

لائحة عم VPN Posture 9.2.1 رادصإلإ ASA إسه نلوكآ

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
التكوين
الرسم التخطيطي للشبكة وتدقق حركة مرور البيانات
التكوينات
ASA
محرك خدمات كشف الهوية (ISE)
إعادة تقييم دورية
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
تصحيح الأخطاء على ISE
تصحيح الأخطاء على ASA
تصحيح أخطاء الوكيل
فشل وضع وكيل NAC
معلومات ذات صلة

المقدمة

يصف هذا المستند كيفية تكوين جهاز الأمان القابل للتكيف (ASA) من إصدار Cisco 9.2.1 لوضع مستخدمي VPN (مقابل محرك خدمات تعريف Cisco ISE) دون الحاجة إلى عقدة وضعية في السطر (IPN).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية بتكوين ASA CLI وتكوين طبقة مأخذ التوصيل الآمنة (VPN SSL)
- معرفة أساسية بتكوين VPN للوصول عن بعد على ASA
- معرفة أساسية بخدمات ISE و Posture

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- برنامج ASA الإصدارات 9.2.1 من Cisco والإصدارات الأحدث
- Microsoft Windows الإصدار 7 مع Cisco AnyConnect Secure Mobility Client الإصدار 3.1
- Cisco ISE الإصدار 1.2 مع تصحيح 5 أو أحدث

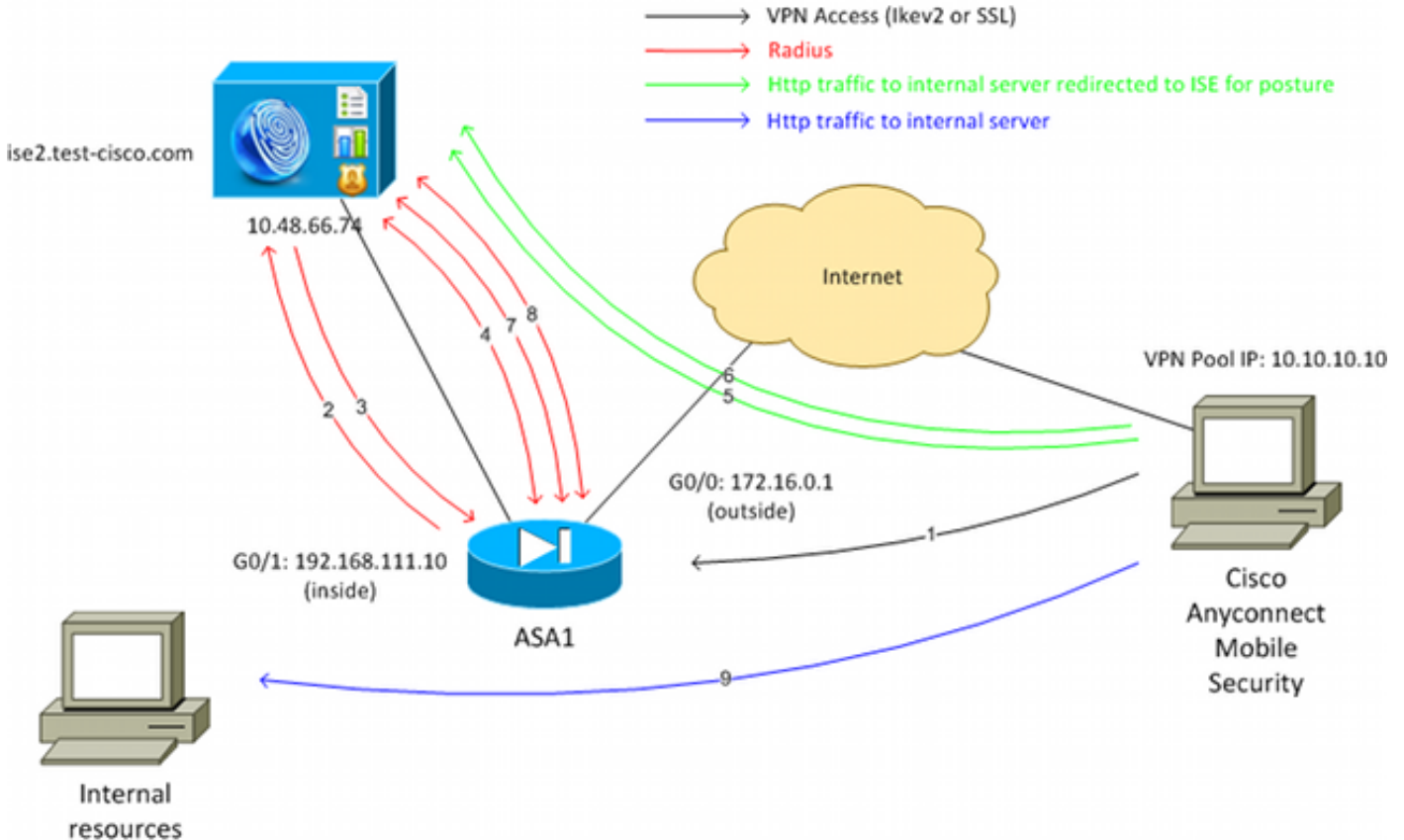
معلومات أساسية

يدعم الإصدار 9.2.1 من Cisco ASA تغيير تفويض (RFC 5176) (RADIUS (CoA)). وهذا يسمح بوضع مستخدمي VPN مقابل Cisco ISE دون الحاجة إلى شبكة IP. بعد أن يقوم مستخدم شبكة VPN بتسجيل الدخول، يقوم ASA بإعادة توجيه حركة مرور بيانات الويب إلى ISE، حيث يتم توفير المستخدم باستخدام وكيل التحكم في الدخول إلى الشبكة (NAC) أو وكيل ويب. يقوم البرنامج الوكيل بإجراء عمليات تحقق محددة على جهاز المستخدم لتحديد مدى توافقه مع مجموعة تم تكوينها من قواعد الوضع، مثل نظام التشغيل (OS) أو برامج التصحيح أو برامج مكافحة الفيروسات أو الخدمة أو التطبيقات أو قواعد التسجيل.

يتم بعد ذلك إرسال نتائج التحقق من صحة الوضع إلى ISE. إذا اعتبر الجهاز شكوى، فيمكن أن يرسل ISE ل RADIUS إلى ASA مع المجموعة الجديدة من سياسات التحويل. بعد نجاح التحقق من صحة الوضع وإعادة توجيه CoA، يتم السماح للمستخدم بالوصول إلى الموارد الداخلية.

التكوين

الرسم التخطيطي للشبكة وتدفق حركة مرور البيانات



وفيما يلي تدفق حركة المرور، كما هو موضح في الرسم التخطيطي للشبكة:

1. يستخدم المستخدم البعيد Cisco AnyConnect للوصول إلى VPN إلى ASA.
2. يرسل ال ASA طلب وصول RADIUS لذلك المستخدم إلى ISE.
3. يتوافق هذا الطلب مع النهج المسمى ASA92-Posture على ISE. ونتيجة لذلك، يتم إرجاع ملف تعريف تخويل ASA92-Posture. يرسل ISE قبول وصول RADIUS مع إثنين من أزواج Cisco Attribute-value:
`url-redirect-acl=redirect` - هذا هو اسم قائمة التحكم في الوصول (ACL) الذي يتم تعريفه محليا على ASA، والذي يحدد حركة المرور التي يجب إعادة توجيهها.
`url-redirect=https://ise2.test-cisco.com:8443/guestportal/gateway?sessionId=xx&action=cpp`
هذا هو عنوان URL الذي يجب إعادة توجيهه المستخدم البعيد إليه. تلميح: يجب أن تكون خوادم نظام اسم المجال (DNS) التي تم تعيينها لعملاء VPN قادرة على حل اسم المجال المؤهل بالكامل (FQDN) الذي تم إرجاعه في عنوان URL لإعادة التوجيه. إذا تم تكوين عوامل تصفية VPN لتقييد الوصول إلى مستوى مجموعة النفق، فتأكد من قدرة تجمع العملاء على الوصول إلى خادم ISE على المنفذ الذي تم تكوينه (TCP 8443 في هذا المثال).
4. يرسل ال ASA RADIUS Accounting-Request start ربط ويستلم إستجابة. وهذا أمر ضروري لإرسال جميع التفاصيل المتعلقة بالدورة إلى فريق الخبراء. وتتضمن هذه التفاصيل session_id وعنوان IP الخارجي لعميل VPN وعنوان IP الخاص ب ASA. يستخدم session_id لـ ISE لتحديد تلك الجلسة. يرسل أيضا ASA معلومات الحساب المؤقت الدورية، حيث تكون السمة الأكثر أهمية هي Framed-IP-Address مع IP الذي يتم تعيينه للعميل بواسطة (10.10.10.10) في هذا المثال.
5. عندما تطابق حركة المرور من مستخدم شبكة VPN قائمة التحكم في الوصول (ACL) المحددة محليا (إعادة التوجيه)، تتم إعادة توجيهها إلى `https://ise2.test-cisco.com:8443`. واعتمادا على التكوين، يقوم ISE بتوفير وكيل NAC أو وكيل الويب.
6. بعد تثبيت العميل على جهاز العميل، يقوم تلقائيا بإجراء فحوصات معينة. في هذا المثال، تبحث عن الملف `c:\test.txt`. كما أنها ترسل تقريرا عن الوضع إلى ISE، والذي يمكن أن يتضمن عمليات تبادل متعددة باستخدام البروتوكول السوبيري والمنافذ TCP/UDP 8905 من أجل الوصول إلى ISE.
7. عندما يستلم ISE تقرير الحالة من الوكيل، فإنه يقوم بمعالجة قواعد التحويل مرة أخرى. هذه المرة، تكون نتيجة الوضع معروفة ويتم الوصول إلى قاعدة أخرى. ويرسل حزمة RADIUS CoA:
إذا كان المستخدم متوافق، فسيتم إرسال اسم قائمة تحكم في الوصول (DAACL) قابل للتنزيل يسمح بالوصول الكامل (متوافق مع قاعدة AuthZ ASA92).
8. إذا كان المستخدم غير متوافق، فسيتم إرسال اسم DAACL الذي يسمح بالوصول المحدود (قاعدة AuthZ ASA92 غير متوافق). ملاحظة: دائما ما يتم تأكيد Cisco RADIUS CoA، أي أن ASA يرسل إستجابة إلى ISE لتأكيد.
ال ASA يزيل إعادة التوجيه. إذا لم يتم تخزين قوائم التحكم في الوصول الخاصة بالمنفذ (DAACL) مؤقتا، فيجب عليها إرسال طلب Access-Request لتنزيلها من ISE. يتم إرفاق قائمة التحكم في الوصول (DAACL) المحددة بجلسة عمل الشبكة الخاصة الظاهرية (VPN).
9. في المرة التالية التي يحاول فيها مستخدم الشبكة الخاصة الظاهرية (VPN) الوصول إلى صفحة الويب، يمكن للمستخدم الوصول إلى جميع الموارد المسموح بها من قبل قائمة التحكم في الوصول للبنية الأساسية (DAACL)

التي تم تثبيتها على ASA.

إذا لم يكن المستخدم متوافقاً، يتم منح حق الوصول المحدود فقط.

ملاحظة: يختلف نموذج التدفق هذا عن معظم السيناريوهات التي تستخدم RADIUS CoA بالنسبة لمصادقة 802.1x السلكية/اللاسلكية، لا يتضمن RADIUS CoA أي سمات. ولا يؤدي ذلك إلا إلى تشغيل المصادقة الثانية التي يتم فيها إرفاق جميع السمات، مثل DACL. بالنسبة لوضع ASA VPN، لا توجد مصادقة ثانية. يتم إرجاع جميع السمات في RADIUS CoA. ال VPN جلسة نشط و ليس من الممكن أن يغير معظم ال VPN مستعمل عملية إعداد.

التكوينات

استعملت هذا قسم in order to شكلت ال ASA وال ISE.

ASA

وفيما يلي تكوين ASA الأساسي للوصول إلى Cisco AnyConnect:

```
ip local pool POOL 10.10.10.10-10.10.10.100 mask 255.255.255.0

interface GigabitEthernet0/0
  nameif outside
  security-level 0
  ip address xxxxx 255.255.255.0
!
interface GigabitEthernet0/1
  nameif inside
  security-level 100
  ip address 192.168.111.10 255.255.255.0

aaa-server ISE protocol radius
aaa-server ISE (inside) host 10.48.66.74
  key cisco

webvpn
  enable outside
  anyconnect-essentials
  anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
  anyconnect enable
  tunnel-group-list enable

group-policy GP-SSL internal
group-policy GP-SSL attributes
vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

tunnel-group RA type remote-access
tunnel-group RA general-attributes
  address-pool POOL
  authentication-server-group ISE
  default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
  group-alias RA enable
```

لتكامل ASA مع ISE Posture (وضع محرك خدمات الهوية (ISE))، تأكد من:

- قم بتكوين خادم المصادقة والتفويض والمحاسبة (AAA) للتحويل الديناميكي لقبول CoA.
- قم بتكوين المحاسبة كمجموعة نفق لإرسال تفاصيل جلسة VPN نحو ISE.

- تكوين عملية المحاسبة المؤقتة التي ستقوم بإرسال عنوان IP المعين للمستخدم وتحديث حالة جلسة العمل بشكل دوري على ISE

- قم بتكوين قائمة التحكم في الوصول (ACL) المعاد توجيهها، والتي تحدد ما إذا كان مسموحًا بحركة مرور DNS و ISE. يتم إعادة توجيه جميع حركات مرور HTTP الأخرى إلى ISE للوضع. هنا مثال التكوين:

```
access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any host 10.48.66.74
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www
```

```
aaa-server ISE protocol radius
authorize-only
interim-accounting-update periodic 1
dynamic-authorization
aaa-server ISE (inside) host 10.48.66.74
key cisco
```

```
tunnel-group RA general-attributes
address-pool POOL
authentication-server-group ISE
accounting-server-group ISE
default-group-policy GP-SSL
```

محرك خدمات كشف الهوية (ISE)

أتمت هذا steps in order to شكلت ال ISE:

1. انتقل إلى إدارة < موارد الشبكة > أجهزة الشبكة وأضف ASA كجهاز شبكة:

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. Below the navigation bar, there are several tabs: 'System', 'Identity Management', 'Network Resources', 'Web Portal Management', and 'Feed Service'. The main content area is titled 'Network Devices List > New Network Device'. The form contains the following fields and options:

- Name:** ASA
- Description:** (empty)
- * IP Address:** 192.168.111.10 / 32
- Model Name:** (dropdown menu)
- Software Version:** (dropdown menu)
- * Network Device Group:**
 - Location:** All Locations (dropdown menu) with a 'Set To Default' button.
 - Device Type:** All Device Types (dropdown menu) with a 'Set To Default' button.
- Authentication Settings:** (checked)
 - Enable Authentication Settings:** (checkbox)
 - Protocol:** RADIUS
 - * Shared Secret:** (masked) with a 'Show' button.

انتقل إلى السياسة < النتائج < التفويض < قائمة التحكم في الوصول (ACL) القابلة للتزليل وقم بتكوين قائمة التحكم في الوصول (ACL) حتى تسمح بالوصول الكامل. يسمح التكوين الافتراضي لقائمة التحكم في الوصول (ACL) لجميع حركة مرور IP على ISE:

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. Below this, there are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', and 'Security Group Access'. The 'Results' tab is selected. On the left, a tree view shows the navigation structure, with 'Downloadable ACLs' highlighted. The main content area displays the configuration for a 'Downloadable ACL' named 'PERMIT_ALL_TRAFFIC'. The description is 'Allow all Traffic'. The DACL content is shown in a table with 10 rows, containing the command 'permit ip any any' in the first row. A 'Check DACL Syntax' button is visible at the bottom.

3. قم بتكوين قائمة تحكم في الوصول (ACL) مماثلة توفر وصولا محدودا (للمستخدمين غير المتوافقين).

4. انتقل إلى السياسة < النتائج < التفويض < ملفات تعريف التحويل وشكلت ملف تعريف التحويل المسمى ASA92-Posture، والذي يعيد توجيه المستخدمين للوضعية. حدد خانة الاختيار إعادة توجيه الويب، وحدد توفير العميل من القائمة المنسدلة، وتأكد من ظهور إعادة التوجيه في حقل قائمة التحكم في الوصول (ACL) الذي تم تحديد قائمة التحكم في الوصول (ACL) محليا على ASA:

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. Below this, there are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', and 'Security Group Access'. The 'Results' tab is active. On the left, a tree view shows the hierarchy: Authentication > Authorization > Authorization Profiles. The main content area displays the configuration for the 'ASA92-posture' Authorization Profile. The 'Name' field is 'ASA92-posture'. The 'Access Type' is 'ACCESS_ACCEPT'. Under 'Common Tasks', 'Web Redirection (CWA, DRW, MDM, NSP, CPP)' is checked, and the 'ACL' is set to 'redirect'.

5. قم بتكوين ملف تعريف التحويل المسمى ASA92 متوافق، والذي يجب أن يرجع فقط DACL المسمى ALLOW_ALL_TRAFFIC الذي يوفر الوصول الكامل للمستخدمين المتوافق:

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. Below this, there are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', and 'Security Group Access'. The 'Results' tab is active. On the left, a tree view shows the hierarchy: Authentication > Authorization > Authorization Profiles. The main content area displays the configuration for the 'ASA92-compliant' Authorization Profile. The 'Name' field is 'ASA92-compliant'. The 'Access Type' is 'ACCESS_ACCEPT'. Under 'Common Tasks', 'DACL Name' is checked, and the dropdown menu is set to 'PERMIT_ALL_TRAFFIC'.

6. قم بتكوين ملف تعريف تحويل مماثل باسم ASA92-غير متوافق، والذي يجب أن يرجع قائمة التحكم في الوصول للوسائط (DACL) ذات الوصول المحدود (للمستخدمين غير المتوافقين).

7. انتقل إلى السياسة < التفويض وتكوين قواعد التحويل:

قم بإنشاء قاعدة تسمح بالوصول الكامل إذا كانت نتائج الوضع متوافقة. والنتيجة هي سياسة التحويل المتوافقة مع ASA92.

قم بإنشاء قاعدة تسمح بالوصول المحدود إذا كانت نتائج الوضع غير متوافقة. والنتيجة هي سياسة التحويل غير المتوافقة.

تأكد من أنه إذا لم يتم الوصول إلى أي من القاعدتين السابقتين، تقوم القاعدة الافتراضية بإرجاع ASA92-Posture، والذي يفرض إعادة التوجيه على ASA.

ASA92 complaint	if Session:PostureStatus EQUALS Compliant	then ASA92-compliant
ASA92 non complaint	if Session:PostureStatus EQUALS NonCompliant	then ASA92-noncompliant
ASA92 redirect	if Radius:NAS-IP-Address EQUALS 192.168.111.10	then ASA92-posture

تحقق قواعد المصادقة الافتراضية من اسم المستخدم في مخزن الهوية الداخلي. إذا كان يجب تغيير ذلك (تم 8. إيداعه في Active Directory (AD)، على سبيل المثال)، فانتقل إلى نهج < مصادقة وقم بالتغيير:

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use.

Policy Type Simple Rule-Based

<input checked="" type="checkbox"/> MAB	: if Wired_MAB OR Wireless_MAB	Allow Protocols : Default Network Access
<input checked="" type="checkbox"/> Default	: use Internal Endpoints	
<input checked="" type="checkbox"/> Dot1X	: if Wired_802.1X OR Wireless_802.1X	Allow Protocols : Default Network Access
<input checked="" type="checkbox"/> Default	: use Internal Users	
<input checked="" type="checkbox"/> Default Rule (if no match)	: Allow Protocols : Default Network Access and use : Internal Users	

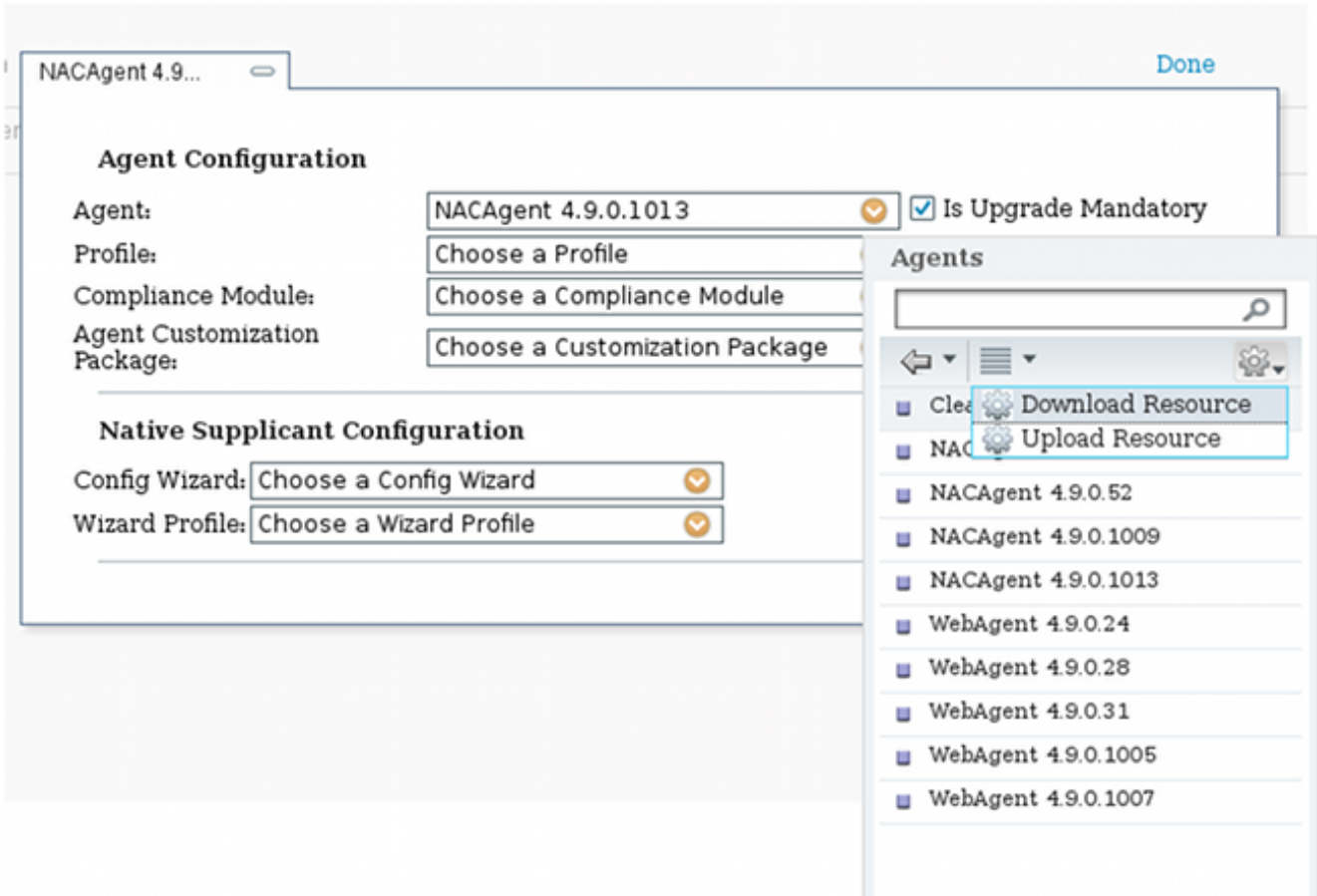
انتقل إلى نهج < إمداد العميل وقم بتكوين قواعد الإمداد. هذه هي القواعد التي تحدد نوع الوكيل الذي يجب توفيره. في هذا المثال، توجد قاعدة بسيطة واحدة فقط، ويحدد ISE وكيل NAC لجميع أنظمة Microsoft Windows:

Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
<input checked="" type="checkbox"/> ASA92-posture	if Any	and Windows All	and Condition(s)	then NACAgent 4.9.0.1013

عندما لا يكون الوكلاء على موقع شركة خدمات الإنترنت ISE، فمن الممكن تنزيلهم:



إذا كان ضروريا، يمكنك الانتقال إلى الإدارة < النظام < الإعدادات < الوكيل وتكوين وكيل ISE (للوصول إلى 10).

11. قم بتكوين قواعد الوضع، التي تتحقق من تكوين العميل. يمكنك تكوين القواعد التي تتحقق من:

الملفات - الوجود، الإصدار، التاريخ

السجل - المفتاح، القيمة، الوجود

التطبيق - اسم العملية، قيد التشغيل، لا قيد التشغيل

الخدمة - اسم الخدمة، قيد التشغيل، لا قيد التشغيل

برنامج مكافحة الفيروسات - تم دعم أكثر من 100 بائع، إصدار، عند تحديث التعريفات

برامج مكافحة التجسس - تم دعم أكثر من 100 بائع، الإصدار، عند تحديث التعريفات

حالة مركبة - مزيج من الكل

شروط القاموس المخصص - استخدام معظم قواميس ISE في هذا المثال، يتم إجراء التحقق من وجود ملف بسيط فقط. إذا كان الملف c:\test.txt موجودا على جهازك، العميل، فإنه متوافق مع الوصول الكامل المسموح به. انتقل إلى سياسة < شروط < شروط الملف وقم بتكوين حالة الملف:

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes Home, Operations, Policy, and Administration. The main menu has Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access, and Policy Elements. The left sidebar shows a tree view with Posture selected, and a search bar. The main content area is titled 'File Condition' and contains the following configuration fields:

- * Name: file_condition
- Description: (empty)
- * File Path: ABSOLUTE_PATH (dropdown) and C:\test.txt (text input)
- * File Type: FileExistence (dropdown)
- * File Operator: Exists (dropdown)
- * Operating System: Windows All (dropdown)

Buttons for 'Save' and 'Reset' are visible at the bottom.

13. انتقل إلى السياسة < النتائج < الوضع > المتطلبات وقم بإنشاء متطلب. يجب استيفاء هذا الشرط عند استيفاء الشرط السابق. وإذا لم يكن كذلك، يتم تنفيذ إجراء الإصلاح. قد يكون هناك العديد من أنواع إجراءات الإصلاح المتاحة، ولكن في هذا المثال، يتم استخدام أبسط واحدة: يتم عرض رسالة معينة.

The screenshot shows the Cisco Identity Services Engine (ISE) Results page. The top navigation bar is the same as in the previous screenshot. The left sidebar shows a tree view with Results selected. The main content area is titled 'Requirements' and contains a table with the following columns: Name, Operating Systems, Conditions, and Remediation Actions.

Name	Operating Systems	Conditions	Remediation Actions
file_requirement	for Windows All	met if file_condition	else Message Text Only
Any_AV_Installation_Win	for Windows All	met if ANY_av_win_inst	else Message Text Only
Any_AV_Definition_Win	for Windows All	met if ANY_av_win_def	else AnyAVDefRemediationWin
Any_AS_Installation_Win	for Windows All	met if ANY_as_win_inst	else Message Text Only
Any_AS_Definition_Win	for Windows All	met if ANY_as_win_def	else AnyASDefRemediationWin
Any_AV_Installation_Mac	for Mac OSX	met if ANY_av_mac_inst	else Message Text Only
Any_AV_Definition_Mac	for Mac OSX	met if ANY_av_mac_def	else AnyAVDefRemediationMac
Any_AS_Installation_Mac	for Mac OSX	met if ANY_as_mac_inst	else Message Text Only
Any_AS_Definition_Mac	for Mac OSX	met if ANY_as_mac_def	else Message Text Only

14. ملاحظة: في السيناريو العادي، يمكن استخدام إجراء معالجة الملف (يوفر ISE الملف القابل للتنزيل). انتقل إلى نهج < Posture (وضعية) واستخدم المتطلب الذي قمت بإنشائه في الخطوة السابقة (المسماة file_requirements) في قواعد الوضع. تتطلب قاعدة الوضع الوحيدة أن تفي كافة أنظمة Microsoft Windows بالملف requirements. وإذا استوفى هذا الشرط، تكون المحطة ممثلة؛ وإذا لم تستوف، تكون المحطة غير ممثلة.

