ISE終端安全評估部署最佳實踐和注意事項

目錄

簡介

本文檔介紹一些基本配置，這些配置通過基於重定向的安全狀態解決了多個使用案例。在這些配置中，客戶端保持相容，但網路接入裝置(NAD)會限制訪問，因為它處於重定向狀態。

限制

本文檔中的配置適用於思科NAD，但不一定適用於第三方NAD。

狀態客戶端行為

安全狀態客戶端將在以下時間觸發探測：

- 初始登入
- 第3層(L3)更改/網路介面卡(NIC)更改（新IP地址、NIC狀態更改）

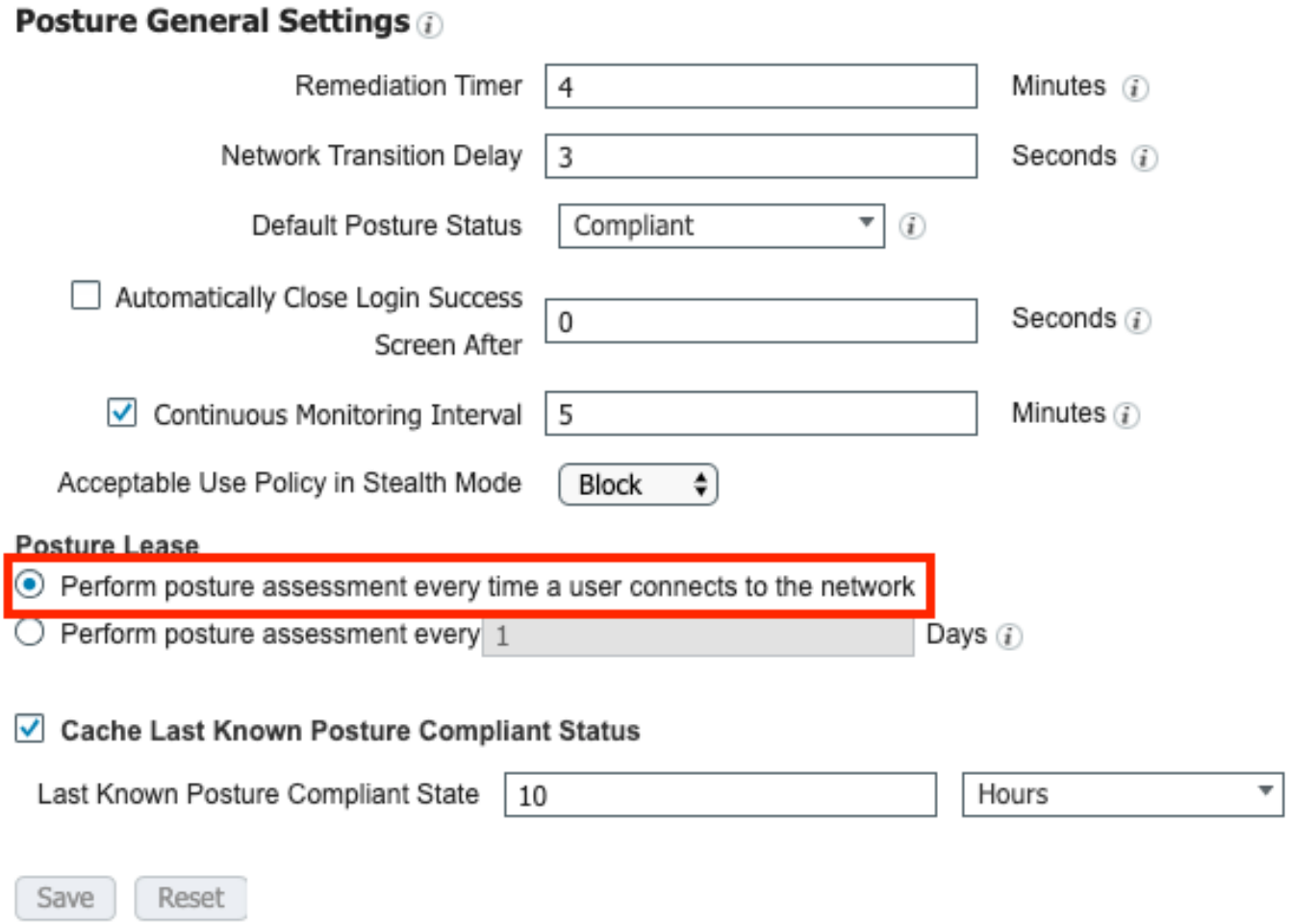
使用案例

使用案例1 — 客戶端重新身份驗證會強制NAD生成新的會話ID。

在此使用案例中，使用者端仍符合要求，但由於重新驗證，因此NAD處於重新導向狀態（重新導向URL和存取清單）。

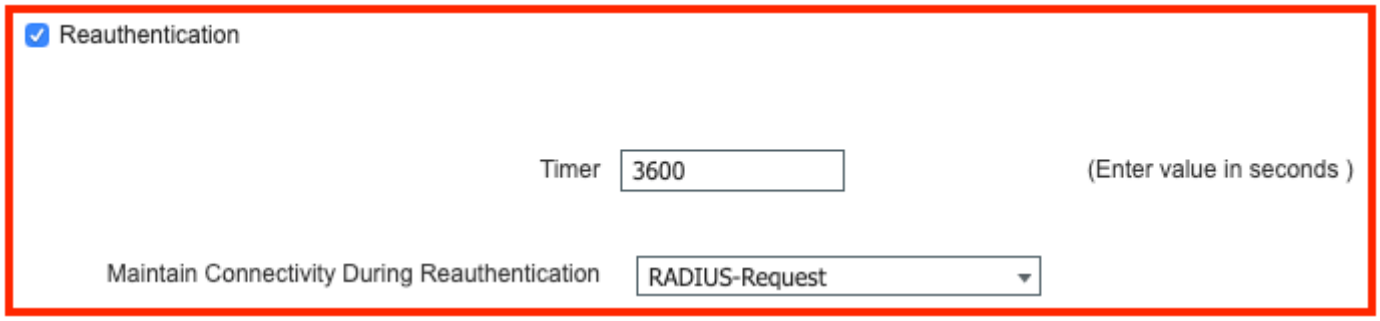
預設情況下，身份服務引擎(ISE)配置為在每次連線到網路時執行狀態評估，更具體地說，是針對每個新會話。

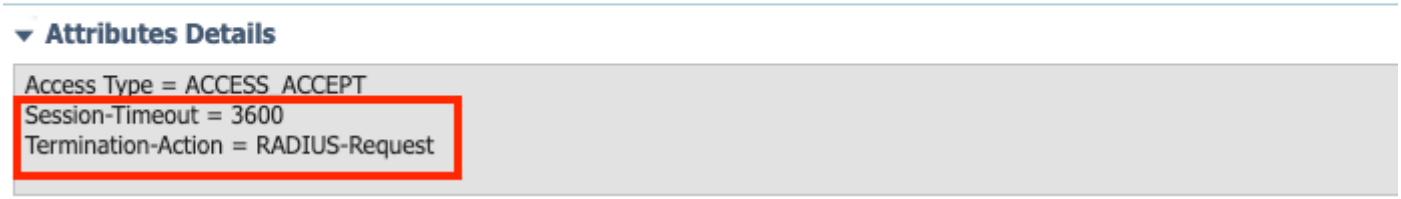
此設定在Work Centers > Posture > Settings > Posture General Settings下配置。



為了防止NAD在重新身份驗證時生成新的會話ID，請在授權配置檔案中配置這些重新身份驗證值。顯示的重新驗證計時器不是標準建議，應根據連線型別（無線/有線）、設計（負載平衡器上的永續性規則是什麼）等考慮重新驗證計時器。

Policy > Policy Elements > Results > Authorization > Authorization Profiles





在交換機上，您需要配置每個介面或模板，以便從ISE獲取其重新身份驗證計時器。

```
authentication timer reauthenticate server
```

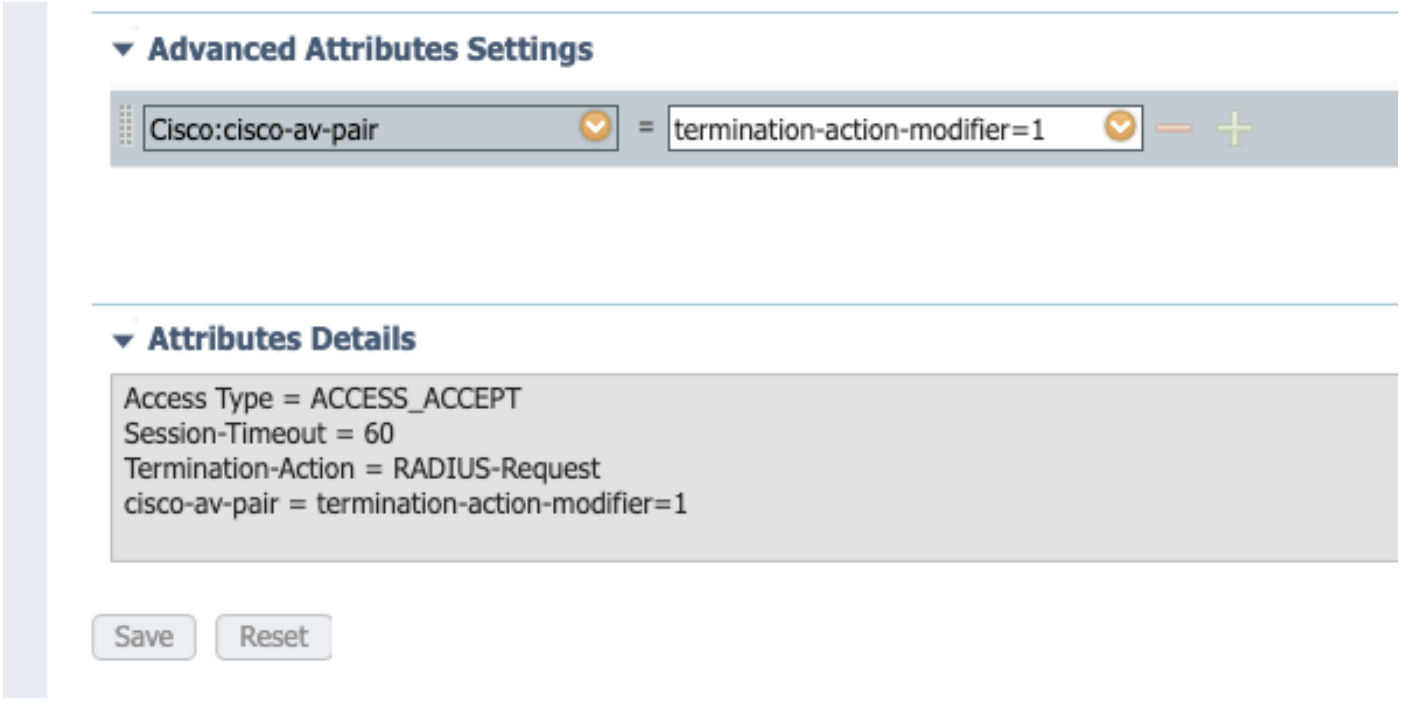
> **附註**：如果存在負載平衡器，則需要確保以重新身份驗證將返回到原始策略服務(PSN)的方式配置永續性。

使用案例2 — 交換機配置為MAB DOT1X和優先順序DOT1X MAB（有線）。

在這種情況下，重新身份驗證將終止，因為在重新身份驗證期間嘗試MAC身份驗證繞過(MAB)時，將傳送802.1x會話的記帳停止。

- 當MAB進程身份驗證失敗時，為MAB進程傳送的記帳停止是正確的，因為客戶端的使用者名稱從802.1X使用者名稱更改為MAB使用者名稱。
- 記賬停止時作為方法id的dot1x也是正確的，因為授權方法是dot1x。
- 當Dot1x方法成功時，它會傳送一個記賬開始，其中方法id為dot1x。同樣，這種行為也符合預期。

為了解決此問題，請在端點相容時使用的authZ設定檔上設定cisco-av-pair:termination-action-modifier = 1。此屬性值(AV)對指定NAD應重新使用在原始身份驗證中選擇的方法，而不考慮配置的順序。



使用案例3 — 無線客戶端漫遊和不同AP的身份驗證將轉至不同的控制器。

對於這種情況，需要設計無線網路，以便可以到達用於漫遊的其它AP的接入點(AP)使用相同的活動控制器。其中一個範例是無線LAN控制器(WLC)狀態化交換(SSO)容錯移轉。有關適用於WLC的高可用性(HA)SSO的詳細資訊，請參閱高可用性(SSO)部署指南。

使用案例4 — 具有負載平衡器的部署（2.6之前的修補程式6、2.7之前的修補程式P2和3.0）。

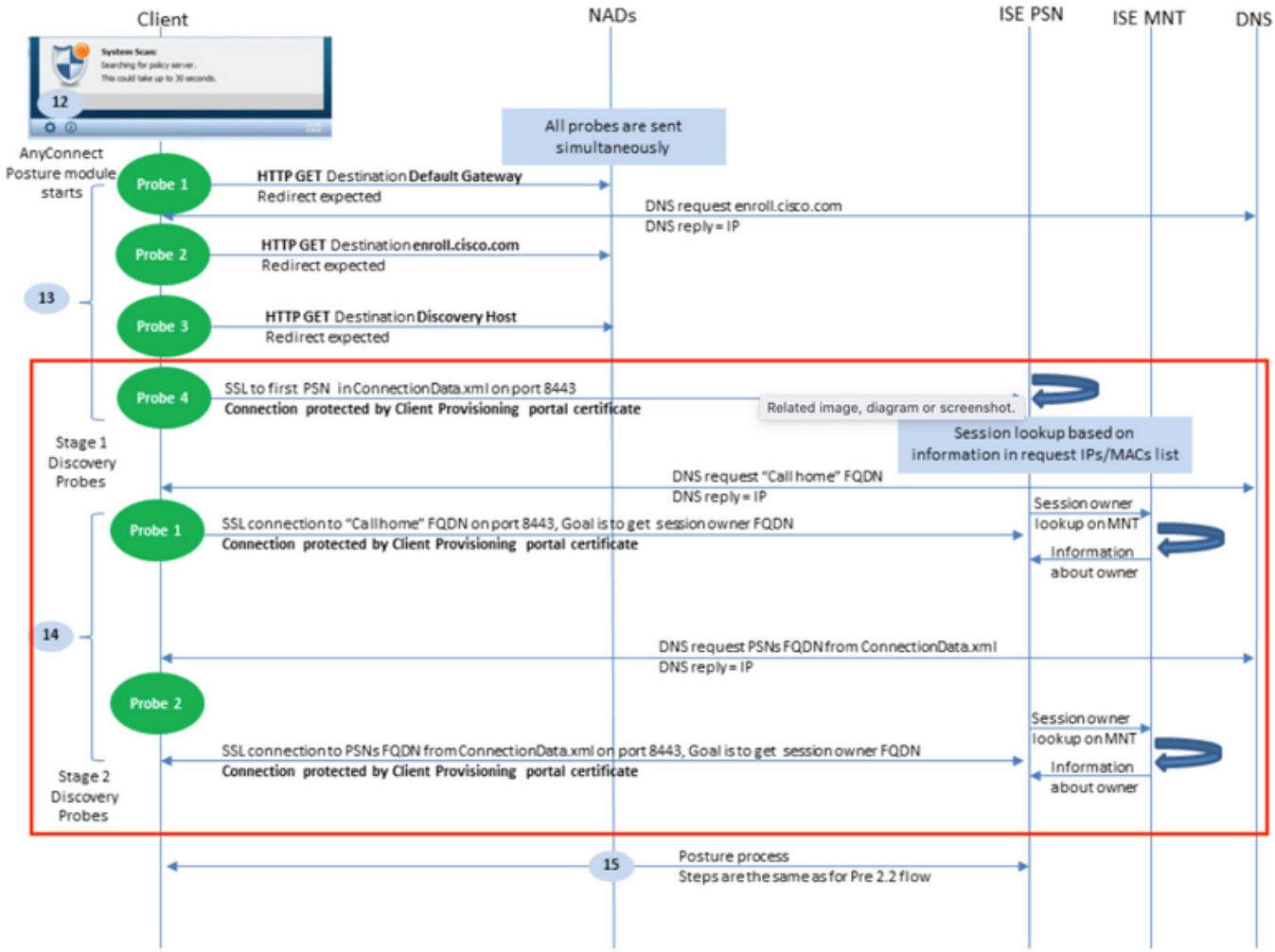
在涉及負載均衡器的部署中，必須確保在對以前的用例進行更改後，會話會繼續到達同一個PSN。在此步驟列出的版本/修補程式之前，狀態狀態不會通過輕量資料分佈（以前為Light Session Directory）在節點之間複製。 因此，不同的PSN可以返回不同的狀態狀態結果。

如果未正確配置永續性，重新身份驗證的會話可能會轉到與最初使用的PSN不同的PSN。如果發生這種情況，新PSN可以將會話合規性狀態標籤為未知，並使用重定向訪問控制清單(ACL)/URL傳遞authZ結果並限制終端訪問。同樣，安全狀態模組不會識別此更改並且不會觸發探測。

有關如何配置負載平衡器的詳細資訊，請參閱Cisco & F5部署指南：使用BIG-IP的ISE負載平衡。它提供負載平衡環境中ISE部署的最佳實踐設計的高級概述和F5特定配置。

使用案例5 — 第2階段發現探測由不同的伺服器響應，而不是通過驗證客戶端（Pre 2.6 Patch 6、2.7 Patch 2和3.0）。

請檢視此圖中的紅色框中的探測器。



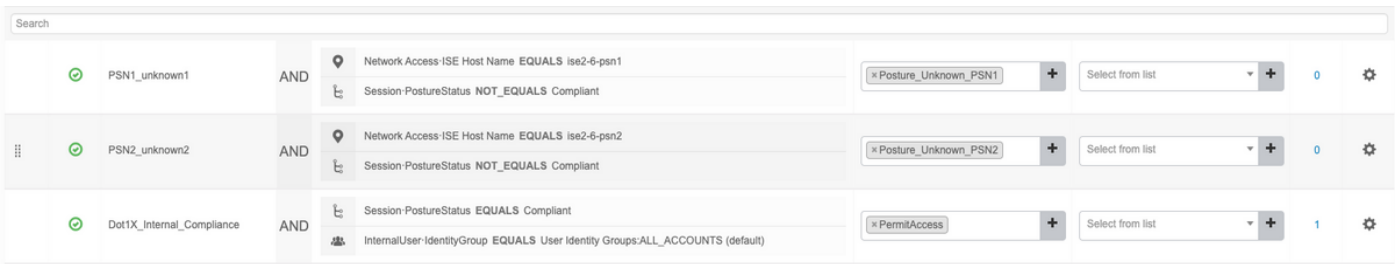
PSN會將會話資料儲存五天，因此，即使客戶端不再使用該節點進行身份驗證，「相容」會話的會話資料有時仍會保留在原始PSN上。如果包含在紅色方框中的探測器由除當前驗證會話的PSN之外的PSN響應，並且PSN先前擁有並標籤了此終結點相容，則終結點上的狀態模組的狀態與當前驗證PSN之間可能存在不匹配。

以下是可能發生這種不相符的幾種常見情況：

- 終端從網路斷開時，不會收到該終端的記帳停止。
- NAD從一個PSN故障切換到另一個PSN。
- 負載均衡器將身份驗證轉發到同一端點的不同PSN。

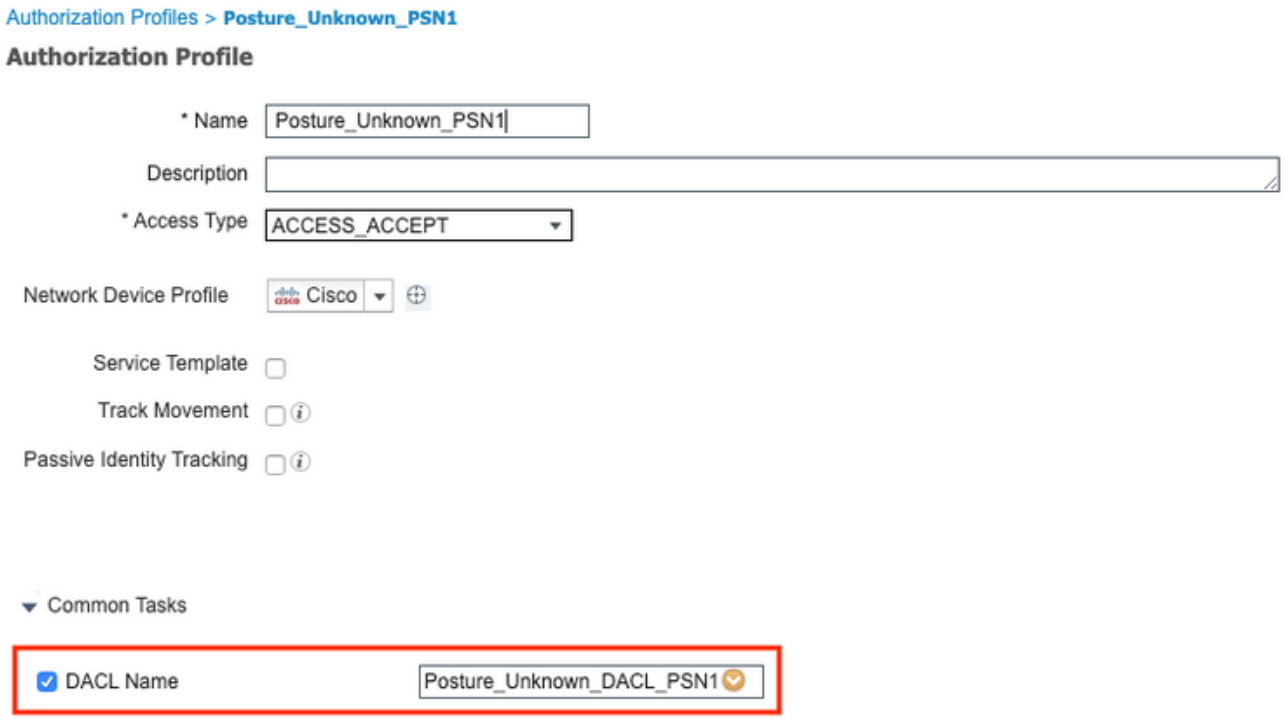
為了防止此行為，可以將ISE配置為僅允許來自特定端點的發現探測到達其當前身份驗證到的PSN。為此，請為部署中的每個PSN配置不同的授權策略。在這些策略中，引用包含可下載訪問控制清單(DACL)的其他authZ配置檔案，DACL僅允許對authZ條件中指定的PSN進行探測。請參閱以下範例：

每個PSN將具有未知狀態狀態的規則：

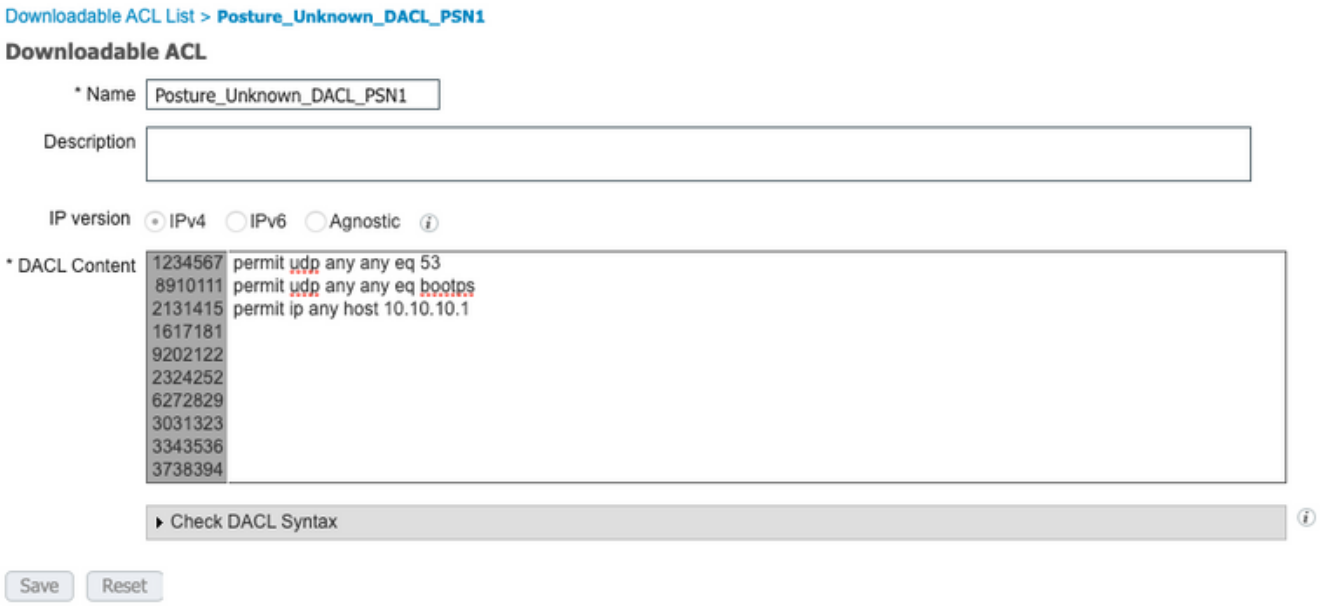


每個配置檔案引用不同的DACL。

附註：對於無線，請使用Airespace ACL。



每個DACL僅允許對處理身份驗證的PSN進行探測訪問。



在上一個示例中，10.10.10.1是PSN 1的IP地址。所引用的DACL可以根據需要更改任何其他服務/IP，但應限制僅訪問處理身份驗證的PSN。

2.6補丁6、2.7補丁2和3.0後的行為更改

狀態已通過光資料分發框架新增到RADIUS會話目錄中。每次在任何PSN上收到狀態更新時，都會

將其複製到部署中的所有PSN。此更改生效後，到達不同PSN的身份驗證和/或探測器對於不同身份驗證的影響將被刪除，並且任何PSN都應該能夠回覆所有端點，無論它們當前是在何處進行身份驗證。

在本文檔的五個使用案例中，請考慮以下行為：

使用案例1 — 客戶端重新身份驗證會強制NAD生成新的會話ID。使用者端仍符合要求，但由於重新驗證，NAD處於重新導向狀態（重新導向URL和存取清單）。

— 此行為不會改變，此配置仍應在ISE和NAD上實施。

使用案例2 — 交換機配置為MAB DOT1X和優先順序DOT1X MAB（有線）。

— 此行為不會改變，此配置仍應在ISE和NAD上實施。

使用案例3 — 無線客戶端漫遊和不同AP的身份驗證將轉至不同的控制器。

— 此行為不會改變，此配置仍應在ISE和NAD上實施。

使用案例4 — 具有負載平衡器的部署。

— 仍應遵循負載平衡指南中定義的最佳做法，但是如果負載平衡器將身份驗證轉發到不同的PSN，則應將正確的狀態狀態返回到客戶端。

使用案例5 — 第2階段發現探測由不同的伺服器響應，而不是使用驗證客戶端

— 這不應是新行為的問題，每個PSN的授權配置檔案也不必要。

維護同一SessionID時的注意事項

使用本文檔中列出的方法時，保持網路連線的使用者可能會在很長一段時間內保持合規狀態。即使他們重新進行身份驗證，會話ID也不會更改，因此ISE將繼續為其與合規狀態匹配的規則傳遞身份驗證結果。

在這種情況下，需要配置定期重新評估，以便要求終端安全評估以確保終端在定義的間隔內保持符合公司策略。

可在Work Centers > Posture > Settings > Ressesment configurations下配置此功能。