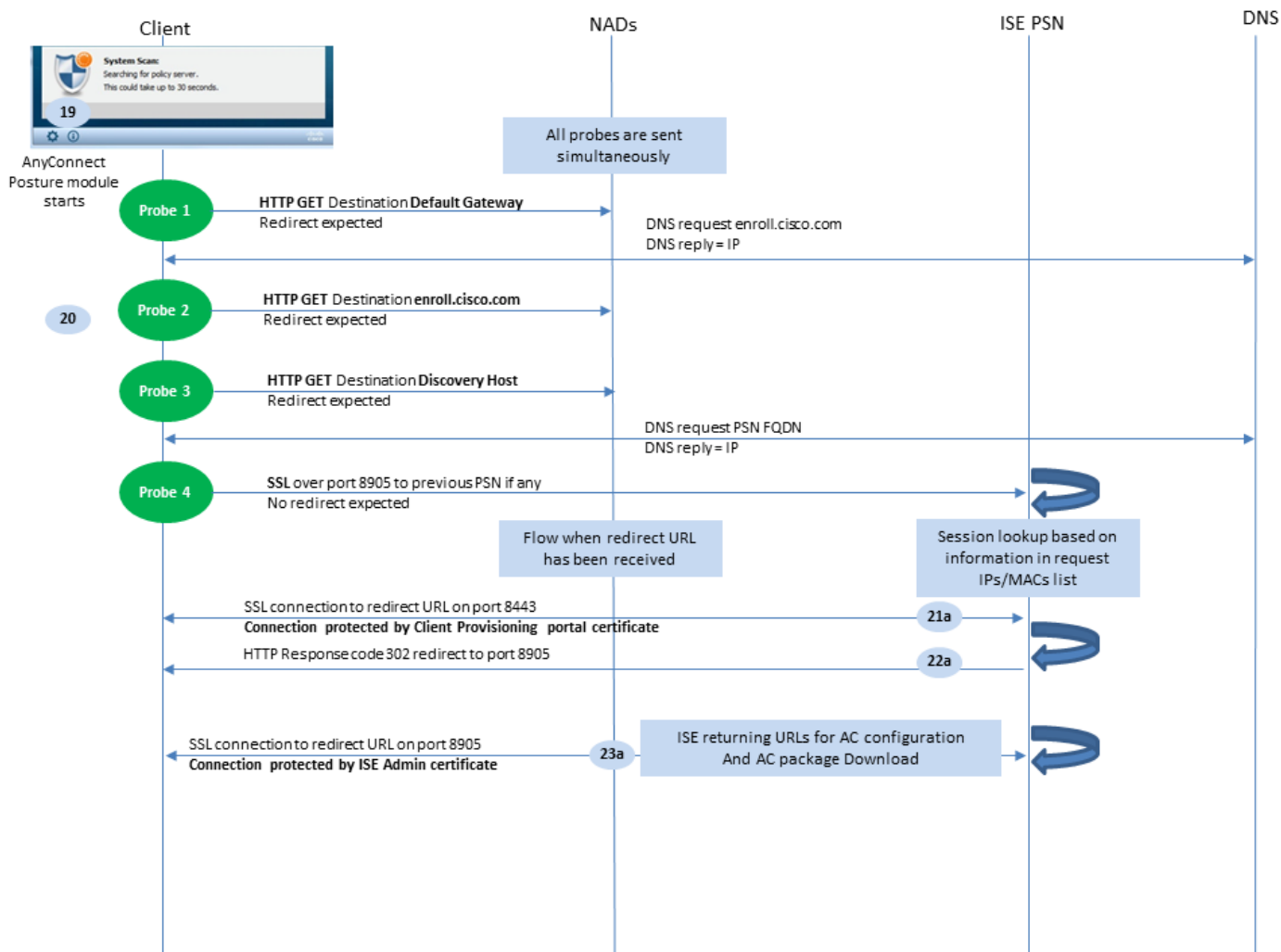
**Opmerking:** voor verbindingen via VPN op MAC OS-apparaten wordt deze sonde genegeerd omdat MAC OS geen standaardgateway heeft op de VPN-adapter.

Stap 17. NSA stuurt een tweede sonde als de eerste mislukt. De tweede sonde is een HTTP GET /auth/discovery to `enroll.cisco.com`. Dit FQDN moet met succes door de DNS server kunnen worden opgelost. In een VPN-scenario met een gesplitste tunnel kan verkeer naar `enroll.cisco.com` moeten door de tunnel worden geleid.

Stap 18. Als één van de sondes slaagt, vestigt NSA een SSL verbinding over haven 8905 met informatie die uit redirect-url wordt verkregen. Deze verbinding wordt beschermd door het ISE-beheercertificaat. Binnen deze verbinding NSA downloads Anyconnect.

Belangrijke overwegingen:

- Voorafgaand aan ISE 2.2 release is SSL-communicatie via poort 8905 een vereiste voor postuur.
- Om certificaatwaarschuwingen te voorkomen, moeten zowel portal- als beheercertificaten aan de clientzijde worden vertrouwd.
- In multi-interface ISE-implementaties kunnen interfaces anders dan G0 worden gebonden aan FQDN op een andere manier dan systeem FQDN (met het gebruik van `ip host CLI-opdracht`). Dit kan problemen opleveren met de validatie van Onderwerpnaam (SN)/Onderwerp Alternatieve Naam (SAN). Als de client van interface G1 wordt omgeleid naar FQDN, kan het systeem FQDN bijvoorbeeld verschillen van de FQDN in de omleiding URL voor het 8905 communicatiecertificaat. Als oplossing voor dit scenario kunt u FQDN's van extra interfaces toevoegen in SAN-velden met beheercertificaat, of u kunt een jokerteken gebruiken in het beheercertificaat.



Figuur 1-3

Stap 19. AnyConnect ISE-poortproces wordt gestart.

AnyConnect ISE-poortmodule start in een van deze situaties:

- Na de installatie
- Na de standaardwijziging van de gatewaywaarde
- Nadat de systeembebruiker zich heeft aangemeld
- Na de gebeurtenis van de systeemmacht

Stap 20. In deze fase start AnyConnect ISE-poortmodule de detectie van beleidsservers. Dit wordt bereikt met een reeks sondes die tegelijkertijd worden verzonden door de AnyConnect ISE-poortmodule.

- Probe 1 - HTTP krijgt /auth/discovery om standaard gateway IP. U moet onthouden dat MAC OS-apparaten geen standaardgateway hebben op de VPN-adapter. Het verwachte resultaat voor de sonde is redirect-url.
- Sonde 2 - HTTP GET/auth/discovery naar server enroll.cisco.com. Dit FQDN moet met succes door de DNS server kunnen worden opgelost. In een VPN-scenario met een gesplitste tunnel kan verkeer naar enroll.cisco.com moeten door de tunnel worden geleid. Het verwachte resultaat voor de sonde is redirect-url.
- Probe 3 - HTTP krijgt /auth/discovery naar discovery host. De waarde van de Discovery-host wordt tijdens de installatie in het AC-poortprofiel teruggestuurd van ISE. Het verwachte



resultaat voor de sonde is redirect-url.

- Probe 4 - HTTP GET /auth/status via SSL op poort 8905 naar eerder verbonden PSN. Dit verzoek bevat informatie over client-IP's en MAC's voor sessielaadpleging aan de kant van ISE. Dit probleem wordt niet getoond tijdens de eerste poging van de houding. De verbinding wordt beschermd door een ISE-beheercertificaat. Als gevolg van deze sonde kan ISE de sessie-ID terugsturen naar de client als de knooppunt waar de sonde landt, hetzelfde knooppunt is waar de gebruiker is geverifieerd.