The screenshot shows the Cisco Identity Services Engine (ISE) Posture Policy configuration page. The top navigation bar includes Home, Operations, Policy, and Administration. The main menu has Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access, and Policy Elements. The left sidebar shows a tree view with Posture selected. The main content area is titled 'Posture Policy' and contains the following configuration:

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

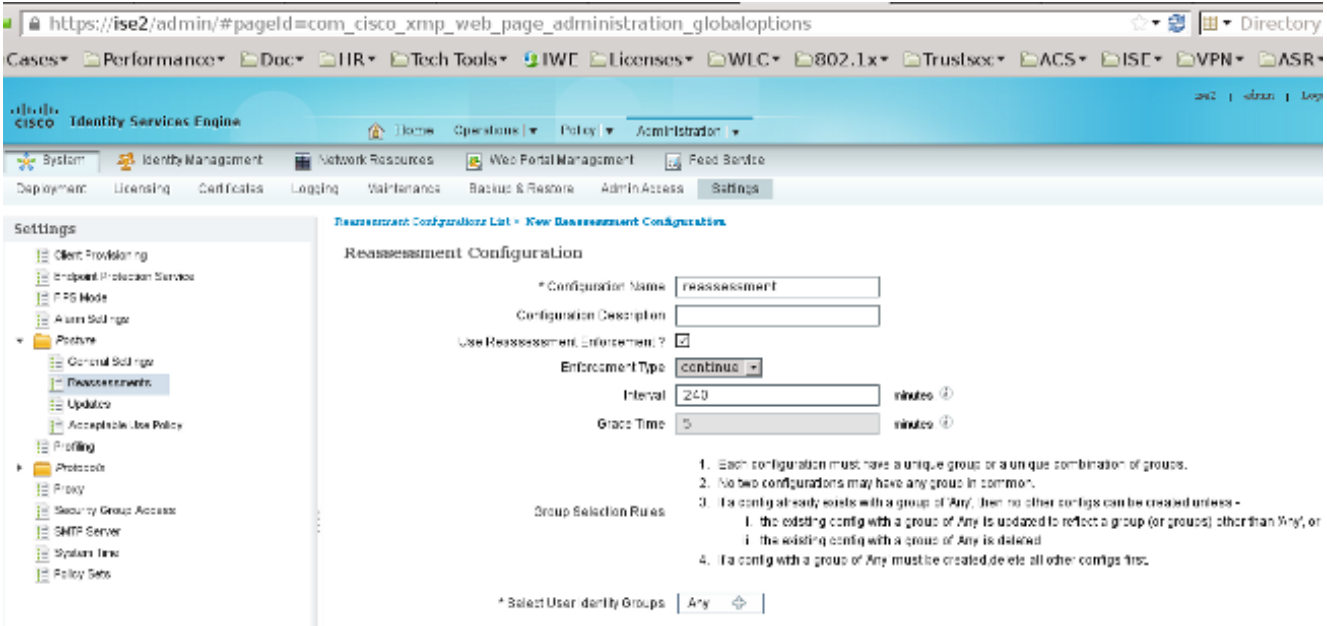
Status	Rule Name	Identity Groups	Operating Systems	Other Conditions	Requirements
✓	posture	if Any	and Windows All		then file_requirement

إعادة تقييم دورية

بشكل افتراضي، الوضع هو حدث لمرة واحدة. ومع ذلك، هناك حاجة في بعض الأحيان إلى التحقق دوريا من امثال المستخدم وتعديل إمكانية الوصول إلى الموارد استنادا إلى النتائج. يتم دفع هذه المعلومات عبر البروتوكول السوبسري (وكيل NAC) أو ترميزها داخل التطبيق (وكيل الويب).

أتمت هذا steps in order to فحصت المستعمل توافق:

1. انتقل إلى إدارة < إعدادات < وضعية < عمليات إعادة التقييم وتمكين إعادة التقييم بشكل عام (لكل تكوين مجموعة هوية):



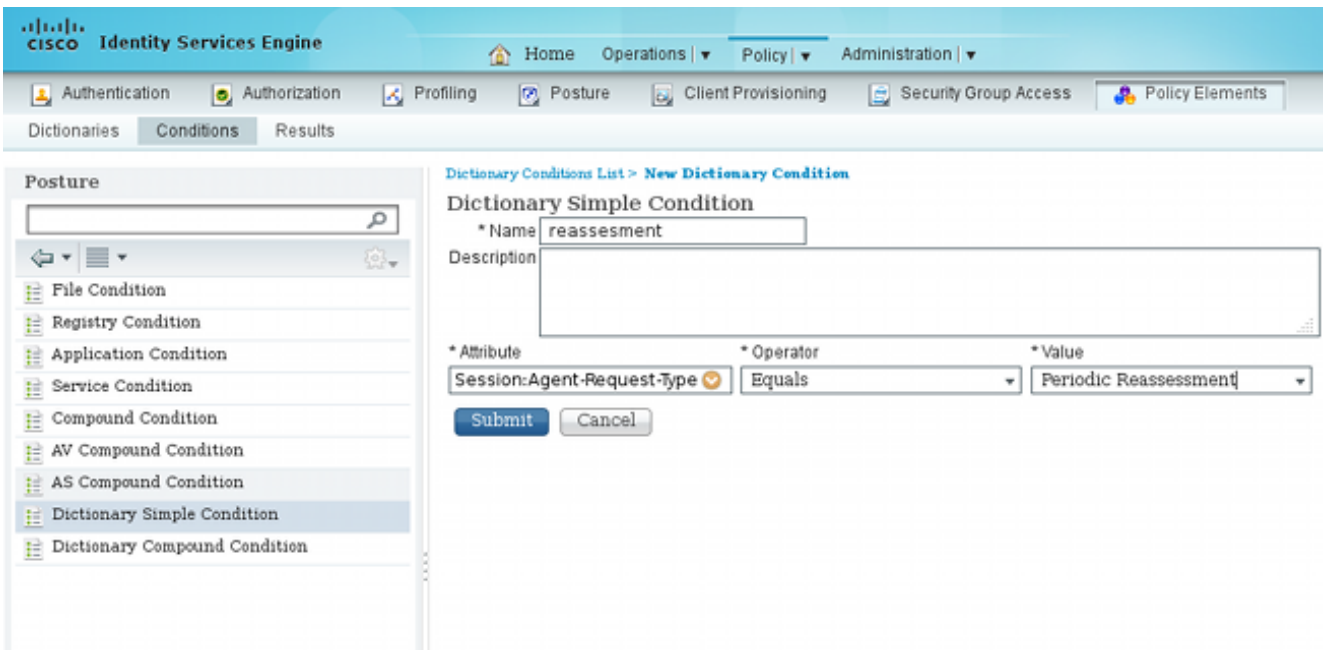
The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The main content area is titled 'Reassessment Configuration'. It contains the following fields and options:

- Configuration Name: reassessment
- Configuration Description: (empty)
- Use Reassessment Enforcement?:
- Enforcement Type: continuous
- Interval: 240 minutes
- Grace Time: 5 minutes
- Group Selection Rules: (empty)
- Select User Identity Groups: Any

Below the main configuration area, there are four numbered instructions:

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.

2. إنشاء حالة حالة تطابق كافة عمليات إعادة التقييم:

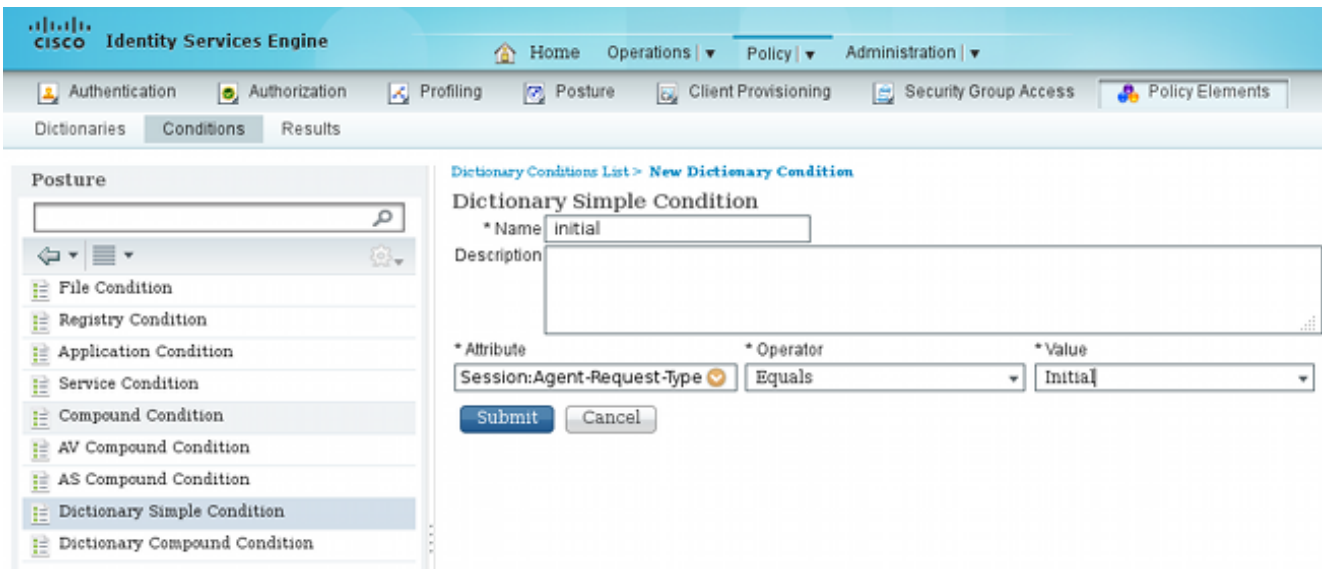


The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The main content area is titled 'Dictionary Simple Condition'. It contains the following fields and options:

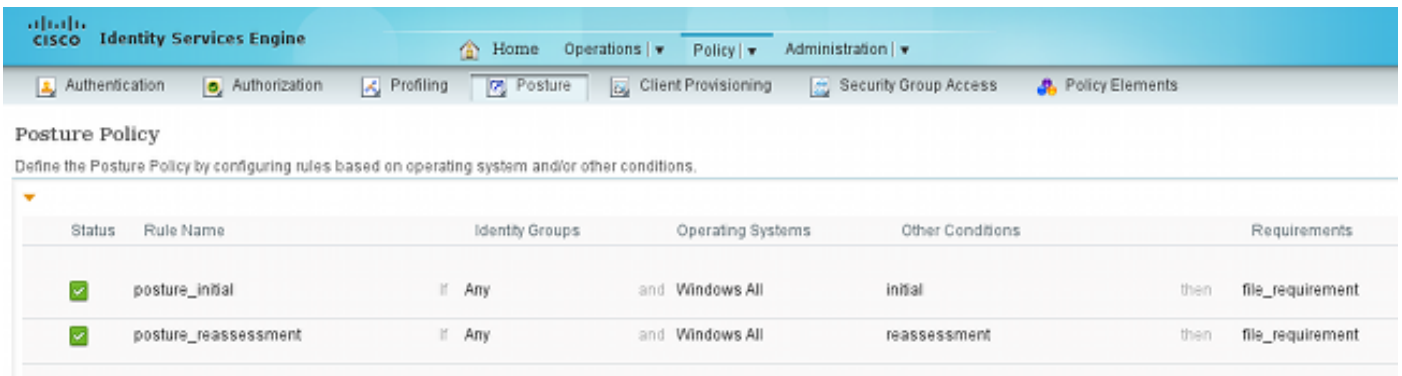
- Name: reassessment
- Description: (empty)
- Attribute: Session:Agent-Request-Type
- Operator: Equals
- Value: Periodic Reassessment

There are 'Submit' and 'Cancel' buttons at the bottom of the form.

3. قم بإنشاء حالة ماثلة تطابق التقييمات الأولية فقط:



يمكن استخدام كلا الشرطين في قواعد الوضع. وتطابق القاعدة الأولى التقييمات الأولية فقط، وتطابق القاعدة الثانية جميع التقييمات اللاحقة:

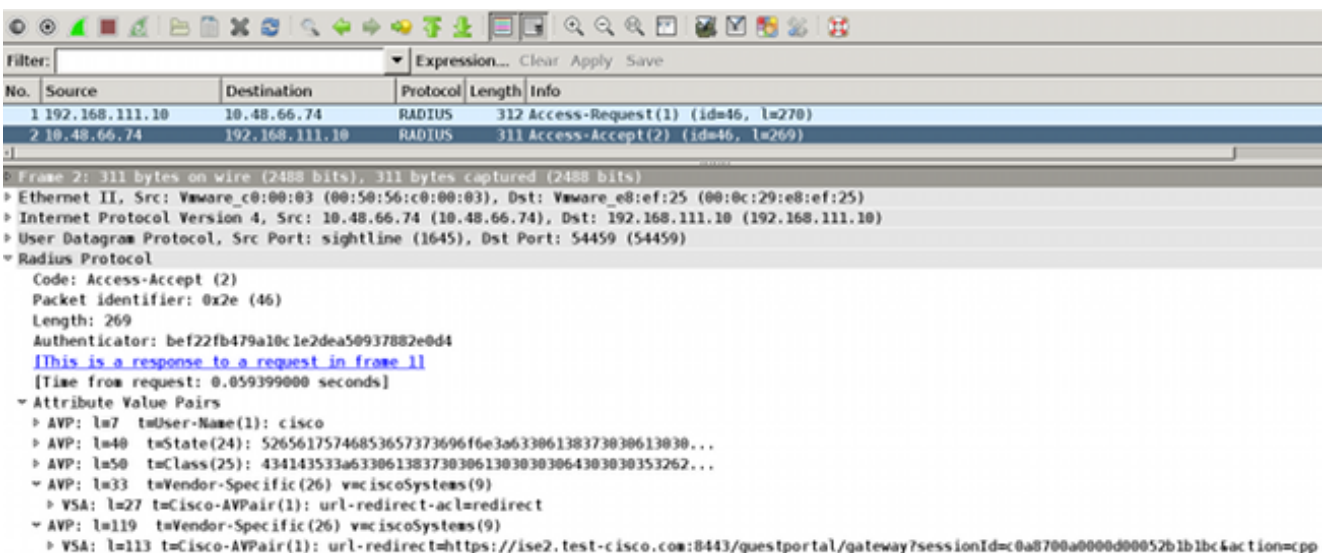


التحقق من الصحة

للتأكد من أن التكوين لديك يعمل بشكل صحيح، فتأكد من إكمال هذه الخطوات كما هو موضح:

1. يتصل مستخدم شبكة VPN بـ ASA.

2. يرسل الـ ASA RADIUS-طلب ويستلم إستجابة مع url-redirect-acl و url-redirect-سم:



.3

تشير سجلات ISE إلى أن التحويل يطابق ملف تعريف الوضع (إدخال السجل الأول):

✓	🔒	#ACSACL#-IP-F	ASA9-2	Compliant	ise2
✓	🔒	192.168.10.67	ASA9-2	ASA92-compliant	Compliant ise2
🔵	🔒	0 cisco 192.168.10.67		Compliant	ise2
✓	🔒	cisco 192.168.10.67	ASA9-2	ASA92-posture	User Identity Gro... Pending ise2

4. يضيف ASA إعادة توجيهه إلى جلسة شبكة VPN:

```
/aaa_url_redirect: Added url redirect:https://ise2.test-cisco.com:8443
guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp
acl:redirect for 10.10.10.10
```

5. تظهر حالة جلسة VPN على ASA أن الوضع مطلوب ويعيد توجيه حركة مرور HTTP:

```
ASA# show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username      : cisco                               Index      : 9
Assigned IP   : 10.10.10.10                          Public IP   : 10.147.24.61
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Essentials
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx      : 16077                                Bytes Rx    : 19497
Pkts Tx      : 43                                    Pkts Rx    : 225
Pkts Tx Drop : 0                                    Pkts Rx Drop : 0
Group Policy  : GP-SSL                               Tunnel Group : RA
Login Time    : 14:55:50 CET Mon Dec 23 2013
Duration     : 0h:01m:34s
Inactivity   : 0h:00m:00s
VLAN Mapping  : N/A                                  VLAN        : none
Audt Sess ID : c0a8700a0000900052b840e6
Security Grp : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

:AnyConnect-Parent
Tunnel ID      : 9.1
Public IP     : 10.147.24.61
Encryption    : none
Hashing       : none
TCP Src Port  : 50025
TCP Dst Port  : 443
Auth Mode     : userPassword
Idle Time Out: 30 Minutes
Idle TO Left  : 28 Minutes
Client OS     : win
Client Type   : AnyConnect
Client Ver    : Cisco AnyConnect VPN Agent for Windows 3.1.02040
Bytes Tx      : 5204                                Bytes Rx    : 779
Pkts Tx      : 4                                    Pkts Rx    : 1
Pkts Tx Drop : 0                                    Pkts Rx Drop : 0

:SSL-Tunnel
Tunnel ID     : 9.2
Assigned IP   : 10.10.10.10                          Public IP   : 10.147.24.61
Encryption    : RC4
Hashing       : SHA1
Encapsulation: TLSv1.0
TCP Src Port  : 50044
TCP Dst Port  : 443
Auth Mode     : userPassword
Idle Time Out: 30 Minutes
Idle TO Left  : 28 Minutes
```

```

Client OS      : Windows
Client Type   : SSL VPN Client
Client Ver    : Cisco AnyConnect VPN Agent for Windows 3.1.02040
Bytes Tx      : 5204
Pkts Tx      : 4
Pkts Tx Drop : 0
Bytes Rx      : 172
Pkts Rx      : 2
Pkts Rx Drop : 0

:DTLS-Tunnel
Tunnel ID    : 9.3
Assigned IP   : 10.10.10.10
Public IP    : 10.147.24.61
Encryption   : AES128
Hashing      : SHA1
Encapsulation: DTLSv1.0
UDP Src Port : 63296
UDP Dst Port : 443
Auth Mode    : userPassword
Idle Time Out: 30 Minutes
Idle TO Left : 29 Minutes
Client OS    : Windows
Client Type  : DTLS VPN Client
Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.02040
Bytes Tx     : 5669
Pkts Tx     : 35
Pkts Tx Drop: 0
Bytes Rx     : 18546
Pkts Rx     : 222
Pkts Rx Drop: 0

```

```

:ISE Posture
?Redirect URL : https://ise2.test-cisco.com:8443/guestportal/gateway
                sessionId=c0a8700a0000900052b840e6&action=cpp
Redirect ACL  : redirect

```

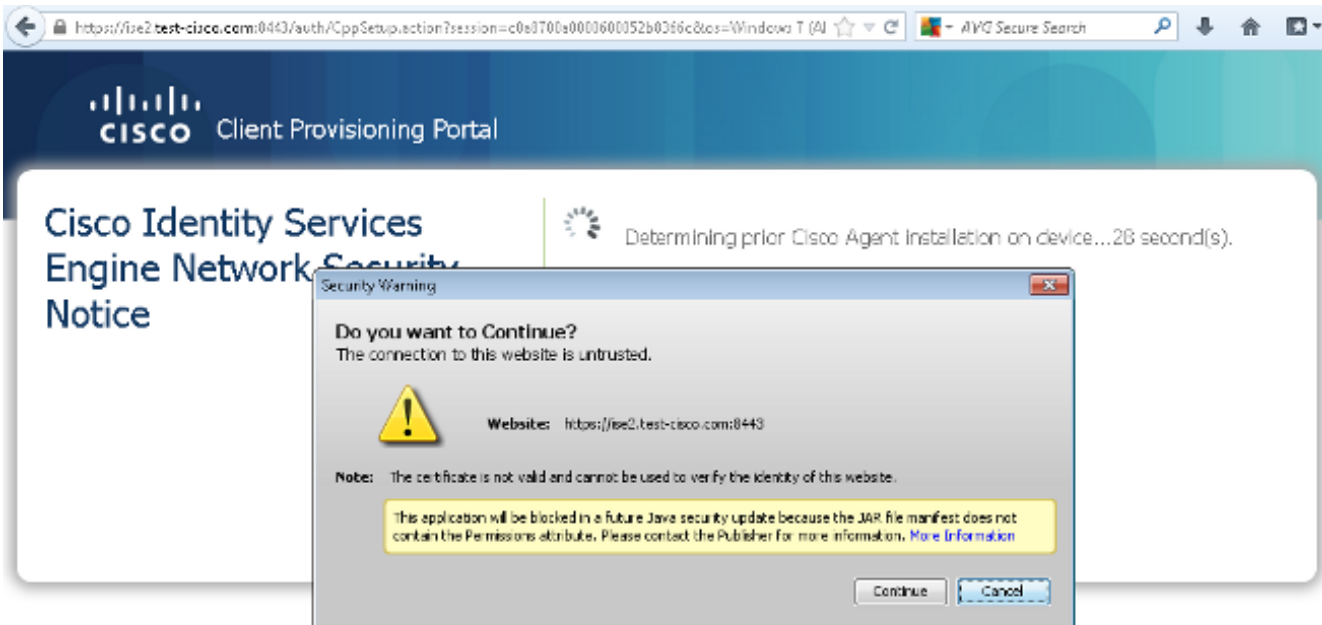
6. تتم إعادة توجيه العميل الذي يقوم ببدء حركة مرور HTTP التي تطابق قائمة التحكم في الوصول (ACL) لإعادة التوجيه إلى ISE:

```

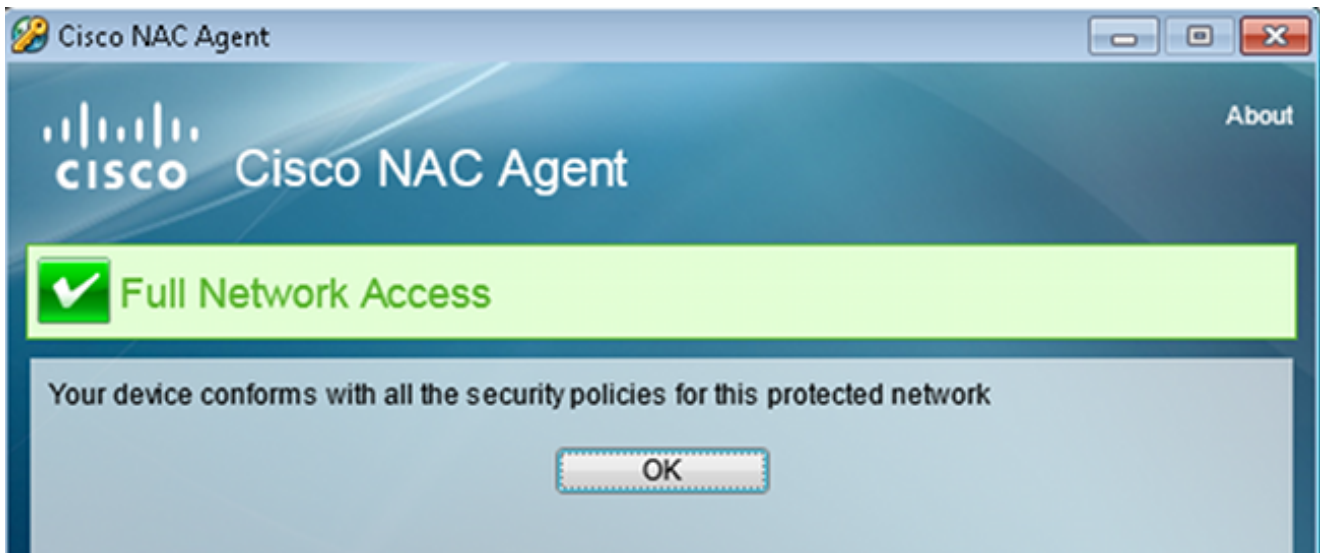
aaa_url_redirect: Created proxy for 10.10.10.10
/aaa_url_redirect: Sending url redirect:https://ise2.test-cisco.com:8443
guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp
for 10.10.10.10

```

7. تتم إعادة توجيه العميل إلى ISE لوضعه:



8. تم تثبيت عامل NAC. بعد تثبيت وكيل NAC، تقوم بتنزيل قواعد الوضع عبر البروتوكول السوبري وإجراء عمليات التحقق لتحديد التوافق. يتم بعد ذلك إرسال تقرير الحالة إلى ISE.



9. يتلقى ISE تقرير الحالة، ويعيد تقييم قواعد التحويل، و(إذا لزم الأمر) يغير حالة التحويل ويرسل CoA. يمكن التحقق من هذا الإجراء في `ise-psc.log`:

```
cisco.cpm.posture.runtime.PostureHandlerImpl --:cisco:c0a8700a0000900052b840e6
    Decrypting report --::
cisco.cpm.posture.runtime.PostureManager --:cisco:c0a8700a0000900052b840e6
User cisco belongs to groups NAC Group:NAC:IdentityGroups:User Identity --::
    Groups:Employee,NAC Group:NAC:IdentityGroups:An
cisco.cpm.posture.runtime.PostureManager --:cisco:c0a8700a0000900052b840e6
    Posture report token for endpoint mac 08-00-27-CD-E8-A2 is Healthy --::
cisco.cpm.posture.runtime.PostureManager --:cisco:c0a8700a0000900052b840e6
    Posture state is compliant for endpoint with mac 08-00-27-CD-E8-A2 --::
cisco.cpm.posture.runtime.PostureCoA --:cisco:c0a8700a0000900052b840e6
    Posture CoA is triggered for endpoint [null] with session --::
    [c0a8700a0000900052b840e6]
```

10. يرسل ISE RADIUS CoA الذي يتضمن `session_id` واسم DACL الذي يسمح بالوصول الكامل:

No.	Source	Destination	Protocol	Length	Info
7	10.48.66.74	192.168.111.10	RADIUS	231	CoA-Request(43) (id=11, l=189)
8	192.168.111.10	10.48.66.74	RADIUS	62	CoA-ACK(44) (id=11, l=20)

```

Frame 7: 231 bytes on wire (1848 bits), 231 bytes captured (1848 bits)
Ethernet II, Src: Vmware_c0:00:03 (00:50:56:c0:00:03), Dst: Vmware_e8:ef:25 (00:0c:29:e8:ef:25)
Internet Protocol Version 4, Src: 10.48.66.74 (10.48.66.74), Dst: 192.168.111.10 (192.168.111.10)
User Datagram Protocol, Src Port: 44354 (44354), Dst Port: mps-raft (1700)
Radius Protocol
  Code: CoA-Request (43)
  Packet identifier: 0xb (11)
  Length: 189
  Authenticator: d20817c6ca828ce7db4ee54f15177b8d
  [The response to this request is in frame 8]
Attribute Value Pairs
  AVP: l=6 t=NAS-IP-Address(4): 10.147.24.61
  AVP: l=15 t=Calling-Station-Id(31): 192.168.10.67
  AVP: l=6 t=Event-Timestamp(55): Dec 18, 2013 15:32:10.000000000 CET
  AVP: l=18 t=Message-Authenticator(80): lee29f1d83e5f3aa4934d60aa617ebeb
  AVP: l=75 t=Vendor-Specific(26) v=ciscoSystems(9)
    VSA: l=69 t=Cisco-AVPair(1): ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1
  AVP: l=49 t=Vendor-Specific(26) v=ciscoSystems(9)
    VSA: l=43 t=Cisco-AVPair(1): audit-session-id=c0a8700a0000d00052b1b1bc

```

وينعكس ذلك في سجلات ISE:

يكون إدخال السجل الأول للمصادقة الأولية التي ترجع توصيف الوضع (مع إعادة التوجيه).

يتم ملء إدخال السجل الثاني بعد تلقي التقرير السويصري المتوافق.

يتم ملء إدخال السجل الثالث عند إرسال CoA، بالإضافة إلى التأكيد (الذي تم وصفه بأنه "تفويض ديناميكي" بنجاح).

يتم إنشاء إدخال السجل النهائي عندما يقوم ASA بتنزيل DACL.

ASA9-2	Compliant	ise2
#ACSACL#-IP-F	Compliant	ise2
192.168.10.67	Compliant	ise2
0 cisco 192.168.10.67	Compliant	ise2
cisco 192.168.10.67	Pending	ise2

11. يظهر تصحيح الأخطاء على ASA أنه تم إستلام CoA وأنه تمت إزالة إعادة التوجيه. يقوم ASA بتنزيل قوائم التحكم في الوصول (DACL) إذا لزم الأمر:

```
ASA# Received RAD_COA_REQUEST
```

```
(RADIUS packet decode (CoA-Request
```

```
        = (Radius: Value (String
-3a 43 69 73 63 6f 53 65 63 75 72 65 2d | ACS:CiscoSecure 53 43 41
6e 65 64 2d 41 43 4c 3d 23 41 43 53 | Defined-ACL=#ACS 69 66 65 44
4c 23 2d 49 50 2d 50 45 52 4d 49 54 5f 41 | ACL#-IP-PERMIT_A 43 41
4c 4c 5f 54 52 41 46 46 49 43 2d 35 31 65 66 37 | LL_TRAFFIC-51ef7
db1 | 31 62 64
```

```
Got AV-Pair with value audit-session-id=c0a8700a0000900052b840e6
=Got AV-Pair with value ACS:CiscoSecure-Defined-ACL
ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1#
```

```
aaa_url_redirect: Deleted url redirect for 10.10.10.10
```

.12 بعد ال VPN جلسة، cisco يتلقى ال DACL يطبق (وصول كامل) للمستخدم:

```
ASA# show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username : cisco Index : 9
Assigned IP : 10.10.10.10 Public IP : 10.147.24.61
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Essentials
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 94042 Bytes Rx : 37079
Pkts Tx : 169 Pkts Rx : 382
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GP-SSL Tunnel Group : RA
Login Time : 14:55:50 CET Mon Dec 23 2013
Duration : 0h:05m:30s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : c0a8700a0000900052b840e6
Security Grp : 0
```

```
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```



```

: AnyConnect-Parent
Tunnel ID      : 9.1
Public IP      : 10.147.24.61
Encryption     : none
TCP Src Port   : 50025
Hashing        : none
TCP Dst Port   : 443
Auth Mode      : userPassword
Idle Time Out  : 30 Minutes
Idle TO Left   : 24 Minutes
Client OS      : win
Client Type    : AnyConnect
Client Ver     : Cisco AnyConnect VPN Agent for Windows 3.1.02040
Bytes Tx       : 5204
Pkts Tx        : 4
Pkts Tx Drop   : 0
Bytes Rx       : 779
Pkts Rx        : 1
Pkts Rx Drop   : 0

: SSL-Tunnel
Tunnel ID      : 9.2
Assigned IP    : 10.10.10.10
Public IP      : 10.147.24.61
Encryption     : RC4
Encapsulation  : TLSv1.0
TCP Dst Port   : 443
Hashing        : SHA1
TCP Src Port   : 50044
Auth Mode      : userPassword
Idle Time Out  : 30 Minutes
Idle TO Left   : 24 Minutes
Client OS      : Windows
Client Type    : SSL VPN Client
Client Ver     : Cisco AnyConnect VPN Agent for Windows 3.1.02040
Bytes Tx       : 5204
Pkts Tx        : 4
Pkts Tx Drop   : 0
Filter Name    : #ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1
Bytes Rx       : 172
Pkts Rx        : 2
Pkts Rx Drop   : 0

: DTLS-Tunnel
Tunnel ID      : 9.3
Assigned IP    : 10.10.10.10
Public IP      : 10.147.24.61
Encryption     : AES128
Encapsulation  : DTLSv1.0
UDP Dst Port   : 443
Hashing        : SHA1
UDP Src Port   : 63296
Auth Mode      : userPassword
Idle Time Out  : 30 Minutes
Idle TO Left   : 29 Minutes
Client OS      : Windows
Client Type    : DTLS VPN Client
Client Ver     : Cisco AnyConnect VPN Agent for Windows 3.1.02040
Bytes Tx       : 83634
Pkts Tx        : 161
Pkts Tx Drop   : 0
Filter Name    : #ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1
Bytes Rx       : 36128
Pkts Rx        : 379
Pkts Rx Drop   : 0

```

ملاحظة: يزيل ASA دائما قواعد إعادة التوجيه، حتى عندما لا يكون لدى CoA أي DACL مرفقة.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

تصحيح الأخطاء على ISE

انتقل إلى إدارة < تسجيل < تكوين سجل تصحيح الأخطاء لتمكين تصحيح الأخطاء. توصي Cisco بتمكين تصحيح الأخطاء المؤقت ل:

- سويسري
- إعادة التوجيه دون إيقاف (NSF)

• NSF-جلسة

• حكم

• وضعية

دخلت هذا أمر في ال CLI in order to شاهدت ال debugs:

```
ise2/admin# show logging application ise-psc.log tail count 100
```

انتقل إلى العمليات < التقارير < تقارير ISE < نقاط النهاية والمستخدمين < تقييم تفاصيل الوضع لعرض تقارير الوضع:

Logged At	Status	Detail	PRA	Identity	Endpoint ID	IP Address	Endpoint OS	Agent	Message
2013-12-23 15:21:34.9	continue			cisco	08:08:27:CD:08:A	10.147.24.32	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 15:08:56.3	continue			cisco	08:08:27:CD:08:A	10.147.24.32	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 14:59:34.3	continue			cisco	08:08:27:CD:08:A	10.147.24.32	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 14:55:28.6	N/A			cisco	08:08:27:CD:08:A	10.147.24.32	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 14:44:45.0	N/A			cisco	08:08:27:CD:08:A	10.147.24.32	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 13:34:30.3	N/A			cisco	08:08:27:7F:5F:8*	10.147.24.32	Windows 7 Ultimate 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 13:27:10.3	N/A			cisco	08:08:27:7F:5F:8*	10.147.24.32	Windows 7 Ultimate 64-bit	Cisco NAC A...	Received a posture report from an endpoint

في صفحة "Posture More Detail Assessment"، يوجد اسم نهج باسم متطلب يتم عرضه، بالإضافة إلى النتائج:

Posture More Detail Assessment

Time Range: From 12/23/2013 12:00:00 AM to 12/23/2013 03:57:31 PM
Generated At: 2013-12-23 15:57:31.248

Client Details

Username:	cisco
Mac Address:	08:00:27:CD:E8:A2
IP address:	10.147.24.92
Session ID:	c0a8700a0000b00052b846c0
Client Operating System:	Windows 7 Enterprise 64-bit
Client NAC Agent:	Cisco NAC Agent for Windows 4.9.0.1013
PRA Enforcement:	1
CoA:	Received a posture report from an endpoint
PRA Grace Time:	
PRA Interval:	240
PRA Action:	continue
User Agreement Status:	NotEnabled
System Name:	MGARCARZ-WS01
System Domain:	cisco.com
System User:	mgarcarz
User Domain:	CI SCO
AV Installed:	McAfee VirusScan Enterprise;8.8.0.975;7227;10/13/2013;McAfeeAV,Cisco Security Agent;6.0.2.130;;;CiscoAV
AS Installed:	Windows Defender;6.1.7600.16385;1.95.191.0;11/19/2010;MicrosoftAS

Posture Report

Posture Status:	Compliant
Logged At:	2013-12-23 15:21:34.902

Posture Policy Details

Policy	Name	Enforcement	Statu	Passed	Failed	Skipped Conditions
posture_initial	file_require...	Mandatory		file_condition		

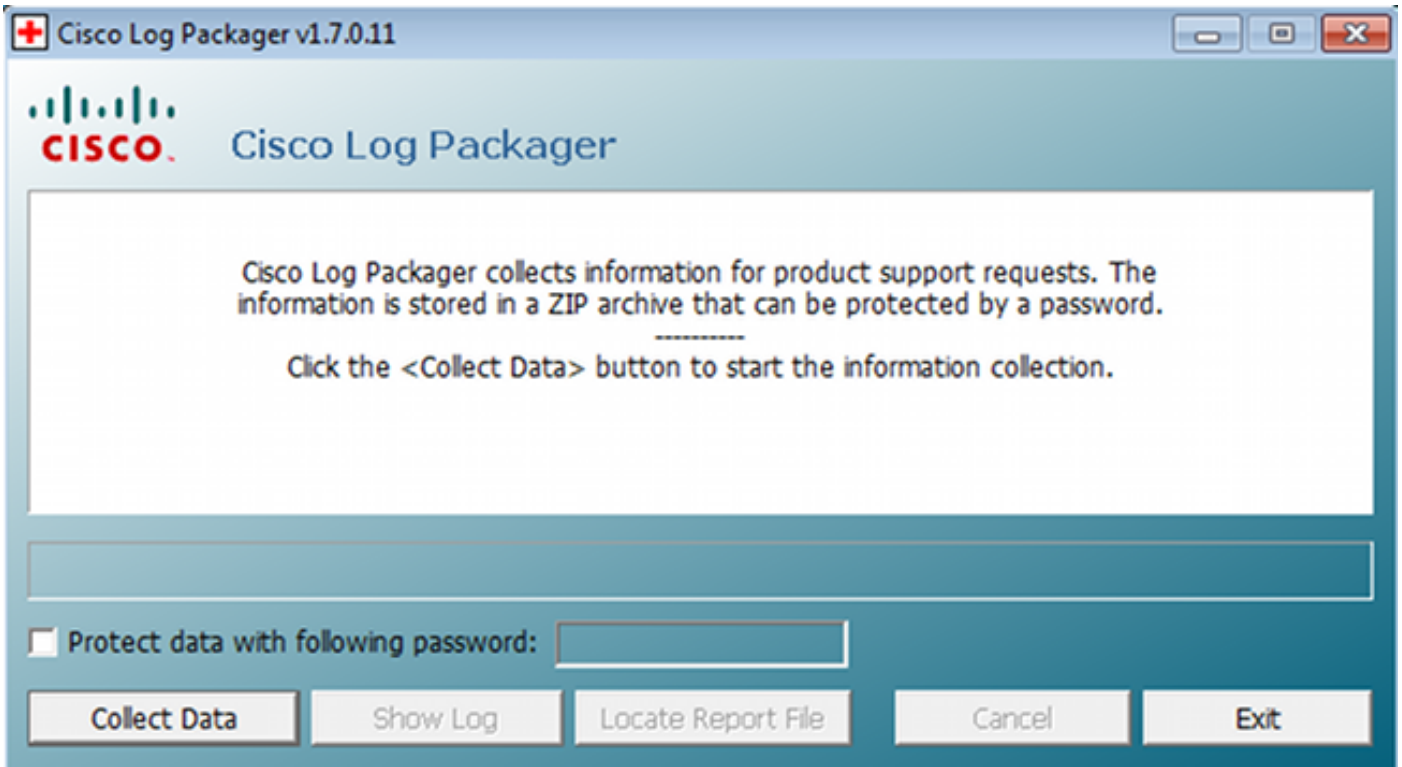
تصحيح الأخطاء على ASA

أنت يستطيع مكنت هذا يضبط على ال ASA:

- debug aaa url-redirect •
- debug aaa تحويل •
- debug radius تحويل ديناميكي ل •
- debug شفرة نصف القطر •
- debug radius user cisco •

تصحيح أخطاء الوكيل

بالنسبة لوكيل NAC، من الممكن تجميع تصحيح الأخطاء باستخدام Cisco Log Packager، والذي يتم استهلاكه من واجهة المستخدم الرسومية (GUI) أو باستخدام واجهة سطر الأوامر (CLI): CCAgentLogPackager.app.



تلميح: يمكنك فك ترميز النتائج باستخدام أداة مركز المساعدة التقنية (TAC).

لاسترداد السجلات لعامل الويب، انتقل إلى المواقع التالية:

• C: < الوثيقة والإعدادات <user> < الإعدادات المحلية < Webagent.log > Temp > (مفكوزة باستخدام أداة (TAC

• ج: < الوثيقة والإعدادات <user> < الإعدادات المحلية < WebSlotSetup.log > Temp >

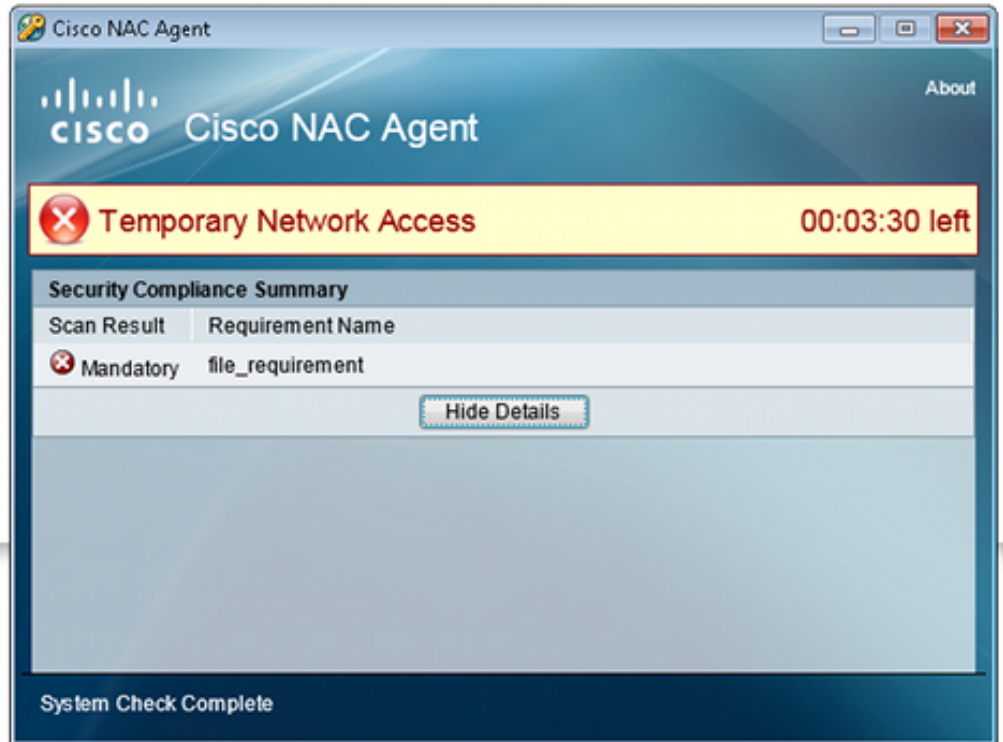
ملاحظة: إذا لم تكن السجلات موجودة في هذه المواقع، فتحقق من متغير بيئة TEMP.

فشل وضع وكيل NAC

في حالة فشل الوضع، يتم عرض السبب على المستخدم:



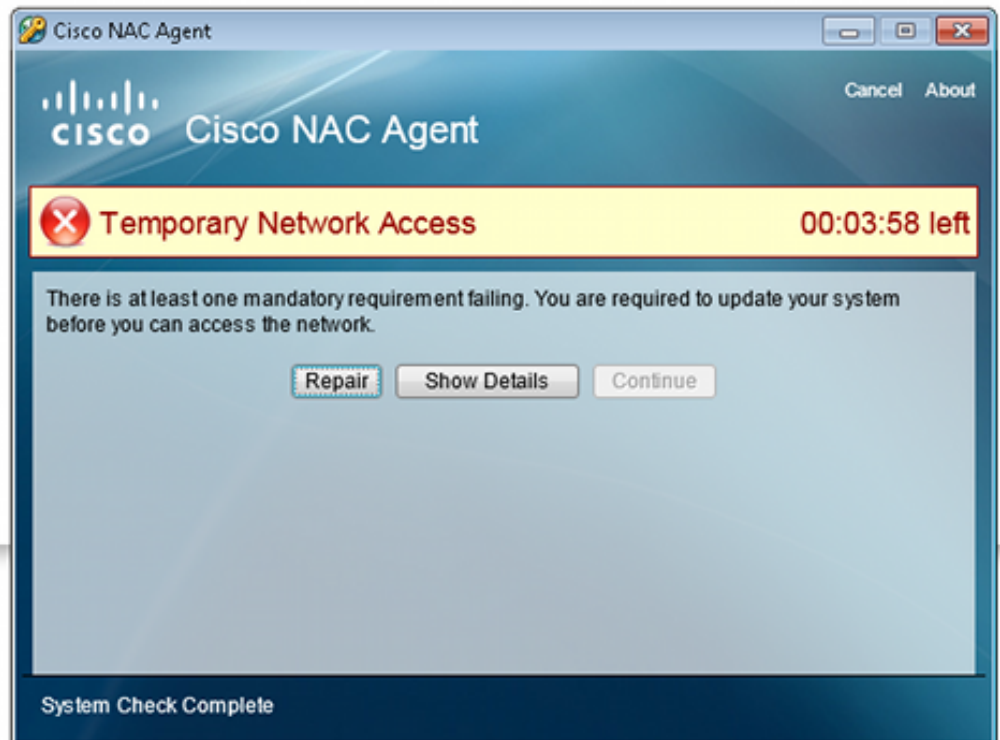
Information



يسمح للمستخدم بعد ذلك بإجراءات الإصلاح إذا تم تكوينها:



Information



معلومات ذات صلة

- [تكوين خادم خارجي لتفويض مستخدم جهاز الأمان](#)
- [دليل تكوين واجهة سطر الأوامر Cisco ASA Series VPN، الإصدار 9.1](#)
- [دليل مستخدم محرك خدمات الهوية من Cisco، إصدار 1.2](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا