VPN Inline Posture (وضعية الشبكة الخاصة الظاهرية (VPN) باستخدام iPEP ISE و ASA)

المحتويات

المقدمة

يقدم هذا المستند معلومات حول كيفية إعداد الوضع المضمن باستخدام جهاز الأمان القابل للتكيف (ASA) ومحرك خدمات الهوية (ISE).

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الإصدار 8.2(4) ل ASA والإصدار 1.1.0.665 ل ISE.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

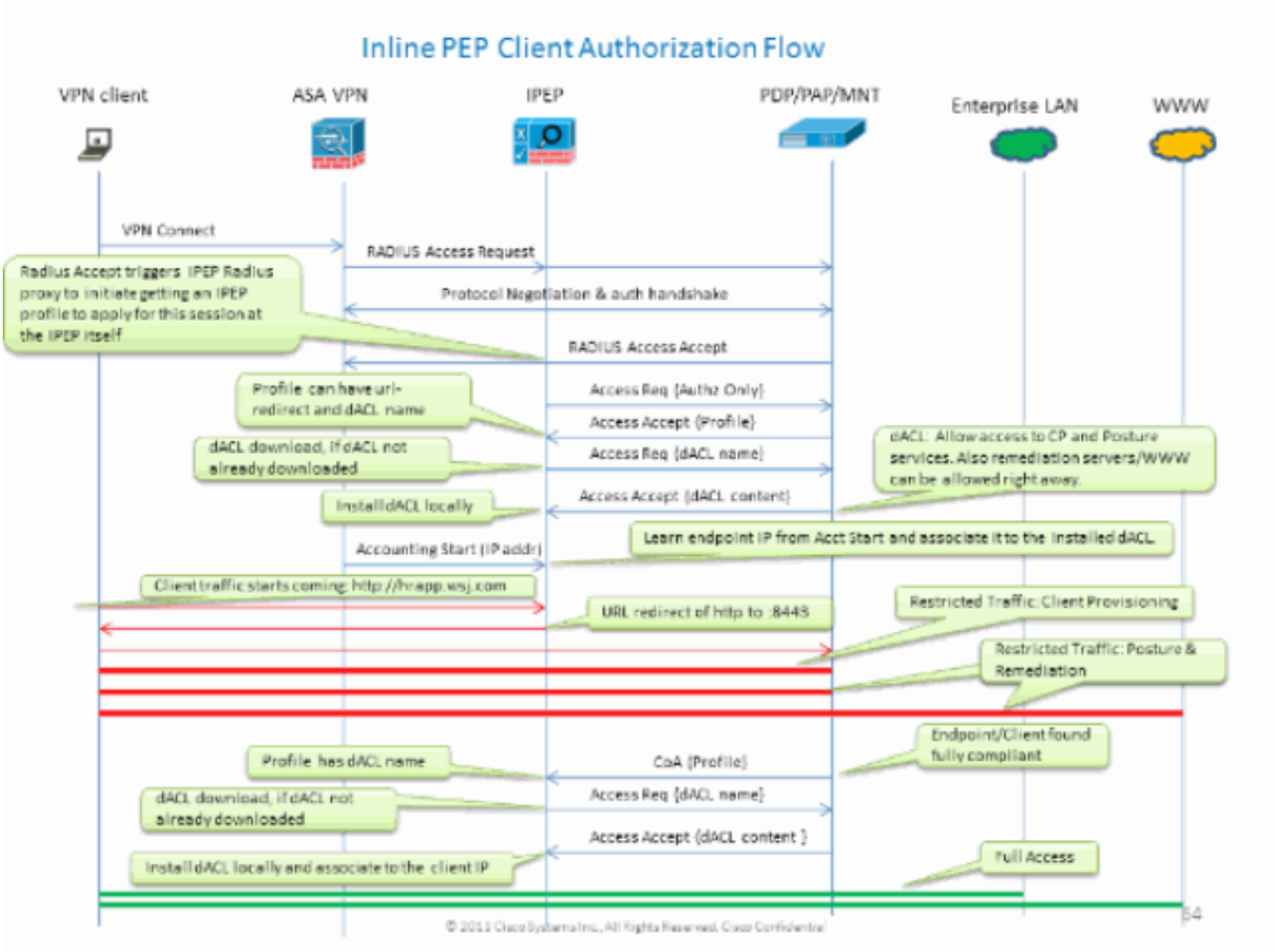
يوفر ISE الكثير من خدمات AAA (Posture (وضعية، وتنميط، ومصادقة، وما إلى ذلك). تدعم بعض أجهزة الشبكة (NAD) تغيير مصادقة (RADIUS (CoA الذي يسمح بتغيير ملف تعريف تخويل الجهاز الطرفي بشكل ديناميكي استنادا إلى وضعية الجهاز أو نتيجة إنشاء ملفات التعريف الخاصة به. لا تدعم NADs الأخرى مثل ASA هذه الميزة بعد. وهذا يعني أن تشغيل ISE في وضع فرض الوضع المضمن (iPEP) مطلوب لتغيير سياسة الوصول إلى الشبكة الخاصة بالجهاز الطرفي بشكل ديناميكي.

المفهوم الأساسي هو أن كل حركة مرور المستخدم سوف تمر من خلال iPEP، مع عمل العقدة أيضا كوكيل RADIUS.

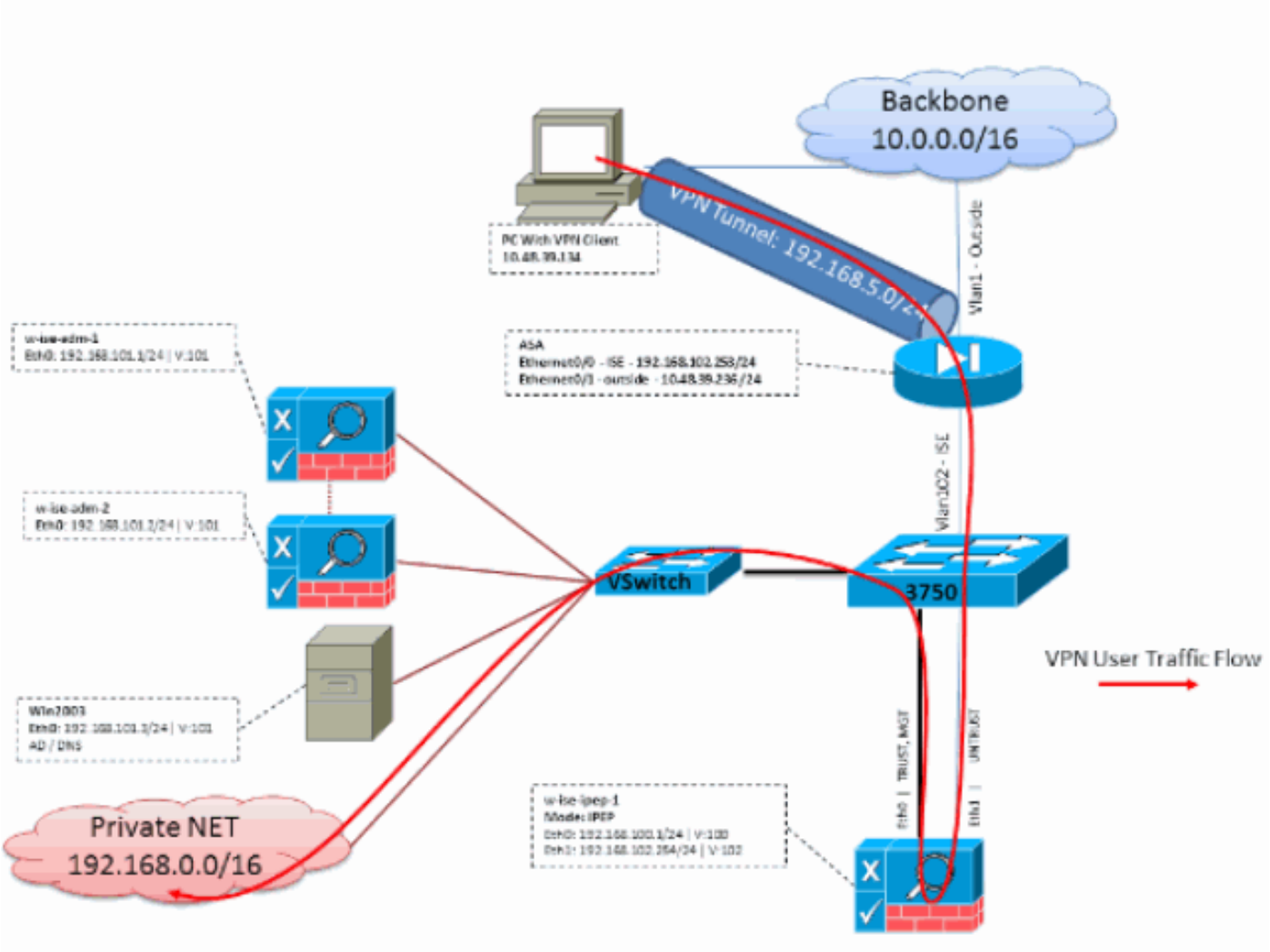
تدفق أساسي

1. سجل مستخدم شبكة VPN الدخول.
2. يرسل ASA الطلب إلى عقدة ISE) iPEP).
3. يعيد بروتوكول iPEP كتابة الطلب (من خلال إضافة سمات زوج AV من Cisco للإشارة إلى أنها مصادقة iPEP) ويرسل الطلب إلى عقدة سياسة ISE) PDP).
4. يرد حزب الشعب الديمقراطي على بروتوكول iPEP الذي سيرسل إلى NAD.
5. إذا تم مصادقة المستخدم، فيجب على NAD إرسال طلب بدء عملية محاسبة (راجع CSCtz84826). سيؤدي هذا إلى تشغيل بدء جلسة العمل على iPEP. في هذه المرحلة، تتم إعادة توجيه المستخدم للوضع. وبالإضافة إلى ذلك، يلزمك تمكين accounting-update- المؤقت للنفق المنشأ من مدخل WebVPN، حيث يتوقع ISE أن يكون للسمة framed-ip-address في محاسبة RADIUS. ومع ذلك، عند الاتصال بالمدخل، لا يعرف بعد عنوان IP لشبكة VPN للعميل لأن النفق لم يتم إنشاؤه. وسيضمن ذلك أن يرسل مكتب المساعدة الفنية تحديثات مؤقتة، مثل الوقت الذي سيتم فيه إنشاء النفق.
6. يمر المستخدم عبر تقييم الوضع، واستنادا إلى النتائج سيقوم بروتوكول PDP بتحديث الجلسة باستخدام CoA على بروتوكول iPEP.

توضح لقطة الشاشة هذه العملية:



[مثال طبولوجيا](#)



تكوين ASA

تكوين ASA هو شبكة VPN بعيدة بسيطة ل IPsec:

```
!
interface Ethernet0/0
nameif ISE
security-level 50
ip address 192.168.102.253 255.255.255.0
!
interface Ethernet0/1
nameif outside
security-level 0
ip address 10.48.39.236 255.255.255.0
!
access-list split extended permit ip 192.168.0.0 255.255.0.0 any
!
aaa-server ISE protocol radius
interim-accounting-update
Mandatory if tunnel established from WEBVPN Portal aaa-server ISE (ISE) host ---!
192.168.102.254 !--- this is the iPEP IP key cisco crypto ipsec transform-set TS1 esp-aes esp-
sha-hmac crypto ipsec security-association lifetime seconds 28800 crypto ipsec security-
association lifetime kilobytes 4608000 crypto dynamic-map DMAP1 10 set transform-set TS1 crypto
dynamic-map DMAP1 10 set reverse-route crypto map CM1 10 ipsec-isakmp dynamic DMAP1 crypto map
CM1 interface outside crypto isakmp enable outside crypto isakmp policy 1 authentication pre-
share encryption aes hash sha group 2 lifetime 86400 ! ip local pool VPN 192.168.5.1-
```

```
192.168.5.100 ! group-policy DfltGrpPolicy attributes dns-server value 192.168.101.3 !--- The
VPN User needs to be able to resolve the CN from the !--- ISE HTTPS Certificate (which is sent
in the radius response) vpn-tunnel-protocol IPSec svc webvpn split-tunnel-policy tunnelspecified
split-tunnel-network-list value split address-pools value VPN ! tunnel-group cisco general-
attributes address-pool VPN authentication-server-group ISE accounting-server-group ISE !---
Does not work without this (see introduction) ! tunnel-group cisco ipsec-attributes pre-shared-
key cisco ! route outside 0.0.0.0 0.0.0.0 10.48.39.5 1 route ISE 192.168.0.0 255.255.0.0
192.168.102.254 1 !--- You need to make sure the traffic to the local subnets !--- are going
! through the inline ISE
```

تكوين ISE

تكوين iPEP

أول شيء يجب القيام به هو إضافة ISE كعقدة iPEP. يمكنك العثور على معلومات إضافية حول العملية هنا:

http://www.cisco.com/en/US/docs/security/ise/1.1/user_guide/ise_ipep_deploy.html#wp1110248.

هذا هو ما يجب عليك في الأساس تكوينه في علامات التبويب المختلفة (لقطات الشاشة الواردة في هذا القسم توضح هذا):

- قم بتكوين إعدادات IP العامة وغير الموثوق بها (في هذه الحالة، IP غير الموثوق به هو 192.168.102.254).
- النشر هو وضع موجه.
- ضع عامل تصفية ثابت ل ASA ليتم السماح له بالمرور من خلال مربع iPEP (وإلا، يتم إسقاط الاتصال ب/من مربع ISE Thru iPEP).
- قم بتكوين ISE النهج كخادم RADIUS و ASA كعميل RADIUS.
- إضافة مسار إلى الشبكة الفرعية لشبكة VPN التي تشير إلى ASA.
- ثبت ال monitore ISE كال logging host (ميناء 20514 افتراضيا؛ في هذه الحالة، السياسة ISE يراقب أيضا).

متطلبات تكوين الشهادة الهامة:

قبل محاولة تسجيل عقدة iPEP، تأكد من استيفاء متطلبات إستخدام المفتاح الموسع للشهادة التالية. إذا لم يتم تكوين الشهادات بشكل صحيح على عقدتي iPEP و Admin، فسيتم إكمال عملية التسجيل. ومع ذلك، ستفقد وصول المسؤول إلى عقدة iPEP. تم استقراء التفاصيل التالية من دليل نشر iPEP ISE 1.1.x:

قد يؤدي وجود مجموعات معينة من السمات في الشهادات المحلية لعقدة "الإدارة" و"الحالة المضمنة" إلى منع المصادقة المتبادلة من العمل.

السمات هي:

- إستخدام مفتاح موسع (EKU)—مصادقة الخادم
- إستخدام مفتاح موسع (EKU)—مصادقة العميل
- مصادقة خادم Netscape CERT Type-SSL
- نوع شهادة Netscape—مصادقة عميل SSL

يلزم توفر أي من المجموعات التالية لشهادة الإدارة:

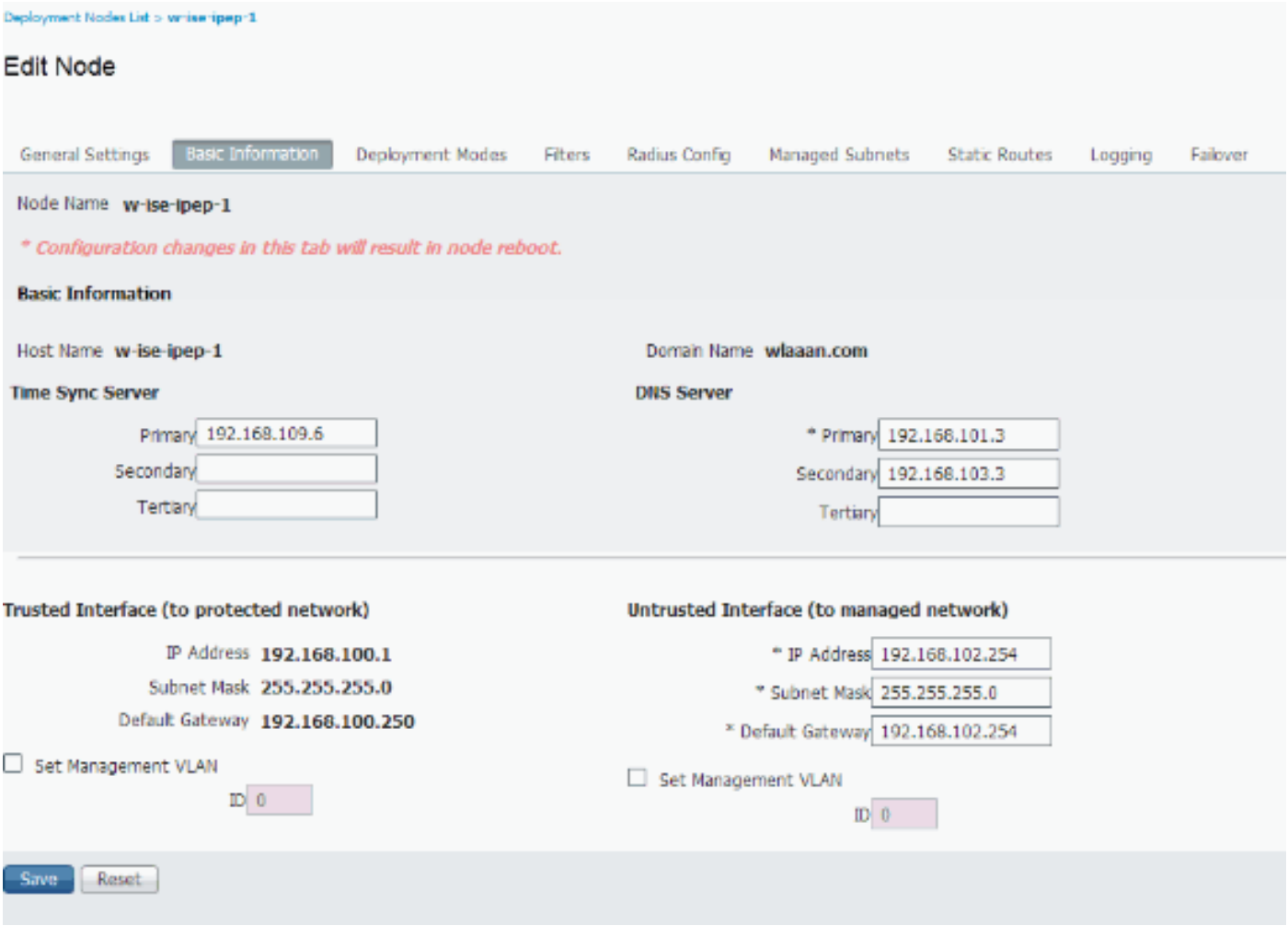
- يجب تعطيل كل من سمتي EKU، إذا تم تعطيل كل من سمتي EKU في شهادة "الحالة المضمنة"، أو يجب تمكين كل من سمتي EKU، إذا تم تمكين سمة الخادم في شهادة "الحالة المضمنة".
- يجب تعطيل كل من سمات "نوع شهادة Netscape"، أو يجب تمكين كليهما.

أي من المجموعات التالية مطلوب لشهادة الوضع المضمن:

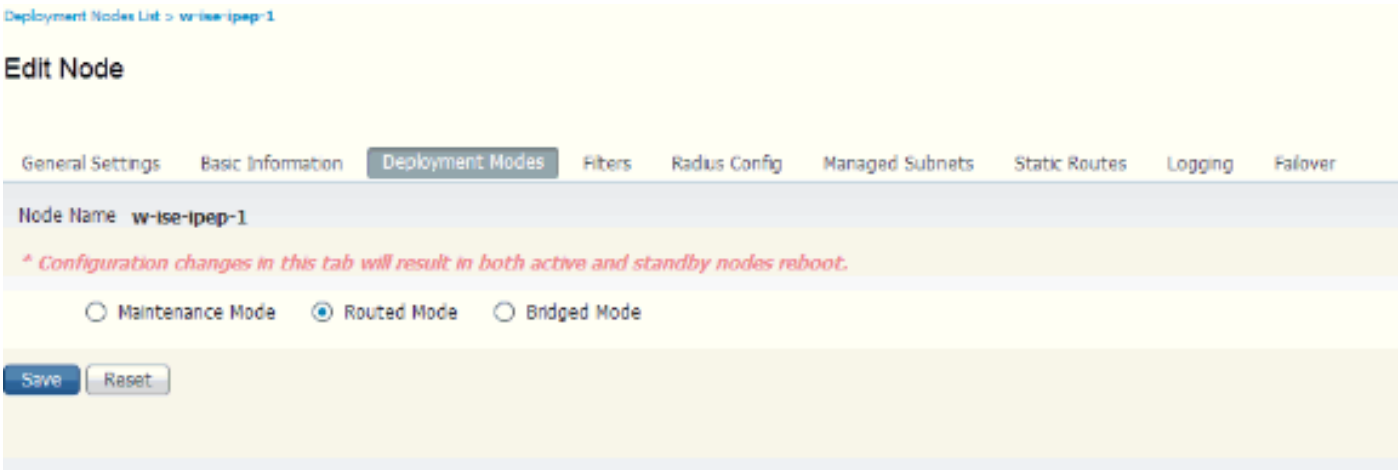
- يجب تعطيل كل من سمتي EKU، أو يجب تمكين كليهما، أو يجب تمكين سمة الخادم وحدها.
- يجب تعطيل كل من سمات "نوع شهادة Netscape"، أو يجب تمكين كليهما، أو يجب تمكين سمة الخادم وحدها.

- حيث يتم إستخدام الشهادات المحلية الموقعة ذاتيا على عقد "الإدارة" و"الحالة المضمنة"، يجب تثبيت شهادة موقعة ذاتيا لعقدة "الإدارة" في قائمة الضمان لعقدة "الحالة المضمنة". بالإضافة إلى ذلك، إذا كان لديك عقدتي إدارة أساسية وثانوية في عملية النشر الخاصة بك، فيجب عليك تثبيت شهادة موقعة ذاتيا من كلا عقدتي الإدارة في قائمة الضمان الخاصة بعقدة الحالة المضمنة.
- حيث يتم إستخدام الشهادات المحلية الموقعة من CA على عقد "الإدارة" و"الحالة المضمنة"، يجب أن تعمل المصادقة المتبادلة بشكل صحيح. في هذه الحالة، يتم تثبيت شهادة CA التوقيع على عقدة الإدارة قبل التسجيل، ويتم نسخ هذه الشهادة نسخا متماثلا إلى عقدة الوضع المضمنة.
- إذا كانت المفاتيح الصادرة من CA مستخدمة لتأمين الاتصال بين عقد "الإدارة" و"الحالة المضمنة"، قبل تسجيل عقدة "الحالة المضمنة"، يجب إضافة المفتاح العام (شهادة CA) من عقدة "الإدارة" إلى قائمة شهادات CA لعقدة "الحالة المضمنة".

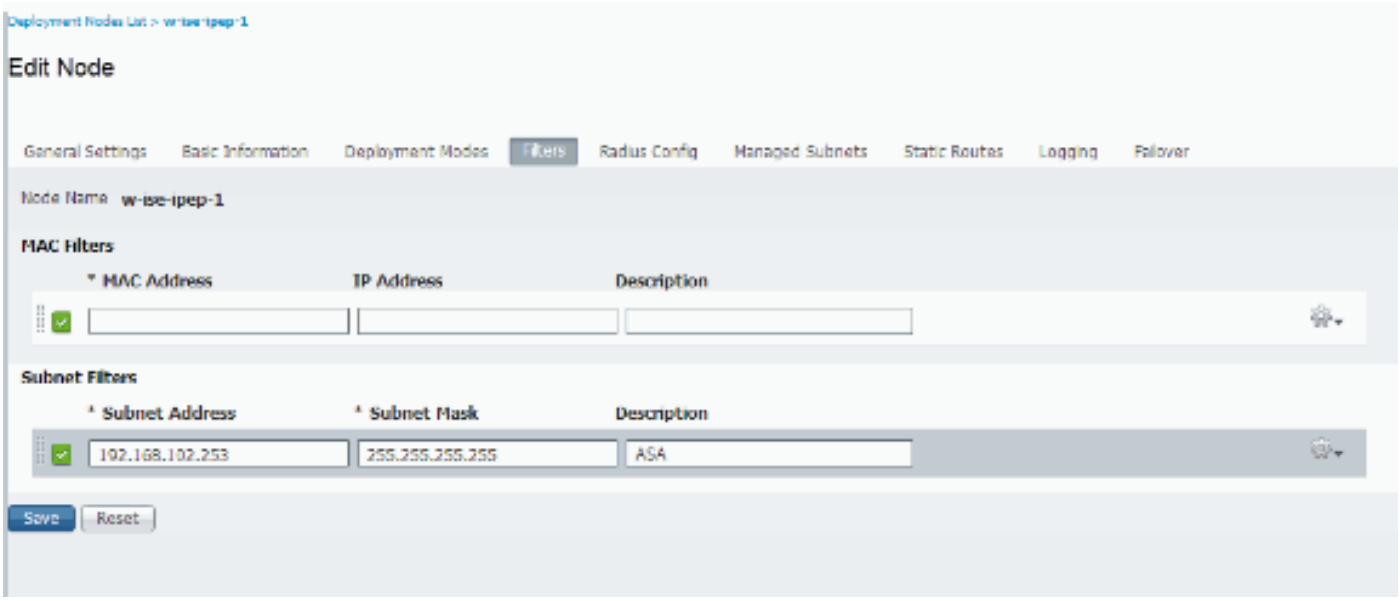
التكوين الأساسي:



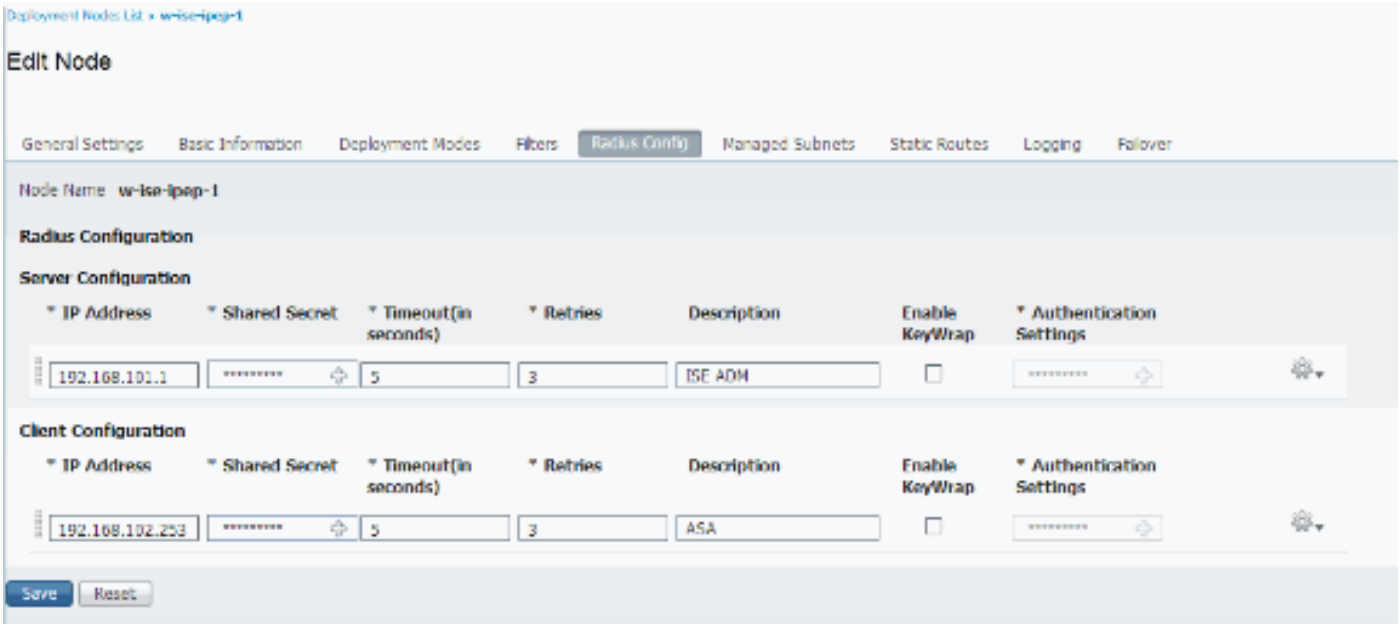
تكوين وضع النشر:



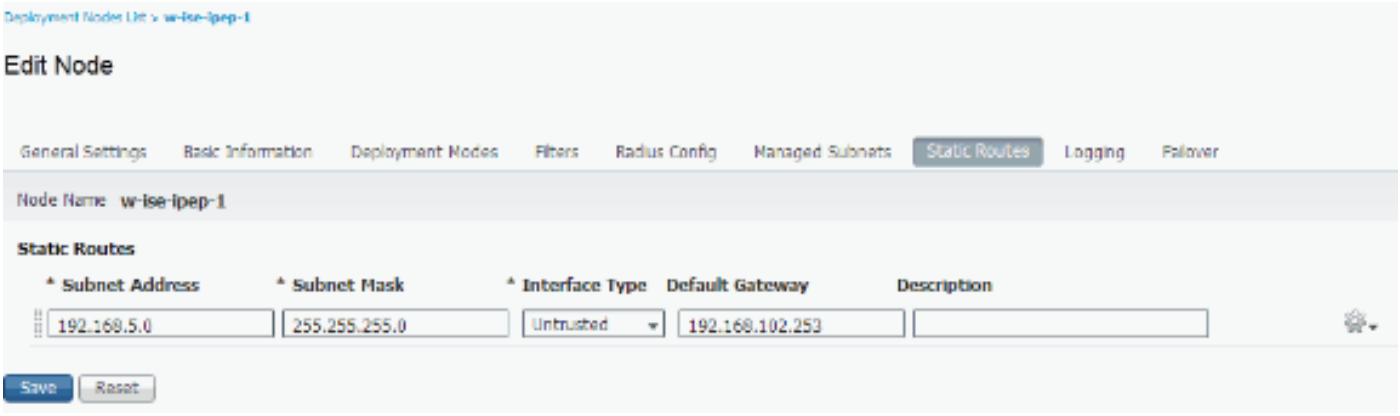
تكوين عوامل التصفية:



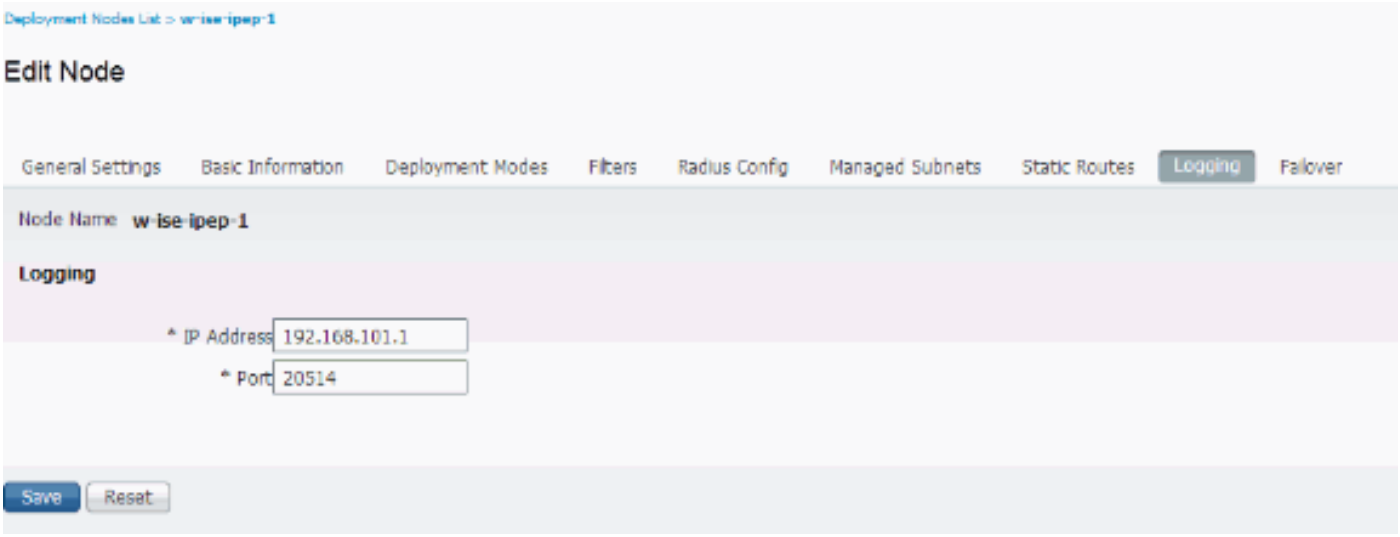
تهيئة RADIUS:



المسارات الثابتة:



التسجيل:



المصادقة وتكوين الوضع

هناك ثلاث حالات للوضع:

- غير معروف: لم يتم إجراء Posture بعد
- متوافق: تم إنشاء الوضع والنظام متوافق
- غير متوافق: تم إجراء Posture (وضعية)، ولكن فشل النظام في تحقق واحد على الأقل

يجب الآن إنشاء ملفات تعريف التخويل (والتي ستكون ملفات تعريف تخويل مضمنة: سيؤدي ذلك إلى إضافة السمة ipep-authz=true في زوج AV من Cisco) التي سيتم إستخدامها في حالة الاختلاف.

وبشكل عام، يرجع ملف التعريف غير المعروف عنوان URL المعاد توجيهه (اكتشاف الوضع) الذي سيقوم بإعادة توجيه حركة مرور المستخدم إلى ISE وسيطلب تثبيت وكيل NAC. إذا كان وكيل NAC مثبتا بالفعل، فهذا سيسمح بإعادة توجيه طلب اكتشاف HTTP الخاص به إلى ISE.

في ملف التعريف هذا، يتم إستخدام قائمة تحكم في الوصول (ACL) تتيح حركة مرور بيانات HTTP إلى ISE و DNS على الأقل.

عادة ما ترجع ملفات التعريف المتوافقة وغير المتوافقة قائمة تحكم في الوصول (ACL) قابلة للتنزيل لمنح الوصول إلى الشبكة بناء على ملف تعريف المستخدم. يمكن لملف التعريف غير المتوافق أن يسمح للمستخدمين بالوصول إلى خادم ويب لتنزيل برنامج مكافحة الفيروسات على سبيل المثال أو منح وصول محدود للشبكة.

في هذا المثال، يتم إنشاء ملفات التعريف غير المعروفة والمتوافقة، ويتم التحقق من وجود notepad.exe كمتطلبات.

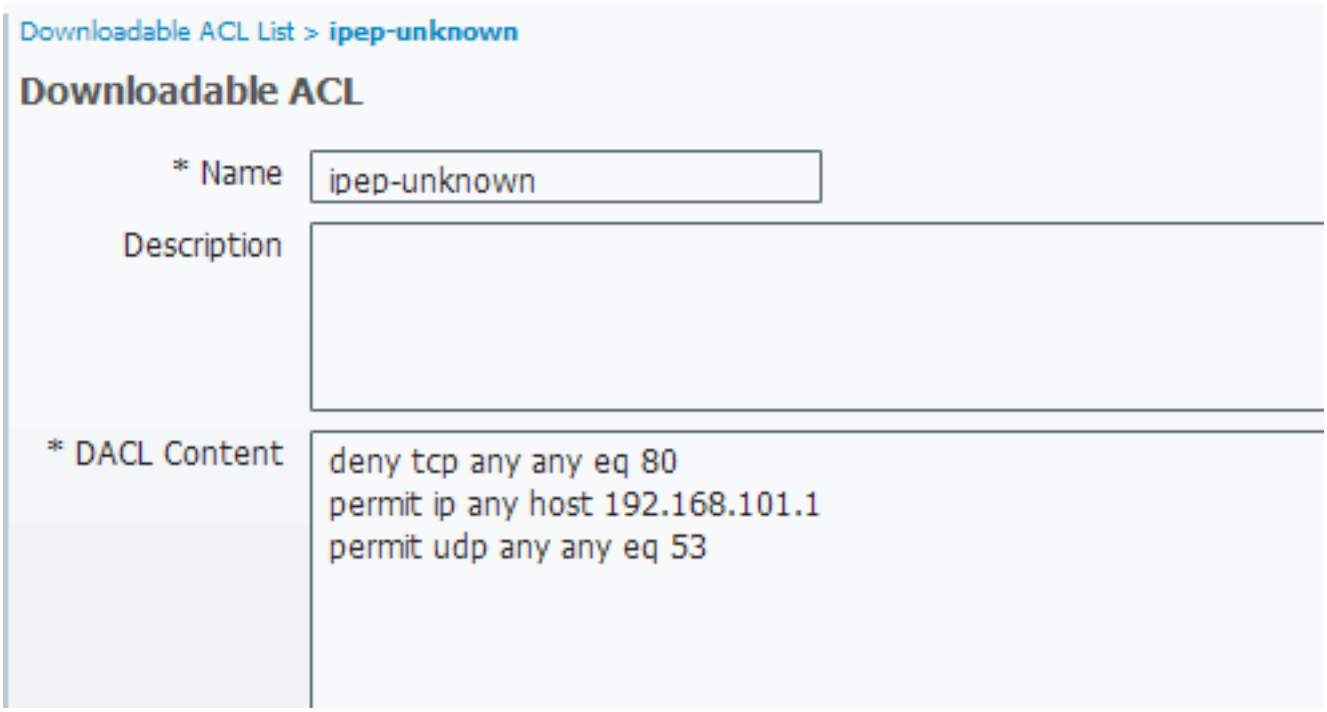
تشكيل توصيفات الوضع

أول ما يجب عمله هو إنشاء قوائم التحكم في الوصول (dACL) وملفات التعريف القابلة للتنزيل:

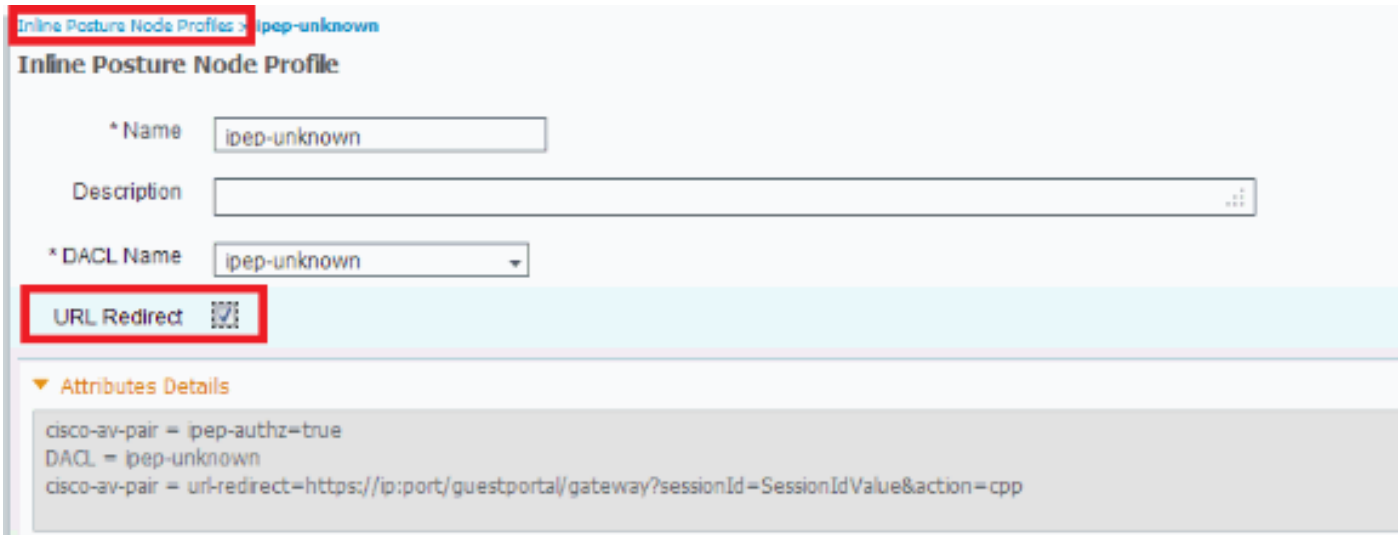
ملاحظة: هذا غير إلزامي لأن يكون اسم قائمة التحكم في الوصول للبنية الأساسية (dACL) مطابقا لاسم ملف التعريف.

- مذعنقائمة التحكم في الوصول (IPEP :(ACL غير معروفملف تعريف التخويل: IPEP غير معروف
- غير متوافققائمة التحكم في الوصول (ACL): غير متوافق مع IPEPملف تعريف التخويل: غير متوافق مع IPEP

قائمة التحكم في الوصول إلى dACL غير معروفة:

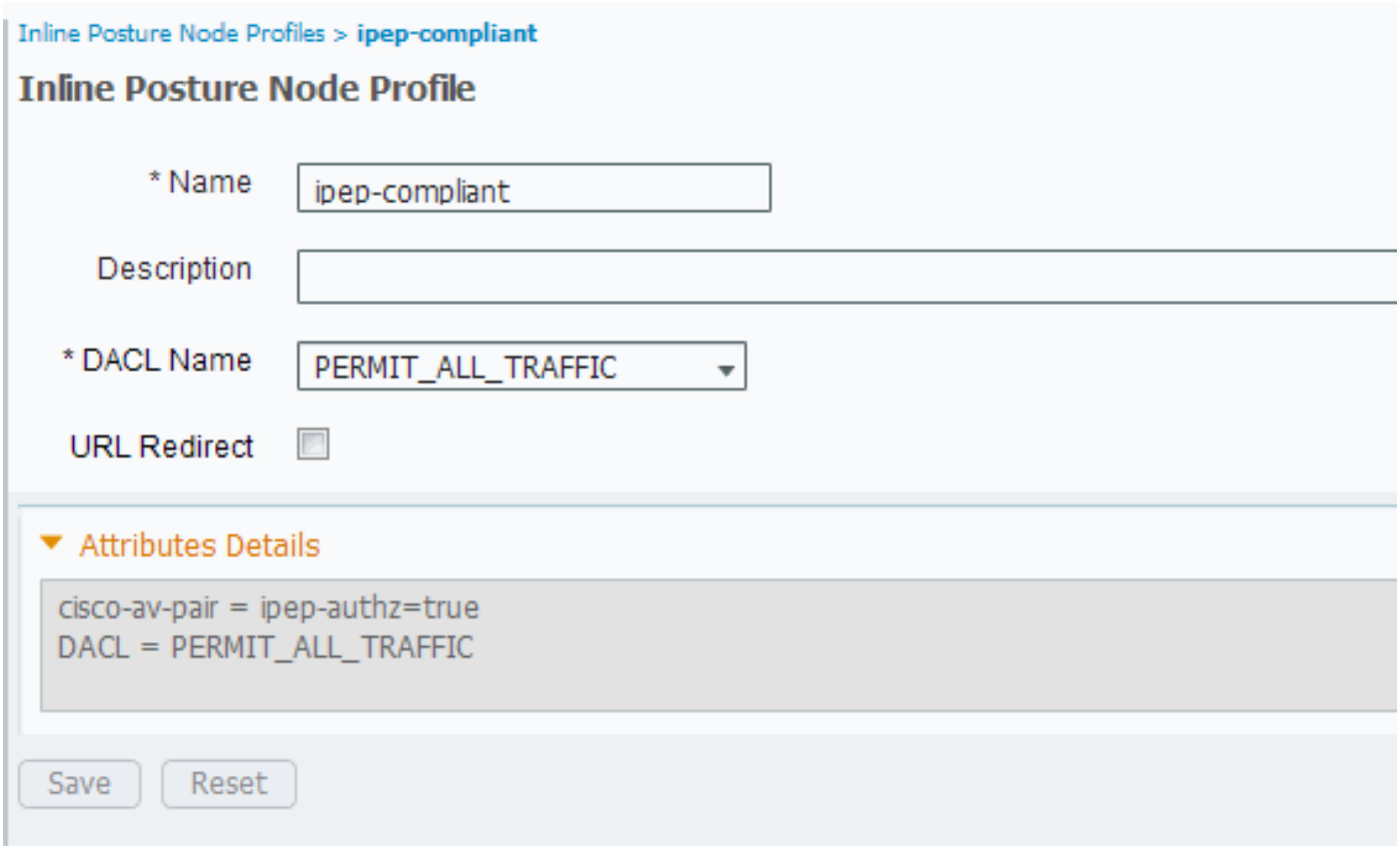


ملف تعريف غير معروف:



قائمة التحكم في الوصول للبنية الأساسية (dACL) متوافقة:

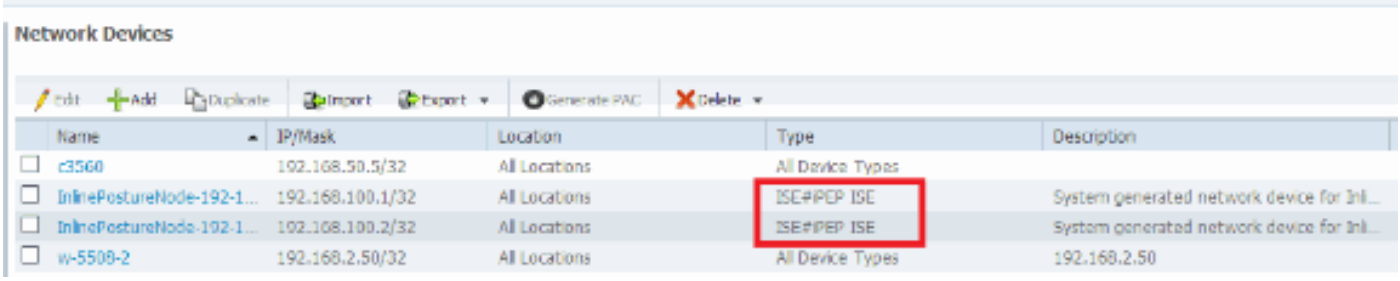
ملف تخصيص متوافق:



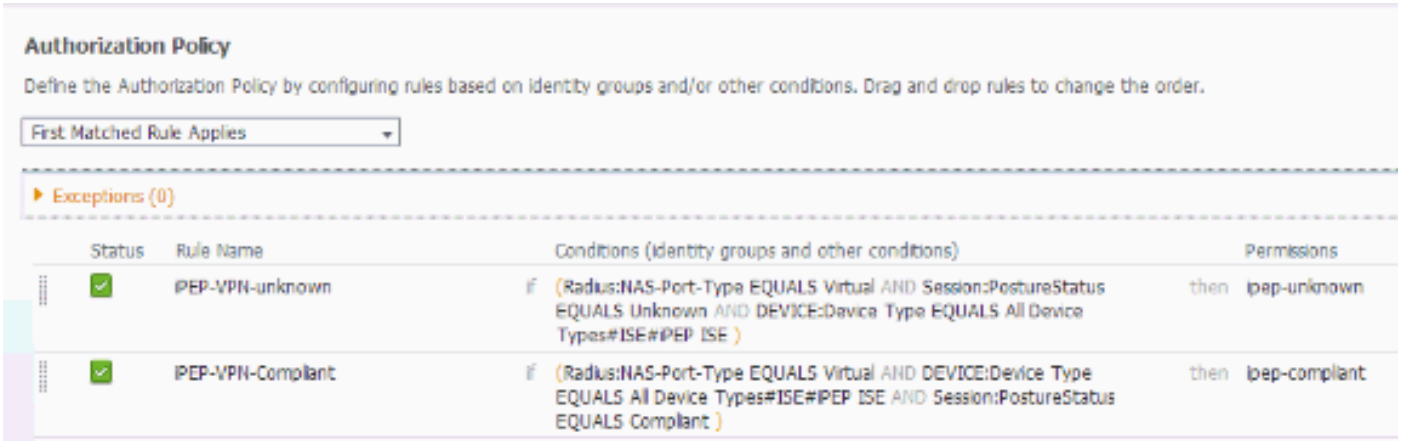
تكوين التفويض

الآن بعد إنشاء التوصيف، يلزمك أن تطابق طلب RADIUS الوارد من iPEP وأن تطبق عليهم التوصيفات الصحيحة.
يتم تحديد ISEs ل iPEP باستخدام نوع جهاز خاص سيتم إستخدامه في قواعد التخويل:

:NADs

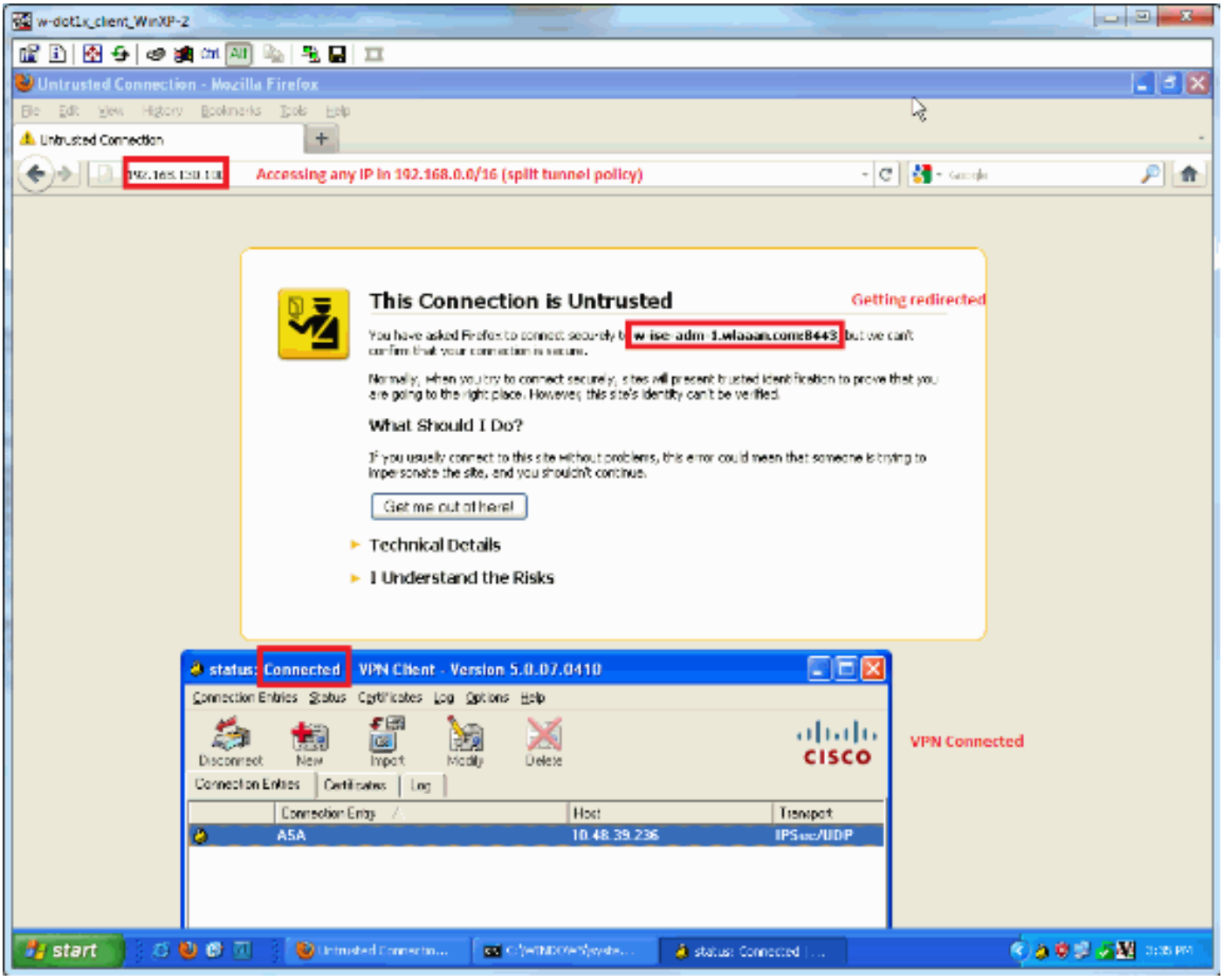


الاعتماد:

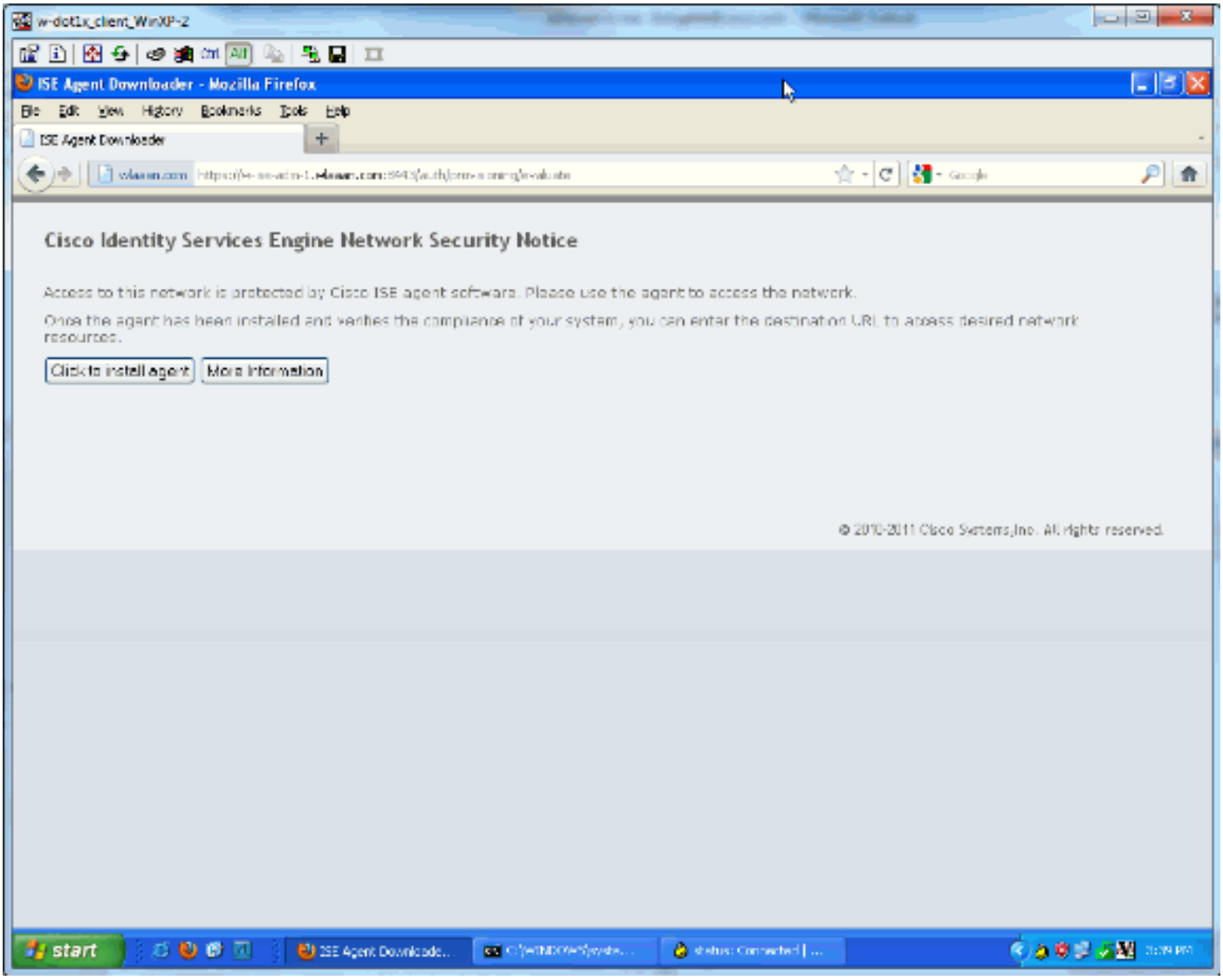


ملاحظة: في حالة عدم تثبيت العميل على الجهاز، يمكنك تحديد قواعد توفير العميل.

نتيجة



تتم مطالبتك بتثبيت الوكيل (في هذا المثال، تم تعيين توفير العميل بالفعل):



بعض المخرجات في هذه المرحلة:

```
ciscoasa# show vpn-sessiondb remote

                                    Session Type: IPsec
          Username     : cisco                  Index        : 26
Assigned IP  : 192.168.5.2           Public IP    : 10.48.39.134
                                       Protocol     : IKE IPsec
                                           License      : IPsec
       Encryption    : AES128                 Hashing      : SHA1
     Bytes Tx      : 143862                 Bytes Rx     : 30628
     Group Policy : DfltGrpPolicy          Tunnel Group : cisco
                     Login Time    : 13:43:55 UTC Mon May 14 2012
                                    Duration     : 0h:09m:37s
                                    Inactivity   : 0h:00m:00s
                                       NAC Result   : Unknown
     VLAN Mapping : N/A                       VLAN         : none
```

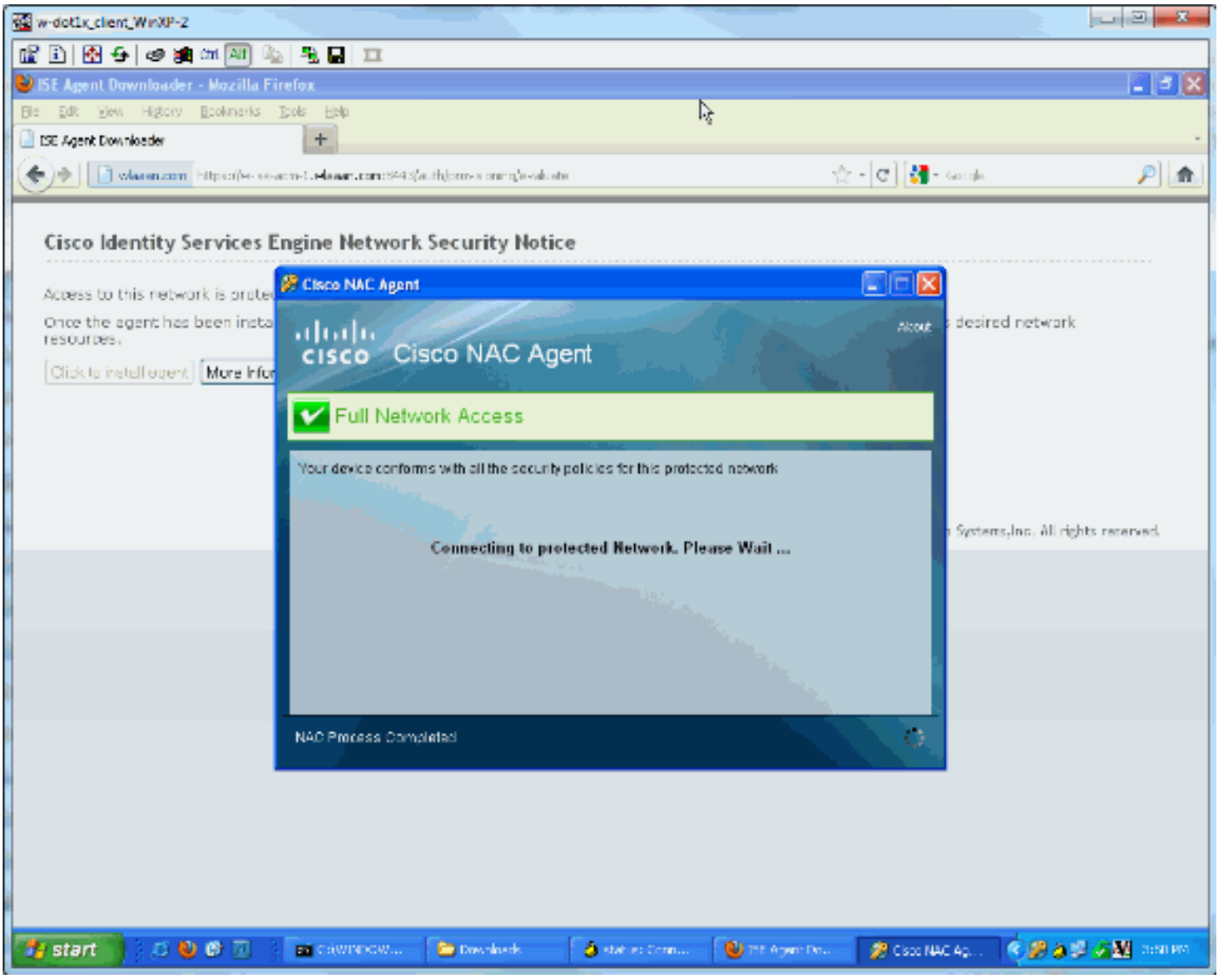
ومن موقع آي بي بي:

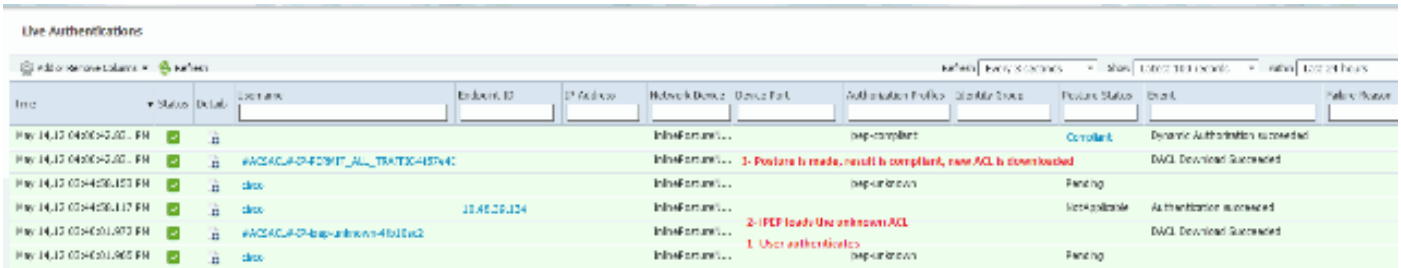
```
w-ise-ipep-1/admin# show pep table session

:((Current Sessions (IP, MAC(if available), Profile ID, VLAN (if any
                                    0 2 00:00:00:00:00:00 192.168.5.2
w-ise-ipep-1/admin# show pep table accesslist normal
:ACSACL#-IP-ipep-unknown-4fb10ac2#
```

```
deny tcp any host 192.168.101.1 eq 80
deny tcp any host 192.168.101.1 eq 443
permit ip any host 192.168.101.1
permit udp any any eq 53
```

بمجرد تنزيل البرنامج وتثبيته:

يجب أن يكتشف العميل ISE تلقائيا ويقوم بتشغيل تقييم الوضع (بافتراض أن قواعد الوضع معرفة بالفعل، وهو موضوع آخر). في هذا مثال، الوضع ناجح، وهذا يظهر:





ملاحظة: توجد إثنتان من المصادقات في لقطة الشاشة أعلاه. ومع ذلك، نظرا لأن مربع بروتوكول iPEP يقوم بتخزين قوائم التحكم في الوصول (ACLs)، فإنه لا يتم تنزيله في كل مرة.

في بروتوكول iPEP:

```
w-ise-ipep-1/admin# show pep table session
```

```
:((Current Sessions (IP, MAC(if available), Profile ID, VLAN (if any
                                    0 3 00:00:00:00:00:00 192.168.5.2
                w-ise-ipep-1/admin# show pep table accesslist normal
                                :ACSACL#-IP-PERMIT_ALL_TRAFFIC-4f57e406#
                                                    permit ip any any

                                        :ACSACL#-IP-ipep-unknown-4fb10ac2#
                                     deny tcp any host 192.168.101.1 eq 80
                                    deny tcp any host 192.168.101.1 eq 443
                                          permit ip any host 192.168.101.1
                                                  permit udp any any eq 53
                                                       #w-ise-ipep-1/admin
```

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems

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).