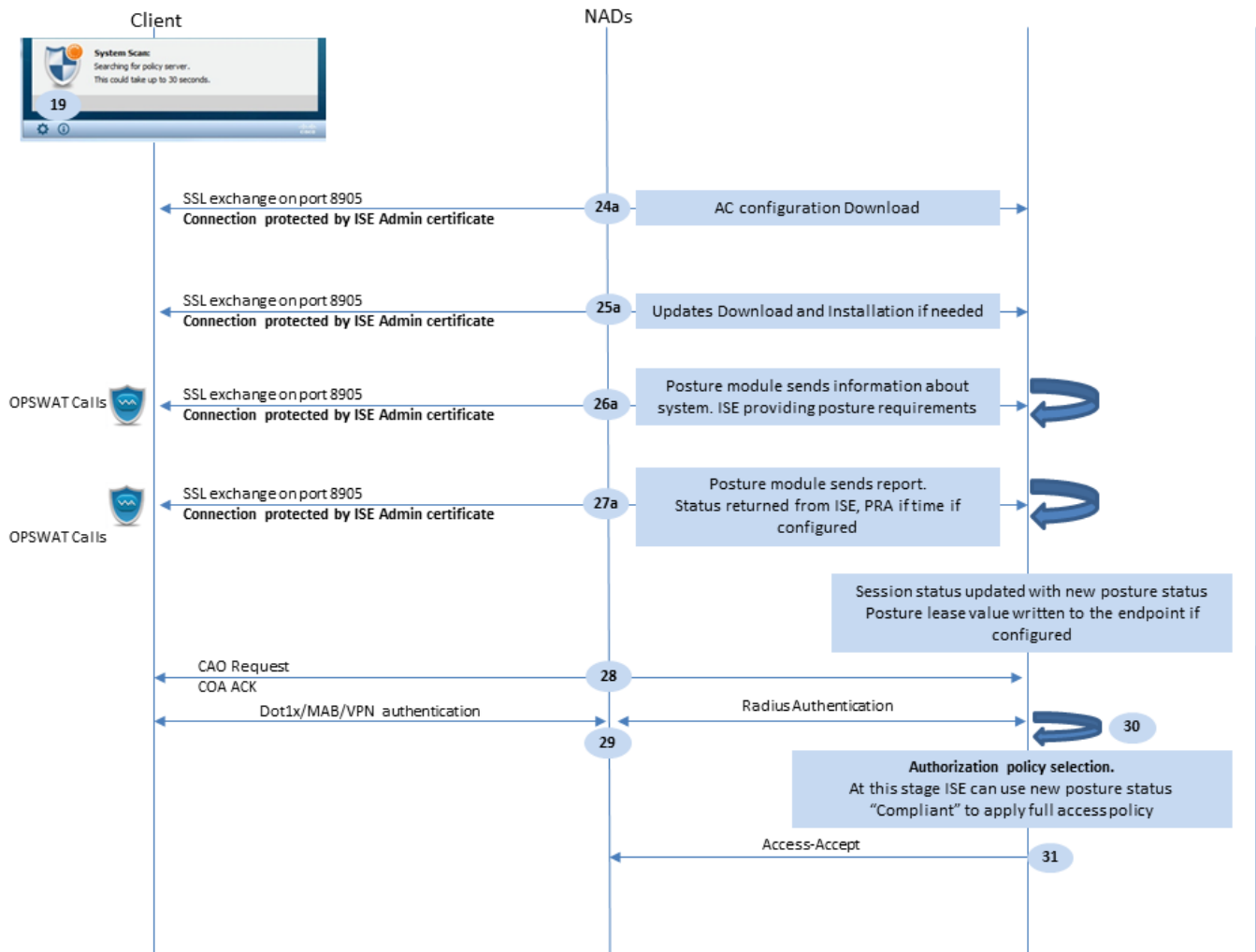
**Opmerking:** dankzij deze sonde kan postuur succesvol worden uitgevoerd, zelfs zonder omleiding onder bepaalde omstandigheden. Een succesvolle houding zonder omleiding vereist dat het huidige PSN dat de sessie heeft geverifieerd, hetzelfde is als het eerder met succes verbonden PSN. Houd in gedachten dat voor ISE 2.2, een succesvolle houding zonder omleiding eerder een uitzondering dan een regel is.

De volgende stappen beschrijven het postuur proces in het geval wanneer de omleiden URL wordt ontvangen (stroom gemarkeerd met letter a) als resultaat van een van de sondes.

Stap 21. AnyConnect ISE Posture-module maakt een verbinding met het client-provisioningportal met het gebruik van een URL die tijdens de detectiefase wordt opgehaald. In dit stadium, maakt ISE nogmaals client provisioning beleid validatie met het gebruik van de informatie van de geverifieerde sessies.

Stap 2. Als het beleid voor clientprovisioning is gedetecteerd, keert ISE terug naar poort 8905.

Stap 23. Agent maakt verbinding met ISE via poort 8905. Tijdens deze verbinding retourneert ISE URL's voor het postuur profiel, compliance module en eventuele connect updates.



Figuur 1-4

Stap 24.AC ISE Posture module configuratie downloaden van ISE.

Stap 25.Updates downloaden en installeren indien nodig.

Stap 26. AC ISE Posture module verzamelt initiële informatie over het systeem (zoals OS versie, geïnstalleerde security producten en hun definitie versie). In deze fase, de AC ISE posteringsmodule impliceert OPSWAT API om informatie over veiligheidsproducten te verzamelen. De verzamelde gegevens worden naar ISE verzonden. Als antwoord op dit verzoek, verstrekt ISE een lijst van de houdingsvereisten. De behoeftenlijst wordt geselecteerd als resultaat van de verwerking van het postuur beleid. Om het juiste beleid aan te passen, gebruikt ISE de apparaatbesturingsversie (aanwezig in het verzoek) en de waarde van de sessie-id om andere vereiste kenmerken (AD/LDAP-groepen) te selecteren. De waarde van de sessie-ID wordt ook door de client verzonden.

Stap 27. In deze stap, de cliënt impliceert OPSWAT vraag en andere mechanismen om houdingsvereisten te controleren. Het eindverslag met de lijst van vereisten en hun status worden naar ISE verzonden. ISE moet de definitieve beslissing nemen over de nalevingsstatus van het eindpunt. Als het eindpunt bij deze stap als niet-conform wordt gemarkeerd, wordt een reeks herstelacties geretourneerd. Voor het conforme eindpunt schrijft ISE compliance status in de sessie en zet ook de laatste posture timestamp in de endpointattributen als Posture Lease is geconfigureerd. Het resultaat van de houding wordt teruggestuurd naar het eindpunt. Bij de Posture Reassessment (PRA) wordt de tijd voor PRA ook door ISE in dit pakket gezet.

Bij een niet-conform scenario moet rekening worden gehouden met deze punten:

- Sommige remediëringsmaatregelen (zoals tekstberichten weergeven, link remediatie, bestandssanering en andere) worden uitgevoerd door de postuur zelf.
- Andere soorten herstel (zoals AV, AS, WSUS en SCCM) vereisen OPSWAT API communicatie tussen de postuur agent en het doelproduct. In dit scenario stuurt postuur agent gewoon een verzoek om herstel naar het product. Oplossing zelf wordt direct uitgevoerd door de beveiligingsproducten.

**Opmerking:** in het geval dat beveiligingsproducten moeten communiceren met externe bronnen (interne/externe updateservers) moet u ervoor zorgen dat deze communicatie is toegestaan in Redirect-ACL/DACL.

Stap 28. ISE stuurt een COA-verzoek naar de NAD die een nieuwe authenticatie voor de gebruiker moet starten. En moet dit verzoek van COA ACK bevestigen. Houd in gedachten dat voor de VPN-cases COA push wordt gebruikt, zodat er geen nieuwe verificatieaanvraag wordt verzonden. In plaats daarvan, ASA verwijdert vorige vergunningsparameters (opnieuw richten URL, opnieuw richten ACL, en DACL) uit de zitting en past nieuwe parameters van het verzoek van Cacao toe.

Stap 29. Nieuwe verificatieaanvraag voor de gebruiker.

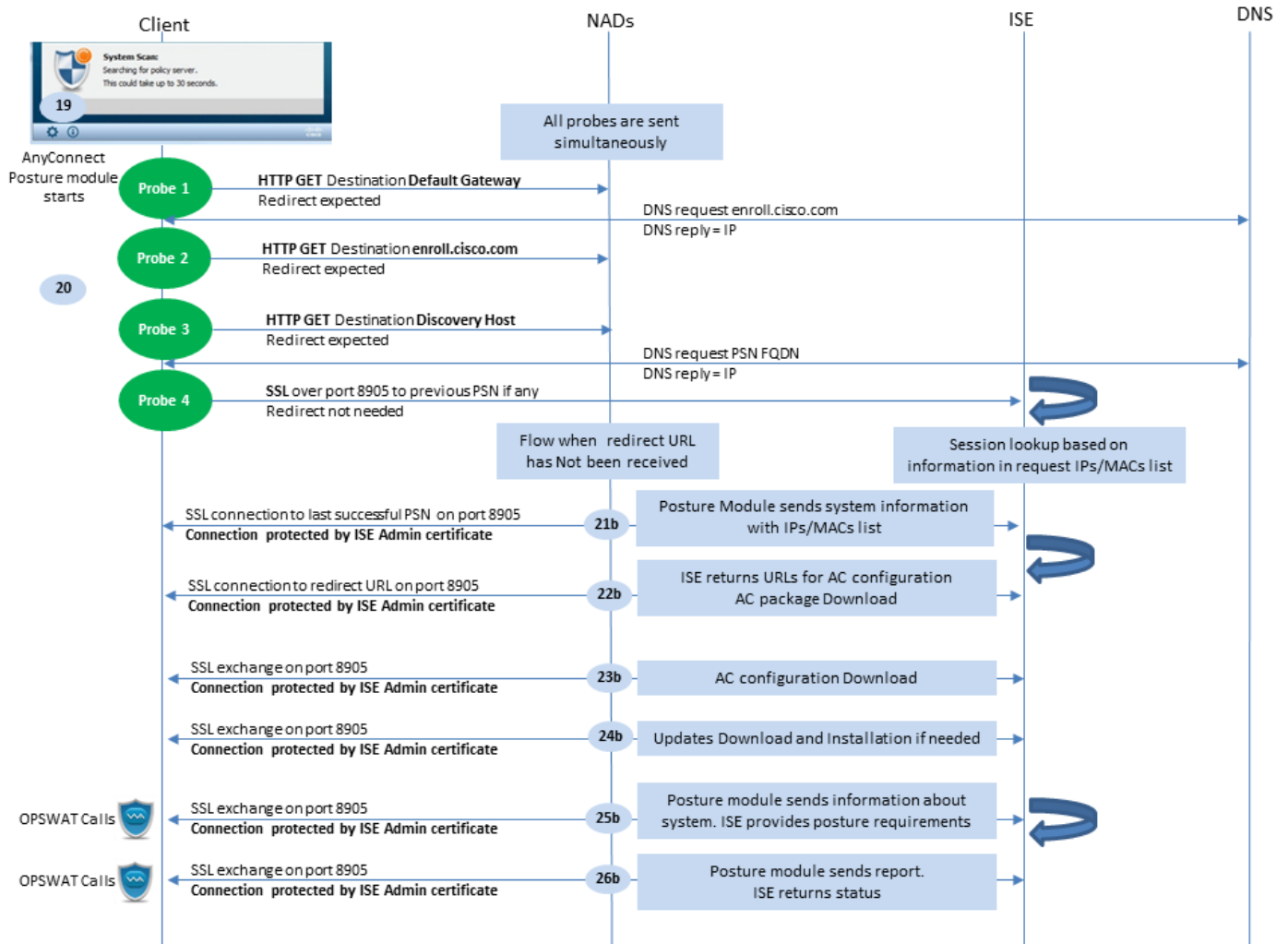
Belangrijke overwegingen:

- Typisch voor Cisco NAD COA, wordt de rede gebruikt door ISE, en dit instrueert en initieert een nieuw verificatieverzoek met de vorige sessie-ID.
- Aan de kant van ISE is dezelfde sessie-ID-waarde een indicatie dat eerder verzamelde sessiekenmerken opnieuw moeten worden gebruikt (klachtenstatus in ons geval) en een nieuw autorisatieprofiel op basis van die kenmerken moet worden toegewezen.
- In het geval van een sessie-ID-wijziging wordt deze verbinding als nieuw behandeld en wordt het volledige postuur opnieuw gestart.
- Om heropstelling te voorkomen bij elke wijziging van een sessie-id kan een postuur-lease worden gebruikt. In dit scenario wordt informatie over de postuur status opgeslagen in de endpointkenmerken die op de ISE blijven, zelfs als de sessie-id wordt opgeslagen. Die is gewijzigd.

