Meilleures pratiques et considérations relatives au déploiement ISE

Contenu

Introduction

Ce document décrit certaines configurations de base qui traitent de plusieurs cas d'utilisation avec une posture basée sur la redirection. Dans ces configurations, le client reste conforme, mais le périphérique d'accès au réseau (NAD) limite l'accès car il est en état de redirection.

Restrictions

Les configurations de ce document fonctionnent pour les NAD Cisco, mais pas nécessairement pour les NAD tiers.

Comportement du client de posture

Le client de posture déclenchera des sondes à ces moments :

- Connexion initiale
- Modification de la couche 3 (couche 3)/modification de la carte réseau (NIC) (nouvelle adresse IP, changement d'état de la carte réseau)

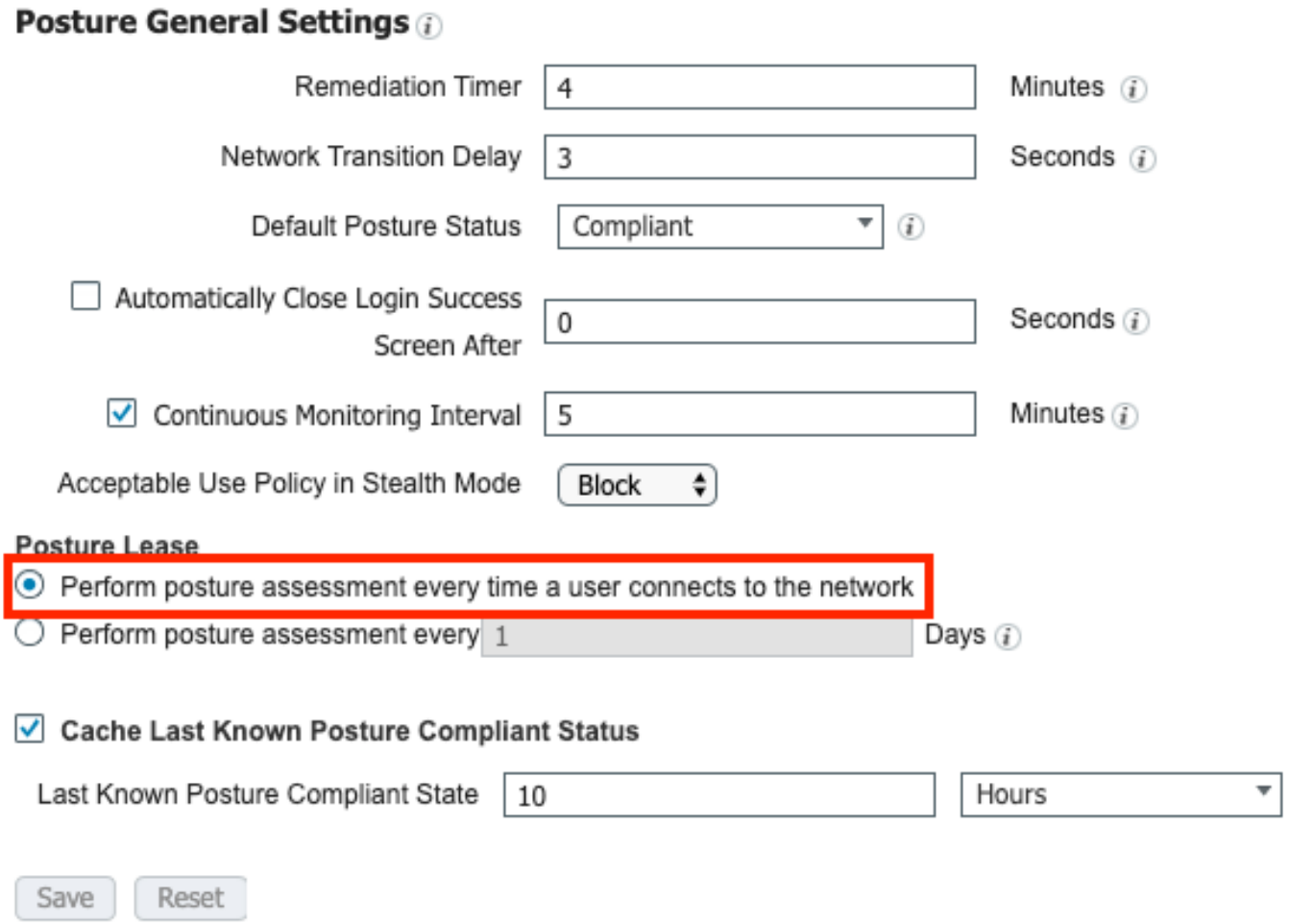
Scénarios :

