ISE-implementaties van optimale praktijken en overwegingen

Inhoud

Inleiding

Dit document beschrijft een aantal basisconfiguraties die meerdere gebruiksgevallen met een op omleiding gebaseerde houding benaderen. In deze configuraties blijft de client compatibel, maar het netwerk access apparaat (NAD) beperkt de toegang omdat het in de redirect status is.

Beperkingen

De configuraties in dit document werken voor Cisco NAD's, maar niet noodzakelijkerwijs voor NAD's van derden.

Gedrag van postclient

De postcliënt zal op deze tijden sondes veroorzaken:

- Eerste aanmelding
- Layer 3 (L3) verandering/Network Interface Card (NIC) verandering (nieuw IP-adres, NIC-statenwijziging)

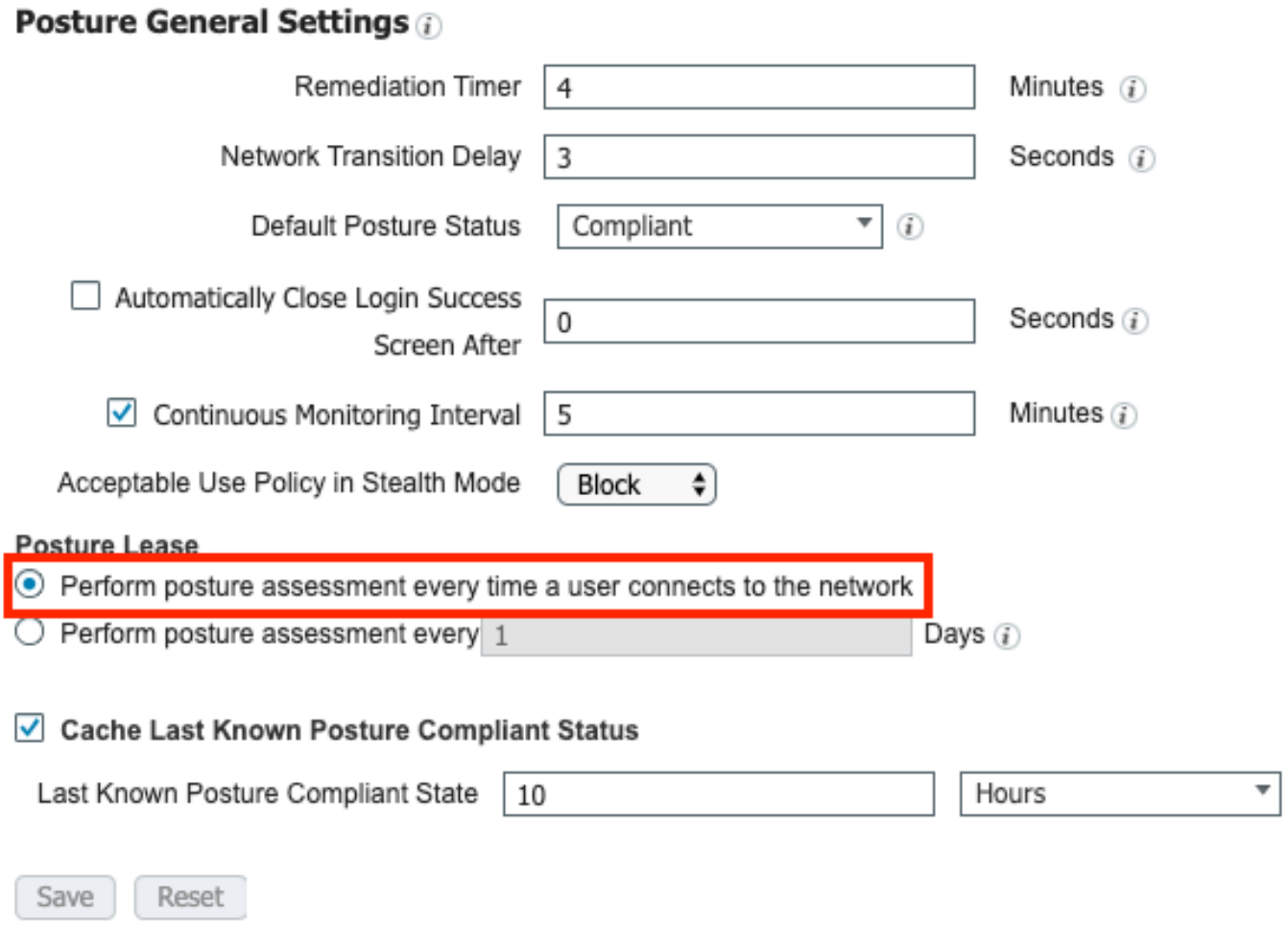
Use cases

Gebruik Case 1 - Client ReAuthentication forceert de NAD om een nieuwe sessie-ID te genereren.

In dit use geval is de client nog steeds compatibel, maar vanwege herauthenticatie is de NAD in de doorlopende staat (doorsturen URL en toegangslijst).

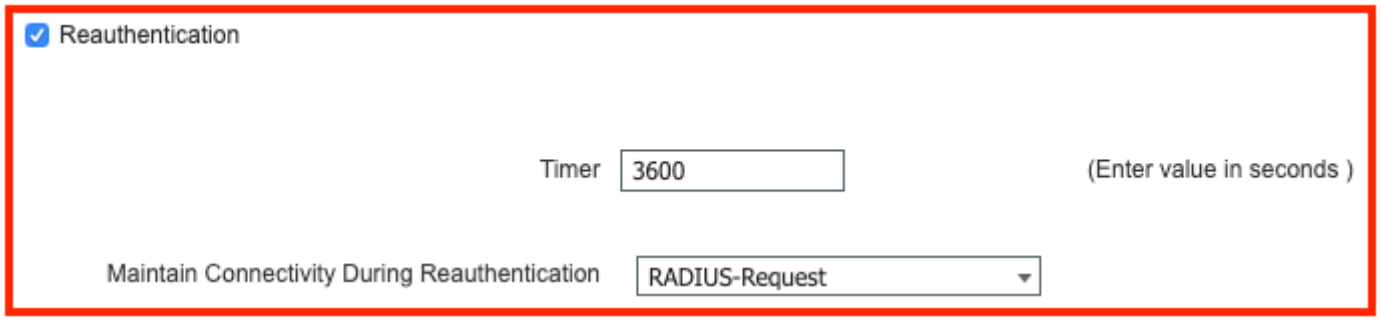
Standaard is ISE (Identity Services Engine) ingesteld om een beoordeling van de positie uit te voeren telkens wanneer deze verbonden is met het netwerk, meer in het bijzonder voor elke nieuwe sessie.

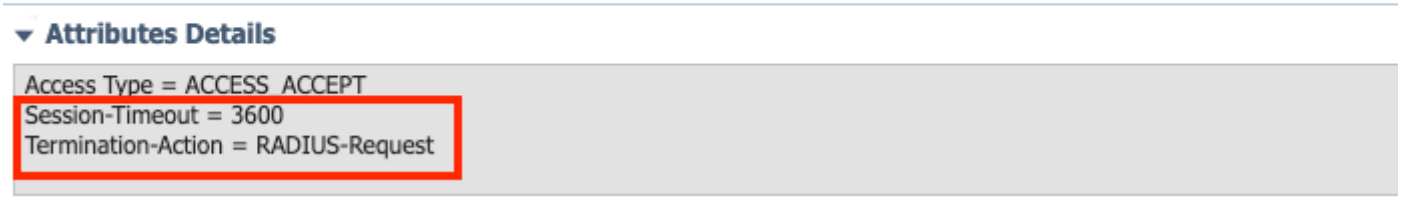
Deze instelling wordt ingesteld onder Workcenters > Posture > Instellingen > Algemene instellingen poseren.