Stap 30. Aan de ISE-zijde wordt een nieuw autorisatiebeleid gekozen op basis van de status van postuur.

Stap 31. Access-Accept met nieuwe autorisatiekenmerken wordt naar de NAD verzonden.

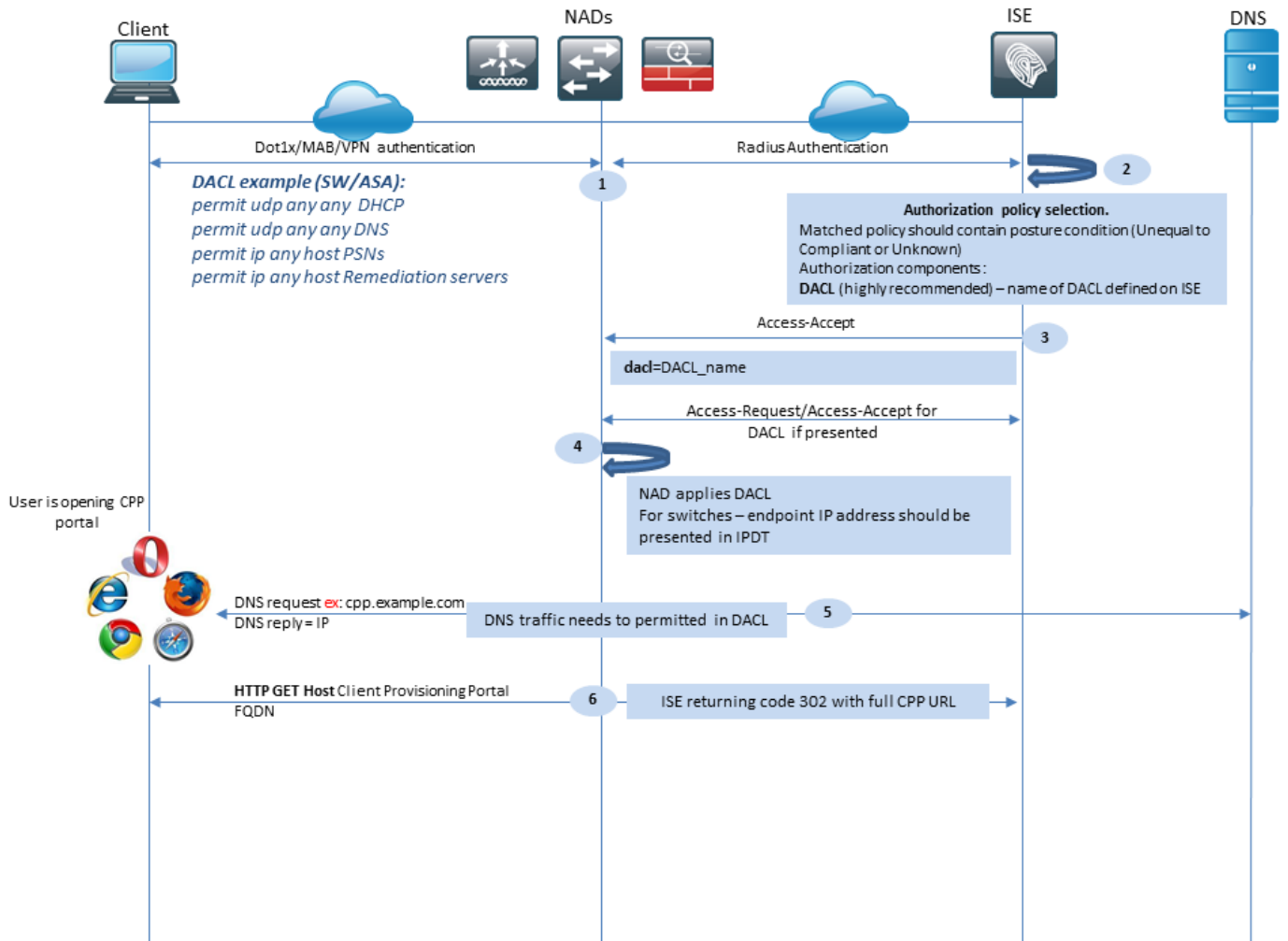
De volgende stroom beschrijft het scenario wanneer de doorverwijzing-URL niet wordt opgehaald (gemarkeerd met letter b) door een poortsonde en de eerder verbonden PSN door de laatste sonde is bevraagd. Alle stappen hier zijn precies hetzelfde als in het geval met redirect URL behalve de replay die wordt teruggestuurd door PSN als resultaat van Probe 4. Als deze sonde op dezelfde PSN landt die eigenaar is van de huidige authenticatiesessie, bevat de replay de waarde van de sessie-id die later door de postuur-agent wordt gebruikt om het proces te voltooien. In het geval dat eerder verbonden head-end niet hetzelfde is als de huidige sessie-eigenaar, is het zoeken naar sessies mislukt en wordt een leeg antwoord teruggestuurd naar de AC ISE-poortmodule. Het uiteindelijke resultaat hiervan is No Policy Server Detected bericht wordt teruggestuurd naar de eindgebruiker.



Figuur 1-5

## Posture Flow in ISE 2.2

ISE 2.2 ondersteunt zowel oude als nieuwe stijlen. Dit is de gedetailleerde verklaring voor de nieuwe stroom:



Figuur 2-1

Stap 1. Verificatie is de eerste stap van de stroom. Het kan dot1x, MAB of VPN zijn.

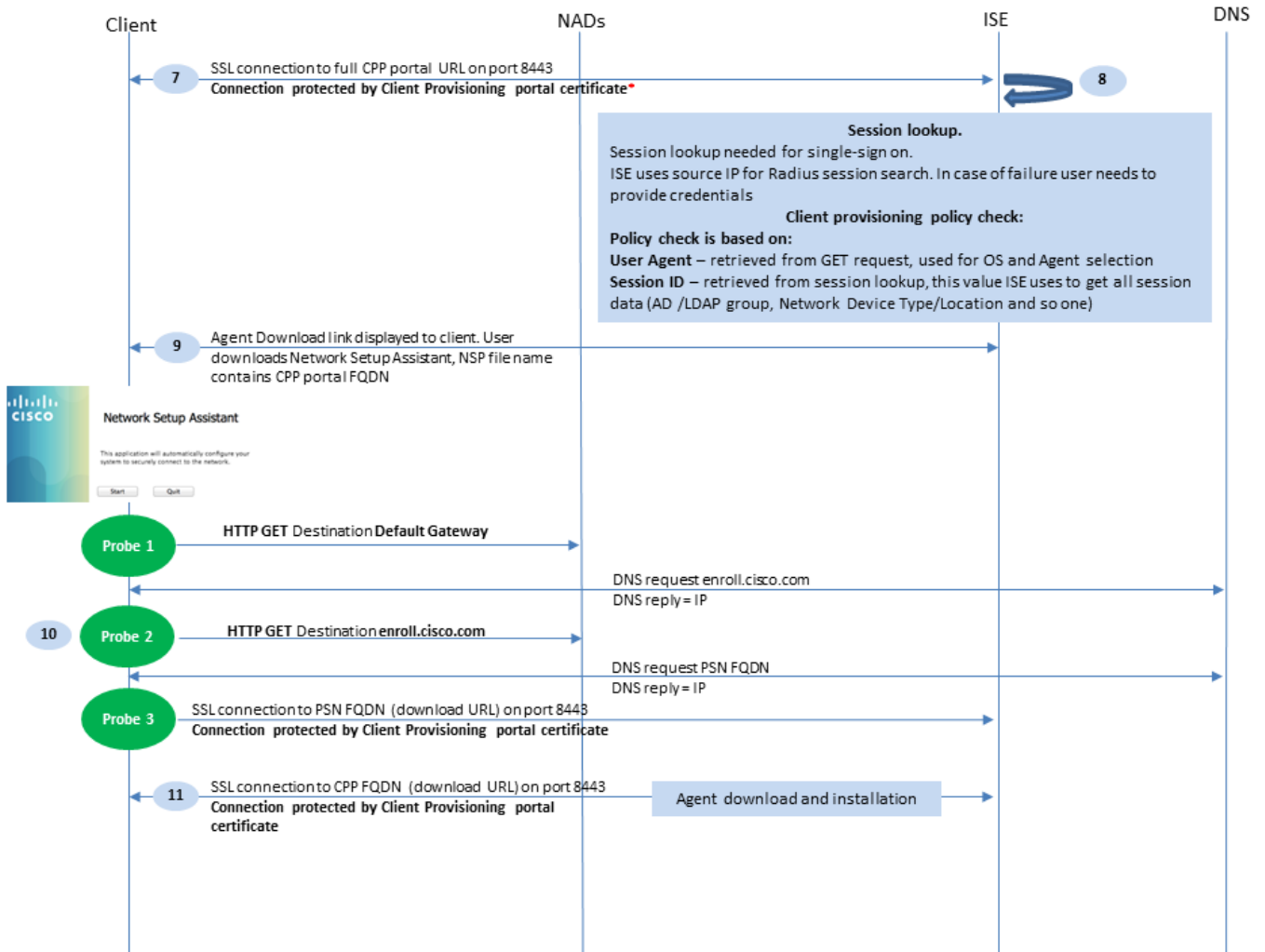
Stap 2. ISE moet de authenticatie en autorisatie beleid voor de gebruiker kiezen. In zijn houding moet het gekozen toelatingsbeleid een verwijzing bevatten naar de postuur-status, die aanvankelijk onbekend of niet van toepassing moet zijn. Om beide gevallen te dekken, kunnen voorwaarden met postuur status ongelijke naleving worden gebruikt. Voor een houding zonder omleiding, is er geen behoefte om enige configuratie van de Omleiding van het Web in het vergunningsprofiel te gebruiken. U kunt nog steeds het gebruik van een DACL of luchtruimACL overwegen om de toegang van gebruikers te beperken in het stadium wanneer de status van de postuur niet beschikbaar is.

Stap 3. ISE retourneert access-Accept met autorisatiekenmerken.

Stap 4. Als de DACL-naam wordt teruggegeven in Access-Accept, start NAD DACL-contentdownload en past het autorisatieprofiel toe op de sessie nadat het is verkregen.

Stap 5. De nieuwe benadering veronderstelt dat omleiding niet mogelijk is, zodat moet de gebruiker de client provisioning portal FQDN handmatig invoeren. FQDN van het CPP-portaal moet worden gedefinieerd in de poortconfiguratie aan de kant van de ISE. Vanuit het DNS-serverperspectief moet A-record naar de ISE-server wijzen waarbij de PSN-rol is ingeschakeld.

Stap 6. De client stuurt HTTP om naar het client provisioning portal FQDN, dit verzoek wordt geparst aan de kant van ISE en de volledige portal URL wordt teruggestuurd naar de client.



Figuur 2-2

Stap 7. SSL verbinding over poort ontvangen in omleiding URL is vastgelegd (standaard 8443). Deze verbinding wordt beschermd door een portaalcertificaat van de kant van de ISE. Het Client Provisioning Portal (CPP) wordt aan de gebruiker gepresenteerd.

Stap 8. Bij deze stap vinden twee gebeurtenissen plaats op ISE:

- Single Sign On (SSO) - ISE probeert op te zoeken naar eerdere succesvolle verificatie. ISE gebruikt het IP-bronadres uit het pakket als een zoekfilter voor live radiussessies.

**Opmerking:** sessie wordt opgehaald op basis van een overeenkomst tussen de bron IP in het pakket en framed IP-adres in de sessie. Het framed IP-adres wordt normaliter opgehaald door ISE van de tussentijdse boekhoudupdates, dus het is vereist om de boekhouding ingeschakeld aan de NAD kant. Ook moet u onthouden dat SSO alleen mogelijk is op het knooppunt dat de sessie bezit. Als de sessie bijvoorbeeld wordt geverifieerd op PSN 1, maar de FQDN zelf naar PSN2 wijst, mislukt het SSO-mechanisme.

- Opzoeken van clientprovisioningbeleid - in het geval van een succesvolle SSO kan ISE gegevens gebruiken van geverifieerde sessies en User-Agent van de clientbrowser. In het geval van een niet-succesvolle SSO moet de gebruiker aanmeldingsgegevens verstrekken en nadat de informatie over gebruikersverificatie uit de interne en externe identiteitsarchieven (AD/LDAP/interne groepen) is gehaald, kan deze worden gebruikt voor de controle van het

beleid voor clientprovisioning.

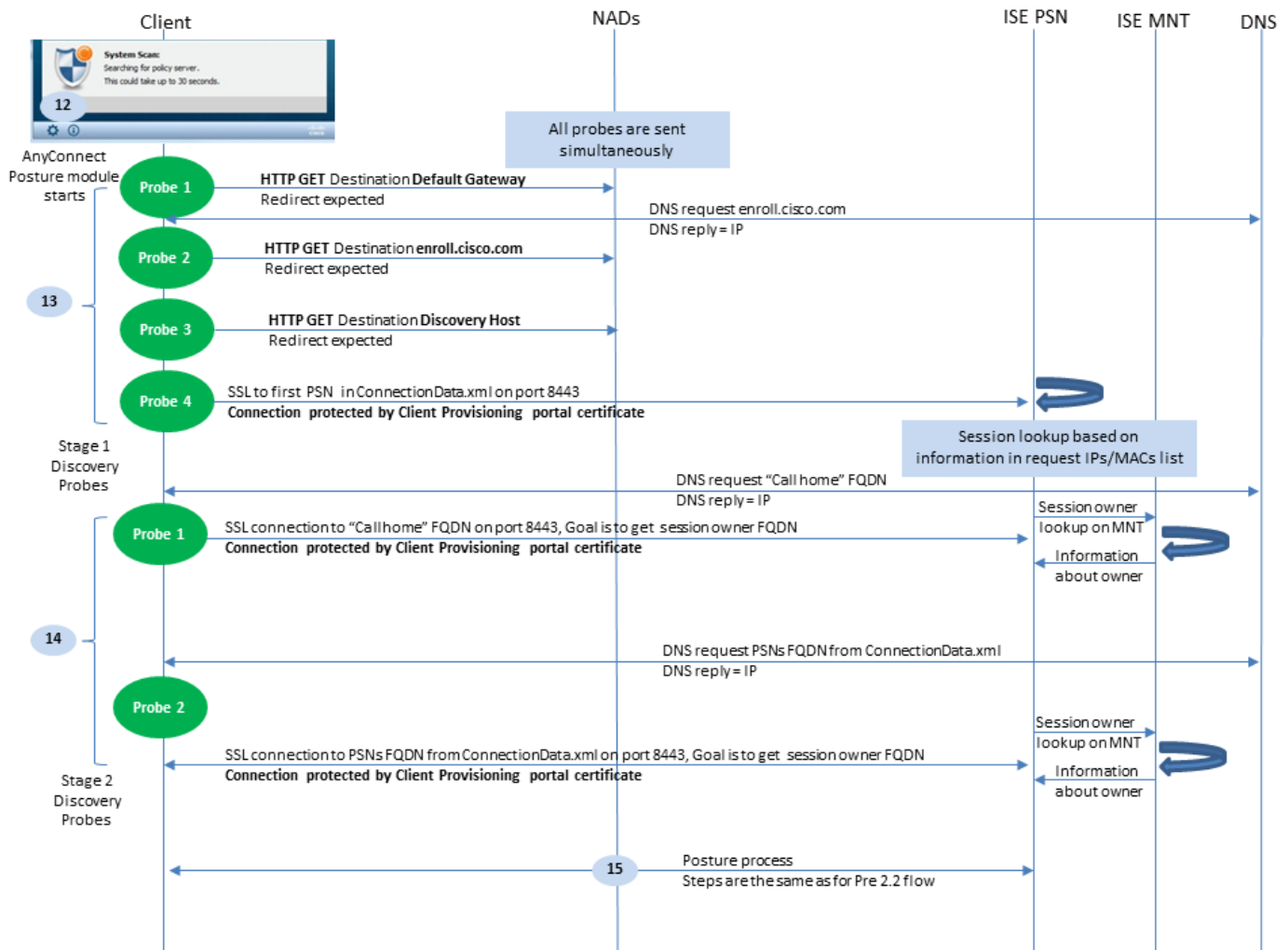
**Opmerking:** vanwege de Cisco bug-id [CSCvd1574](#), kunt u een fout zien bij de selectie van het beleid voor clientprovisioning voor de niet-SSO-gevallen waarin de externe gebruiker lid is van meerdere AD/LDAP-groepen die zijn toegevoegd in de configuratie van de externe identiteitsopslag. Het genoemde defect is bevestigd dat begint vanaf ISE 2.3 FCS en de fix vereist om te gebruiken van bevat in voorwaarde met AD-groep in plaats van EQUAL.

Stap 9. Na de selectie van het beleid van de cliëntlevering, toont ISE de agent download URL aan de gebruiker. Nadat u op download NSA klikt, wordt de toepassing naar de gebruiker geduwd. NSA filename bevat FQDN van het CPP portaal.

Stap 10. In deze stap, NSA stelt sondes in werking om een verbinding aan ISE te vestigen. Twee sondes zijn klassieke sondes, en de derde is ontworpen om de ontdekking van ISE in milieu's zonder url omleiding toe te staan.

- NSA verstuurt de eerste detectiesonde - HTTP /auth/discovery naar de Default gateway. De NSA verwacht dat dit zal resulteren in een herverwijzende url.
- NSA stuurt een tweede sonde als de eerste mislukt. De tweede sonde is een HTTP GET /auth/discovery to `enroll.cisco.com`. Dit FQDN moet met succes door de DNS server kunnen worden opgelost. In een VPN-scenario met een gesplitste tunnel kan verkeer naar `enroll.cisco.com` moeten door de tunnel worden geleid.
- NSA verstuurt de derde sonde via de CPP-poortpoort naar het client-provisioningportal FQDN. Dit verzoek bevat informatie over de portal-sessie-id die ISE in staat stelt om te bepalen welke bronnen moeten worden geleverd.

Stap 11. NSA downloadt AnyConnect en/of specifieke modules. Het downloadproces verloopt via de portaalpoort voor clientprovisioning.



Figuur 2-3

Stap 12. In ISE 2.2 is het postuur opgedeeld in twee fasen. De eerste fase bevat een set van traditionele poortdetectiesondes om achterwaartse compatibiliteit te ondersteunen met implementaties die vertrouwen op de url-omleiding.

Stap 13. De eerste fase bevat alle traditionele postuur detectiesondes. Om meer details over de sondes te krijgen, herzie Stap 20. in de pre-ISE 2.2 houding stroom.

Stap 14. Stage twee bevat twee detectiepeilingen die de AC ISE-poortmodule in staat stellen om een verbinding te maken met het PSN waar de sessie wordt geverifieerd in omgevingen waar omleiding niet wordt ondersteund. Tijdens fase twee zijn alle sondes sequentieel.

- Probe 1 - Tijdens de eerste sonde, probeert de AC ISE postermodule te vestigen met IP/FQDNs van de "Call Home List". Een lijst van de doelstellingen voor de sonde moet in het profiel van de AC houding aan de kant van ISE worden gevormd. U kunt IP's/FQDN's definiëren, gescheiden door komma's, met een dubbele punt kunt u het poortnummer definiëren voor elke Call Home-bestemming. Deze poort moet gelijk zijn aan de poort waarop het client provisioningportal wordt uitgevoerd. Aan de clientzijde vindt u informatie over call home servers in ISEPostureCFG.xml, kan dit bestand worden gevonden in de map -

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture\.

Als het doel van de call home de sessie niet bezit, is in deze fase een raadpleging voor de eigenaar nodig. AC ISE Posture module geeft ISE de opdracht om het zoeken van de eigenaar te starten met behulp van een speciale doel-URL - /auth/ng-discovery verzoek. Het



bevat ook de client-IP's en MAC's lijst. Nadat dit bericht door de PSN-sessie is ontvangen, wordt eerst lokaal opgezocht (bij deze raadpleging worden zowel IP's als MAC's gebruikt van het verzoek dat door de AC ISE-poortmodule is verstuurd). Als de sessie niet wordt gevonden, start PSN een MNT node query. Dit verzoek bevat alleen de MACs-lijst, waardoor de FQDN van de eigenaar moet worden verkregen van de MNT. Daarna geeft PSN de eigenaren FQDN terug aan de klant. Het volgende verzoek van de client wordt verzonden naar sessieeigenaar FQDN met auth/status in URL en lijst van IP's en MAC's.

- Sonde 2 - In dit stadium, probeert de module van de Posthouding van AC ISE PSN FQDNs die in worden gevestigd `ConnectionData.xml`. U kunt dit bestand vinden in `c:\Users\ . AC ISE Posture module` maakt dit bestand na de eerste postuur poging. Het bestand bevat een lijst met ISE-PSN-FQDN's. De inhoud van de lijst kan dynamisch worden bijgewerkt tijdens de volgende verbindingsoogingen. Het einddoel van deze sonde is om de FQDN van de huidige sessieeigenaar te krijgen. Implementatie is identiek aan Sonde 1. met het enige verschil in de selectie van de sondbestemming. Het bestand zelf bevindt zich in de map van de huidige gebruiker als het apparaat door meerdere gebruikers wordt gebruikt. Een andere gebruiker kan geen informatie uit dit bestand gebruiken. Dit kan leiden gebruikers naar het kip en ei probleem in omgevingen zonder omleiding wanneer Call home doelen niet worden gespecificeerd.

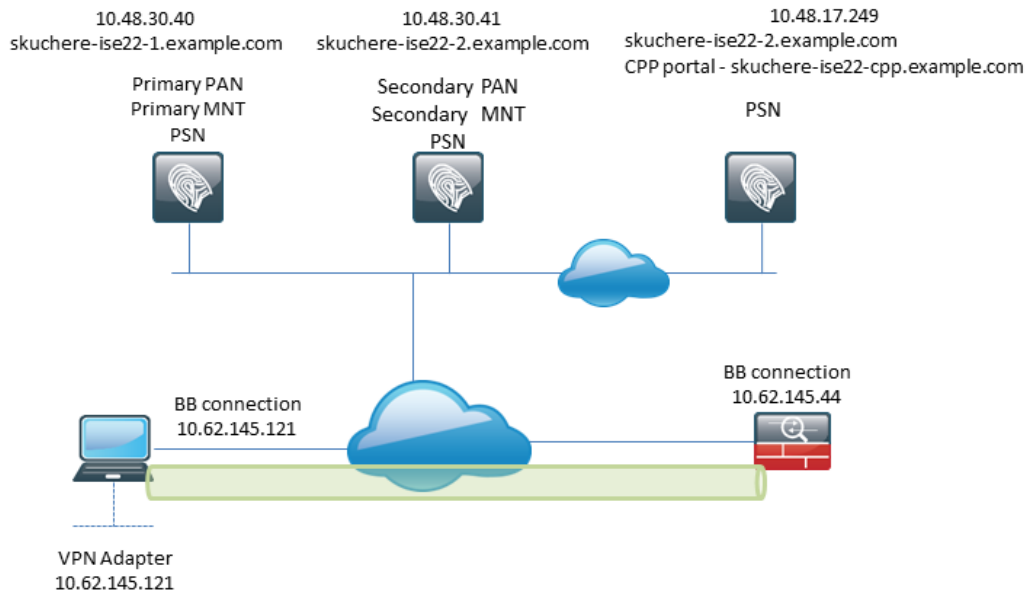
Stap 15. Nadat informatie over de sessieeigenaar is verkregen, zijn alle volgende stappen identiek aan de pre-ISE 2.2-stroom.

## Configureren

Voor dit document wordt ASA v gebruikt als netwerktoegangsapparaat. Alle testen worden uitgevoerd met postuur via VPN. ASA-configuratie voor postuur via VPN-ondersteuning valt buiten het bereik van het document. Raadpleeg voor meer informatie [ASA versie 9.2.1 VPN-houding met ISE-configuratievoorbeeld](#).

**Opmerking:** voor implementaties met VPN-gebruikers is de aanbevolen instelling een op omleiding gebaseerde houding. Configuratie van `callhomelist` wordt niet aanbevolen. Zorg er voor dat DACL wordt toegepast voor alle niet op VPN gebaseerde gebruikers, zodat ze niet praten met PSN waar postuur is ingesteld.

## Netwerkdigram



Figuur 3-1

Deze topologie wordt gebruikt in tests. Met ASA is het mogelijk om het scenario eenvoudig te simuleren wanneer het SSO-mechanisme voor het Client Provisioning portal faalt aan de PSN-kant, vanwege de NAT-functie. In het geval van een normale posteringsstroom via VPN moet een netwerkmodule fijn werken omdat NAT normaal gesproken niet wordt afgedwongen voor VPN-IP's wanneer gebruikers het bedrijfsnetwerk binnenkomen.

## Configuraties

### Configuratie van clientprovisioning

Dit zijn de stappen om de AnyConnect-configuratie voor te bereiden.

Stap 1. Anyconnect pakket downloaden. AnyConnect pakket zelf is niet beschikbaar voor directe download van ISE dus voordat u begint, zorg ervoor dat AC beschikbaar is op uw PC. Deze link kan worden gebruikt voor AC download -

<https://www.cisco.com/site/us/en/products/security/secure-client/index.html>. In dit document anyconnect-win-4.4.00243-webdeploy-k9.pkg de verpakking wordt gebruikt.

Stap 2. Ga naar om het AC-pakket naar ISE te uploaden Policy > Policy Elements > Results > Client Provisioning > Resources en klik op Add. Kies Agent-resources op de lokale schijf. Kies in het nieuwe venster Cisco Provided Packages klikt u op browse en kies het AC-pakket op uw PC.

### Agent Resources From Local Disk

Category  ⓘ

anyconnect-win-4.4.00243-webdeploy-k9.pkg

▼ **AnyConnect Uploaded Resources**

Name	Type	Version	Description
AnyConnectDesktopWindows 4.4.24...	AnyConnectDesktopWindows	4.4.243.0	AnyConnect Secure Mobility Clie...

Figuur 3-2

Klik **Submit** om de import te voltooien.

Stap 3. De conformiteitsmodule moet naar ISE worden geüpload. Klik op dezelfde pagina **Add** en kies de **Agent resources from Cisco site**. In de resourcelijst moet u een nalevingsmodule controleren. Voor dit document wordt **AnyConnectComplianceModuleWindows 4.2.508.0** conformiteitsmodule wordt gebruikt.

Stap 4. Nu moet het profiel AC worden gemaakt. Klik **Add** en kies de **NAC agent or Anyconnect posture profile**.

### ISE Posture Agent Profile Settings > **New Profile**

**Posture Agent Profile Settings**

**a.**

\* Name:  **b.**

Description:

### Agent Behavior

Figuur 3-3

- Kies het type profiel. AnyConnect moet voor dit scenario worden gebruikt.
- Specificeer de profielnaam. Naar het **Posture Protocol** deel van het profiel.

## Posture Protocol

Parameter	Value	Notes
PRA retransmission time	<input type="text" value="120"/> secs	
Discovery host	<input type="text"/>	
* Server name rules	<input type="text" value="*"/> <b>a.</b>	need to be blank by default to force admin to enter a value. "*" means agent will connect to all
Call Home List	<input type="text" value="skuchere-ise22-2.examp"/> <b>b.</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	<input type="text" value="30"/> secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.

