Postura en línea VPN usando el iPEP ISE y ASA

Contenido

Introducción

Este documento proporciona la información sobre cómo configurar la postura en línea con un dispositivo de seguridad adaptante (ASA) y un Identity Services Engine (ISE).

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en la versión 8.2(4) para el ASA y la versión 1.1.0.665 para el ISE.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

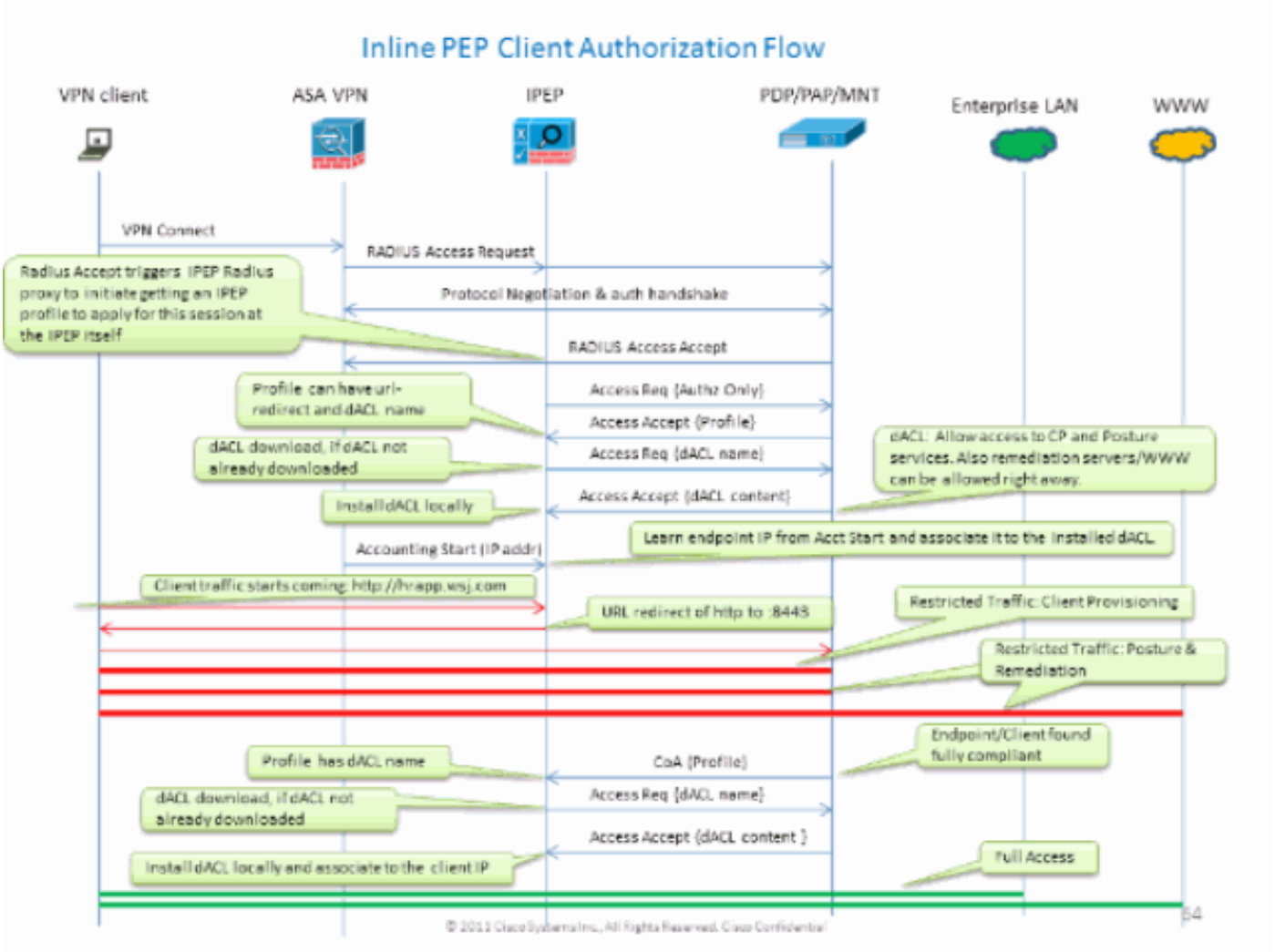
El ISE proporciona muchos servicios AAA (postura, perfilado, autenticación, etc). El cambio del radio del soporte de algunos dispositivos de red (NAD) de la autorización (CoA) que permite cambiar dinámicamente el perfil de la autorización de un dispositivo extremo basó en su postura o resultado del perfilado. Otros NAD tales como el ASA no soportan esta característica todavía. Esto significa que un ISE que se ejecuta en el modo de implementación en línea de la postura (iPEP) es necesario cambiar dinámicamente la directiva de acceso a la red de un dispositivo extremo.

El concepto básico es que todo el tráfico de usuarios pasará a través del iPEP, con el nodo también actuando como representación de RADIUS.