Om de NAD ervan te weerhouden bij het genereren van een nieuwe sessie-ID, moet u deze waarden voor herverificatie in het autorisatieprofiel configureren. De weergegeven reparatie-timer is geen standaardaanbeveling, herauthenticatie-timers dienen te worden overwogen per implementatie op basis van het aansluittype (draadloos/bedraad), ontwerp (wat de persistentieregels op de loadstabilisator zijn), enzovoort.

Beleidselementen > Resultaten > Vergunningsprofielen > Vergunningsprofielen





Op switches, moet u elke interface of sjabloon configureren om de verificatietimer bij ISE te zetten.

```
authentication timer reauthenticate server
```

> **Opmerking:** Als er een taakverdeler is, moet u ervoor zorgen dat de persistentie zodanig is geconfigureerd dat reauthenticaties worden teruggegeven aan de originele Policy Service (PSN).

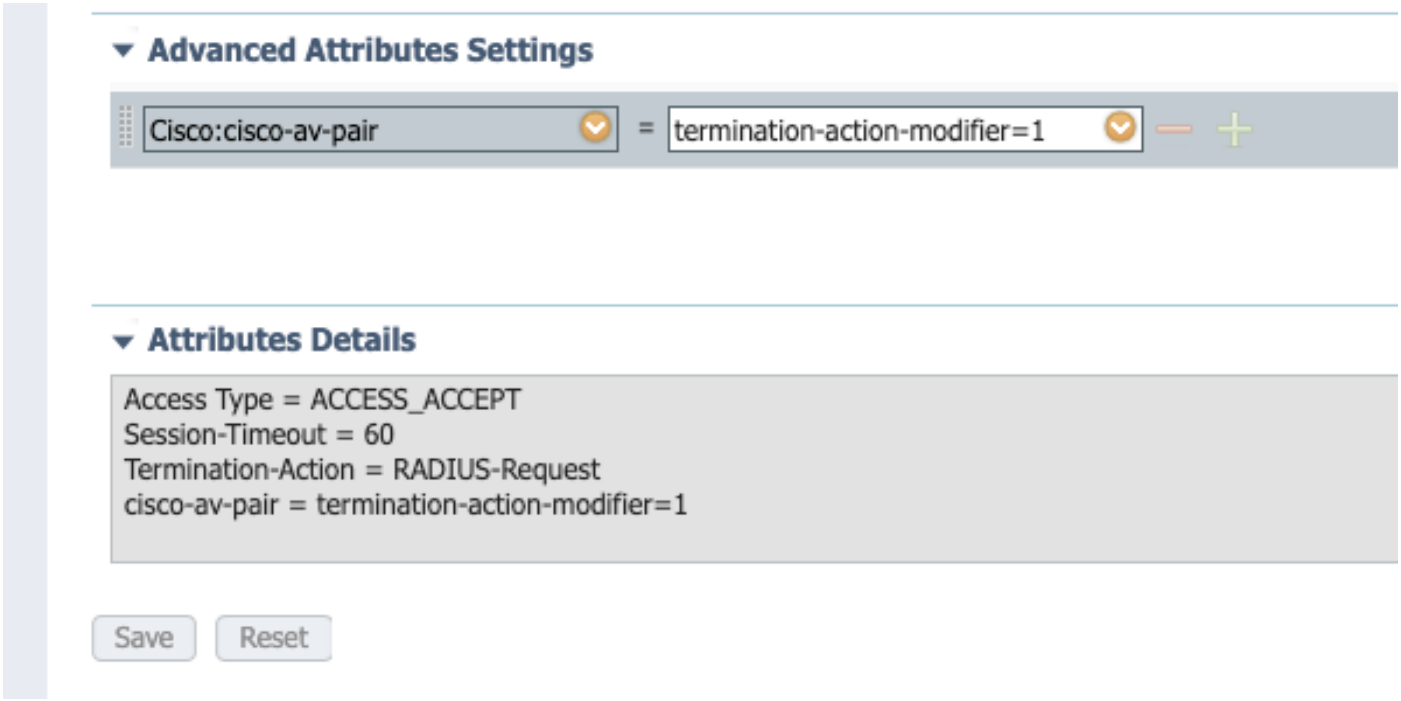
Gebruik Case 2 - de schakelaar is ingesteld met bestelling MAB DOT1X en prioriteit DOT1X MAB (bekabeld).

