نشر وضع ISE

المحتويات

المقدمة

قيود

سلوك عميل الوضع

حالات الاستخدام

- أستخدم الحالة 1 - تفرض إعادة مصادقة العميل NAD لإنشاء معرف جلسة جديد
- استخدام الحالة 2 - يتم تكوين المحول باستخدام الأمر MAB DOT1x والأولوية DOT1x MAB (سلكي)
- استخدام الحالة 3 - تنقل العملاء اللاسلكيين والمصادقة على نقاط الوصول المختلفة إلى وحدات تحكم مختلفة
- استخدام الحالة 4 - عمليات النشر باستخدام وحدات موازنة الأحمال (حزمة تصحيح 6 من النوع PRE 2.6 و 2.7 Patch P2 و 3.0)
- استخدام الحالة 5 - المرحلة 2 من استعلامات الاكتشاف التي يتم الاستجابة لها بواسطة خادم مختلف عن العميل الذي تتم مصادقته (حزمة تصحيح 6 مسبقا 2.6 و 2.7 ومجموعة تصحيح 2 و 3.0)

Behavior Change Post 2.6 Patch 6 و 2.7 Patch 2 و 3.0

الاعتبارات عند الاحتفاظ بنفس معرف جلسة العمل

المقدمة

يصف هذا وثيقة بعض خط أساسي تشكيل أن يتناول عدة حالات إستخدام مع حالة مبنية على إعادة توجيه.

قيود

تعمل التكوينات الواردة في هذا المستند لأجهزة Cisco NAD، ولكن ليس بالضرورة لأجهزة NAD من إنتاج جهات أخرى.

سلوك عميل الوضع

يمكن لعميل الوضع تشغيل المسابير في هذه الأوقات:

- تسجيل الدخول الأولي
- تغيير طبقة 3 (L3)/تغيير بطاقة واجهة الشبكة (NIC) (عنوان IP جديد، تغيير حالة NIC)

حالات الاستخدام

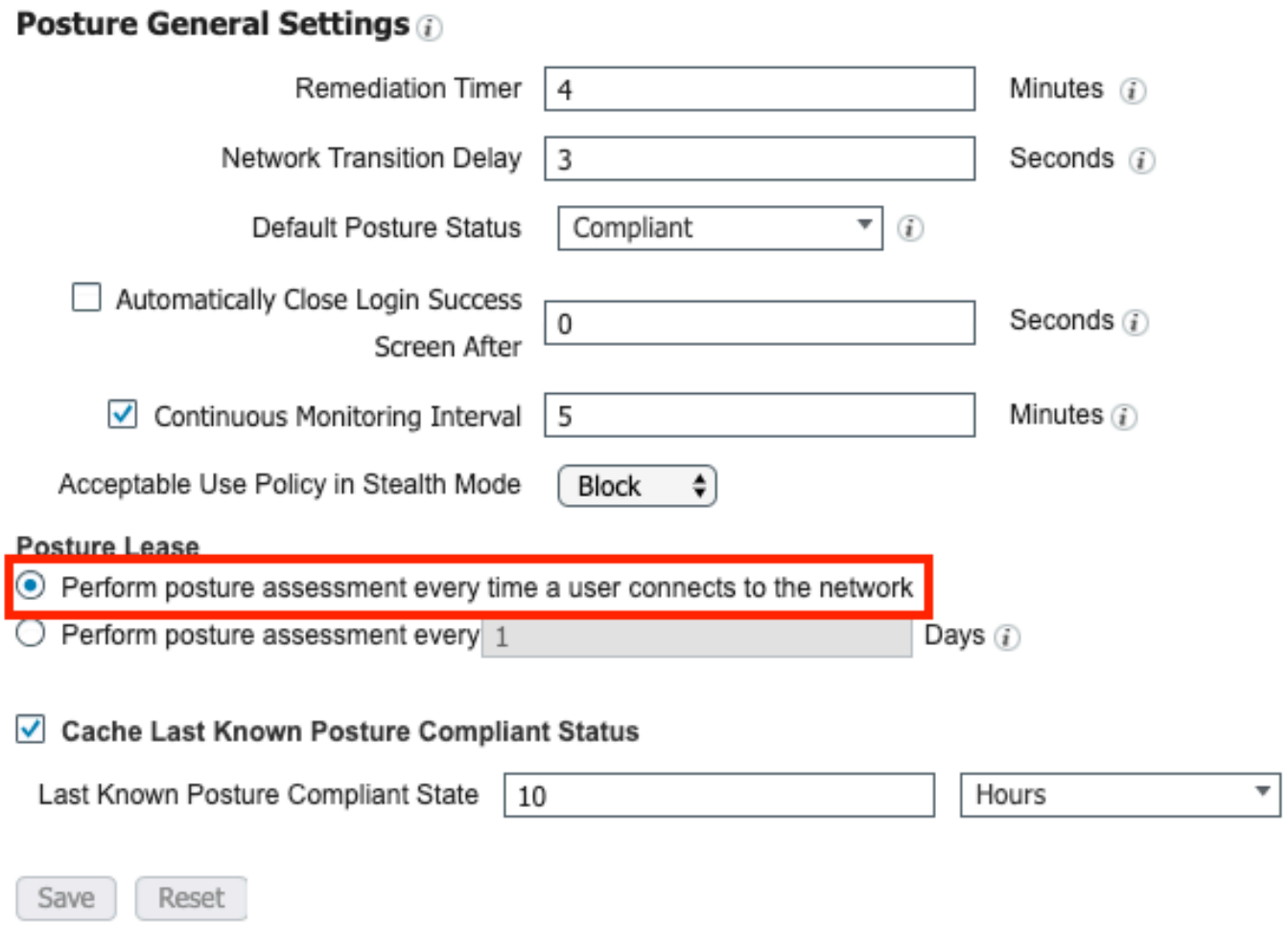
أستخدم الحالة 1 - تفرض إعادة مصادقة العميل NAD لإنشاء معرف جلسة جديد