Cas d'utilisation 1 - La réauthentification du client force la NAD à générer un nouvel ID de session.

Dans ce cas d'utilisation, le client est toujours conforme, mais en raison de la réauthentification, la NAD est dans l'état de redirection (URL de redirection et liste d'accès).

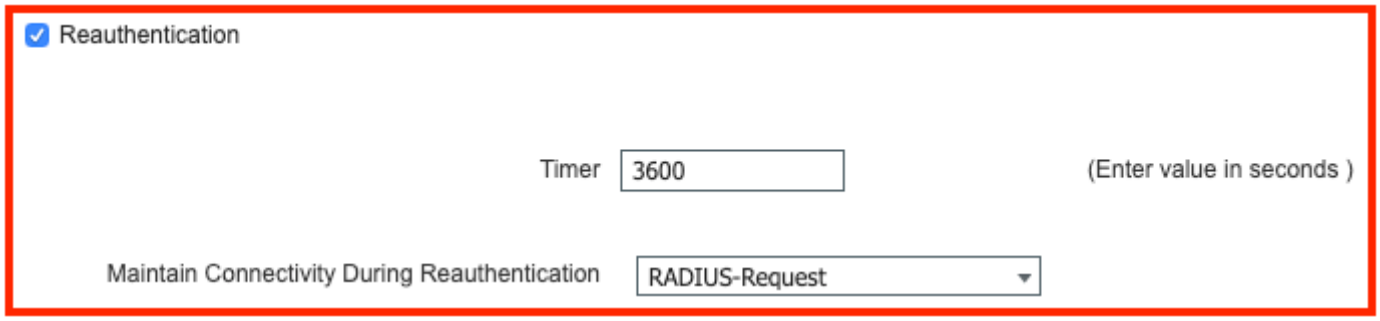
Par défaut, Identity Services Engine (ISE) est configuré pour effectuer une évaluation de la position chaque fois qu'il se connecte au réseau, en particulier pour chaque nouvelle session.

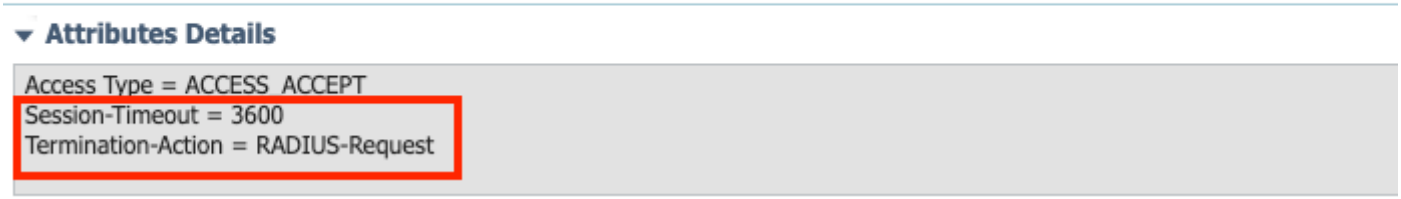
Ce paramètre est configuré sous Centres de travail > Posture > Settings > Posture General Settings.



Afin d'empêcher la NAD de générer un nouvel ID de session lors de la réauthentification, configurez ces valeurs de réauthentification dans le profil d'autorisation. Le compteur de réauthentification affiché n'est pas une recommandation standard, les compteurs de réauthentification doivent être pris en compte par déploiement en fonction du type de connexion (sans fil/filaire), de la conception (quelles sont les règles de persistance sur le répartiteur de charge), etc.

Stratégie > Éléments de stratégie > Résultats > Autorisation > Profils d'autorisation





Sur les commutateurs, vous devez configurer chaque interface, ou modèle, pour obtenir son compteur de réauthentification auprès d'ISE.

```
authentication timer reauthenticate server
```

> **Note**: S'il existe un équilibrage de charge, vous devez vous assurer que la persistance est configurée de manière à ce que les réauthentifications soient retournées au service de stratégie d'origine (PSN).

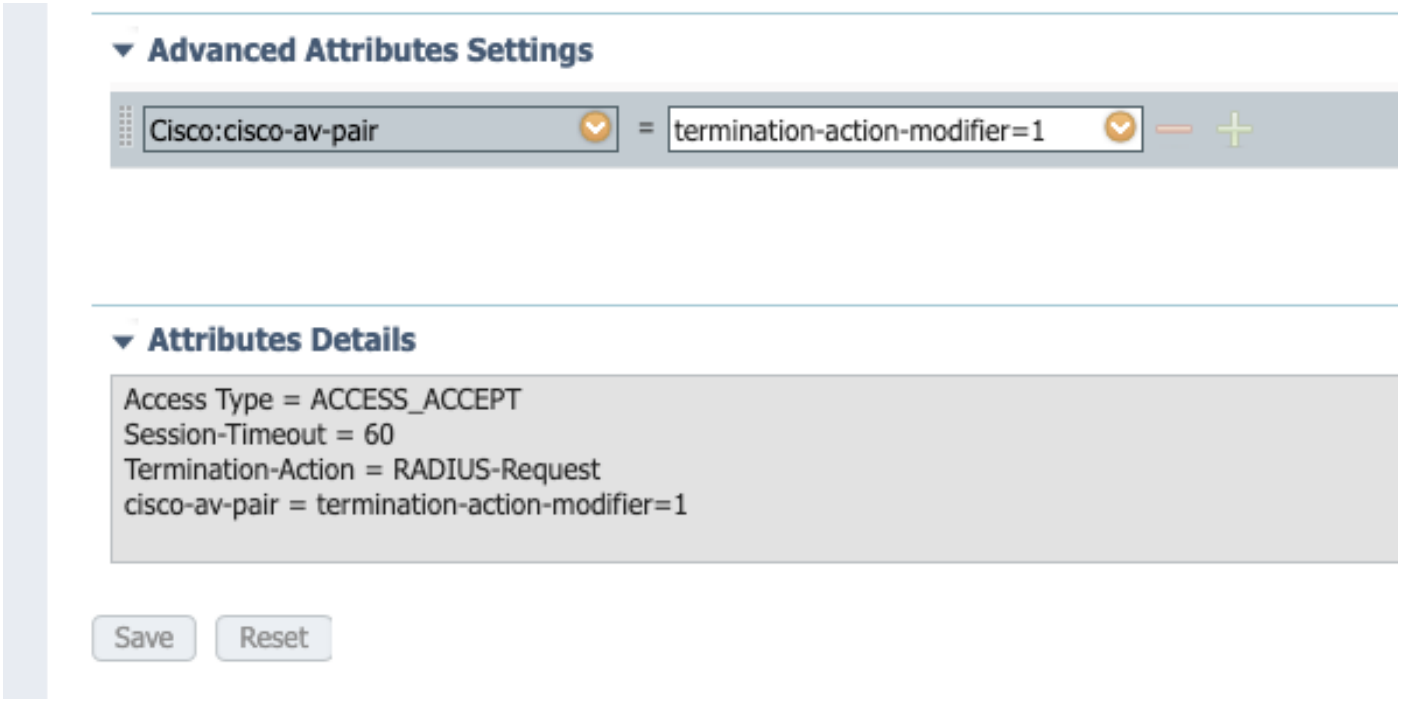
Cas d'utilisation 2 : le commutateur est configuré avec la commande MAB DOT1X et la priorité DOT1X MAB (câblée).