In dit geval zullen reauthenticaties worden beëindigd, omdat een boekhoudingsstop voor de 802.1x-sessie zal worden verstuurd wanneer MAC Verificatiebypass (MAB) tijdens herverificatie wordt geprobeerd.

- Het boekhoudingsstop dat voor het MAB-proces wordt verstuurd wanneer de authenticatie niet verloopt, is correct, aangezien de gebruikersnaam voor de client verandert van de 802.1X-gebruikersnaam naar de MAB-gebruikersnaam.
- Dot1x als methode-id in de boekhoudstop is ook correct aangezien de goedkeuringsmethode dot1x was.
- Als de Dot1x-methode slaagt, wordt er een beginnen met de methode-id als dot1x. Ook op dit punt is dit gedrag zoals verwacht.

Om deze kwestie op te lossen, moet u het cisco-av-paar configureren:beëindiging-actie-modifier = 1 op het authZ profiel dat wordt gebruikt wanneer een eindpunt compatibel is. Dit eigenschap-waarde (AV) paar specificeert dat de NAD de methode die in de oorspronkelijke authenticatie is

geselecteerd, ongeacht de geconfigureerde volgorde opnieuw moet gebruiken.



Gebruik Case 3 - Draadloze klanten roamen en authenticaties voor verschillende AP's gaan naar verschillende controllers.

Voor deze situatie moet het draadloze netwerk zodanig worden ontworpen dat de toegangspunten (AP's) binnen bereik van andere AP's voor roaming dezelfde actieve controller gebruiken. Een voorbeeld is een Wireless LAN Controller (WLC) stateful Switching (SSO)-failover. Zie High Availability (SSO) Deployment Guide voor meer informatie over SSO's met hoge beschikbaarheid voor WLC.

Gebruik case 4 - implementaties met taakverdeling (pre 2.6, Patch 6, 2.7, Patch P2 en 3.0).

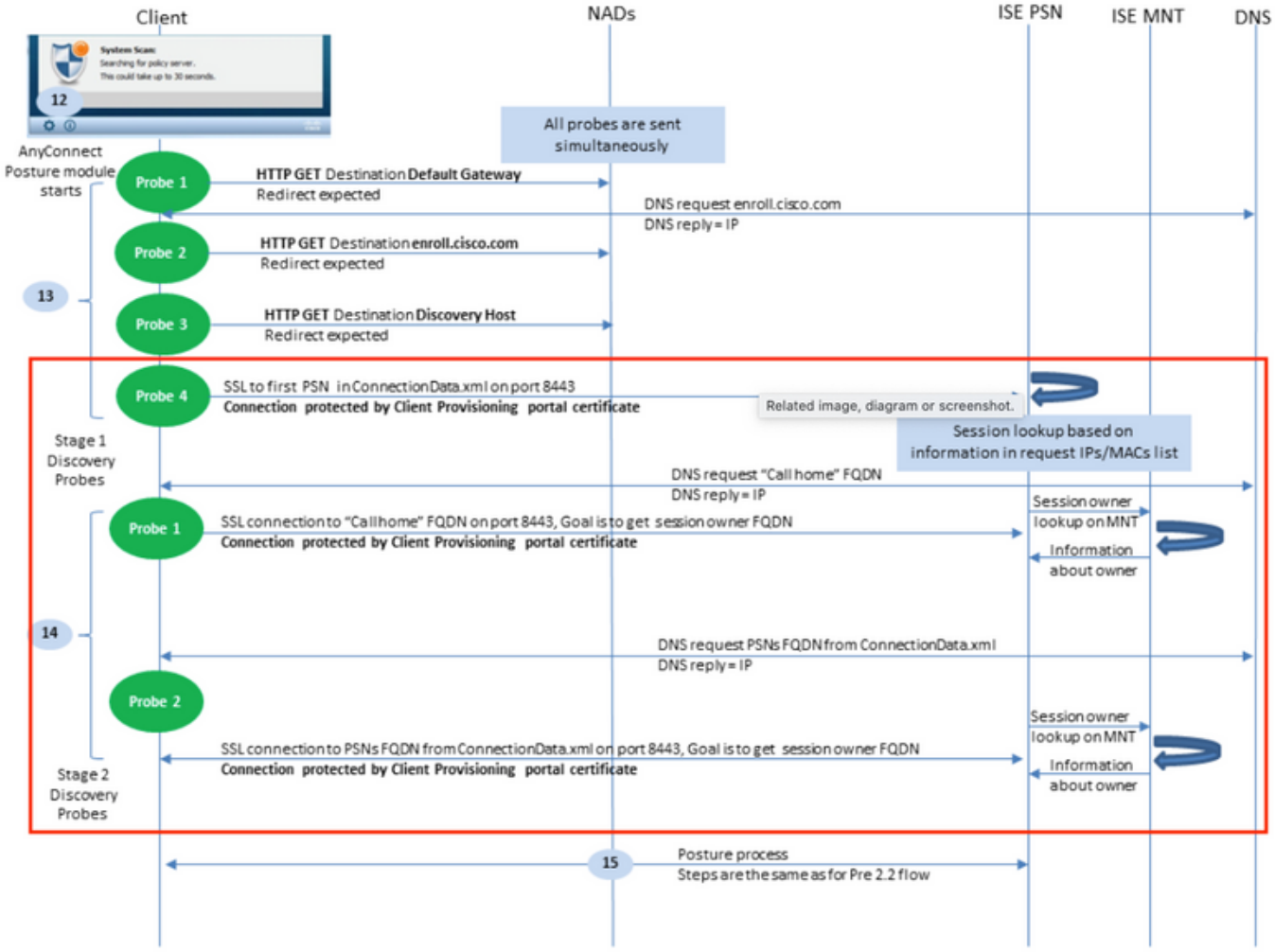
Bij implementaties met taakverdeling is het belangrijk om ervoor te zorgen dat, nadat u de wijzigingen in de vorige gebruiksgevallen hebt aangebracht, de sessies naar dezelfde PSN blijven gaan. Vóór de versie/de patches die voor deze stap zijn aangegeven, wordt de status van de positie niet herhaald tussen de knooppunten via Light Data Dirtion (voorheen Light Session Directory). Daarom is het mogelijk voor verschillende PSN's om verschillende resultaten van de poststatus terug te geven.

Als persistentie niet correct is ingesteld, kunnen sessies die opnieuw authentiek verklaren naar een ander PSN gaan dan die dat oorspronkelijk werd gebruikt. Als dit gebeurt, kan het nieuwe PSN de status van de sessieconformiteit als onbekend markeren en het resultaat van de authZ met de ACL/URL (Direct Access Control Control List)/URL doorgeven en de toegang tot de eindpunten beperken. Opnieuw zou deze verandering op de NAD niet door de postmodule worden herkend en zullen de sondes niet worden geactiveerd.

Zie de implementatiegids van Cisco en F5 voor meer informatie over het configureren van taakstabilisators: ISE-taakverdeling met behulp van BIG-IP. Het biedt een overzicht op hoog niveau en F5 specifieke configuratie van een best practice-ontwerp voor ISE-implementaties in een belastingsgebalanceerde omgeving.

Gebruik Case 5 - Niveau 2 ontdekkingsspelden worden beantwoord door een andere server dan de client is geauthentiseerd met (Pre 2.6 Patch 6, 2.7 Patch 2 en 3.0).

Kijk eens naar de sondes in het rode vakje in dit diagram.



PSN's zullen sessiegegevens gedurende vijf dagen opslaan, dus soms blijven sessiegegevens voor een "conforme" sessie behouden op het oorspronkelijke PSN, zelfs als de client niet langer echt is met dat knooppunt. Als de sondes die in het rode vakje zijn omgeven, worden beantwoord door een andere PSN dan die welke momenteel de sessie echt maakt EN die PSN voorheen eigenaar was van en gemarkeerd heeft als dit eindpunt, is het mogelijk dat er een mismatch is tussen de posterstatus van de postmodule op het eindpunt en de huidige authenticatie PSN.

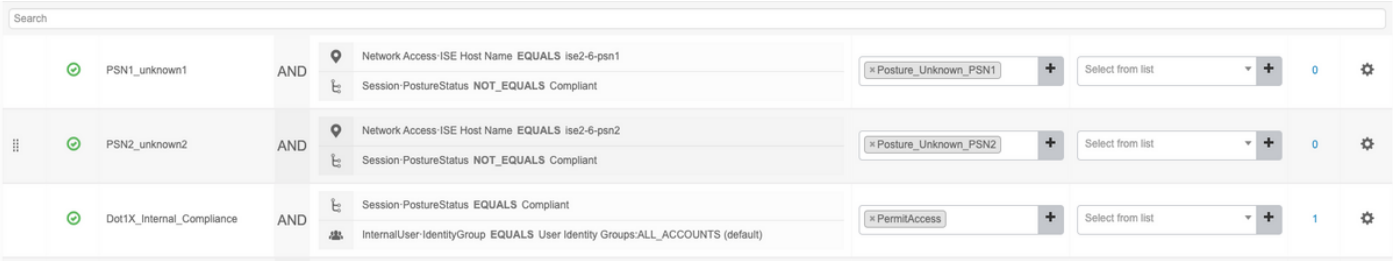
Hier zijn een paar gebruikelijke scenario's waar deze mismatch kan voorkomen:

- Een boekhoudingsstop wordt niet ontvangen voor een eindpunt wanneer het van het netwerk losmaakt.
- De NAD is niet van de ene PSN op de andere overgestapt.
- Een taakbalk stuurt authenticaties naar verschillende PSN's voor hetzelfde eindpunt.

Om van dit gedrag te beschermen, kan ISE worden geconfigureerd om alleen ontdekkingsspelden van een bepaald eindpunt toe te staan om het PSN te bereiken waar het momenteel voor authentiek is. Om dit te bereiken, moet u een ander autorisatiebeleid voor elke PSN in uw plaatsing vormen. In dit beleid dient u een ander authZ-profiel te verwijzen dat een DACL-toegangscontrolelijst (Downloadable Access Control List) bevat, zodat de sondes ALLEEN kunnen

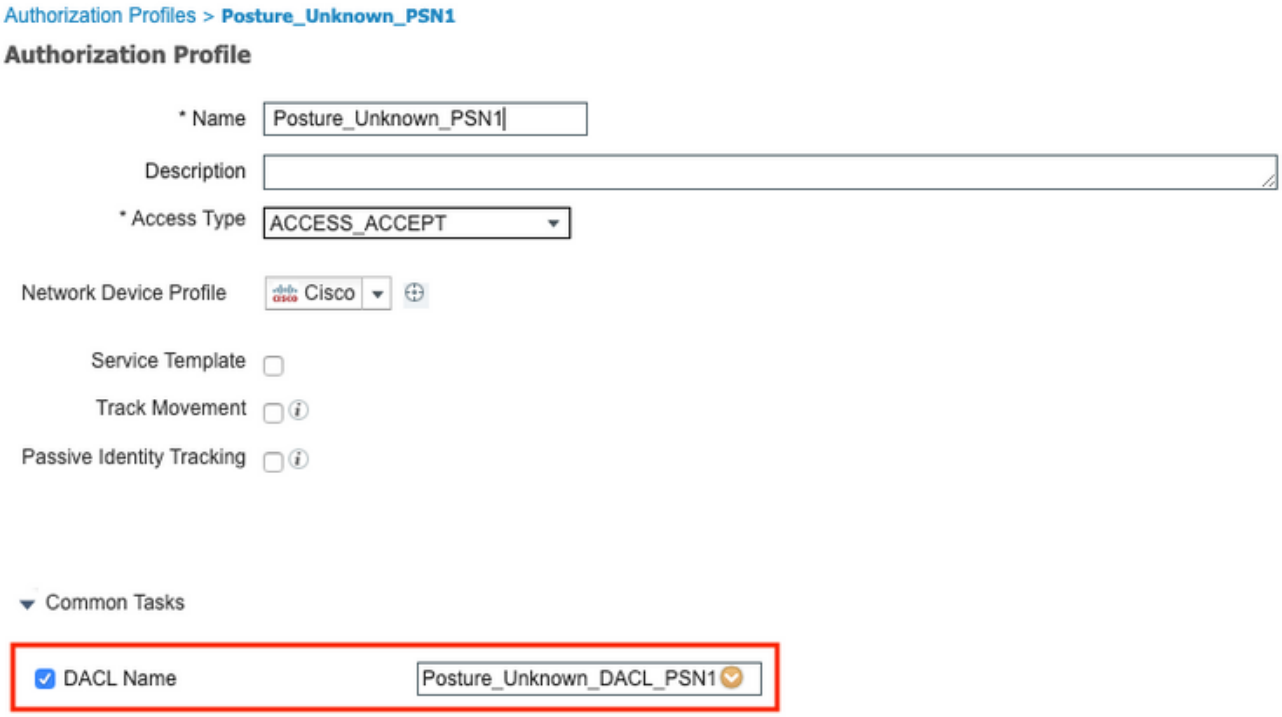
worden gebruikt voor de PSN-modus die in de authZ-modus is gespecificeerd. Zie dit voorbeeld:

Elke PSN heeft een regel voor de onbekende posterstatus:

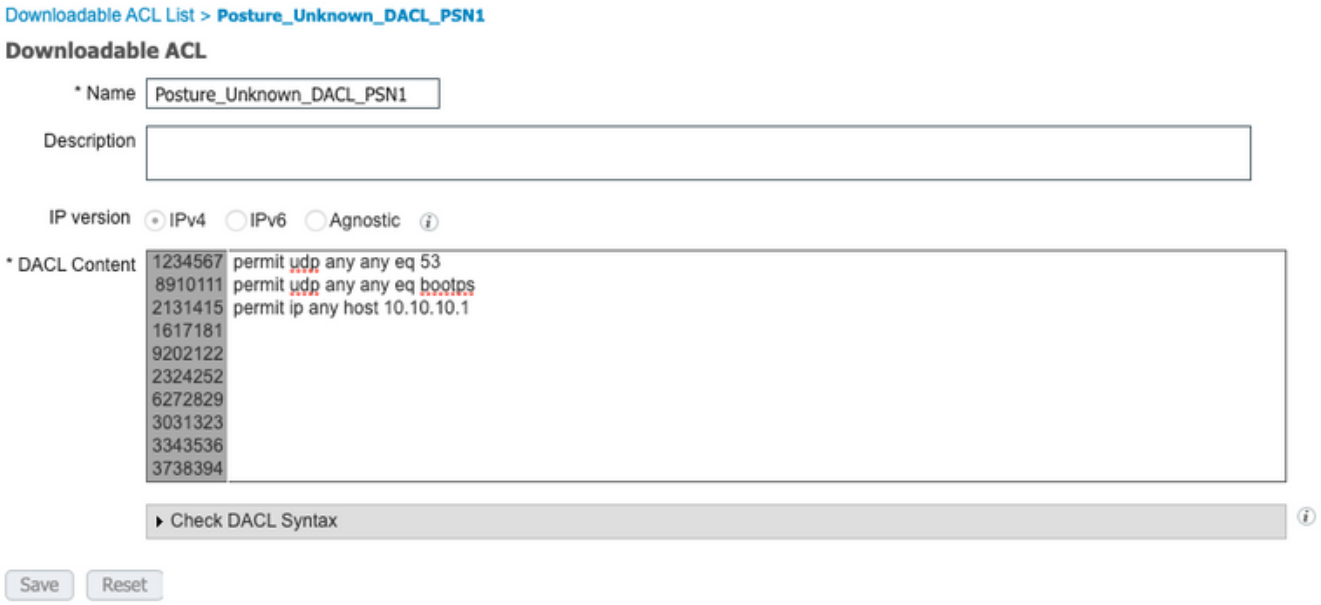


Elk afzonderlijk profiel verwijst naar een andere DACL.

> **Opmerking:** Gebruik Airespace ACL's voor draadloze verbindingen.



Elke DACL geeft alleen toegang tot de PSN die de verificatie verwerkt.



In het vorige voorbeeld is 10.10.10.1 het IP-adres van PSN 1. De DACL waarnaar verwezen wordt kan worden gewijzigd voor extra services/IP's indien nodig, maar zou de toegang tot alleen het PSN moeten beperken dat de verificatie verwerkt.

Gedragsverandering Post 2.6 Patch 6, 2.7 Patch 2 en 3.0

De status van de post is in de RADIUS-sessiemap toegevoegd via het Lichtgegevensdistributieframe. Telkens wanneer een posterstatus update op een PSN wordt ontvangen, zal deze in de implementatie worden herhaald naar ALLE PSN's. Zodra deze wijziging van kracht is, worden de implicaties van authenticaties en of sondes die verschillende PSN's bereiken op verschillende authenticaties verwijderd en kan elke PSN op alle eindpunten antwoorden, ongeacht waar ze momenteel echt zijn bevonden.

Denk bij de vijf gebruiksgevallen in dit document aan deze gedragingen:

Gebruik Case 1 - Client ReAuthentication forceert de NAD om een nieuwe sessie-ID te genereren. De client is nog steeds compatibel, maar vanwege herauthenticatie is NAD in de staat van herleiding (herdirect URL en toegangslijst).

- Dit gedrag zal niet veranderen en deze configuratie moet nog steeds worden toegepast op ISE en de NAD's.

Gebruik Case 2 - de schakelaar is ingesteld met bestelling MAB DOT1X en prioriteit DOT1X MAB (bekabeld).

- Dit gedrag zal niet veranderen en deze configuratie moet nog steeds worden toegepast op ISE en de NAD's.

Gebruik Case 3 - Draadloze klanten roamen en authenticaties voor verschillende AP's gaan naar verschillende controllers.

- Dit gedrag zal niet veranderen en deze configuratie moet nog steeds worden toegepast op ISE en de NAD's.

Gebruik Case 4 - implementaties met taakverdeling.

- de beste praktijken die in de belastingsbalanshandleiding zijn gedefinieerd, dienen nog te worden gevolgd, maar indien de belastingsbalanser authenticaties naar verschillende PSN's doorstuurt, moet de juiste posterstatus aan de klant worden teruggegeven.

Gebruik Case 5 - Stage 2 zoeksondes waarop een andere server reageert dan de client is echt bevonden

- Dit mag geen probleem zijn met het nieuwe gedrag en het vergunningprofiel per PSN dient niet noodzakelijk te zijn.

OVERWEGINGEN BIJ HET BEHOUDEN VAN DEZELFDE SessionID

Wanneer u de methoden gebruikt die in dit document worden opgesomd, kan een gebruiker die op het netwerk blijft aangesloten mogelijk lange tijd aan de eisen blijven voldoen. Ondanks dat ze opnieuw echt worden, verandert de sessieID niet en daarom zal ISE het resultaat AuthZ blijven doorgeven voor hun regel die de conforme status weergeeft.

In dit geval moet Periodieke herbeoordeling zodanig worden geconfigureerd dat Posture vereist is om te verzekeren dat het eindpunt op bepaalde tijdstippen in overeenstemming blijft met het beleid van het bedrijfsleven.

Dit kan worden ingesteld onder Workcenters > Posture > Instellingen > Herwaarderingsconfiguraties.