في حالة الاستخدام هذه، لا يزال العميل متوافقا، ولكن بسبب إعادة المصادقة، يكون NAD

في حالة إعادة التوجيه (عنوان URL وقائمة الوصول المعاد توجيههما).

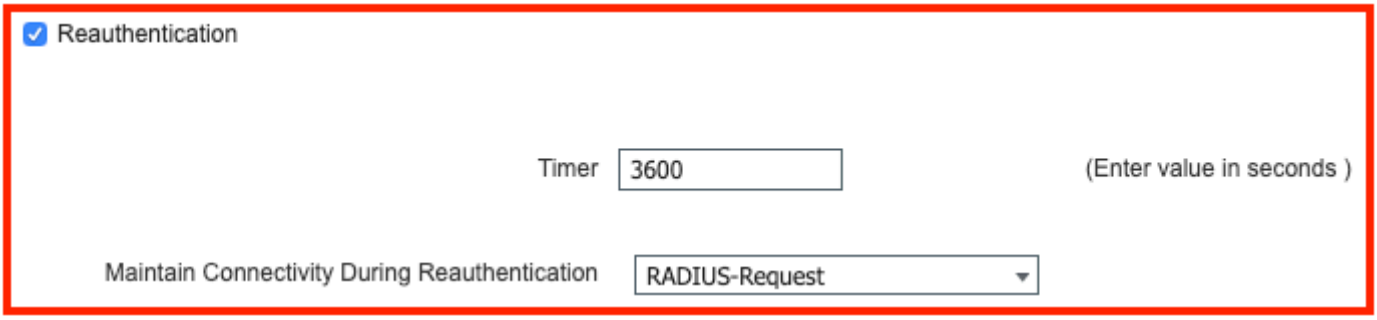
وبشكل افتراضي، يتم تكوين محرك خدمات الهوية (ISE) لإجراء تقييم للوضع في كل مرة يتصل فيها بالشبكة، وبشكل أكثر تحديدا لكل جلسة عمل جديدة.

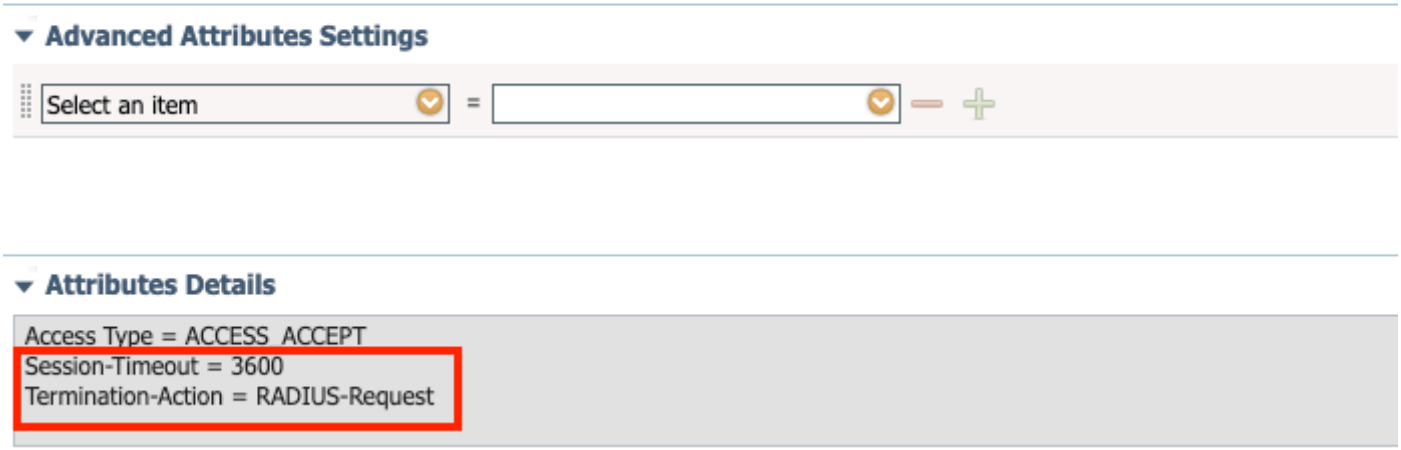
يتم تكوين هذا الإعداد ضمن مراكز العمل > الوضع > الإعدادات > الإعدادات العامة للوضع.



لمنع NAD من إنشاء معرف جلسة جديد على إعادة المصادقة، قم بتكوين قيم إعادة المصادقة هذه في ملف تعريف التخويل. وحدة توقيت إعادة المصادقة المعروضة ليست توصية قياسية وتأخذ في الاعتبار وحدات توقيت إعادة المصادقة لكل عملية نشر استنادا إلى نوع الاتصال (السلكي/سلكي) والتصميم (ما هي قواعد الاستمرار على موازن التحميل) وما إلى ذلك.

السياسة > عناصر السياسة > النتائج > التخويل > توصيفات التخويل





في المحولات، يلزمك تكوين كل واجهة، أو قالب، للحصول على مؤقت إعادة المصادقة الخاص بها من ISE.

```
authentication timer reauthenticate server
```

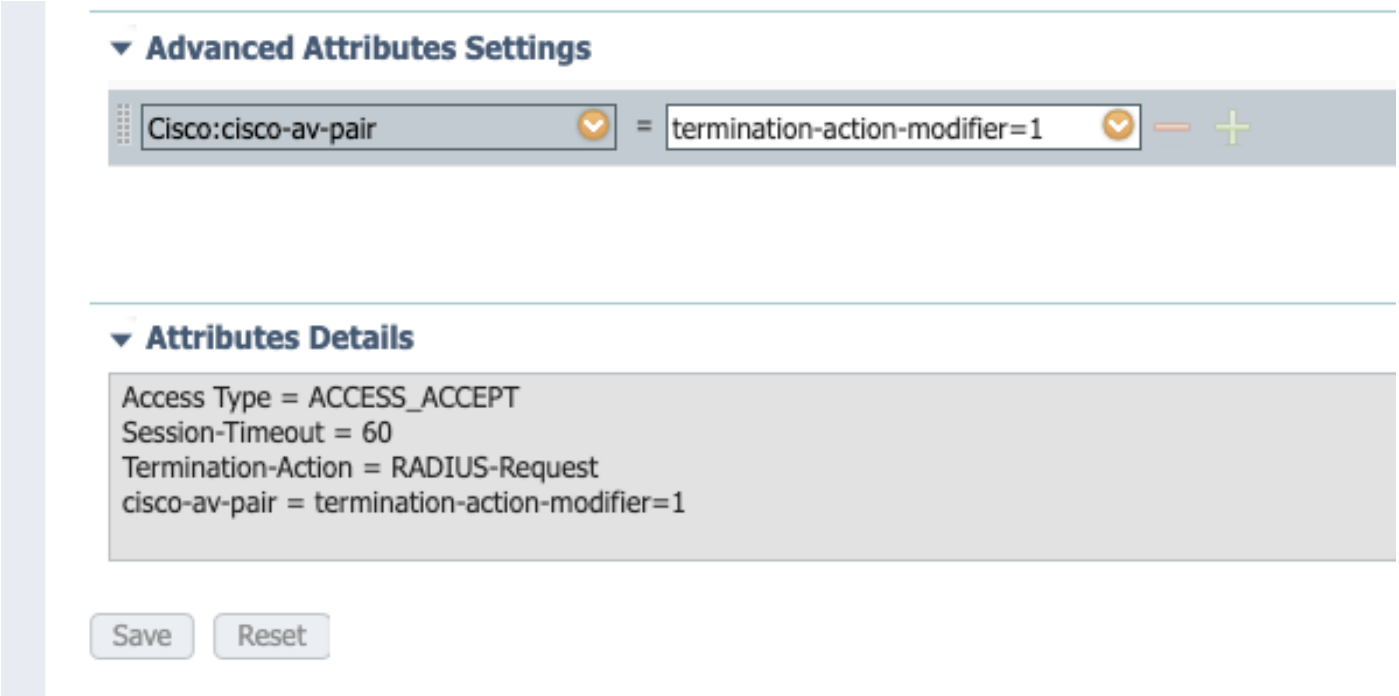
> ملاحظة: في حالة وجود موازن حمل، تحتاج إلى التأكد من تكوين الاستمرارية بطريقة يمكن بها إرجاع عمليات إعادة المصادقة إلى خدمة النهج الأصلية (PSN).

إستخدام الحالة 2 - يتم تكوين المحول باستخدام الأمر MAB DOT1x والأولوية DOT1x MAB (سلكي)

في هذه الحالة، reauthentication يستطيع كنت أنهيت لأن حساب توقف ل 802.1x جلسة يستطيع كنت أرسلت عندما ماك صحة هوية مجرى جانبي (MAB) حاولت أثناء reauthentication.

- نقطة توقف المحاسبة التي يتم إرسالها لعملية MAB عند فشل المصادقة صحيحة، حيث يتغير اسم المستخدم للعميل من اسم مستخدم 802.1X إلى اسم مستخدم MAB.
- Dot1x كمعرف الأسلوب في توقف المحاسبة صحيح أيضا حيث أن طريقة التخويل كانت dot1x.
- عندما تنجح طريقة Dot1x، فإنها ترسل بداية محاسبة بمعرف الأسلوب على هيئة dot1x. وهنا أيضا، هذا السلوك هو كما هو متوقع.

لحل هذه المشكلة، قم بتكوين Cisco-av-pair:termination-action-modifier=1 على ملف تعريف AuthZ المستخدم عندما تكون نقطة النهاية متوافقة. يحدد زوج قيمة السمة (AV) هذا أن NAD يعيد إستخدام الطريقة المختارة في المصادقة الأصلية بغض النظر عن الأمر الذي تم تكوينه.



إستخدام الحالة 3 - تنقل العملاء اللاسلكيين والمصادقة على نقاط الوصول المختلفة إلى وحدات تحكم مختلفة

في هذه الحالة، يلزم تصميم الشبكة اللاسلكية بحيث تستخدم نفس وحدة التحكم النشطة لنقاط الوصول (APs) الواقعة ضمن نطاق الوصول إلى نقاط الوصول الأخرى للتجول. وأحد الأمثلة على ذلك هو تجاوز فشل نقل بيانات الحالة (SSO) لوحدة تحكم الشبكة المحلية اللاسلكية (WLC). للحصول على مزيد من المعلومات حول SSO (HA) عالية التوفر لمركز التحكم في الشبكة المحلية اللاسلكية (WLC)، راجع دليل نشر التوافر العالي (SSO).

إستخدام الحالة 4 - عمليات النشر باستخدام وحدات موازنة الأحمال (حزمة تصحيح 6 من النوع PRE 2.6 و 2.7 Patch P2 و 3.0)

في عمليات النشر التي تتضمن موازن التحميل، من المهم التأكد من أنه بعد إجراء التغييرات في حالات الاستخدام السابقة، تستمر الجلسات في الانتقال إلى نفس PSN. قبل الإصدار/برامج التصحيح المدرجة لهذه الخطوة، لا يتم نسخ حالة الوضع نسخا متماثلا بين العقد عبر توزيع البيانات الخفيفة (المعروف سابقا باسم دليل جلسة العمل الخفيفة). ولهذا السبب، من الممكن أن ترجع شبكات PSN المختلفة نتائج حالة الوضع المختلفة.

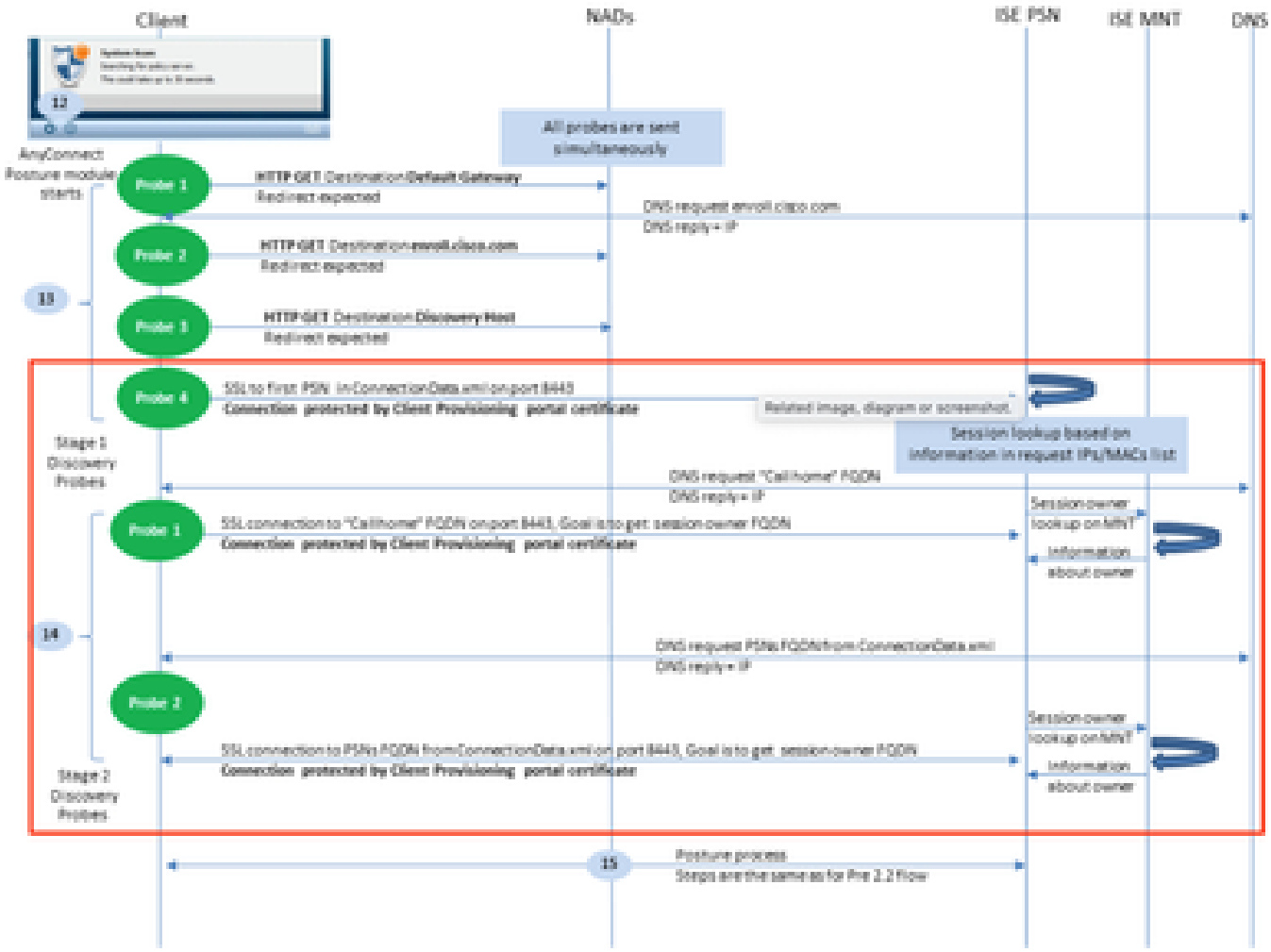
إن لا يشكل مثابرة يكون بشكل صحيح، جلسة أن reauthentication يستطيع ذهبت إلى PSN مختلف من أن كان استعملت أصلا. إذا حدث ذلك، فيمكن أن يقوم PSN الجديد بوضع علامة غير معروف على حالة توافق الجلسات وتمرير نتيجة المصادقة مع قائمة التحكم بالوصول المباشر (ACL)/URL والحد من الوصول إلى نقاط النهاية. مرة أخرى، لن يتم التعرف على هذا

التغيير في NAD بواسطة وحدة الوضع ولن يتم تشغيل المسابير.

للحصول على مزيد من المعلومات حول كيفية تكوين موازين التحميل، راجع دليل نشر Cisco & F5: موازنة حمل ISE باستخدام بروتوكول IP الكبير. وهو وجهة نظر عامة عالية المستوى وتهيئة خاصة بعامل F5 لتصميم أفضل الممارسات لعمليات نشر معيار ISE في بيئة متوازنة للتحميل.

إستخدام الحالة 5 - المرحلة 2 من استعلامات الاكتشاف التي يتم الاستجابة لها بواسطة خادم مختلف عن العميل الذي تم مصادقته (حزمة تصحيح 6 (3.0 و 2 حزمة تصحيح ومجموعة 2.7 و 2.6 مسبقا

ألق نظرة على المسابير ضمن المربع الأحمر في هذا الرسم التخطيطي..



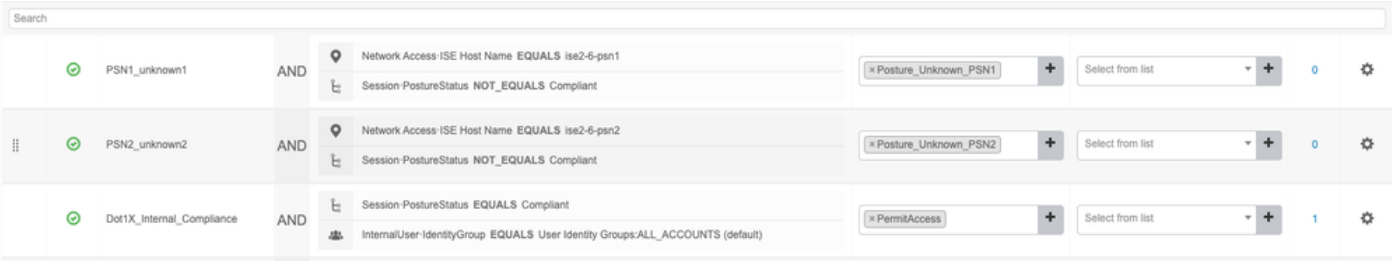
يخزن PSNs بيانات الجلسة لخمسة أيام، لذلك في بعض الأحيان بيانات الجلسة لجلسة عمل متوافق تبقى حية على PSN الأصلي حتى إذا لم يعد العميل يصدق مع أن عقدة. إذا تم الرد على المسابير الموجودة في المربع الأحمر بواسطة PSN آخر من الذي يصادق الجلسة حاليا وأن PSN قد امتلك من قبل وقام بوضع علامة متوافقة مع نقطة النهاية هذه، فمن الممكن أن يكون هناك عدم تطابق بين حالة الوضع للوحدة النمطية على نقطة النهاية و PSN الحالي الذي تم مصادقته.

فيما يلي بعض السيناريوهات الشائعة حيث يمكن أن يحدث عدم التطابق هذا:

- ال يتم تلقي توقف محاسبة لنقطة نهاية عند قطع إتصالها بالشبكة.
- فشل NAD من PSN إلى آخر.
- يقوم موازن التحميل بإعادة توجيه المصادقات إلى شبكات PSN مختلفة لنفس نقطة النهاية.

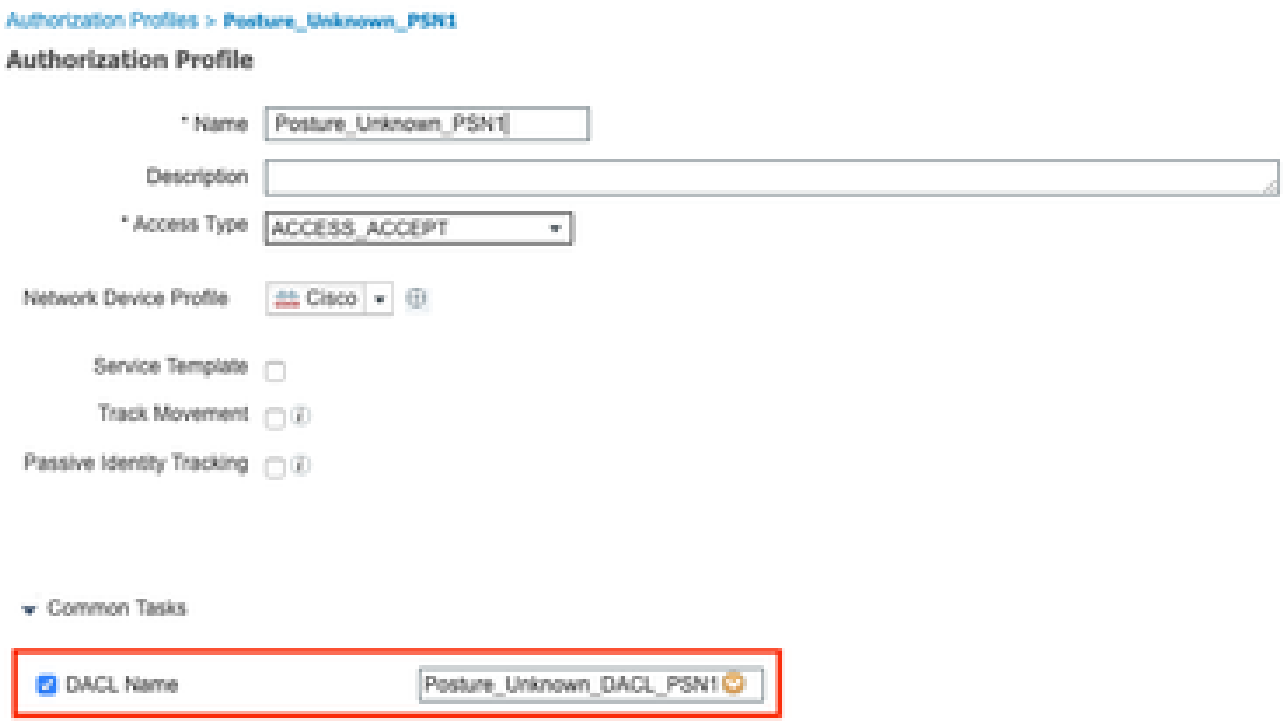
لحماية من هذا السلوك، يمكن تكوين ISE للسماح فقط باستكشافات الاكتشاف من نقطة نهاية معينة للوصول إلى PSN الذي تتم المصادقة عليه حاليا. للحصول على هذا الإجراء، قم بتكوين سياسة تفويض مختلفة لكل PSN في النشر الخاص بك. في هذه السياسات، راجع ملف تعريف مصادقة (AuthZ) مختلف يحتوي على قائمة تحكم في الوصول قابلة للتنزيل (DACL) التي تسمح بالبحث فقط إلى PSN المحدد في حالة AuthZ. راجع هذا المثال:

يحتوي كل PSN على قاعدة لحالة الوضع غير المعروف:

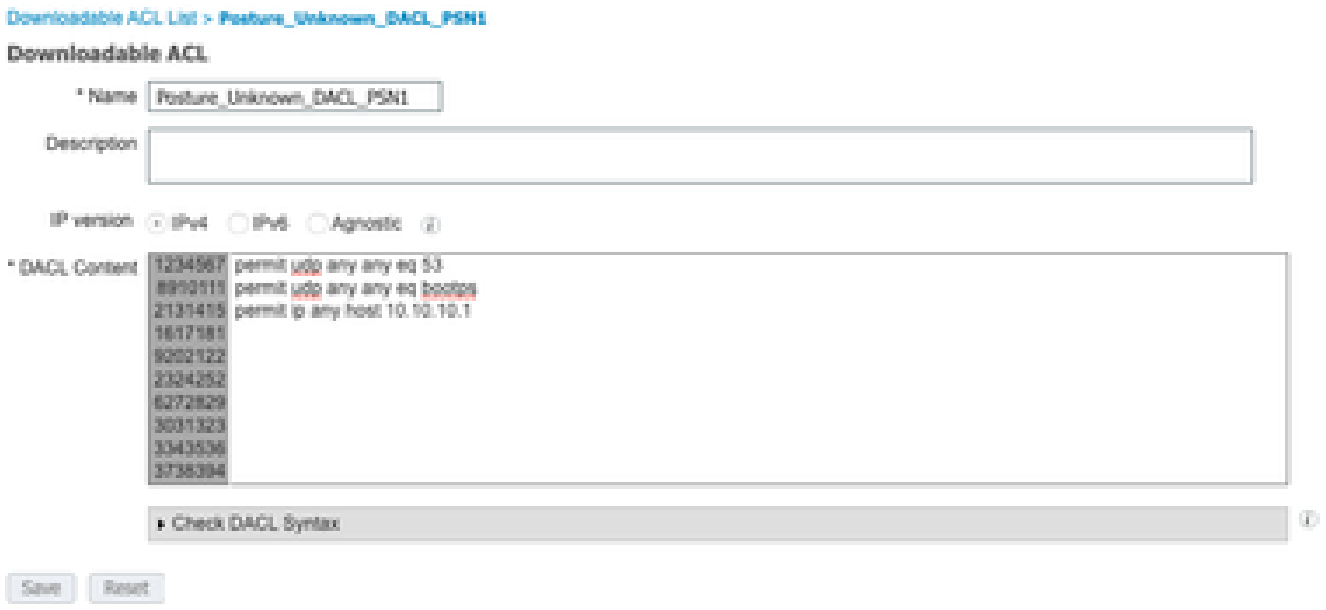


يشير كل ملف تخصيص منفرد إلى DACL مختلف.

ملاحظة: للاتصال اللاسلكي، أستخدم قوائم التحكم في الوصول (ACL) من Airespace.



ال تسمح كل قائمة تحكم في الوصول إلى البنية الأساسية (DACL) إلا بالوصول إلى PSN الذي يعالج المصادقة.



في المثال السابق، يمثل 10.10.10.1 عنوان IP الخاص ب PSN 1. يمكن تغيير قائمة التحكم في الوصول الخاصة بالمنفذ (DACL) المشار إليها لأي خدمات/IP إضافية حسب الحاجة، ولكنها تحد من الوصول إلى PSN الذي يتعامل مع المصادقة فقط.

Behavior Change Post 2.6 Patch 6 و 2.7 Patch 2 و 3.0

تمت إضافة حالة الوضع إلى دليل جلسة RADIUS من خلال إطار عمل توزيع البيانات الخفيفة. في كل مرة يتم تلقي تحديث حالة الوضع على أي PSN، يتم نسخه إلى جميع PSNs في النشر. ما إن يكون هذا تغيير سارٍ المفعول، أزلت التأثيرات من مصادقات و/أو مستكشفات أن يبلغ PSN مختلف على مصدقات مختلفة، وأي PSN يستطيع الرد على كل نقاط النهاية بغض النظر عن أين هي مصدق حاليا.

في حالات الاستخدام الخمسة في هذا المستند، ضع في الاعتبار هذه السلوكيات:

أستخدم الحالة 1 - تفرض إعادة مصادقة العميل NAD لإنشاء معرف جلسة جديد. لا يزال العميل متوافقا، ولكن بسبب إعادة المصادقة، فإن NAD في حالة إعادة التوجيه (عنوان URL وقائمة الوصول المعاد توجيهها).

- لا يتغير هذا السلوك وما يزال يمكن تنفيذ هذا التكوين على ISE و NADs.

أستخدم الحالة 2 - يتم تكوين المحول باستخدام الأمر MAB DOT1X والأولوية DOT1X MAB (سلكي).

- لا يتغير هذا السلوك وما يزال يمكن تنفيذ هذا التكوين على ISE و NADs.

أستخدم الحالة 3 - تنتقل عمليات التجوال الخاصة بالعملاء اللاسلكيين والمصادقة الخاصة بنقاط الوصول المختلفة إلى وحدات تحكم مختلفة.

- لا يتغير هذا السلوك وما يزال يمكن تنفيذ هذا التكوين على ISE و NADs.

إستخدام الحالة 4 - عمليات النشر باستخدام وحدات موازنة الأحمال.

- ال يزال من الممكن اتباع أفضل الممارسات المحددة في دليل موازنة الأحمال، ولكن في حالة إعادة توجيه عمليات المصادقة إلى شبكات PSN مختلفة بواسطة موازن التحميل، يمكن إرجاع حالة الوضع الصحيحة إلى العميل.

إستخدام الحالة 5 - يتم الاستجابة لمستكشفات المرحلة 2 بواسطة خادم مختلف عن الخادم الذي تمت مصادقة العميل عليه

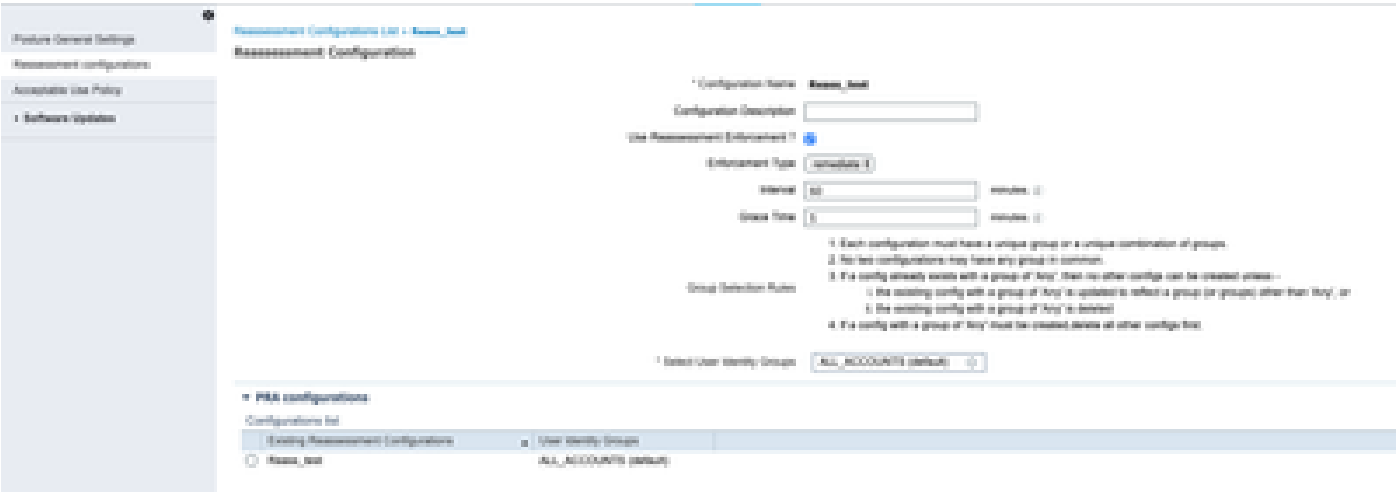
- ال يمكن أن تكون هذه مشكلة في السلوك الجديد، كما أن ملف تعريف التخويل لكل PSN غير ضروري.

الاعتبارات عند الاحتفاظ بنفس معرف جلسة العمل

عندما تستخدم الطرق الواردة في هذا المستند، فمن المحتمل أن يظل المستخدم المتصل بالشبكة متواقفا لفترات طويلة من الوقت. على الرغم من أنها تعيد المصادقة، فإن معرف جلسة العمل ال يتغير وبالتالي يستمر ISE في تمرير نتيجة AuthZ لقاعدة مطابقة حالة التوافق.

وفي هذه الحالة، يلزم تكوين عملية إعادة التقييم الدوري بحيث تكون الوضعية مطلوبة للتأكد من أن نقطة النهاية ال تزال متوافقة مع سياسات الشركة على فترات محددة.

يمكن تكوين هذا تحت مركز العمل > الوضع > الإعدادات > تكوينات إعادة التقييم.



حول هذه الترجمة

ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائماً إلى المستند الإنجليزي الأصلي (الرابط متوفر).