Dans ce cas, les réauthentifications seront terminées, car un arrêt de comptabilité pour la session 802.1x sera envoyé lorsque le contournement d'authentification MAC (MAB) est tenté pendant la réauthentification.

- L'arrêt de la comptabilité envoyé pour le processus MAB en cas d'échec de l'authentification est correct, car le nom d'utilisateur du client passe du nom d'utilisateur 802.1X au nom d'utilisateur MAB.
- Dot1x comme ID de méthode dans l'arrêt comptable est également correct car la méthode d'autorisation était dot1x.
- Lorsque la méthode Dot1x réussit, elle envoie un début de comptabilisation avec l'id de méthode dot1x. Ici aussi, ce comportement est comme prévu.

Afin de résoudre ce problème, configurez cisco-av-pair:termination-action-modificateur = 1 sur le profil authZ utilisé lorsqu'un point de terminaison est conforme. Cette paire attribut-valeur (AV) spécifie que la NAD doit réutiliser la méthode choisie dans l'authentification d'origine, quel que soit

l'ordre configuré.



Cas d'utilisation 3 : les clients sans fil se déplacent et les authentifications pour différents points d'accès se rendent à différents contrôleurs.

Dans ce cas, le réseau sans fil doit être conçu de sorte que les points d'accès (AP) à portée d'autres points d'accès pour l'itinérance utilisent le même contrôleur actif. Un exemple est le basculement SSO (Stateful switchover) du contrôleur de réseau local sans fil (WLC). Pour plus d'informations sur la haute disponibilité (HA) SSO pour WLC, consultez le Guide de déploiement de la haute disponibilité (SSO).

Cas d'utilisation 4 - Déploiements avec équilibreurs de charge (Pre 2.6 Patch 6, 2.7 Patch P2 et 3.0).

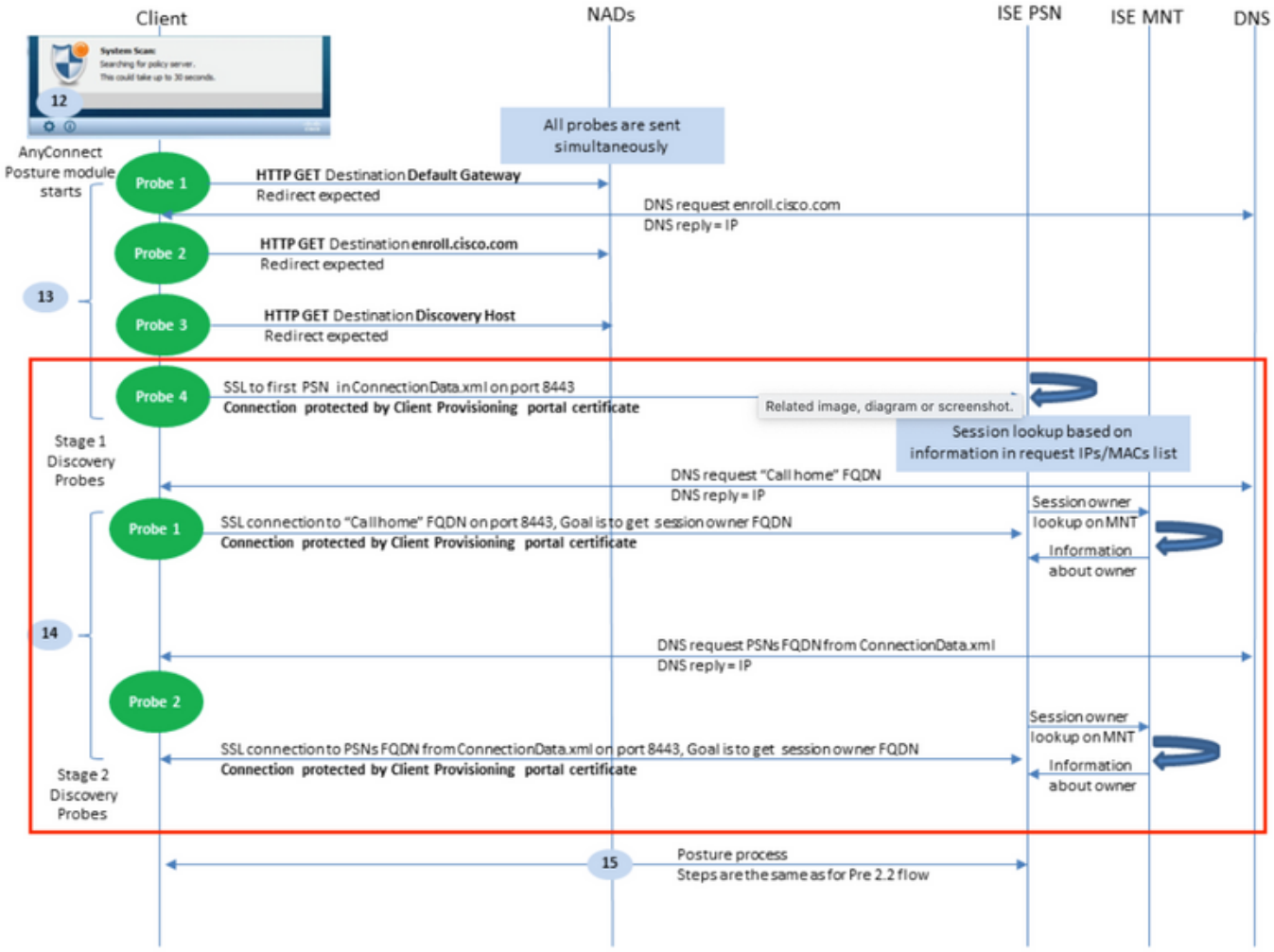
Dans les déploiements avec équilibreurs de charge impliqués, il est important de s'assurer qu'après avoir effectué les modifications dans les cas d'utilisation précédents, les sessions continuent à aller sur le même PSN. Avant la version/les correctifs répertoriés pour cette étape, l'état de la position n'est pas répliqué entre les noeuds via la distribution de données claires (anciennement Light Session Directory). Pour cette raison, il est possible que différents PSN retournent des résultats d'état différents.

Si la persistance n'est pas configurée correctement, les sessions qui se réauthentifient peuvent se rendre sur un PSN différent de celui utilisé à l'origine. Si cela se produit, le nouveau PSN pourrait marquer l'état de conformité des sessions comme inconnu et transmettre le résultat authZ avec la liste de contrôle d'accès (ACL)/URL et limiter l'accès aux points d'extrémité. Encore une fois, ce changement sur la NAD ne serait pas reconnu par le module de posture et les sondes ne seront pas déclenchées.

Pour plus d'informations sur la configuration des équilibreurs de charge, reportez-vous au Guide de déploiement de Cisco & F5 : Équilibrage de charge ISE avec BIG-IP. Il fournit une vue d'ensemble de haut niveau et une configuration spécifique de F5 d'une conception des meilleures pratiques pour les déploiements ISE dans un environnement à charge équilibrée.

Cas d'utilisation 5 - Les sondes de détection de l'étape 2 sont traitées par un serveur différent de celui avec lequel le client est authentifié (Pre 2.6 Patch 6, 2.7 Patch 2 et 3.0).

Regardez les sondes de la zone rouge dans ce diagramme.



Les PSN stockeront les données de session pendant cinq jours, de sorte que parfois les données de session d'une session « conforme » demeurent sur le PSN d'origine même si le client ne s'authentifie plus auprès de ce noeud. Si les sondes contenues dans la zone rouge sont traitées par un PSN autre que celui qui authentifie actuellement la session ET que PSN a précédemment possédé et marqué ce terminal conforme, il est possible qu'il y ait une incompatibilité entre l'état de posture du module de posture sur le terminal et le PSN d'authentification en cours.

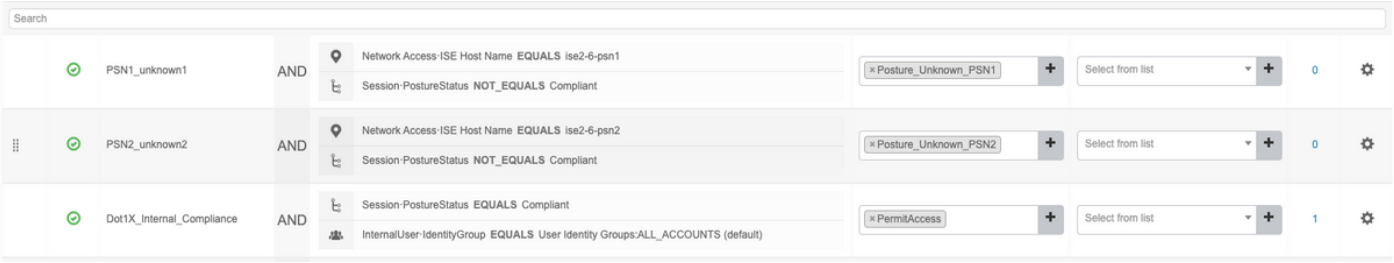
Voici quelques scénarios courants dans lesquels cette incompatibilité peut se produire :

- Un arrêt de compte n'est pas reçu pour un point d'extrémité lorsqu'il se déconnecte du réseau.
- La NAD a échoué d'un PSN à un autre.
- Un équilibreur de charge transfère les authentifications vers différents PSN pour le même terminal.

Afin de se protéger de ce comportement, ISE peut être configuré pour autoriser uniquement les sondes de détection d'un point d'extrémité particulier à atteindre le PSN auquel il s'authentifie actuellement. Pour ce faire, configurez une politique d'autorisation différente pour chaque PSN de votre déploiement. Dans ces stratégies, référencez un profil authZ différent qui contient une liste de contrôle d'accès téléchargeable (DACL) qui autorise UNIQUEMENT les sondes sur le PSN

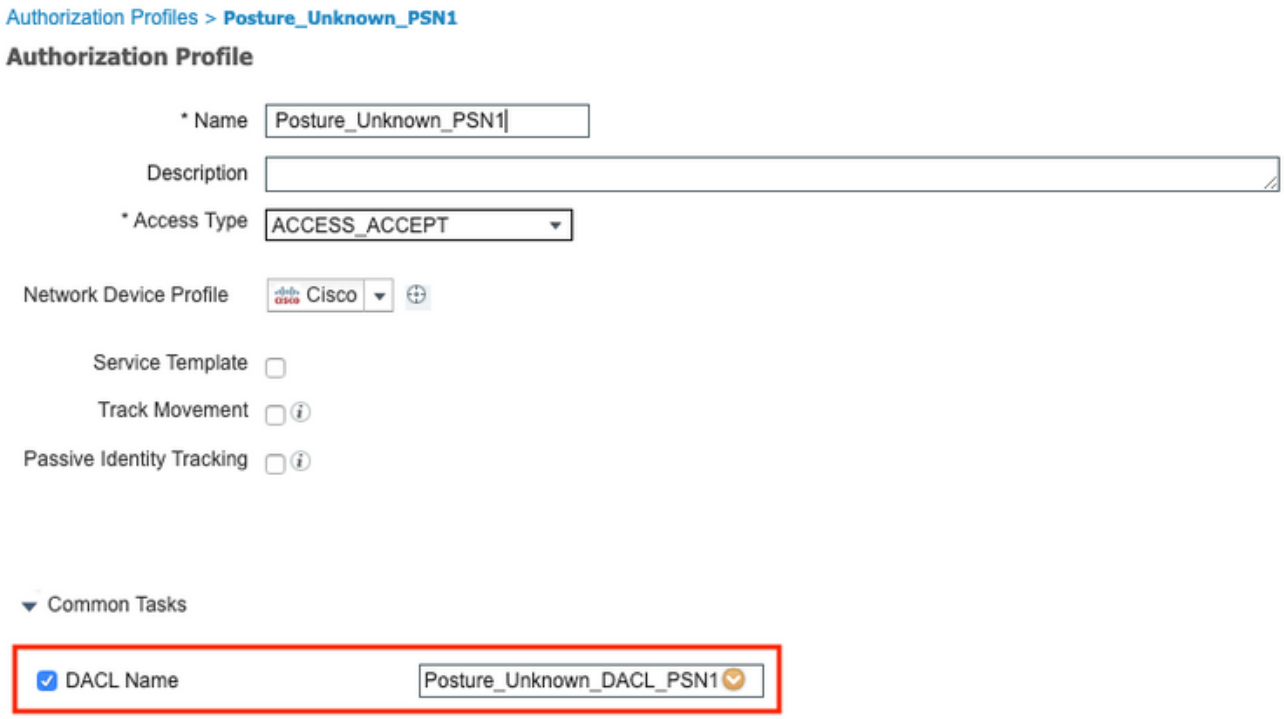
spécifié dans la condition authZ. Voir cet exemple :

Chaque PSN aura une règle pour l'état de posture inconnu :

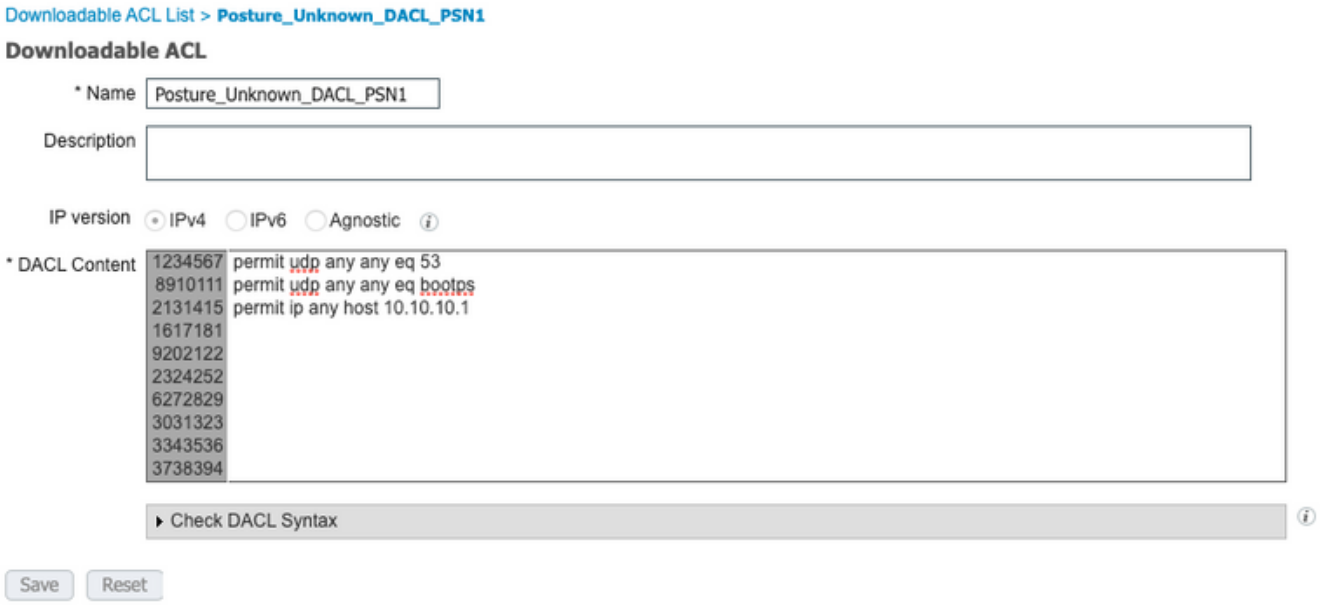


Chaque profil individuel fait référence à une liste de contrôle d'accès DACL différente.

> **Note**: Pour les connexions sans fil, utilisez des listes de contrôle d'accès Airespace.



Chaque DACL autorise uniquement l'accès de sonde au PSN qui gère l'authentification.



Dans l'exemple précédent, 10.10.10.1 est l'adresse IP de PSN 1. La DACL référencée peut être modifiée pour tous les services/adresses IP supplémentaires si nécessaire, mais doit limiter l'accès au seul PSN qui gère l'authentification.

Correctif de changement de comportement 2.6, correctif 2.7 et correctif 3.0

L'état de la position a été ajouté au répertoire de session RADIUS via le cadre de distribution de données claires. Chaque fois qu'une mise à jour d'état de position est reçue sur un PSN, elle est répliquée sur TOUS les PSN du déploiement. Une fois cette modification en vigueur, les implications des authentifications et/ou des sondes qui atteignent différents PSN sur différentes authentifications sont supprimées et tout PSN devrait pouvoir répondre à tous les points de terminaison, quel que soit l'endroit où ils sont actuellement authentifiés.

Dans les cinq cas d'utilisation de ce document, tenez compte des comportements suivants :

Cas d'utilisation 1 - La réauthentification du client force la NAD à générer un nouvel ID de session. Le client est toujours conforme, mais en raison de la réauthentification, la NAD est dans l'état de redirection (URL de redirection et liste d'accès).

- Ce comportement ne changera pas et cette configuration doit encore être implémentée sur ISE et les NAD.

Cas d'utilisation 2 : le commutateur est configuré avec la commande MAB DOT1X et la priorité DOT1X MAB (câblée).

- Ce comportement ne changera pas et cette configuration doit encore être implémentée sur ISE et les NAD.

Cas d'utilisation 3 : les clients sans fil se déplacent et les authentifications pour différents points d'accès se rendent à différents contrôleurs.

- Ce comportement ne changera pas et cette configuration doit encore être implémentée sur ISE et les NAD.

Cas d'utilisation 4 - Déploiements avec équilibrage de charge.

- Les meilleures pratiques définies dans le guide d'équilibrage de charge doivent toujours être suivies, mais si les authentifications sont transmises à différents PSN par l'équilibreur de charge, l'état correct doit être retourné au client.

Cas d'utilisation 5 - Les sondes de découverte de l'étape 2 sont traitées par un serveur différent de celui avec lequel le client est authentifié.

- Ceci ne doit pas être un problème avec le nouveau comportement et le profil d'autorisation par PSN ne doit pas être nécessaire.

Considérations relatives à la maintenance du même ID de session

Lorsque vous utilisez les méthodes répertoriées dans ce document, un utilisateur qui reste connecté au réseau peut potentiellement rester conforme pendant de longues périodes. Même s'ils se réauthentifient, l'ID de session ne change pas et, par conséquent, ISE continuera à transmettre le résultat AuthZ pour leur règle correspondant à l'état conforme.

Dans ce cas, une réévaluation périodique doit être configurée de sorte que la posture soit requise pour s'assurer que le terminal reste conforme aux politiques de l'entreprise à des intervalles définis.

Vous pouvez le configurer sous Centres de travail > Posture > Settings > Resessment configurations.