ISEポスチャ導入のベストプラクティスと考慮事項

内容

概要

このドキュメントでは、リダイレクトベースのポスチャを使用するいくつかの使用例に対処するベースライン設定について説明します。これらの設定では、クライアントは準拠していますが、ネットワークアクセスデバイス(NAD)はリダイレクト状態であるため、アクセスを制限します。

制約事項

このドキュメントの設定はCisco NADに対して機能しますが、必ずしもサードパーティのNADに対しては機能しません。

ポスチャクライアントの動作

ポスチャクライアントは、次のタイミングでプローブをトリガーします。

- 初期ログイン
- レイヤ3(L3)の変更/ネットワークインターフェイスカード(NIC)の変更（新しいIPアドレス、NICの状態変更）

使用例

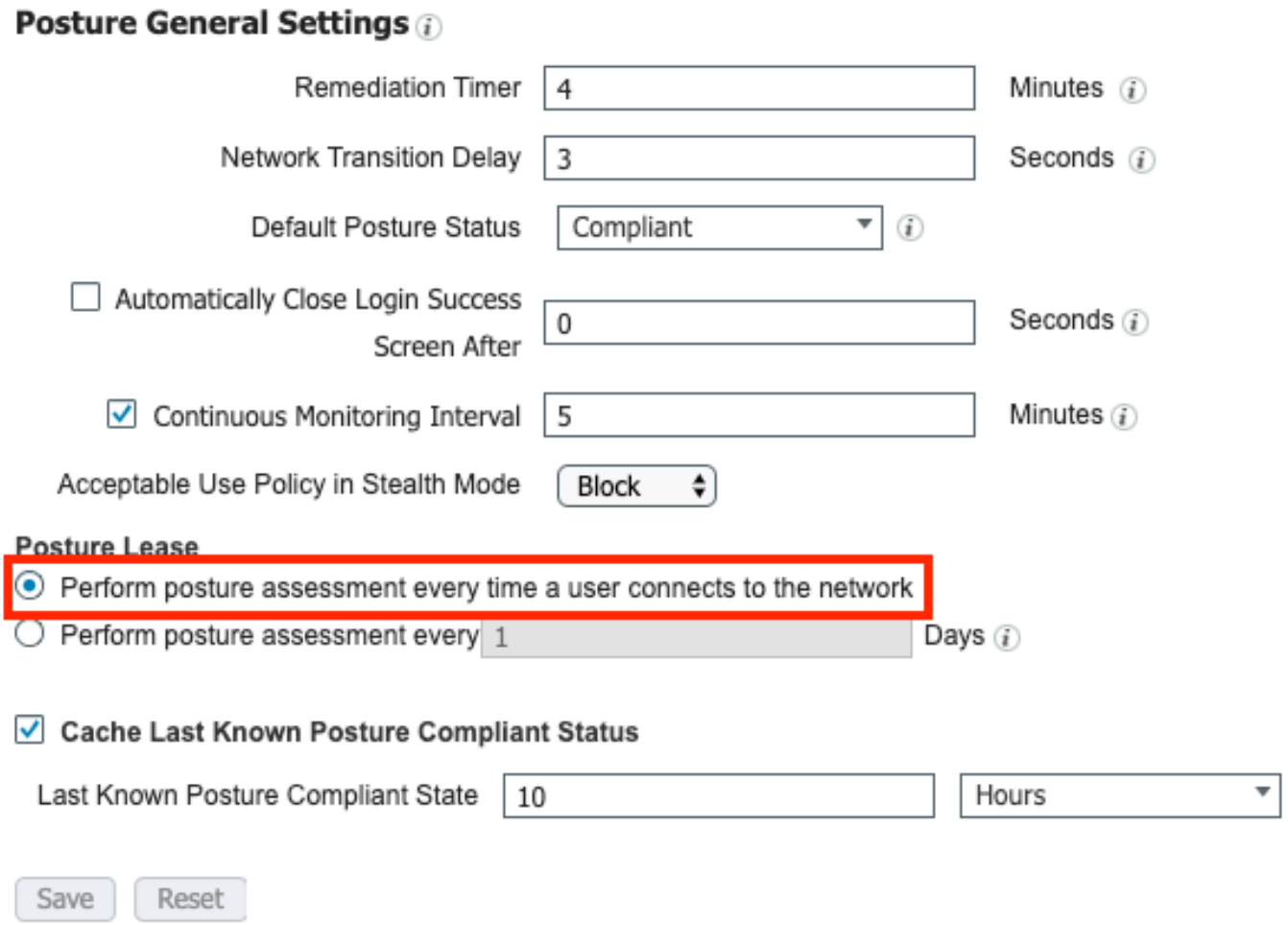
使用例1：クライアント再認証により、NADは新しいセッションIDを生成します。

この使用例では、クライアントは依然として準拠していますが、再認証が行われるため、NADは

リダイレクト状態（リダイレクトURLとアクセスリスト）になります。

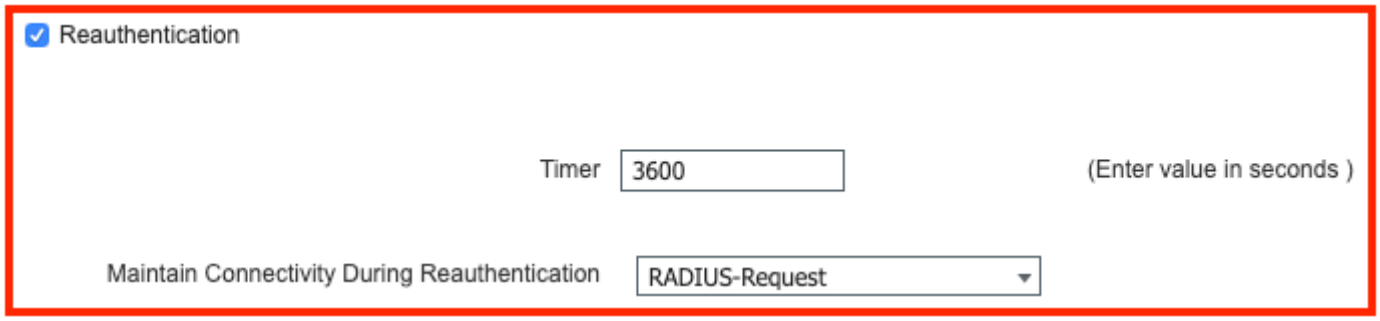
デフォルトでは、Identity Services Engine(ISE)は、ネットワークに接続するたびにポスチャ評価を実行するように設定されます。特に、新しいセッションごとに実行されます。

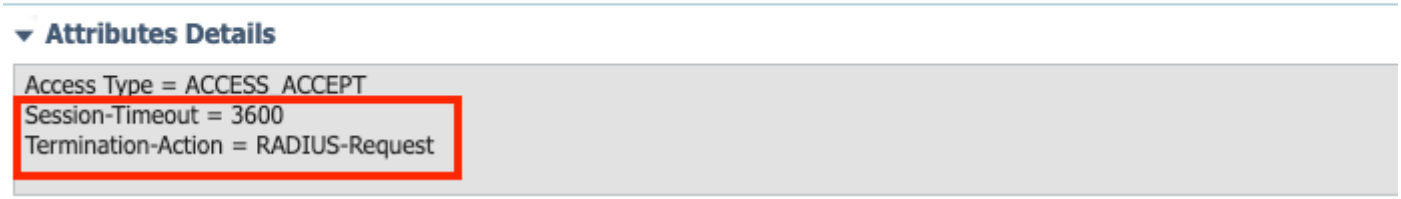
この設定は、[Work Centers] > [Posture] > [Settings] > [Posture General Settings]で設定します。



再認証時にNADが新しいセッションIDを生成しないように、認可プロファイルでこれらの再認証値を設定します。表示される再認証タイマーは標準的な推奨事項ではなく、再認証タイマーは接続タイプ（無線/有線）、設計（ロードバランサの持続性ルール）などに基づいて導入ごとに考慮する必要があります。

[Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles]





スイッチでは、ISEから再認証タイマーを取得するために、各インターフェイスまたはテンプレートを設定する必要があります。

```
authentication timer reauthenticate server
```

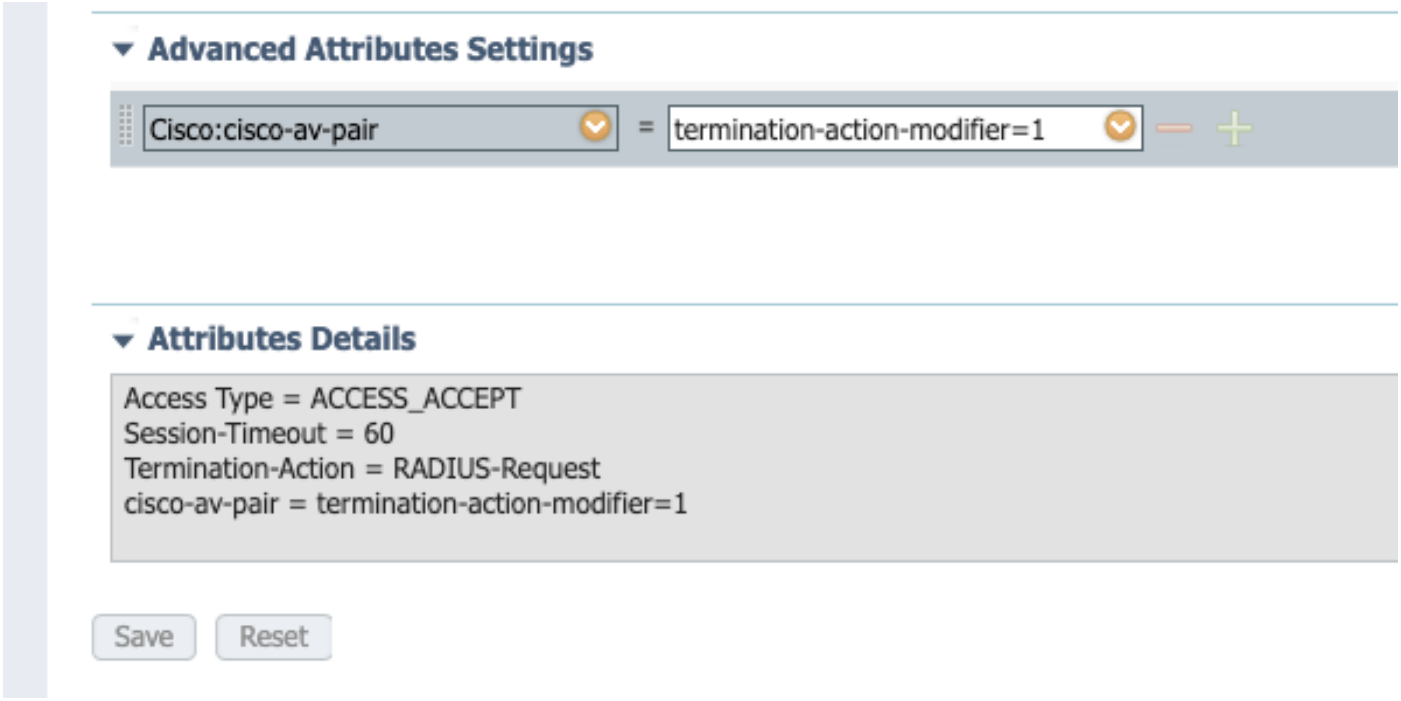
> **注**：ロードバランサがある場合は、再認証が元のポリシーサービス(PSN)に戻るように永続性が設定されていることを確認する必要があります。

使用例2：スイッチは、MAB DOT1XとプライオリティDOT1X MAB（有線）の順に設定されます。

この場合、再認証中にMAC認証バイパス(MAB)が試行されると、802.1xセッションのアカウンティング停止が送信されるため、再認証は終了します。

- クライアントのユーザ名が802.1Xのユーザ名からMABのユーザ名に変更されるため、MABプロセスに送信されるアカウンティング停止は正しいです。
- 認証方式がdot1xであるため、アカウンティング停止時のmethod-idであるdot1xも正しいです。
- Dot1xメソッドが成功すると、method-idをdot1xとしてアカウンティング開始を送信します。ここでも、この動作は予想どおりです。

この問題を解決するには、エンドポイントが準拠している場合に使用するauthZプロファイルにcisco-av-pair:termination-action-modifier = 1を設定します。この属性値(AV)ペアは、設定された順序に関係なく、NADが元の認証で選択された方式を再利用することを指定します。



使用例3：異なるAPのワイヤレスクライアントのローミングと認証は、異なるコントローラに行われます。

この状況では、ローミングのために他のAPに到達できるアクセスポイント(AP)が同じアクティブコントローラを使用するように、ワイヤレスネットワークを設計する必要があります。たとえば、ワイヤレスLANコントローラ(WLC)ステートフルスイッチオーバー(SSO)フェールオーバーです。WLCのハイアベイラビリティ(HA)SSOの詳細については、『ハイアベイラビリティ(SSO)導入ガイド』を参照してください。

使用例4 – ロードバランサ（2.6より前のパッチ6、2.7パッチP2、および3.0）を使用した導入

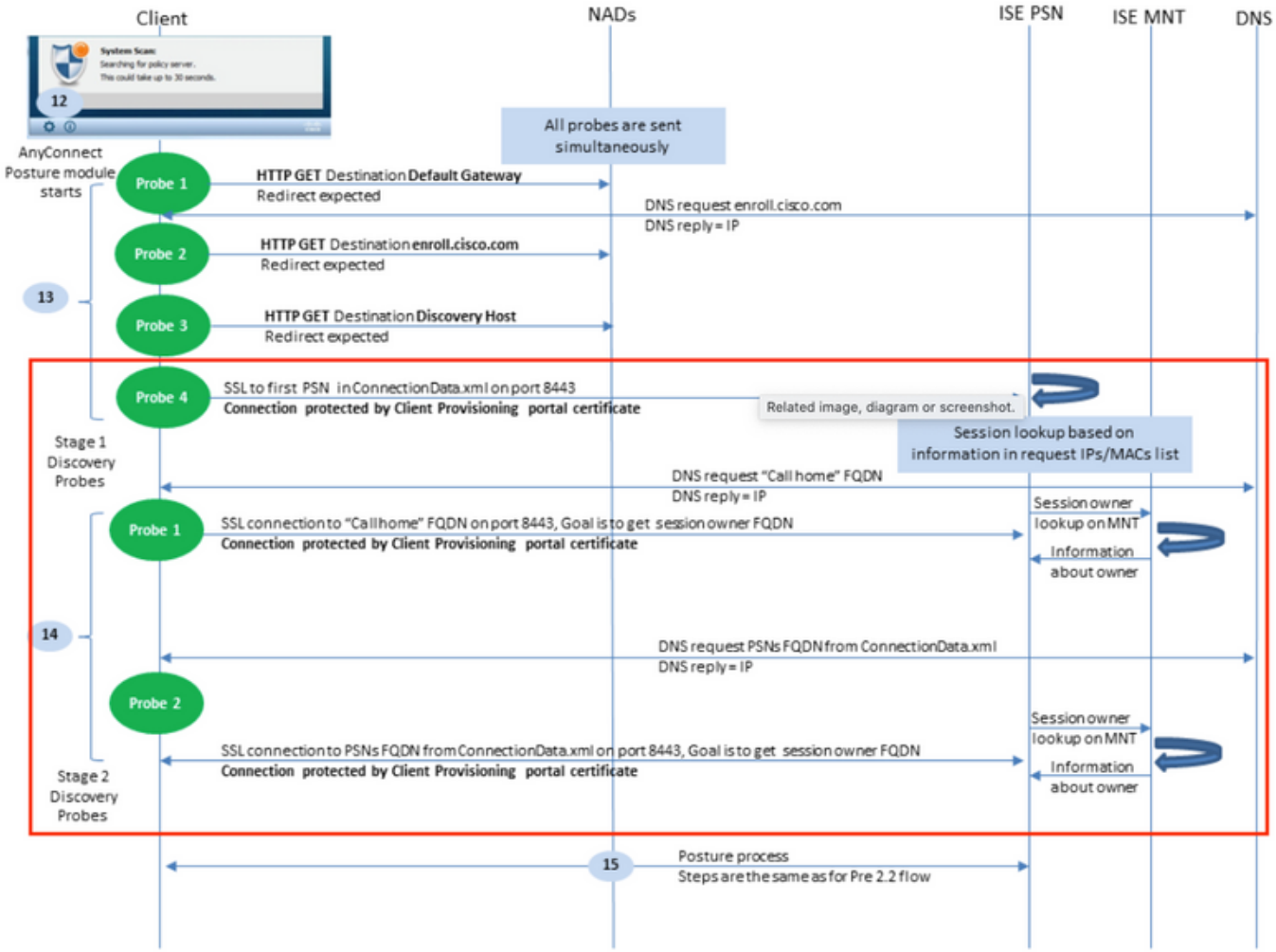
ロードバランサが関係する展開では、以前のユースケースで変更を加えた後も、セッションが同じPSNに移動し続けることを確認することが重要です。このステップでリストされているバージョン/パッチより前は、ポスチャステータスはLight Data Distribution（以前のLight Session Directory）を介してノード間で複製されません。 このため、異なるPSNが異なるポスチャステータス結果を返す可能性があります。

永続性が正しく設定されていない場合、再認証されるセッションは、最初に使用されたセッションとは異なるPSNに到達する可能性があります。この場合、新しいPSNはセッションコンプライアンスステータスをunknownとマークし、redirect access control list（ACL；リダイレクトアクセスコントロールリスト）/URLでauthZの結果を渡し、エンドポイントのアクセスを制限できます。ここでも、NADのこの変更はポスチャモジュールによって認識されず、プローブはトリガーされません。

ロードバランサの設定方法の詳細については、『Cisco & F5 Deployment Guide:BIG-IPを使用したISEロードバランシング。ロードバランシング環境でのISE導入のベストプラクティス設計の概要とF5固有の設定を示します。

使用例5 – ステージ2検出プローブは、クライアントが認証されている（2.6より前のパッチ6、2.7パッチ2、および3.0）とは異なるサーバによって応答されます。

次の図の赤いボックス内のプローブを確認します。



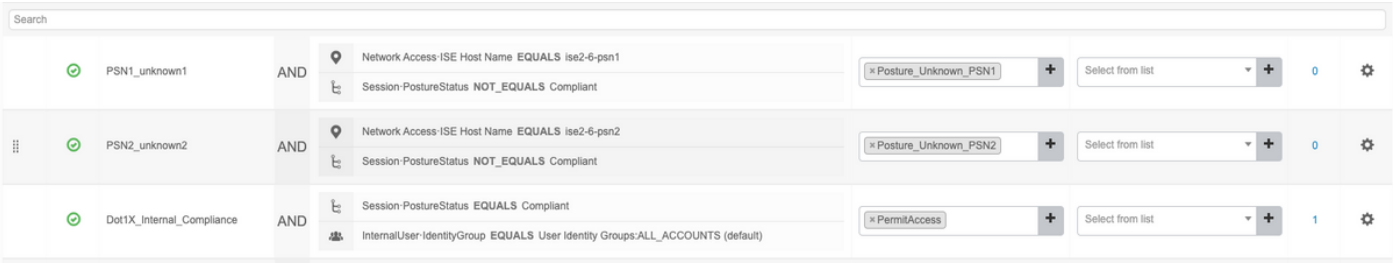
PSNは5日間セッションデータを保存するため、クライアントがそのノードで認証を行わなくなった場合でも、「準拠」セッションのセッションデータが元のPSNに残っている場合があります。赤いボックスに囲まれたプローブが、現在セッションを認証しているPSN以外のPSNによって応答され、PSNが以前にこのエンドポイントを所有してマークしている場合、エンドポイントのポスチャモジュールのポスチャステータスと現在の認証PSNがの間不一致があります。

この不一致が発生する可能性がある一般的なシナリオを次に示します。

- エンドポイントがネットワークから切断されても、エンドポイントに対するアカウンティング停止は受信されません。
- NADは、あるPSNから別のPSNにフェールオーバーしました。
- ロードバランサは、同じエンドポイントの異なるPSNに認証を転送します。

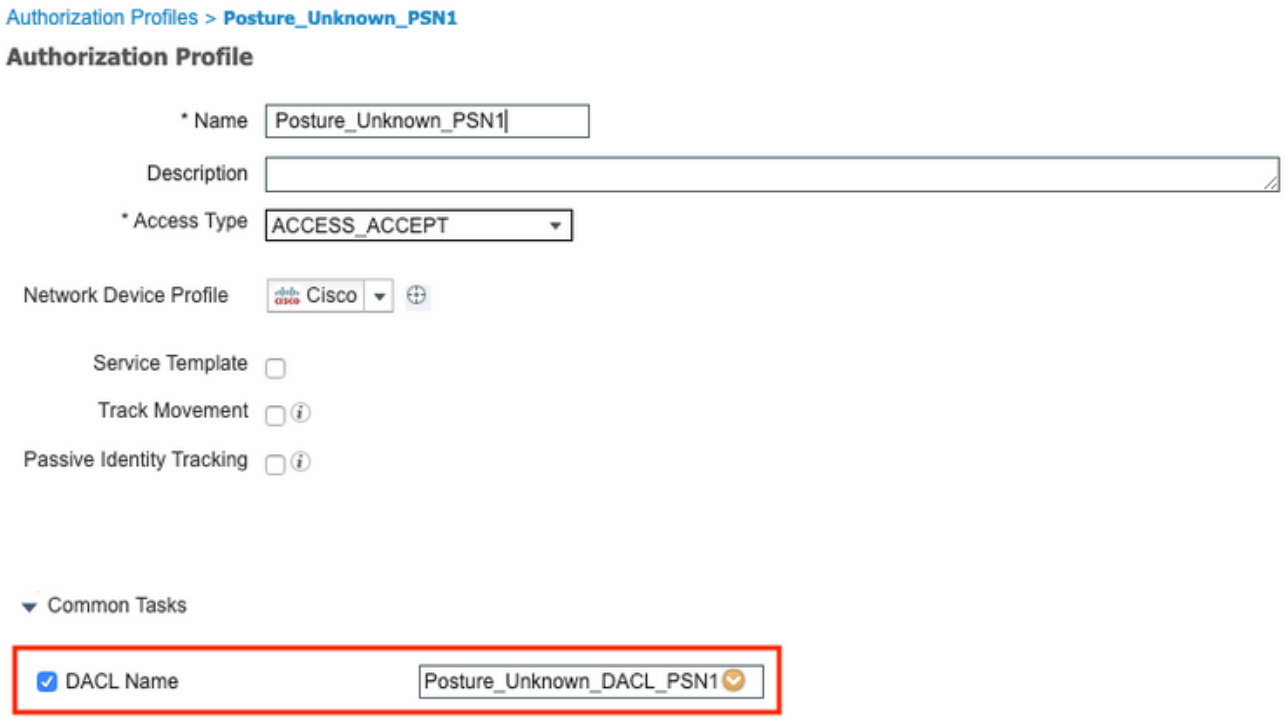
この動作から保護するために、ISEは、特定のエンドポイントからの検出プローブが、現在認証されているPSNに到達することを許可するように設定できます。これを実現するには、展開内の各PSNに異なる認可ポリシーを設定します。これらのポリシーでは、authZ条件で指定されたPSNのみにプローブを許可するDownloadable Access Control List(DACL)を含む別のauthZプロファイルを参照します。次の例を参照してください。

各PSNには、不明なポスチャステータスのルールがあります。

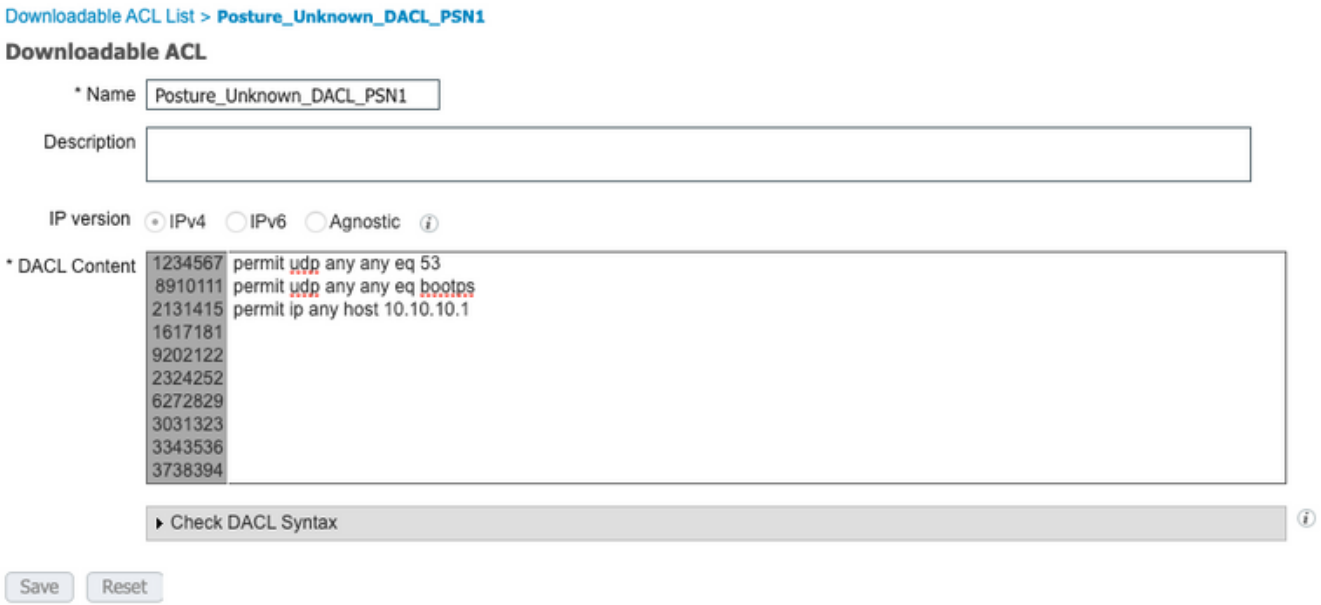


各プロファイルは異なるDACLを参照します。

注：ワイヤレスの場合は、Airespace ACLを使用します。



各DACLは、認証を処理するPSNへのプローブアクセスのみを許可します。



前の例では、10.10.10.1はPSN 1のIPアドレスです。参照されるDACLは、必要に応じて追加のサービス/IPに対して変更できますが、アクセスを認証を処理するPSNのみに制限する必要があります。

2.6パッチ6、2.7パッチ2、3.0以降の動作変更

ポスチャステータスは、Light Data Distribution(LDS)フレームワークを介してRADIUSセッションディレクトリに追加されました。ポスチャステータスの更新が任意のPSNで受信されるたびに、展開のすべてのPSNに複製されます。この変更が有効になると、異なる認証で異なるPSNに到達する認証やプローブの影響が削除され、すべてのPSNは、現在認証されている場所に関係なく、すべてのエンドポイントに応答できるようになります。

このドキュメントの5つの使用例では、次の動作を考慮します。

使用例1：クライアント再認証により、NADは新しいセッションIDを生成します。クライアントは引き続き準拠していますが、再認証が行われるため、NADはリダイレクト状態（リダイレクトURLとアクセスリスト）になります。

– この動作は変更されず、この設定はISEとNADに実装する必要があります。

使用例2：スイッチは、MAB DOT1XとプライオリティDOT1X MAB（有線）の順に設定されます。

– この動作は変更されず、この設定はISEとNADに実装する必要があります。

使用例3：異なるAPのワイヤレスクライアントのローミングと認証は、異なるコントローラに行われます。

– この動作は変更されず、この設定はISEとNADに実装する必要があります。

使用例4 – ロードバランサを使用した導入

– ロードバランシングガイドで定義されているベストプラクティスに従う必要がありますが、認証がロードバランサによって異なるPSNに転送される場合は、正しいポスチャステータスをクライアントに返す必要があります。

使用例5 – ステージ2検出プローブは、クライアントが認証されたサーバとは別のサーバによって応答されます。

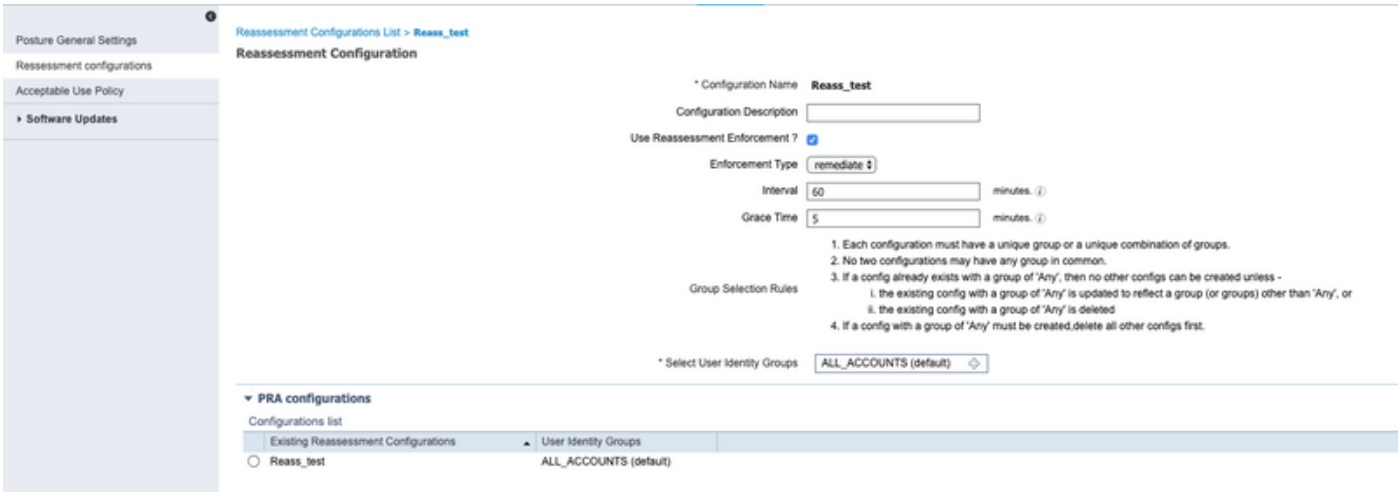
– これは新しいベアラに関する問題ではなく、PSNごとの認可プロファイルは不要です。

同じセッションIDを維持する場合の考慮事項

このドキュメントに記載されている方法を使用すると、ネットワークに接続されたままのユーザは、長期的に準拠している可能性があります。再認証されても、sessionIDは変更されないため、ISEは準拠ステータスに一致するルールのAuthZ結果を引き続き渡します。

この場合、エンドポイントが定義された間隔で企業ポリシーに準拠していることを確認するためにポスチャが必要になるように、定期的再評価を設定する必要があります。

これは、[Work Centers] > [Posture] > [Settings] > [Ressement configurations]で設定できます。


Posture General Settings
Ressessment configurations
Acceptable Use Policy
Software Updates
Reassessment Configurations List > Reass_test
Reassessment Configuration
* Configuration Name
Reass_test
Configuration Description
Use Reassessment Enforcement ?
Enforcement Type
remediate
Interval
60
minutes.
Grace Time
5
minutes.
Group Selection Rules
1. Each configuration must have a unique group or a unique combination of groups.
2. No two configurations may have any group in common.
3. If a config already exists with a group of 'Any', then no other configs can be created unless -
i. the existing config with a group of 'Any' is updated to reflect a group (or groups) other than 'Any', or
ii. the existing config with a group of 'Any' is deleted
4. If a config with a group of 'Any' must be created,delete all other configs first.
* Select User Identity Groups
ALL_ACCOUNTS (default)
PRA configurations
Configurations list
Existing Reassessment Configurations
User Identity Groups
Reass_test
ALL_ACCOUNTS (default)