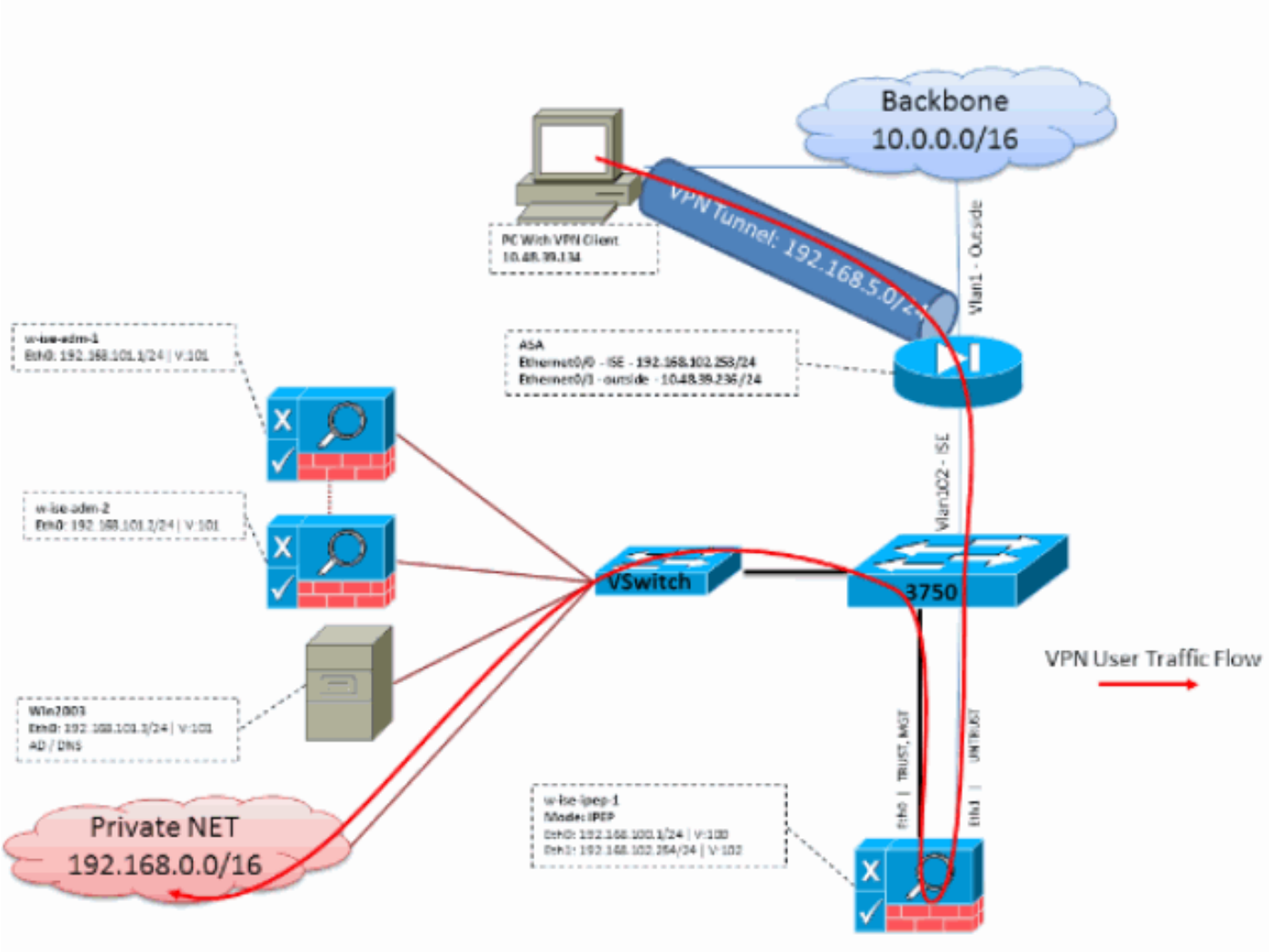
Flujo básico

1. El usuario de VPN abre una sesión.
2. El ASA envía la petición al nodo del iPEP (ISE).
3. El iPEP reescribe la petición (agregando los atributos del cisco av-pair para indicar esto es una autenticación del iPEP) y envía la petición al nodo de la directiva ISE (PDP).
4. El PDP contesta de nuevo al iPEP que remitirá al NAD.
5. Si autentican al usuario, el NAD DEBE enviar una petición del estadística-principio (véase CSCtz84826). Esto accionará el inicio de sesión en el iPEP. En esta etapa, reorientan al usuario para la postura. Además, usted necesita habilitar la interino-estadística-actualización para el túnel establecido del portal del WEBVPN, pues el ISE espera tener el Framed-IP-direccionamiento del atributo en las estadísticas del radio. Sin embargo, al conectar con el portal, la dirección IP VPN del cliente todavía no se sabe porque el túnel no se establece. Esto se asegurará de que el ASA envíe las actualizaciones interinas, por ejemplo cuando el túnel será establecido.
6. El usuario pasa con la evaluación de la postura, y basado en los resultados el PDP pondrá al día la sesión usando el CoA en el iPEP.

Este tiro de pantalla ilustra este proceso:



Ejemplo de topología



Configuración ASA

La configuración ASA es un telecontrol VPN del IPSec simple:

```
!
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 !
```

Configuración ISE

configuración del iPEP

La primera cosa a hacer es agregar un ISE como nodo del iPEP. Usted puede encontrar la información adicional sobre el proceso aquí:

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

Esto es básicamente lo que usted tiene que configurar en las diversas lenguetas (el screenshots proporcionado en esta sección ilustra esto):

- IP untrusted de la configuración y configuraciones del IP global (en este caso, el IP untrusted es 192.168.102.254).
- El despliegue es modo ruteado.
- Ponga un filtro estático para que el ASA sea permitido pasar a través del cuadro del iPEP (si no, la Conectividad a/desde el ISE a través del cuadro del iPEP se cae).
- Configure la directiva ISE como servidor de RADIUS y el ASA como cliente RADIUS.
- Agregue una ruta a la subred VPN esas puntas al ASA.
- Fije el ISE que monitorea como el host de registro (puerto 20514 por abandono; en este caso, la directiva ISE está monitoreando también).

Requisitos para la configuración importantes del certificado:

Antes de intentar registrar un nodo del iPEP, asegúrese de que el certificado siguiente los Requisitos de uso dominantes ampliados está resuelto. Si los Certificados no se configuran correctamente en el iPEP y los Nodos Admin, el proceso de inscripción completará. Sin embargo, usted perderá el acceso admin al nodo del iPEP. Los detalles siguientes se han extrapolado del Guía de despliegue del iPEP ISE 1.1.x:

La presencia de ciertas combinaciones de atributos en los Certificados locales de la administración y de los Nodos en línea de la postura puede evitar que la autenticación recíproca trabaje.

Los atributos son:

- Uso dominante extendido (EKU) — Autenticación de servidor
- Uso dominante extendido (EKU) — Autenticación de cliente
- Tipo CERT de Netscape — Autenticación de servidor SSL
- Tipo CERT de Netscape — Autenticación de cliente SSL

Cualquiera de las combinaciones siguientes se requiere para el certificado de la administración:

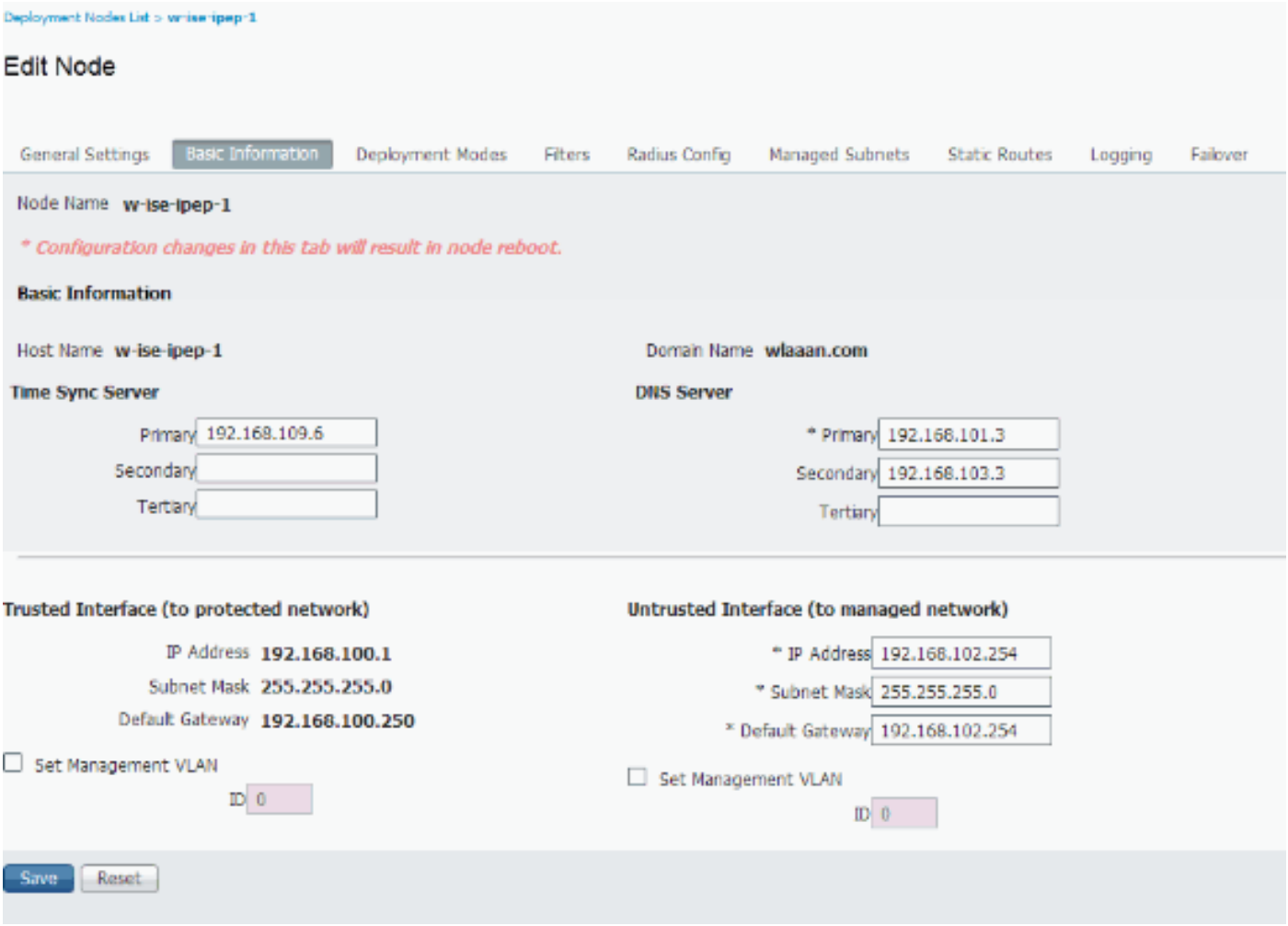
- Ambos atributos del EKU deben ser inhabilitados, si ambos atributos del EKU se inhabilitan

en el certificado en línea de la postura, o ambos atributos del EKU deben ser habilitados, si el atributo del servidor se habilita en el certificado en línea de la postura.
- Ambos atributos types CERT de Netscape deben ser inhabilitados, o ambos deben ser habilitados.

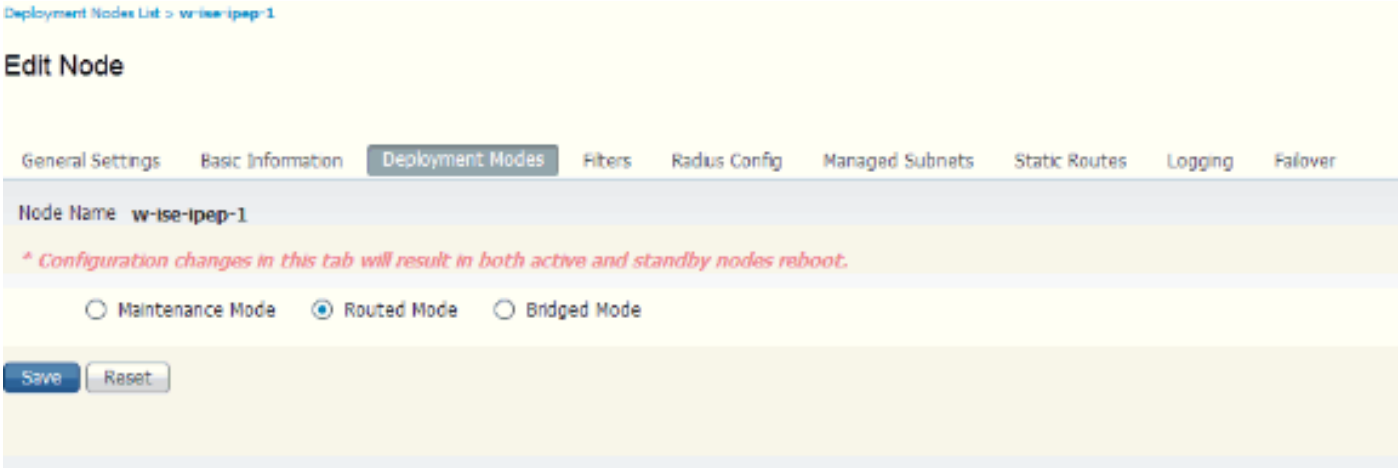
Cualquiera de las combinaciones siguientes se requiere para el certificado en línea de la postura:

- Ambos atributos del EKU deben ser inhabilitados, o ambos deben ser habilitados, o el atributo del servidor solamente debe ser habilitado.
- Ambos atributos types CERT de Netscape deben ser inhabilitados, o ambos deben ser habilitados, o el atributo del servidor solamente debe ser habilitado.
- Donde los Certificados locales uno mismo-firmados se utilizan en la administración y los Nodos en línea de la postura, usted debe instalar el certificado autofirmado del nodo de la administración en la lista de la confianza del nodo en línea de la postura. Además, si usted tiene Nodos primarios y secundarios de la administración en su despliegue, usted debe instalar el certificado autofirmado de ambos Nodos de la administración en la lista de la confianza del nodo en línea de la postura.
- Donde los Certificados locales CA-firmados se utilizan en la administración y los Nodos en línea de la postura, la autenticación recíproca debe trabajar correctamente. En este caso, el certificado de CA de firma está instalado en el nodo de la administración antes del registro, y este certificado se replica al nodo en línea de la postura.
- Si las claves CA-publicadas se utilizan para la comunicación de sujeción entre la administración y los Nodos en línea de la postura, antes de que usted registre el nodo en línea de la postura, usted debe agregar la clave pública (certificado de CA) del nodo de la administración a la lista del certificado de CA del nodo en línea de la postura.

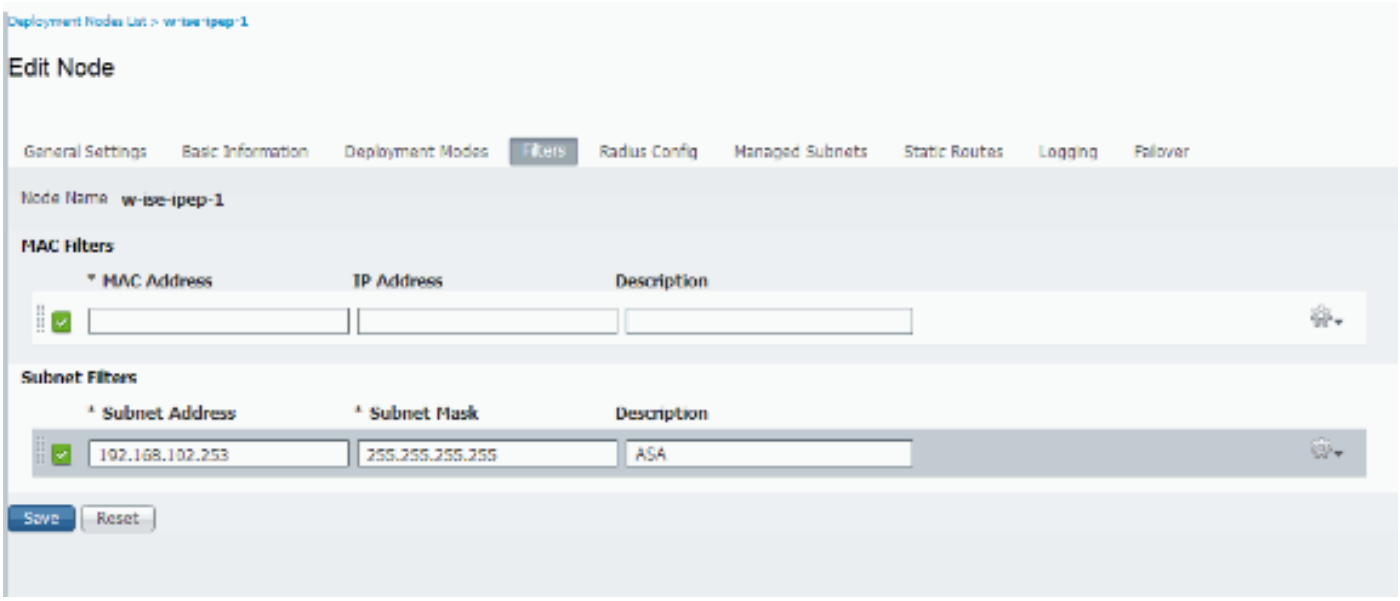
Configuración básica:



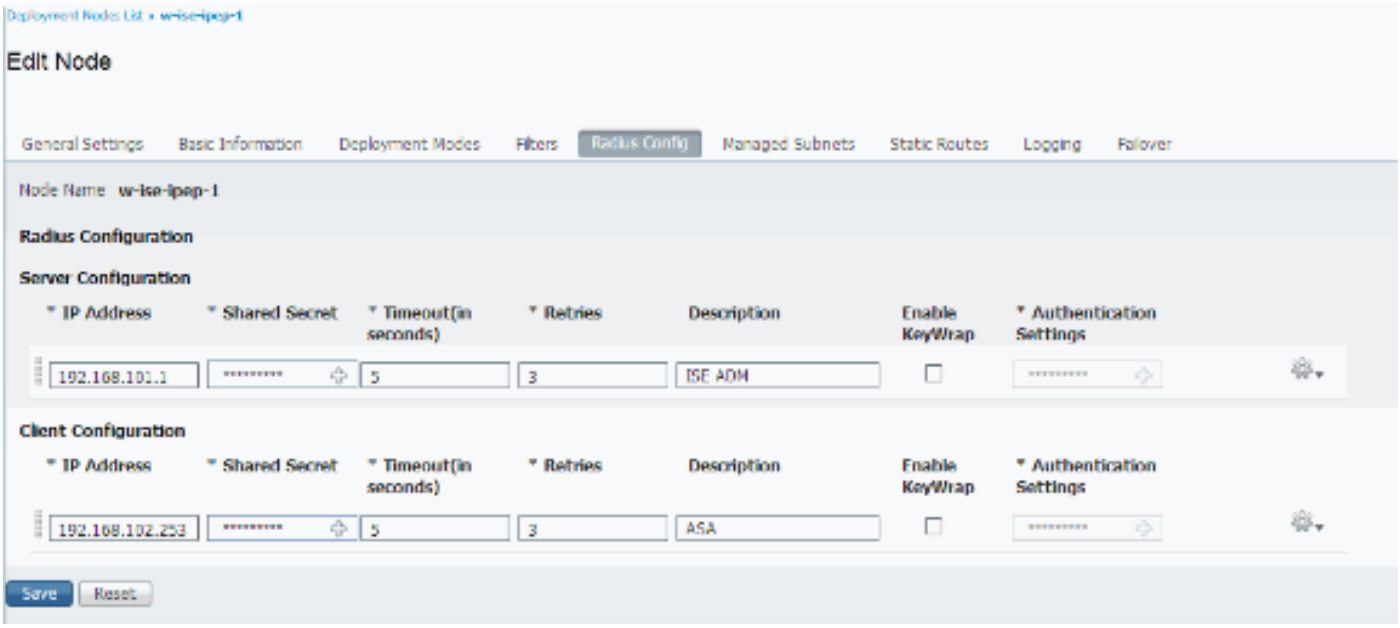
Configuración de modo del despliegue:



Configuración de filtros:

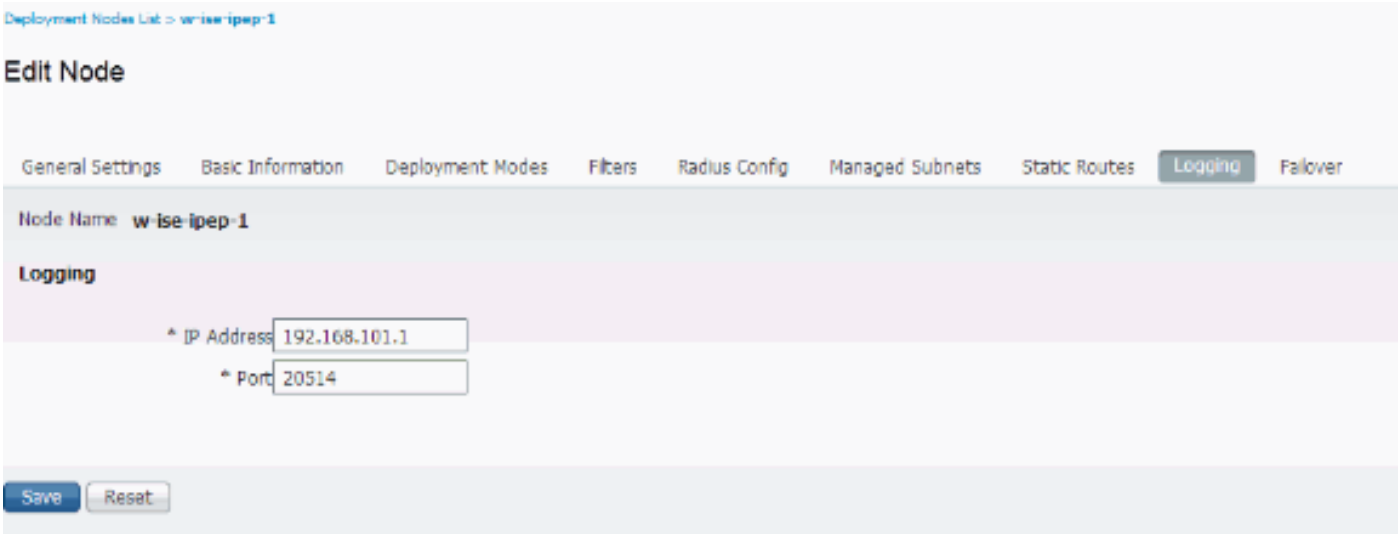


Configuración de RADIUS:



Static rutas:

Registración:



Autenticación y configuración de la postura

Hay tres estados de la postura:

- Desconocido: La postura todavía no se hace
- Obediente: Se hace la postura y el sistema es obediente
- No obediente: Se hace la postura, pero el sistema falló por lo menos un control

Ahora los perfiles de la autorización tienen que ser creados (que serán autorización en línea perfilan: Esto agregará el atributo del ipep-authz=true en el cisco av-pair) que será utilizado para el diverso caso.

Comúnmente, el perfil el desconocido vuelve la reorientación URL (detección de la postura) que remitirá el tráfico del usuario al ISE y pedirá instalar el agente del NAC. Si el agente del NAC está instalado ya, éste permitirá que su petición de la detección HTTP sea remitida al ISE.

En este perfil, un ACL que permite tráfico HTTP al ISE y el DNS por lo menos se utiliza.

Los perfiles obedientes y no obedientes vuelven generalmente a ACL descargable para conceder el acceso a la red basado en el perfil del usuario. El perfil no obediente puede permitir que los usuarios accedan a un servidor Web para descargar un antivirus por ejemplo, o conceda el acceso a la red limitado.

En este ejemplo, se crean los perfiles desconocidos y obedientes, y la presencia de notepad.exe mientras que se marcan los requisitos.

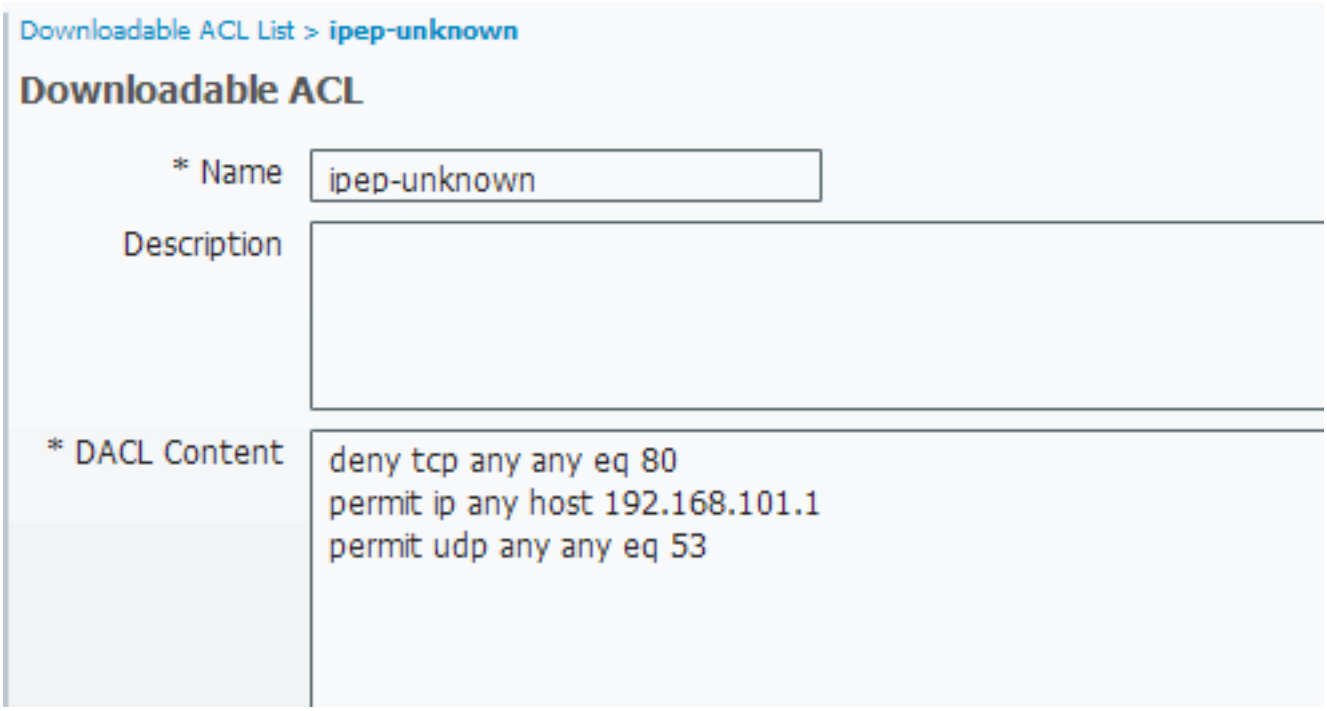
La postura perfila la configuración

La primera cosa a hacer es crear los ACL transferibles (dACL) y los perfiles:

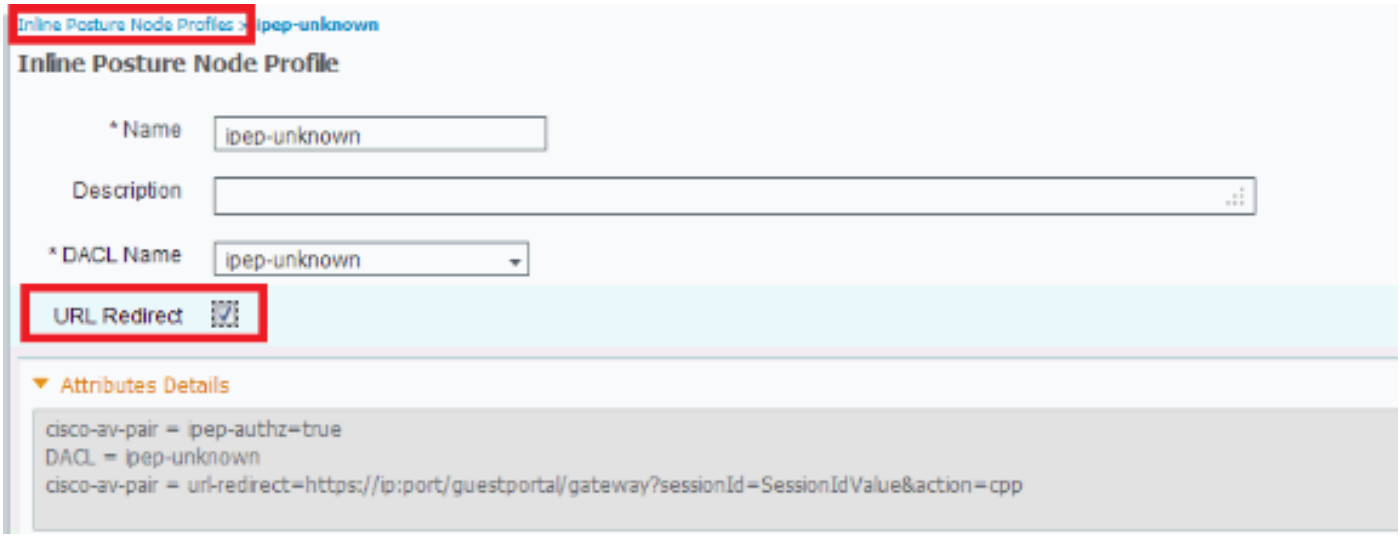
Note: Esto no es obligatorio tener el nombre del dACL que corresponde con el nombre del perfil.

- ObedienteACL: ipep-desconocidoPerfil de la autorización: ipep-desconocido
- No obedienteACL: ipep-NON-obedientePerfil de la autorización: ipep-NON-obediente

DACL desconocido:

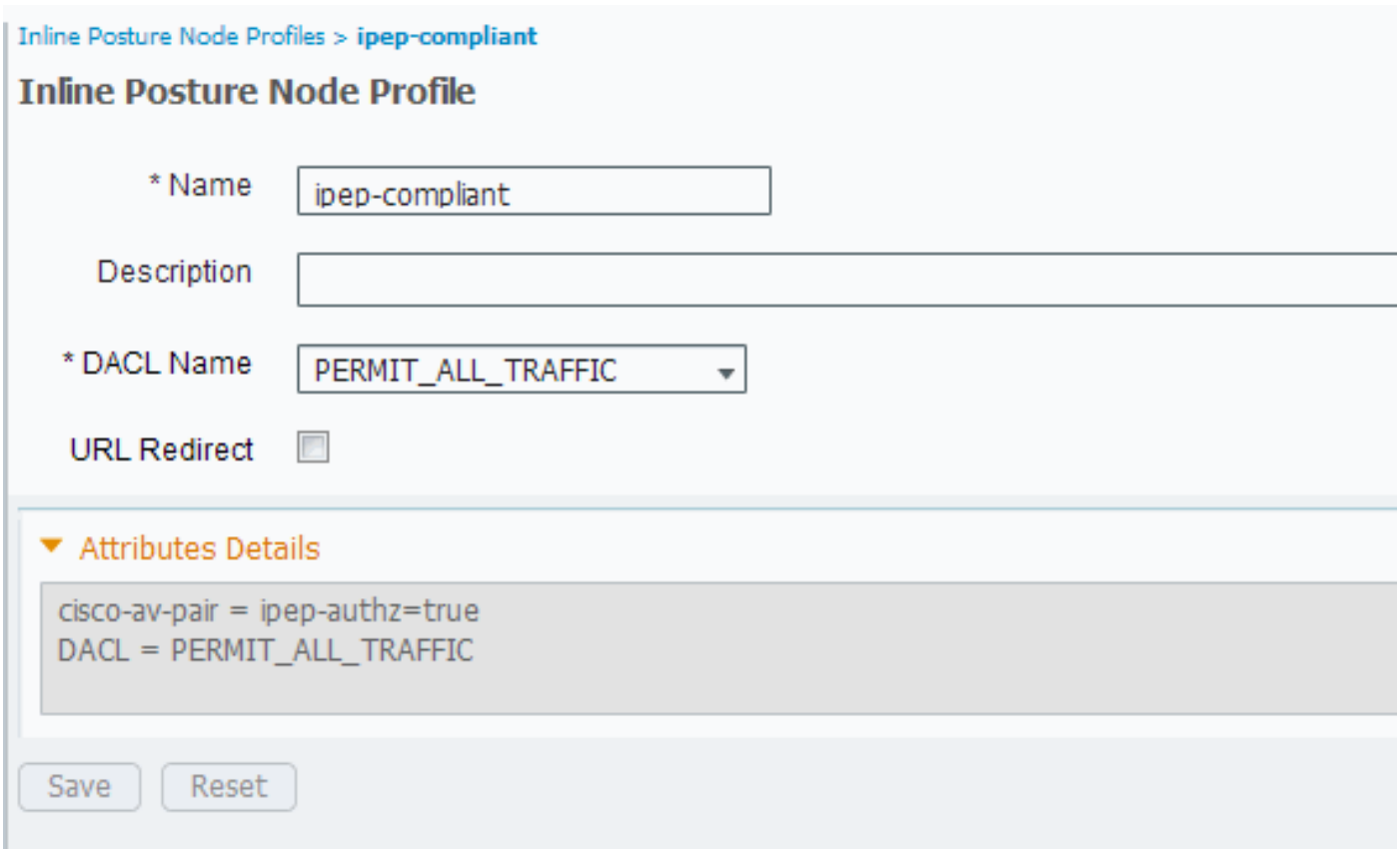


Perfil desconocido:



DACL obediente:

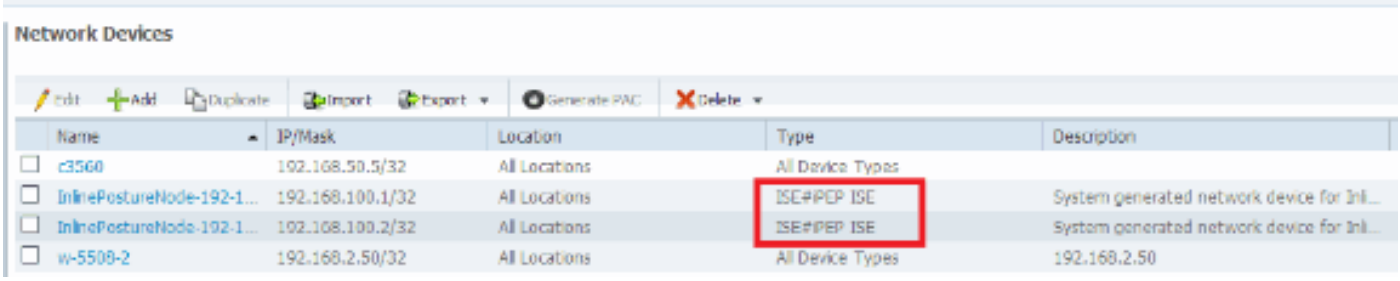
Perfil obediente:



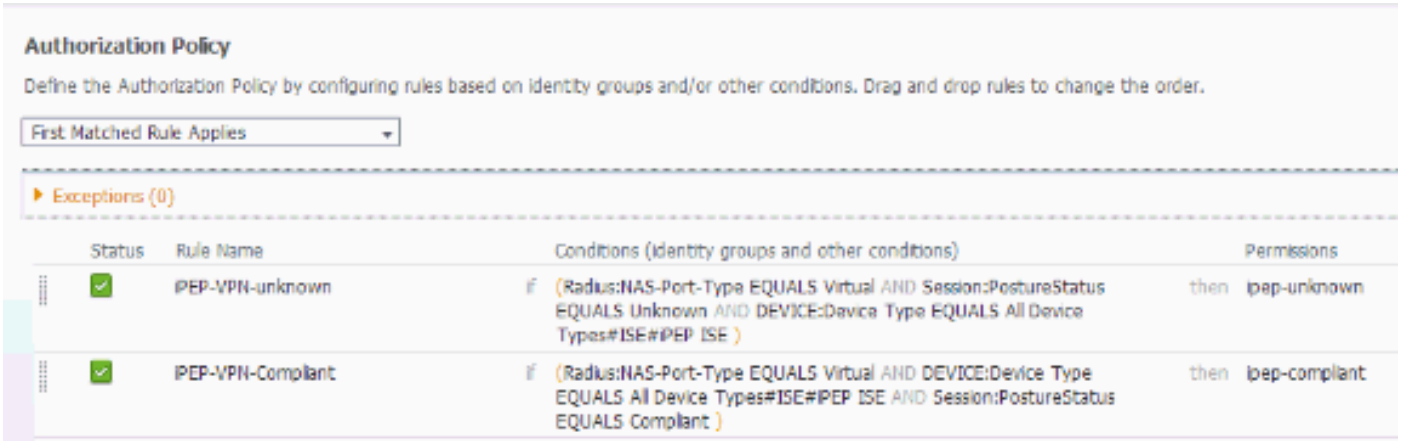
Configuración de la autorización

Ahora que se crea el perfil, usted necesita hacer juego el pedido de RADIUS que viene del iPEP y aplicar a ellos los perfiles de la derecha. El iPEP ISE se define con un tipo de dispositivo especial que sea utilizado en las reglas de la autorización:

NAD:

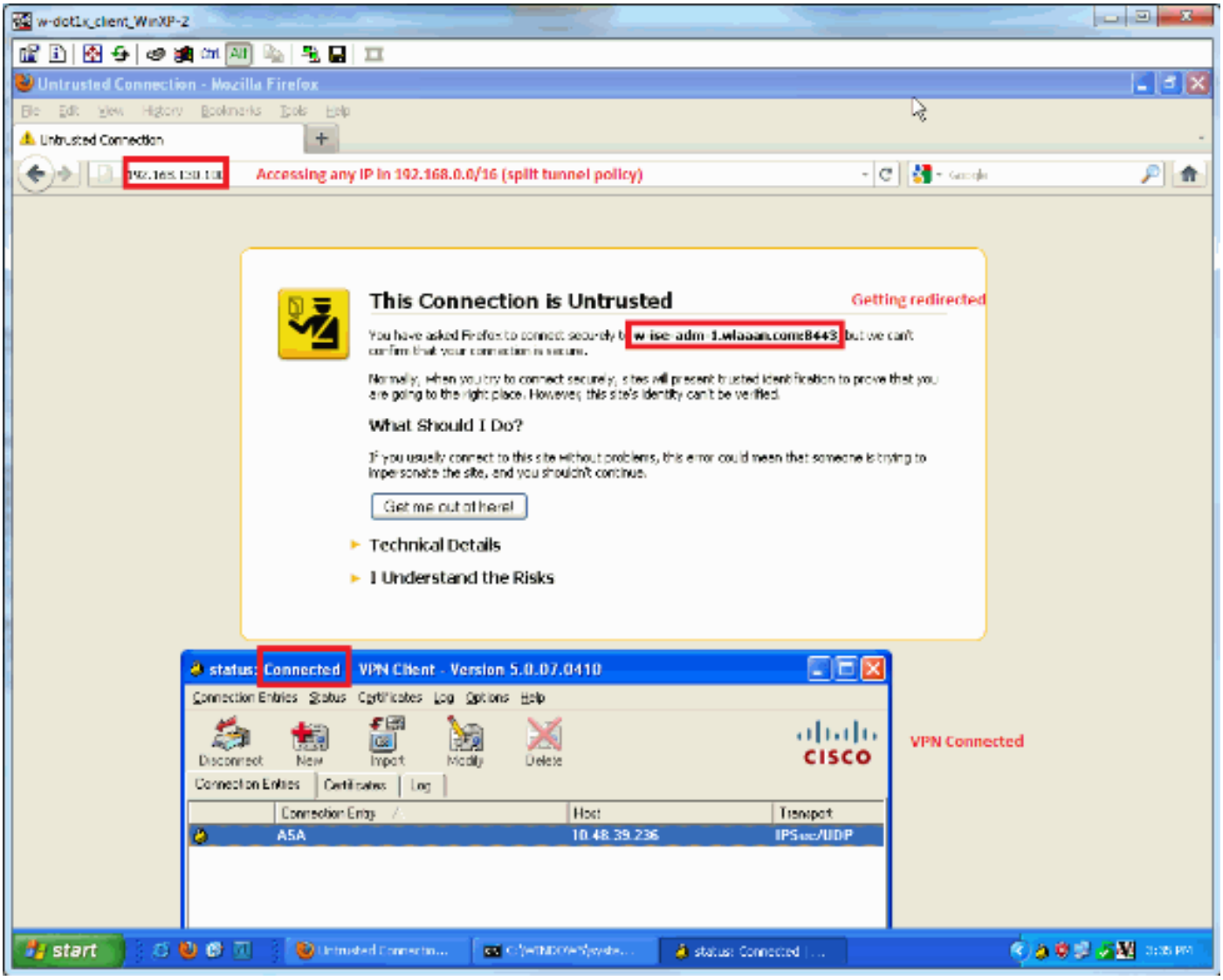


Autorización:

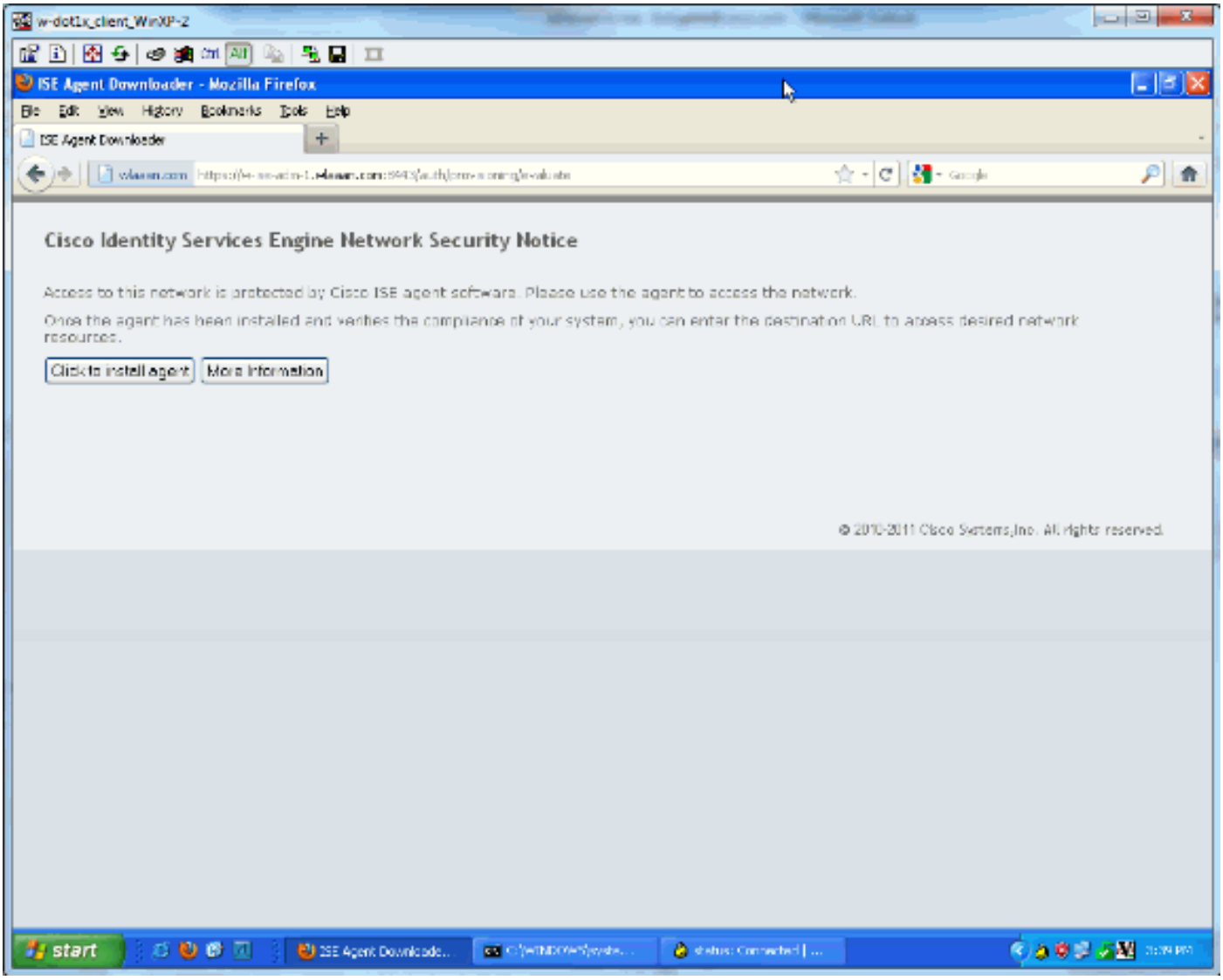


Note: Si el agente no está instalado en la máquina, usted puede definir las reglas del aprovisionamiento del cliente.

Resultado



A le indican que instale el agente (en este ejemplo, el aprovisionamiento del cliente se fija ya):



Una cierta salida en esta etapa:

```
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
```

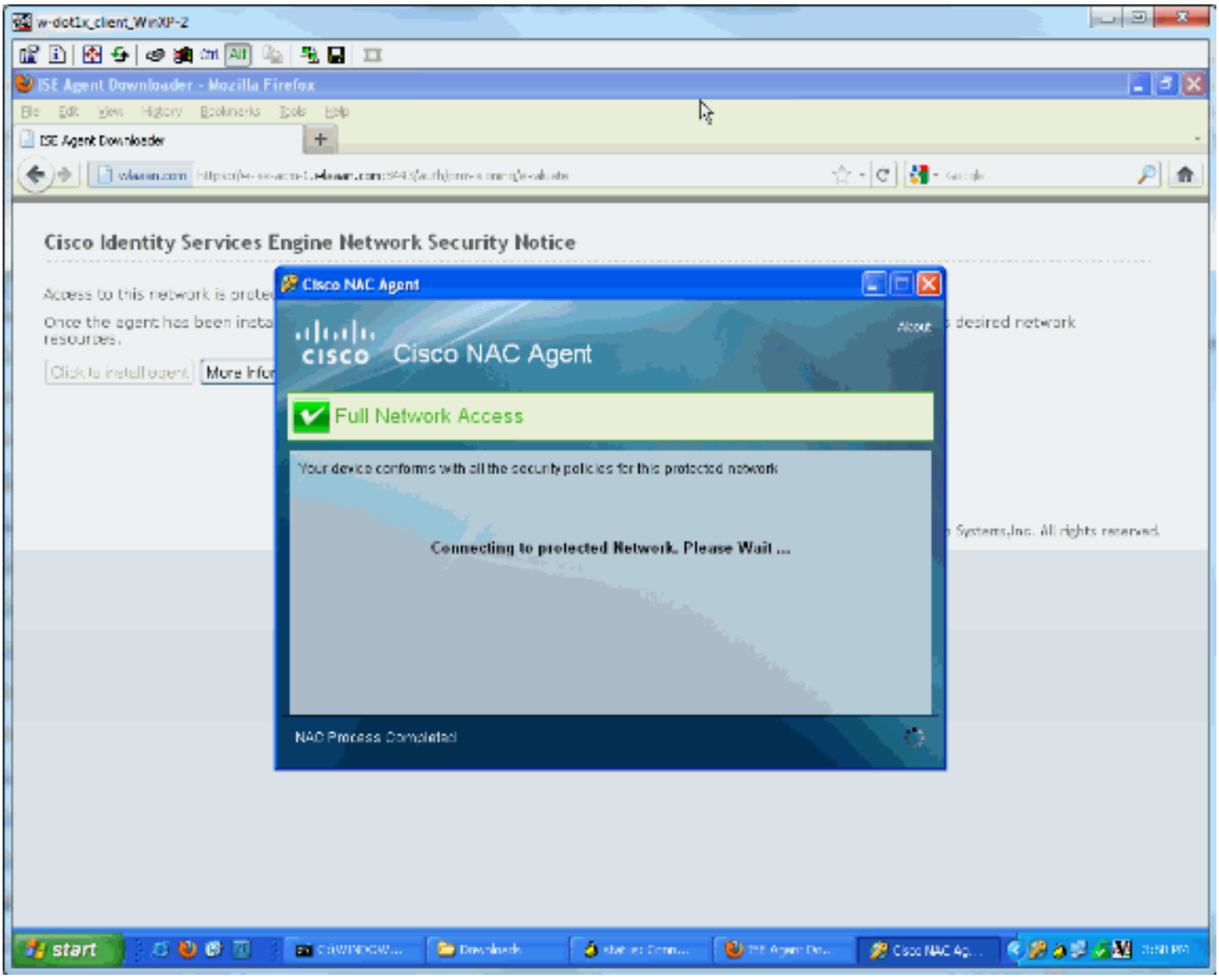
Y del iPEP:

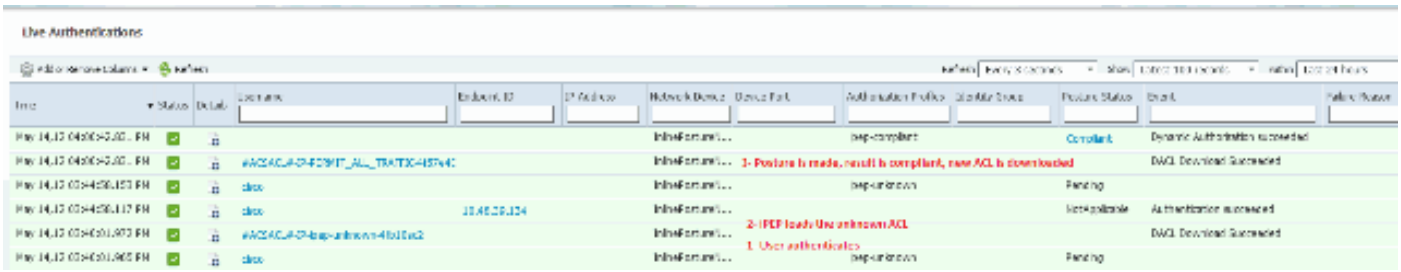
```
w-ise-ipep-1/admin# show pep table session

Current Sessions (IP, MAC(if available), Profile ID, VLAN (if any)):
192.168.5.2 00:00:00:00:00:00 2 0
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
```

Una vez que se descarga y está instalado el agente:

El agente debe detectar automáticamente el ISE y funciona con la evaluación de la postura (si se asume que le tenga las reglas de la postura definidas ya, que es otro tema). En este ejemplo, la postura es acertada, y ésta aparece:





Note: Hay dos autenticaciones en el tiro de pantalla arriba. Sin embargo, porque el cuadro del iPEP oculta los ACL, no se descarga cada vez.

En el iPEP:

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

Current Sessions (IP, MAC(if available), Profile ID, VLAN (if any)):
192.168.5.2 00:00:00:00:00:00 3 0
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#
```

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems