

Comparación del flujo de redirección de postura de ISE con el flujo sin redirección de postura de ISE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Flujo de estado previo a ISE 2.2](#)

[Flujo de estado posterior a ISE 2.2](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración de aprovisionamiento de clientes](#)

[Políticas y condiciones de estado](#)

[Configuración de Client Provisioning Portal](#)

[Configurar perfiles y directivas de autorización](#)

[Verificación](#)

[Troubleshoot](#)

[Información general](#)

[Solución de problemas comunes](#)

[Problemas relacionados con SSO](#)

[Solucionar problemas de selección de directiva de aprovisionamiento de clientes](#)

[Troubleshooting del Proceso de Postura](#)

Introducción

Este documento describe la comparación del flujo sin redirección de estado admitido en ISE 2.2 y versiones posteriores con el flujo de redirección de estado admitido desde versiones anteriores de ISE.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Flujo de estado en ISE
- Configuración de los componentes de estado en ISE
- Configuración del dispositivo de seguridad adaptable (ASA) para el estado en redes privadas virtuales (VPN)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ISE versión 2.2
- Cisco ASA v con software 9.6 (2)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Este documento describe una nueva funcionalidad introducida en Identity Service Engine (ISE) 2.2 que permite que ISE admita un flujo de estado sin ningún tipo de soporte de redirección en un dispositivo de acceso a la red (NAD) o ISE.

La condición es un componente central de Cisco ISE. La posición como componente puede estar representada por tres elementos principales:

1. ISE como punto de decisión y distribución de configuración de políticas.
Desde la perspectiva del administrador en ISE, usted configura las políticas de estado (qué condiciones exactas se deben cumplir para marcar un dispositivo como compatible con la empresa), las políticas de aprovisionamiento de clientes (qué software de agente se debe instalar en qué tipo de dispositivos) y las políticas de autorización (a qué tipo de permisos se deben asignar, depende de su estado).
2. Un dispositivo de acceso a la red como punto de aplicación de políticas.
En el lado NAD, las restricciones de autorización reales se aplican en el momento de la autenticación del usuario. ISE como punto de política proporciona parámetros de autorización como ACL descargada (dACL)/VLAN/URL de redirección/lista de control de acceso (ACL) de redirección. Tradicionalmente, para que se produzca el estado, se requiere que los NAD admitan la redirección (para indicar al software de usuario o agente con qué nodo de ISE se debe establecer contacto) y el cambio de autorización (CoA) para volver a autenticar al usuario una vez determinado el estado del terminal.
3. Software de agente como punto de recopilación de datos e interacción con el usuario final.
Cisco ISE utiliza tres tipos de software de agente: AnyConnect ISE Posture Module, NAC Agent y Web Agent. El agente recibe información sobre los requisitos de estado de ISE y proporciona un informe a ISE sobre el estado de los requisitos.

Nota: Este documento se basa en el módulo de postura de Anyconnect ISE, que es el único que admite totalmente la postura sin redirección.

En la condición de flujo anterior a ISE 2.2, los NAD no solo se utilizan para autenticar usuarios y restringir el acceso, sino también para proporcionar información al software del agente sobre un nodo de ISE específico con el que se debe contactar. Como parte del proceso de redirección, la información sobre el nodo de ISE se devuelve al software del agente.

Históricamente, el soporte de redirección, tanto por parte de NAD como de ISE, era un requisito esencial para la implementación de la postura. En ISE 2.2, se elimina el requisito de admitir la redirección tanto para el aprovisionamiento inicial del cliente como para el proceso de estado.

Aprovisionamiento de clientes sin redirección: en ISE 2.2 puede acceder al portal de aprovisionamiento de clientes (CPP) directamente a través del nombre de dominio completamente calificado (FQDN) del portal. Es similar a la forma en que accede al Portal del patrocinador o al Portal de Mi dispositivo.

Proceso de estado sin redirección: durante la instalación del agente desde el portal CPP, la información sobre los servidores ISE se guarda en el lado del cliente, lo que hace posible la comunicación directa.

Flujo de estado previo a ISE 2.2

En esta imagen se muestra una explicación paso a paso del flujo del módulo de posición de Anyconnect ISE anterior a ISE 2.2:

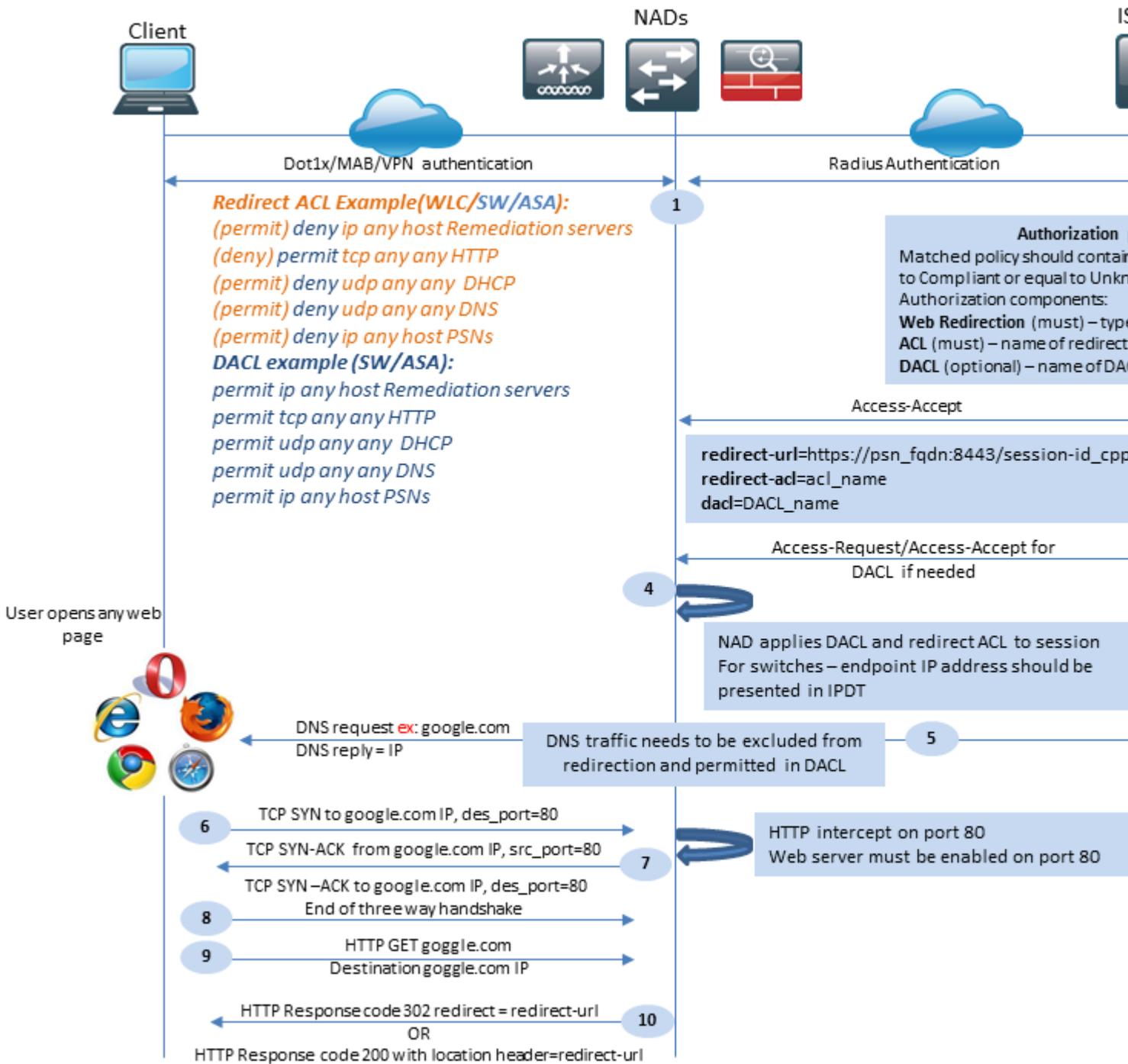


Figura 1-1

Paso 1. La autenticación es el primer paso del flujo, puede ser dot1x, MAB o VPN.

Paso 2. ISE debe elegir una política de autenticación y autorización para el usuario. En el escenario de estado elegido, la directiva de autorización debe contener una referencia al estado de estado, que inicialmente debe ser desconocido o no aplicable. Para cubrir ambos casos, se pueden utilizar condiciones con estado de condición y cumplimiento desigual.

El perfil de autorización elegido debe contener información sobre la redirección:

- Redirección web: para el caso de estado, el tipo de redirección web se debe especificar como aprovisionamiento de cliente (estado).
- ACL: esta sección debe contener el nombre de ACL configurado en el lado NAD. Esta ACL se utiliza para indicar a NAD qué tráfico debe omitir la redirección y cuál debe redirigirse realmente.
- DACL: se puede utilizar junto con la lista de acceso de redirección, pero debe tener en cuenta que las diferentes plataformas procesan DACL y ACL de redirección en un orden diferente.

Por ejemplo, ASA siempre procesa la DACL antes de redirigir la ACL. Al mismo tiempo, algunas plataformas de switch lo procesan de la misma manera que ASA, y otras plataformas de switch procesan primero la ACL de redirección y luego verifican la ACL/ACL de interfaz si se debe descartar o permitir el tráfico.

Nota: Después de activar la opción de redirección web en el perfil de autorización, debe seleccionar el portal de destino para la redirección.

Paso 3. ISE devuelve Access-Accept con atributos de autorización. ISE genera automáticamente la URL de redirección en los atributos de autorización. Contiene estos componentes:

- FQDN del nodo de ISE en el que se realizó la autenticación. En algunos casos, el FQDN dinámico se puede sobrescribir mediante la configuración del perfil de autorización (IP/nombre de host/FQDN estático) en la sección Redirección web. Si se utiliza el valor estático, debe apuntar al mismo nodo ISE donde se procesó la autenticación. En el caso del equilibrador de carga (LB), este FQDN puede apuntar a LB VIP, pero solo en el caso de que LB esté configurado para vincular las conexiones RADIUS y SSL.
- Puerto: el valor del puerto se obtiene de la configuración del portal de destino.
- ID de sesión: ISE toma este valor de la ID de sesión de auditoría del par AV de Cisco presentada en Access-Request. NAD genera dinámicamente el valor en sí.
- ID del portal: identificador de un portal de destino en el lado de ISE.

Paso 4. NAD aplica una directiva de autorización a la sesión. Además, si se configura DACL, su contenido se solicita antes de que se apliquen las políticas de autorización.

Consideraciones importantes:

- Todos los dispositivos NAD deben tener una ACL configurada localmente con el mismo nombre que la recibida en Access-Accept como redirect-acl.
- Switches: la dirección IP del cliente se debe presentar en la salida de `show authentication session interface details` para aplicar correctamente la redirección y las ACL. La dirección IP del cliente se aprende mediante la función IPDT (del inglés IP Device Tracking Feature, función de seguimiento de dispositivos IP).

Paso 5. El cliente envía una solicitud DNS para el FQDN que se introduce en el explorador web. En esta etapa, el tráfico DNS debe omitir la redirección y el servidor DNS debe devolver la dirección IP correcta.

Paso 6. El cliente envía TCP SYN a la dirección IP que se recibe en la respuesta DNS. La dirección IP de

origen en el paquete es la IP del cliente y la dirección IP de destino es la IP del recurso solicitado. El puerto de destino es igual a 80, excepto en los casos en los que se configura un proxy HTTP directo en el explorador web del cliente.

El paso 7.NAD intercepta las solicitudes del cliente y prepara los paquetes SYN-ACK con una IP de origen igual a la IP de recurso solicitada, una IP de destino igual a la IP del cliente y un puerto de origen igual a 80.

Consideraciones importantes:

- Los NAD deben tener un servidor HTTP que se ejecute en el puerto en el que el cliente envía las solicitudes. De forma predeterminada, es el puerto 80.
- Si el cliente utiliza un servidor web proxy HTTP directo, el servidor HTTP debe ejecutarse en el puerto proxy del NAS. Este escenario está fuera del alcance de este documento.
- En los casos en que NAD no tiene una dirección IP local en el cliente, la subred SYN-ACK se envía con la tabla de ruteo NAD (por la interfaz de administración generalmente). En este escenario, el paquete se enruta sobre la infraestructura L3 y debe ser enrutado de vuelta hacia el cliente por un dispositivo ascendente L3. Si el dispositivo L3 es un firewall con estado, se debe proporcionar una excepción adicional para dicho ruteo asimétrico.

Paso 8. El cliente finaliza el protocolo de enlace de tres vías TCP mediante ACK.

Paso 9. Un cliente envía HTTP GET para el recurso de destino.

Paso 10. NAD devuelve una URL de redirección al cliente con código HTTP 302 (página movida); en algunos NAD, la redirección se puede devolver dentro del mensaje HTTP 200 OK en el encabezado de ubicación.

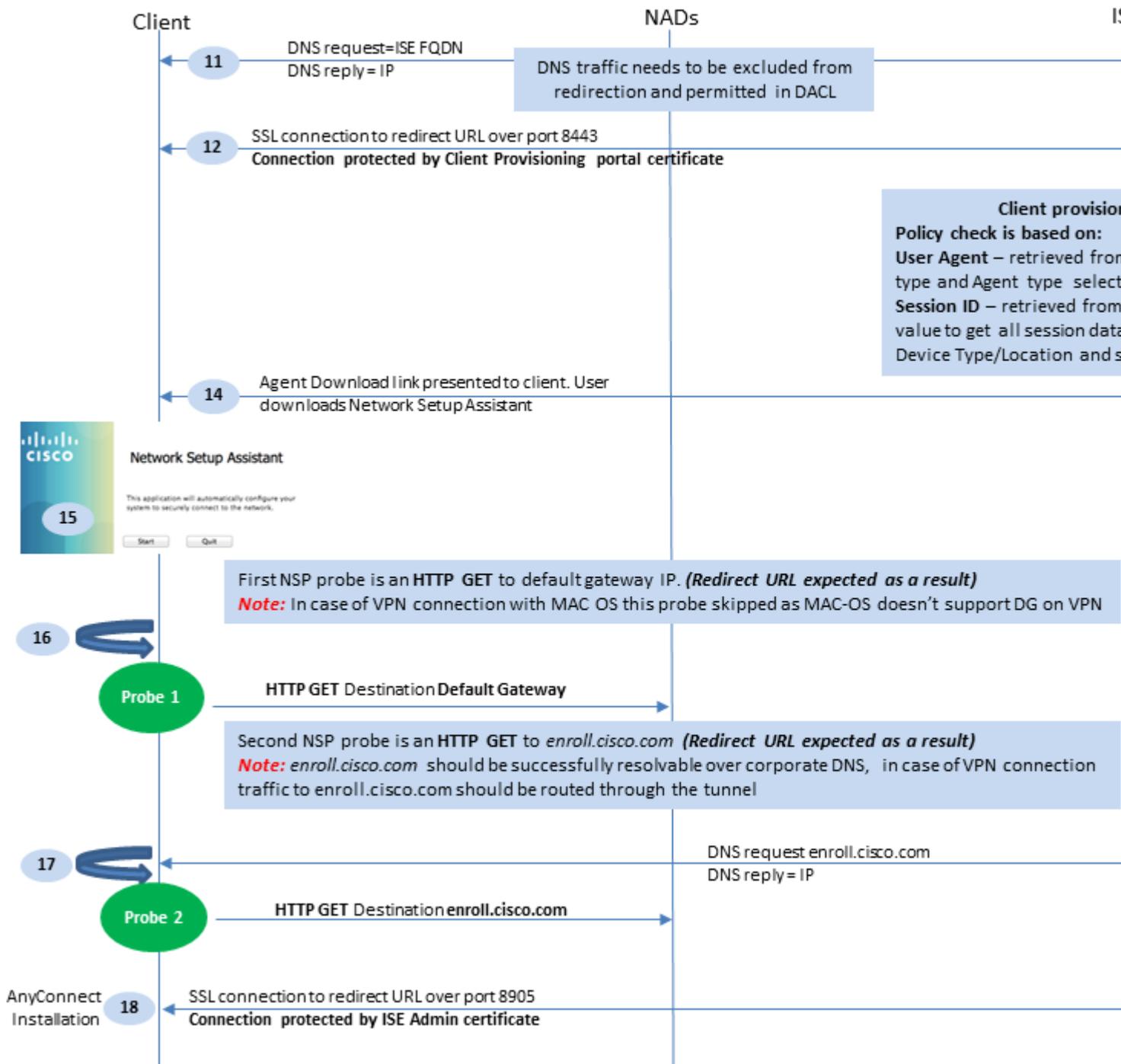


Figura 1-2

Paso 11. El cliente envía una solicitud DNS para el FQDN desde la URL de redirección. El FQDN debe poder resolverse en el servidor DNS.

Paso 12. Se establece la conexión SSL a través del puerto recibido en la URL de redirección (valor predeterminado: 8443). Esta conexión está protegida por un certificado de portal del lado de ISE. El portal de aprovisionamiento de clientes (CPP) se presenta al usuario.

Paso 13. Antes de proporcionar una opción de descarga al cliente, ISE debe seleccionar la política de aprovisionamiento de clientes (CP) objetivo. El sistema operativo (SO) del cliente detectado en el agente de usuario del explorador y otra información necesaria para la selección de directivas de CPP se recuperan de la sesión de autenticación (como los grupos AD/LDAP, etc.). ISE conoce la sesión de destino a partir de la ID de sesión presentada en la URL de redirección.

Paso 14. El enlace de descarga de Network Setup Assistant (NSA) se devuelve al cliente. El cliente descarga la aplicación.

Nota: Normalmente, puede ver la NSA como parte del flujo de BYOD para Windows y Android, pero también esta aplicación se puede utilizar para instalar Anyconnect o sus componentes desde ISE.

Paso 15. El usuario ejecuta la aplicación NSA.

Paso 16. La NSA envía el primer sondeo de detección: HTTP /auth/discovery al gateway predeterminado. Como resultado, la NSA espera una URL de redirección.

Nota: Para conexiones sobre VPN en dispositivos MAC OS, esta sonda se ignora, ya que MAC OS no tiene un gateway predeterminado en el adaptador VPN.

Paso 17. NSA envía una segunda sonda si falla la primera. La segunda sonda es un HTTP GET /auth/discovery to enroll.cisco.com. El servidor DNS debe poder resolver este FQDN correctamente. En un escenario de VPN con un túnel dividido, el tráfico a enroll.cisco.com debe enrutarse a través del túnel.

Paso 18. Si alguno de los sondeos tiene éxito, la NSA establece una conexión SSL a través del puerto 8905 con información obtenida de redirect-url. Esta conexión está protegida por el certificado de administración de ISE. Dentro de esta conexión, la NSA descarga Anyconnect.

Consideraciones importantes:

- Antes de la versión ISE 2.2, la comunicación SSL a través del puerto 8905 era un requisito para el estado.
- Para evitar advertencias de certificado, los certificados de portal y de administrador deben ser de confianza en el cliente.
- En las implementaciones de ISE con varias interfaces, las interfaces que no sean G0 se pueden vincular al FQDN de forma distinta al FQDN del sistema (con el uso de ip host CLI). Esto puede causar problemas con la validación del nombre del sujeto (SN)/nombre alternativo del sujeto (SAN). Si el cliente se redirige a FQDN desde la interfaz G1, por ejemplo, el FQDN del sistema puede diferir del FQDN en la URL de redirección para el certificado de comunicación 8905. Como solución para este escenario, puede agregar FQDN de interfaces adicionales en los campos SAN del certificado de administración, o puede utilizar un comodín en el certificado de administración.

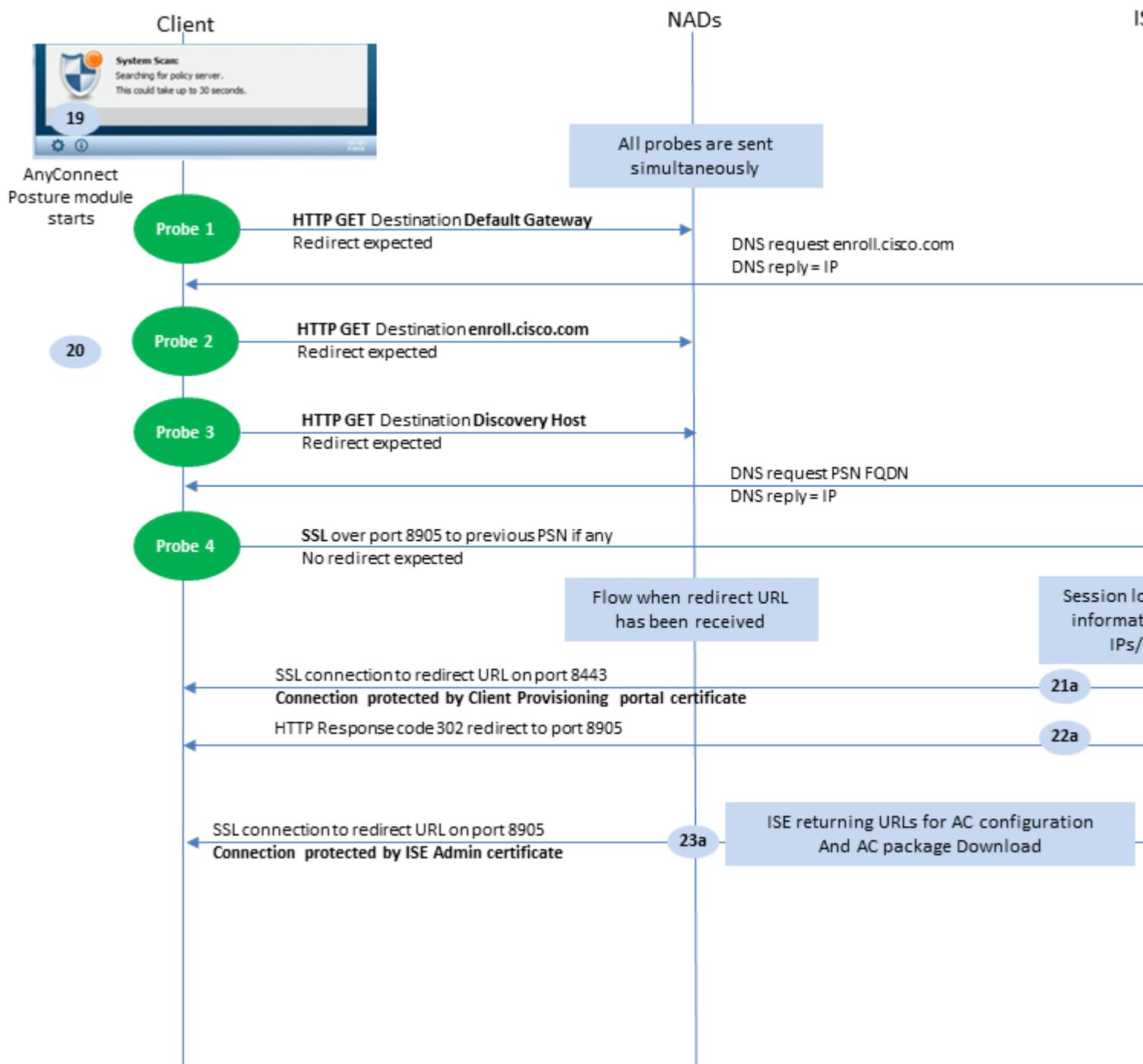


Figura 1-3

Paso 19. Se inicia el proceso de estado de Anyconnect ISE.

El módulo de estado de ISE de Anyconnect se inicia en cualquiera de estas situaciones:

- Después de la instalación
- Después de cambiar el valor predeterminado del gateway
- Después del evento de inicio de sesión del usuario del sistema
- Después del evento de alimentación del sistema

Paso 20. En esta etapa, Anyconnect ISE Posture Module inicia la detección del servidor de políticas. Esto se logra con una serie de sondas que se envían al mismo tiempo mediante el módulo Anyconnect ISE Posture.

- Sondeo 1: HTTP obtiene /auth/discovery a la IP de gateway predeterminada. Debe recordar que los dispositivos MAC OS no tienen un gateway predeterminado en el adaptador VPN. El resultado esperado para la sonda es redirect-url.
- Sondeo 2 - HTTP GET /auth/discovery to enroll.cisco.com. El servidor DNS debe poder resolver este FQDN correctamente. En un escenario de VPN con un túnel dividido, el tráfico a enroll.cisco.com debe enrutarse a través del túnel. El resultado esperado para la sonda es redirect-url.
- Sondeo 3: HTTP get /auth/discovery to discovery host. ISE devuelve el valor de host de detección durante la instalación en el perfil de estado de CA. El resultado esperado para la sonda es redirect-url.
- Sondeo 4: HTTP GET /auth/status over SSL en el puerto 8905 a PSN conectado anteriormente. Esta solicitud contiene información sobre la lista de direcciones IP y MAC del cliente para la búsqueda de sesiones en el lado de ISE. Este problema no se presenta durante el primer intento de postura. La conexión está protegida por un certificado de administrador de ISE. Como resultado de este sondeo, ISE puede devolver el ID de sesión al cliente si el nodo en el que aterrizó el sondeo es el mismo nodo en el que se ha autenticado al usuario.

Nota: Como resultado de esta sonda, la postura se puede realizar correctamente incluso sin redirección de trabajo en algunas circunstancias. El estado correcto sin redirección requiere que el PSN actual que autenticó la sesión sea el mismo que el PSN conectado correctamente anteriormente. Tenga en cuenta que, antes de ISE 2.2, una postura correcta sin redirección es más una excepción que una regla.

Los siguientes pasos describen el proceso de estado en el caso en que se recibe la URL de redirección (flujo marcado con la letra a) como resultado de uno de los sondeos.

Paso 21. El módulo de estado de ISE de Anyconnect establece una conexión con el portal de aprovisionamiento de clientes mediante el uso de una URL recuperada durante la fase de detección. En esta etapa, ISE realiza una validación de la política de aprovisionamiento de clientes una vez más con el uso de la información de las sesiones autenticadas.

Paso 2. Si se detecta una política de aprovisionamiento de clientes, ISE devuelve la redirección al puerto 8905.

Paso 23. El agente establece una conexión con ISE a través del puerto 8905. Durante esta conexión, ISE devuelve las URL del perfil de estado, el módulo de conformidad y las actualizaciones de AnyConnect.

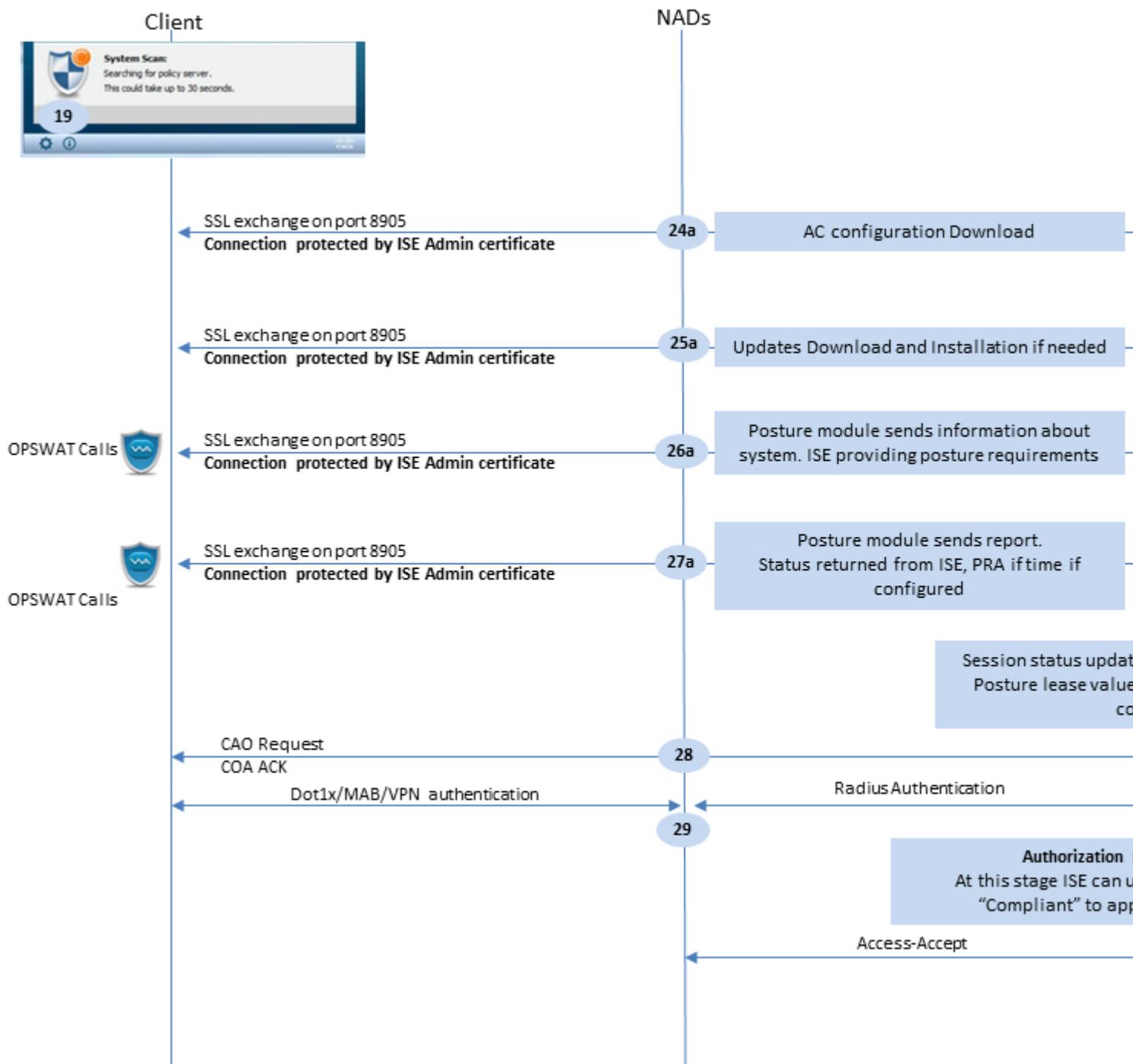


Figura 1-4

Paso 24. Descarga de la configuración del módulo de estado de ISE de ISE.

Paso 25. Descarga e instalación de actualizaciones si es necesario.

Paso 26. El módulo de estado de AC ISE recopila información inicial sobre el sistema (como la versión del sistema operativo, los productos de seguridad instalados y su versión de definición). En esta etapa, el módulo de estado de AC ISE incluye la API OPSWAT para recopilar información sobre los productos de seguridad. Los datos recopilados se envían a ISE. Como respuesta a esta solicitud, ISE proporciona una lista de requisitos de estado. La lista de requisitos se selecciona como resultado del procesamiento de la política de estado. Para que coincida con la política correcta, ISE utiliza la versión del sistema operativo del dispositivo (presente en la solicitud) y el valor de ID de sesión para seleccionar otros atributos necesarios (grupos AD/LDAP). El valor de ID de sesión también lo envía el cliente.

Paso 27. En este paso, el cliente incluye llamadas OPSWAT y otros mecanismos para comprobar los requisitos de estado. El informe final con la lista de requisitos y su estado se envía a ISE. ISE debe tomar la decisión final sobre el estado de cumplimiento de los terminales. Si el terminal se marca como no conforme en este paso, se devuelve un conjunto de acciones de remediación. Para el terminal que cumple las normas, ISE escribe el estado de conformidad en la sesión y también coloca la marca de tiempo de la última postura en los atributos del terminal si se configura la concesión de condición. El resultado de la postura se devuelve al punto final. En el caso de la reevaluación de posición (PRA), ISE también introduce el tiempo para la PRA en este paquete.

En un escenario de incumplimiento, tenga en cuenta los siguientes puntos:

- El propio agente de estado ejecuta algunas acciones de corrección (como mostrar mensajes de texto, remediación de vínculos, remediación de archivos, etc.).
- Otros tipos de remediación (como AV, AS, WSUS y SCCM) requieren la comunicación de la API OPSWAT entre el agente de estado y el producto de destino. En esta situación, el agente de estado simplemente envía una solicitud de remediación al producto. Los productos de seguridad llevan a cabo la remediación directamente.

Nota: En caso de que el producto de seguridad tenga que comunicarse con recursos externos (servidores de actualización internos/externos), debe asegurarse de que esta comunicación esté permitida en Redirect-ACL/DACL.

Paso 28. ISE envía una solicitud de COA al NAD, que debe activar una nueva autenticación para el usuario. NAD debe confirmar esta solicitud mediante COA ACK. Tenga en cuenta que para los casos de VPN se utiliza el comando COA push, por lo que no se envía una nueva solicitud de autenticación. En su lugar, ASA elimina los parámetros de autorización anteriores (redirección de URL, redirección de ACL y DACL) de la sesión y aplica los nuevos parámetros de la solicitud COA.

Paso 29. Nueva solicitud de autenticación para el usuario.

Consideraciones importantes:

- Normalmente, para Cisco NAD COA, ISE utiliza reauth, lo que indica a NAD que inicie una nueva solicitud de autenticación con el ID de sesión anterior.
- En el lado de ISE, el mismo valor de ID de sesión es una indicación de que los atributos de sesión recopilados anteriormente se deben reutilizar (estado de queja en nuestro caso) y se debe asignar un nuevo perfil de autorización basado en esos atributos.
- En caso de un cambio de ID de sesión, esta conexión se trata como nueva y se reinicia el proceso de estado completo.
- Para evitar la recaída en cada cambio de id. de sesión, se puede utilizar un arrendamiento de estado. En esta situación, la información sobre el estado se almacena en los atributos del terminal que permanece en ISE incluso si se activa la ID de sesión. Se ha cambiado.

Paso 30. Se selecciona una nueva política de autorización en el lado de ISE en función del estado.

Paso 31. Access-Accept con los nuevos atributos de autorización se envía al NAD.

El siguiente flujo describe el escenario en el que la URL de redirección no se recupera (marcada con la letra b) mediante ningún sondeo de estado y el PSN conectado anteriormente ha sido consultado por el último sondeo. Todos los pasos aquí son exactamente los mismos que en el caso de la URL de redirección, excepto la reproducción que devuelve PSN como resultado de la sonda 4. Si esta sonda aterrizó en el mismo PSN que es propietario de la sesión de autenticación actual, la reproducción contiene el valor de ID de sesión que

posteriormente utiliza el agente de estado para finalizar el proceso. En caso de que la cabecera conectada anteriormente no sea la misma que la del propietario de la sesión actual, la búsqueda de sesión falla y se devuelve una respuesta vacía al módulo de estado de AC ISE. Como resultado final de esto, el No Policy Server Detected se devuelve al usuario final.

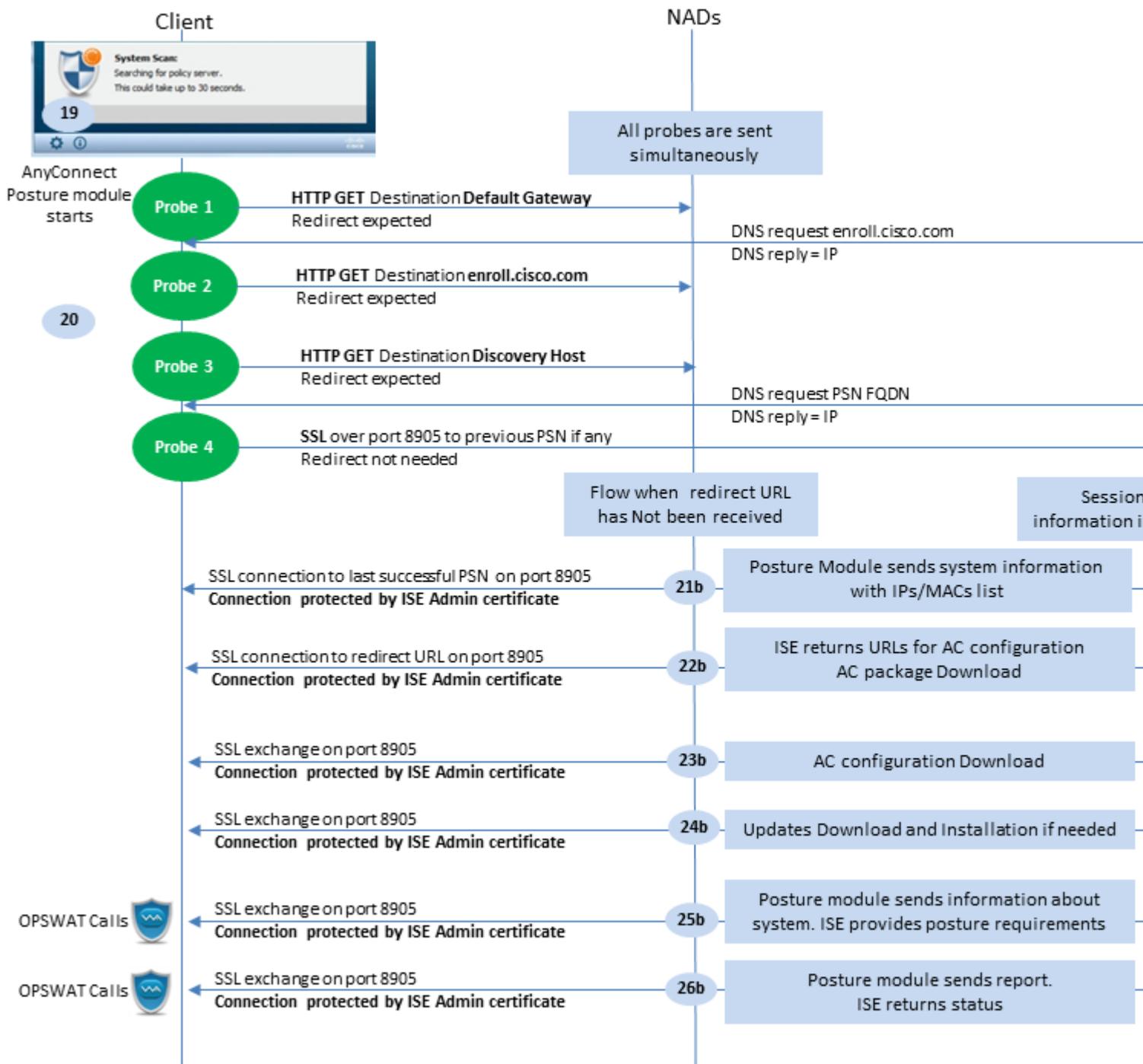


Figura 1-5

Flujo de estado posterior a ISE 2.2

ISE 2.2 y las versiones más recientes admiten flujos de redirección y sin redirección de forma

simultánea. Esta es la explicación detallada para el flujo de postura sin redirección:

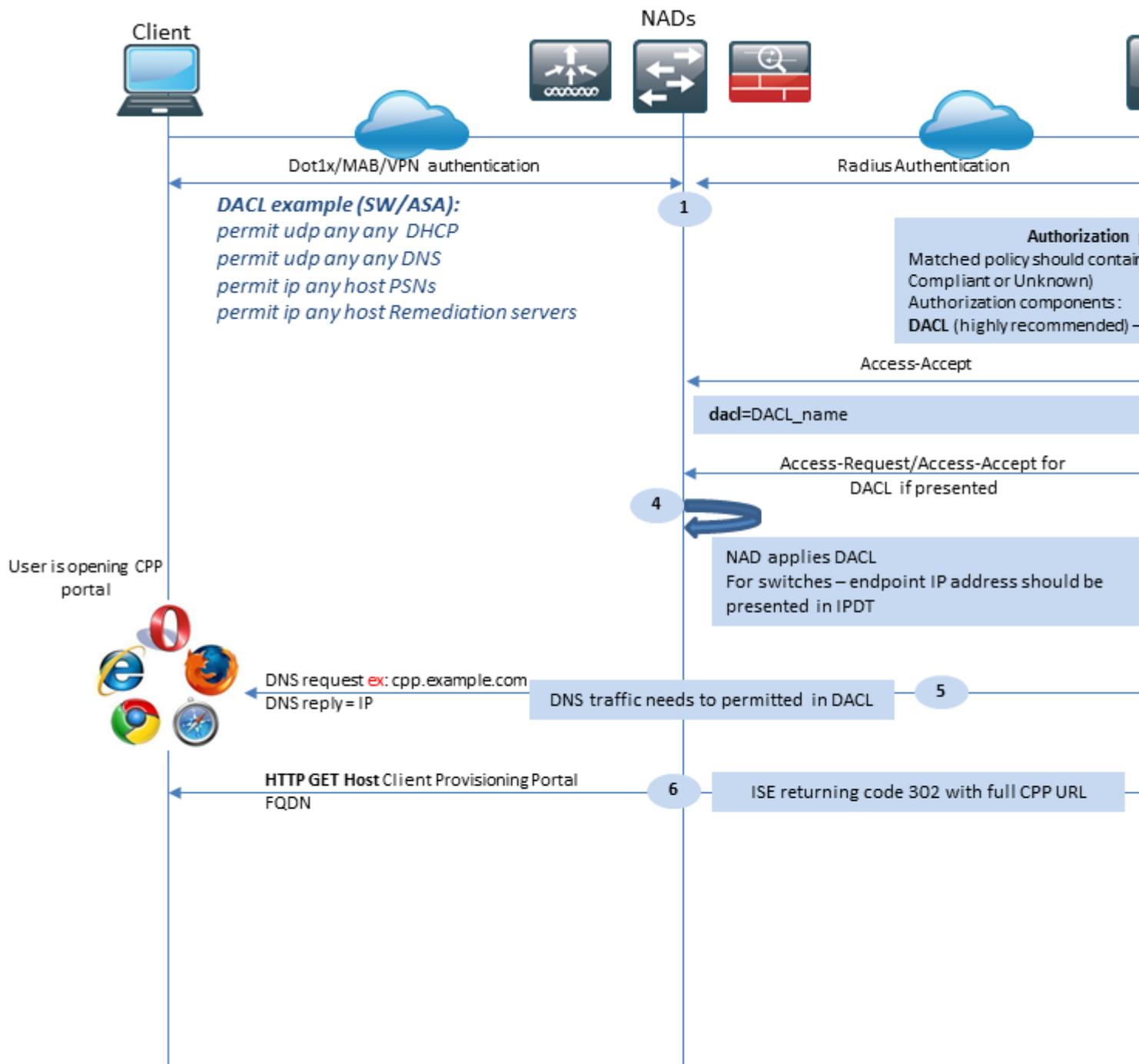


Figura 2-1

Paso 1. La autenticación es el primer paso del flujo. Puede ser dot1x, MAB o VPN.

Paso 2. ISE debe elegir la política de autenticación y autorización para el usuario. En estado, el escenario elegido para la directiva de autorización debe contener una referencia al estado del estado, que inicialmente debe ser desconocido o no aplicable. Para cubrir ambos casos, se pueden utilizar condiciones con estado de condición y cumplimiento desigual. Para un estado sin redirección, no es necesario utilizar ninguna configuración de redirección web en el perfil de autorización. Puede seguir considerando el uso de una DACL o una ACL del espacio aéreo para limitar el acceso de los usuarios en la etapa en la que el estado no está disponible.

El paso 3. ISE devuelve Access-Accept con atributos de autorización.

Paso 4. Si el nombre de DACL se devuelve en Access-Accept, NAD inicia la descarga de contenido de DACL y aplica el perfil de autorización a la sesión después de que se haya obtenido.

Paso 5. El nuevo enfoque supone que la redirección no es posible, por lo que el usuario debe introducir el FQDN del portal de aprovisionamiento de clientes manualmente. El FQDN del portal CPP debe definirse en la configuración del portal en el lado de ISE. Desde la perspectiva del servidor DNS, el registro A debe señalar al servidor ISE con la función PSN habilitada.

Paso 6. El cliente envía HTTP para obtener el FQDN del portal de aprovisionamiento de clientes, esta solicitud se analiza en el lado de ISE y la URL completa del portal se devuelve al cliente.

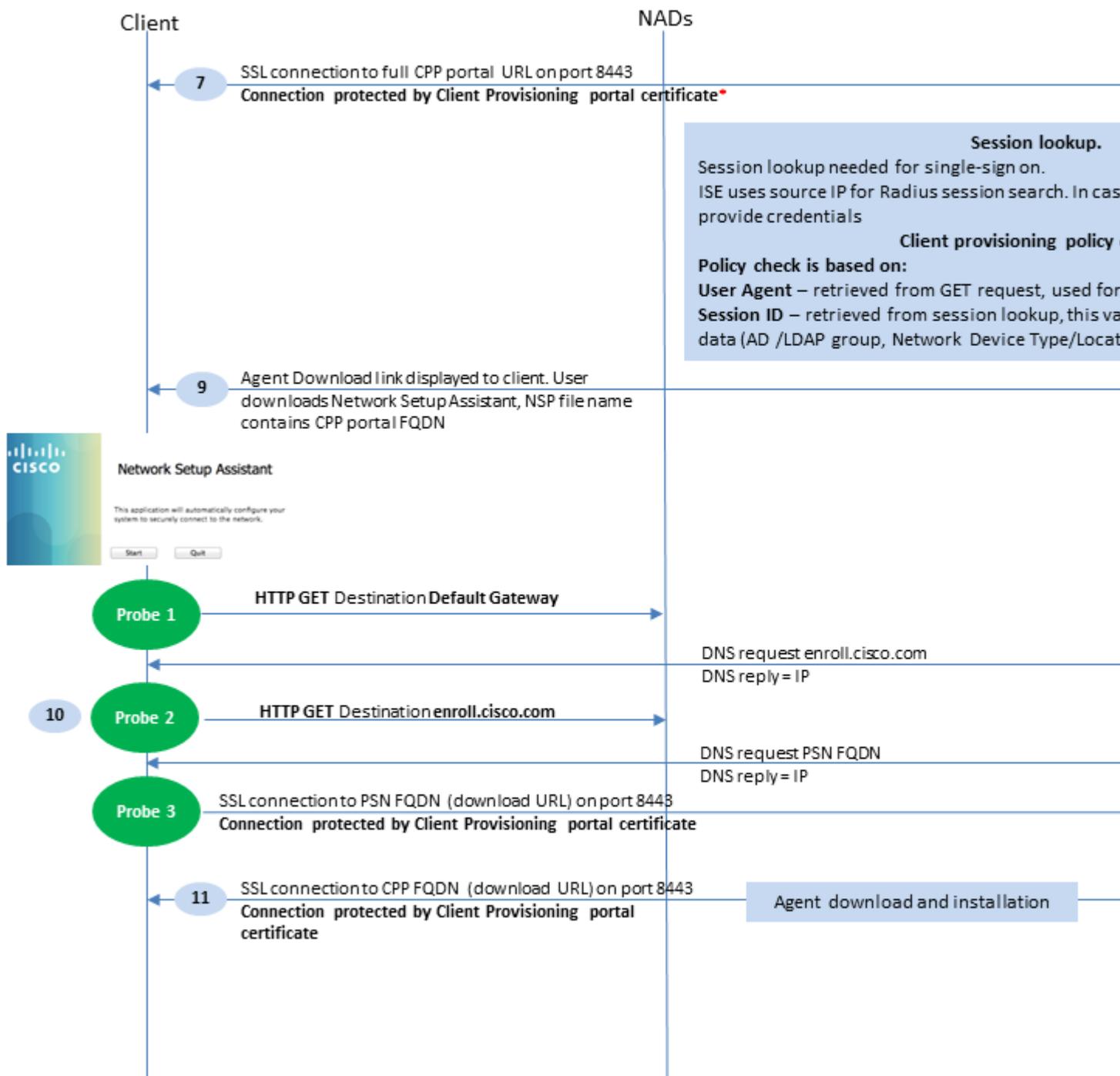


Figura 2-2

Se establece la conexión 7.SSL a través del puerto recibido en la URL de redirección (el valor predeterminado es 8443). Esta conexión está protegida por un certificado de portal del lado de ISE. El portal de aprovisionamiento de clientes (CPP) se presenta al usuario.

Paso 8. En este paso se producen dos eventos en ISE:

- Inicio de sesión único (SSO): ISE intenta buscar una autenticación anterior correcta. ISE utiliza la dirección IP de origen del paquete como filtro de búsqueda para las sesiones de radio en directo.

