قارن تدفق إعادة توجيه ISE Posture (وضعية محرك خدمات الهوية (ISE)) بتدفق غير موجه لوضع ISE

المحتويات

المقدمة

يصف هذا المستند مقارنة التدفق غير الموجه للوضع المدعوم في إصدارات ISE 2.2 والإصدارات الأعلى مع تدفق إعادة توجيه الوضع المدعوم منذ إصدارات ISE السابقة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تدفق Posture على ISE
- تكوين مكونات الوضع على ISE

- تكوين أجهزة الأمان المعدلة (ASA) للوضع عبر الشبكات الخاصة الظاهرية (VPN)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- ISE الإصدار 2.2 من Cisco
- Cisco ASAv مع برنامج 9.6 (2)

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يصف هذا المستند وظيفة جديدة تم إدخالها في Identity Service Engine (ISE) 2.2 والتي تسمح لـ ISE بدعم تدفق Posture دون أي نوع من دعم إعادة التوجيه على جهاز الوصول إلى الشبكة (NAD) أو ISE.

Posture (وضعية) هو مكون أساسي من Cisco ISE. الوضع كمكون يمكن تمثيله بثلاثة عناصر رئيسية:

1. ISE كنقطة توزيع وتقرير لتكوين السياسة.
   من منظور المسؤول على ISE، تقوم بتكوين سياسات الوضع (ما هي الشروط المحددة التي يجب استيفاؤها لوضع علامة على الجهاز على أنه متوافق مع الشركة)، وسياسات إمداد العميل (ما هو البرنامج الوكيل الذي يجب تثبيته على أي نوع من الأجهزة)، ونهج التخويل (ما نوع الأذونات التي يجب التكليف بها، وذلك يتوقف على حالة وضعية الجهاز).
2. جهاز وصول إلى الشبكة كنقطة لإنفاذ السياسة.
   وعلى الجانب NAD، يتم تطبيق قيود التخويل الفعلية في وقت مصادقة المستخدم. توفر خدمة ISE كنقطة نهج معلمات التفويض مثل قائمة التحكم في الوصول (dACL) وقائمة التحكم في الوصول المعاد توجيهها VLAN/Redirect-URL/شبكة (ACL). وبشكل تقليدي، يلزم NADs دعم إعادة التوجيه للوضعية، وللوضعية أن تحدث بعد تغيير (إرشاد برنامج المستخدم أو الوكيل الذي يجب الاتصال بعقدة ISE) وتفويض (CoA) لإعادة مصادقة المستخدم بعد تحديد حالة الوضع لنقطة النهاية.
3. برنامج الوكيل كنقطة لجمع البيانات والتفاعل مع المستخدم النهائي.
   يستخدم Cisco ISE ثلاثة أنواع من برنامج الوكيل: AnyConnect ISE Posture Module، و NAC Agent، و Web Agent. يقدم ISE متطلبات الوضع من ISE ويستلم الوكيل معلومات حول متطلبات الوضع إلى ISE حول حالة المتطلبات.

ملاحظة: يستند هذا المستند إلى وحدة AnyConnect ISE Posture Module التي هي الوحدة النمطية الوحيدة التي تدعم الوضع بشكل كامل دون إعادة التوجيه.

في وضعية التدفق ISE 2.2، لا يتم إستخدام NAD لمصادقة المستخدمين وتقييد الوصول

فقط، بل أيضا لتوفير معلومات للبرنامج الوكيل حول عقدة ISE معينة يجب الاتصال بها. وكجزء من عملية إعادة التوجيه، يتم إرجاع المعلومات المتعلقة بعقدة ISE إلى برنامج الوكيل.

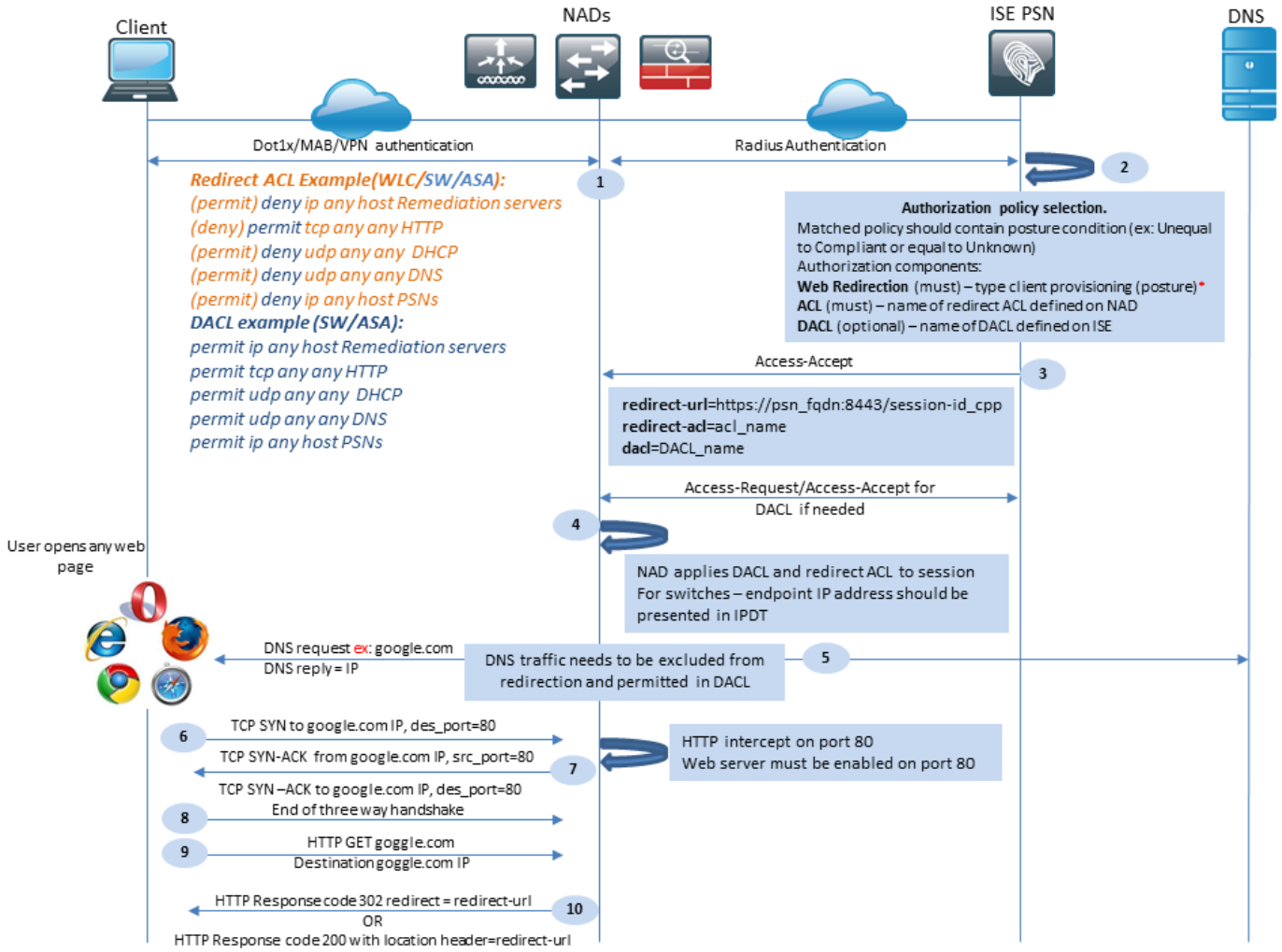
وتاريخيا، كان دعم إعادة التوجيه إما على NAD أو على جانب ISE متطلبا أساسيا لتنفيذ الموقف. في ISE 2.2 يتم إلغاء متطلب دعم إعادة التوجيه لكل من عمليتي إمداد العملاء الأولي ووضعية التشغيل.

إمداد العميل دون إعادة التوجيه - في ISE 2.2 يمكن الوصول إلى مدخل إمداد العميل (CPP) مباشرة عبر المدخل اسم المجال المؤهل بالكامل (FQDN). هذا مماثل للطريقة التي يمكن بها الوصول إلى بوابة الكفيل أو بوابة MyDevice.

عملية الوضع دون إعادة التوجيه - أثناء تثبيت الوكيل من بوابة حماية مستوى التحكم (CPP) يتم حفظ معلومات حول خوادم ISE على جانب العميل مما يجعل الاتصال المباشر ممكنا.

Posture Flow Pre ISE 2.2

تعرض هذه الصورة شرح خطوة بخطوة لتدفق وحدة وضع AnyConnect ISE النمطية قبل ISE 2.2:



شكل 1-1

الخطوة 1. المصادقة هي الخطوة الأولى من التدفق، ويمكن أن تكون dot1x أو MAB أو VPN.

الخطوة 2. يحتاج ISE إلى إختيار نهج مصادقة وتفويض للمستخدم. في سيناريو الوضع، يجب أن تحتوي سياسة التخويل المختارة على إشارة إلى حالة الوضع، والتي يجب أن تكون في البداية إما غير معروفة أو غير قابلة للتطبيق. وتغطي كل من هذه الحالات، يمكن إستخدام شروط ذات وضع غير متكافئ في المتثال.

يجب أن يحتوي ملف تعريف التخويل المختار على معلومات حول إعادة التوجيه:

- إعادة توجيه ويب- بالنسبة لحالة الوضع، يجب تحديد نوع إعادة توجيه ويب كإعداد عميل (Posture).
- ACL- يجب أن يحتوي هذا القسم على اسم قائمة التحكم في الوصول (ACL) الذي تم تكوينه على جانب NAD. يتم إستخدام قائمة التحكم في الوصول (ACL) هذه لتعليم حركة المرور التي يجب أن تتجاوز إعادة التوجيه والتي يجب إعادة توجيهها بالفعل.
- DACL- يمكن إستخدامها مع قائمة الوصول المعاد توجيهها ولكن يجب أن تضع في الاعتبار أن الأنظمة الأساسية المختلفة تعالج قوائم التحكم في الوصول (ACL) من Dell (DACL) وقوائم التحكم في الوصول (ACL) المعاد توجيهها بترتيب مختلف.

على سبيل المثال، يعمل ASA دائما على معالجة قائمة التحكم في الوصول (DACL) قبل إعادة توجيهها إلى قائمة التحكم في الوصول (ACL). وفي الوقت نفسه، تعالج بعض منصات المحولات بنفس الطريقة مثل ASA، وتقوم منصات المحولات الأخرى بمعالجة قائمة التحكم في الوصول الخاصة بإعادة التوجيه أولا ثم التحقق من قائمة التحكم في الوصول للواجهة/DACL إذا كان يجب إسقاط حركة المرور أو السماح بها.

ملاحظة: بعد تمكين خيار إعادة توجيه الويب في ملف تعريف التخويل، يجب إختيار المدخل الهدف لإعادة التوجيه.

الخطوة 3. يقوم ISE بإرجاع Access-Accept باستخدام سمات التخويل. يتم إنشاء URL لإعادة التوجيه في سمات التخويل تلقائيا بواسطة ISE. يحتوي على المكونات التالية:

- عقدة FQDN الخاصة ب ISE التي حدثت عليها المصادقة. في بعض الحالات، يمكن الكتابة فوق FQDN الديناميكي بواسطة تكوين ملف تعريف التخويل (IP/hostname/FQDN الثابت) في قسم إعادة توجيه الويب. إذا تم إستخدام القيمة الثابتة، فيجب أن تشير إلى نفس عقدة ISE حيث تمت معالجة المصادقة. في حالة موازن التحميل (LB)، يمكن أن يشير FQDN هذا إلى LB VIP ولكن فقط في حالة تكوين LB لربط إتصالات RADIUS و SSL معا.
- المنفذ- يتم الحصول على قيمة المنفذ من تكوين المدخل الهدف.
- معرف جلسة العمل- يتم أخذ هذه القيمة من قبل ISE من معرف جلسة تدقيق زوج Cisco AV المقدم في Access-Request. يتم إنشاء القيمة نفسها ديناميكيا بواسطة NAD.
- معرف المدخل- معرف المدخل الهدف على جانب ISE.

الخطوة 4. يطبق NAD سياسة تخويل على الجلسة. وبالإضافة إلى ذلك، في حالة تكوين قائمة التحكم في الوصول للبنية الأساسية (DACL)، يتم طلب محتواها قبل تطبيق نهج

التخويل.

اعتبارات هامة:

- يجب أن يكون لكل NADs- جهاز قائمة تحكم في الوصول (ACL) تم تكوينها محليا بنفس اسم الجهاز الذي تم إستقباله في Access-Accept كقائمة تحكم في الوصول لإعادة التوجيه.
- المحولات- يجب تقديم عنوان IP الخاص بالعميل في إخراج show authentication session interface details لتنفيذ إعادة التوجيه وقوائم التحكم في الوصول (ACL) بنجاح. يتم التعرف على عنوان IP للعميل بواسطة ميزة تعقب جهاز IP (IPDT).

الخطوة 5. يرسل العميل طلب DNS ل FQDN الذي تم إدخاله إلى مستعرض الويب. في هذه المرحلة، يجب أن تتجاوز حركة مرور DNS إعادة التوجيه ويجب إرجاع عنوان IP الصحيح بواسطة خادم DNS.

الخطوة 6. يرسل العميل TCP SYN إلى عنوان IP الذي يتم إستقباله في رد DNS. عنوان IP المصدر في الحزمة هو IP العميل وعنوان IP للوجهة هو IP الخاص بالمورد المطلوب. يواي منفذ الوجهة 80، باستثناء الحالات التي تم فيها تكوين وكيل HTTP المباشر في مستعرض ويب العميل.

تعترض الخطوة 7.nad طلبات العميل وتعد حزم SYN-ACK مع مصدر IP يواي المورد المطلوب، وغاية IP يواي العميل، ومصدر ميناء يواي 80.

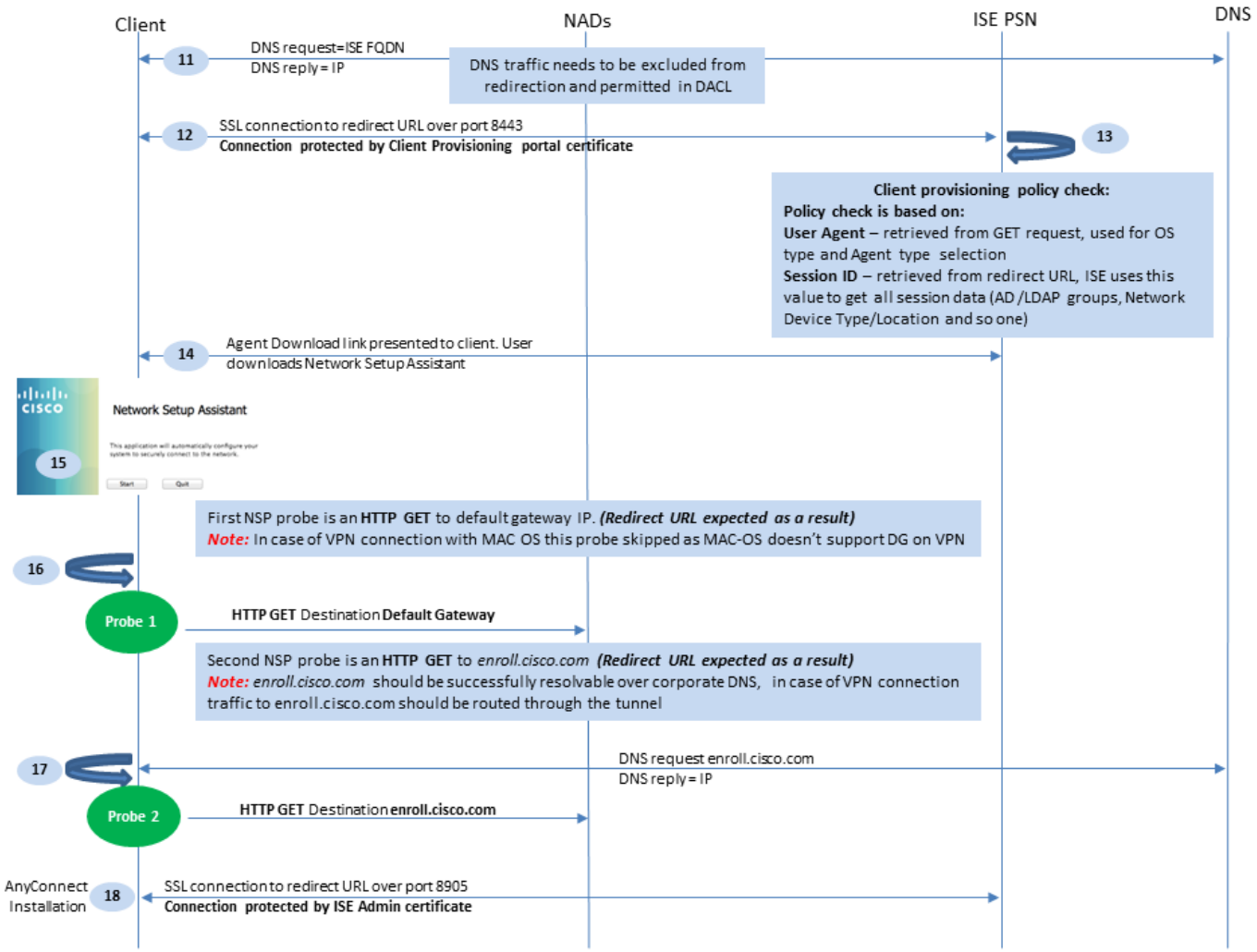
اعتبارات هامة:

- يجب أن يكون لدى NADs خادم HTTP قيد التشغيل على المنفذ الذي يرسل العميل الطلبات عليه. افتراضي، هو ميناء 80.
- إذا كان العميل يستخدم خادم ويب وكيل HTTP مباشرة، فيجب تشغيل خادم HTTP على منفذ الوكيل على NAS. هذا السيناريو خارج نطاق هذا المستند.
- في الحالات التي ال يكون NAD فيها عنوان IP محلي في العميل، يتم إرسال الشبكة الفرعية SYN-ACK مع جدول التوجيه NAD (عبر واجهة الإدارة عادة). في هذا السيناريو، يتم توجيه الحزمة عبر البنية الأساسية من المستوى الثالث ويجب توجيهها مرة أخرى إلى العميل بواسطة جهاز تدفق من المستوى الثالث. إذا كان جهاز L3 هو جدار حماية ذو حالة، فيجب منح إستثناء إضافي لهذا التوجيه غير المتماثل.

الخطوة 8. ينتهي العميل من مصافحة TCP ثالثية الإتجاه بواسطة ACK.

الخطوة 9. تم إرسال HTTP GET للمورد الهدف بواسطة عميل.

الخطوة 10. NAD يرجع URL إعادة التوجيه إلى العميل مع رمز HTTP 302 (تم نقل الصفحة)، يمكن إرجاع بعض إعادة توجيه NAD داخل رسالة HTTP 200 OK في رأس الموقع.



شكل 1-2

الخطوة 11. يرسل العميل طلب DNS ل FQDN من عنوان URL لإعادة التوجيه. يجب حل FQDN على جانب خادم DNS.

الخطوة 12. تم إنشاء اتصال SSL عبر المنفذ الذي تم إستالمه في عنوان URL لإعادة التوجيه (الافتراضي 8443). هذا الاتصال محمي بشهادة مدخل من جانب ISE. يتم تقديم مدخل توفير العميل (CPP) إلى المستخدم.

الخطوة 13.قبل توفير خيار تنزيل إلى العميل، يجب على ISE إختيار سياسة إمداد العميل الهدف (CP). يتم إستردار نظام التشغيل (OS) الخاص بالعميل الذي تم اكتشافه من وكيل مستخدم المستعرض والمعلومات الأخرى المطلوبة لتحديد نهج CPP من جلسة المصادقة (مثل مجموعات AD/LDAP وما إلى ذلك). يعرف ISE الجلسة المستهدفة من معرف الجلسة المعروض في URL إعادة التوجيه.

الخطوة 14. يتم إرجاع إرتباط التنزيل لمساعد إعداد الشبكة (NSA) إلى العميل. يقوم العميل بتنزيل التطبيق.

ملاحظة: عادة ما يمكنك رؤية NSA كجزء من تدفق BYOD لأنظمة التشغيل Windows و Android، ولكن يمكن إستخدام هذا التطبيق أيضا لتثبيت AnyConnect أو مكوناته من

ISE.

الخطوة 15.يقوم المستخدم بتشغيل تطبيق NSA.

الخطوة 16. يرسل NSA أول تحقيق اكتشاف - HTTP /auth/discovery إلى البوابة الافتراضية. تتوقع NSA إعادة توجيه url كنتيجة لذلك.

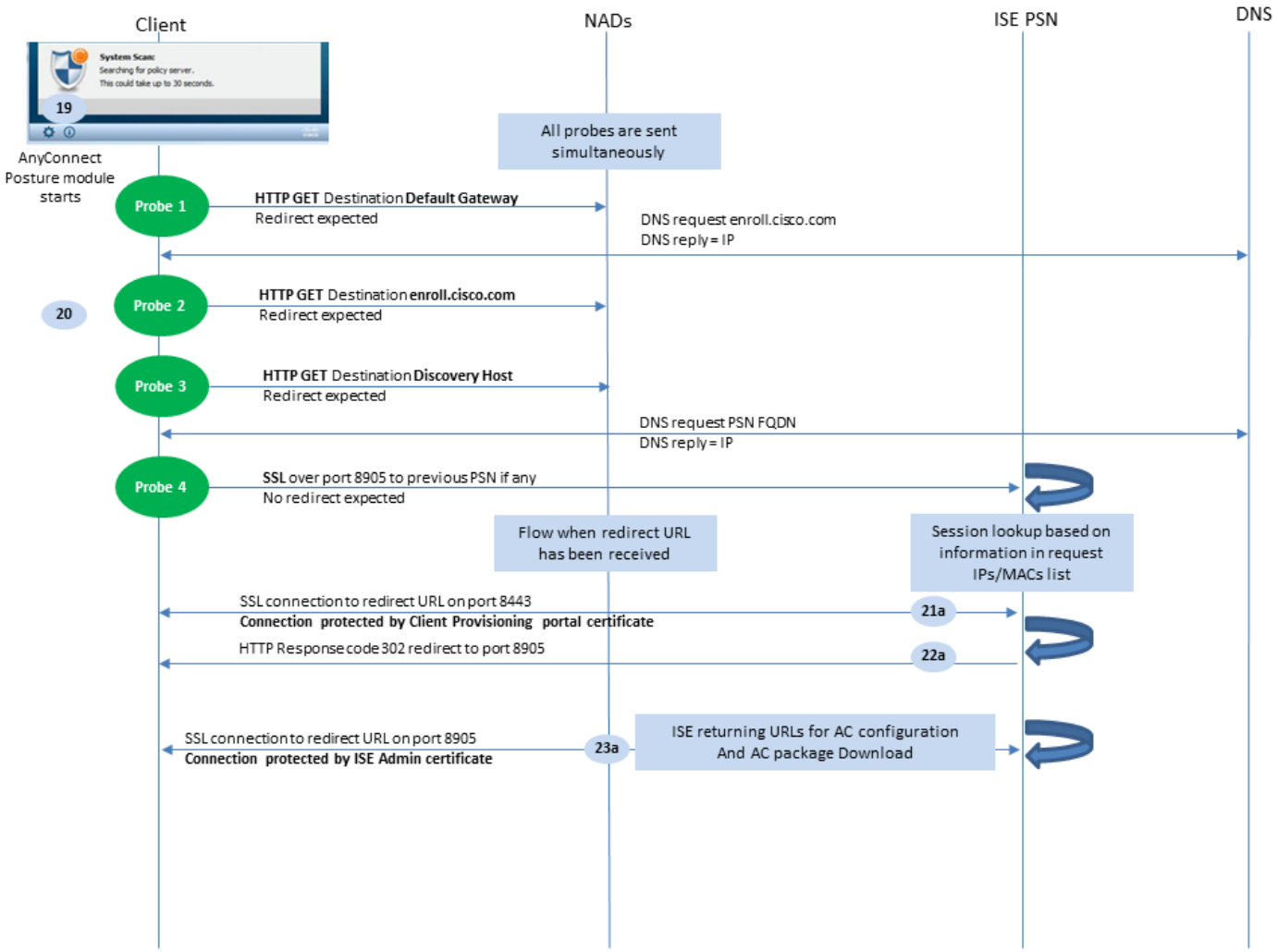
ملاحظة: بالنسبة للاتصالات عبر VPN على أجهزة Mac OS، يتم تجاهل هذا المسار، حيث أن نظام التشغيل Mac OS لا يحتوي على عبارة افتراضية على محول VPN.

الخطوة 17.NSA ترسل تحقيقا ثانيا إذا فشل التحقيق الأول. المسار الثاني هو HTTP GET/auth/discovery to enroll.cisco.com. يجب حل FQDN هذا بنجاح بواسطة خادم DNS. في سيناريو شبكة VPN مع نفق انقسام، يتم نقل البيانات إلى enroll.cisco.com يجب توجيهه عبر النفق.

الخطوة 18. إذا نجح أي من الاستقصاءات، يقوم NSA بإنشاء اتصال SSL عبر المنفذ 8905 باستخدام المعلومات التي تم الحصول عليها من redirect-url. هذا الاتصال محمي بواسطة شهادة مسؤول ISE. دخل هذا الاتصال تقوم NSA بتنزيل AnyConnect.

اعتبارات هامة:

- قبل إصدار ISE 2.2، يكون اتصال SSL عبر المنفذ 8905 متطلبا للوضع.
- لتجنب تحذيرات الشهادات يجب أن تكون شهادات المدخل والمسؤول موثوقا بها على جانب العميل.
- في واجهات نشر ISE المتعددة غير G0 يمكن ربطها ب FQDN بشكل مختلف من FQDN للنظام (باستخدام أمر CLI ip host). قد يتسبب ذلك في حدوث مشاكل في التحقق من صحة اسم الموضوع (SN)/الاسم البديل للموضوع (SAN). إذا تمت إعادة توجيه العميل إلى FQDN من الواجهة G1، على سبيل المثال، يمكن أن يختلف FQDN للنظام عن FQDN في عنوان URL لإعادة التوجيه لشهادة اتصال 8905. كحل لهذا السيناريو، يمكنك إضافة FQDN لواجهات إضافية في حقول SAN لشهادة المسؤول، أو يمكنك إستخدام حرف بدل في شهادة المسؤول.



شكل 1-3

الخطوة 19.تم تشغيل عملية وضع AnyConnect ISE.

تبدأ وحدة AnyConnect ISE Posture (وضعية محرك خدمات الهوية (ISE)) في أي من هذه الحالات:

- بعد التثبيت
- بعد تغيير قيمة العبارة الافتراضية
- بعد حدث تسجيل دخول مستخدم النظام
- بعد حدث طاقة النظام

الخطوة 20. في هذه المرحلة، تقوم وحدة AnyConnect ISE Posture Module بتهيئة اكتشاف خادم النهج. ويتم تحقيق ذلك باستخدام سلسلة من المستكشفات التي يتم إرسالها في نفس الوقت بواسطة وحدة وضع AnyConnect ISE.

- Probe 1 - HTTP get /auth/discovery لتقصير البوابة IP. يجب تذكر أن أجهزة Mac OS ال تحتوي على عبارة افتراضية على محول VPN. النتيجة المتوقعة للتحقيق هي redirect-url.
- مسبار 2 - HTTP GET/auth/discovery to enroll.cisco.com. يجب حل FQDN هذا بنجاح بواسطة خادم DNS. في سيناريو شبكة VPN مع نفق انقسام، يتم نقل البيانات إلى enroll.cisco.com يجب توجيهه عبر النفق. النتيجة المتوقعة للتحقيق هي redirect-url.
- Probe 3 - HTTP الحصول على /auth/discovery لمضيف اكتشاف. يتم إرجاع قيمة مضيف

الاكتشاف من ISE أثناء التثبيت في ملف تعريف وضعية التيار المتردد. النتيجة المتوقعة للتحقيق هي redirect-url.

- تحقيق 4 - HTTP الحصول/المصادقة/الحالة عبر SSL على المنفذ 8905 إلى PSN الذي تم توصيله سابقا. يحتوي هذا الطلب على معلومات حول IPs العميل وقائمة MACs للبحث عن جلسة العمل على جانب ISE. تتم عرض هذه المشكلة أثناء محاولة الوضع الأولي. تتم حماية الاتصال بواسطة شهادة مسؤول ISE. ونتيجة لهذا التحقيق، يمكن أن يقوم ISE بإرجاع معرف جلسة العمل إلى العميل إذا كانت العقدة التي هبط عليها المسبار هي نفس العقدة التي تم مصادقة المستخدم عليها.

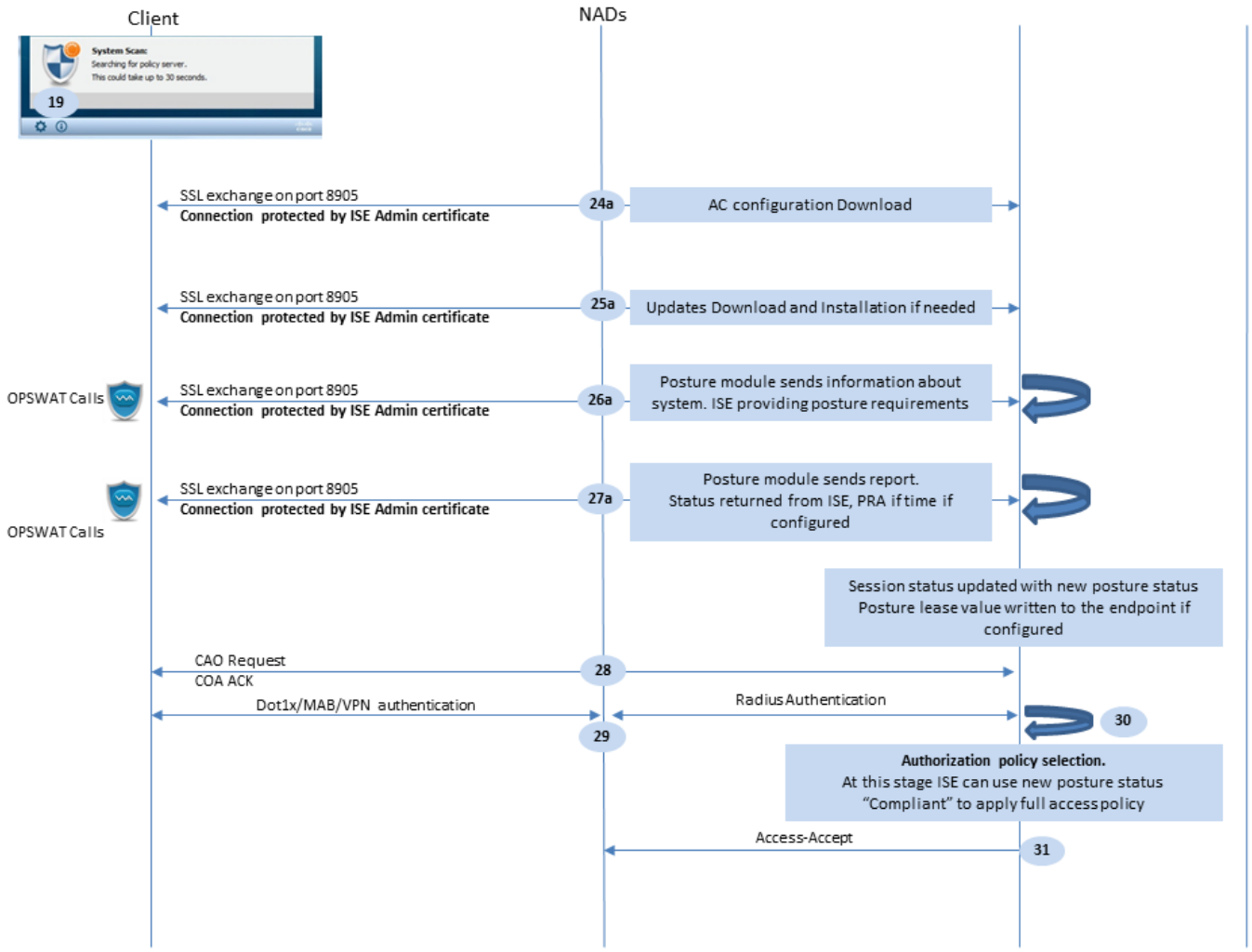
ملاحظة: نتيجة لهذا التحقيق، يمكن القيام بالموقف بنجاح حتى بدون العمل على إعادة التوجيه في بعض الظروف. يتطلب الوضع الناجح بدون إعادة التوجيه أن يكون PSN الحالي الذي صادق الجلسة هو نفسه PSN الذي تم توصيله سابقا بنجاح. تذكر أنه قبل ISE 2.2، فإن وضعية النجاح بدون إعادة التوجيه هي إستثناء وليست قاعدة.

تصف الخطوات التالية عملية الوضع في الحالة التي يتم فيها تلقي عنوان URL لإعادة التوجيه (تم وضع علامة على التدفق بالحرف أ) كنتيجة لأحد المسابير.

الخطوة 21. تقوم وحدة AnyConnect ISE Posture بإنشاء اتصال بمدخل توفير العميل باستخدام URL الذي تم إسترداده أثناء مرحلة الاكتشاف. في هذه المرحلة، يقوم ISE بالتحقق من صحة سياسة إمداد العميل مرة أخرى باستخدام المعلومات من جلسات العمل المصدق عليها.

الخطوة 22.إذا تم الكشف عن سياسة إمداد العميل، ترجع ISE بإعادة التوجيه إلى المنفذ 8905.

الخطوة 23. ينشئ الوكيل اتصال ب ISE عبر المنفذ 8905. خلال هذا الاتصال، يقوم ISE بإرجاع عناوين URL لملف تعريف الوضع ووحدة التوافق النمطية وتحديثات AnyConnect.



شكل 1-4

الخطوة 24.AC ISE Posture Module download من ISE.

الخطوة 25.تحديث التنزيل والتثبيت إذا لزم الأمر.

الخطوة 26. تقوم وحدة AC ISE Posture (وضعية محرك خدمات الهوية (AC) بتجميع المعلومات الأولية حول النظام (مثل إصدار OS ومنتجات الأمان المثبتة وإصدار تعريفها). وفي هذه المرحلة، تشمل وحدة AC ISE Posture API من OPSWAT لجمع معلومات عن المنتجات الأمنية. يتم إرسال البيانات المجمعة إلى ISE. وكرد على هذا الطلب، يوفر ISE قائمة متطلبات الوضع. تم تحديد قائمة المتطلبات كنتيجة لمعالجة نهج الوضع. لمطابقة النهج الصحيح، يستخدم ISE إصدار نظام تشغيل الجهاز (الموجود في الطلب) وقيمة معرف جلسة العمل الاختياري سمات مطلوبة أخرى (مجموعات AD/LDAP). يتم إرسال قيمة معرف جلسة العمل بواسطة العميل أيضا.

الخطوة 27. وفي هذه الخطوة، يقوم العميل بإجراء مكالمات مع مكتب مرافق الأسلحة والتكتيكات الخاصة، بالإضافة إلى آليات أخرى للتحقق من متطلبات الوضع. يتم إرسال التقرير النهائي المزود بقائمة المتطلبات وحالتها إلى ISE. يحتاج ISE إلى اتخاذ القرار النهائي حول حالة التوافق مع نقطة النهاية. إذا تم تمييز نقطة النهاية على أنها غير متوافقة في هذه الخطوة، يتم إرجاع مجموعة من إجراءات الإصلاح. بالنسبة لنقطة النهاية المتوافقة، يقوم ISE بكتابة حالة التوافق في جلسة العمل، كما يضع آخر طابع زمني للوضع على سمات نقطة النهاية إذا تم تكوين تأجير Posture. يتم إرسال نتيجة الوضع

مرة أخرى إلى نقطة النهاية. في حالة وضع وقت إعادة تقييم الوضع (PRA) ل PRA يتم وضعه من قبل ISE في هذه الحزمة أيضا.

في سيناريو غير متوافق تأخذ هذه النقاط بعين الاعتبار:

- يتم تنفيذ بعض إجراءات الإصلاح (مثل عرض الرسائل النصية، ومعالجة الارتباط، ومعالجة الملفات، وغيرها) بواسطة عامل الوضع نفسه.
- أنواع الإصلاح الأخرى (مثل AV. كما هو الحال مع WSUS و SCCM) تتطلب اتصال OPSWAT API بين عامل الوضع والمنتج المستهدف. في هذا السيناريو، يرسل عامل وضعية المستخدم طلب إصلاح إلى المنتج فقط. تتم عملية الإصلاح نفسها بواسطة منتجات الأمان مباشرة.

ملاحظة: في حالة اضطرار منتج الأمان للاتصال بالموارد الخارجية (خوادم تحديث داخلية/خارجية)، يجب التأكد من السماح بهذا الاتصال في قائمة التحكم في الوصول الخاصة بالمنفذ (DACL).

28.ISE طلب COA إلى NAD الذي يجب أن يؤدي إلى تشغيل مصادقة جديدة ترسل الخطوة للمستخدم. ويجب أن تؤكد NAD هذا الطلب من قبل COA ACK. تذكر أنه بالنسبة لحالات الشبكات الخاصة الظاهرية (VPN)، يتم إستخدام الدفع بوجود الخدمة (COA) يتم ذلك إرسال طلب مصادقة جديد. بدلا من ذلك، يزيل ASA معلمات التخويل السابقة (إعادة توجيه URL، وإعادة توجيه ACL، و DACL) من جلسة العمل ويطبق معلمات جديدة من طلب COA.

الخطوة 29.طلب مصادقة جديد للمستخدم.

اعتبارات هامة:

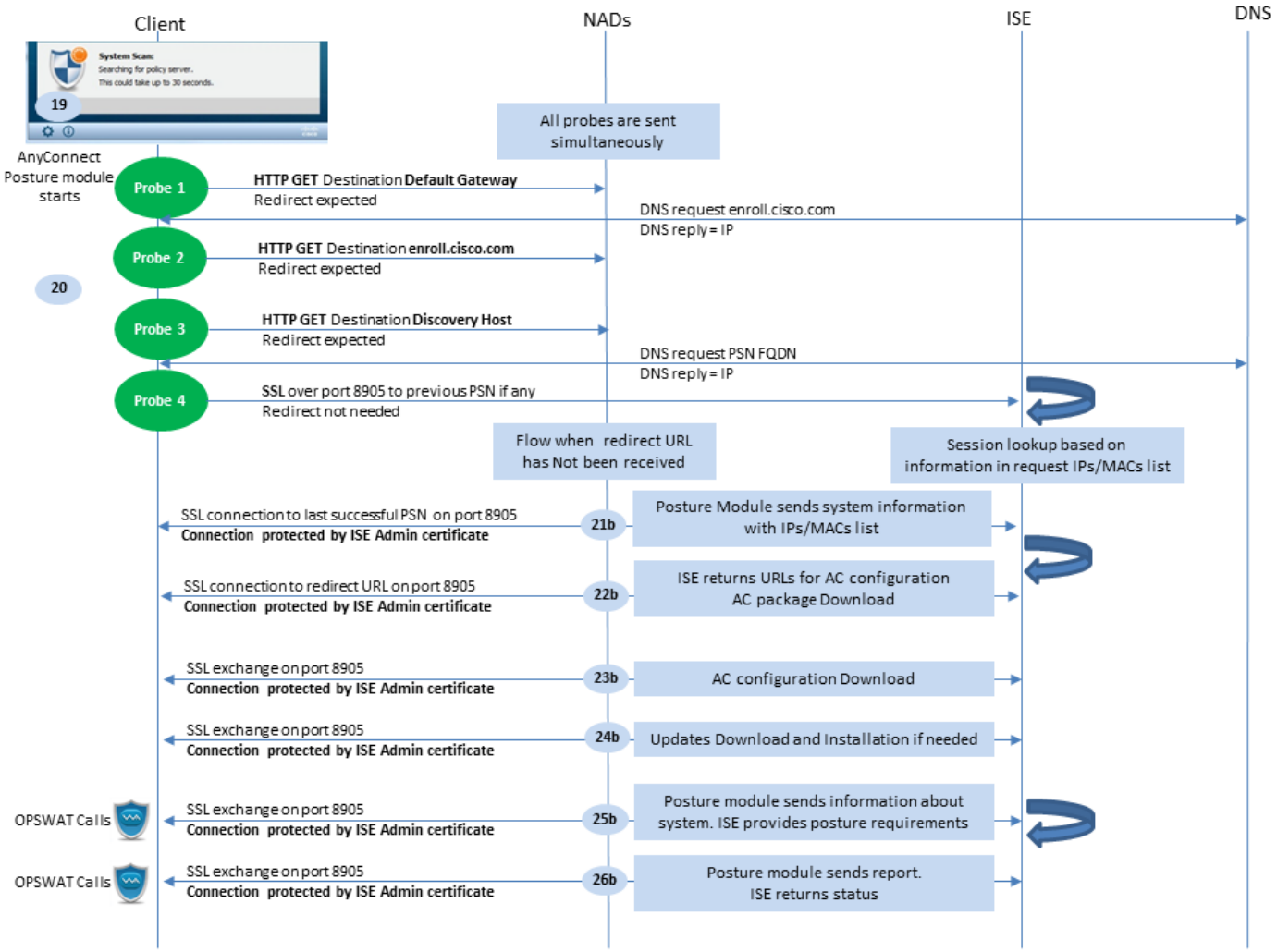
- بشكل نموذجي ل Cisco NAD COA، يتم إستخدام المصادقة من قبل ISE، وهذا يرشد ويبدأ طلب مصادقة جديد باستخدام معرف الجلسة السابقة.
- على جانب ISE، تمثل قيمة معرف جلسة العمل نفسها إشارة إلى أنه يجب إعادة إستخدام سمات جلسة العمل التي تم تجميعها مسبقا (حالة الشكوى في حالتان) ويجب تعيين ملف تعريف تخويل جديد استنادا إلى هذه السمات.
- في حالة تغيير معرف جلسة العمل، يتم التعامل مع هذا الاتصال كجديد، ويتم إعادة تشغيل عملية الوضع الكامل.
- لتجنب إعادة الوضع في كل تغيير لمعرف جلسة العمل، يمكن إستخدام تأجير الوضع. في هذا السيناريو، يتم تخزين المعلومات حول حالة الوضع في سمات نقطة النهاية التي تبقى على ISE حتى إذا كان معرف الجلسة GEتم تغيير ts.

الخطوة 30. يتم تحديد نهج تخويل جديد على جانب ISE استنادا إلى حالة الوضع.

الخطوة 31. يتم إرسال قبول الوصول مع سمات التخويل الجديدة إلى NAD.

يصف التدفق التالي السيناريو عندما ال يتم إسترداد URL لإعادة التوجيه (المعلم بحرف B) من قبل أي تحقيق في الوضع وقد تم الاستعلام عن PSN المتصل مسبقا بواسطة المسبار الأخير. جميع الخطوات هنا هي نفسها تماما كما في الحالة مع URL لإعادة التوجيه باستثناء إعادة التشغيل التي أرجعها PSN نتيجة Probe 4. إذا سقط هذا المسبار على ال

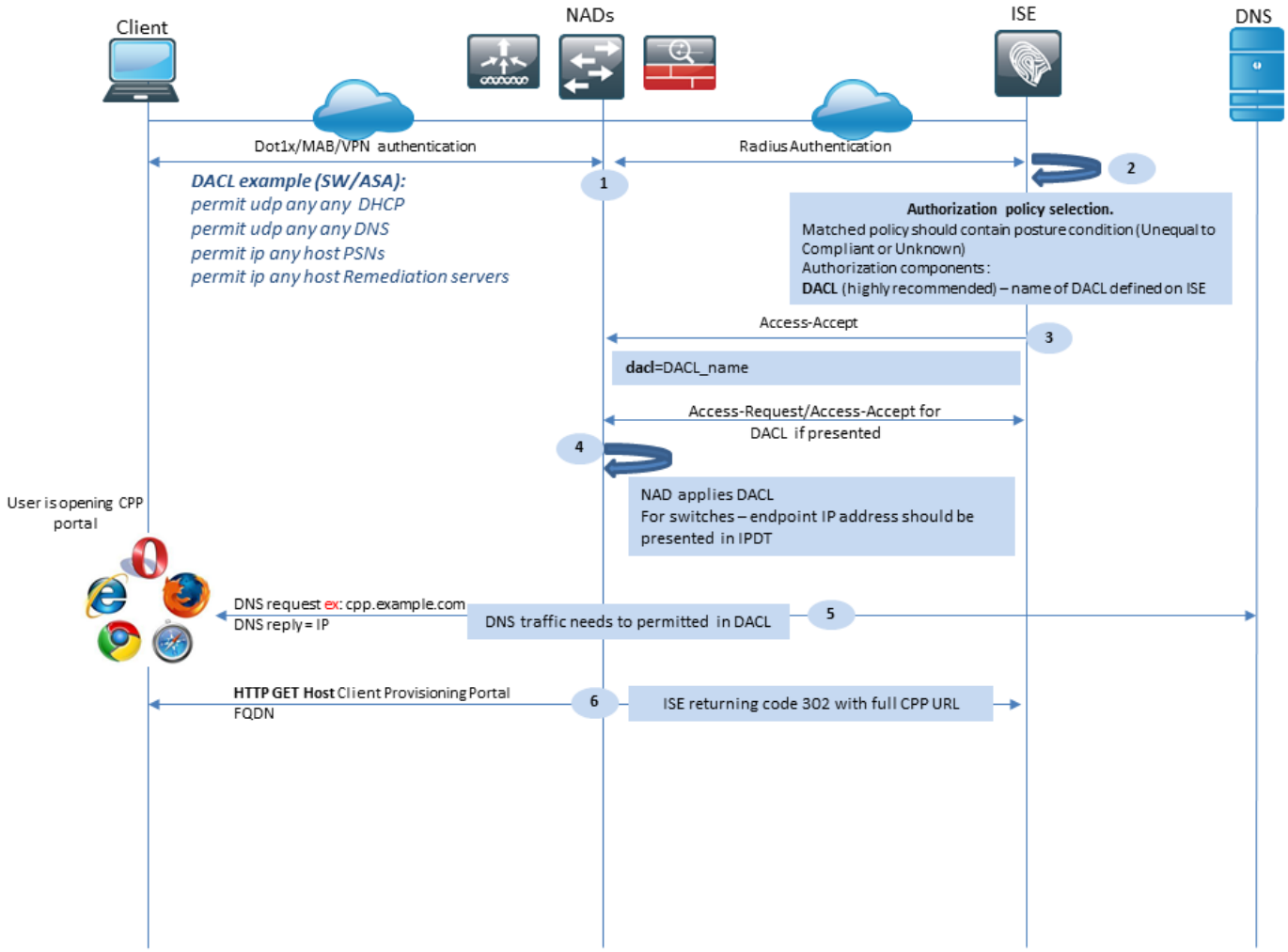
نفسه PSN أي مالك لجلسة المصادقة الحالية، فإن إعادة التشغيل تحتوي على قيمة معرف جلسة العمل التي يتم إستخدامها لاحقا بواسطة عامل الوضع لإنهاء العملية. في حالة عدم تطابق وحدة الاستقبال والبث المتصلة سابقا مع مالك الجلسة الحالية، يفشل البحث عن جلسة العمل وترجع إستجابة فارغة إلى وحدة AC ISE Posture النمطية. كنتيجة نهائية لهذا، فإن No Policy Server Detected تم إرجاع الرسالة إلى المستخدم النهائي.



شكل 1-5

Posture Flow ISE 2.2

يدعم الإصدار ISE 2.2 والإصدارات الأحدث كل من عمليات إعادة التوجيه والتدفقات غير القابلة لإعادة التوجيه في آن واحد. هذا هو الشرح التفصيلي لتدفق الوضع دون إعادة توجيه:



شكل 2-1

الخطوة 1.المصادقة هي الخطوة الأولى من التدفق. وه يستطيع كنت dot1x، MAB، أو VPN.

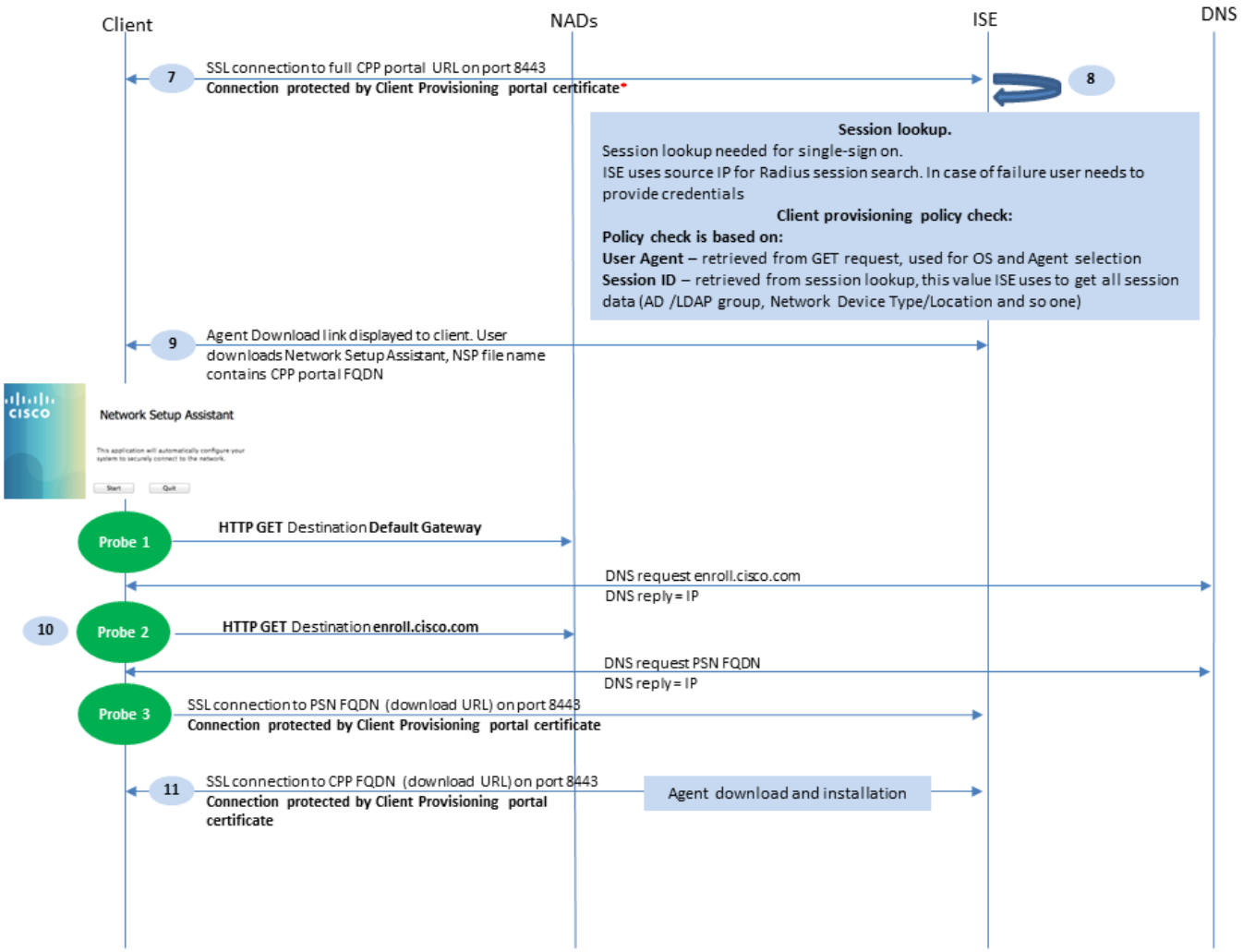
يجب أن تختار الخطوة 2.ISE نهج المصادقة والتفويض للمستخدم. في الوضع، يجب أن تحتوي سياسة التخويل التي تم إختيارها للسيناريو على إشارة إلى حالة الوضع، والتي يجب أن تكون في البداية غير معروفة أو غير قابلة للتطبيق. ولتغطية كل من هذه الحالات، يمكن إستخدام شروط ذات وضع غير متكافئ في المصادقة. للوضع بدون إعادة توجيه، ال حاجة لاستخدام أي تكوين إعادة توجيه ويب في ملف تعريف التخويل. ال يزال بإمكانك النظر في إستخدام قائمة التحكم في الوصول إلى المجال الجوي أو قائمة التحكم في الوصول إلى DACL للحد من وصول المستخدم في المرحلة التي ال تتوفر فيها حالة الوضع.

ترجع الخطوة 3.ISE قبول الوصول باستخدام سمات التخويل.

الخطوة 4. إذا تم إرجاع اسم قائمة التحكم في الوصول (DACL) في Access-Accept، وتقوم بعدء تنزيل محتوى قائمة التحكم في الوصول للبنية الأساسية (DACL) وتطبيق ملف تعريف التخويل على جلسة العمل بعد الحصول عليه.

الخطوة 5. يفترض النهج الجديد أن إعادة التوجيه غير ممكنة، لذلك يجب على المستخدم إدخال FQDN لبوابة إمداد العميل يدويا. يجب تحديد FQDN لبوابة CPP في تكوين البوابة على جانب ISE. من منظور خادم DNS، يجب أن يشير السجل A إلى خادم ISE مع تمكين دور PSN.

الخطوة 6. يرسل العميل HTTP للوصول إلى FQDN الخاص بواجهة إمداد العميل، ويتم توزيع هذا الطلب على جانب ISE ويعاد عنوان URL الخاص بالمدخل الكامل إلى العميل.



شكل 2-2

يتم إنشاء اتصال الخطوة 7.SSL عبر المنفذ الذي يتم إستلامه في عنوان URL لإعادة التوجيه (الافتراضي 8443). هذا الاتصال محمي بشهادة مدخل من جانب ISE. يتم تقديم بوابة إمداد العميل (CPP) إلى المستخدم.

الخطوة 8. في هذه الخطوة تحدث حدثان على ISE:

- تسجيل دخول أحادي (SSO) - يحاول ISE البحث عن مصادقة ناجحة سابقة. يستخدم ISE عنوان IP المصدر من الحزمة كمرشح بحث لجلسات نصف القطر النشط.

ملاحظة: يتم إسترداد الجلسة استنادا إلى تطابق بين IP المصدر في الحزمة وعنوان IP المؤطر في الجلسة. وعادة ما يتم إسترداد عنوان IP المؤطر بواسطة ISE من تحديثات المحاسبة المؤقتة، لذلك يلزم تمكين المحاسبة على جانب NAD. أيضا، أنت ينبغي تذكرت أن SSO يمكن فقط على العقدة التي تملك الجلسة. على سبيل المثال، إذا تم مصادقة الجلسة على PSN 1، ولكن FQDN نفسه يشير إلى PSN2، فإن آلية SSO تفشل.

- البحث عن سياسة إمداد العميل - في حالة نجاح SSO، يمكن لـ ISE إستخدام البيانات من جلسة العمل المصدق عليها ووكيل المستخدم من مستعرض العميل. في حالة فشل عملية تسجيل الدخول الموحد (SSO)، يجب على المستخدم توفير بيانات الاعتماد وبعد إسترداد معلومات مصادقة المستخدم من مخازن الهوية الداخلية والخارجية (AD/LDAP/المجموعات الداخلية)، يمكن إستخدامها للتحقق من سياسة توفير العميل.

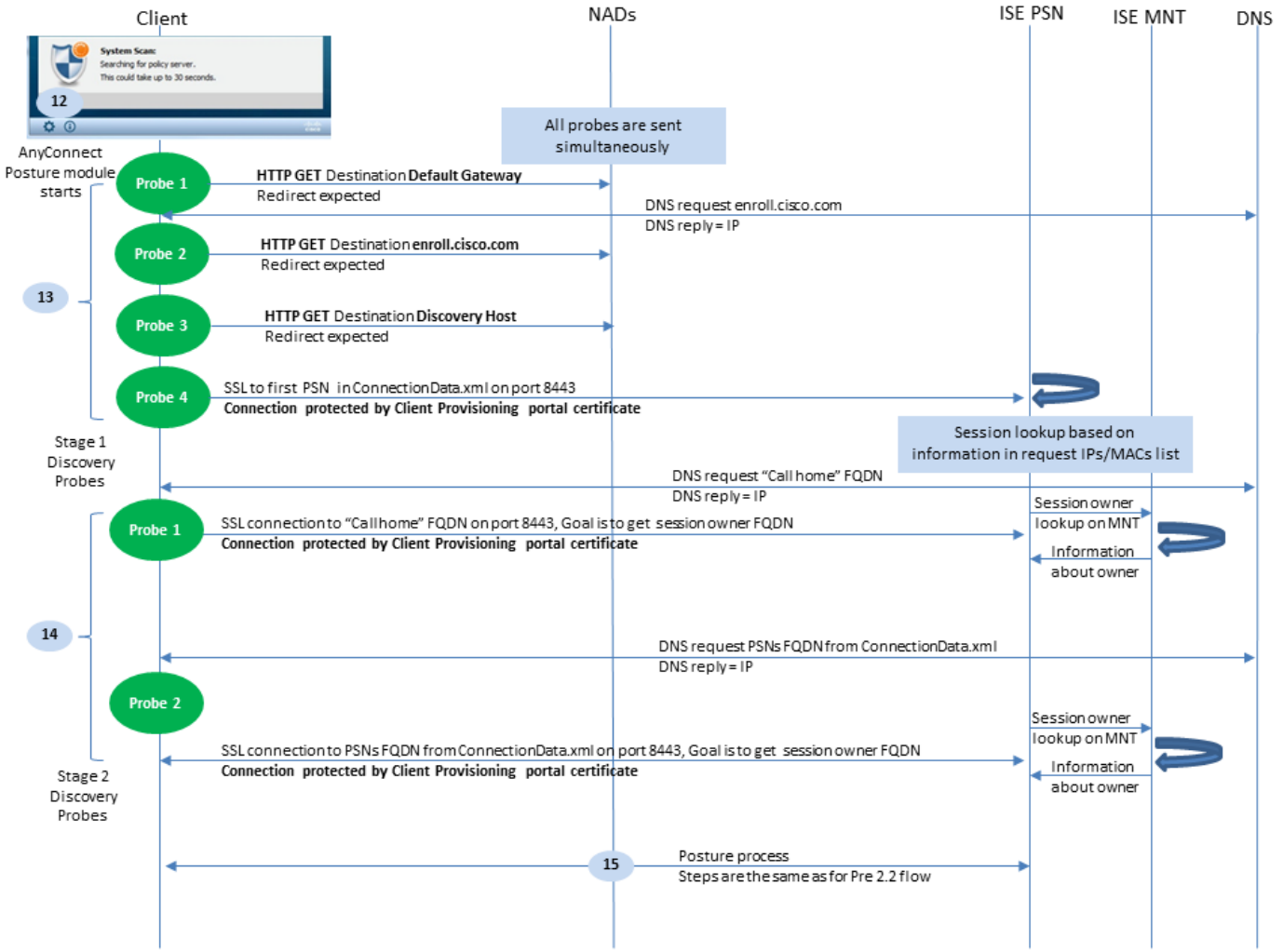
ملاحظة: نظرا لوجود عرف تصحيح الأخطاء من Cisco CSCvd11574، يمكنك مشاهدة خطأ في وقت تحديد سياسة إمداد العميل للحالات غير SSO عندما يكون المستخدم الخارجي عضوا في مجموعات AD/LDAP متعددة تمت إضافتها في تكوين مخزن الهوية الخارجية. تم إصلاح الخلل المذكور الذي يبدأ من ISE 2.3 FCS ويتطلب الإصلاح إستخدام CONTAINS في حالة مجموعة AD بدلا من EQUAL.

الخطوة 9. بعد تحديد نهج توفير العميل، يعرض ISE عنوان URL الخاص بتنزيل العميل للمستخدم. بعد النقر فوق تنزيل NSA، يتم دفع التطبيق إلى المستخدم. يحتوي اسم ملف NSA على FQDN لبوابة CPP.

الخطوة 10.في هذه الخطوة، يقوم NSA بتشغيل مستكشفات لإنشاء اتصال بـ ISE. يوجد مسار من المسايير التقليدية، بينما تم تصميم المسار الثالث للسماح باكتشاف ISE في البيئات بدون إعادة توجيه عنوان URL.

- يرسل NSA أولا تحقيق اكتشاف - HTTP /auth/discovery إلى البوابة الافتراضية. تتوقع NSA إعادة توجيه url كنتيجة لذلك.
- ترسل وكالة الأمن القومي تحقيقا ثانيا إذا فشل التحقيق الأول. المسار الثاني هو HTTP GET/auth/discovery to enroll.cisco.com. يجب حل FQDN هذا بنجاح بواسطة خادم DNS. في سيناريو شبكة VPN مع نفق انقسام، يتم نقل البيانات إلى enroll.cisco.com يجب توجيهه عبر النفق.
- يرسل NSA التحقيق الثالث عبر منفذ بوابة CPP إلى FQDN لبوابة إمداد العميل. يحتوي هذا الطلب على معلومات حول معرف جلسة عمل المدخل الذي يسمح لـ ISE بتحديد الموارد التي يجب توفيرها.

الخطوة 11. تقوم NSA بتنزيل AnyConnect و/أو وحدات معينة. يتم إجراء عملية التنزيل عبر منفذ إمداد العميل للمدخل.



شكل 2-3

الخطوة 12. في ISE 2.2، تنقسم عملية الوضع إلى مرحلتين. تحتوي المرحلة الأولى على مجموعة من عمليات أستكشاف الوضع التقليدي لدعم التوافق مع عمليات النشر السابقة التي تعتمد على إعادة توجيه عنوان URL.

الخطوة 13. تحتوي المرحلة الأولى على جميع مستكشفات اكتشاف الوضع التقليدي. للحصول على مزيد من التفاصيل حول المسابير، راجع الخطوة 20. في تدفق الوضع قبل ISE 2.2.

تحتوي الخطوة 14.Stage 2 على إثنين من استكشافات الاكتشاف التي تسمح لوحدة AC ISE Posture النمطية بإنشاء اتصال ب PSN حيث تتم مصادقة الجلسة في البيئات التي لا يتم فيها دعم إعادة التوجيه. خلال المرحلة الثانية، تكون جميع المسابر متتابعة.

- Probe 1 - أثناء التحقيق الأول، تحاول وحدة وضعية AC ISE الإنشاء باستخدام IP/FQDNs من "قائمة الاتصال بالمنزل". يجب تكوين قائمة بأهداف التحقيق في ملف تعريف AC Posture (وضعية التيار المتردد) على جانب ISE. يمكنك تحديد IPs/FQDNs مفصولة بفاصلات، باستخدام علامة نقطية يمكنك تحديد رقم المنفذ لكل وجهة اتصال رئيسية. يجب أن يكون هذا المنفذ مساويا للمنفذ الذي يتم تشغيل بوابة إمداد العميل عليه. توجد معلومات على جانب العميل حول الاتصال بالخوادم المنزلية في ISEPostureCFG.xmlيمكن العثور على هذا الملف في المجلد - C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture\.

في حالة عدم امتلاك هذه إستدعاء المنزل للجلسة، يلزم إجراء بحث عن المالك في هذه المرحلة. ترشد وحدة AC ISE Posture (وضعية محرك خدمات الهوية (ISE)) ISE لبدء بحث المالك باستخدام عنوان URL هذه خاص - /auth/ng-discovery طلب. كما يحتوي أيضا على قائمة عناوين IP و MAC الخاصة بالعميل. بعد إستلام هذه الرسالة بواسطة جلسة VPN، يتم إجراء بحث الوأ محليا (يستخدم اذا البحث الك من IPs و MACs من الطلب الذي تم إرساله بواسطة وحدة وضع AC ISE). إذا لم يتم العثور على جلسة العمل، يقوم PSN بعد استعلام عقدة MNT. يحتوي اذا الطلب على قائمة MACs فقط، وتتيجة لذلك، يجب الحصول على FQDN الخاص بالمالك من MNT. بعد هذا، ترجع PSN المالكين FQDN مرة أخرى إلى العميل. يتم إرسال الطلب التالي من العميل إلى FQDN لمالك جلسة العمل مع المصادقة/الحالة في URL وقائمة عناوين IP و MACs.

- Probe 2 - في هذه المرحلة، تحاول وحدة وضع AC ISE Posture PSN FQDNs الموجودة في ConnectionData.xml. يمكن العثور على اذا الملف في C:\Users\

  \AppData\Local\Cisco\Cisco AnyConnect Secure Mobility Client\

  . تقوم وحدة AC ISE Posture النمطية بإنشاء اذا الملف بعد محاولة الوضع الأولى. يحتوي الملف على قائمة بقوائم ISE PSNs FQDNs. يمكن تحديث محتوى القائمة ديناميكيا أثناء محاولات الاتصال التالية. الهدف النهائي لهذا التحقيق هو الحصول على FQDN لمالك الجلسة الحالية. التنفيذ مطابق ل Probe 1. مع الفرق الوحيد في تحديد وجهة المسار.
  الملف نفسه موجود في مجلد المستخدم الحالي في حالة إستخدام الجهاز من قبل عدة مستخدمين. ال يمكن لمستخدم آخر إستخدام معلومات من اذا الملف. قد يؤدي اذا إلى حدوث مشكلة الدجاجة والبيضة في البيانات التي ال يتم فيها إعادة التوجيه عند عدم تحديد أهداف الاتصال بالمنزل.

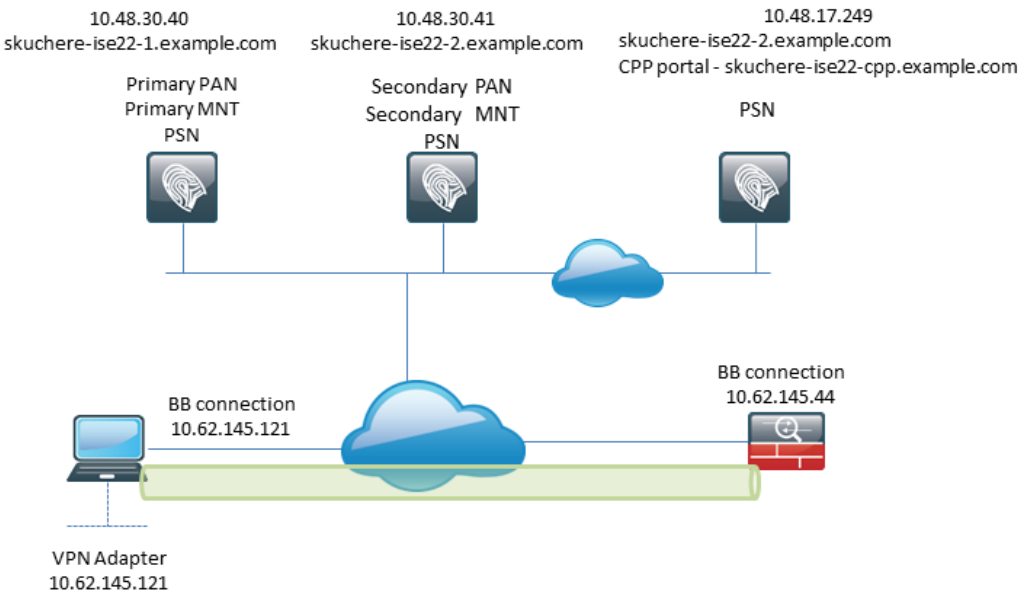
الخطوة 15. بعد الحصول على معلومات حول مالك جلسة العمل، تتطابق جميع الخطوات التالية مع تدفق ISE 2.2.

التكوين

بالنسبة لهذا المستند، يتم إستخدام ASAv كجهاز وصول إلى الشبكة. يتم إجراء جميع الاختبارات باستخدام الوضع عبر VPN. خارج نطاق المستند تكوين ASA للوضع عبر VPN. لمزيد من التفاصيل، ارجع إلى [ASA الإصدار 9.2.1 VPN Posture (وضعية الشبكة) مع مثال تكوين ISE](#).

ملاحظة: بالنسبة للنشر مع مستخدمي شبكة VPN، يكون الإعداد الموصى به هو الوضع القائم على إعادة التوجيه. ال يوصى بتكوين CallHomelist. بالنسبة لجميع المستخدمين الذين ال تستند إلى شبكة VPN، تأكد من تطبيق قائمة التحكم في الوصول للمنفذ (DACL) بحيث ال يتحدثون إلى PSN حيث تم تكوين الوضع.

الرسم التخطيطي للشبكة



شكل 3-1

هذه الطوبولوجيا تستخدم في الاختبارات. باستخدام ASA، من الممكن محاكاة السيناريو بسهولة عند فشل آلية SSO لمدخل إمداد العميل على جانب PSN، بسبب ميزة NAT. في حالة تدفق الوضع العادي عبر شبكة VPN، يجب أن يعمل SSO بشكل جيد نظرا لأن NAT ال يتم فرضه عادة لشبكات VPN IP عندما يدخل المستخدمون شبكة الشركة.

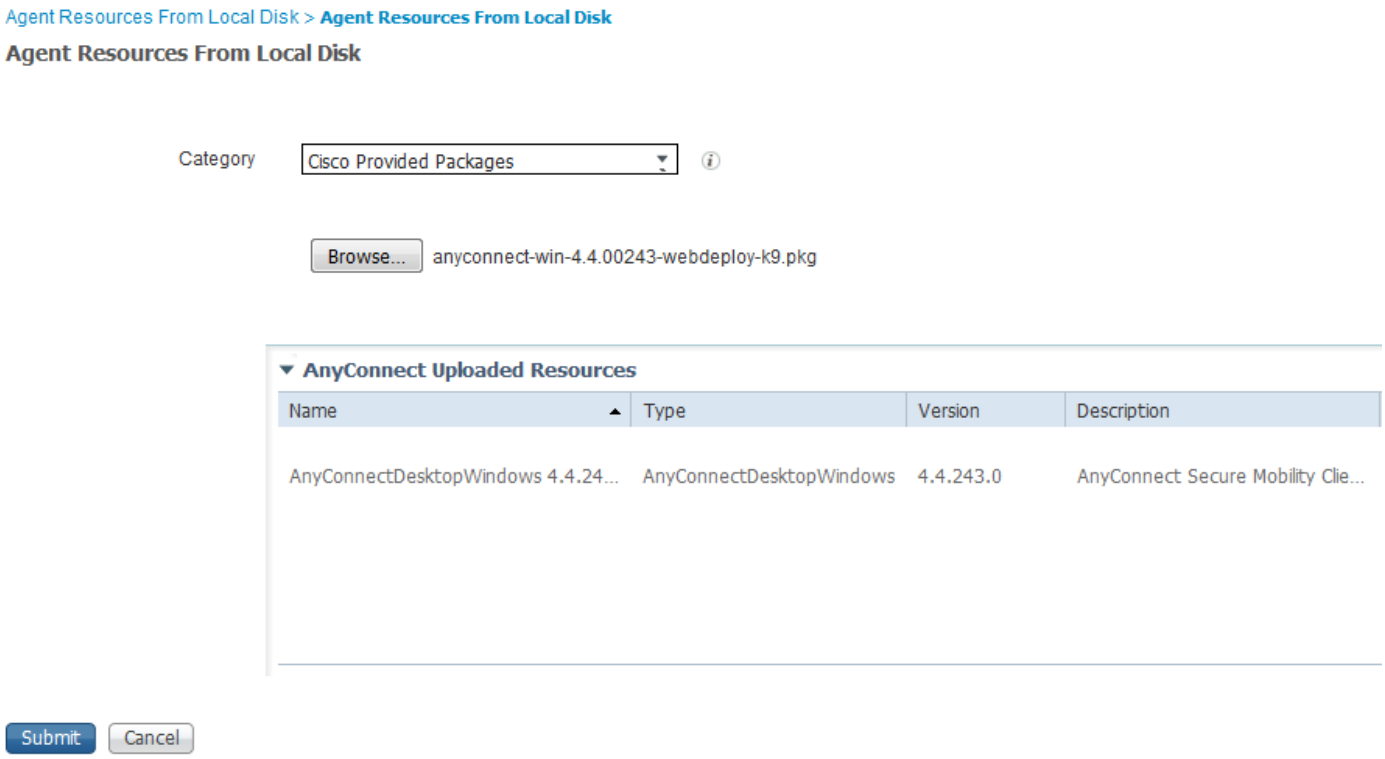
التكوينات

تكوين إمداد العميل

هذه هي الخطوات لإعداد تكوين AnyConnect.

الخطوة 1. تنزيل حزمة AnyConnect. ال تتوفر حزمة AnyConnect نفسها للتنزيل المباشر من ISE، لذلك قبل البدء، تأكد من توفر التيار المتردد على الكمبيوتر الشخصي. يمكن إستخدام هذا الارتباط لتنزيل التيار المتردد - https://www.cisco.com/site/us/en/products/security/secure-client/index.html. في هذا المستند، anyconnect-win-4.4.00243-webdeploy-k9.pkg تم إستخدام الحزمة.

الخطوة 2. لتحميل حزمة AC إلى ISE، انتقل إلى Policy > Policy Elements > Results > Client Provisioning > Resourcesوانقر فوق Add. أختر مورد "الوكيل" من القرص المحلي. في النافذة الجديدة، أختر Cisco Provided Packages,انقر browse واختر حزمة التيار المتردد على الكمبيوتر الشخصي.

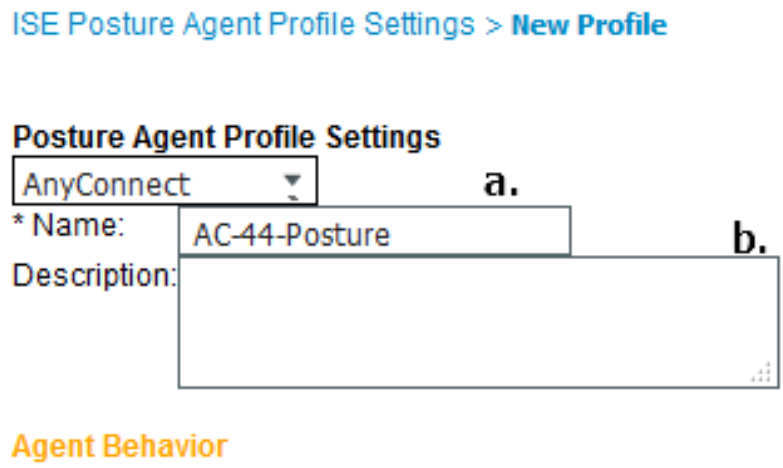


شكل 3-2

انقر Submit لإنهاء الاستيراد.

الخطوة 3. يجب تحميل وحدة التوافق النمطية إلى ISE. في نفس الصفحة، انقر Add واختيار Agent resources from Cisco site. في قائمة الموارد، يجب عليك التحقق من وحدة التوافق النمطية. لهذا المستند، تم AnyConnectComplianceModuleWindows 4.2.508.0 يتم إستخدام وحدة التوافق.

الخطوة 4. يجب إنشاء ملف تعريف AC Posture الآن. انقر Add واختيار NAC agent or Anyconnect posture profile.



شكل 3-3

- أختر نوع ملف التخصيص. يجب إستخدام AnyConnect لهذا السيناريو.

- حدد اسم ملف التعريف. انتقل إلى Posture Protocol قسم من التوصيف.

Posture Protocol

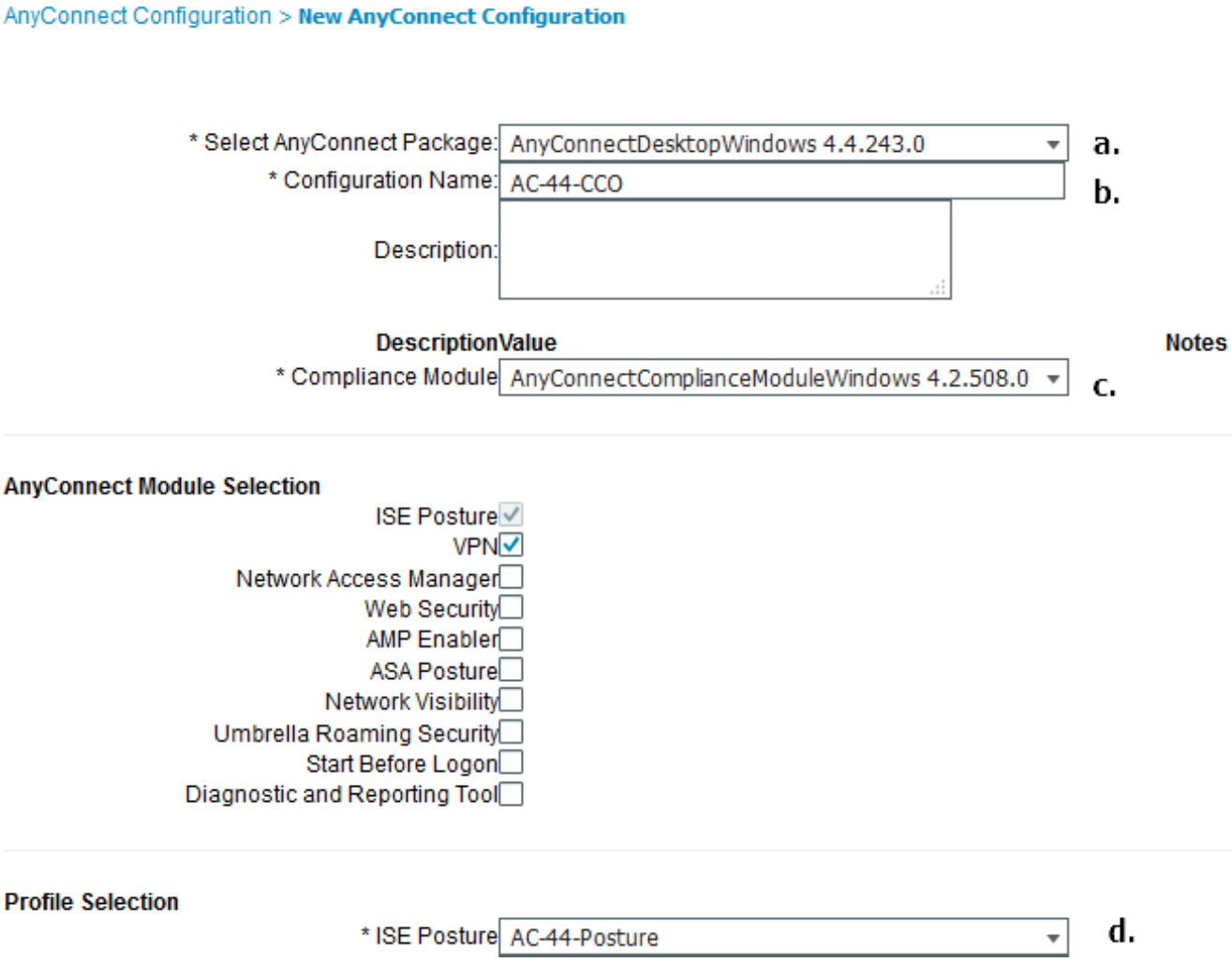
Parameter	Value	Notes
PRA retransmission time	120 secs	
Discovery host		
* Server name rules	* a.	need to be blank by default to force admin to enter a value. "*" means agent will connect to all
Call Home List	skuchere-ise22-2.examp b.	List of IP addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.

شكل 3-4

- تحديد Server Name Rules، ال يمكن أن يكون هذا الحقل فارغا. يمكن أن يحتوي الحقل على FQDN مع حرف بدل الذي يقيد اتصال وحدة وضع ISE ل AC إلى PSNs من مساحة الاسم المناسبة. ضع نجمة إذا كان يجب السماح بأي FQDN.
- الأسماء و IPs المحددة هنا قيد الاستخدام أثناء المرحلة 2 من اكتشاف الوضع. يمكنك إضافة أسماء منفصلة حسب أرقام المنافذ بالإضافة إلى أرقام المنافذ بعد FQDN/IP باستخدام النقطتين. في حال نشر التيار المتردد خارج النطاق (وليس من بوابة إمداد عميل ISE) باستخدام GPO أو أي نظام إمداد برمجي آخر، يصبح وجود عناوين Call Home أمرا ضروريا لأن هذا مسبر واحد فقط يمكنه الوصول إلى ISE PSN بنجاح. وهذا يعني أنه في حالة توفير التيار المتردد خارج النطاق، يجب على المسؤول إنشاء ملف تعريف AC ISE Posture باستخدام محرر ملف تعريف التيار المتردد وتوفير هذا الملف مع تثبيت AC.

ملاحظة: ضع في اعتبارك أن وجود عناوين الاتصال بالمنزل أمر بالغ الأهمية لأجهزة الكمبيوتر متعددة المستخدمين. مراجعة الخطوة 14. في تدفق Posture بعد ISE 2.2.

الخطوة 5.قم بإنشاء تكوين AC. انتقل إلى Policy > Policy Elements > Results > Client Provisioning > Resources، انقر Add، ثم أختر AnyConnect Configuration.

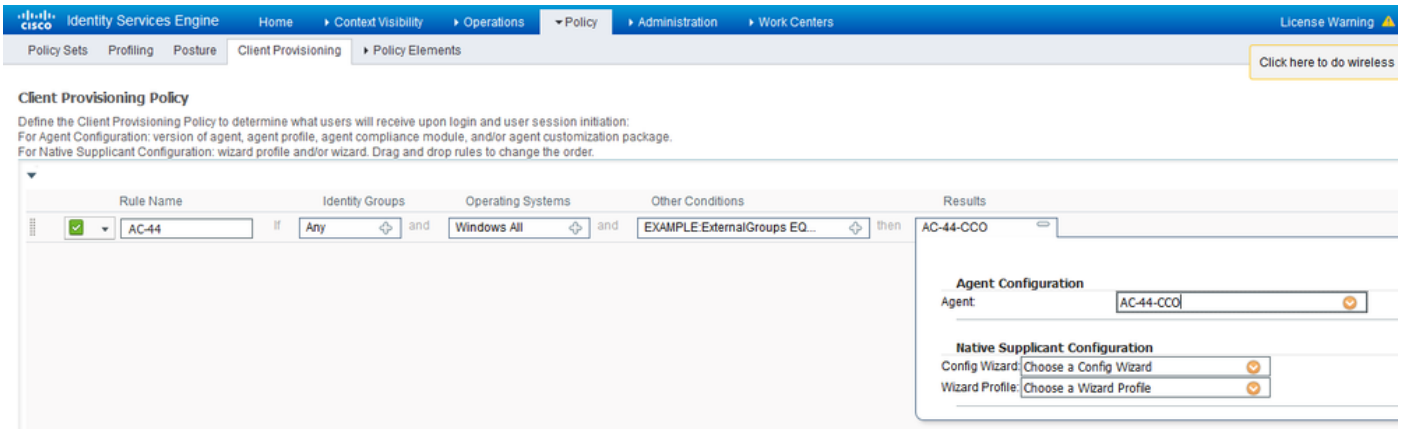


شكل 3-5

- أختر حزمة التياز المتردد.
- قم بتوفير اسم تكوين التياز المتردد.
- أختر إصدار وحدة التوافق النمطية.
- أختر ملف تعريف تكوين وضعية التياز المتردد من القائمة المنسدلة.

الخطوة 6. تكوين نهج توفير العميل. انتقل إلى Policy > Client Provisioning. في حالة التكوين الأولي، يمكنك تعبئة القيم الفارغة في السياسة المقدمة مع الافتراضيات. إذا احتجت لإضافة سياسة إلى تكوين الوضع الموجود، انتقل إلى السياسة التي يمكن إعادة إستخدامها واختر Duplicate Above أو Duplicate Below . كما يمكن إنشاء سياسة جديدة تماما.

هذا مثال على السياسة المستخدمة في المستند.



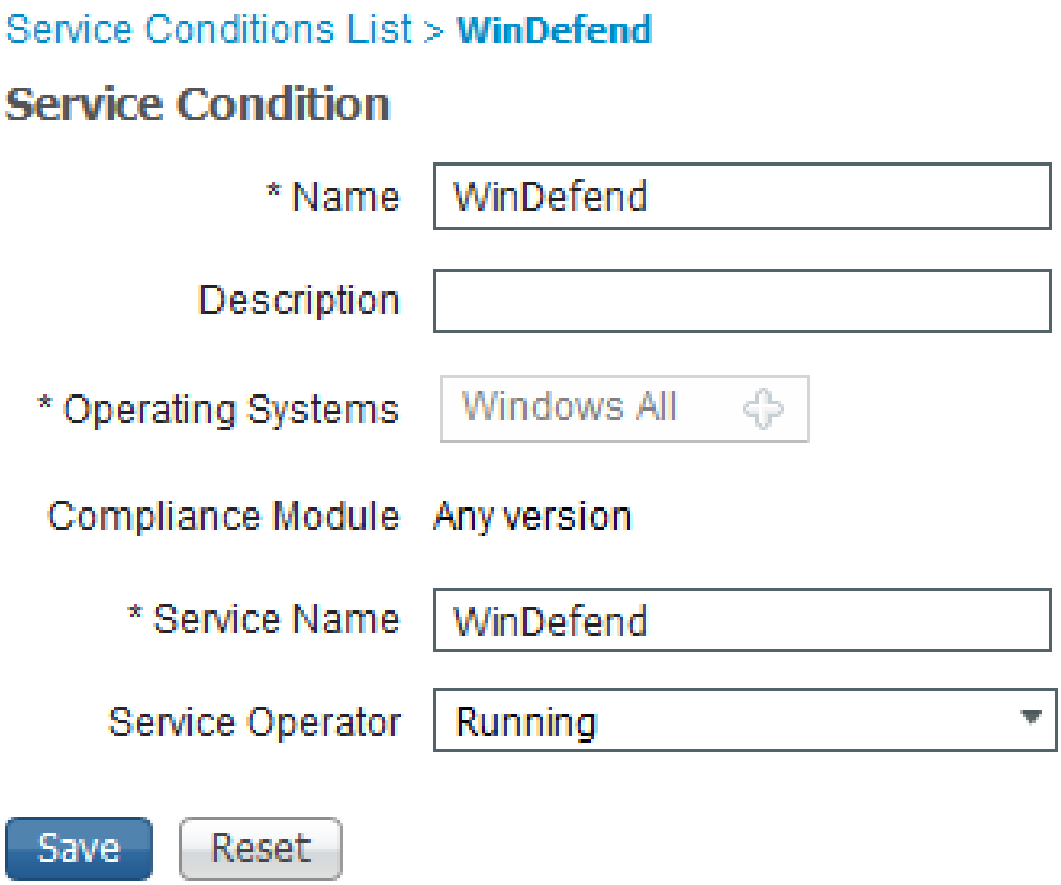
شكل 3-6

أختر تكوين التيار المتردد في قسم النتائج. تذكر أنه في حالة فشل SSO، يمكن أن يكون ل ISE سمات فقط من تسجيل الدخول إلى البوابة. تقتصر هذه السمات على المعلومات التي يمكن إستردادها حول المستخدمين من مخازن الهوية الداخلية والخارجية. في هذا المستند، يتم إستخدام مجموعة AD كشرط في نهج توفير العميل.

سياسات وشروط الوضع

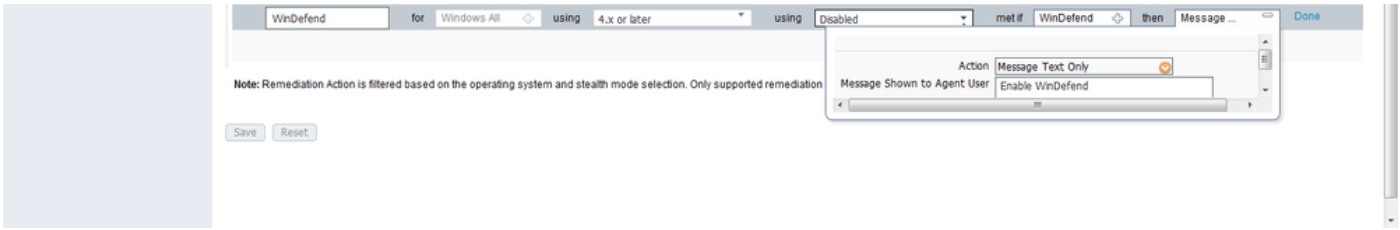
يتم إستخدام فحص بسيط للوضع. تم تكوين ISE للتحقق من حالة خدمة Window Defender على جانب الجهاز الطرفي. قد تكون سيناريوهات الحياة الواقعية أكثر تعقيدا ولكن خطوات التكوين العام هي نفسها.

الخطوة 1. قم بإنشاء حالة. توجد شروط الوضع في Policy > Policy Elements > Conditions > Posture. أختر نوع شرط الوضع. فيما يلي مثال على حالة خدمة يجب التحقق مما إذا كانت خدمة Windows Defender قيد التشغيل.



شكل 3-7

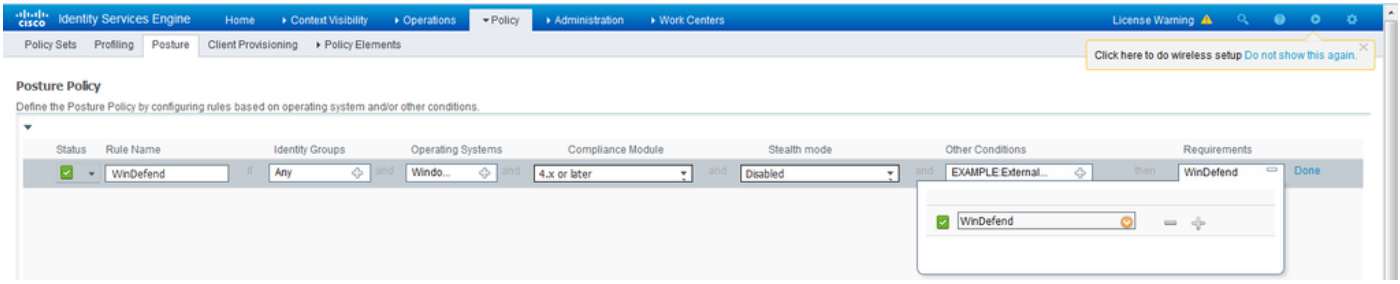
خطوة 2.Posture متطلب تشكيل. انتقل إلى Policy > Policy Elements > Results > Posture > Requirements. هذا مثال على التحقق من Window Defender:



شكل 3-8

أختر شرط الوضع الخاص بك في المتطلب الجديد وحدد إجراء الإصلاح.

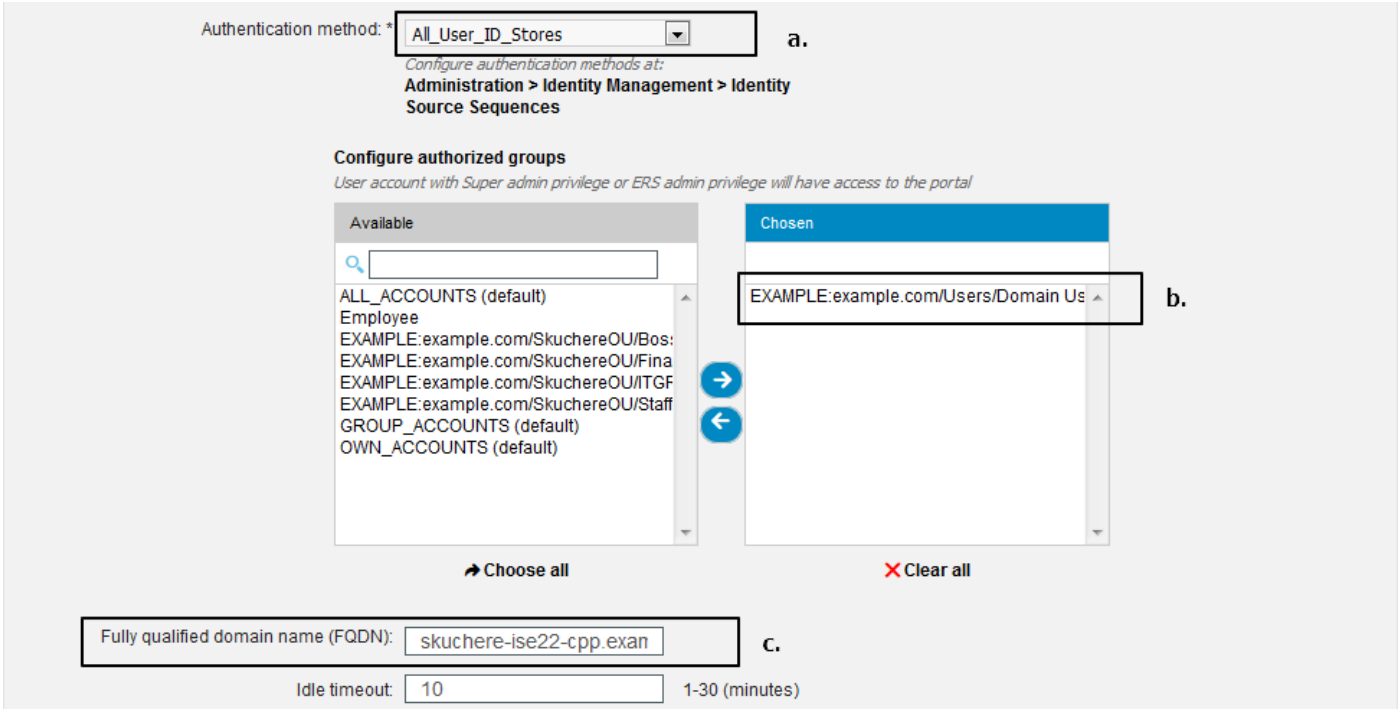
الخطوة 3. تكوين نهج الوضع. انتقل إلى Policy > Posture. هنا، يمكنك العثور على مثال للنهج المستخدم لهذا المستند. يحتوي النهج على متطلبات Windows Defender المعينة كإلزامية ويحتوي فقط على اسم مجموعة AD خارجي كشرط.



شكل 3-9

تكوين مدخل توفير العميل

بالنسبة للوضع دون إعادة التوجيه، يجب تحرير تكوين مدخل توفير العميل. انتقل إلى Administration > Device Portal Management > Client Provisioning.يمكنك إما إستخدام البوابة الافتراضية أو إنشاء البوابة الخاصة بك. يمكن إستخدام نفس المدخل لكل من الوضعيات مع ودون إعادة التوجيه.



شكل 3-10

يجب تحرير هذه الإعدادات في تكوين المدخل لسيناريو عدم إعادة التوجيه:

- في المصادقة، حدد تسلسل مصدر الهوية الذي يجب إستخدامه إذا تعذر على SSO تحديد موقع جلسة للمستخدم.
- طبقا لقائمة "تسلسل مصدر الهوية" المحددة للمجموعات المتاحة، يتم ملؤها. عند هذه النقطة، يجب تحديد المجموعات المعتمدة لتسجيل الدخول إلى المدخل.
- يجب تحديد FQDN لمدخل توفير العميل لسيناريوهات عند الحاجة إلى نشر AC من مدخل إمداد العميل. يجب حل FQDN هذا إلى ISE PSNs IPs. يجب توجيه المستخدمين لتحديد FQDN في مستعرض الويب أثناء محاولة الاتصال الأولى.

تكوين توصيفات التخويل والنهج

يجب تقييد الوصول الأولي للعملاء في حالة عدم توفر حالة الوضع. ومن الممكن تحقيق هذه الغاية بطرق متعددة:

- تعيين قائمة التحكم في الوصول للبنية الأساسية (DACL) - أثناء مرحلة الوصول المقيد، يمكن تعيين قائمة التحكم في الوصول للبنية الأساسية (DACL) للمستخدم للحد من الوصول. يمكن إستخدام هذا النهج لأجهزة الوصول إلى الشبكة من Cisco.
- VLAN Assignment - قبل أن يمكن وضع المستخدمين الناجحين في شبكة VLAN المقيدة، يجب أن يعمل هذا النهج بشكل جيد لأي مورد و NAD تقريبا.
- RADIUS Filter-ID - باستخدام هذه السمة، يمكن تعيين قائمة التحكم في الوصول (ACL) المعرفة محليا على NAD للمستخدم الذي لديه حالة وضع غير معروفة. وانظر لأن هذه سمة قياسية من سمات RFC، فيجب أن يعمل هذا النهج بشكل جيد لجميع موردي NAD.

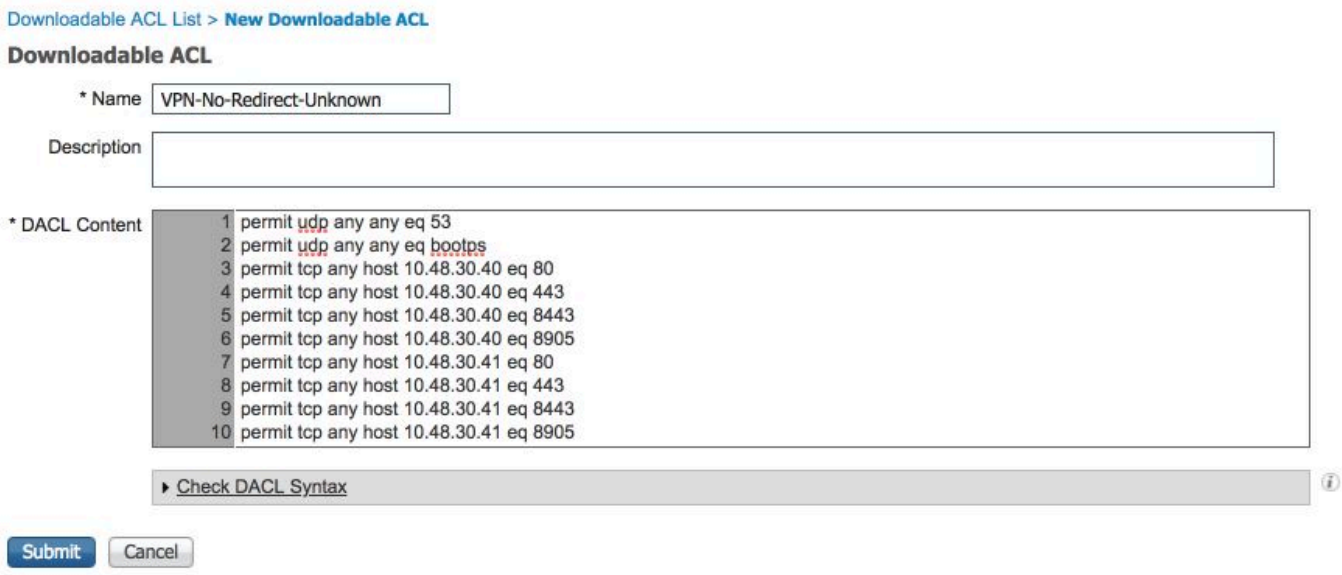
الخطوة 1. تكوين قائمة التحكم في الوصول إلى النقل (DACL). نظرا لأن هذا المثال يستند إلى ASA، يمكن إستخدام قائمة التحكم في الوصول الخاصة بالمنفذ (DACL) ل NAD. بالنسبة لسيناريوهات الحياة الواقعية، يجب مراعاة شبكة VLAN أو معرف المرشح كخيارات ممكنة.

لإنشاء DACL، انتقل إلى Policy > Policy Elements > Results > Authorization > Downloadable ACLsوانقر فوق Add.

أثناء حالة الوضع غير المعروف، يجب توفير هذه الأذونات على الأقل:

- حركة مرور DNS
- حركة مرور DHCP
- حركة المرور إلى ISE PSNs (المنافذ 443 و 80 إلمكانية فتح FQDN سهل من البوابة. المنفذ الذي يتم تشغيل بوابة CP عليه وه 8443 بشكل افتراضي ومنفذ 8905 للتوافق مع الإصدارات السابقة)
- حركة مرور البيانات إلى خوادم الإصلاح إذا لزم الأمر

هذا مثال على قائمة التحكم في الوصول للبنية الأساسية (DACL) بدون خوادم الإصلاح:



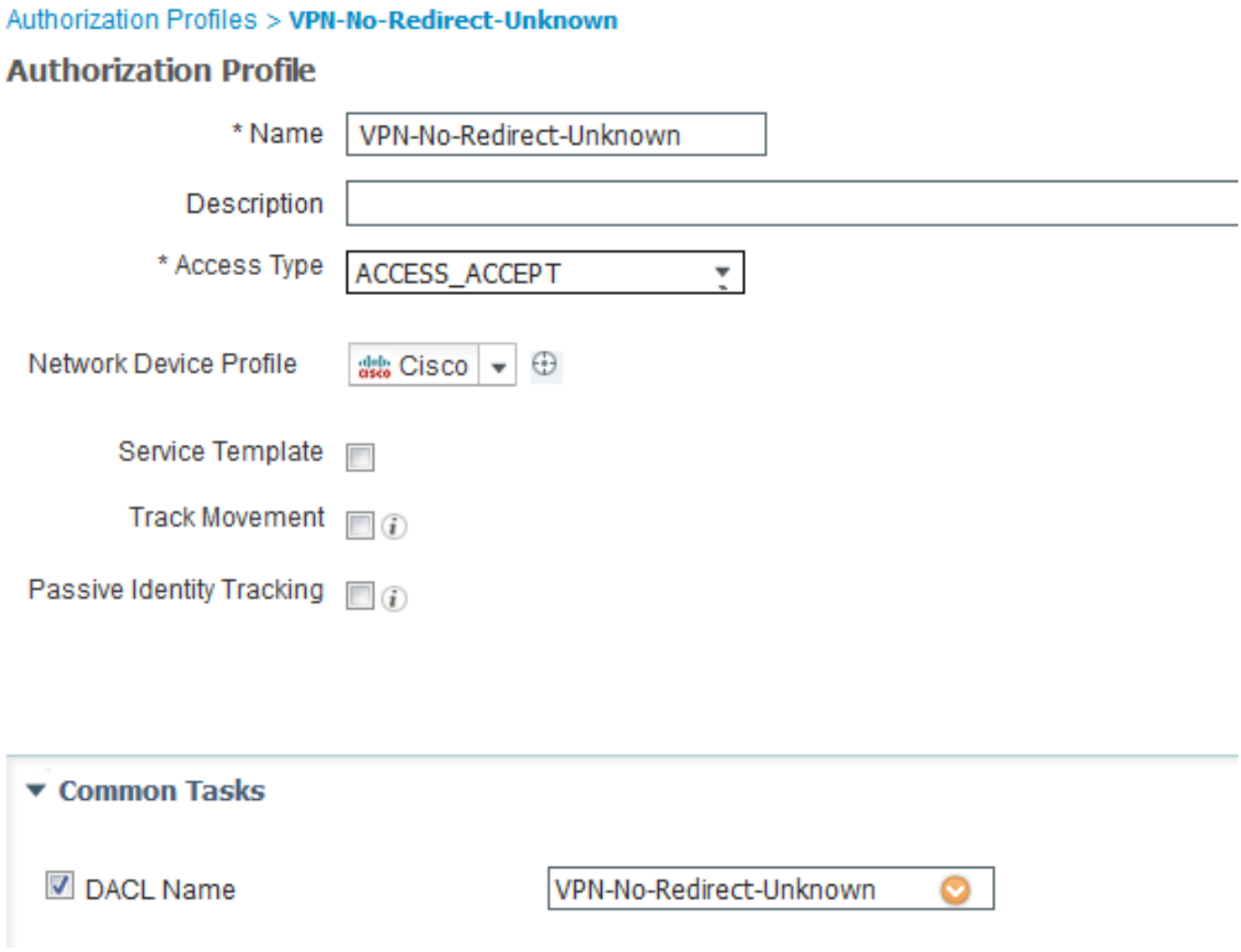
شكل 3-11

الخطوة 2. تكوين ملف تعريف التخويل.

كما هو معتاد بالنسبة للوضع، يلزم وجود توصيف تخويل. يجب أن يحتوي النوع الأول على أي نوع من تقييدات الوصول إلى الشبكة (ملف تعريف مع DACL المستخدم في هذا المثال). يمكن تطبيق ملف التعريف هذا على عمليات المصادقة التي لا تساوي حالة الوضع لها التوافق. يمكن أن يحتوي ملف التعريف الثاني للتخويل على السماح بالوصول فقط ويمكن تطبيقه على جلسات ذات حالة وضعية مساوية للتوافق.

لإنشاء ملف تعريف تخويل انتقل إلى Policy > Policy Elements > Results > Authorization > Authorization Profiles.

مثال على ملف تعريف الوصول المقيد:



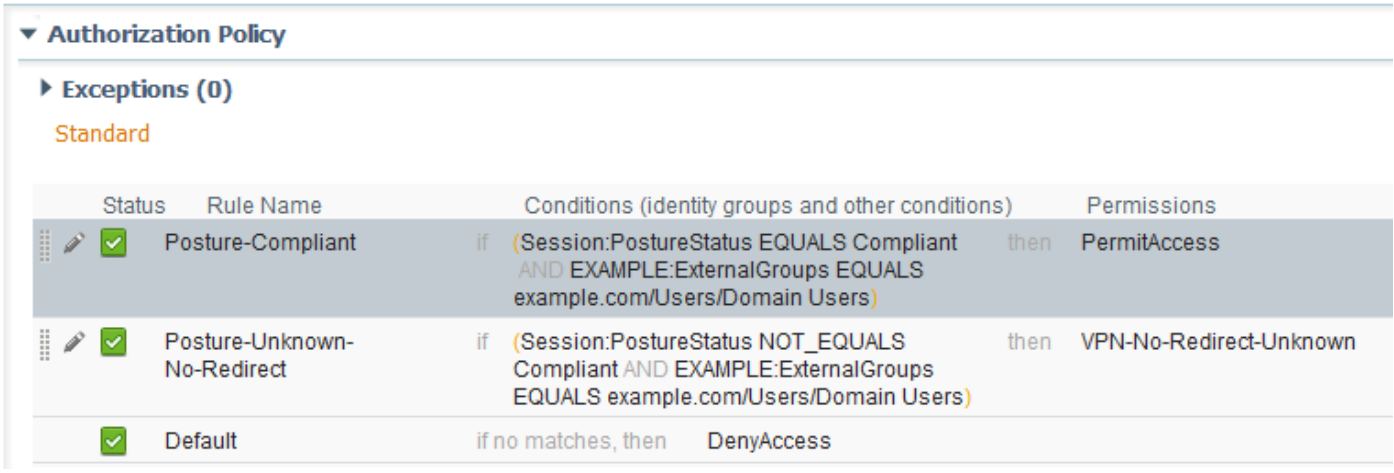
شكل 3-12

في هذا المثال، يتم إستخدام ISE Profile PermitAccess الافتراضي للجلسة بعد التحقق من حالة الوضع الناجح.

الخطوة 3. تكوين نهج التخويل. أثناء هذه الخطوة، يجب إنشاء نهج تخويل. الأولى هي

مطابقة طلب المصادقة الأولي مع حالة الوضع غير المعروف، والثانية هي تخصيص وصول كامل بعد عملية الوضع الناجح.

هذا مثال على سياسات التخويل البسيطة لهذه الحالة:



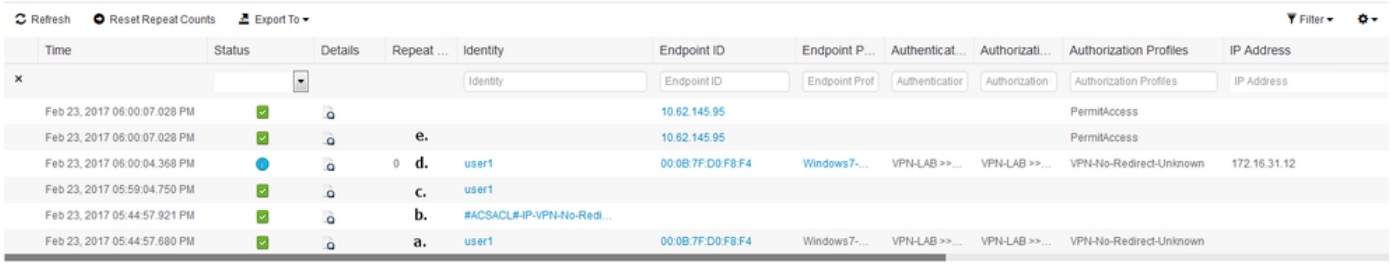
شكل 3-13

لا يعد تكوين نهج المصادقة جزءا من هذا المستند ولكن يجب أن تضع في الاعتبار أنه يجب قبل معالجة نهج التخويل المصادقة الناجحة.

التحقق من الصحة

يمكن أن يتألف التحقق الأساسي من التدفق من ثلاث خطوات رئيسية:

الخطوة 1. التحقق من تدفق المصادقة.



الشكل 4-1

1. المصادقة الأولية. بالنسبة لهذه الخطوة، قد تكون مهتما بالتحقق من صحة ما تم تطبيق ملف تعريف التخويل عليه. في حالة تطبيق ملف تعريف تخويل غير متوقع، تحقق من تقرير مصادقة مفصل. يمكنك فتح هذا التقرير بنقرة على العدسة المكبرة في عمود التفاصيل. يمكنك مقارنة السمات في تقارير المصادقة التفصيلية مع الشروط في سياسة التخويل التي تتوقع مطابقتها.

2. حدث تنزيل DACL. لا يتم عرض هذه السلسلة إلا في الحالة التي يحتوي فيها ملف تعريف التخويل المحدد للمصادقة الأولية على اسم DACL.

3. مصادقة المدخل - تشير هذه الخطوة في التدفق إلى أن آلية SSO فشلت في تحديد موقع جلسة عمل المستخدم. يمكن أن يحدث ذلك لأسباب متعددة:
   - لم يتم تكوين NAD لإرسال رسائل محاسبة أو أن عنوان IP المؤطر غير موجود بها
   - تم حل FQDN لبوابة CPP إلى IP لعقدة ISE بشكل مختلف عن العقدة التي تمت معالجة المصادقة الأولية فيها
   - العميل موجود خلف ال NAT

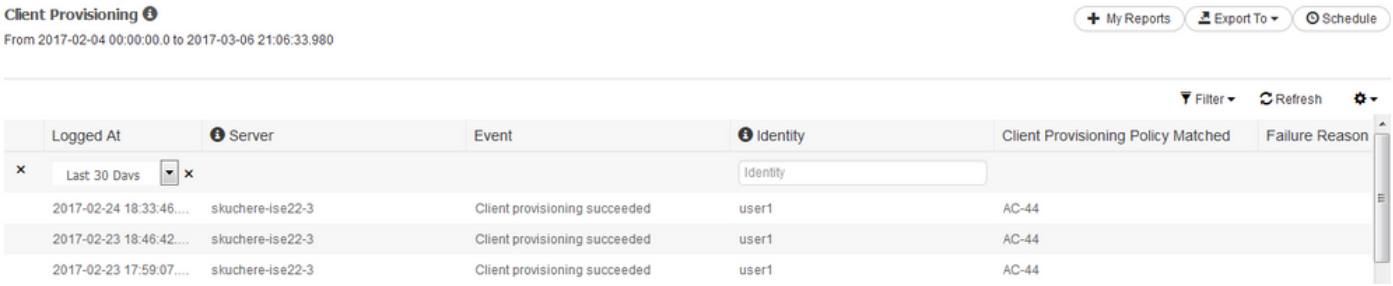
4. تغيير بيانات جلسة العمل. في هذا المثال تحديدا، تغيرت حالة جلسة العمل من "غير معروف" إلى "متوافق".

5. COA إلى جهاز الوصول إلى الشبكة. يجب أن تكون عملية COA هذه ناجحة لدفع المصادقة الجديدة من جانب NAD وتعييانت سياسة التخويل الجديدة إلى جانب ISE. في حالة فشل COA، يمكنك فتح تقرير مفصل للتحقق من السبب. يمكن أن تكون القضايا الأكثر شيوعا للكاكاو:
   - مهلة COA - في هذه الحالة، إما أن PSN الذي أرسل الطلب لم يتم تكوينه كعميل COA على جانب NAD، أو أن طلب COA قد تم إسقاطه في مكان ما على الطريق.
   - ACK السالب للكاكاو - يشير إلى أن الكاكاو قد تم إستلامه من قبل NAD ولكن لسبب ما ال يمكن تأكيد عملية الكاكاو. وبالنسبة لهذا السيناريو، يجب أن يحتوي التقرير المفصل على شرح أكثر تفصيلا.

ونظرا لاستخدام ASA كعنوان NAD لهذا المثال، ال يمكنك أن ترى أي طلب مصادقة لاحق للمستخدم. يحدث هذا بسبب حقيقة أن ISE يستخدم دفع COA ل ASA الذي يتجنب مقاطعة خدمة VPN. وفي مثل هذا السيناريو، يحتوي COA نفسه على معلمات تخويل جديدة، لذلك ال تكون هناك حاجة إلى إعادة المصادقة.

الخطوة 2.التحقق من تحديد نهج توفير العميل - لهذا الغرض، يمكنك تشغيل تقرير على ISE يمكن أن يساعدك على فهم نهج توفير العميل التي تم تطبيقها على المستخدم.

انتقل إلى Operations > Reports Endpoint and Users > Client Provisioning وشغل التقرير للتاريخ لليل انتا محتاج.



الشكل 4-2

باستخدام هذا التقرير، يمكنك التحقق من تحديد نهج توفير العميل. وفي حالة الفشل يجب أيضا عرض الأسباب في Failure Reason عمود.

الخطوة 3.التحقق من صحة تقرير الوضع - انتقل إلى Operations > Reports Endpoint and Users > Posture Assessment by Endpoint.

الشكل 4-3

يمكنك فتح تقرير مفصل من هنا لكل حدث معين للتحقق، على سبيل المثال، من معرف جلسة العمل الذي ينتمي إليه هذا التقرير، أي متطلبات الوضع المحددة تم تحديدها من قبل ISE لنقطة النهاية وحالة كل متطلب.

استكشاف الأخطاء وإصلاحها

معلومات عامة

لاستكشاف أخطاء عملية الوضع وإصلاحها، يجب تمكين مكونات ISE هذه لتصحيح الأخطاء على عقد ISE حيث يمكن أن تحدث عملية الوضع:

- client-webapp - المكون المسؤول عن توفير الوكيل. ملفات السجل الهدف guest.log و ise-psc.log.
- guestacess - المكون المسؤول عن مكون مدخل تزويد العميل والبحث عن مالك جلسة العمل (عندما يأتي الطلب إلى PSN خاطئ). ملف السجل الهدف - guest.log.
- provisioning - المكون المسؤول عن معالجة سياسة توفير العملاء. ملف السجل الهدف - guest.log.
- posture - كافة الأحداث المتعلقة بالوضع. ملف السجل الهدف - ise-psc.log.

بالنسبة لاستكشاف الأخطاء وإصلاحها من جانب العميل، يمكنك إستخدام ما يلي:

- acisensa.log -في حالة فشل توفير العميل على جانب العميل، يتم إنشاء هذا الملف في نفس المجلد الذي تم تنزيل NSA إليه (دليل التنزيلات ل Windows عادة).
- AnyConnect_ISEPosture.txt - يمكن العثور على هذا الملف في حزمة DART في الدليل Cisco AnyConnect ISE Posture Module. تم تسجيل جميع المعلومات حول اكتشاف ISE PSN والخطوات العامة لتدفق الوضع في هذا الملف.

أستكشاف المشكلات الشائعة وإصلاحها

المشاكل المتعلقة بالمسوحات القياسية القياسية

في حالة نجاح أحد مزودي الخدمة (SSO)، يمكنك رؤية هذه الرسائل في ise-psc.log، تشير هذه المجموعة من الرسائل إلى أن البحث عن جلسة العمل قد انتهى بنجاح ويمكن تجاوز المصادقة على المدخل.

```
<#root>

2016-11-09 15:07:35,951 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRu

looking for Radius session with input values : sessionId: null, MacAddr: null, ipAddr: 10.62.145.121


2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRu
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRu
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRu
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRu
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRu

Found session c0a801010002600058232bb8 using ipAddr 10.62.145.121
```

5-1 انفذة النص

يمكنك إستخدام عنوان IP لنقطة النهاية كمفتاح بحث للعثور على هذه المعلومات.

بعد ذلك بقليل في سجل الضيوف، يجب أن ترى أن المصادقة قد تم تخطيها:

```
<#root>

2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] guestaccess.flowmanager.step.cp.CPI
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] com.cisco.ise.portalSessionManager.
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] com.cisco.ise.portalSessionManager.
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] guestaccess.flowmanager.step.cp.CPI

Login step will be skipped, as the session =c0a801010002600058232bb8 already established for mac address


2016-11-09 15:07:36,066 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cpm.guestaccess.flowmanager.process
```

5-2 انفذة النص

وفي حال لم يتم العثور على الجلسة، فإن ise-psc log يحتوي الملف على معلومات حول فشل البحث عن الجلسة:

```
<#root>

2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cisco.cpm.posture.runtime.PostureRu
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cisco.cpm.posture.runtime.PostureRu
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cisco.cpm.posture.runtime.PostureRu

looking for session using IP 10.62.145.44


2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cisco.cpm.posture.runtime.PostureRu
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cisco.cpm.posture.runtime.PostureRu
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cisco.cpm.posture.runtime.PostureRu

No Radius session found
```

5-3 نافذة النص

في guest.log في مثل هذه الحالة، يجب أن ترى مصادقة المستخدم الكاملة على المدخل:

<#root>

```
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.flowmanager.step.St
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.flowmanager.step.St
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.flowmanager.step.St

Returning next step =LOGIN

2017-02-23 17:59:00,780 INFO [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.flowmanager.step.Ste
```

5-4 نافذة النص

في حالة فشل المصادقة على البوابة، يجب التركيز على التحقق من تكوين البوابة - أي مخزن هوية قيد الاستخدام؟ ما هي المجموعات المسموح لها بتسجيل الدخول؟

أستكشاف أخطاء تحديد نهج توفير العميل وإصلاحها

في حالة فشل نهج تزويد العميل أو معالجة النهج بشكل غير صحيح، يمكنك التحقق من guest.log للحصول على مزيد من التفاصيل:

<#root>

```
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.G

2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.common.utils.OSMapp
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.common.utils.OSMapp
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.
2017-02-23 17:59:07,505 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.

:user1:- CP Policy Status =SUCCESS, needToDoVlan=false, CoaAction=NO_COA
```

5-5 نافذة النص

في السلسلة الأولى، يمكنك رؤية كيفية إدخال معلومات حول جلسة العمل في محرك تحديد النهج، في حالة عدم تطابق النهج أو عدم تطابق النهج بشكل صحيح، يمكنك مقارنة السمات من هنا مع تكوين نهج توفير العميل. تشير السلسلة الأخيرة إلى حالة تحديد النهج.

أستكشاف أخطاء عملية الوضع وإصلاحها

من جانب العميل، يجب أن تكون مهتما بالتحقيق في التحقيقات ونتائجها. هذا مثال على تحقيق ناجح للمرحلة الأولى:

```
****************************************

Date : 02/23/2017
Time : 17:59:57
Type : Unknown
Source : acise

Description : Function: Target::Probe
Thread Id: 0x4F8
File: SwiftHttpRunner.cpp
Line: 1415
Level: debug

PSN probe skuchere-ise22-cpp.example.com with path /auth/status, status is -1..

****************************************
```

5-6 نافذة النص

في هذه المرحلة، يرجع PSN إلى معلومات التيار المتردد حول مالك الجلسة. يمكنك رؤية هذه الرسائل لاحقا:

```
****************************************

Date : 02/23/2017
Time : 17:59:58
Type : Unknown
Source : acise

Description : Function: Target::probeRecentConnectedHeadEnd
Thread Id: 0xBE4
File: SwiftHttpRunner.cpp
Line: 1674
Level: debug

Target skuchere-ise22-2.example.com, posture status is Unknown..

****************************************
```

5-7 نافذة النص

يقوم مالك جلسة العمل بإعادة كافة المعلومات المطلوبة إلى الوكيل:

```
**************************************

Date : 02/23/2017
Time : 17:59:58
Type : Unknown
Source : acise

Description : Function: SwiftHttpRunner::invokePosture
Thread Id: 0xFCC
File: SwiftHttpRunner.cpp
Line: 1339
Level: debug

MSG_NS_SWISS_NEW_SESSION, <?xml version="1.0" ?>
<root>
 <IP></IP>
 <FQDN>skuchere-ise22-2.example.com</FQDN>
 <PostureDomain>posture_domain</PostureDomain>
 <sessionId>c0a801010009e00058af0f7b</sessionId>
 <configUri>/auth/anyconnect?uuid=106a93c0-9f71-471c-ac6c-a2f935d51a36</configUri>
 <AcPackUri>/auth/provisioning/download/81d12d4b-ff58-41a3-84db-5d7c73d08304</AcPackUri>
 <AcPackPort>8443</AcPackPort>
 <AcPackVer>4.4.243.0</AcPackVer>
 <PostureStatus>Unknown</PostureStatus>
 <PosturePort>8443</PosturePort>
 <PosturePath>/auth/perfigo_validate.jsp</PosturePath>
 <PRAConfig>0</PRAConfig>
 <StatusPath>/auth/status</StatusPath>
 <BackupServers>skuchere-ise22-1.example.com,skuchere-ise22-3.example.com</BackupServers>
</root>
.

**************************************
```

5-8 انافذة النص

من جانب PSN، يمكنك التركيز على هذه الرسائل في guest.log عندما تتوقع أن الطلب الأولي الذي يأتي إلى العقدة ال يملك الجلسة:

```
<#root>

2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi

mac_list from http request ==> 00:0B:7F:D0:F8:F4,00:0B:7F:D0:F8:F4


2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi

iplist from http request ==> 172.16.31.12,10.62.145.95
```

```
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,368 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,369 ERROR [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov

Session Info is null


2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi

Performing MNT look up for macAddress ==> 00-0B-7F-D0-F8-F4


2017-02-23 17:59:56,539 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi

Performed MNT lookup, found session 0 with session id c0a801010009e00058af0f7b


2017-02-23 17:59:56,539 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
```

5-9 نافذة النص

هنا أنت يستطيع رأيت أن PSN يجاول أن الوأ يجد جلسة محلياً، وبعد فشل يدأ طلب إلى MNT مع الإستعلام عن IPs و MACs قائمة أن يجد الجلسة مالك.

بعد ذلك بقليل، يجب أن ترى طلبا من العميل على PSN الصحيح:

<#root>

```
2017-02-23 17:59:56,790 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun

ooking for session using session ID: null, IP addrs: [172.16.31.12, 10.62.145.95], mac Addrs [00:0B:7F:D


2017-02-23 17:59:56,790 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,791 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,792 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,792 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun

Found session c0a801010009e00058af0f7b using ipAddr 172.16.31.12
```

5-10 نافذة النص

تقوم PSN، كخطوة تالية، بإجراء بحث عن سياسة إمداد العميل لجلسة العمل هذه:

<#root>

```
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] com.cisco.cpm.swiss.SwissServer -:::
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,795 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 17:59:58,203 DEBUG [http-bio-10.48.30.41-8443-exec-8][] com.cisco.cpm.swiss.SwissServer -:::
2017-02-23 17:59:58,907 DEBUG [http-bio-10.48.30.41-8443-exec-10][] cisco.cpm.posture.util.AgentUtil -:
```

Increase MnT counter at CP:ClientProvisioning.ProvisionedResource.AC-44-Posture

انفذة النص 5-11

في الخطوة التالية، يمكنك رؤية عملية تحديد متطلبات الوضع. في نهاية الخطوة، يتم إعداد قائمة بالمتطلبات وإعادتها إلى الوكيل:

<#root>

```
2017-02-23 18:00:00,372 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureHan
```

About to query posture policy for user user1 with endpoint mac 00-0b-7f-d0-f8-f4

```
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureMan
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,432 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,433 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,433 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:03,884 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cpm.posture.runtime.agent.AgentXmlGe
2017-02-23 18:00:03,904 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cpm.posture.runtime.agent.AgentXmlGe
2017-02-23 18:00:03,904 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cpm.posture.runtime.agent.AgentXmlGe
2017-02-23 18:00:04,069 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureHan
 <version>ISE: 2.2.0.470</version>
 <encryption>0</encryption>
 <package>
 <id>10</id>
```

WinDefend

Enable WinDefend

3

0

3

WinDefend

3

301

WinDefend

running

(WinDefend)

</package>
</cleanmachines>

5-12 نافذة النص

لاحقا، يمكنك أن ترى أن تقرير الوضع تم إستلامه بواسطة PSN:

```
2017-02-23 18:00:04,231 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureHan
2017-02-23 18:00:04,231 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureHan
```

5-13 نافذة النص

في نهاية التدفق، يقوم ISE بتعليم نقطة النهاية على أنها متوافقة ويبدأ COA:

```
2017-02-23 18:00:04,272 INFO [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureMana
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureCoA
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureCoA
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureCoA
2017-02-23 18:00:04,273 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureCoA
2017-02-23 18:00:04,273 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureCoA
```

5-14 نافذة النص

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 دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).