Comparer le flux de redirection de position ISE au flux sans redirection de position ISE

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Débit de posture pré ISE 2.2
- Post-flux postérieur ISE 2.2
- Configurer
  - Diagramme du réseau
  - Configurations
    - Configuration du provisionnement client
    - Politiques et conditions de posture
    - Configurer le portail de provisionnement client
    - Configurer les profils et les stratégies d'autorisation
- Vérifier
- Dépannage
  - Informations générales
  - Dépanner des problèmes courants
    - Problèmes liés à SSO
    - Dépannage de la sélection de stratégie de provisionnement client
    - Dépannage du processus de posture

Introduction

Ce document décrit le flux sans redirection de posture (à partir de la version ISE 2.2) par rapport au flux de redirection de posture pris en charge par les versions ISE antérieures.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Flux de posture sur ISE
- Configuration des composants de posture sur ISE
- Configuration d'appliance de sécurité adaptatif (ASA) pour la position sur les réseaux privés virtuels (VPN)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ISE version 2.2
- Cisco ASAv avec logiciel 9.6 (2)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Ce document décrit une nouvelle fonctionnalité introduite dans Identity Service Engine (ISE) 2.2 qui permet à ISE de prendre en charge un flux de posture sans aucun type de support de redirection sur un périphérique d'accès réseau (NAD) ou ISE.

La posture est un composant essentiel de Cisco ISE. La posture en tant que composant peut être représentée par trois éléments principaux :

1. ISE en tant que distribution de la configuration des politiques et point de décision.
   Du point de vue de l'administrateur sur ISE, vous configurez des stratégies de positionnement (conditions exactes à remplir pour marquer un périphérique comme conforme à l'entreprise), des stratégies de provisionnement client (quel logiciel d'agent doit être installé sur quel type de périphériques) et des stratégies d'autorisation (à quel type d'autorisations doit être attribuée, en fonction de leur statut).
2. Périphérique d'accès réseau servant de point d'application des politiques.
   Du côté du NAD, les restrictions d'autorisation réelles sont appliquées au moment de l'authentification de l'utilisateur. ISE en tant que point de stratégie fournit des paramètres d'autorisation tels que ACL téléchargée (dACL)/VLAN/Redirect-URL/ACL (Redirect Access Control List). Traditionnellement, pour que la posture se produise, les NAD doivent prendre en charge la redirection (pour indiquer à l'utilisateur ou à l'agent logiciel quel noeud ISE doit être contacté) et le changement d'autorisation (CoA) pour réauthentifier l'utilisateur une fois que l'état de la posture du point d'extrémité est déterminé.
3. Logiciel de l'agent comme point de collecte de données et d'interaction avec l'utilisateur final.
   Cisco ISE utilise trois types de logiciels d'agent : Module de posture AnyConnect ISE, agent NAC et agent Web. L'agent reçoit des informations sur les exigences de posture de la part de l'ISE et fournit un rapport à l'ISE sur l'état des exigences.

Remarque : Ce document est basé sur Anyconnect ISE Posture Module qui est le seul qui prend entièrement en charge la posture sans redirection.

Dans la posture de flux antérieure à ISE 2.2, les NAD ne sont pas seulement utilisés pour

authentifier les utilisateurs et restreindre l'accès, mais également pour fournir des informations au logiciel de l'agent sur un noeud ISE spécifique qui doit être contacté. Dans le cadre du processus de redirection, les informations relatives au noeud ISE sont renvoyées au logiciel de l'agent.

Historiquement, la prise en charge de la redirection (du côté NAD ou ISE) était une exigence essentielle pour la mise en oeuvre de la posture. Dans ISE 2.2, l'exigence de prise en charge de la redirection est éliminée pour le processus initial de mise en service et de posture du client.

Mise en service du client sans redirection : dans ISE 2.2, vous pouvez accéder au Client Provisioning Portal (CPP) directement via le portail Fully Qualified Domain Name (FQDN). Cette méthode est similaire à celle utilisée pour accéder au portail du sponsor ou au portail MyDevice.

Processus de posture sans redirection : pendant l'installation de l'agent à partir du portail CPP, les informations sur les serveurs ISE sont enregistrées côté client, ce qui rend possible la communication directe.

Débit de posture pré ISE 2.2

Cette image montre une explication étape par étape du flux du module de posture ISE Anyconnect antérieur à ISE 2.2 :

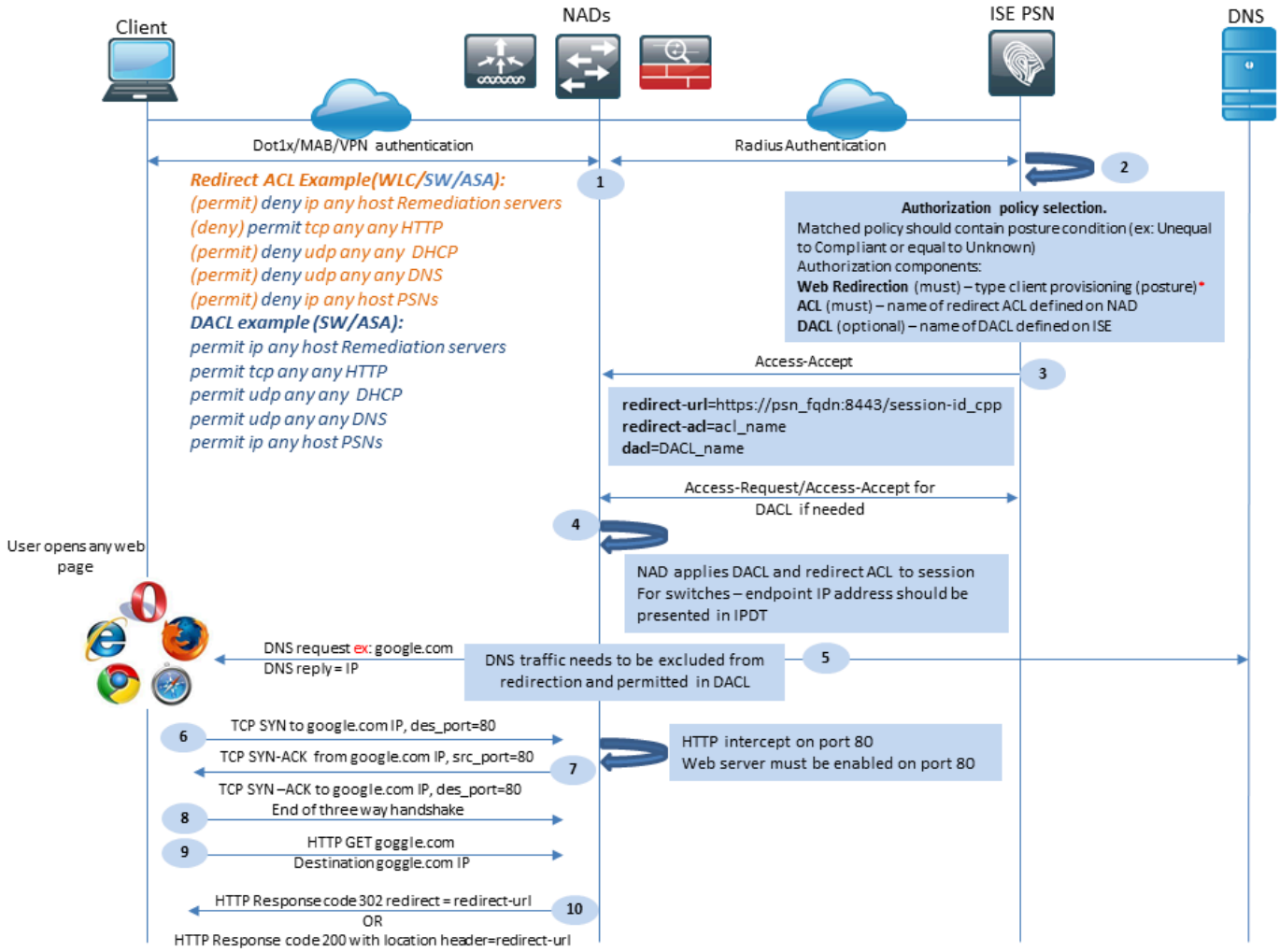


Figure 1-1

Étape 1. L’authentification est la première étape du flux, elle peut être dot1x, MAB ou VPN.

Étape 2. ISE doit choisir une stratégie d’authentification et d’autorisation pour l’utilisateur. Dans le scénario de posture, la stratégie d'autorisation choisie doit contenir une référence à l'état de posture, qui doit initialement être soit inconnu, soit non applicable. Pour couvrir ces deux cas, des conditions avec un statut de posture inégal conformité peuvent être utilisées.

Le profil d'autorisation choisi doit contenir des informations sur la redirection :

- Redirection Web : dans le cas d'une position, le type de redirection Web doit être spécifié en tant que mise en service du client (position).
- ACL : cette section doit contenir le nom de la liste de contrôle d'accès configurée côté NAD. Cette liste de contrôle d’accès est utilisée pour indiquer à NAD quel trafic doit contourner la redirection et quel trafic doit être réellement redirigé.
- DACL : il peut être utilisé avec la liste de contrôle d'accès de redirection, mais les différentes plates-formes traitent les listes de contrôle d'accès de redirection et DACL dans un ordre différent.

Par exemple, ASA traite toujours la liste de contrôle d'accès avant de la rediriger. En même temps, certaines plates-formes de commutation la traitent de la même manière qu'ASA, et d'autres plates-formes de commutation traitent d'abord la liste de contrôle d'accès Redirect, puis vérifient la liste de contrôle d'accès DACL/Interface si le trafic doit être abandonné ou autorisé.

Remarque : Après avoir activé l'option de redirection Web dans le profil d'autorisation, vous devez sélectionner le portail cible pour la redirection.

Étape 3. ISE renvoie Access-Accept avec des attributs d’autorisation. L'URL de redirection dans les attributs d'autorisation est automatiquement générée par ISE. Il contient les composants suivants :

- Nom de domaine complet du noeud ISE sur lequel l’authentification a eu lieu. Dans certains cas, le nom de domaine complet dynamique peut être remplacé par la configuration du profil d'autorisation (IP statique/nom d'hôte/nom de domaine complet) dans la section Redirection Web.

Si la valeur statique est utilisée, elle doit pointer vers le même noeud ISE où l'authentification a été traitée.

Dans le cas de l'équilibreur de charge (LB), ce nom de domaine complet peut pointer vers le VIP LB, mais uniquement dans le cas où LB est configuré pour lier des connexions Radius et SSL.

- Port : la valeur du port est obtenue à partir de la configuration du portail cible.
- ID de session : cette valeur est prise par ISE à partir de l'ID de session d'audit de paire AV Cisco présenté dans Access-Request. La valeur elle-même est générée dynamiquement par NAD.
- ID de portail : identifiant d'un portail cible côté ISE.

Étape 4. NAD applique une stratégie d'autorisation à la session. En outre, si la liste de contrôle d'accès est configurée, son contenu est demandé avant l'application des stratégies d'autorisation.

Considérations importantes :

- Tous les NAD - Le périphérique doit avoir une ACL configurée localement avec le même nom que celui reçu dans Access-Accept comme redirect-acl.
- Commutateurs : l'adresse IP du client doit être présentée dans le résultat de la commande pour`show authentication session interface details`appliquer correctement la redirection et les listes de contrôle d'accès. L'adresse IP du client est apprise par la fonctionnalité de suivi de périphérique IP (IPDT).

Étape 5. Le client envoie une requête DNS pour le nom de domaine complet qui est entré dans le navigateur Web. À ce stade, le trafic DNS doit contourner la redirection et l'adresse IP correcte doit être renvoyée par le serveur DNS.

Étape 6. Le client envoie TCP SYN à l'adresse IP qui est reçue dans la réponse DNS. L'adresse IP source du paquet est l'adresse IP du client et l'adresse IP de destination est l'adresse IP de la ressource demandée. Le port de destination est égal à 80, sauf dans les cas où un proxy HTTP direct est configuré dans le navigateur Web du client.

Étape 7.NAD intercepte les requêtes du client et prépare les paquets SYN-ACK avec une adresse IP source égale à l'adresse IP de ressource demandée, une adresse IP de destination égale à l'adresse IP du client et un port source égal à 80.

Considérations importantes :

- Les NAD doivent avoir un serveur HTTP exécuté sur le port sur lequel le client envoie des requêtes. Par défaut, il s'agit du port 80.
- Si le client utilise un serveur Web proxy HTTP direct, le serveur HTTP doit s'exécuter sur le port proxy du NAS. Ce scénario sort du cadre de ce document.
- Dans les cas où NAD n'a pas d'adresse IP locale dans le client, le sous-réseau SYN-ACK est envoyé avec la table de routage NAD (sur l'interface de gestion généralement).

Dans ce scénario, le paquet est routé sur l'infrastructure de couche 3 et doit être redirigé vers le client par un périphérique en amont de couche 3.

Si le périphérique L3 est un pare-feu avec état, une exception supplémentaire doit être fournie pour ce type de routage asymétrique.

Étape 8. Le client termine la connexion TCP en trois étapes par ACK.

Étape 9. HTTP GET pour la ressource cible est envoyé par un client.

Étape 10. NAD renvoie une URL de redirection au client avec le code HTTP 302 (page déplacée), sur certains NAD, la redirection peut être retournée à l'intérieur du message HTTP 200 OK dans

l'en-tête de l'emplacement.

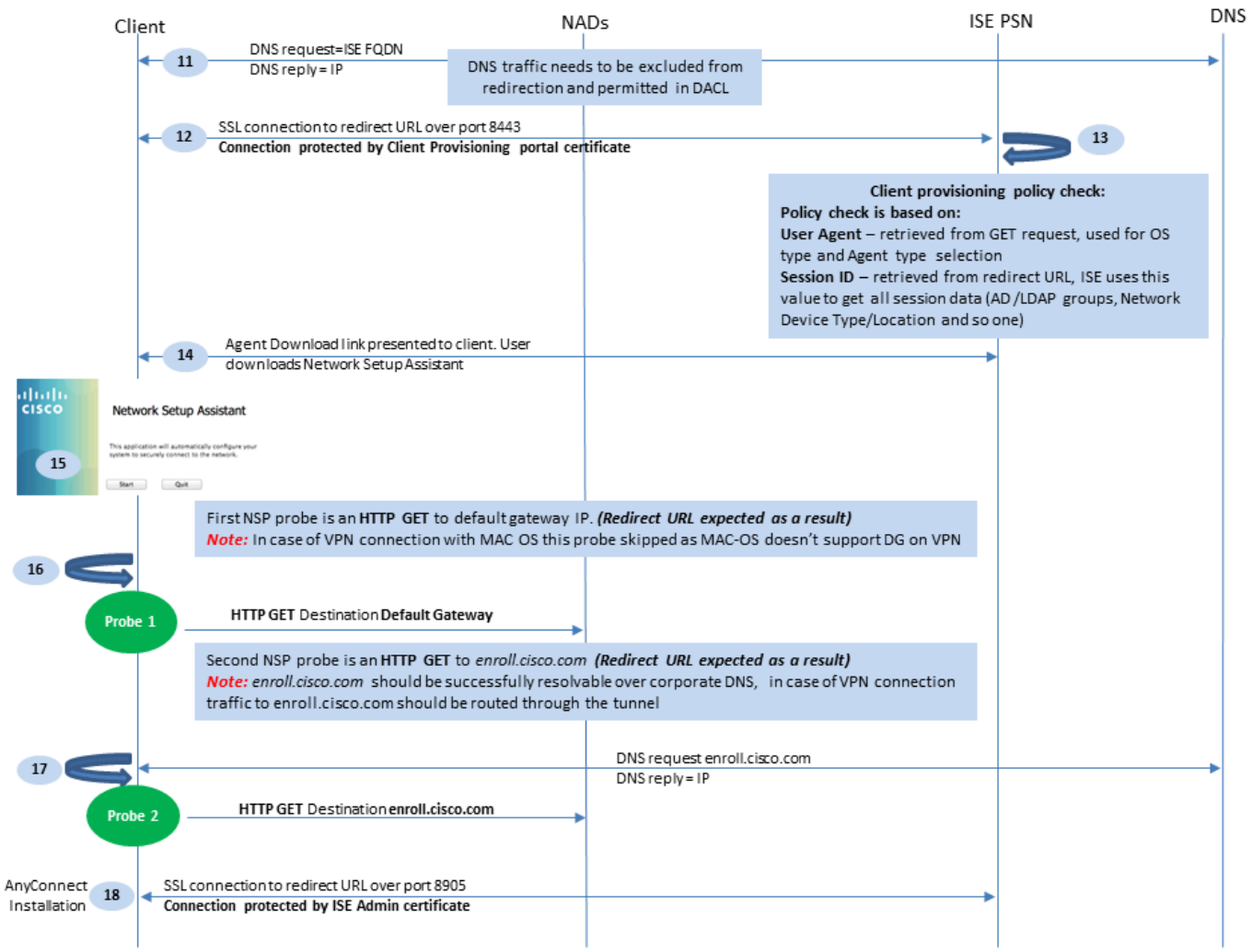


Figure 1-2

Étape 11. Le client envoie une requête DNS pour le nom de domaine complet à partir de l'URL de redirection. Le nom de domaine complet doit pouvoir être résolu côté serveur DNS.

Étape 12. La connexion SSL sur le port reçu dans l'URL de redirection est établie (8443 par défaut). Cette connexion est protégée par un certificat de portail côté ISE. Client Provisioning Portal (CPP) est présenté à l'utilisateur.

Étape 13.Avant de fournir une option de téléchargement au client, ISE doit sélectionner la stratégie de mise en service du client cible (CP). Le système d'exploitation (OS) du client détecté à partir de l'agent utilisateur du navigateur et d'autres informations requises pour la sélection de la stratégie CPP sont récupérés à partir de la session d'authentification (comme les groupes AD/LDAP, etc.). ISE connaît la session cible à partir de l'ID de session présenté dans l'URL de redirection.

Étape 14. Le lien de téléchargement de l'Assistant de configuration réseau (NSA) est renvoyé au client. Le client télécharge l'application.

Remarque : Normalement, vous pouvez voir NSA comme partie du flux BYOD pour Windows et Android, mais aussi cette application peut être utilisée pour installer Anyconnect ou ses composants à partir d'ISE.

Étape 15. L'utilisateur exécute l'application NSA.

Étape 16. NSA envoie la première sonde de détection - HTTP /auth/discovery à la passerelle par défaut. La NSA attend la redirection-url en conséquence.

Remarque : Pour les connexions sur VPN sur des périphériques MAC OS, cette sonde est ignorée car MAC OS n'a pas de passerelle par défaut sur l'adaptateur VPN.

Étape 17.NSA envoie une seconde sonde si la première échoue. La deuxième sonde est une HTTP GET /auth/discovery to`enroll.cisco.com`. Ce nom de domaine complet doit pouvoir être résolu par le serveur DNS. Dans un scénario VPN avec un tunnel partagé, le trafic vers`enroll.cisco.com`doit être acheminé via le tunnel.

Étape 18. Si l'une des sondes réussit, NSA établit une connexion SSL sur le port 8905 avec les informations obtenues à partir de redirect-url. Cette connexion est protégée par le certificat d'administration ISE. Au sein de cette connexion, NSA télécharge Anyconnect.

Considérations importantes :

- Avant la version ISE 2.2, la communication SSL sur le port 8905 est requise pour la posture.
- Pour éviter les avertissements de certificat, les certificats du portail et d'administration doivent être approuvés côté client.
- `ip host`Dans les déploiements ISE multi-interfaces, les interfaces autres que G0 peuvent être liées au nom de domaine complet différemment du nom de domaine complet du système (à l'aide de la commande CLI). Cela peut entraîner des problèmes avec la validation Nom de sujet (SN)/Autre nom de sujet (SAN). Par exemple, si le client est redirigé vers le nom de domaine complet à partir de l'interface G1, le nom de domaine complet du système peut être différent du nom de domaine complet de l'URL de redirection du certificat de communication 8905. Pour résoudre ce scénario, vous pouvez ajouter des noms de domaine complets d'interfaces supplémentaires dans les champs SAN du certificat d'administration ou utiliser un caractère générique dans le certificat d'administration.

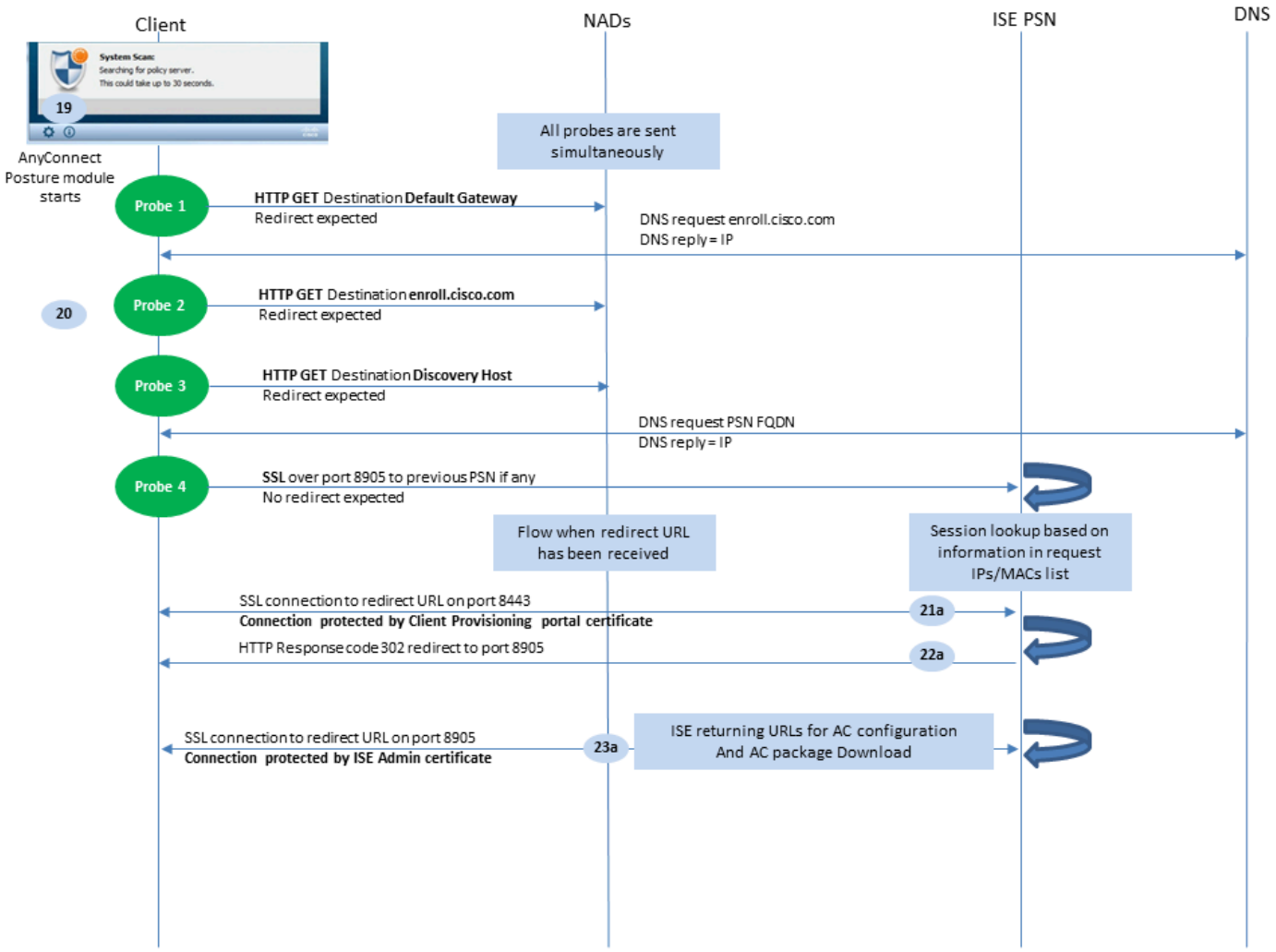


Figure 1-3

Étape 19. Lancement du processus de positionnement d'Anyconnect ISE

Le module Anyconnect ISE Posture démarre dans l'une des situations suivantes :

- Après l'installation
- Après la modification de la valeur de passerelle par défaut
- Après l'événement de connexion utilisateur système
- Après l'événement d'alimentation du système

Étape 20. À ce stade, Anyconnect ISE Posture Module lance la détection du serveur de stratégies. Pour ce faire, une série de sondes sont envoyées en même temps par le module Anyconnect ISE Posture.

- Sonde 1 - HTTP get /auth/discovery to default gateway IP. Supposons que les périphériques MAC OS ne disposent pas d'une passerelle par défaut sur l'adaptateur VPN. Le résultat attendu pour la sonde est redirect-url.
- Sonde 2 - HTTP GET /auth/discovery to`enroll.cisco.com`. Ce nom de domaine complet doit pouvoir être résolu par le serveur DNS. Dans un scénario VPN avec un tunnel partagé, le trafic vers`enroll.cisco.com`doit être acheminé via le tunnel. Le résultat attendu pour la sonde est redirect-url.

- Sonde 3 : HTTP get /auth/discovery to discovery host. La valeur d'hôte Discovery est renvoyée par ISE lors de l'installation dans le profil de position AC. Le résultat attendu pour la sonde est redirect-url.
- Sonde 4 : HTTP GET /auth/status sur SSL sur le port 8905 vers PSN précédemment connecté. Cette demande contient des informations sur la liste des adresses IP et MAC du client pour la recherche de session côté ISE. Ce problème n'est pas présenté lors de la première tentative de posture. La connexion est protégée par un certificat d'administration ISE. Suite à cette analyse, ISE peut renvoyer l'ID de session au client si le noeud où l'analyse a atterri est le même que celui où l'utilisateur a été authentifié.

Remarque : Grâce à cette sonde, la posture peut être effectuée avec succès même sans redirection de travail dans certaines circonstances. Une position réussie sans redirection nécessite que le PSN actuel qui a authentifié la session soit le même que le PSN précédemment connecté avec succès. Gardez à l'esprit qu'avant ISE 2.2, une posture réussie sans redirection est plus une exception qu'une règle.

Les étapes suivantes décrivent le processus de posture dans le cas où l'URL de redirection est reçue (flux marqué avec la lettre a) à la suite de l'une des sondes.

Étape 21. Le module Anyconnect ISE Posture établit une connexion au portail d’approvisionnement du client à l’aide d’une URL récupérée pendant la phase de détection. À ce stade, ISE procède à nouveau à la validation de la stratégie de provisionnement du client en utilisant les informations des sessions authentifiées.

Étape 22.Si la stratégie de mise en service du client est détectée, ISE renvoie la redirection vers le port 8905.

Étape 23. L’agent établit une connexion à ISE sur le port 8905. Pendant cette connexion, ISE renvoie des URL pour le profil de position, le module de conformité et les mises à jour anyconnect.

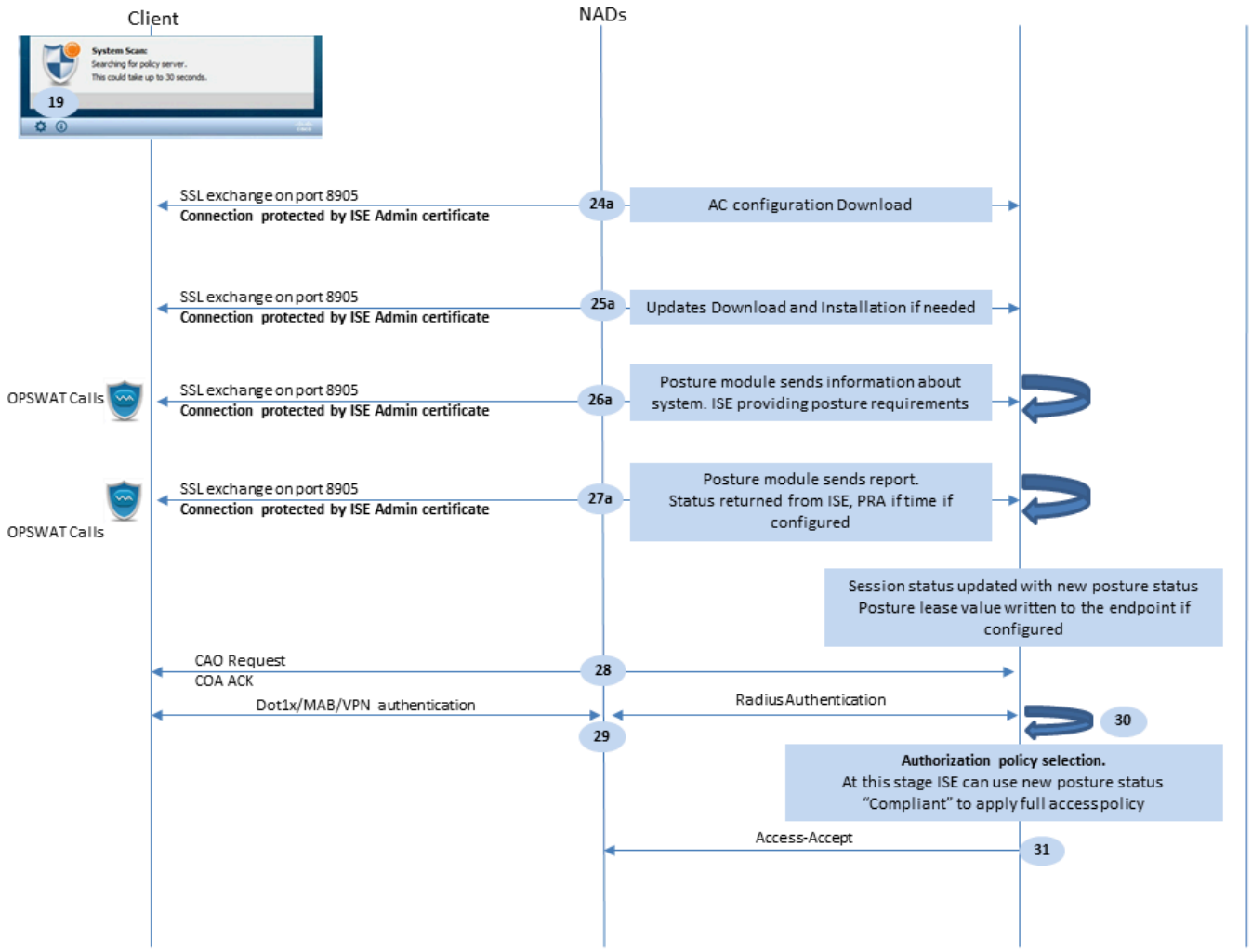


Figure 1-4

Étape 24.Téléchargement de la configuration du module de posture ISE AC depuis ISE.

Étape 25. Mise à jour du téléchargement et de l'installation si nécessaire.

Étape 26. Le module AC ISE Posture collecte les informations initiales sur le système (comme la version du système d'exploitation, les produits de sécurité installés et leur version de définition). À ce stade, le module de posture d'AC ISE fait appel à l'API OPSWAT pour collecter des informations sur les produits de sécurité. Les données collectées sont envoyées à ISE. En réponse à cette demande, ISE fournit une liste des exigences de posture. La liste des exigences est sélectionnée à la suite du traitement de la stratégie de posture. Pour faire correspondre la stratégie correcte, ISE utilise la version du système d'exploitation du périphérique (présente dans la demande) et la valeur de l'ID de session pour sélectionner d'autres attributs requis (groupes AD/LDAP). La valeur de l'ID de session est également envoyée par le client.

Étape 27. À cette étape, le client fait appel à des appels OPSWAT et à d'autres mécanismes pour vérifier les exigences de posture. Le rapport final avec la liste des exigences et leur état est envoyé à ISE. ISE doit prendre la décision finale concernant l'état de conformité du point de terminaison. Si le point de terminaison est marqué comme non conforme à cette étape, un ensemble d'actions correctives est retourné. Pour le point de terminaison conforme, ISE écrit l'état de conformité dans la session et place également le dernier horodatage de position sur les

attributs du point de terminaison si le bail de position est configuré. Le résultat de la position est renvoyé au point d'extrémité. Dans le cas de la réévaluation de la position (PRA), le temps de PRA est également placé par ISE dans ce paquet.

Dans un scénario de non-conformité, tenez compte des points suivants :

- Certaines actions de conversion (comme les messages texte affichés, la conversion de lien, la conversion de fichier, etc.) sont exécutées par l'agent de posture lui-même.
- D'autres types de conversion (comme AV. AS, WSUS et SCCM) nécessitent une communication API OPSWAT entre l'agent de posture et le produit cible. Dans ce scénario, l'agent se contente d'envoyer une demande de résolution au produit. La correction proprement dite est effectuée directement par les produits de sécurité.

Remarque : Dans le cas où le produit de sécurité doit communiquer avec des ressources externes (serveurs de mise à jour internes/externes), vous devez vous assurer que cette communication est autorisée dans Redirect-ACL/DACL.

Étape 28.ISE envoie une demande de certificat d’authenticité au NAD qui doit déclencher une nouvelle authentification pour l’utilisateur. Le NAD doit confirmer cette demande par la fonction ACK du certificat d’authenticité. Gardez à l'esprit que pour les cas VPN, la diffusion de certificat d'authenticité est utilisée, de sorte qu'aucune nouvelle demande d'authentification n'est envoyée. Au lieu de cela, ASA supprime les paramètres d'autorisation précédents (URL de redirection, ACL de redirection et DACL) de la session et applique de nouveaux paramètres à partir de la demande de certificat d'authenticité.

Étape 29.Nouvelle demande d’authentification de l’utilisateur.

Considérations importantes :

- En général, pour le certificat d'authenticité Cisco NAD, REAUTH est utilisé par ISE, ce qui indique à NAD d'initier une nouvelle demande d'authentification avec l'ID de session précédent.
- Du côté de l'ISE, la même valeur d'ID de session indique que les attributs de session précédemment collectés doivent être réutilisés (état de réclamation dans notre cas) et qu'un nouveau profil d'autorisation basé sur ces attributs doit être attribué.
- En cas de changement d'ID de session, cette connexion est traitée comme nouvelle et le processus complet de positionnement est redémarré.
- Afin d'éviter une nouvelle posture à chaque changement d'ID de session, un bail de posture peut être utilisé. Dans ce scénario, les informations sur l'état de la position sont stockées dans les attributs de point de terminaison qui restent sur l'ISE même si l'ID de session est modifié.

Étape 30. Une nouvelle stratégie d’autorisation est sélectionnée côté ISE en fonction de l’état de la position.

Étape 31. Access-Accept avec de nouveaux attributs d'autorisation est envoyé au NAD.

Le flux suivant décrit le scénario où l'URL de redirection n'est pas récupérée (marquée par la lettre b) par une sonde de position et où le PSN précédemment connecté a été interrogé par la dernière sonde. Toutes les étapes ici sont exactement les mêmes que dans le cas de l'URL de redirection à l'exception de la relecture qui est retournée par PSN suite à la Sonde 4. Si cette sonde a atterri sur le même PSN qui est un propriétaire pour la session d'authentification en cours, la relecture contient la valeur d'ID de session qui est plus tard utilisée par l'agent de posture pour terminer le processus. Dans le cas où la tête de réseau précédemment connectée n'est pas la même que le propriétaire de la session actuelle, la recherche de session échoue et une réponse vide est renvoyée au module de posture ISE CA. En conséquence, le message est`No Policy Server Detected`renvoyé à l'utilisateur final.

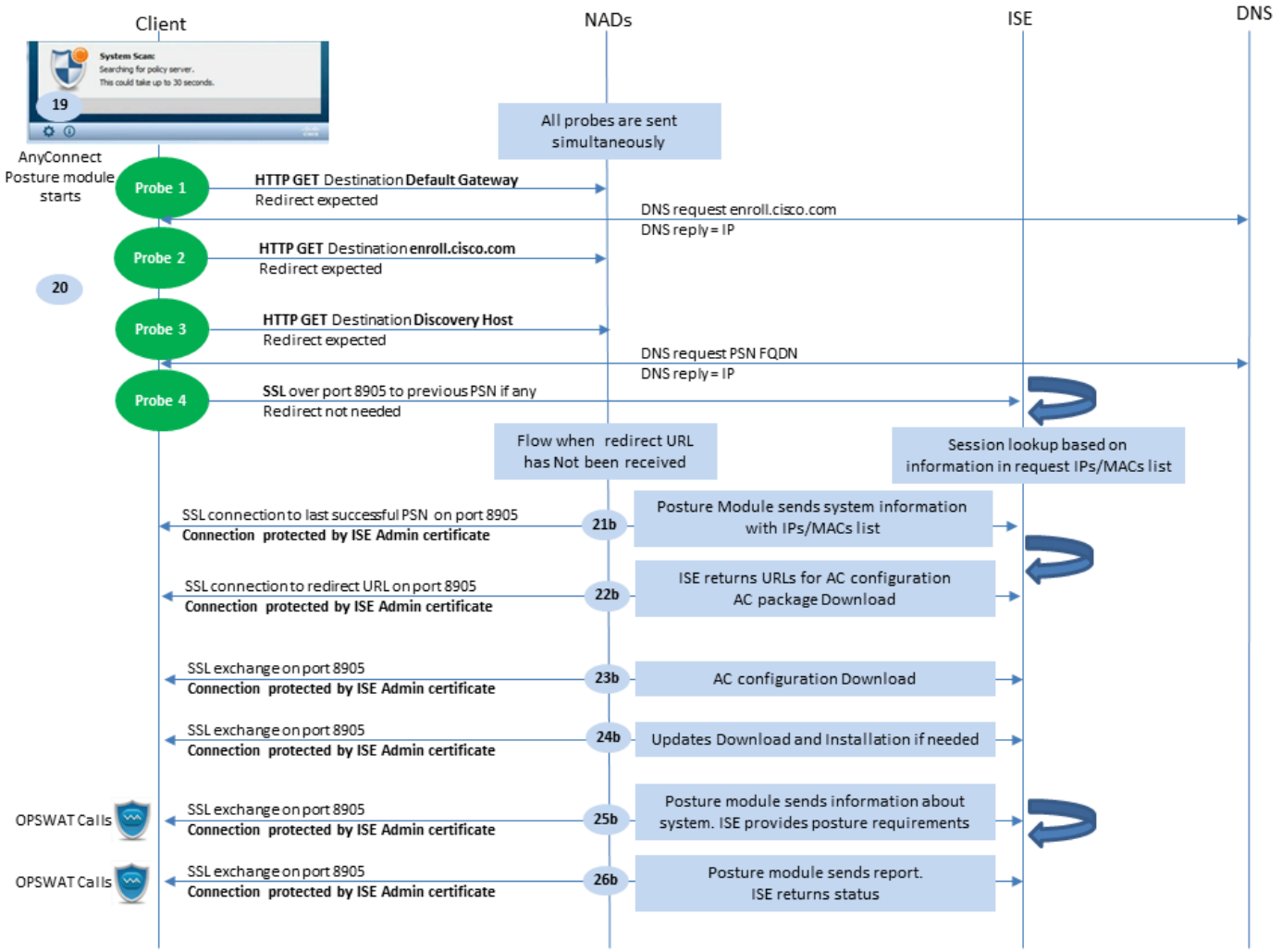


Figure 1-5

Post-flux postérieur ISE 2.2

ISE 2.2 et les versions ultérieures prennent en charge simultanément les flux de redirection et les

flux sans redirection. Voici l'explication détaillée du flux de posture sans redirection :

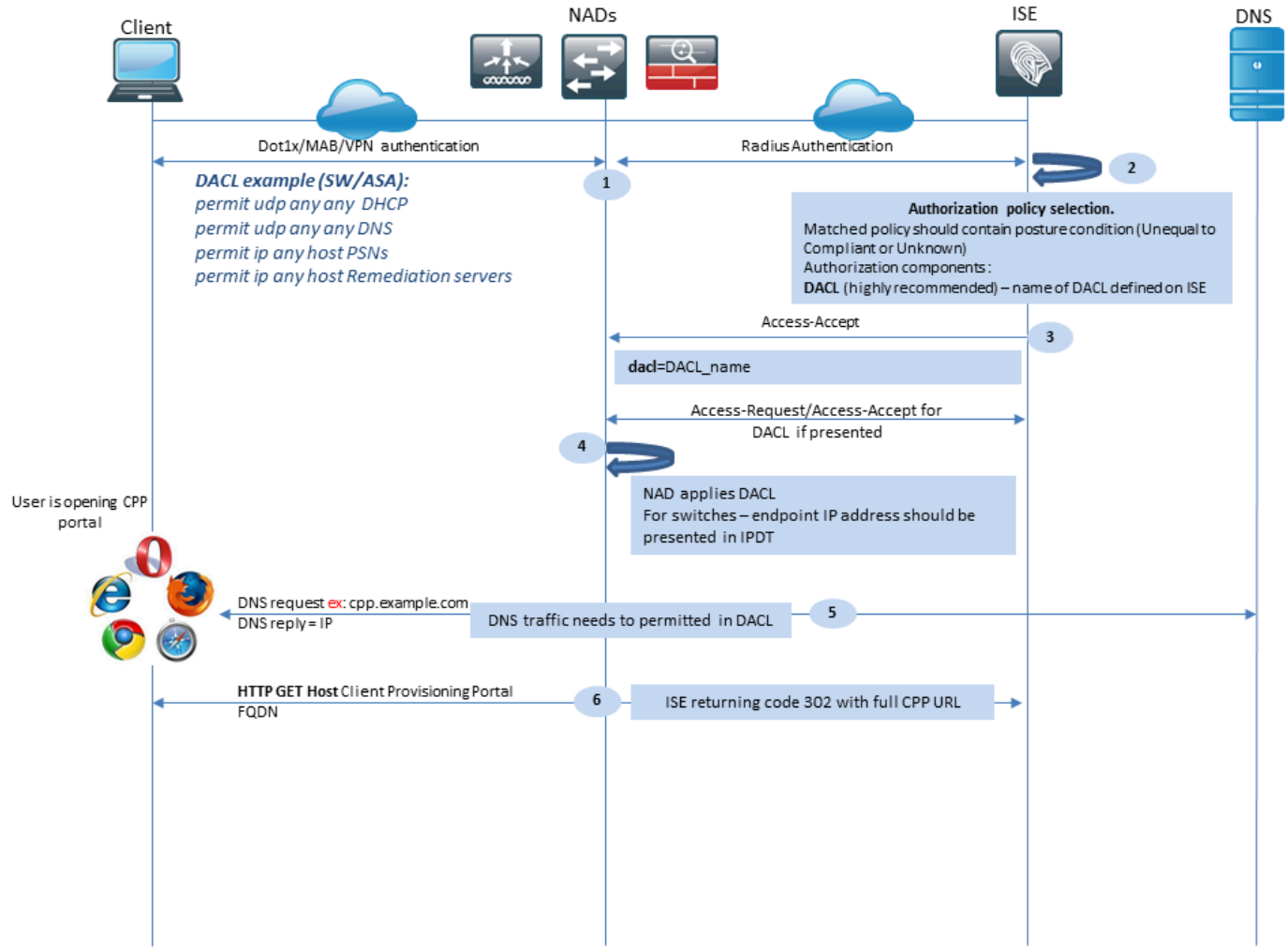


Figure 2-1

Étape 1.L'authentification est la première étape du flux. Il peut s'agir de dot1x, MAB ou VPN.

Étape 2.ISE doit choisir la stratégie d'authentification et d'autorisation de l'utilisateur. Dans la position, la stratégie d'autorisation du scénario choisi doit contenir une référence à l'état de la position, qui doit initialement être soit inconnu, soit non applicable. Pour couvrir ces deux cas, il est possible d'utiliser des conditions avec un statut de conformité inégal. Pour une posture sans redirection, il n'est pas nécessaire d'utiliser une configuration de redirection Web dans le profil d'autorisation. Vous pouvez toujours envisager l'utilisation d'une DACL ou d'une ACL d'espace aérien pour limiter l'accès des utilisateurs au stade où l'état de position n'est pas disponible.

Étape 3.ISE renvoie Access-Accept avec des attributs d'autorisation.

Étape 4. Si le nom de la liste de contrôle d'accès est renvoyé dans Access-Accept, NAD lance le téléchargement du contenu de la liste de contrôle d'accès et applique le profil d'autorisation à la session après l'avoir obtenue.

Étape 5. La nouvelle approche suppose que la redirection n'est pas possible. L'utilisateur doit donc entrer manuellement le nom de domaine complet du portail d'approvisionnement du client.

Le nom de domaine complet du portail CPP doit être défini dans la configuration du portail côté ISE. Du point de vue du serveur DNS, l'enregistrement A doit pointer vers le serveur ISE avec le rôle PSN activé.

Étape 6. Le client envoie HTTP pour accéder au nom de domaine complet du portail d'approvisionnement du client, cette demande est analysée côté ISE et l'URL complète du portail est renvoyée au client.

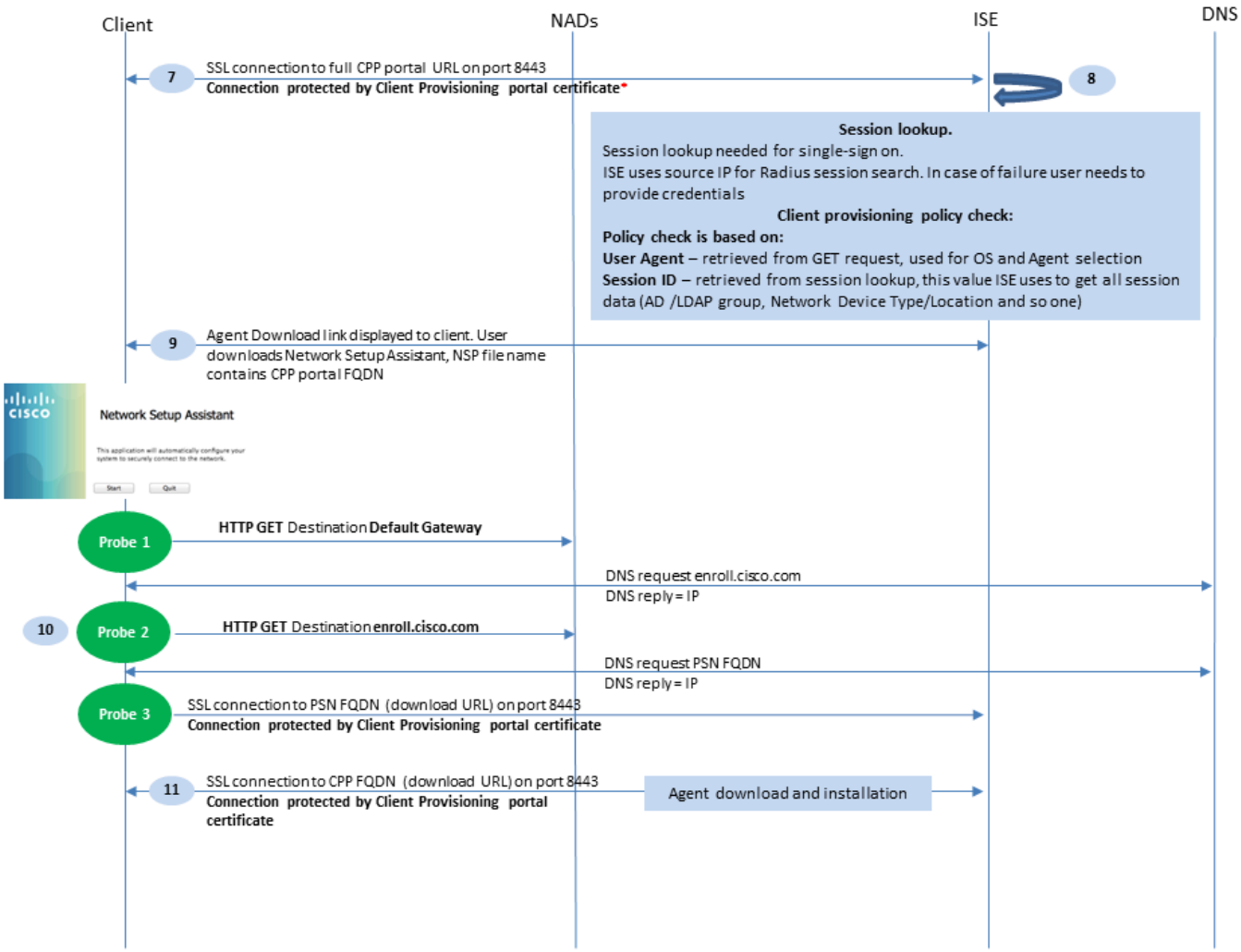


Figure 2-2

Étape 7.La connexion SSL sur le port reçu dans l'URL de redirection est établie (8443 par défaut). Cette connexion est protégée par un certificat de portail côté ISE. Le portail d'approvisionnement client (CPP) est présenté à l'utilisateur.

Étape 8. À cette étape, deux événements se produisent sur ISE :

- Authentification unique (SSO) - ISE tente de rechercher les authentifications précédentes réussies. ISE utilise l'adresse IP source du paquet comme filtre de recherche pour les sessions RADIUS actives.

Remarque : La session est récupérée en fonction d'une correspondance entre l'adresse IP source dans le paquet et l'adresse IP tramée dans la session. L'adresse IP tramée est normalement récupérée par ISE à partir des mises à jour de comptabilité intermédiaires. Il est donc nécessaire d'activer la comptabilité du côté NAD. De plus, vous devez vous rappeler que l'authentification unique n'est possible que sur le noeud propriétaire de la session. Si, par exemple, la session est authentifiée sur PSN1, mais que le nom de domaine complet lui-même pointe vers PSN2, le mécanisme SSO échoue.

- Recherche de stratégie d'approvisionnement du client : en cas d'authentification unique réussie, ISE peut utiliser les données de la session authentifiée et de l'agent utilisateur à partir du navigateur du client. En cas d'échec de l'authentification unique, l'utilisateur doit fournir des informations d'identification et, une fois les informations d'authentification de l'utilisateur récupérées des magasins d'identités internes et externes (AD/LDAP/groupes internes), elles peuvent être utilisées pour la vérification de la stratégie d'approvisionnement du client.

Remarque : En raison de l'ID de bogue Cisco CSCvd1574, vous pouvez voir une erreur au moment de la sélection de la stratégie d'approvisionnement du client pour les cas de non-SSO lorsque l'utilisateur externe est membre de plusieurs groupes AD/LDAP ajoutés dans la configuration du magasin d'identités externe. Le défaut mentionné est réparé qui commence par ISE 2.3 FCS et le correctif nécessite l'utilisation de CONTAINS dans une condition avec groupe AD au lieu de EQUAL.

Étape 9. Après la sélection de la stratégie d'approvisionnement du client, ISE affiche l'URL de téléchargement de l'agent pour l'utilisateur. Après avoir cliqué sur télécharger NSA, l'application est envoyée à l'utilisateur. Le nom de fichier NSA contient le nom de domaine complet du portail CPP.

Étape 10.À cette étape, NSA exécute des sondes pour établir une connexion à l'ISE. Deux sondes sont classiques et la troisième est conçue pour permettre la découverte ISE dans des environnements sans redirection d'URL.

- NSA envoie la première sonde de détection - HTTP /auth/discovery à la passerelle par défaut. La NSA attend la redirection-url en conséquence.
- La NSA envoie une seconde sonde si la première échoue. La deuxième sonde est une HTTP GET /auth/discovery to enroll.cisco.com. Ce nom de domaine complet doit pouvoir être résolu par le serveur DNS. Dans un scénario VPN avec un tunnel partagé, le trafic vers enroll.cisco.com doit être acheminé via le tunnel.
- NSA envoie la troisième sonde sur le port du portail CPP au FQDN du portail d'approvisionnement du client. Cette demande contient des informations sur l'ID de session du portail qui permet à ISE d'identifier les ressources qui doivent être fournies.

Étape 1. NSA télécharge Anyconnect et/ou des modules spécifiques. Le processus de téléchargement est effectué sur le port du portail de mise en service du client.

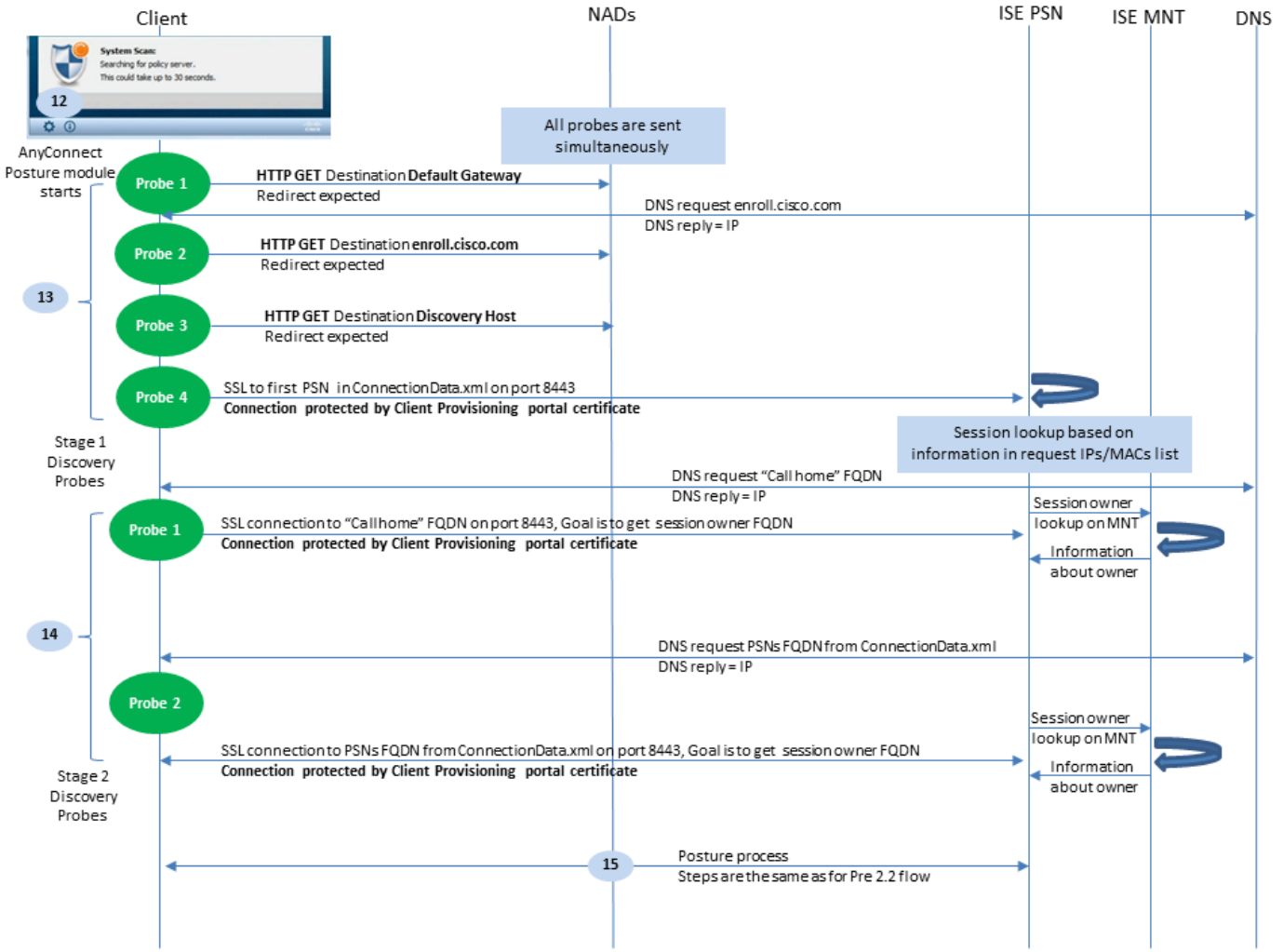


Figure 2-3

Étape 12. Dans ISE 2.2, le processus de posture est divisé en deux étapes. La première étape contient un ensemble de sondes de détection de position traditionnelles pour prendre en charge la rétrocompatibilité avec les déploiements qui reposent sur la redirection d'URL.

Étape 13. La première étape contient toutes les sondes traditionnelles de découverte de posture. Pour obtenir plus de détails sur les sondes, reportez-vous à l'étape 20. du flux de posture antérieur à ISE 2.2.

Étape 14.L'étape 2 contient deux sondes de détection qui permettent au module de posture ISE AC d'établir une connexion au PSN où la session est authentifiée dans des environnements où la redirection n'est pas prise en charge. Au cours de l'étape 2, toutes les sondes sont séquentielles.

- Sonde 1 : au cours de la première sonde, le module de posture ISE AC tente de s'établir avec des adresses IP/FQDN de la liste Call Home. La liste des cibles de la sonde doit être configurée dans le profil de position CA du côté ISE. Vous pouvez définir des adresses IP/noms de domaine complets séparés par des virgules, avec deux-points, vous pouvez définir le numéro de port pour chaque destination Call Home. Ce port doit être égal au port sur lequel le portail d'approvisionnement du client s'exécute. Du côté client, les informations sur les serveurs d'appel à distance se trouvent dansISEPostureCFG.xml, ce fichier se trouve dans le dossier -C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture\.

Si la cible call home n'est pas propriétaire de la session, une recherche du propriétaire est nécessaire à ce stade. Le module AC ISE Posture indique à ISE de lancer la recherche de propriétaire à l'aide d'une URL cible spéciale - /auth/ng-discoveryrequest. Elle contient également la liste des adresses IP et MAC du client. Une fois ce message reçu par la session PSN, une recherche est d'abord effectuée localement (cette recherche utilise à la fois les adresses IP et les adresses MAC de la requête envoyée par le module de posture ISE AC). Si la session est introuvable, PSN lance une requête de noeud MNT. Cette requête ne contient que la liste des adresses MAC. Par conséquent, le nom de domaine complet du propriétaire doit être obtenu auprès du MNT. Après cela, PSN renvoie le nom de domaine complet du propriétaire au client. La demande suivante du client est envoyée au nom de domaine complet du propriétaire de la session avec l'état/l'authentification dans l'URL et la liste des adresses IP et MAC.

- Sonde 2 : à ce stade, le module de posture ISE AC essaie les FQDN PSN qui se trouvent dansConnectionData.xml. Vous pouvez trouver ce fichier dansC:\Users\

  \AppData\Local\Cisco\Cisco AnyConnect Secure Mobility Client\

  . Le module de posture ISE AC crée ce fichier après la première tentative de posture. Le fichier contient une liste des noms de domaine complets des PSN ISE. Le contenu de la liste peut être mis à jour dynamiquement lors des prochaines tentatives de connexion. L'objectif final de cette sonde est d'obtenir le nom de domaine complet (FQDN) du propriétaire de session actuel. L'implémentation est identique à celle de la sonde 1, avec la seule différence dans la sélection de la destination de la sonde.
  Le fichier lui-même se trouve dans le dossier de l'utilisateur actuel au cas où le périphérique serait utilisé par plusieurs utilisateurs. Un autre utilisateur ne peut pas utiliser les informations de ce fichier. Cela peut conduire les utilisateurs à la poule et l'oeuf problème dans les environnements sans redirection lorsque Call Home cibles ne sont pas spécifiées.

Étape 15. Une fois les informations relatives au propriétaire de la session obtenues, toutes les étapes suivantes sont identiques au flux antérieur à ISE 2.2.

Configurer

Pour ce document, ASAv est utilisé comme périphérique d'accès réseau. Tous les tests sont effectués avec la posture sur VPN. La configuration ASA pour la prise en charge de la position sur VPN est en dehors de la portée du document. Pour plus de détails, référez-vous à Exemple de configuration d'ASA version 9.2.1 VPN Posture with ISE.

Remarque : Pour le déploiement avec des utilisateurs VPN, le paramètre recommandé est la position basée sur la redirection. La configuration de callhomelist n'est pas recommandée. Pour tous les utilisateurs non basés sur un VPN, assurez-vous que la liste DACL est appliquée de sorte qu'ils ne parlent pas à PSN où la position est configurée.

Diagramme du réseau

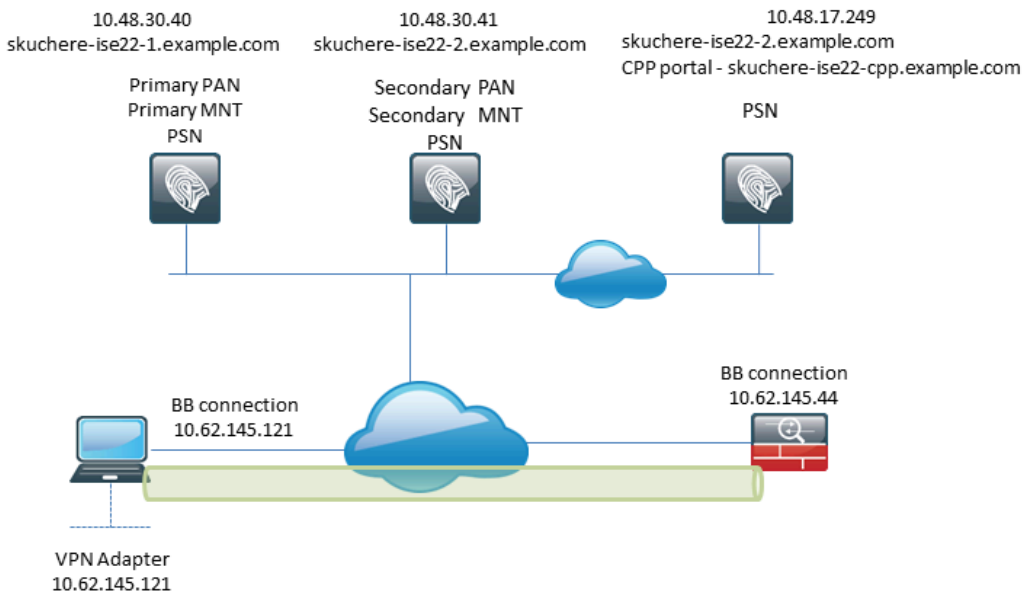


Figure 3-1

Cette topologie est utilisée dans les tests. Avec ASA, il est possible de simuler facilement le scénario lorsque le mécanisme SSO pour le portail d'approvisionnement de client échoue du côté PSN, en raison de la fonctionnalité NAT. Dans le cas d'un flux de posture régulier sur VPN, l'authentification unique doit fonctionner correctement car la fonction NAT n'est normalement pas appliquée pour les adresses IP VPN lorsque les utilisateurs entrent dans le réseau d'entreprise.

Configurations

Configuration du provisionnement client

Voici les étapes à suivre pour préparer la configuration Anyconnect.

Étape 1. Téléchargement du package Anyconnect Le package Anyconnect lui-même n'est pas disponible en téléchargement direct à partir d'ISE. Avant de commencer, assurez-vous qu'AC est disponible sur votre PC. Ce lien peut être utilisé pour le téléchargement AC - https://www.cisco.com/site/us/en/products/security/secure-client/index.html. Dans ce document, le paquet,anyconnect-win-4.4.00243-webdeploy-k9.pkgest utilisé.

Étape 2. Afin de télécharger le package AC vers ISE, accédez àPolicy > Policy Elements > Results > Client Provisioning > Resourceset cliquez surAdd. Sélectionnez les ressources Agent sur le disque local. Dans la nouvelle fenêtre, choisissezCisco Provided Packages, cliquez surbrowseet choisissez le package AC sur votre PC.

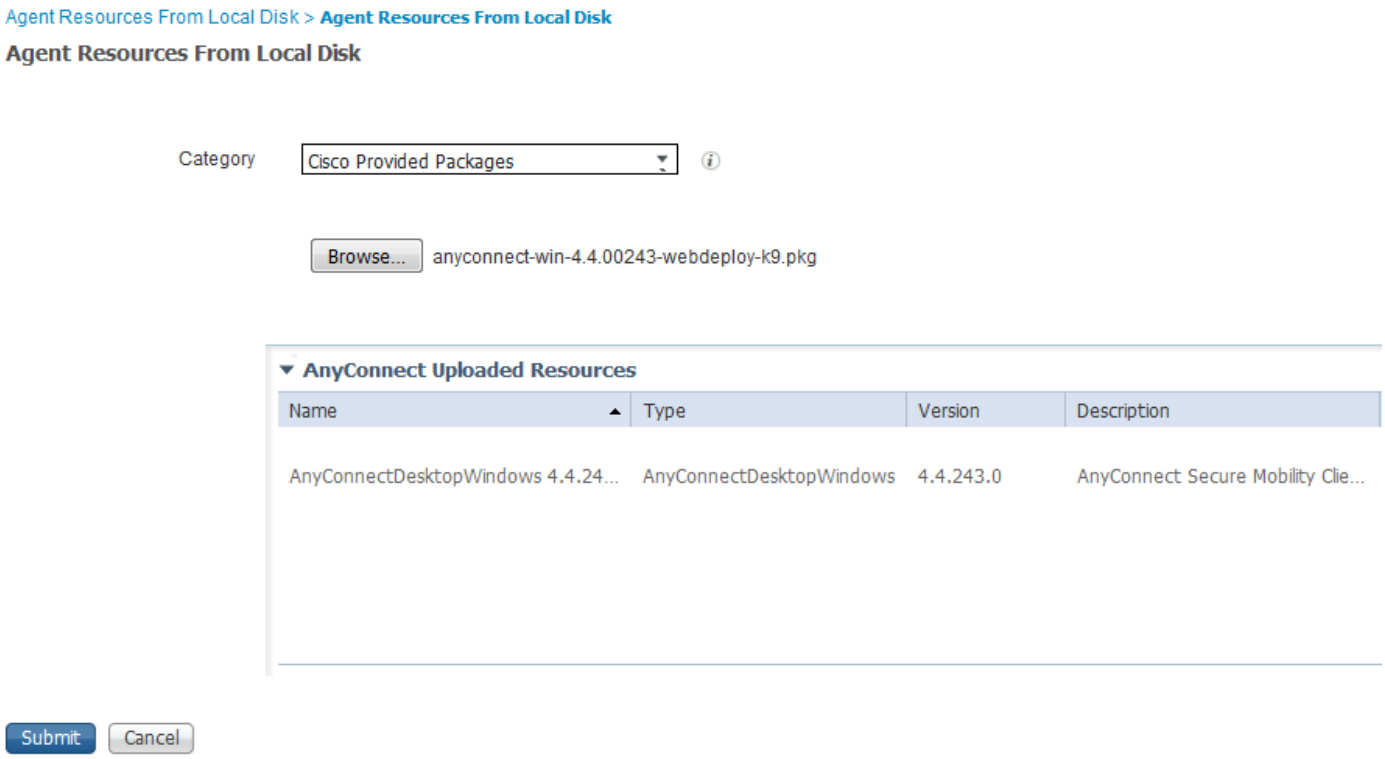


Figure 3-2

Cliquez surSubmitpour terminer l'importation.

Étape 3. Le module de conformité doit être téléchargé vers ISE. Sur la même page, cliquez surAddet choisissez leAgent resources from Cisco site. Dans la liste des ressources, vous devez vérifier un module de conformité. Pour ce document, la AnyConnectComplianceModuleWindows 4.2.508.0 le module de conformité est utilisé.

Étape 4. Maintenant, le profil de posture AC doit être créé. Cliquez surAddet sélectionnez leNAC agent or Anyconnect posture profile.

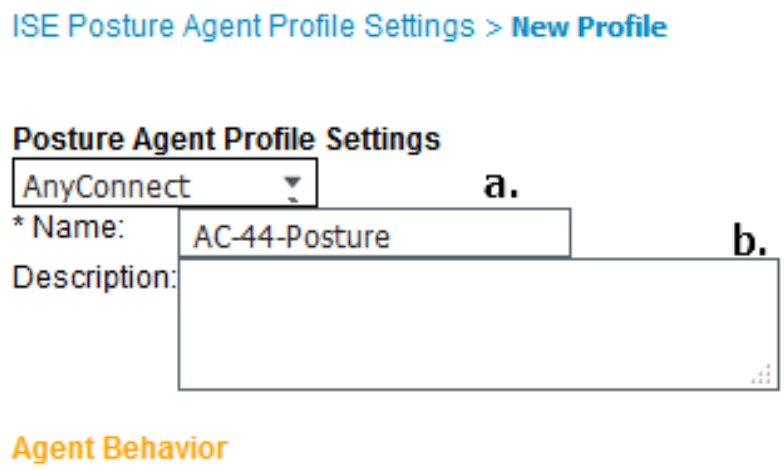


Figure 3-3

- Sélectionnez le type de profil. AnyConnect doit être utilisé pour ce scénario.

- Spécifiez le nom du profil. Accédez à la sectionPosture Protocoldu profil.

Posture Protocol

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

Figure 3-4

- Spécifiez leServer Name Rules, ce champ ne peut pas être vide. Le champ peut contenir un nom de domaine complet avec un caractère générique qui restreint la connexion du module de posture ISE AC aux PSN à partir de l'espace de noms approprié. Placez une étoile si un nom de domaine complet doit être autorisé.
- Les noms et les adresses IP spécifiés ici sont utilisés lors de l'étape 2 de la détection de position. Vous pouvez séparer les noms par des virgules et les numéros de port peuvent être ajoutés après FQDN/IP à l'aide des deux-points. Dans le cas où l'AC déployée hors bande (pas à partir du portail d'approvisionnement du client ISE) avec l'utilisation de l'objet de stratégie de groupe ou de tout autre système d'approvisionnement de logiciel, la présence d'adresses Call Home devient essentielle car il ne s'agit que d'une seule sonde qui peut atteindre le PSN ISE avec succès. Cela signifie que dans le cas d'une mise en service CA hors bande, l'administrateur doit créer un profil de position ISE CA à l'aide de l'éditeur de profil CA et mettre en service ce fichier avec l'installation CA.

Remarque : Gardez à l'esprit que la présence d'adresses Call Home est essentielle pour les PC multi-utilisateurs. Examinez l'étape 14. dans le flux de posture post-ISE 2.2.

Étape 5.Créez une configuration CA. Accédez àPolicy > Policy Elements > Results > Client Provisioning > Resources, cliquez surAdd, puis choisissezAnyConnect Configuration.

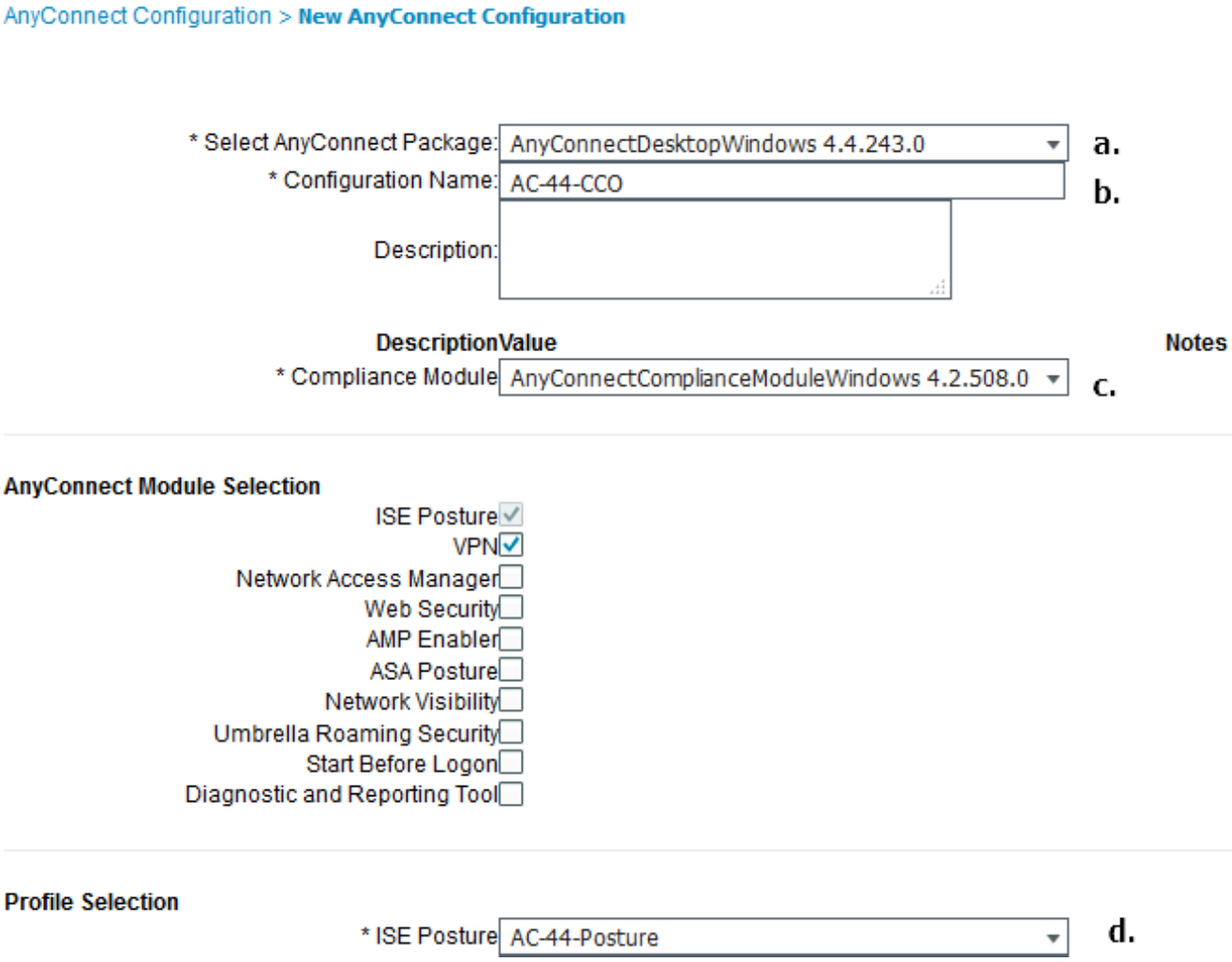


Figure 3-5

- Sélectionnez le package AC.
- Fournissez le nom de configuration AC.
- Sélectionnez la version du module de conformité.
- Sélectionnez le profil de configuration de la position AC dans la liste déroulante.

Étape 6 : configuration de la stratégie d'approvisionnement du client Accédez à Policy > Client Provisioning. Dans le cas de la configuration initiale, vous pouvez remplir des valeurs vides dans la stratégie présentée avec des valeurs par défaut. Si vous devez ajouter une stratégie à la configuration de position qui existe, accédez à la stratégie qui peut être réutilisée et choisissezDuplicate Aboveou Duplicate Below. Une toute nouvelle politique peut également être créée.

Ceci est un exemple de la politique utilisée dans le document.

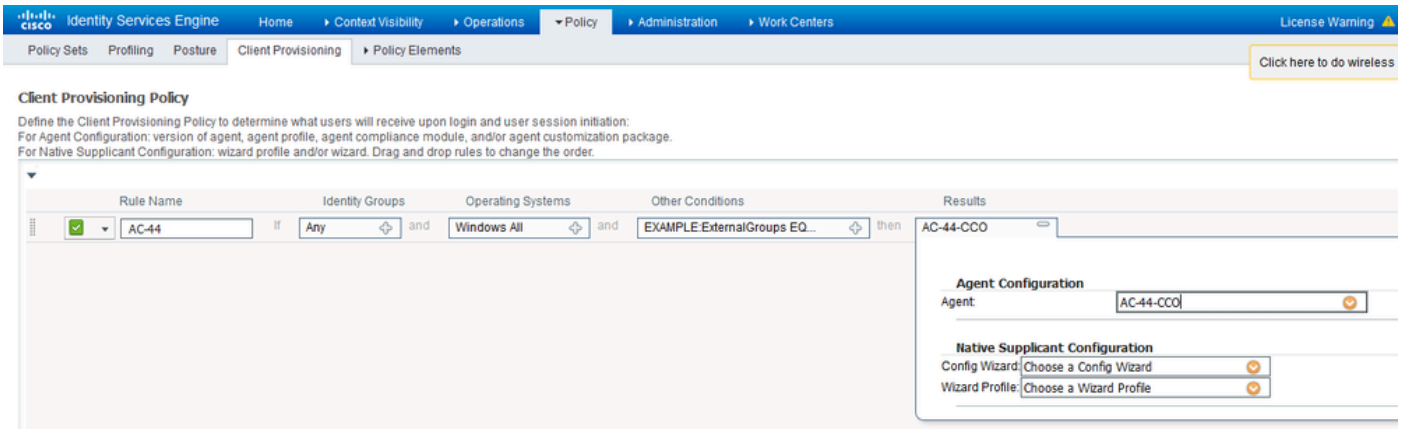


Figure 3-6

Sélectionnez votre configuration CA dans la section Résultat. Gardez à l'esprit qu'en cas de défaillance SSO, ISE ne peut avoir que des attributs de connexion au portail. Ces attributs sont limités aux informations qui peuvent être récupérées sur les utilisateurs à partir des magasins d'identités internes et externes. Dans ce document, le groupe AD est utilisé comme condition dans la stratégie d'approvisionnement du client.

Politiques et conditions de posture

Un simple contrôle de posture est utilisé. ISE est configuré pour vérifier l'état du service Windows Defender côté périphérique final. Les scénarios réels peuvent être beaucoup plus complexes, mais les étapes de configuration générales sont les mêmes.

Étape 1. Créer une condition de posture Les conditions de posture se trouvent dans Policy > Policy Elements > Conditions > Posture. Choisissez le type de condition de position. Voici un exemple de condition de service qui doit vérifier si le service Windows Defender est en cours d'exécution.

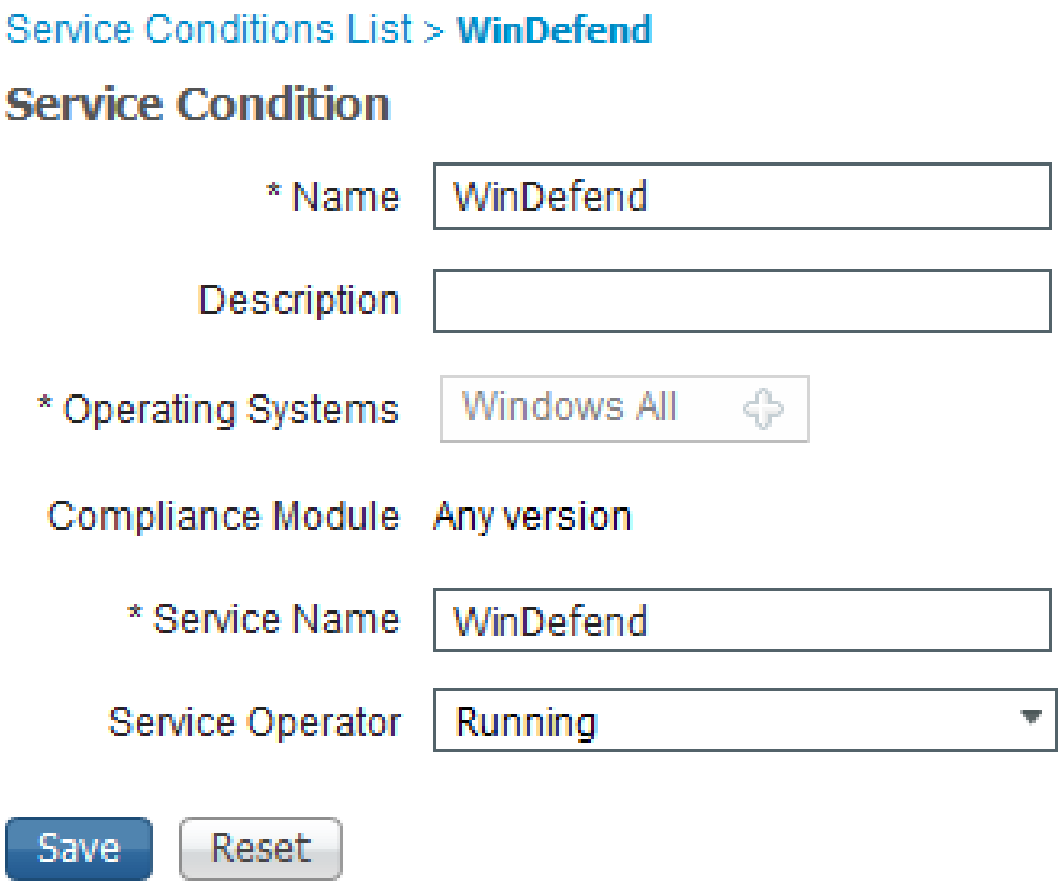


Figure 3-7

Étape 2.Configuration des exigences de posture. Accédez àPolicy > Policy Elements > Results > Posture > Requirements. Voici un exemple de vérification de Windows Defender :

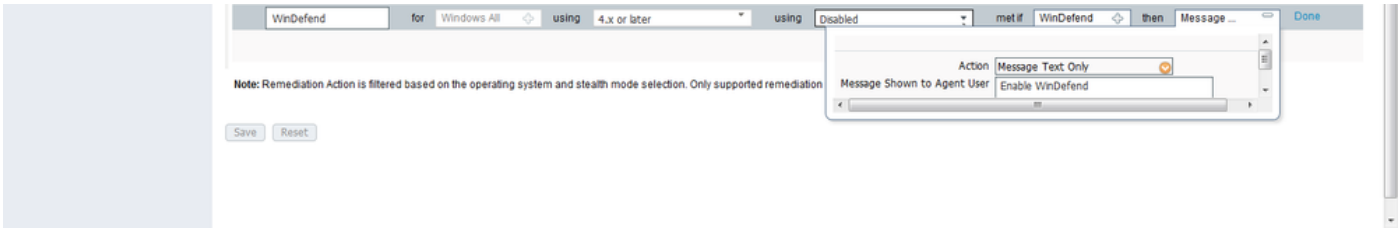


Figure 3-8

Choisissez votre condition de posture dans la nouvelle condition requise et spécifiez l'action corrective.

Étape 3. Configuration de la stratégie de position Accédez à Policy > Posture. Vous trouverez ici un exemple de la stratégie utilisée pour ce document. La condition requise de Windows Defender est attribuée comme obligatoire et ne contient comme condition que le nom du groupe AD externe.

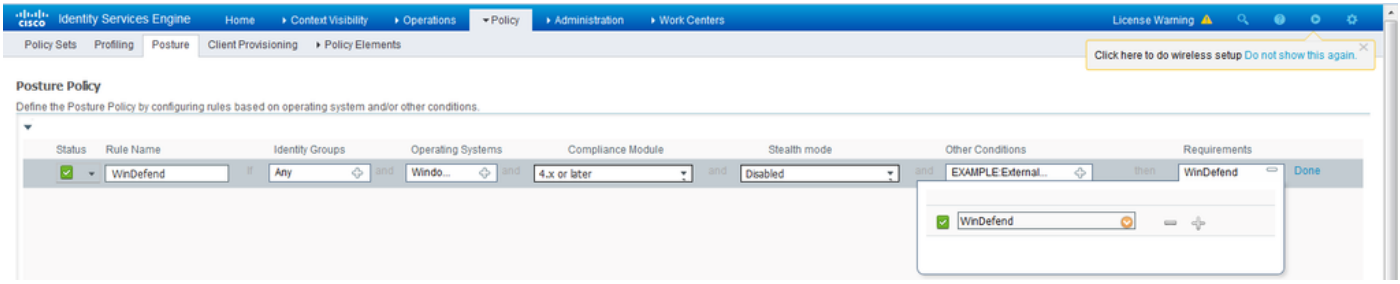


Figure 3-9

Configurer le portail de provisionnement client

Pour la position sans redirection, la configuration du portail d'approvisionnement du client doit être modifiée. Accédez àAdministration > Device Portal Management > Client Provisioning. Vous pouvez soit utiliser le portail par défaut, soit créer le vôtre. Le même portail peut être utilisé pour les deux postures avec et sans redirection.

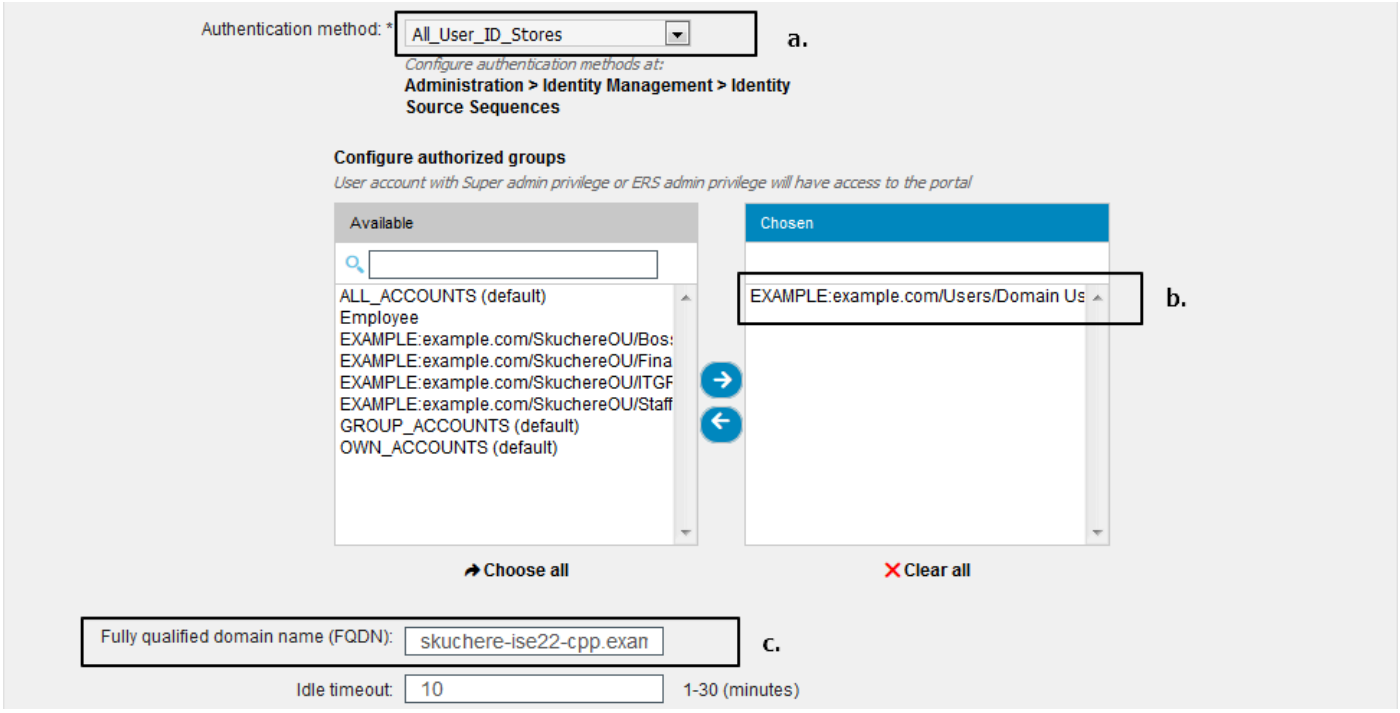


Figure 3-10

Ces paramètres doivent être modifiés dans la configuration du portail pour le scénario de non-redirection :

- Dans Authentification, spécifiez la séquence source d'identité qui doit être utilisée si SSO ne parvient pas à localiser une session pour l'utilisateur.
- Conformément à la liste de la séquence source d'identité sélectionnée des groupes disponibles est renseignée. À ce stade, vous devez sélectionner les groupes autorisés pour la connexion au portail.
- Le nom de domaine complet du portail de mise en service du client doit être spécifié pour les scénarios où le contrôle d'accès doit être déployé à partir du portail de mise en service du client. Ce nom de domaine complet doit pouvoir être résolu en adresses IP de PSN ISE. Les

utilisateurs doivent être invités à spécifier le nom de domaine complet dans le navigateur Web lors de la première tentative de connexion.

Configurer les profils et les stratégies d'autorisation

L'accès initial des clients lorsque l'état de posture n'est pas disponible doit être restreint. Cela peut se faire de plusieurs manières :

- Attribution de DACL - Pendant la phase d'accès restreint, la DACL peut être attribuée à l'utilisateur pour limiter l'accès. Cette approche peut être utilisée pour les périphériques d'accès réseau Cisco.
- Attribution de VLAN : avant que les utilisateurs qui réussissent puissent être placés dans un VLAN restreint, cette approche doit fonctionner correctement pour presque tous les fournisseurs NAD.
- Radius Filter-Id : avec cet attribut, la liste de contrôle d'accès définie localement sur NAD peut être attribuée à l'utilisateur dont l'état est inconnu. Étant donné qu'il s'agit d'un attribut RFC standard, cette approche doit fonctionner correctement pour tous les fournisseurs NAD.

Étape 1 : configuration de la liste DACL Puisque cet exemple est basé sur ASA, une liste de contrôle d'accès NAD peut être utilisée. Pour les scénarios réels, vous devez considérer VLAN ou Filter-ID comme des options possibles.

Pour créer une liste de contrôle d'accès DACL, accédez àPolicy > Policy Elements > Results > Authorization > Downloadable ACLset cliquez sur Add.

Pendant l'état de position inconnue, au moins ces autorisations doivent être fournies :

- trafic DNS
- Trafic DHCP
- Trafic vers les PSN ISE (ports 80 et 443) pour une possibilité d'ouvrir le FQDN convivial du portail. Le port sur lequel le portail CP est exécuté est 8443 par défaut et le port 8905 pour la compatibilité descendante)
- Trafic vers les serveurs de conversion si nécessaire

Voici un exemple de liste de contrôle d'accès sans serveurs de conversion :

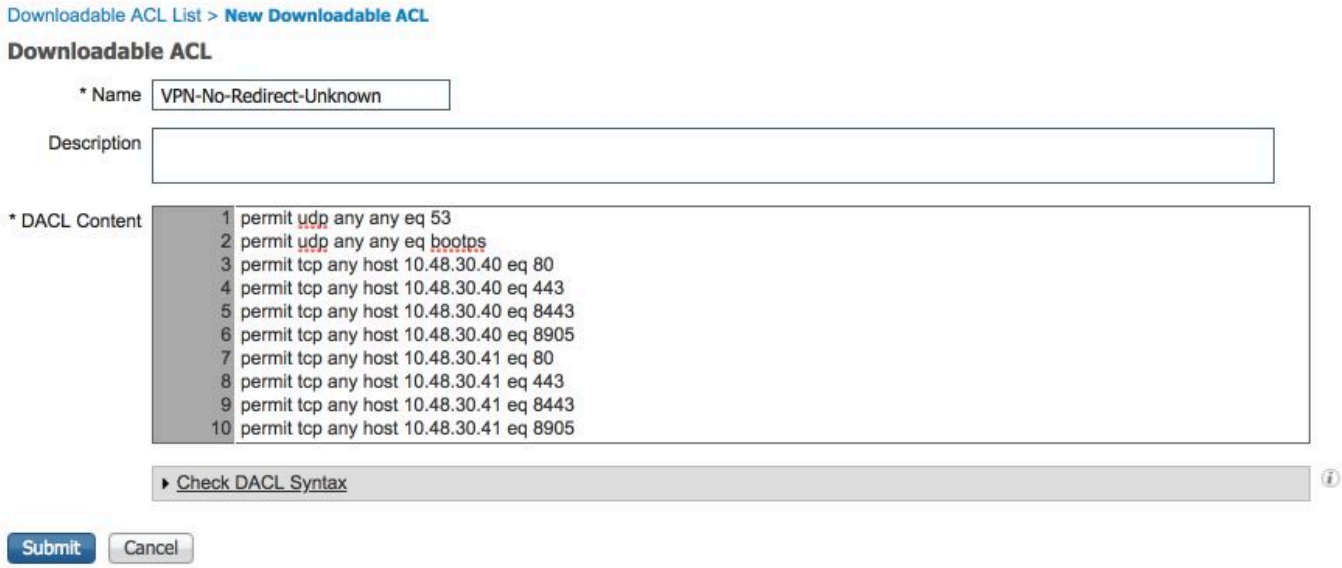


Figure 3-11

Étape 2 : configuration du profil d’autorisation

Comme d'habitude pour la posture, deux profils d'autorisation sont requis. La première doit contenir tout type de restrictions d'accès au réseau (profil avec DACL utilisé dans cet exemple). Ce profil peut être appliqué aux authentifications pour lesquelles l'état de posture n'est pas égal à conforme. Le second profil d'autorisation peut contenir uniquement un accès autorisé et peut être appliqué aux sessions dont l'état de position est égal à la conformité.

Pour créer un profil d'autorisation, accédez àPolicy > Policy Elements > Results > Authorization > Authorization Profiles.

Exemple de profil d'accès restreint :

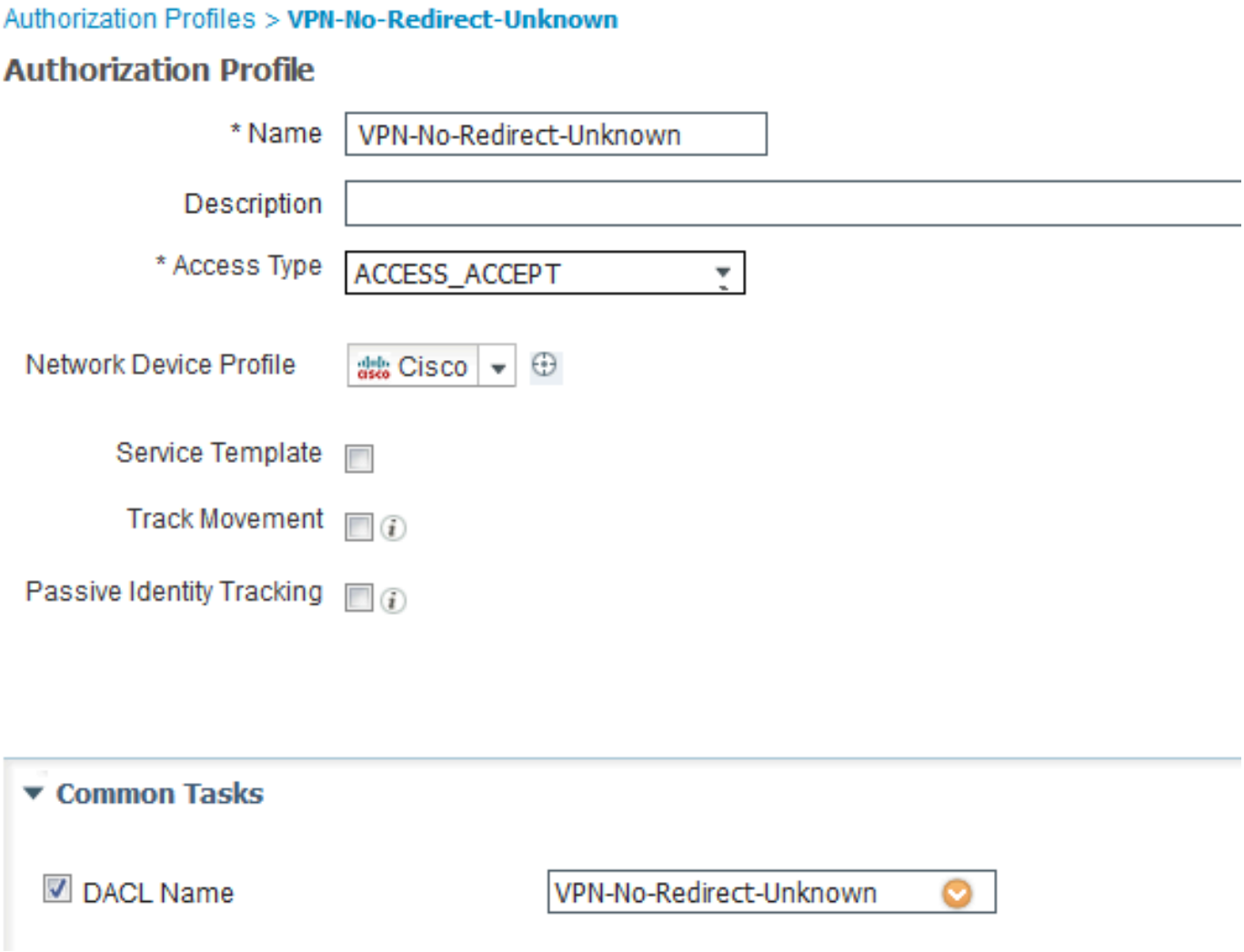


Figure 3-12

Dans cet exemple, le profil ISE par défaut PermitAccess est utilisé pour la session après une vérification de l'état de la position réussie.

Étape 3 : configuration de la stratégie d’autorisation Au cours de cette étape, deux stratégies d’autorisation doivent être créées. La première consiste à faire correspondre la demande d'authentification initiale avec l'état de posture inconnu et la seconde consiste à attribuer un accès complet après un processus de posture réussi.

Voici un exemple de stratégies d'autorisation simples pour ce cas :

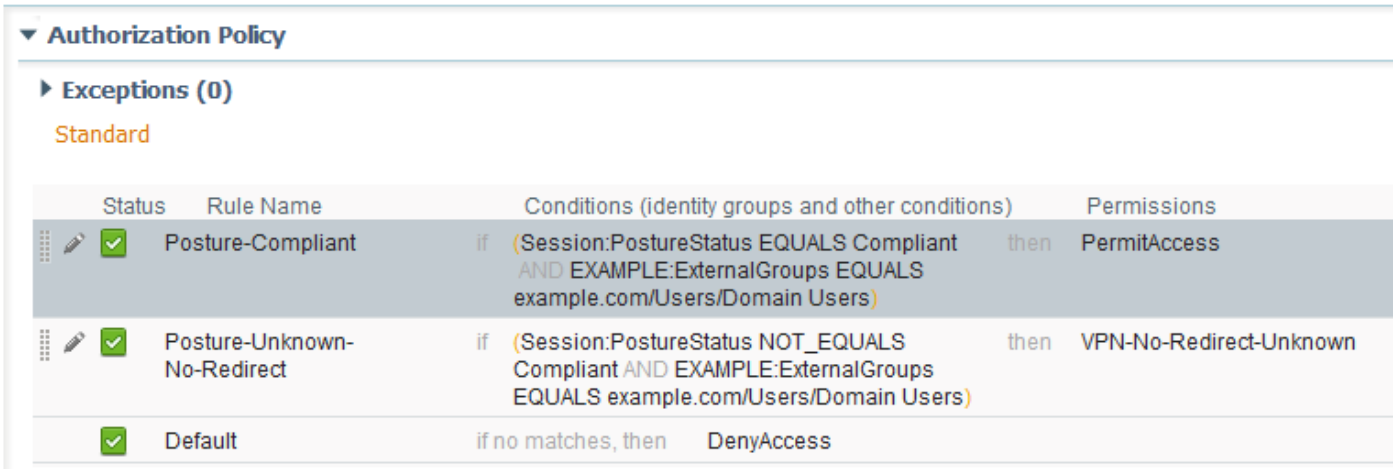


Figure 3-13

La configuration de la stratégie d'authentification ne fait pas partie de ce document, mais vous devez garder à l'esprit qu'avant de traiter la stratégie d'autorisation, une authentification réussie doit avoir lieu.

Vérifier

La vérification de base du flux peut consister en trois étapes principales :

Étape 1 : vérification du flux d’authentification

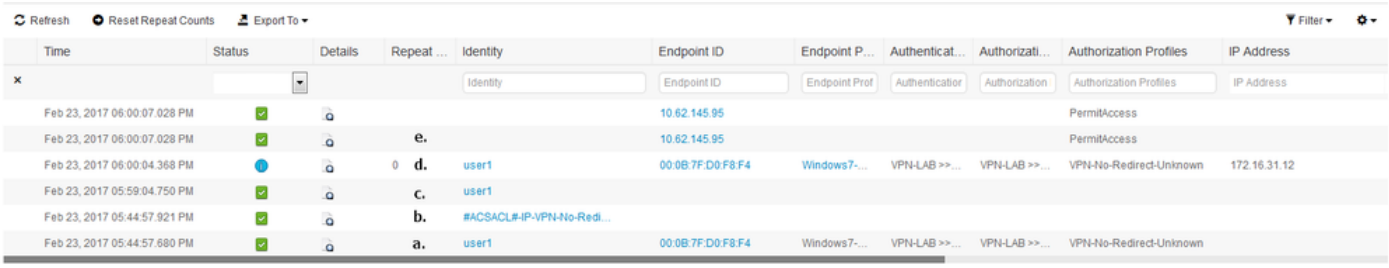


Figure 4-1

1. Authentification initiale Pour cette étape, vous pouvez être intéressé par la validation dont le profil d'autorisation a été appliqué. Si un profil d'autorisation inattendu a été appliqué, recherchez un rapport d'authentification détaillé. Vous pouvez ouvrir ce rapport en cliquant sur la loupe dans la colonne Détails. Vous pouvez comparer les attributs des rapports d'authentification détaillés avec les conditions de la stratégie d'autorisation que vous souhaitez voir correspondre.

2. Événement de téléchargement DACL. Cette chaîne est présentée uniquement dans le cas où le profil d'autorisation sélectionné pour l'authentification initiale contient un nom DACL.

3. Authentification du portail : cette étape du flux indique que le mécanisme SSO n'a pas réussi

à localiser la session utilisateur. Cela peut s'expliquer par de nombreuses raisons :

- NAD n'est pas configuré pour envoyer des messages de comptabilité ou l'adresse IP tramée n'y est pas présente
- Le nom de domaine complet du portail CPP a été résolu sur l'adresse IP du noeud ISE différente de celle du noeud où l'authentification initiale a été traitée
- Le client est situé derrière la fonction NAT

4. Modification des données de session. Dans cet exemple particulier, l'état de session est passé de Inconnu à Conforme.

5. COA vers le périphérique d'accès réseau. Ce certificat d'authenticité doit réussir à pousser une nouvelle authentification du côté NAD et de nouvelles affectations de stratégie d'autorisation du côté ISE. Si le certificat d'authenticité a échoué, vous pouvez ouvrir un rapport détaillé pour en connaître la raison. Les problèmes les plus courants liés au certificat d'authenticité peuvent être :
   - Expiration du certificat d'authenticité : dans ce cas, soit le PSN qui a envoyé la demande n'est pas configuré en tant que client de certificat d'authenticité du côté NAD, soit la demande de certificat d'authenticité a été abandonnée en cours de route.
   - ACK négatif du certificat d'authenticité : indique que le certificat d'authenticité a été reçu par NAD, mais qu'il est impossible de confirmer son fonctionnement pour une raison quelconque. Pour ce scénario, un rapport détaillé doit contenir une explication plus détaillée.

Comme ASA est utilisé comme NAD pour cet exemple, vous ne pouvez voir aucune demande d'authentification ultérieure pour l'utilisateur. Cela est dû au fait que l'ISE utilise la poussée de certificat d'authenticité pour ASA, ce qui évite l'interruption du service VPN. Dans un tel scénario, le certificat d'authenticité contient lui-même de nouveaux paramètres d'autorisation, donc une nouvelle authentification n'est pas nécessaire.

Étape 2.Vérification de la sélection de la stratégie d'approvisionnement du client - Pour cela, vous pouvez exécuter un rapport sur ISE qui peut vous aider à comprendre quelles stratégies d'approvisionnement du client ont été appliquées pour l'utilisateur.

Accédez au rapportOperations > Reports Endpoint and Users > Client Provisioninget exécutez-le à la date souhaitée.

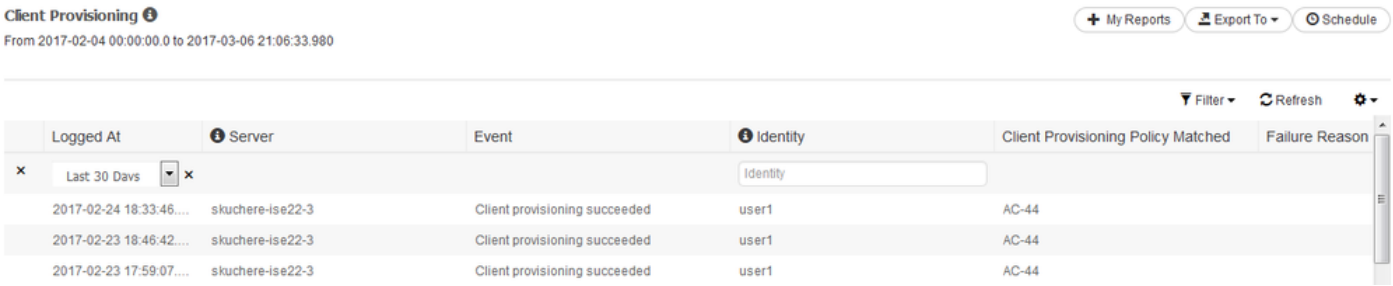


Figure 4-2

Avec ce rapport, vous pouvez vérifier quelle stratégie de provisionnement du client a été sélectionnée. En outre, en cas d'échec, les raisons doivent être indiquées dans la colonne «Failure

Reason».

Étape 3.Vérification du rapport de position - Accédez àOperations > Reports Endpoint and Users > Posture Assessment by Endpoint.



Figure 4-3

Vous pouvez ouvrir ici un rapport détaillé pour chaque événement particulier afin de vérifier, par exemple, à quel ID de session appartient ce rapport, quelles exigences exactes en matière de position ont été sélectionnées par ISE pour le terminal et l'état de chaque exigence.

Dépannage

Informations générales

Pour le dépannage du processus de posture, ces composants ISE doivent être activés pour le débogage sur les noeuds ISE où le processus de posture peut se produire :

- client-webapp - Le composant responsable du provisionnement de l'agent. Fichiers journaux ciblesguest.logetise-psc.log.
- guestacess - Le composant responsable de la recherche du propriétaire de session et du composant du portail d'approvisionnement du client (lorsque la requête parvient au mauvais PSN). Fichier journal cible - guest.log.
- provisioning - Composant responsable du traitement de la stratégie d'approvisionnement du client. Fichier journal cible -guest.log.
- posture - Tous les événements liés à la position. Fichier journal cible - ise-psc.log.

Pour le dépannage côté client, vous pouvez utiliser les éléments suivants :

- acisensa.log - En cas d'échec de mise en service du client côté client, ce fichier est créé dans le même dossier que celui dans lequel NSA a été téléchargé (télécharge normalement le répertoire pour Windows).
- AnyConnect_ISEPosture.txt - Ce fichier se trouve dans le bundle DART du répertoireCisco AnyConnect ISE Posture Module. Toutes les informations sur la découverte ISE PSN et les étapes générales du flux de posture sont consignées dans ce fichier.

Dépanner des problèmes courants

Problèmes liés à SSO

En cas de réussite de l'authentification unique, vous pouvez voir ces messages dans la ise-psc.log, cet ensemble de messages indique que la recherche de session s'est terminée correctement et que l'authentification sur le portail peut être ignorée.

<#root>

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

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

Found session c0a801010002600058232bb8 using ipAddr 10.62.145.121
```

Fenêtre de texte 5-1

Vous pouvez utiliser l'adresse IP du point d'extrémité comme clé de recherche pour trouver ces informations.

Un peu plus tard dans le journal des invités, vous devez voir que l'authentification a été ignorée :

<#root>

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

Login step will be skipped, as the session =c0a801010002600058232bb8 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.process
```

Fenêtre de texte 5-2

Si l'authentification unique ne fonctionne pas, le fichier contient desise-psc loginformations sur l'échec de la recherche de session :

<#root>

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

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

No Radius session found
```

Fenêtre de texte 5-3

Dans ce cas,guest.logvous devez voir l'authentification complète de l'utilisateur sur le portail :

<#root>

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

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.Ste
```

Fenêtre de texte 5-4

En cas d'échec d'authentification sur le portail, vous devez vous concentrer sur la vérification de la configuration du portail : quel magasin d'identités est utilisé ? Quels groupes sont autorisés à se connecter ?

Dépannage de la sélection de stratégie de provisionnement client

En cas d'échec des stratégies d'approvisionnement du client ou de traitement de stratégie incorrect, vous pouvez consulter le fichierguest.logpour plus de détails :

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

Fenêtre de texte 5-5

Dans la première chaîne, vous pouvez voir comment les informations sur la session sont injectées dans le moteur de sélection de stratégie. En cas de non-correspondance de stratégie ou de correspondance de stratégie incorrecte, vous pouvez comparer les attributs d'ici avec la configuration de stratégie d'approvisionnement du client. La dernière chaîne indique l'état de sélection de la stratégie.

Dépannage du processus de posture

Du côté du client, vous devez être intéressé par l'investigation des sondes et de leurs résultats. Voici un exemple de sonde de l'étape 1 réussie :

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

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..

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

Fenêtre de texte 5-6

À ce stade, PSN retourne aux informations AC sur le propriétaire de la session. Vous pouvez voir ces deux messages plus tard :

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

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..

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

Fenêtre de texte 5-7

Les propriétaires de session renvoient à l'agent toutes les informations requises :

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

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>
.

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

Fenêtre de texte 5-8

Du côté PSN, vous pouvez vous concentrer sur ces messages dans leguest.loglorsque vous vous attendez à ce que la requête initiale qui arrive au noeud ne soit pas propriétaire de la session :

<#root>

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

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.NextGenDi

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

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

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.NextGenDi

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

Fenêtre de texte 5-9

Ici, vous pouvez voir que PSN essaie d'abord de trouver une session localement, et après l'échec lance une requête à MNT avec l'utilisation de la liste des adresses IP et MAC pour localiser le propriétaire de la session.

Un peu plus tard, vous devez voir une requête du client sur le PSN correct :

<#root>

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

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

Found session c0a801010009e00058af0f7b using ipAddr 172.16.31.12
```

Fenêtre de texte 5-10

Dans l'étape suivante, PSN effectue une recherche de stratégie d'approvisionnement de client pour cette session :

<#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.PostureRun
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,795 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
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
```

Fenêtre de texte 5-11

Dans l'étape suivante, vous pouvez voir le processus de sélection des exigences de posture. À la fin de l'étape, une liste des exigences est préparée et renvoyée à l'agent :

<#root>

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

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.PostureMan
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,432 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,433 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,433 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
```

```
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:03,884 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cpm.posture.runtime.agent.AgentXmlGe
2017-02-23 18:00:03,904 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cpm.posture.runtime.agent.AgentXmlGe
2017-02-23 18:00:03,904 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cpm.posture.runtime.agent.AgentXmlGe
2017-02-23 18:00:04,069 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureHan
 <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>
```

Fenêtre de texte 5-12

Plus tard, vous pouvez voir que le rapport de posture a été reçu par PSN :

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

Fenêtre de texte 5-13

À la fin du flux, ISE marque le terminal comme conforme et lance le certificat d'authenticité :

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

Fenêtre de texte 5-14

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.