ISE-Statusumleitungsfluss mit umleitungslosem ISE-Statusumleitungsfluss vergleichen

Inhalt

Einleitung

Dieses Dokument beschreibt den Vergleich des in ISE 2.2 und höheren Versionen unterstützten umleitungslosen Datenflusses mit dem seit früheren ISE-Versionen unterstützten Umleitungsfluss.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Statusüberprüfung für ISE
- Konfiguration von Statuskomponenten auf der ISE
- Adaptive Security Appliance (ASA)-Konfiguration für den Status über Virtual Private Networks (VPN)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ISE Version 2.2

- Cisco ASAv mit Software 9.6 (2)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

In diesem Dokument wird eine neue Funktion der Identity Service Engine (ISE) 2.2 beschrieben, die es der ISE ermöglicht, einen Statusfluss ohne jegliche Umleitungsunterstützung auf einem Netzwerkzugriffsgerät (Network Access Device, NAD) oder der ISE zu unterstützen.

Der Status ist eine Kernkomponente der Cisco ISE. Die Haltung als Komponente kann durch drei Hauptelemente dargestellt werden:

1. ISE als Verteilungs- und Entscheidungspunkt für Richtlinienkonfigurationen
   Aus der Sicht des Administrators konfigurieren Sie für ISE Statusrichtlinien (welche Bedingungen erfüllt sein müssen, damit ein Gerät als mit dem Unternehmen kompatibel gekennzeichnet wird), Richtlinien für die Client-Bereitstellung (welche Agentensoftware auf welchen Geräten installiert werden muss) und Autorisierungsrichtlinien (welche Berechtigungen zugewiesen werden müssen, hängt von deren Status ab).
2. Ein Netzwerkzugriffsgerät als Richtliniendurchsetzungspunkt.
   Auf der NAD-Seite werden zum Zeitpunkt der Benutzerauthentifizierung tatsächliche Autorisierungseinschränkungen angewendet. Die ISE als Richtlinienpunkt stellt Autorisierungsparameter wie Downloaded ACL (dACL)/VLAN/Redirect-URL/Redirect Access Control List (ACL) bereit. In der Regel müssen NADs die Umleitung unterstützen (um Benutzer- oder Agenten-Software anzuweisen, mit dem der ISE-Knoten verbunden werden muss) und den Autorisierungswechsel (Change of Authorization, CoA) unterstützen, um den Benutzer nach Feststellung des Status des Endpunkts erneut zu authentifizieren.
3. Agenten-Software zur Datenerfassung und Interaktion mit dem Endbenutzer.
   Die Cisco ISE verwendet drei Arten von Agent-Software: AnyConnect ISE Posture Module, NAC Agent und Web Agent. Der Agent erhält von der ISE Informationen zu Statusanforderungen und übermittelt der ISE einen Bericht über den Status der Anforderungen.

Hinweis: Dieses Dokument basiert auf dem AnyConnect ISE Posture Module. Dieses Modul ist das einzige Modul, das den Status vollständig und ohne Umleitung unterstützt.

Vor der ISE 2.2 werden NADs nicht nur zur Authentifizierung von Benutzern und zur Zugriffsbeschränkung verwendet, sondern auch, um Agentensoftware Informationen über einen bestimmten ISE-Knoten bereitzustellen, die kontaktiert werden müssen. Im Rahmen des Umleitungsprozesses werden die Informationen über den ISE-Knoten an die Agent-Software zurückgegeben.

In der Vergangenheit war die Unterstützung der Umleitung entweder auf NAD- oder auf ISE-Seite eine wesentliche Anforderung für die Implementierung des Status. In ISE 2.2 entfällt die Notwendigkeit der Unterstützung der Umleitung sowohl für die anfängliche Client-Bereitstellung als auch für den Statusprozess.

Client-Bereitstellung ohne Umleitung: In ISE 2.2 können Sie direkt über das Portal FQDN (Fully Qualified Domain Name) auf das Client-Bereitstellungsportal (CPP) zugreifen. Dies ähnelt dem Zugriff auf das Sponsorportal oder das MyDevice Portal.

Statusprozess ohne Umleitung - Bei der Agenteninstallation aus dem CPP-Portal werden auf der Clientseite Informationen zu ISE-Servern gespeichert, die eine direkte Kommunikation ermöglichen.

Statusüberprüfung vor ISE 2.2

Dieses Bild zeigt eine schrittweise Erklärung des AnyConnect ISE Posture Module-Flows vor ISE 2.2:

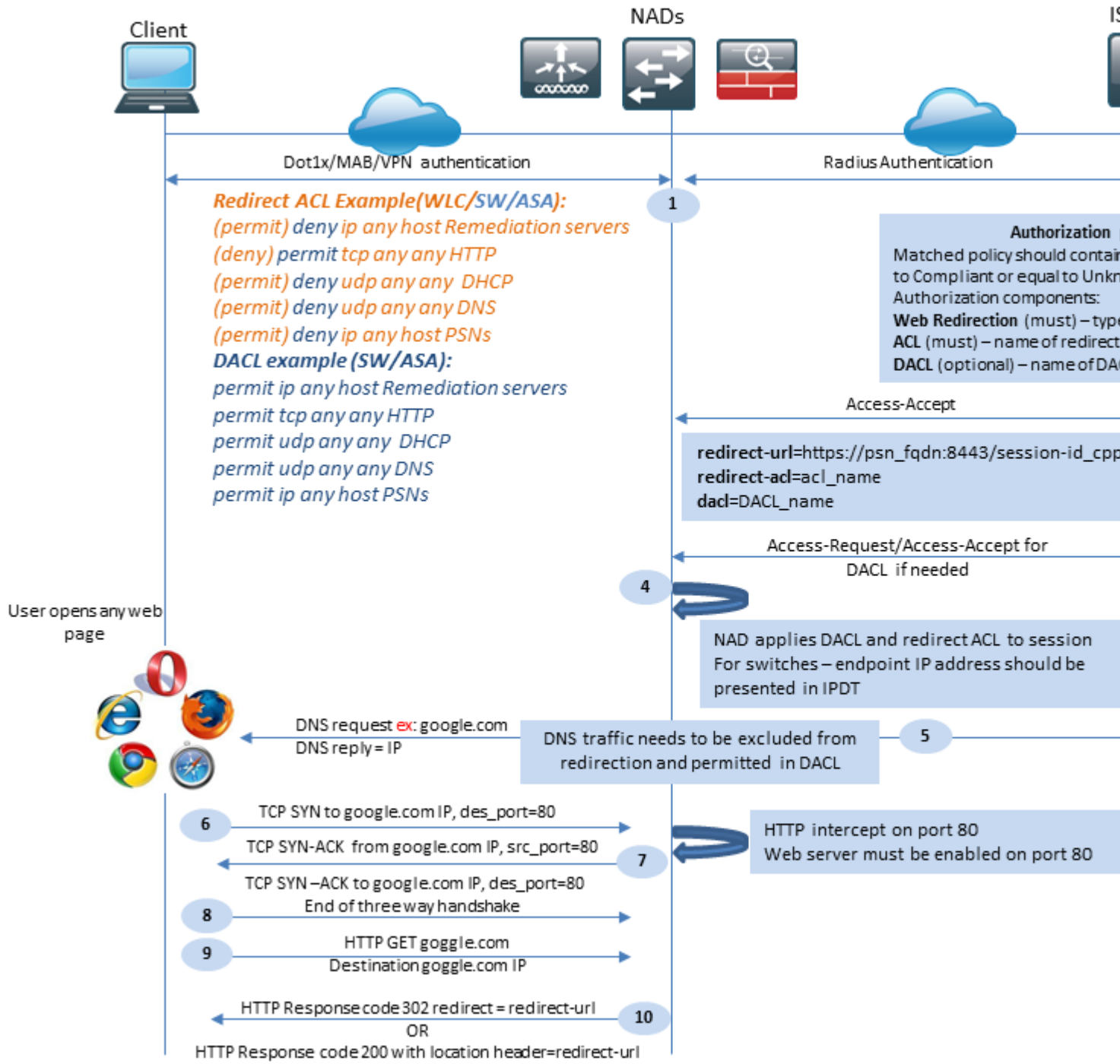

Abbildung 1-1

Schritt 1: Die Authentifizierung ist der erste Schritt des Datenflusses. Sie kann dot1x, MAB oder VPN sein.

Schritt 2: Die ISE muss eine Authentifizierungs- und Autorisierungsrichtlinie für den Benutzer auswählen. Im Statusszenario muss die gewählte Autorisierungsrichtlinie einen Verweis auf den Status enthalten, der zunächst entweder unbekannt oder nicht zutreffend sein muss. Um diese beiden Fälle abzudecken, können Bedingungen mit Statusstatus und ungleicher Konformität verwendet werden.

Das ausgewählte Autorisierungsprofil muss Informationen zur Umleitung enthalten:

- Web-Umleitung - Für den Status muss der Web-Umleitungstyp als Client-Bereitstellung (Status) angegeben werden.
- ACL: Dieser Abschnitt muss den ACL-Namen enthalten, der auf der NAD-Seite konfiguriert wurde. Mit dieser ACL wird der NAD mitgeteilt, welcher Datenverkehr die Umleitung umgehen und welcher tatsächlich umgeleitet werden muss.
- DACL- Sie kann zusammen mit einer Umleitungszugriffsliste verwendet werden, Sie müssen jedoch berücksichtigen, dass verschiedene Plattformen DACLs und Umleitungszugriffskontrolllisten in einer anderen Reihenfolge verarbeiten.

Beispielsweise verarbeitet ASA immer DACL, bevor sie ACL umleitet. Einige Switch-Plattformen verarbeiten die ACL auf die gleiche Weise wie die ASA. Andere Switch-Plattformen verarbeiten zuerst die Umleitungszugriffskontrollliste und überprüfen dann die DACL/Schnittstellen-ACL, ob der Datenverkehr verworfen oder zugelassen werden muss.

Hinweis: Nachdem Sie die Web-Umleitungsoption im Autorisierungsprofil aktiviert haben, muss das Zielportal für die Umleitung ausgewählt werden.

Schritt 3: ISE gibt Access-Accept mit Autorisierungsattributen zurück. Die Umleitungs-URL in den Autorisierungsattributen wird automatisch von der ISE generiert. Es enthält folgende Komponenten:

- FQDN des ISE-Knotens, für den die Authentifizierung erfolgt ist. In einigen Fällen kann dynamischer FQDN durch die Konfiguration des Autorisierungsprofils (statische IP/Hostname/FQDN) im Abschnitt "Web Redirection" (Webumleitung) überschrieben werden. Wenn der statische Wert verwendet wird, muss er auf denselben ISE-Knoten verweisen, in dem die Authentifizierung verarbeitet wurde. Im Fall des Load Balancers (LB) kann dieser FQDN auf LB VIP verweisen, jedoch nur, wenn LB so konfiguriert ist, dass es Radius- und SSL-Verbindungen miteinander verbindet.
- Port: Der Port-Wert wird aus der Konfiguration des Zielportals abgerufen.
- Session ID: Dieser Wert wird von der ISE aus der Audit-Session-ID des Cisco AV-Paars entnommen, die in Access-Request angegeben ist. Der Wert selbst wird von NAD dynamisch generiert.
- Portal-ID - Kennung eines Zielportals auf der ISE-Seite.

Schritt 4: NAD wendet eine Autorisierungsrichtlinie auf die Sitzung an. Wenn DACL konfiguriert ist, wird der Inhalt außerdem angefordert, bevor Autorisierungsrichtlinien angewendet werden.

Wichtige Überlegungen:

- Alle NADs- Geräte müssen über lokal konfigurierte ACLs mit demselben Namen verfügen, der unter Access-Accept (Access-Accept) als redirect-acl (Umleitungszugriffskontrollliste) empfangen wurde.
- Switches - Die IP-Adresse des Clients muss in der Ausgabe von `show authentication session interface details` , um die Umleitung und ACLs erfolgreich anzuwenden. Die Client-IP-Adresse wird von der IP-Geräteverfolgungsfunktion (IP Device Tracking Feature, IPDT) abgerufen.

Schritt 5: Der Client sendet eine DNS-Anfrage für den FQDN, die in den Webbrowser eingegeben wird. In dieser Phase muss der DNS-Datenverkehr die Umleitung umgehen, und der DNS-Server muss die richtige IP-Adresse zurückgeben.

Schritt 6: Der Client sendet TCP SYN an die IP-Adresse, die in der DNS-Antwort empfangen wird. Die Quell-IP-Adresse des Pakets ist die Client-IP-Adresse, und die Ziel-IP-Adresse ist die IP-Adresse der angeforderten Ressource. Der Zielport ist gleich 80, außer in Fällen, in denen ein direkter HTTP-Proxy im Client-Webbrowser konfiguriert ist.

Schritt 7: NAD fängt Client-Anfragen ab und bereitet SYN-ACK-Pakete mit einer Quell-IP vor, die der angeforderten Ressourcen-IP entspricht, einer Ziel-IP, die der Client-IP entspricht, und einem Quell-Port, der 80 entspricht.

Wichtige Überlegungen:

- NADs müssen über einen HTTP-Server verfügen, der auf dem Port ausgeführt wird, an den der Client Anfragen sendet. Standardmäßig ist dies Port 80.
- Wenn der Client einen direkten HTTP-Proxy-Webserver verwendet, muss der HTTP-Server auf dem Proxy-Port des NAS ausgeführt werden. Dieses Szenario wird in diesem Dokument nicht behandelt.
- Wenn NAD keine lokale IP-Adresse im Client hat, wird das Subnetz SYN-ACK mit der NAD-Routing-Tabelle gesendet (in der Regel über die Management-Schnittstelle). In diesem Szenario wird das Paket über die L3-Infrastruktur geroutet und muss von einem L3-Upstream-Gerät zurück zum Client geroutet werden. Wenn es sich bei dem L3-Gerät um eine Stateful-Firewall handelt, muss eine zusätzliche Ausnahme für solch asymmetrisches Routing angegeben werden.

Schritt 8: Der Client beendet den TCP-Drei-Wege-Handshake durch ACK.

Schritt 9. HTTP GET für die Zielressource wird von einem Client gesendet.

Schritt 10. NAD gibt eine Umleitungs-URL zum Client mit HTTP-Code 302 (Seite verschoben) zurück. Bei einigen NADs kann die Umleitung innerhalb der HTTP 200 OK-Nachricht im Location-Header zurückgegeben werden.

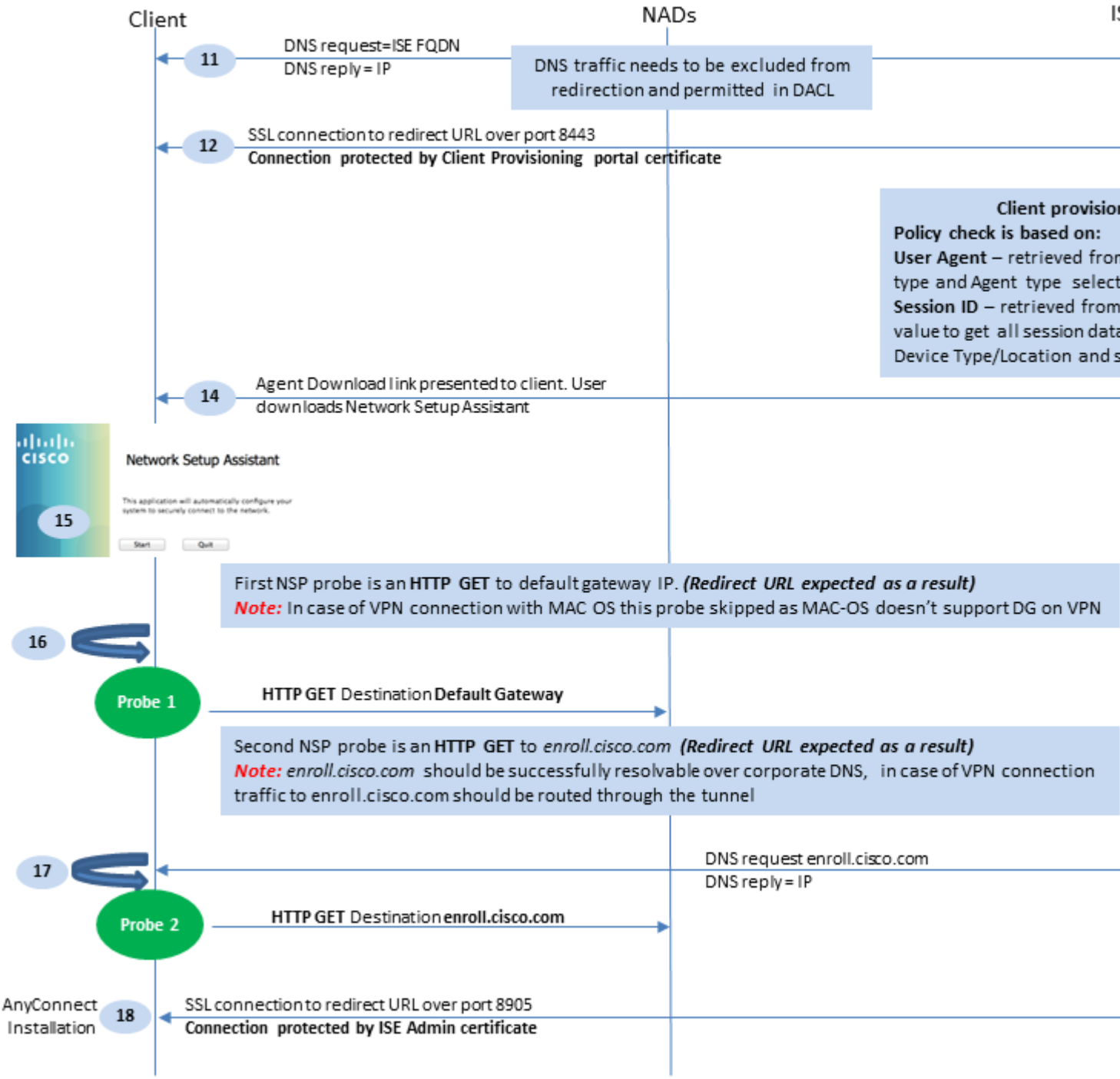

Abbildung 1-2

Schritt 11. Der Client sendet eine DNS-Anforderung für den FQDN von der Umleitungs-URL. FQDN muss auf der Seite des DNS-Servers auflösbar sein.

Schritt 12: Die SSL-Verbindung über den in der Umleitungs-URL empfangenen Port wurde hergestellt (Standard 8443). Diese Verbindung wird durch ein Portalzertifikat von der ISE-Seite geschützt. Dem Benutzer wird das Client Provisioning Portal (CPP) angezeigt.

Schritt 13:Bevor Sie dem Client eine Download-Option zur Verfügung stellen, muss die ISE die Ziel-Client-Bereitstellungsrichtlinie auswählen. Das vom Browser-Benutzer-Agenten erkannte Betriebssystem (OS) des Clients und andere Informationen, die für die CPP-Richtlinienauswahl erforderlich sind, werden aus der Authentifizierungssitzung abgerufen (wie AD/LDAP-Gruppen usw.). Die ISE kennt die Zielsitzung aus der Sitzungs-ID, die in der Umleitungs-URL angegeben ist.

Schritt 14: Der Download-Link des Network Setup Assistant (NSA) wird an den Client zurückgegeben. Der Client lädt die Anwendung herunter.

> **Hinweis**: Normalerweise können Sie NSA als Teil des BYOD-Flusses für Windows und Android sehen, aber auch diese Anwendung kann verwendet werden, um AnyConnect oder seine Komponenten von der ISE zu installieren.

Schritt 15:Der Benutzer führt die NSA-Anwendung aus.

Schritt 16: NSA sendet die erste Erkennungssonde - HTTP/auth/discovery - an das Standard-Gateway. Die NSA erwartet daher eine Weiterleitungs-URL.

> **Hinweis**: Bei Verbindungen über VPN auf MAC OS-Geräten wird dieser Test ignoriert, da das MAC OS keinen Standard-Gateway auf dem VPN-Adapter hat.

Schritt 17: NSA sendet eine zweite Anfrage, wenn die erste fehlschlägt. Der zweite Prüfpunkt ist HTTP GET /auth/discovery, um `enroll.cisco.com`. Dieser FQDN muss vom DNS-Server erfolgreich aufgelöst werden können. In einem VPN-Szenario mit einem Split-Tunnel `enroll.cisco.com` muss durch den Tunnel geleitet werden.

Schritt 18: Wenn einer der Tests erfolgreich ist, stellt die NSA eine SSL-Verbindung über Port 8905 mit den Informationen her, die von redirect-url abgerufen werden. Diese Verbindung wird durch das ISE-Administratorzertifikat geschützt. Innerhalb dieser Verbindung lädt die NSA AnyConnect herunter.

Wichtige Überlegungen:

- Vor der ISE Version 2.2 ist die SSL-Kommunikation über Port 8905 eine Voraussetzung für den Status.
- Um Zertifikatwarnungen zu vermeiden, müssen Portal- und Admin-Zertifikate auf der Clientseite als vertrauenswürdig eingestuft werden.
- Bei ISE-Bereitstellungen mit mehreren Schnittstellen können andere Schnittstellen als G0 anders an den FQDN gebunden werden als der System-FQDN (bei Verwendung von `ip host` CLI-Befehl) Dies kann zu Problemen bei der Validierung von Subject Name (SN)/Subject Alternative Name (SAN) führen. Wird der Client beispielsweise von der Schnittstelle G1 auf FQDN umgeleitet, kann sich der System-FQDN vom FQDN in der Umleitungs-URL für das Kommunikationszertifikat 8905 unterscheiden. Als Lösung für dieses Szenario können Sie FQDNs zusätzlicher Schnittstellen in den SAN-Feldern des Admin-Zertifikats hinzufügen oder einen Platzhalter im Admin-Zertifikat verwenden.

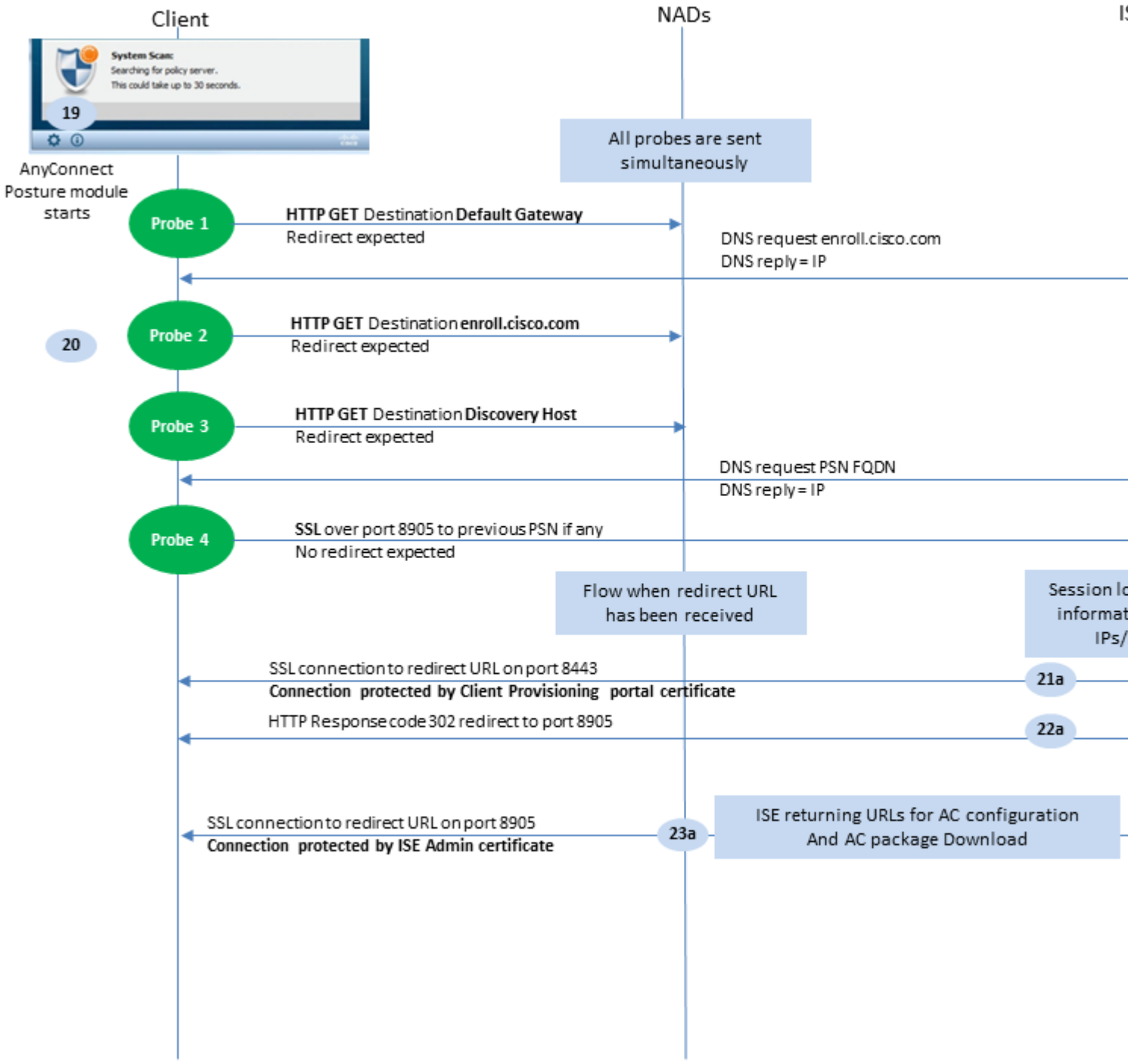

Abbildung 1-3

Schritt 19.Der Statusprozess für AnyConnect ISE wird gestartet.

AnyConnect ISE Posture-Modul beginnt in einer der folgenden Situationen:

- Nach der Installation
- Nach Änderung des Standardgatewaywerts
- Nach dem Anmeldeereignis des Systembenutzers
- Nach dem Systemeinschaltungsereignis

Schritt 20: Zu diesem Zeitpunkt initiiert das AnyConnect ISE-Statusmodul die Richtlinienserver-Erkennung. Dies wird durch eine Reihe von Tests erreicht, die gleichzeitig vom AnyConnect ISE Posture-Modul gesendet werden.

- Probe 1: HTTP get /auth/discovery to default gateway IP. Beachten Sie, dass MAC OS-Geräte keinen Standard-Gateway auf dem VPN-Adapter haben. Das erwartete Ergebnis für die Anfrage ist redirect-url.
- Sonde 2 - HTTP GET /auth/discovery zu enroll.cisco.com. Dieser FQDN muss vom DNS-Server erfolgreich aufgelöst werden können. In einem VPN-Szenario mit einem Split-Tunnel enroll.cisco.com muss durch den Tunnel geleitet werden. Das erwartete Ergebnis für die Anfrage ist redirect-url.
- Probe 3: HTTP get /auth/discovery to discovery host. Der Discovery-Hostwert wird von der ISE während der Installation im AC-Statusprofil zurückgegeben. Das erwartete Ergebnis für die Anfrage ist redirect-url.
- Probe 4: HTTP GET /auth/status over SSL on port 8905 to previous connected PSN. Diese Anfrage enthält Informationen zu Client-IPs und zur MAC-Liste für die ISE-seitige Sitzungssuche. Dieses Problem tritt beim ersten Haltungsversuch nicht auf. Die Verbindung wird durch ein ISE-Administratorzertifikat geschützt. Als Ergebnis dieser Überprüfung kann ISE die Sitzungs-ID an den Client zurückgeben, wenn der Knoten, auf dem die Überprüfung gelandet ist, derselbe Knoten ist, auf dem der Benutzer authentifiziert wurde.

Hinweis: Aufgrund dieser Überprüfung kann die Haltung unter bestimmten Umständen auch ohne funktionierende Umleitung erfolgreich durchgeführt werden. Für einen erfolgreichen Status ohne Umleitung muss das aktuelle PSN, das die Sitzung authentifiziert hat, mit dem zuvor erfolgreich verbundenen PSN identisch sein. Beachten Sie, dass vor ISE 2.2 erfolgreiche Statusüberprüfungen ohne Umleitung eher eine Ausnahme als eine Regel sind.

Die nächsten Schritte beschreiben den Status-Prozess für den Fall, dass die Umleitungs-URL als Ergebnis einer der Sonden empfangen wird (Fluss mit Buchstabe a markiert).

Schritt 21: Das AnyConnect ISE Posture-Modul stellt unter Verwendung einer während der Erkennungsphase abgerufenen URL eine Verbindung zum Client-Bereitstellungsportal her. In dieser Phase validiert die ISE die Richtlinien für die Clientbereitstellung erneut unter Verwendung der Informationen aus den authentifizierten Sitzungen.

Schritt 22:Wenn eine Client-Bereitstellungsrichtlinie erkannt wird, gibt die ISE die Umleitung an Port 8905 zurück.

Schritt 23: Der Agent stellt eine Verbindung zur ISE über Port 8905 her. Während dieser Verbindung gibt die ISE URLs für Statusprofile, Compliance-Module und AnyConnect-Updates zurück.

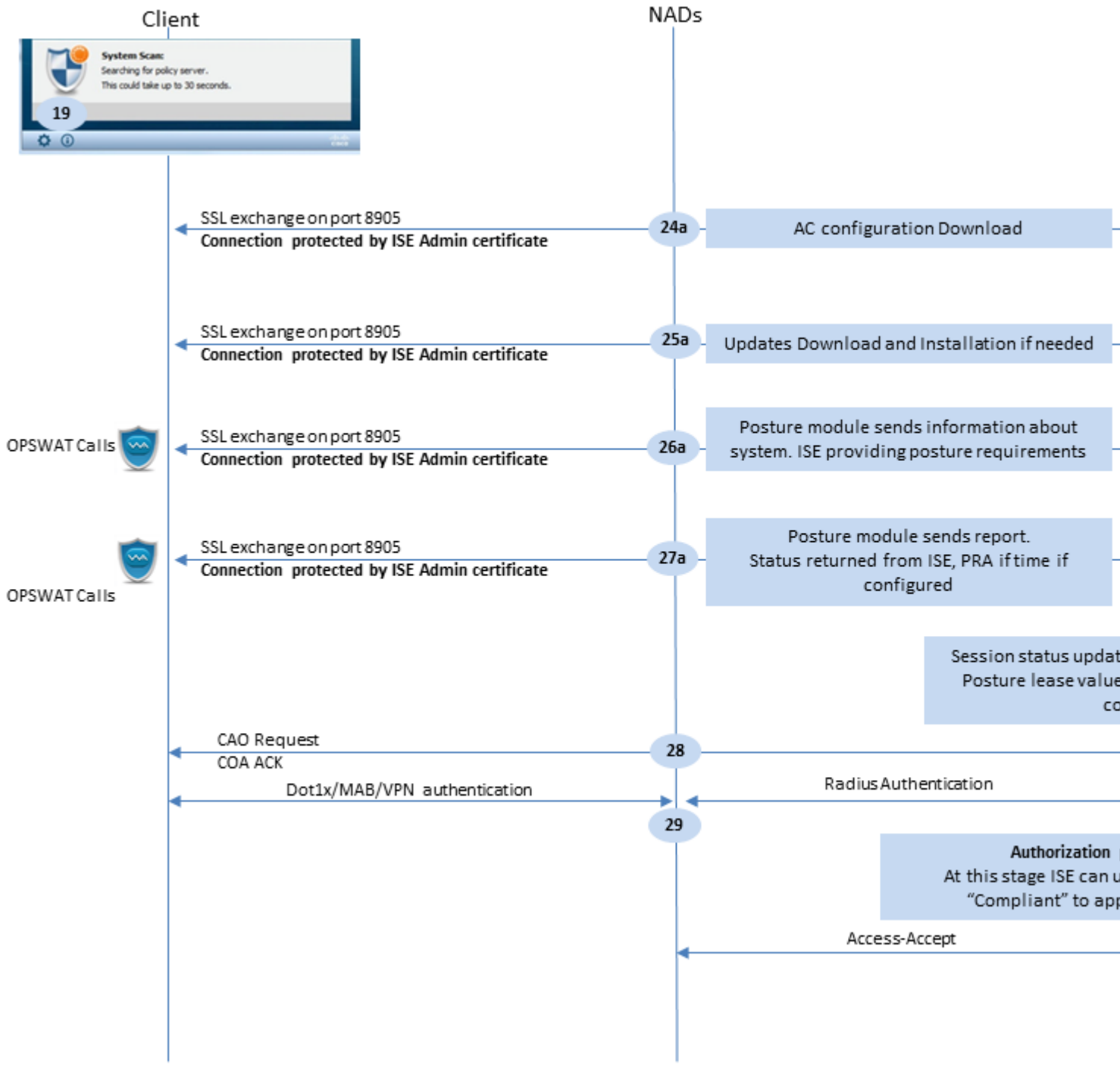

Abbildung 1-4

Schritt 24.AC ISE Posture-Modulkonfiguration von ISE herunterladen.

Schritt 25.Updates herunterladen und Installation, wenn erforderlich.

Schritt 26: Das AC ISE Posture-Modul sammelt erste Informationen über das System (wie Betriebssystemversion, installierte Sicherheitsprodukte und deren Definitionsversion). Zu diesem Zeitpunkt umfasst das AC ISE-Statusmodul eine OPSWAT-API, um Informationen über Sicherheitsprodukte zu sammeln. Die erfassten Daten werden an die ISE gesendet. Als Antwort auf diese Anfrage stellt die ISE eine Liste mit Statusanforderungen bereit. Die Anforderungsliste wird als Ergebnis der Verarbeitung von Statusrichtlinien ausgewählt. Um die richtige Richtlinie abzugleichen, verwendet die ISE die Betriebssystemversion des Geräts (in der Anforderung vorhanden) und die Sitzungs-ID, um andere erforderliche Attribute (AD/LDAP-Gruppen) auszuwählen. Der Sitzungs-ID-Wert wird ebenfalls vom

Client gesendet.

Schritt 27: In diesem Schritt umfasst der Client OPSWAT-Aufrufe und andere Mechanismen, um Statusanforderungen zu überprüfen. Der Abschlussbericht mit der Anforderungsliste und deren Status wird an die ISE gesendet. Die ISE muss die endgültige Entscheidung über den Endpunkt-Compliance-Status treffen. Wenn das Endgerät in diesem Schritt als nicht konform markiert wird, werden eine Reihe von Korrekturmaßnahmen zurückgegeben. Für den kompatiblen Endpunkt schreibt die ISE den Compliance-Status in die Sitzung und überträgt den letzten Status-Timestamp an die Endpunkteigenschaften, wenn der Status-Lease konfiguriert ist. Das Statusergebnis wird an den Endpunkt zurückgesendet. Bei der Statusüberprüfung (PRA) wird die Zeit für PRA von der ISE ebenfalls in dieses Paket eingefügt.

Bei einem nicht konformen Szenario berücksichtigen Sie folgende Punkte:

- Einige Wiederherstellungsaktionen (wie die Anzeige von Textnachrichten, die Wiederherstellung von Links, die Wiederherstellung von Dateien usw.) werden vom Status-Agenten selbst ausgeführt.
- Andere Sanierungsarten (wie AV. AS, WSUS und SCCM) erfordern eine OPSWAT-API-Kommunikation zwischen dem Status-Agent und dem Zielprodukt. In diesem Szenario sendet der Statusagent lediglich eine Wiederherstellungsanforderung an das Produkt. Die eigentliche Behebung erfolgt durch die Security-Produkte direkt.

Hinweis: Wenn ein Sicherheitsprodukt mit externen Ressourcen (interne/externe Update-Server) kommunizieren muss, müssen Sie sicherstellen, dass diese Kommunikation in der Redirect-ACL/DACL zulässig ist.

Schritt 28: ISE sendet eine COA-Anforderung an den NAD, die eine neue Authentifizierung für den Benutzer auslösen muss. NAD muss diese Anfrage von COA ACK bestätigen. Beachten Sie, dass für die VPN-Fälle COA-Push verwendet wird, sodass keine neue Authentifizierungsanfrage gesendet wird. Stattdessen entfernt ASA frühere Autorisierungsparameter (Umleitungs-URL, Umleitungs-ACL und DACL) aus der Sitzung und wendet neue Parameter aus der COA-Anforderung an.

Schritt 29.Neue Authentifizierungsanforderung für den Benutzer.

Wichtige Überlegungen:

- In der Regel wird bei Cisco NAD COA Bürokratie von der ISE verwendet. Dadurch wird NAD angewiesen, eine neue Authentifizierungsanforderung mit der vorherigen Sitzungs-ID zu initiieren.
- Auf Seiten der ISE ist derselbe Session-ID-Wert ein Hinweis darauf, dass zuvor erfasste Session-Attribute wiederverwendet werden müssen (Reklamationsstatus in unserem Fall) und ein neues, auf diesen Attributen basierendes Autorisierungsprofil zugewiesen werden muss.
- Bei einer Änderung der Sitzungs-ID wird diese Verbindung als neu behandelt, und der gesamte Statusprozess wird neu gestartet.
- Um eine Rückstellung zu vermeiden Bei jeder Änderung der Sitzungs-ID kann ein Status-Lease verwendet werden. In diesem Szenario werden Informationen über den Status in den Endpunkteigenschaften gespeichert, die auch dann auf der ISE verbleiben, wenn die Sitzungs-ID geEs hat sich geändert.

Schritt 30: ISE-seitig wird eine neue Autorisierungsrichtlinie ausgewählt, die auf dem Status basiert.

Schritt 31: Access-Accept mit neuen Autorisierungsattributen wird an den NAD gesendet.

Der nächste Datenstrom beschreibt das Szenario, in dem die Umleitungs-URL nicht von einem Statusprüfkopf abgerufen (mit Buchstabe b gekennzeichnet) wird und der zuvor verbundene PSN vom

letzten Prüfkopf abgefragt wurde. Alle Schritte hier sind genau die gleichen wie im Fall mit Umleitungs-URL mit Ausnahme der Wiedergabe, die von PSN als Ergebnis von Probe 4 zurückgegeben wird. Wenn dieser Test auf demselben PSN gelandet ist, der ein Besitzer für die aktuelle Authentifizierungssitzung ist, enthält die Wiedergabe den Sitzungs-ID-Wert, der später vom Status-Agent verwendet wird, um den Prozess abzuschließen. Wenn das zuvor verbundene Headend nicht mit dem aktuellen Sitzungseigentümer identisch ist, schlägt die Sitzungssuche fehl, und das AC ISE-Statusmodul erhält eine leere Antwort. Dies hat letztendlich zur Folge, dass No Policy Server Detected -Nachricht an den Endbenutzer zurückgesendet.

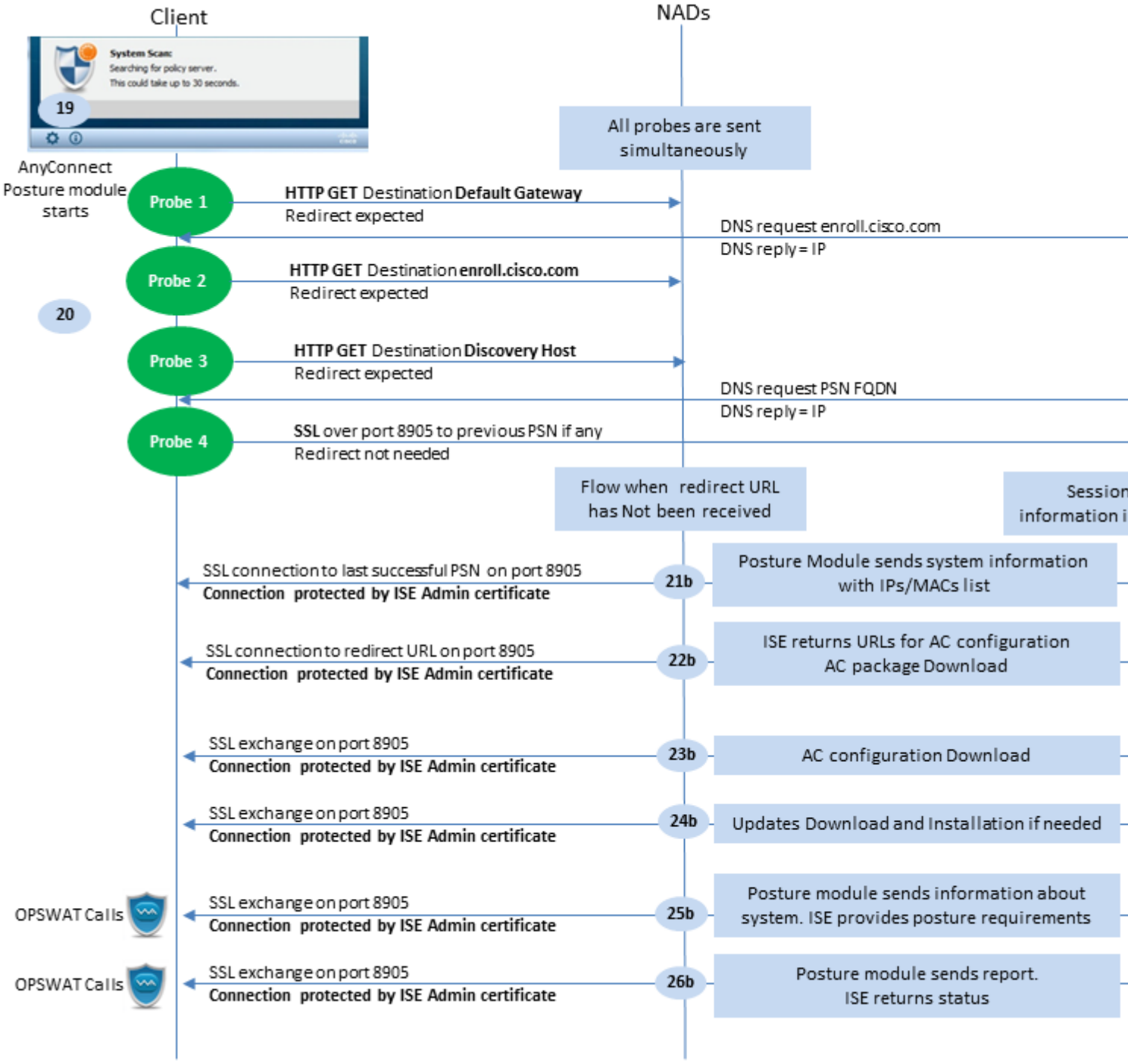

Abbildung 1-5

Statusüberprüfung nach ISE 2.2

ISE 2.2 und neuere Versionen unterstützen sowohl Umleitung als auch umleitungslose Datenflüsse gleichzeitig. Dies ist die detaillierte Erklärung für einen umleitungslosen Statusfluss:

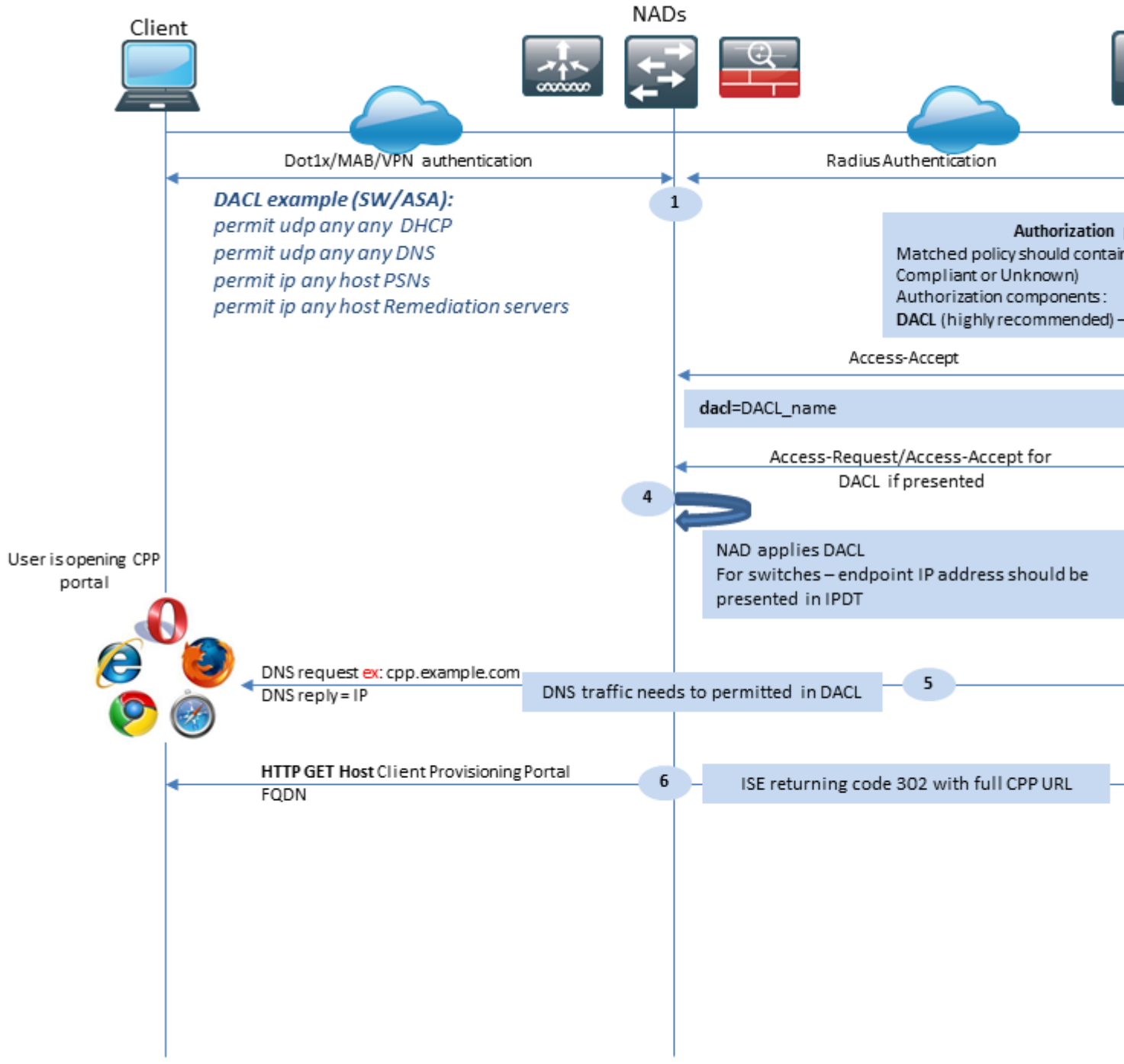

Abbildung 2-1

Schritt 1: Die Authentifizierung ist der erste Schritt des Datenflusses. Dabei kann es sich um dot1x, MAB oder VPN handeln.

Schritt 2: ISE muss die Authentifizierungs- und Autorisierungsrichtlinie für den Benutzer auswählen. In Statusinformationen muss die im Szenario gewählte Autorisierungsrichtlinie einen Verweis auf den Status enthalten, der zunächst entweder unbekannt oder nicht zutreffend sein muss. Um diese beiden Fälle

abzudecken, können Bedingungen mit Statusstatus und ungleicher Konformität verwendet werden. Bei einem Status ohne Umleitung muss im Autorisierungsprofil keine Webumleitungskonfiguration verwendet werden. Sie können weiterhin die Verwendung einer DACL oder einer Airspace-ACL in Betracht ziehen, um den Benutzerzugriff in der Phase zu beschränken, in der kein Statusstatus verfügbar ist.

Schritt 3: ISE gibt Access-Accept mit Autorisierungsattributen zurück.

Schritt 4: Wenn der DACL-Name in Access-Accept zurückgegeben wird, initiiert NAD den Download des DACL-Inhalts und wendet das Autorisierungsprofil nach dem Abrufen auf die Sitzung an.

Schritt 5: Bei dem neuen Ansatz wird davon ausgegangen, dass eine Umleitung nicht möglich ist. Daher muss der Benutzer den FQDN des Clientbereitstellungsportals manuell eingeben. Der FQDN des CPP-Portals muss in der Portkonfiguration auf der ISE-Seite definiert werden. Aus Sicht des DNS-Servers muss ein A-Eintrag auf den ISE-Server mit aktivierter PSN-Rolle verweisen.

Schritt 6: Der Client sendet HTTP, um an den FQDN des Clientbereitstellungsportals zu gelangen. Diese Anforderung wird auf der ISE-Seite analysiert, und die vollständige Portal-URL wird an den Client zurückgegeben.

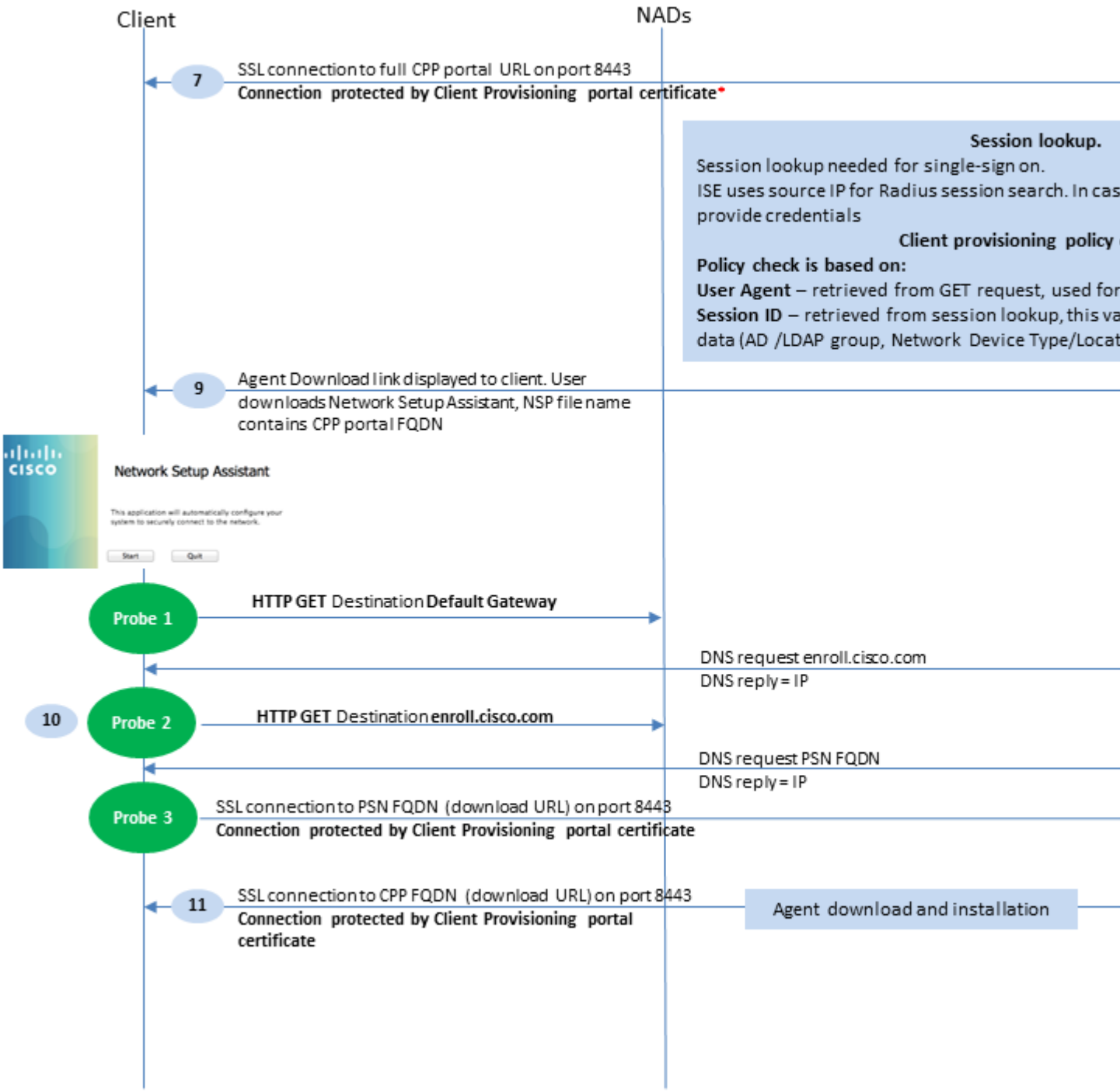

Abbildung 2-2

Schritt 7: Die SSL-Verbindung über den in der Umleitungs-URL empfangenen Port wird hergestellt (Standard 8443). Diese Verbindung wird durch ein Portalzertifikat von der ISE-Seite geschützt. Dem Benutzer wird das Client Provisioning Portal (CPP) angezeigt.

Schritt 8: In diesem Schritt treten auf der ISE zwei Ereignisse auf:

- Single Sign On (SSO) - ISE versucht, eine frühere erfolgreiche Authentifizierung nachzuschlagen. Die ISE verwendet die IP-Quelladresse des Pakets als Suchfilter für Live-Radiussitzungen.

Hinweis: Die Sitzung wird basierend auf einer Übereinstimmung zwischen der Quell-IP im Paket und

---

der Frame-IP-Adresse in der Sitzung abgerufen. Die eingerahmte IP-Adresse wird normalerweise von der ISE aus den Zwischenaktualisierungen der Buchhaltung abgerufen. Daher muss die Buchhaltung auf der NAD-Seite aktiviert sein. Beachten Sie außerdem, dass SSO nur auf dem Knoten möglich ist, der Besitzer der Sitzung ist. Wenn die Sitzung beispielsweise auf PSN 1 authentifiziert wird, der FQDN selbst jedoch auf PSN2 verweist, schlägt der SSO-Mechanismus fehl.

- Richtliniensuche für die Client-Bereitstellung: Bei einer erfolgreichen SSO kann die ISE Daten aus der authentifizierten Sitzung und den Benutzer-Agenten aus dem Client-Browser verwenden. Bei einer nicht erfolgreichen SSO muss der Benutzer Anmeldeinformationen angeben. Nachdem die Benutzerauthentifizierungsinformationen aus internen und externen Identitätsspeichern (AD/LDAP/Interne Gruppen) abgerufen wurden, können sie für die Richtlinienüberprüfung der Clientbereitstellung verwendet werden.

Hinweis: Aufgrund der Cisco Bug-ID CSCvd11574 wird bei der Richtlinienauswahl für die Clientbereitstellung für die Nicht-SSO-Fälle ein Fehler angezeigt, wenn der externe Benutzer Mitglied mehrerer AD/LDAP-Gruppen ist, die in der Konfiguration des externen Identitätsspeichers hinzugefügt wurden. Der genannte Fehler wurde behoben, der mit ISE 2.3 FCS beginnt, und der Fix erfordert die Verwendung von CONTAINS in der Bedingung mit der AD-Gruppe anstelle von EQUAL.

Schritt 9. Nach der Richtlinienauswahl für die Client-Bereitstellung zeigt die ISE dem Benutzer die URL für den Agentendownload an. Wenn Sie auf "NSA herunterladen" klicken, wird die Anwendung an den Benutzer übertragen. Der NSA-Dateiname enthält den FQDN des CPP-Portals.

Schritt 10.In diesem Schritt führt die NSA Tests durch, um eine Verbindung zur ISE herzustellen. Bei zwei dieser Tests handelt es sich um einen klassischen Test. Der dritte wurde entwickelt, um die ISE-Erkennung in Umgebungen ohne URL-Umleitung zu ermöglichen.

- NSA sendet die erste Erkennungssonde - HTTP/auth/discovery - an das Standard-Gateway. Die NSA erwartet daher eine Weiterleitungs-URL.
- Die NSA sendet eine zweite Anfrage, wenn die erste fehlschlägt. Der zweite Prüfpunkt ist HTTP GET /auth/discovery, um enroll.cisco.com. Dieser FQDN muss vom DNS-Server erfolgreich aufgelöst werden können. In einem VPN-Szenario mit einem Split-Tunnel enroll.cisco.com muss durch den Tunnel geleitet werden.
- Die NSA sendet die dritte Anfrage über den CPP-Portal-Port an den FQDN des Client-Bereitstellungsportals. Diese Anfrage enthält Informationen zur Portal-Session-ID, anhand derer die ISE feststellen kann, welche Ressourcen bereitgestellt werden müssen.

Schritt 11. NSA lädt AnyConnect und/oder bestimmte Module herunter. Der Download-Prozess erfolgt über den Port des Client-Bereitstellungsportals.

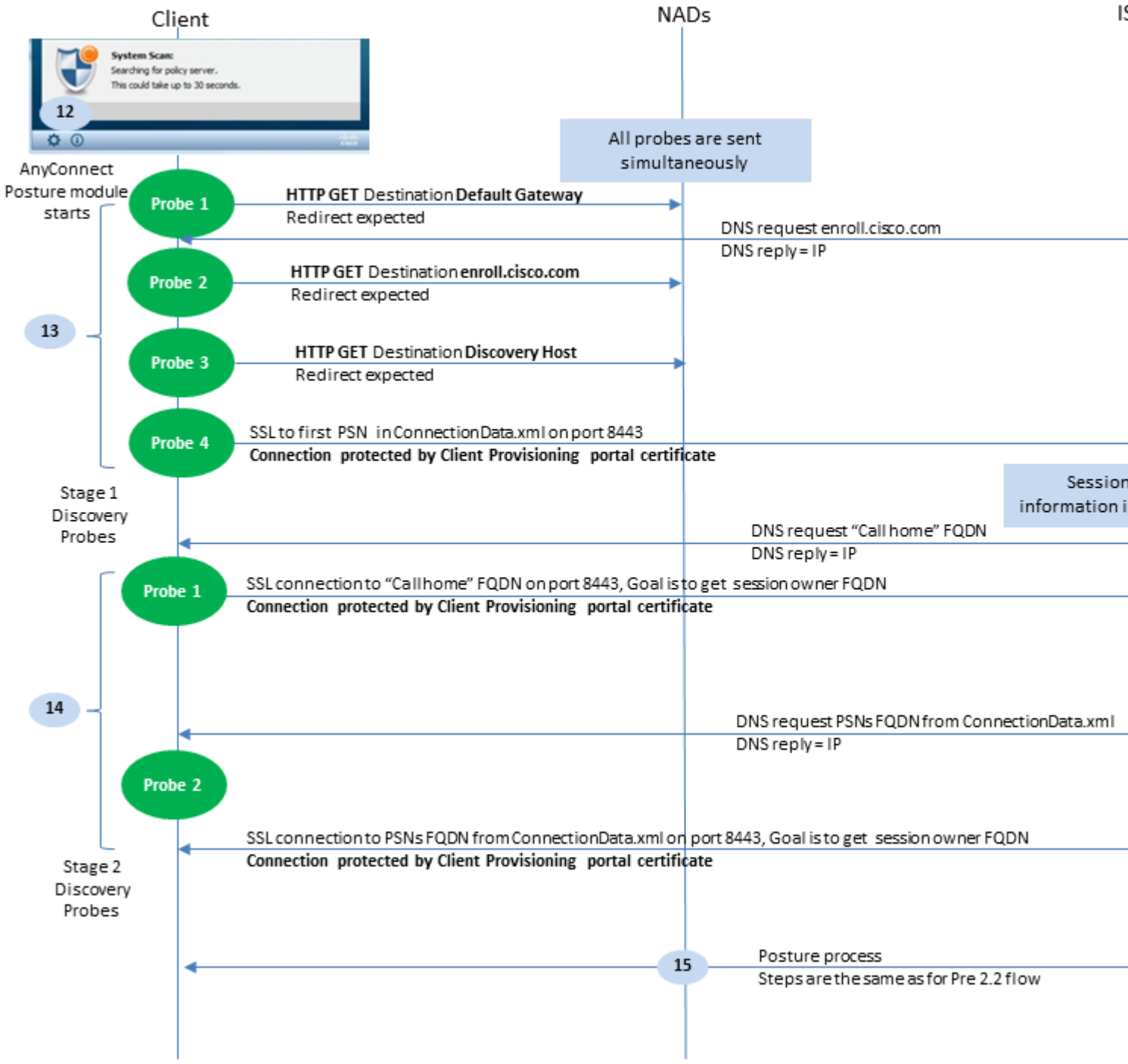

Abbildung 2-3

Schritt 12: In ISE 2.2 ist der Statusprozess in zwei Stufen unterteilt. Die erste Phase enthält eine Reihe traditioneller Statuserkennungssonden, um die Abwärtskompatibilität mit Bereitstellungen zu unterstützen, die auf der URL-Umleitung basieren.

Schritt 13: Die erste Stufe enthält alle traditionellen Körperhaltungs-Erkennungssonden. Weitere Informationen zu den Tests finden Sie in Schritt 20 im Status-Flow vor ISE 2.2.

Schritt 14.Phase zwei enthält zwei Erkennungssonden, mit denen das AC ISE Statusmodul eine Verbindung zum PSN herstellen kann, bei dem die Sitzung in Umgebungen authentifiziert wird, in denen eine Umleitung nicht unterstützt wird**.** Während der zweiten Phase sind alle Sonden sequenziell.

- Probe 1: Während der ersten Untersuchung versucht das AC ISE-Statusmodul, eine Verbindung mit

IP/FQDNs aus der 'Call Home List' herzustellen. Eine Liste der Ziele für den Prüfpunkt muss im AC-Statusprofil auf der ISE-Seite konfiguriert werden. Sie können IPs/FQDNs durch Kommas getrennt definieren, mit einem Doppelpunkt können Sie die Portnummer für jedes Call Home-Ziel definieren. Dieser Port muss dem Port entsprechen, auf dem das Client-Bereitstellungsportal ausgeführt wird. Client-seitige Informationen zu Call Home-Servern finden Sie unter ISEPostureCFG.xmlfinden Sie diese Datei im Ordner - C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture\.
Falls das Call Home-Ziel nicht Eigentümer der Sitzung ist, muss zu diesem Zeitpunkt nach dem Besitzer gesucht werden. Das Statusmodul der AC ISE weist die ISE an, eine Owner-Suche unter Verwendung einer speziellen Ziel-URL zu starten. /auth/ng-discovery Anfrage. Er enthält auch die Liste der Client-IPs und -MACs. Nachdem diese Nachricht von der PSN-Sitzung empfangen wurde, wird zunächst lokal eine Suche durchgeführt (bei dieser Suche werden sowohl IPs als auch MACs aus der vom AC ISE-Statusmodul gesendeten Anforderung verwendet). Wenn die Sitzung nicht gefunden wird, initiiert PSN eine MNT-Knotenabfrage. Diese Anforderung enthält nur die MAC-Liste. Daher muss der FQDN des Besitzers vom MNT bezogen werden. Anschließend gibt PSN den Besitzer-FQDN an den Client zurück. Die nächste Anforderung vom Client wird an den FQDN des Sitzungseigentümers gesendet, der über eine Auth-/Statusangabe in einer URL und einer Liste mit IPs und MACs verfügt.

- Prüfpunkt 2: Zu diesem Zeitpunkt testet das AC ISE-Statusmodul die PSN-FQDNs, die sich in ConnectionData.xml. Diese Datei finden Sie unter C:\Users\

  \AppData\Local\Cisco\Cisco AnyConnect Secure Mobility Client\
  . Das AC ISE Posture-Modul erstellt diese Datei nach dem ersten Statusversuch. Die Datei enthält eine Liste der FQDNs der ISE-PSNs. Der Inhalt der Liste kann bei den nächsten Verbindungsversuchen dynamisch aktualisiert werden. Das Endziel dieser Überprüfung besteht darin, den FQDN des aktuellen Sitzungseigentümers zu ermitteln. Die Implementierung ist identisch mit Probe 1., mit dem einzigen Unterschied bei der Auswahl des Testziels.
  Die Datei selbst befindet sich im Ordner des aktuellen Benutzers, falls das Gerät von mehreren Benutzern verwendet wird. Ein anderer Benutzer kann die Informationen aus dieser Datei nicht verwenden. Dies kann Benutzer in Umgebungen ohne Umleitung zum Problem mit Hühnern und Eiern führen, wenn keine Call Home-Ziele angegeben werden.

Schritt 15: Nachdem Informationen über den Sitzungseigentümer abgerufen wurden, sind alle nachfolgenden Schritte mit dem Fluss vor ISE 2.2 identisch.

Konfigurieren

Für dieses Dokument wird ASAv als Netzwerkzugriffsgerät verwendet. Alle Tests werden mit einem Status über VPN durchgeführt. Die ASA-Konfiguration zur Unterstützung von Statusinformationen über VPN wird im Dokument nicht behandelt. Weitere Informationen finden Sie im Konfigurationsbeispiel für den VPN-Status der ASA Version 9.2.1 mit ISE.

Hinweis: Für die Bereitstellung mit VPN-Benutzern wird ein umleitungsbasierter Status empfohlen. Die Konfiguration der Telefonliste wird nicht empfohlen. Stellen Sie für alle nicht VPN-basierten Benutzer sicher, dass die DACL so angewendet wird, dass sie bei konfiguriertem Status nicht mit dem PSN kommunizieren.

Netzwerkdiagramm

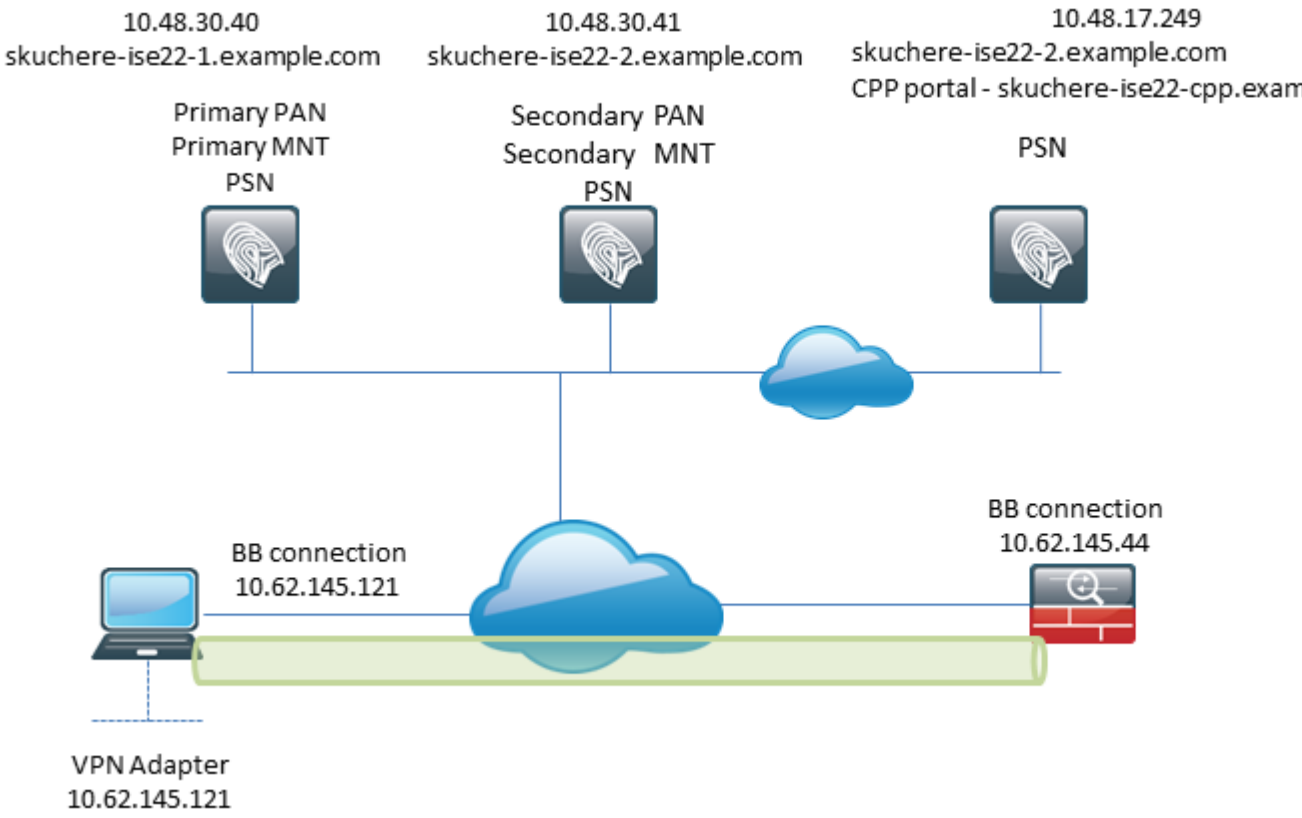

Abbildung 3-1

Diese Topologie wird in Tests verwendet. Mit ASA kann das Szenario einfach simuliert werden, wenn der SSO-Mechanismus für das Client-Bereitstellungsportal auf der PSN-Seite aufgrund der NAT-Funktion ausfällt. Im Fall eines regulären Statusflusses über VPN muss SSO gut funktionieren, da NAT für VPN-IPs normalerweise nicht erzwungen wird, wenn Benutzer in das Unternehmensnetzwerk eintreten.

Konfigurationen

Konfiguration der Client-Bereitstellung

Dies sind die Schritte zum Vorbereiten der AnyConnect-Konfiguration.

Schritt 1: Download von AnyConnect-Paketen. AnyConnect-Paket selbst ist nicht zum direkten Download von der ISE verfügbar. Stellen Sie daher vor dem Start sicher, dass AC auf Ihrem PC verfügbar ist. Dieser Link kann für den AC-Download verwendet werden - https://www.cisco.com/site/us/en/products/security/secure-client/index.html In diesem Dokument anyconnect-win-4.4.00243-webdeploy-k9.pkg -Paket verwendet wird.

Schritt 2: Um das AC-Paket auf die ISE hochzuladen, navigieren Sie zu Policy > Policy Elements > Results > Client Provisioning > Resourcesund klicke auf Add. Wählen Sie Agent-Ressourcen von der lokalen Festplatte aus. Wählen Sie im neuen Fenster Cisco Provided Packages,Klicken Sie auf browse und wählen Sie das Wechselstrompaket auf Ihrem PC aus.

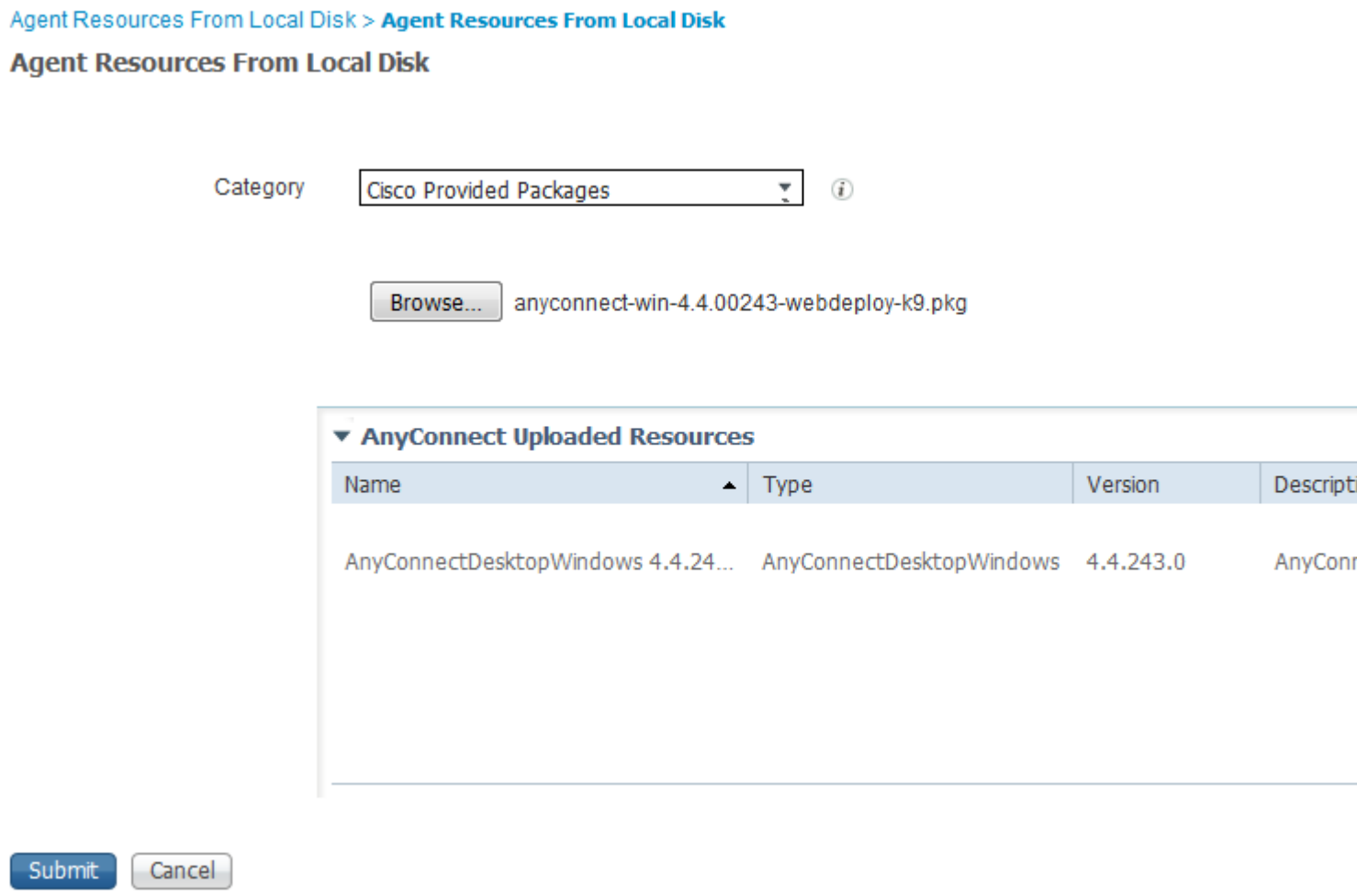

Abbildung 3-2

Klicken Sie auf Submit um den Import abzuschließen.

Schritt 3: Das Compliance-Modul muss in die ISE hochgeladen werden. Klicken Sie auf derselben Seite auf Add und wählen Sie Agent resources from Cisco site. In der Ressourcenliste müssen Sie ein Kompatibilitätsmodul überprüfen. Für dieses Dokument AnyConnectComplianceModuleWindows 4.2.508.0 Compliance-Modul verwendet.

Schritt 4: Jetzt muss ein AC-Statusprofil erstellt werden. Klicken Sie auf Add und wählen Sie NAC agent or Anyconnect posture profile.

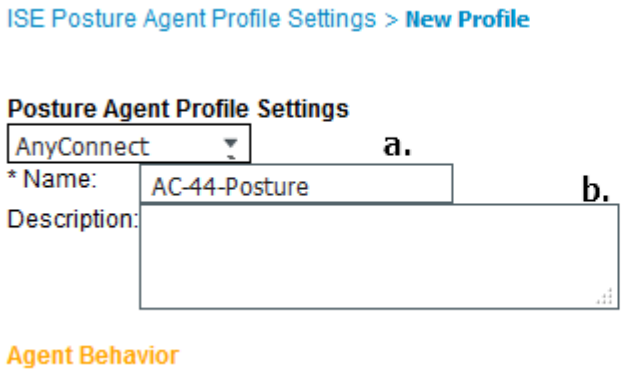

Abbildung 3-3

- Wählen Sie den Profiltyp aus. Für dieses Szenario muss AnyConnect verwendet werden.
- Geben Sie den Profilnamen an. Navigieren Sie zum Posture Protocol Abschnitt des Profils.

Posture Protocol

Parameter	Value	Notes
PRA retransmission time	120 secs	
Discovery host		
* Server name rules	* a.	need to be blank by default to force ad enter a value. "*" means agent will con to all
Call Home List	skuchere-ise22-2.examp b.	List of IP addresses, FQDNs with or w port must be comma-separated and w colon in between the IP address/FQDN the port. Example: IPaddress/FQDN:P (Port number should be the same, spe in the Client Provisioning portal)
Back-off Timer	30 secs	Enter value of back-off timer in second supported range is between 10s - 600

Abbildung 3-4

- Geben Sie Server Name Rules, darf dieses Feld nicht leer sein. Das Feld kann einen FQDN mit einem Platzhalter enthalten, der die Verbindung des AC ISE-Statusmoduls auf PSNs aus dem entsprechenden Namespace beschränkt. Stern setzen, wenn ein FQDN erlaubt sein muss.
- Die hier angegebenen Namen und IPs werden in Phase 2 der Statuserkennung verwendet. Sie können Namen durch Koma trennen und Portnummern können nach FQDN/IP mithilfe des Doppelpunkts hinzugefügt werden. Falls das AC Out-of-Band (nicht über das ISE-Client-Bereitstellungsportal) mithilfe des GPO oder eines anderen Software-Bereitstellungssystems bereitstellt, ist das Vorhandensein von Call Home-Adressen von entscheidender Bedeutung, da dies nur ein Prüfpunkt ist, der ISE PSN erfolgreich erreichen kann. Das bedeutet, dass der Administrator bei der Out-Of-Band-AC-Bereitstellung unter Verwendung des AC-Profil-Editors ein AC ISE-Statusprofil erstellen und diese Datei zusammen mit der AC-Installation bereitstellen muss.

Hinweis: Beachten Sie, dass das Vorhandensein von Call Home-Adressen für PCs mit mehreren Benutzern von entscheidender Bedeutung ist. Überprüfen Sie Schritt 14 in Statusüberprüfung nach ISE 2.2.

Schritt 5:Erstellen einer AC-Konfiguration Navigieren Sie zu Policy > Policy Elements > Results > Client Provisioning > Resources, Klicken Sie auf Add, und wählen Sie AnyConnect Configuration.

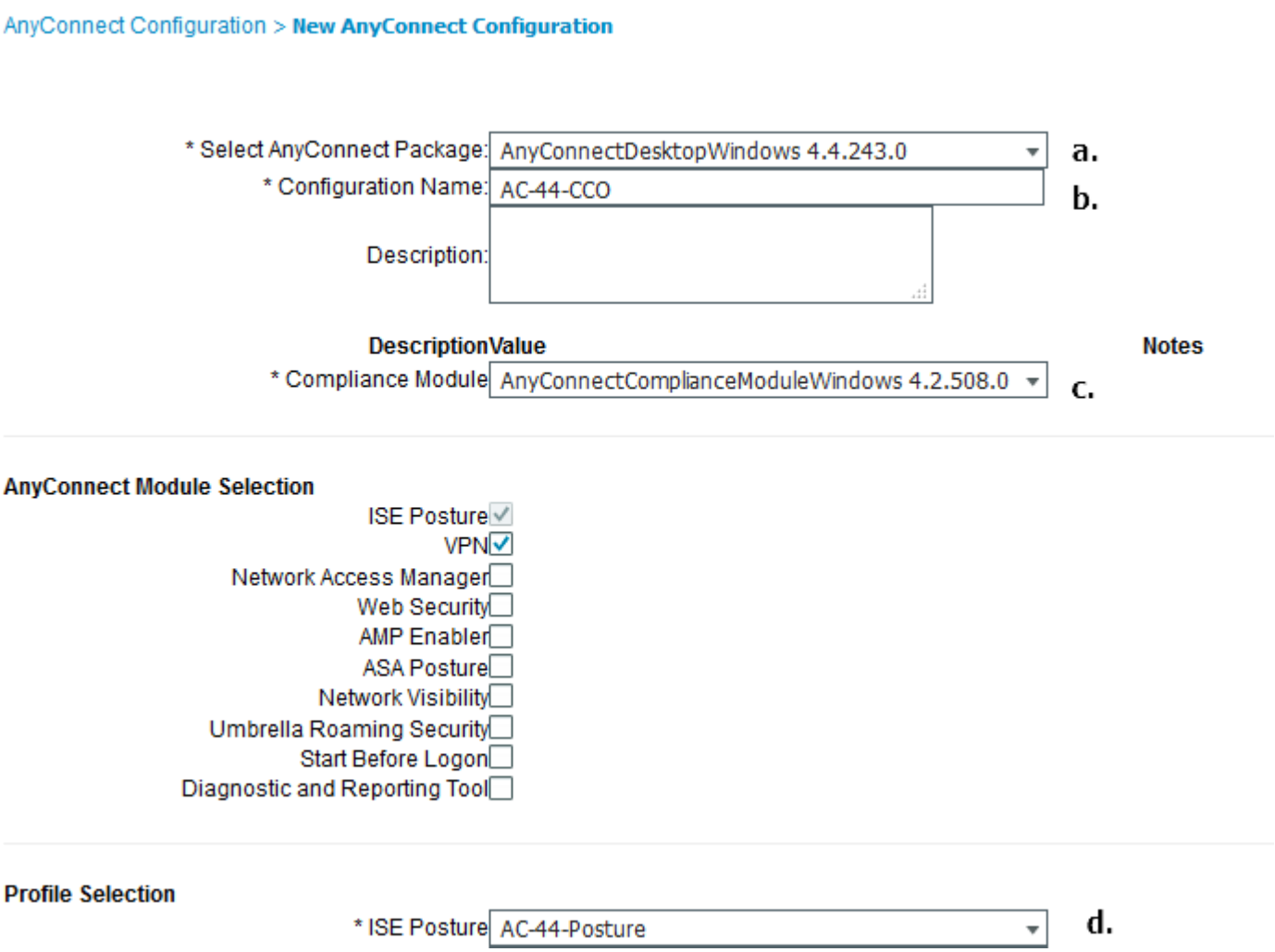

Abbildung 3-5

- Wählen Sie das AC-Paket aus.
- Geben Sie den AC-Konfigurationsnamen an.
- Wählen Sie die Version des Compliance-Moduls aus.
- Wählen Sie aus der Dropdown-Liste das Profil für die Konfiguration des Netzstatus aus.

Schritt 6: Konfigurieren der Richtlinie für die Clientbereitstellung Navigieren Sie zu Policy > Client Provisioning. Bei der Erstkonfiguration können Sie leere Werte in die vorgestellte Richtlinie mit Standardwerten füllen. Wenn Sie der vorhandenen Statuskonfiguration eine Richtlinie hinzufügen müssen, navigieren Sie zu der Richtlinie, die wiederverwendet werden kann, und wählen Sie Duplicate Above Oder Duplicate Below . Eine brandneue Richtlinie kann ebenfalls erstellt werden.

Dies ist ein Beispiel für die im Dokument verwendete Richtlinie.

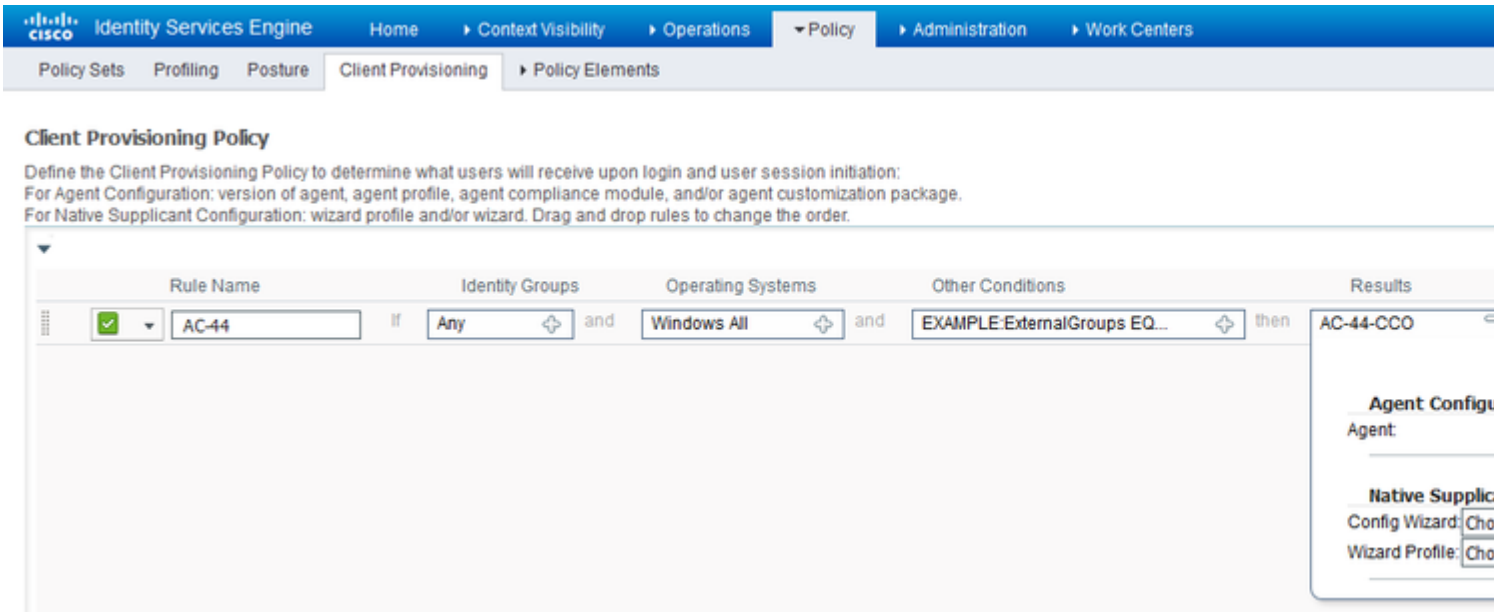

Abbildung 3-6

Wählen Sie im Ergebnisabschnitt Ihre AC-Konfiguration aus. Beachten Sie, dass die ISE bei einem SSO-Ausfall nur über Attribute von der Anmeldung bis zum Portal verfügen kann. Diese Attribute beschränken sich auf Informationen, die über Benutzer aus internen und externen Identitätsdaten abgerufen werden können. In diesem Dokument wird die AD-Gruppe als Bedingung in der Richtlinie für die Clientbereitstellung verwendet.

Statusrichtlinien und -bedingungen

Es wird eine einfache Statusüberprüfung verwendet. Die ISE ist so konfiguriert, dass der Status des Window Defender-Dienstes auf der Seite des Endgeräts überprüft wird. Die tatsächlichen Szenarien können viel komplizierter sein, aber die allgemeinen Konfigurationsschritte sind identisch.

Schritt 1: Erstellen Sie einen Sicherheitsstatus. Statusbedingungen befinden sich in Policy > Policy Elements > Conditions > Posture. Wählen Sie den Typ des Statuszustands aus. Das folgende Beispiel zeigt eine Dienstbedingung, die überprüfen muss, ob der Dienst Windows Defender ausgeführt wird.

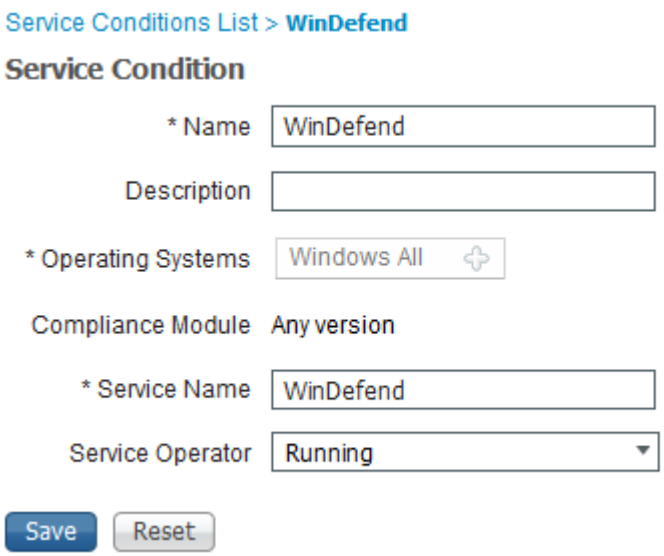

Abbildung 3-7

Schritt 2: Konfiguration der Statusanforderungen. Navigieren Sie zu Policy > Policy Elements > Results > Posture > Requirements. Dies ist ein Beispiel für eine Windows Defender-Prüfung:

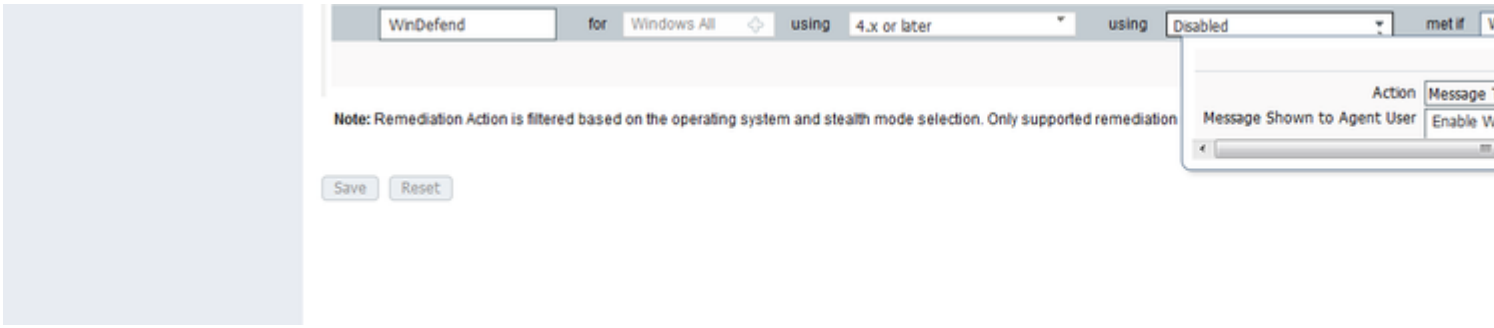

Abbildung 3-8

Wählen Sie den Status für die neue Anforderung aus, und geben Sie eine Korrekturmaßnahme an.

Schritt 3: Konfiguration von Statusrichtlinien. Navigieren Sie zu Policy > Posture. Hier finden Sie ein Beispiel für die in diesem Dokument verwendete Richtlinie. Der Richtlinie wurde die Windows Defender-Anforderung als obligatorisch zugewiesen, und sie enthält nur den externen AD-Gruppennamen als Bedingung.

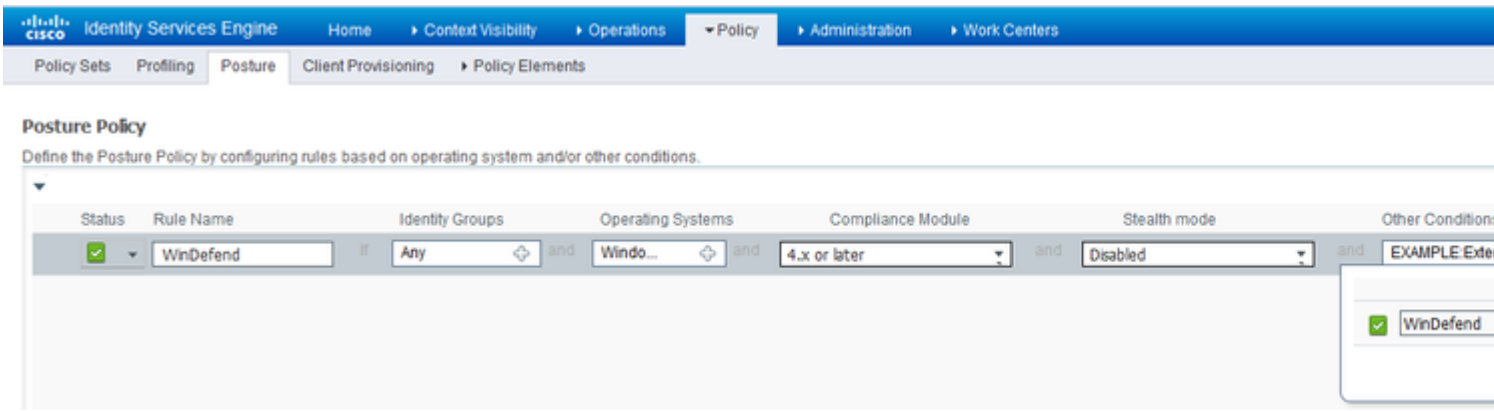

Abbildung 3-9

Konfigurieren des Client-Bereitstellungsportals

Bei einem Status ohne Umleitung muss die Konfiguration des Client-Bereitstellungsportals bearbeitet werden. Navigieren Sie zu Administration > Device Portal Management > Client Provisioning.Sie können entweder das Standardportal verwenden oder ein eigenes erstellen. Das gleiche Portal kann für beide Haltungen mit und ohne Umleitung genutzt werden.

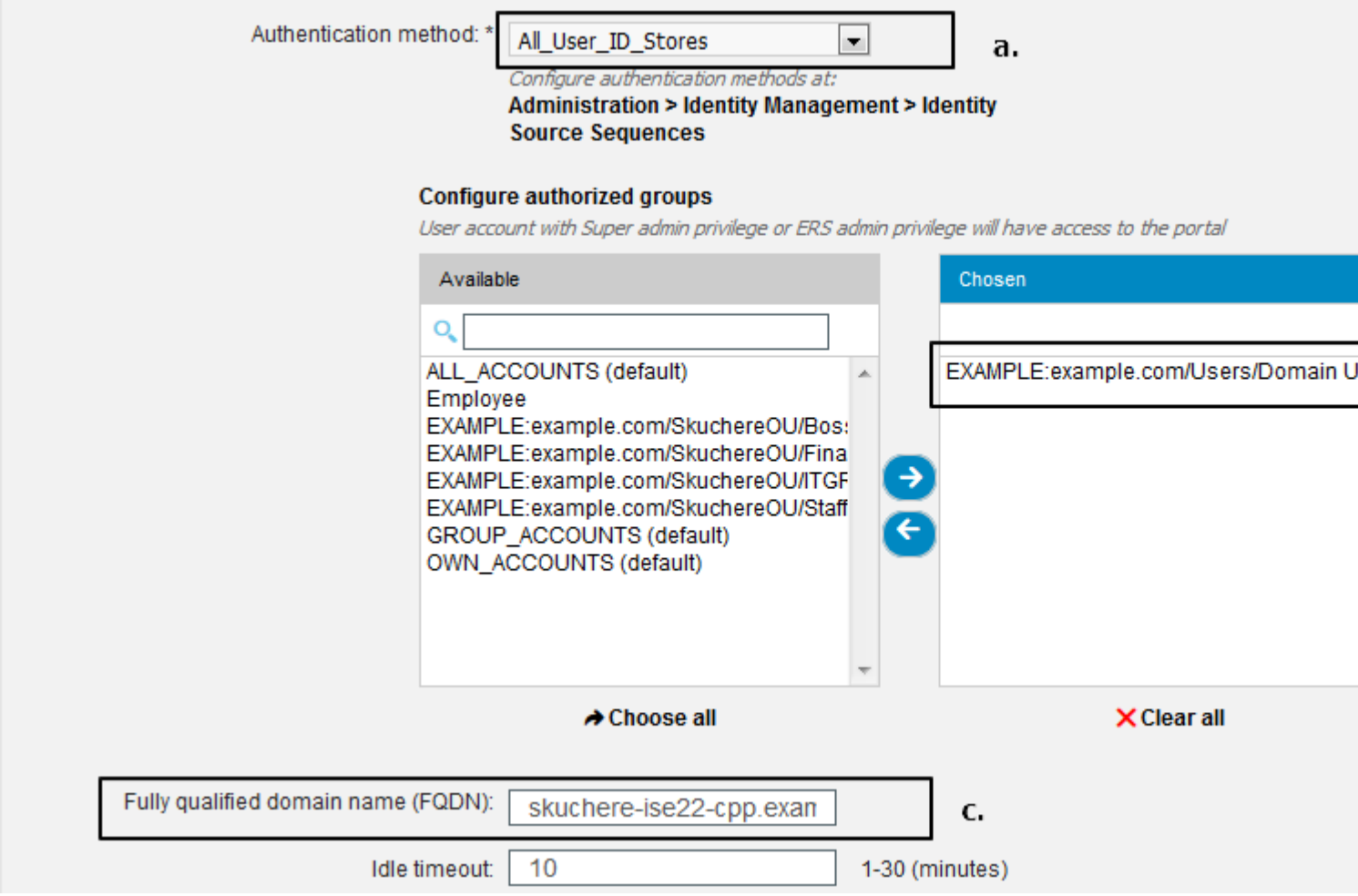

Abbildung 3-10

Diese Einstellungen müssen in der Portalkonfiguration für das Szenario ohne Umleitung bearbeitet werden:

- Geben Sie unter Authentication (Authentifizierung) Identity Source Sequence an, die verwendet werden muss, wenn SSO keine Sitzung für den Benutzer finden kann.
- Gemäß der ausgewählten Identity Source Sequence-Liste werden die verfügbaren Gruppen aufgefüllt. An diesem Punkt müssen Sie Gruppen auswählen, die für die Portal-Anmeldung autorisiert sind.
- Der FQDN des Client-Bereitstellungsportals muss für Szenarien angegeben werden, in denen Wechselstrom vom Client-Bereitstellungsportal bereitgestellt werden muss. Dieser FQDN muss in ISE PSNs IPs auflösbar sein. Benutzer müssen angewiesen werden, den FQDN beim ersten Verbindungsversuch im Webbrowser anzugeben.

Autorisierungsprofile und Richtlinien konfigurieren

Der Erstzugriff für Clients, die keinen Statusstatus haben, muss eingeschränkt werden. Dies kann auf verschiedene Weise erreicht werden:

- DACL-Zuweisung - Während der Phase des eingeschränkten Zugriffs kann dem Benutzer DACL zugewiesen werden, um den Zugriff zu beschränken. Dieser Ansatz kann für Cisco Netzwerkzugriffsgeräte verwendet werden.
- VLAN-Zuweisung - Bevor Benutzer mit eingeschränktem VLAN auf einen erfolgreichen Status zugreifen können, muss dieser Ansatz bei fast allen NAD-Anbietern reibungslos funktionieren.
- Radius-Filter-ID - Mit diesem Attribut kann eine lokal in NAD definierte ACL einem Benutzer mit unbekanntem Status zugewiesen werden. Da es sich hierbei um ein RFC-Standardattribut handelt, muss dieser Ansatz bei allen NAD-Anbietern gut funktionieren.

Schritt 1: Konfigurieren der DACL Da dieses Beispiel auf ASA basiert, kann eine NAD-DACL verwendet werden. In realen Szenarien müssen Sie VLAN oder Filter-ID als mögliche Optionen in Betracht ziehen.

Um DACL zu erstellen, navigieren Sie zu Policy > Policy Elements > Results > Authorization > Downloadable ACLsund klicke auf Add**.**

Im unbekannten Status müssen mindestens diese Berechtigungen erteilt werden:

- DNS-Datenverkehr
- DHCP-Datenverkehr
- Verkehr zu ISE PSNs (Ports 80 und 443 für eine Möglichkeit, freundlichen FQDN des Portals zu öffnen. Standardmäßig ist der Port, auf dem das CP-Portal ausgeführt wird, 8443, aus Gründen der Abwärtskompatibilität Port 8905.)
- Datenverkehr zu Problembehebungsservern (falls erforderlich)

Dies ist ein Beispiel für DACL ohne Wiederherstellungsserver:

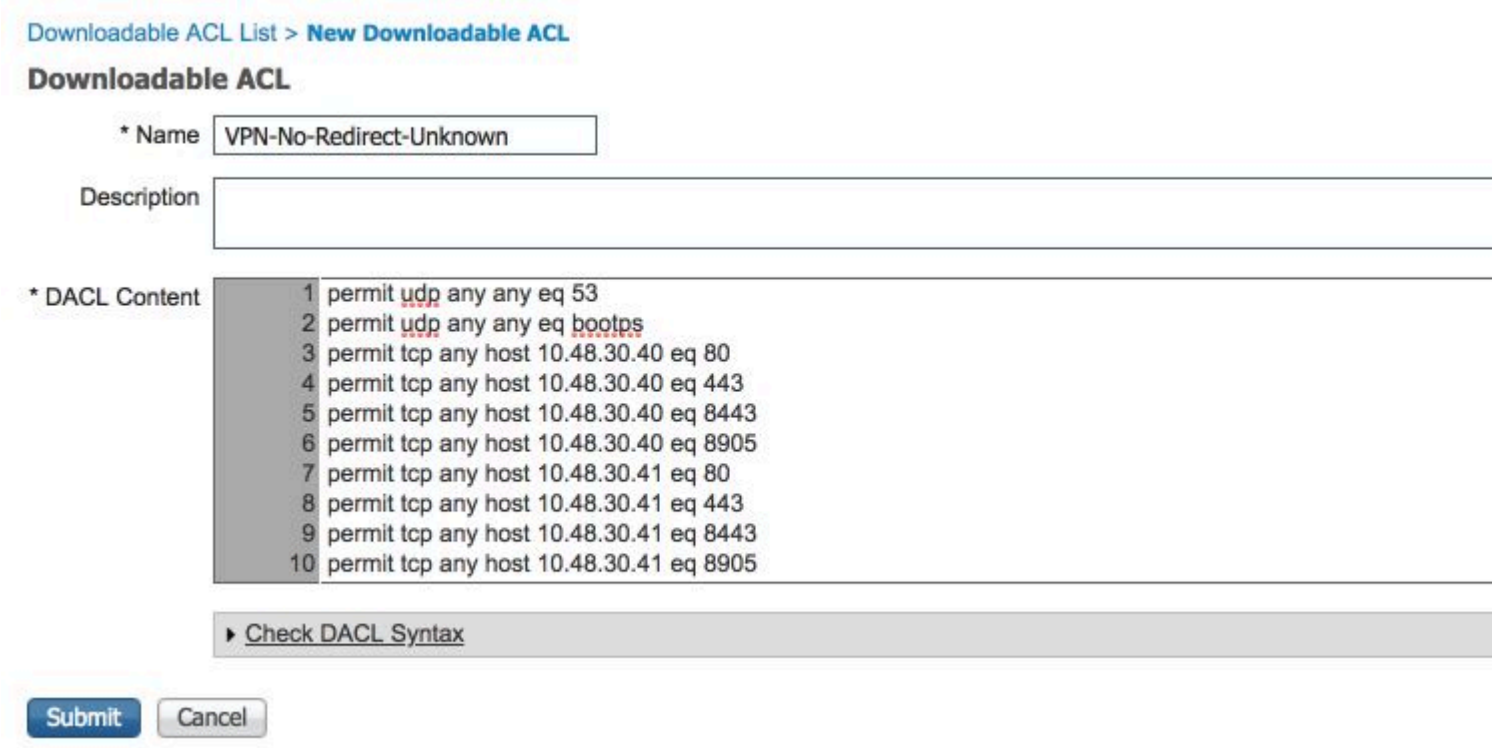

Abbildung 3-11

Schritt 2: Autorisierungsprofil konfigurieren.

Wie üblich sind für die Haltung zwei Berechtigungsprofile erforderlich. Die erste muss jede Art von Netzwerkzugriffsbeschränkung enthalten (in diesem Beispiel wird das Profil mit DACL verwendet). Dieses Profil kann auf die Authentifizierungen angewendet werden, deren Status nicht konform ist. Das zweite Autorisierungsprofil enthält Berechtigungen für den Zugriff und kann für Sitzungen angewendet werden, deren Status der Compliance entspricht.

Navigieren Sie zum Erstellen eines Autorisierungsprofils zu Policy > Policy Elements > Results > Authorization > Authorization Profiles.

Beispiel für ein Profil mit eingeschränktem Zugriff:

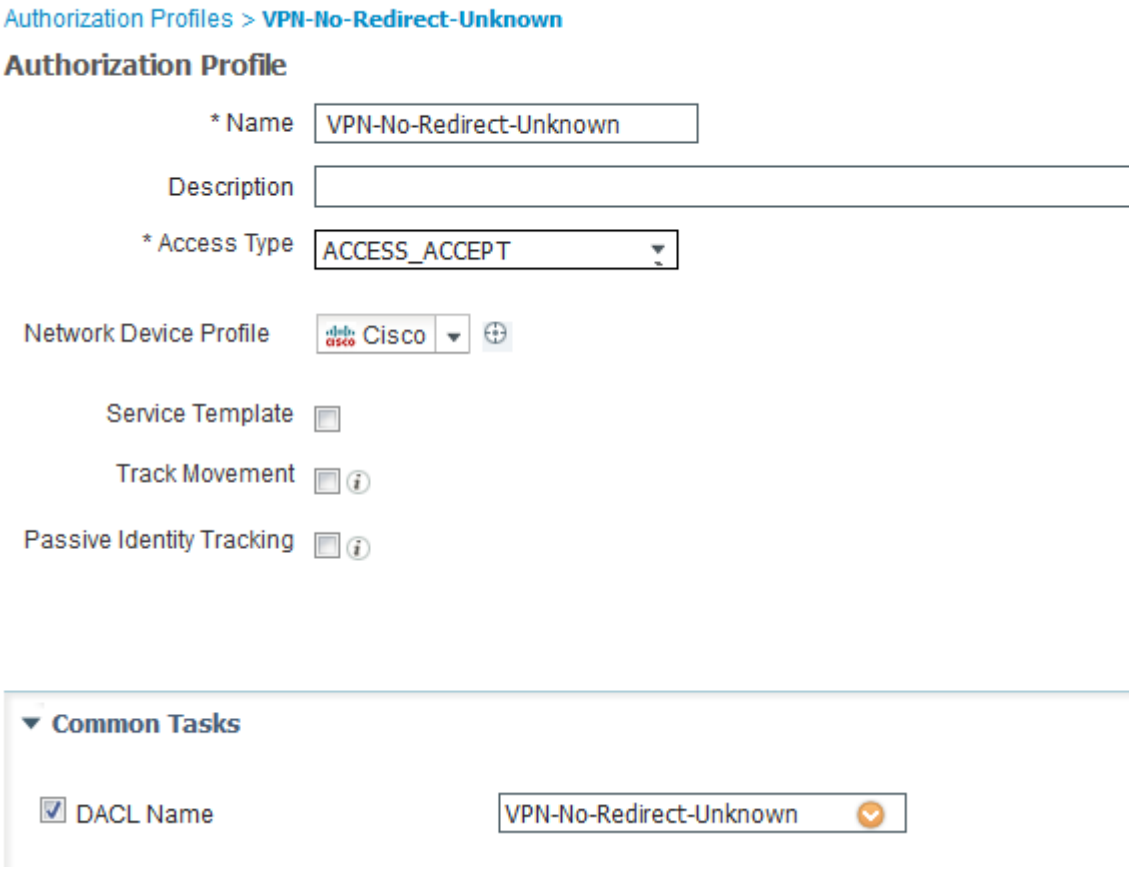

Abbildung 3-12

In diesem Beispiel wird das Standard-ISE-Profil PermitAccess für die Sitzung nach einer erfolgreichen Statusüberprüfung verwendet.

Schritt 3: Autorisierungsrichtlinie konfigurieren In diesem Schritt müssen zwei Autorisierungsrichtlinien erstellt werden. Eine besteht darin, die erste Authentifizierungsanforderung mit einem unbekannten Status abzugleichen, und die zweite besteht darin, nach einem erfolgreichen Statusprozess den vollständigen Zugriff zuzuweisen.

Dies ist ein Beispiel für einfache Autorisierungsrichtlinien in diesem Fall:

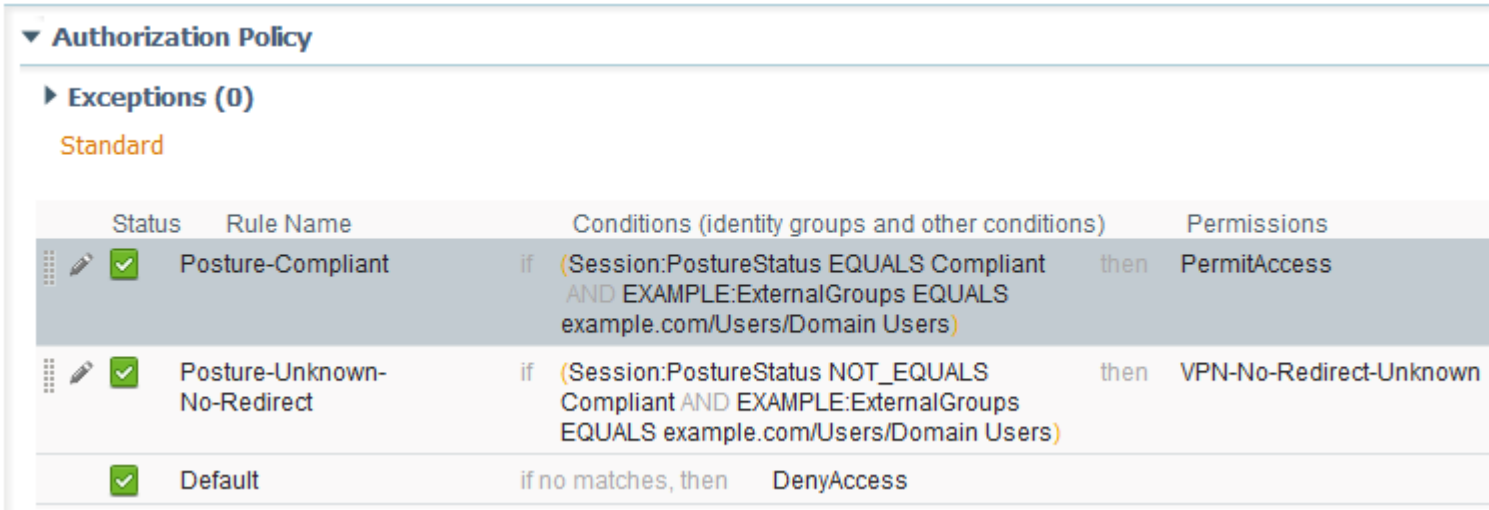

Abbildung 3-13

Die Konfiguration der Authentifizierungsrichtlinie ist nicht Teil dieses Dokuments. Sie sollten jedoch bedenken, dass eine erfolgreiche Authentifizierung vor der Verarbeitung der Autorisierungsrichtlinie erfolgen muss.

Überprüfung

Die grundlegende Überprüfung des Datenflusses kann aus drei Hauptschritten bestehen:

Schritt 1: Überprüfung des Authentifizierungsflusses.

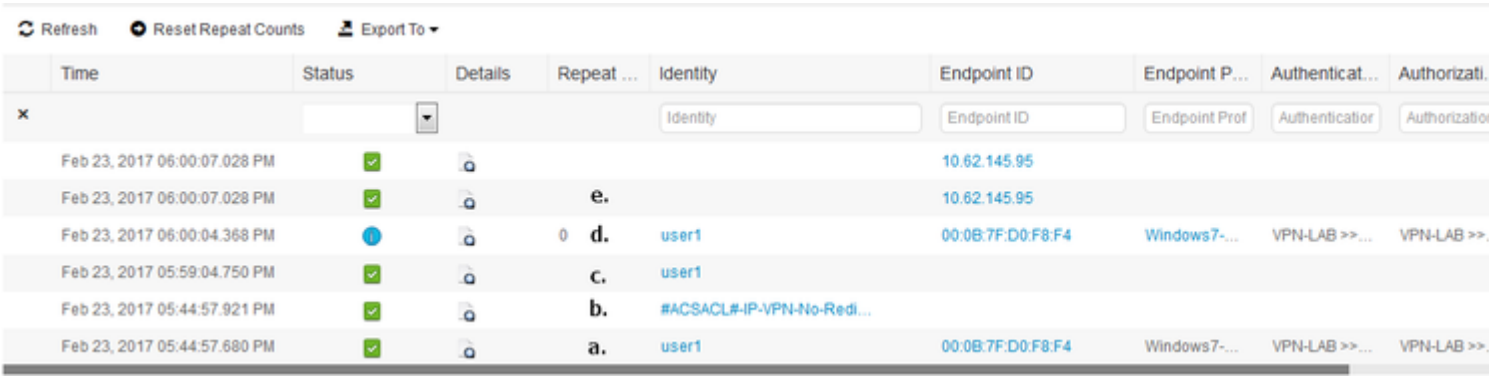

Abbildung 4-1

1. Anfängliche Authentifizierung. Für diesen Schritt können Sie daran interessiert sein, für welche Validierung das Autorisierungsprofil angewendet wurde. Wenn ein unerwartetes Autorisierungsprofil angewendet wurde, untersuchen Sie einen detaillierten Authentifizierungsbericht. Sie können diesen Bericht mit einem Klick auf die Lupe in der Spalte Details öffnen. Sie können Attribute in detaillierten Authentifizierungsberichten mit Bedingungen in der Autorisierungsrichtlinie vergleichen, die Sie voraussichtlich abgleichen werden.

2. DACL-Downloadereignis. Diese Zeichenfolge wird nur angezeigt, wenn das für die Erstauthentifizierung ausgewählte Autorisierungsprofil einen DACL-Namen enthält.

3. Portal authentication: Dieser Schritt im Fluss gibt an, dass der SSO-Mechanismus die Benutzersitzung nicht gefunden hat. Dies kann aus mehreren Gründen passieren:
   - NAD ist nicht für das Senden von Abrechnungsnachrichten konfiguriert, oder darin ist keine eingerahmte IP-Adresse vorhanden.
   - Der FQDN des CPP-Portals wurde in die IP-Adresse des ISE-Knotens aufgelöst, die sich von der des Knotens unterscheidet, in dem die anfängliche Authentifizierung verarbeitet wurde
   - Der Client befindet sich hinter der NAT

4. Sitzungsdaten ändern sich. In diesem Beispiel hat sich der Sitzungsstatus von "Unbekannt" in "Compliant" geändert.

5. COA zum Netzwerkzugriffsgerät. Dieser COA muss erfolgreich sein, um eine neue Authentifizierung von der NAD-Seite und eine neue Autorisierungsrichtlinienzuweisung auf der ISE-Seite weiterzugeben. Wenn der COA fehlschlägt, können Sie einen ausführlichen Bericht öffnen, um den Grund zu untersuchen. Die häufigsten Probleme im Zusammenhang mit dem COA können sein:

- COA-Zeitüberschreitung - In diesem Fall wird entweder der PSN, der die Anforderung gesendet hat, nicht als COA-Client auf der NAD-Seite konfiguriert, oder die COA-Anforderung wurde unterwegs verworfen.
- COA negativ ACK - Geben Sie an, dass COA von NAD empfangen wurde, der COA-Vorgang aus irgendeinem Grund jedoch nicht bestätigt werden kann. Für dieses Szenario muss ein ausführlicher Bericht eine ausführlichere Erklärung enthalten.

Da ASA in diesem Beispiel als NAD verwendet wird, wird keine nachfolgende Authentifizierungsanforderung für den Benutzer angezeigt. Dies liegt daran, dass die ISE COA-Push für ASA verwendet, wodurch Unterbrechungen des VPN-Services vermieden werden. In einem solchen Szenario enthält COA selbst neue Autorisierungsparameter, sodass eine erneute Authentifizierung nicht erforderlich ist.

Schritt 2: Überprüfung der Auswahl der Client-Bereitstellungsrichtlinie - Zu diesem Zweck können Sie einen Bericht auf der ISE ausführen, der Ihnen helfen kann, zu verstehen, welche Client-Bereitstellungsrichtlinien für den Benutzer angewendet wurden.

Navigieren Sie zu Operations > Reports Endpoint and Users > Client Provisioning und führen Sie den Bericht für das gewünschte Datum aus.

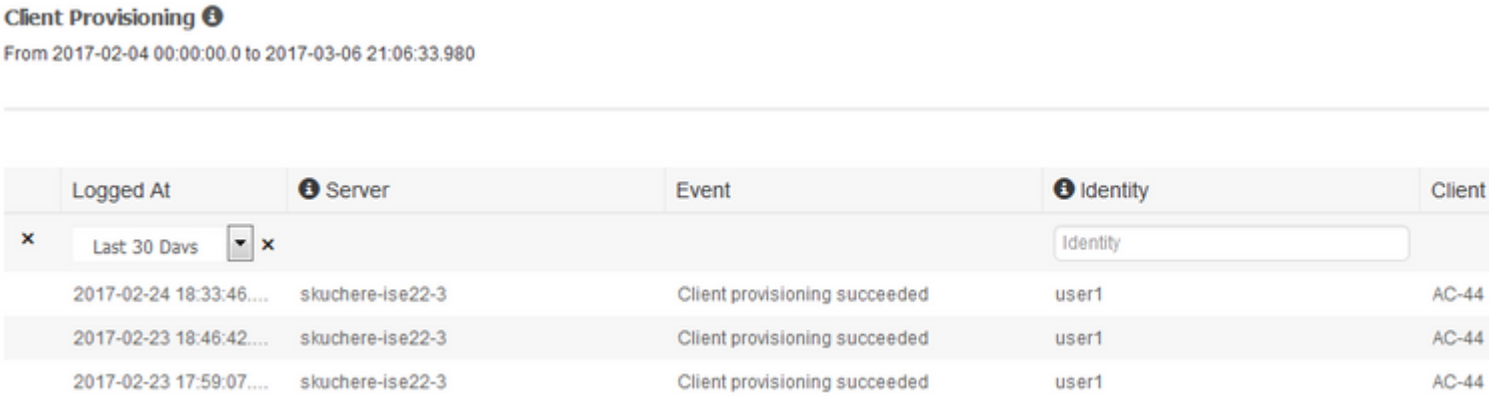

Abbildung 4-2

Mit diesem Bericht können Sie überprüfen, welche Client-Bereitstellungsrichtlinie ausgewählt wurde. Außerdem müssen im Falle eines Fehlers die Gründe im Failure Reason Spalte.

Schritt 3: Überprüfung des Statusberichts - Navigieren Sie zu Operations > Reports Endpoint and Users > Posture Assessment by Endpoint.

Abbildung 4-3

Sie können hier für jedes Ereignis einen detaillierten Bericht öffnen, um z. B. zu überprüfen, zu welcher

Sitzungs-ID dieser Bericht gehört, welche Statusanforderungen die ISE für den Endpunkt ausgewählt hat und welchen Status die einzelnen Anforderungen haben.

Fehlerbehebung

Allgemeine Informationen

Zur Fehlerbehebung bei Statusprozessen müssen diese ISE-Komponenten aktiviert werden, um auf den ISE-Knoten zu debuggen, auf denen der Statusprozess erfolgen kann:

- client-webapp - Die für die Agentenbereitstellung verantwortliche Komponente. Zielprotokolldateien guest.log und ise-psc.log.
- guestacess - Die Komponente, die für die Suche der Client-Bereitstellungsportalkomponente und des Sitzungseigentümers verantwortlich ist (wenn die Anforderung das falsche PSN betrifft). Ziel-Protokolldatei - guest.log.
- provisioning - Die Komponente, die für die Richtlinienverarbeitung für die Clientbereitstellung verantwortlich ist. Ziel-Protokolldatei - guest.log.
- posture - Alle Statusereignisse. Ziel-Protokolldatei - ise-psc.log.

Für die clientseitige Fehlerbehebung können Sie Folgendes verwenden:

- acisensa.log - Bei Client-Fehler wird diese Datei im selben Ordner erstellt, in den die NSA heruntergeladen wurde (lädt normalerweise das Verzeichnis für Windows herunter).
- AnyConnect_ISEPosture.txt - Diese Datei befindet sich im DART-Paket im Verzeichnis Cisco AnyConnect ISE Posture Module. Alle Informationen über die ISE-PSN-Erkennung und die allgemeinen Schritte des Statusflusses werden in dieser Datei protokolliert.

Fehlerbehebung Häufige Probleme

SSO-bezogene Probleme

Bei einer erfolgreichen SSO werden diese Meldungen im ise-psc.logangegeben ist, weist diese Gruppe von Nachrichten darauf hin, dass die Sitzungssuche erfolgreich abgeschlossen wurde und die Authentifizierung im Portal übersprungen werden kann.

<#root>

```
2016-11-09 15:07:35,951 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRun
```

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.PostureRun
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRun
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRun
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRun
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRun
```

Found session c0a801010002600058232bb8 using ipAddr 10.62.145.121

Textfenster 5-1

Sie können die IP-Adresse des Endgeräts als Suchschlüssel verwenden, um diese Informationen zu finden.

Etwas später im Gastprotokoll müssen Sie feststellen, dass die Authentifizierung übersprungen wurde:

<#root>

```
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] guestaccess.flowmanager.step.cp.CPIn
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] com.cisco.ise.portalSessionManager.P
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] com.cisco.ise.portalSessionManager.P
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] guestaccess.flowmanager.step.cp.CPIn

Login step will be skipped, as the session =c0a8010100026000058232bb8 already established for mac address

2016-11-09 15:07:36,066 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cpm.guestaccess.flowmanager.processo
```

Textfenster 5-2

Falls die SSO nicht funktioniert, ise-psc log enthält Informationen über einen Sitzungssuchfehler:

<#root>

```
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cisco.cpm.posture.runtime.PostureRun

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.PostureRun
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cisco.cpm.posture.runtime.PostureRun

No Radius session found
```

Textfenster 5-3

Im guest.log In diesem Fall muss die vollständige Benutzerauthentifizierung auf dem Portal angezeigt werden:

<#root>

```
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.flowmanager.step.Ste
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.flowmanager.step.Ste
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.flowmanager.step.Ste

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.Step
```

Textfenster 5-4

Bei Authentifizierungsfehlern im Portal müssen Sie sich auf die Überprüfung der Portalkonfiguration konzentrieren. Welcher Identitätsspeicher wird verwendet? Welche Gruppen sind zur Anmeldung berechtigt?

Fehlerbehebung bei der Richtlinienauswahl für die Client-Bereitstellung

Wenn die Richtlinien für die Clientbereitstellung fehlschlagen oder die Richtlinien nicht korrekt verarbeitet werden, können Sie die guest.log für weitere Informationen:

<#root>

```
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.C

2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.common.utils.OSMappe
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.common.utils.OSMappe
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.C
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.C
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.C
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.C
2017-02-23 17:59:07,505 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.C

:user1:- CP Policy Status =SUCCESS, needToDoVlan=false, CoaAction=NO_COA
```

Textfenster 5-5

In der ersten Zeichenfolge sehen Sie, wie Informationen über die Sitzung in die Richtlinienauswahl-Engine eingespeist werden. Wenn keine oder eine falsche Richtlinienübereinstimmung vorliegt, können Sie hier Attribute mit der Konfiguration der Client-Bereitstellungsrichtlinie vergleichen. Die letzte Zeichenfolge gibt den Status der Richtlinienauswahl an.

Fehlerbehebung Statusprozess

Auf Seiten des Auftraggebers müssen Sie sich für die Untersuchung der Sonden und deren Ergebnisse interessieren. Dies ist ein Beispiel für eine erfolgreiche Phase-1-Prüfung:

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

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..

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

Textfenster 5-6

Zu diesem Zeitpunkt kehrt PSN zu AC-Informationen über den Sitzungsbesitzer zurück. Sie können die folgenden Nachrichten später sehen:

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

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..

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

Textfenster 5-7

Sitzungsbesitzer senden alle erforderlichen Informationen an den Agenten zurück:

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

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>
.

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

Textfenster 5-8

Auf der PSN-Seite können Sie sich auf diese Meldungen im guest.log Wenn Sie erwarten, dass die ursprüngliche Anforderung, die zum Knoten kommt, nicht für die Sitzung zuständig ist:

<#root>

```
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDis
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDis

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.NextGenDis

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.NextGenDis
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Provi
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Provi
2017-02-23 17:59:56,368 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDis
2017-02-23 17:59:56,369 ERROR [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Provi

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.NextGenDis
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDis
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDis

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.NextGenDis

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.Provi
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Provi
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Provi
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Provi
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Provi
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDis
```

```
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDis
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDis
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Provi
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Provi
```

Textfenster 5-9

Hier können Sie sehen, dass PSN zuerst versucht, eine Sitzung lokal zu finden, und nach einem Fehler eine Anfrage an MNT initiiert, indem die IP- und MAC-Liste verwendet wird, um den Sitzungsbesitzer zu finden.

Etwas später müssen Sie eine Anfrage vom Client auf dem richtigen PSN sehen:

<#root>

```
2017-02-23 17:59:56,790 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRunt

ooking for session using session ID: null, IP addrs: [172.16.31.12, 10.62.145.95], mac Addrs [00:0B:7F:D


2017-02-23 17:59:56,790 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRunt
2017-02-23 17:59:56,791 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRunt
2017-02-23 17:59:56,792 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRunt
2017-02-23 17:59:56,792 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRunt

Found session c0a801010009e00058af0f7b using ipAddr 172.16.31.12
```

Textfenster 5-10

Im nächsten Schritt führt PSN für diese Sitzung eine Suche nach einer Client-Bereitstellungsrichtlinie durch:

<#root>

```
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] com.cisco.cpm.swiss.SwissServer -::::
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRunt
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRunt
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRunt
2017-02-23 17:59:56,795 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 17:59:58,203 DEBUG [http-bio-10.48.30.41-8443-exec-8][] com.cisco.cpm.swiss.SwissServer -::::
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
```

Textfenster 5-11

Im nächsten Schritt sehen Sie den Prozess der Auswahl der Statusanforderungen. Am Ende des Schritts wird eine Liste der Anforderungen erstellt und an den Agenten zurückgegeben:

<#root>

2017-02-23 18:00:00,372 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureHand

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.PostureMana
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 18:00:00,432 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 18:00:00,433 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 18:00:00,433 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 18:00:03,884 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cpm.posture.runtime.agent.AgentXmlGen
2017-02-23 18:00:03,904 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cpm.posture.runtime.agent.AgentXmlGen
2017-02-23 18:00:03,904 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cpm.posture.runtime.agent.AgentXmlGen
2017-02-23 18:00:04,069 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureHand
<version>ISE: 2.2.0.470</version>
<encryption>0</encryption>
<package>
<id>10</id>

WinDefend

Enable WinDefend

3

0

3

WinDefend

3

301

WinDefend

```
      running

      (WinDefend)

 </package>
</cleanmachines>
```

Textfenster 5-12

Später können Sie sehen, dass der Statusbericht von PSN empfangen wurde:

```
2017-02-23 18:00:04,231 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureHand
2017-02-23 18:00:04,231 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureHand
```

Textfenster 5-13

Am Ende des Ablaufs markiert die ISE den Endpunkt als konform und initiiert die COA:

```
2017-02-23 18:00:04,272 INFO [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureManag
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureCoA
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureCoA
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureCoA
2017-02-23 18:00:04,273 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureCoA
2017-02-23 18:00:04,273 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureCoA
```

Textfenster 5-14

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.