Figuur 3-4

- Specificeer de `Server Name Rules` Dit veld mag niet leeg zijn. Het veld kan FQDN bevatten met jokertekens die de poortmodule van AC ISE beperkt tot PSN's vanuit de juiste naamruimte. Plaats een ster als een FQDN moet worden toegestaan.
- De hier gespecificeerde namen en IPs zijn in gebruik tijdens fase 2 van de postureontdekking. U kunt namen door coma scheiden evenals poortnummers kunnen worden toegevoegd na FQDN/IP met het gebruik van de dubbele punt. In het geval dat de AC out-of-band (niet van het ISE-client provisioningportal) met het gebruik van de GPO of een andere software provisioning systeem aanwezigheid van Call Home-adressen essentieel worden omdat dit slechts één sonde is die met succes ISE PSN kan bereiken. Dit betekent dat in het geval van out-of-band AC-provisioning, de beheerder een AC ISE-poortprofiel moet maken met het gebruik van de AC-profiel editor en dit bestand moet provisioneren samen met AC-installatie.

**Opmerking:** Houd in gedachten dat de aanwezigheid van Call home-adressen van cruciaal belang is voor PC's met meerdere gebruikers. Beoordeel stap 14. in Posture flow post-ISE 2.2.

Stap 5. Maak AC-configuratie. Naar navigeren `Policy > Policy Elements > Results > Client Provisioning > Resources`, klikken `Adden` kies vervolgens `AnyConnect Configuration`.

\* Select AnyConnect Package: AnyConnectDesktopWindows 4.4.243.0 **a.**

\* Configuration Name: AC-44-CCO **b.**

Description:

**DescriptionValue** **Notes**

\* Compliance Module: AnyConnectComplianceModuleWindows 4.2.508.0 **c.**

---

**AnyConnect Module Selection**

- ISE Posture
- VPN
- Network Access Manager
- Web Security
- AMP Enabler
- ASA Posture
- Network Visibility
- Umbrella Roaming Security
- Start Before Logon
- Diagnostic and Reporting Tool

---

**Profile Selection**

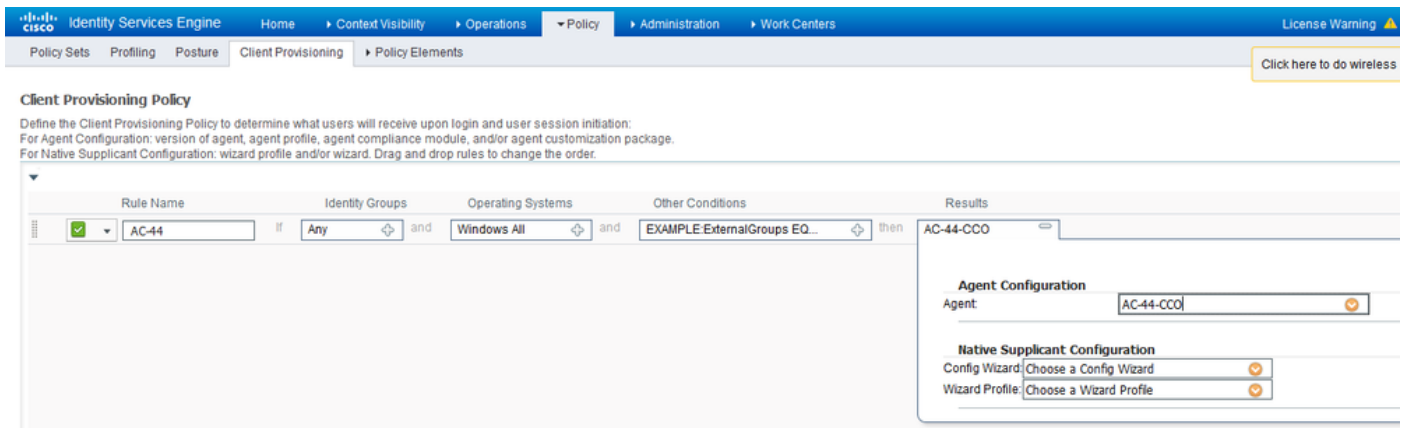
\* ISE Posture: AC-44-Posture **d.**

Figuur 3-5

- Kies het AC-pakket.
- Typ de naam van de AC-configuratie.
- Kies de compliance module versie.
- Kies het configuratieprofiel voor de AC-houding in de vervolgkeuzelijst.

Stap 6. Configureer het provisioningbeleid van clients. Naar navigeren Policy > Client Provisioning. In het geval van de initiële configuratie kunt u lege waarden invullen in het beleid dat met defaults wordt gepresenteerd. Als u een beleid moet toevoegen aan de postuur configuratie die bestaat, navigeer dan naar het beleid dat kan worden hergebruikt en kies Duplicate Above of Duplicate Below . Er kan ook een gloednieuw beleid worden gecreëerd.

Dit is een voorbeeld van het beleid dat in het document wordt gebruikt.



Figuur 3-6

Kies uw AC-configuratie in het resultaatgedeelte. Houd in gedachten, dat in geval van SSO-storing ISE alleen attributen kan hebben van login naar portal. Deze eigenschappen zijn beperkt tot informatie die over gebruikers uit interne en externe identiteitswinkels kan worden teruggehaald. In dit document wordt de AD-groep gebruikt als voorwaarde in het beleid voor clientprovisioning.

### Houdbaarheid beleid en voorwaarden

Er wordt een eenvoudige postuur gecontroleerd. ISE is ingesteld om de status van de Windows Defender-service aan de kant van het eindapparaat te controleren. Reallife scenario's kunnen veel gecompliceerder zijn, maar algemene configuratie stappen zijn hetzelfde.

Stap 1. Houdingstoestand aanmaken Posterijen bevinden zich in [Policy > Policy Elements > Conditions > Posture](#). Kies het type houding voorwaarde. Hier is een voorbeeld van een Servicevoorwaarde die moet controleren of de Windows Defender-service actief is.

#### [Service Conditions List > WinDefend](#)

### Service Condition

\* Name

Description

\* Operating Systems

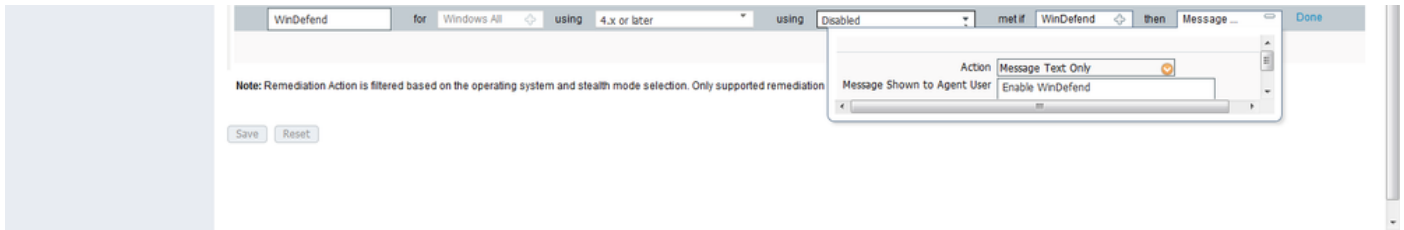
Compliance Module

\* Service Name

Service Operator

Figuur 3-7

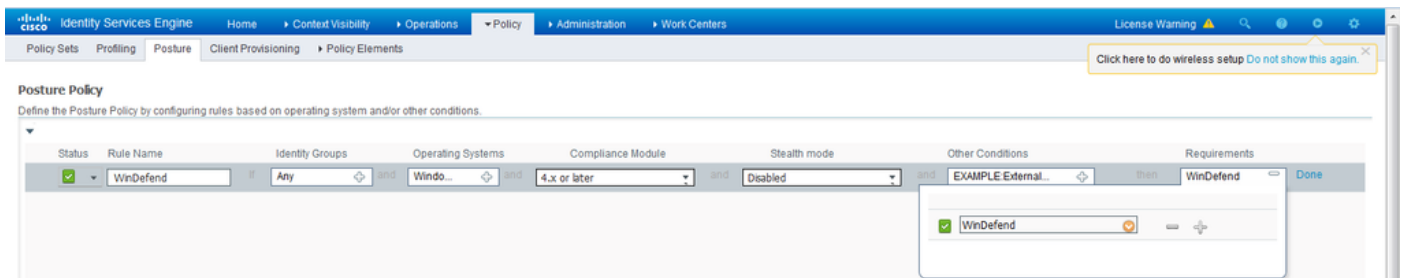
Stap 2. Configuratie van positievereisten. Naar navigeren Policy > Policy Elements > Results > Posture > Requirements. Dit is een voorbeeld van een Windows Defender-controle:



Figuur 3-8

Kies uw houding voorwaarde in de nieuwe vereiste en specificeer remediërende actie.

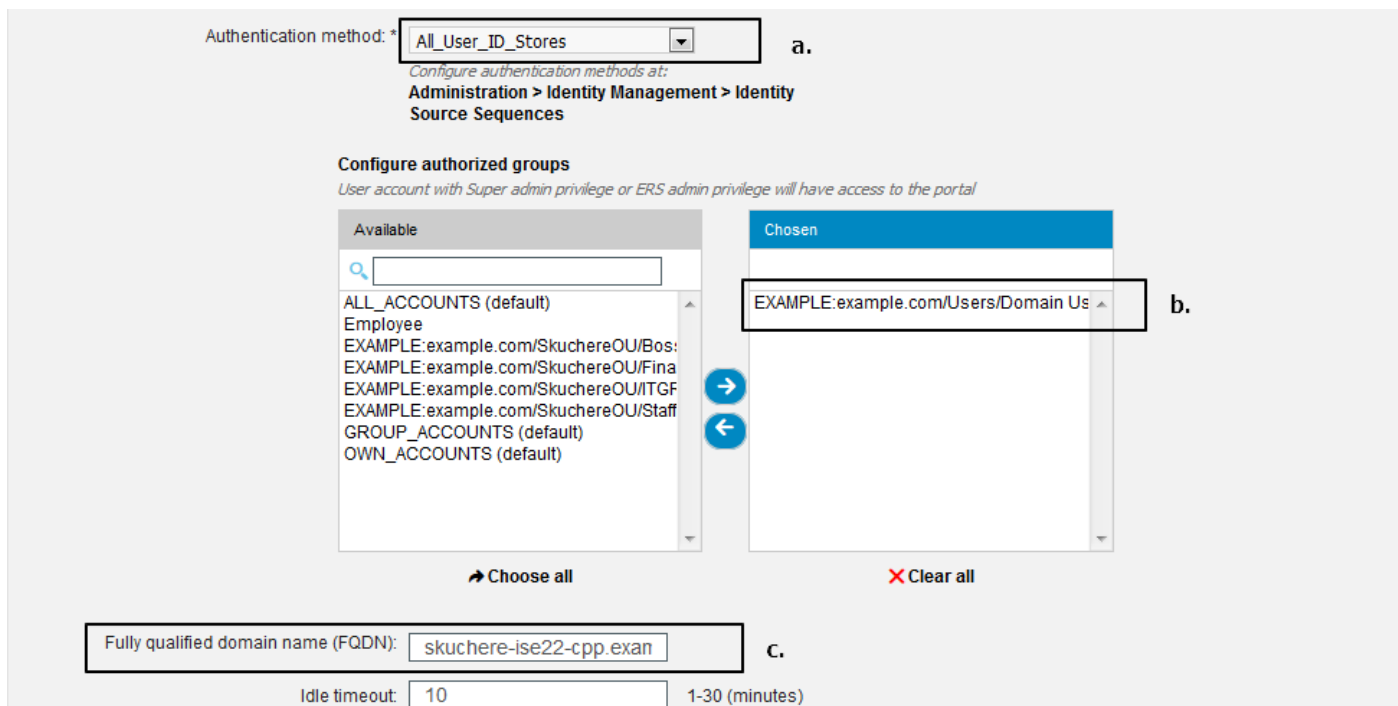
Stap 3. Posture policy configuratie. Naar navigeren Policy > Posture. Hier vindt u een voorbeeld van het beleid dat voor dit document wordt gebruikt. Het beleid heeft Windows Defender-vereiste als verplicht toegewezen en bevat alleen externe AD-groepsnaam als voorwaarde.



Figuur 3-9

## Het client-provisioningportal configureren

Voor houding zonder omleiding, moet de configuratie van het portaal van de cliëntlevering worden uitgegeven. Naar navigeren Administration > Device Portal Management > Client Provisioning. U kunt of het standaardportaal gebruiken of uw creëren. Het zelfde portaal kan voor beide houdingen met en zonder omleiding worden gebruikt.



Figuur 3-10

Deze instellingen moeten worden bewerkt in de poortconfiguratie voor het niet-omleidingsscenario:

- Specificeer in Verificatie de Identity Source Sequence die moet worden gebruikt als SSO geen sessie voor de gebruiker kan vinden.
- Zoals in de geselecteerde lijst met beschikbare groepen van Identity Source Sequence wordt ingevuld. Op dit punt moet u groepen selecteren die zijn geautoriseerd voor portal login.
- FQDN van het portaal van de cliëntlevering moet voor scenario's worden gespecificeerd wanneer AC van het portaal van de cliëntlevering moet worden opgesteld. Dit FQDN moet oplosbaar zijn in ISE-PSN-IP's. Gebruikers moeten worden geïnstrueerd om de FQDN in de webbrowser te specificeren tijdens de eerste verbindingsooging.

### Autorisatieprofielen en -beleid configureren

De initiële toegang voor cliënten wanneer de status van de houding niet beschikbaar is moet worden beperkt. Dit kan op verschillende manieren worden bereikt:

- DACL-toewijzing - Tijdens de beperkte toegangsfase kan DACL worden toegewezen aan de gebruiker om toegang te beperken. Deze benadering kan worden gebruikt voor Cisco-netwerktoegangsapparaten.
- VLAN Assignment - Voordat succesvolle postuur-gebruikers in beperkt VLAN kunnen worden gezet, moet deze aanpak werken voor bijna elke NAD-leverancier.
- Radius Filter-ID - Met dit kenmerk kan ACL die lokaal is gedefinieerd op NAD worden toegewezen aan de gebruiker met een onbekende postuur-status. Aangezien dit een standaard RFC attribuut is, moet deze benadering goed werken voor alle NAD leveranciers.

Stap 1. DACL configureren. Aangezien dit voorbeeld op ASA is gebaseerd, kan NAD DACL worden gebruikt. Voor real-life scenario's, moet u VLAN of Filter-ID als mogelijke opties overwegen.



Om DACL te maken, navigeer naar Policy > Policy Elements > Results > Authorization > Downloadable ACLs en klik op Add.

Tijdens de onbekende houding, moeten minstens deze toestemmingen worden verstrekt:

- DNS-verkeer
- DHCP-verkeer
- Verkeer naar ISE PSNs (poorten 80 en 443 voor een mogelijkheid om vriendelijke FQDN van portal te openen. De poort waarop het CP-portal draait is standaard 8443 en poort 8905 voor achterwaartse compatibiliteit)
- Verkeer naar herstelservers indien nodig

Dit is een voorbeeld van DACL zonder herstelservers:

Downloadable ACL List > New Downloadable ACL

**Downloadable ACL**

\* Name

Description

\* DACL Content

```
1 permit udp any any eq 53
2 permit udp any any eq bootps
3 permit tcp any host 10.48.30.40 eq 80
4 permit tcp any host 10.48.30.40 eq 443
5 permit tcp any host 10.48.30.40 eq 8443
6 permit tcp any host 10.48.30.40 eq 8905
7 permit tcp any host 10.48.30.41 eq 80
8 permit tcp any host 10.48.30.41 eq 443
9 permit tcp any host 10.48.30.41 eq 8443
10 permit tcp any host 10.48.30.41 eq 8905
```

ⓘ

Figuur 3-11

Stap 2. Configureer het autorisatieprofiel.

Zoals gebruikelijk voor de houding zijn twee autorisatieprofielen vereist. De eerste moet alle soorten beperkingen voor netwerktoegang bevatten (profiel met DACL in dit voorbeeld gebruikt). Dit profiel kan worden toegepast op de verificaties waarvoor de status van de postuur niet gelijk is aan de compatibiliteit. Het tweede autorisatieprofiel kan net toegang toestaan en kan worden toegepast voor sessies met een postuur status gelijk aan naleving.

Om een autorisatieprofiel te maken, navigeert u naar Policy > Policy Elements > Results > Authorization > Authorization Profiles.

Voorbeeld van het profiel van beperkte toegang:

## Authorization Profile


\* Name

Description

\* Access Type

Network Device Profile    

Service Template

Track Movement  

Passive Identity Tracking  

### ▼ Common Tasks

DACL Name  

Figuur 3-12

In dit voorbeeld wordt de standaard ISE-profiel PermitAccess gebruikt voor de sessie na een succesvolle postuur status controle.

Stap 3. Configureer het autorisatiebeleid. Tijdens deze stap moeten twee toelatingsbeleidsmaatregelen worden genomen. De eerste is om het eerste authenticatieverzoek aan te passen aan een onbekende postuur status en de tweede is om volledige toegang toe te wijzen na een succesvol postuur proces.

Dit is een voorbeeld van een eenvoudig vergunningenbeleid voor deze zaak:

▼ Authorization Policy

► Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Posture-Compliant	if (Session:PostureStatus EQUALS Compliant AND EXAMPLE:ExternalGroups EQUALS example.com/Users/Domain Users)	then PermitAccess
✓	Posture-Unknown-No-Redirect	if (Session:PostureStatus NOT_EQUALS Compliant AND EXAMPLE:ExternalGroups EQUALS example.com/Users/Domain Users)	then VPN-No-Redirect-Unknown
✓	Default	if no matches, then	DenyAccess

Figuur 3-13

De configuratie van het verificatiebeleid maakt geen deel uit van dit document, maar u moet in gedachten houden dat een succesvolle verificatie moet plaatsvinden voordat de verwerking van het autorisatiebeleid kan plaatsvinden.

## Verifiëren

De basisverificatie van de stroom kan uit drie hoofdstappen bestaan:

Stap 1. Verificatie van de verificatiestroom.

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorization Profiles	IP Address
Feb 23, 2017 06:00:07.028 PM	✓			Identity	Endpoint ID	Endpoint Prof	Authenticator	Authorization	Authorization Profiles	IP Address
Feb 23, 2017 06:00:07.028 PM	✓			e.	10.62.145.95				PermitAccess	
Feb 23, 2017 06:00:04.368 PM	✓		0	d. user1	00:0B:7F:D0:F8:F4	Windows7-...	VPN-LAB >>...	VPN-LAB >>...	VPN-No-Redirect-Unknown	172.16.31.12
Feb 23, 2017 05:59:04.750 PM	✓			c. user1						
Feb 23, 2017 05:44:57.921 PM	✓			b. #ACSACL#IP-VPN-No-Redi...						
Feb 23, 2017 05:44:57.680 PM	✓			a. user1	00:0B:7F:D0:F8:F4	Windows7-...	VPN-LAB >>...	VPN-LAB >>...	VPN-No-Redirect-Unknown	

Figuur 4-1

1. Eerste verificatie. Voor deze stap kunt u geïnteresseerd zijn in de validatie waarvan het autorisatieprofiel is toegepast. Als er een onverwacht autorisatieprofiel is toegepast, onderzoekt u een gedetailleerd verificatierapport. U kunt dit rapport openen met een klik op het vergrootglas in de kolom Details. U kunt attributen in gedetailleerde verificatierapporten vergelijken met voorwaarden in het autorisatiebeleid die u verwacht te matchen.
2. DACL-downloadgebeurtenis. Deze string wordt alleen getoond in het geval dat het autorisatieprofiel dat geselecteerd is voor de initiële verificatie, een DACL-naam bevat.
3. Portal authenticatie - Deze stap in de stroom geeft aan dat het SSO-mechanisme er niet in is geslaagd om de gebruikerssessie te vinden. Dit kan om meerdere redenen gebeuren: NAD is niet ingesteld voor het verzenden van boekhoudberichten of het framed IP-adres is niet aanwezig in deze berichtenCPP-portal FQDN is opgelost in het IP van het ISE-

knooppunt dat verschilt van het knooppunt waar de eerste verificatie is verwerktDe client bevindt zich achter de NAT

4. Sessiegegevens wijzigen. In dit specifieke voorbeeld is de sessiestatus veranderd van Onbekend in Conform.
5. Koppeling aan het netwerktoegangsapparaat. Dit COA moet succesvol zijn om nieuwe authenticatie van de NAD kant en nieuwe autorisatiebeleidstoe wijzingen aan de ISE kant te duwen. Als COA heeft gefaald, kunt u een gedetailleerd rapport openen om de reden te onderzoeken. De meest voorkomende problemen met Cacao kunnen zijn: COA-time-out - In dat geval wordt ofwel het PSN dat het verzoek heeft verzonden niet geconfigureerd als een COA-client aan de NAD-kant, of het COA-verzoek is ergens onderweg ingetrokken.Cacao negatief ACK - Geeft aan dat Cacao is ontvangen door NAD, maar om een of andere reden kan de Cacao-operatie niet worden bevestigd. Voor dit scenario moet een gedetailleerd verslag een gedetailleerdere toelichting bevatten.

Aangezien ASA als NAD wordt gebruikt voor dit voorbeeld, kunt u geen verder authenticatieverzoek voor de gebruiker zien. Dit gebeurt vanwege het feit dat ISE COA push voor ASA gebruikt waardoor VPN-servicestoringen worden vermeden. In een dergelijk scenario bevat COA zelf nieuwe autorisatieparameters, zodat herverificatie niet nodig is.

Stap 2. De controle van de voorzieningsbeleidselectie van de cliënt - hiervoor, kunt u een rapport over ISE in werking stellen dat u kan helpen om te begrijpen welk beleid van de cliëntlevering voor de gebruiker werd toegepast.

Naar navigeren Operations > Reports Endpoint and Users > Client Provisioning en voer het rapport uit voor de gewenste datum.

Logged At	Server	Event	Identity	Client Provisioning Policy Matched	Failure Reason
2017-02-24 18:33:46...	skuchere-ise22-3	Client provisioning succeeded	user1	AC-44	
2017-02-23 18:46:42...	skuchere-ise22-3	Client provisioning succeeded	user1	AC-44	
2017-02-23 17:59:07...	skuchere-ise22-3	Client provisioning succeeded	user1	AC-44	

Figuur 4-2

Met dit rapport kunt u controleren welk beleid voor clientprovisioning is geselecteerd. In geval van verzuim moeten de redenen ook in de Failure Reason kolom.

Stap 3. Posture rapport verificatie - Navigeer naar Operations > Reports Endpoint and Users > Posture Assessment by Endpoint.

Logged At	Status	Details	Identity	Endpoint ID	IP Address	Endpoint OS
2017-02-24 18:34:31...	✓		user1	00:0B:7F:D0:F8:F4	10.62.145.44	Windows 7 Professional 64-
2017-02-23 19:33:35...	✓		user1	00:0B:7F:D0:F8:F4	10.62.145.44	Windows 7 Professional 64-

Figuur 4-3

U kunt vanaf hier een gedetailleerd rapport openen voor elke bepaalde gebeurtenis om te controleren, bijvoorbeeld, tot welke sessie-ID dit rapport behoort, welke exacte positievereisten werden geselecteerd door ISE voor het eindpunt en de status voor elke vereiste.

## Problemen oplossen

### Algemene informatie

Voor het oplossen van problemen in het postuur van een postuur moeten deze ISE-componenten kunnen worden ingeschakeld om te debuggen op de ISE-knooppunten waar het postuur kan plaatsvinden:

- client-webapp - Het onderdeel dat verantwoordelijk is voor provisioning van agents.  
Streeflogbestanden `guest.log` en `ise-psc.log`.
- guestaccess - Het onderdeel dat verantwoordelijk is voor het opzoeken van de onderdelen- en sessieeigenaar van de client provisioningportal (als het verzoek bij het verkeerde PSN komt).  
Logbestand doel - `guest.log`.
- provisioning - Het onderdeel dat verantwoordelijk is voor de verwerking van het beleid voor klantprovisioning. Logbestand doel - `guest.log`.
- posture - Alle posture-gerelateerde voorvallen. Logbestand doel - `ise-psc.log`.

Voor het oplossen van problemen aan de clientzijde kunt u deze gebruiken:

- `acisensa.log` - In het geval van client provisioning fout aan de kant van de client, dit bestand wordt gemaakt in dezelfde map waarnaar NSA is gedownload (downloads directory voor Windows normaal).
- `AnyConnect_ISEPosture.txt` - Dit bestand vindt u in de DART-bundel in de map `Cisco AnyConnect ISE Posture Module`. Alle informatie over ISE-PSN-detectie en algemene stappen van postuur wordt in dit bestand vastgelegd.

### Gemeenschappelijke problemen oplossen

#### Verwante problemen met betrekking tot SO

In het geval van een succesvolle SSO, kunt u deze berichten in zien `ise-psc.log`, geeft deze serie berichten aan dat het zoeken van sessies met succes is afgerond en dat verificatie op het portal kan worden overgeslagen.

```
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 addr: [10.62.145.121], mac Addr: [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
```

### Tekstvenster 5-1

U kunt het IP-adres van het eindpunt gebruiken als een zoek sleutel om deze informatie te vinden.

Een beetje later in het gastenlogboek, moet u zien dat de authenticatie is overgeslagen:

```
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
```

### Tekstvenster 5-2

Indien de aanvullende mededeling van punten van bezwaar niet werkt, ise-psc log bestand bevat informatie over zoekfout sessie:

```
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 addr: [10.62.145.44], mac Addr: [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
```

### Tekstvenster 5-3

In het `guest.log` in dat geval moet u volledige gebruikersverificatie op de portal zien:

```
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
```

#### Tekstvenster 5-4

In het geval van verificatiefouten op het portal moet u zich richten op de verificatie van de poortconfiguratie - Welk identiteitsarchief is in gebruik? Welke groepen zijn geautoriseerd voor aanmelding?

### Selectie van beleid voor clientprovisioning voor probleemoplossing

In het geval van fouten in het beleid voor clientprovisioning of onjuiste beleidsverwerking, kunt u de `guest.log` dossier voor meer details:

```
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
```

#### Tekstvenster 5-5

In de eerste string kunt u zien hoe informatie over de sessie wordt ingespoten in de policy selectie engine, in het geval er geen policy match of onjuiste policy match is, kunt u kenmerken van hier vergelijken met uw client provisioning policy configuratie. De laatste tekenreeks geeft de status van de beleidsselectie aan.

### Opdrachtproces voor probleemoplossing

Aan de kant van de klant, moet u geïnteresseerd zijn in het onderzoek van de sondes en hun resultaten. Dit is een voorbeeld van een succesvolle fase 1 sonde:

\*\*\*\*\*

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..

\*\*\*\*\*

### Tekstvenster 5-6

In deze fase keert PSN terug naar AC informatie over de sessieeigenaar. U kunt deze paar berichten later zien:

\*\*\*\*\*

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..

\*\*\*\*\*

### Tekstvenster 5-7

De eigenaars van de zitting keren aan de agent alle vereiste informatie terug:

\*\*\*\*\*

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>
```

.

\*\*\*\*\*

### Tekstvenster 5-8

Vanuit de PSN-kant kunt u zich richten op deze berichten in de `guest.log` wanneer u verwacht dat het initiële verzoek dat bij de knoop komt de zitting niet bezit:

```
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
```

### Tekstvenster 5-9

Hier kunt u zien dat PSN eerst probeert om een sessie lokaal te vinden, en na mislukking initieert een verzoek aan MNT met het gebruik van de IPs en MACs lijst om de sessieeigenaar te vinden.

Een beetje later moet u een verzoek van de klant op de juiste PSN zien:

```
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
```

### Tekstvenster 5-10

Als volgende stap voert PSN het beleid voor clientprovisioning uit voor deze sessie:

```
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
```

### Tekstvenster 5-11

In de volgende stap, kunt u het proces van de selectie van de houdingsvereisten zien. Aan het eind van de stap, wordt een lijst van vereisten voorbereid en aan de agent teruggegeven:

```
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: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: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>
```

Tekstvenster 5-12

Later kun je zien dat het verslag van de houding werd ontvangen door 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
```

Tekstvenster 5-13

Aan het eind van de stroom, merkt ISE het eindpunt als volgzzaam en initieert 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]
```

Tekstvenster 5-14

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.