Nota: La sesión se recupera en función de una coincidencia entre la IP de origen en el paquete y la dirección IP entramada en la sesión. ISE recupera normalmente la dirección IP con trama a partir de las actualizaciones de cuentas provisionales, por lo que es necesario tener la contabilidad habilitada en el lado NAD. Además, debe recordar que SSO sólo es posible en el nodo que posee la sesión. Si, por ejemplo, la sesión se autentica en PSN 1, pero el FQDN en sí apunta a PSN2, el mecanismo SSO falla.

- Búsqueda de políticas de aprovisionamiento de clientes: en caso de un SSO correcto, ISE puede utilizar datos de la sesión autenticada y el agente de usuario del navegador del cliente. En caso de un SSO fallido, el usuario debe proporcionar credenciales y después de que la información de autenticación de usuario se recupere de los almacenes de identidad internos y externos (grupos AD/LDAP/Internal), se puede utilizar para la comprobación de políticas de aprovisionamiento de clientes.

Nota: debido al Id. de error de Cisco [CSCvd1574](#), puede ver un error en el momento de la selección de la política de aprovisionamiento del cliente para los casos que no son de SSO cuando el usuario externo es miembro de varios grupos AD/LDAP agregados en la configuración del almacén de identidades externas. El defecto mencionado se corrige a partir de ISE 2.3 FCS y la corrección requiere el uso de CONTAINS en condiciones con el grupo AD en lugar de EQUAL.

Paso 9. Después de seleccionar la política de aprovisionamiento de clientes, ISE muestra la URL de descarga del agente al usuario. Después de hacer clic en Descargar NSA, la aplicación se envía al usuario. El nombre de archivo de la NSA contiene el FQDN del portal CPP.

Paso 10. En este paso, la NSA ejecuta sondeos para establecer una conexión con ISE. Dos sondeos son clásicos y el tercero está diseñado para permitir la detección de ISE en entornos sin redirección de URL.

- La NSA envía el primer sondeo de detección: HTTP /auth/discovery al gateway predeterminado. Como resultado, la NSA espera una URL de redirección.
- La NSA envía una segunda sonda si falla la primera. La segunda sonda es un HTTP GET /auth/discovery to enroll.cisco.com. El servidor DNS debe poder resolver este FQDN correctamente. En un escenario de VPN con un túnel dividido, el tráfico a enroll.cisco.com debe enrutarse a través del túnel.
- La NSA envía la tercera sonda a través del puerto del portal CPP al FQDN del portal de aprovisionamiento de clientes. Esta solicitud contiene información sobre la ID de sesión del portal, que permite a ISE identificar qué recursos deben proporcionarse.

Paso 11. La NSA descarga Anyconnect y/o módulos específicos. El proceso de descarga se realiza a través del puerto del portal de aprovisionamiento de clientes.

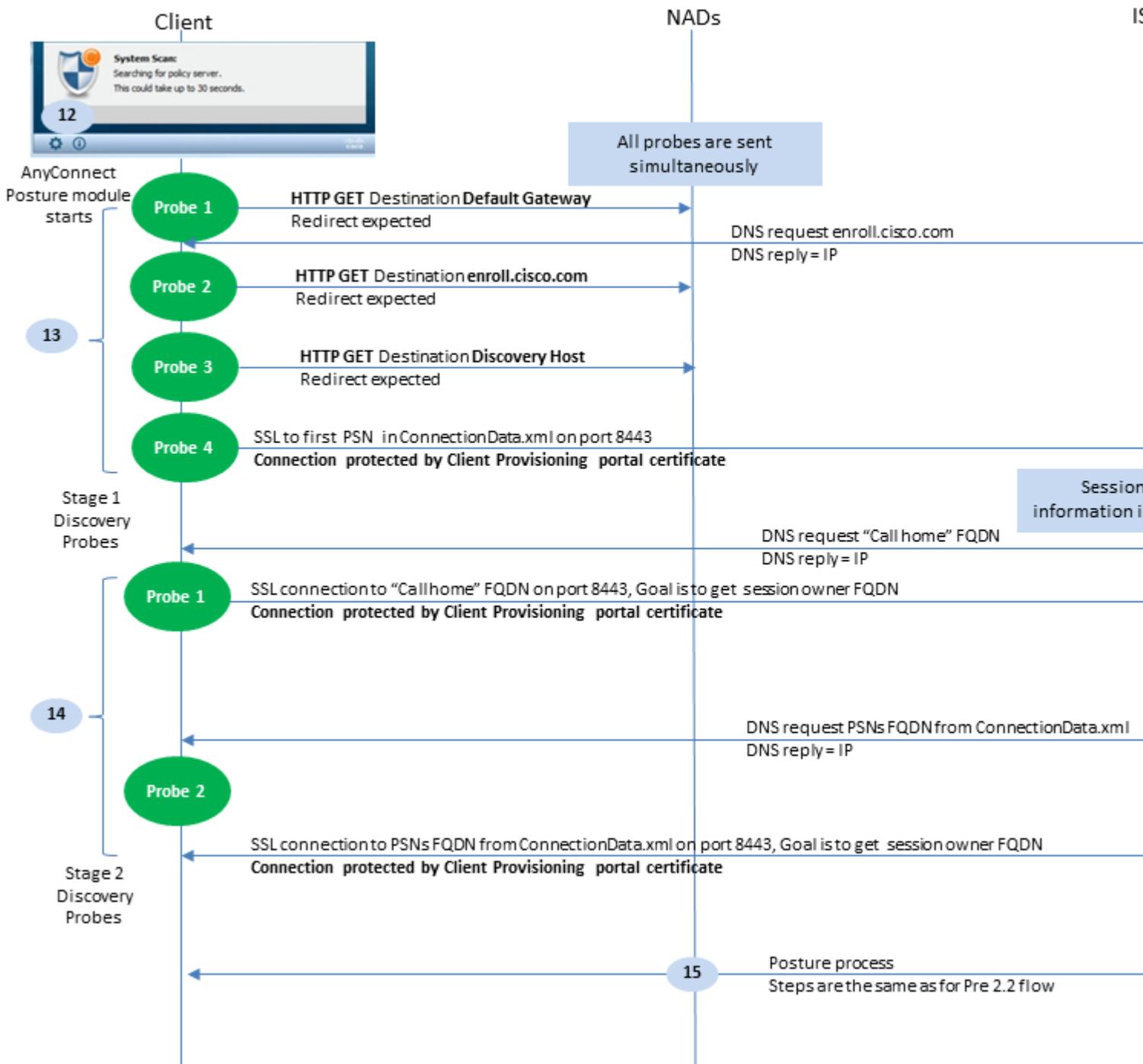


Figura 2-3

Paso 12. En ISE 2.2, el proceso de estado se divide en dos etapas. La primera etapa contiene un conjunto de sondeos de detección de estado tradicionales para admitir la compatibilidad con versiones anteriores con implementaciones que se basan en la redirección de url.

Paso 13. La primera etapa contiene todas las sondas de detección de postura tradicionales. Para obtener más información sobre las sondas, revise el paso 20 del flujo de estado anterior a ISE 2.2.

La etapa 14.2 contiene dos sondas de detección que permiten al módulo de estado de AC ISE establecer una conexión con PSN donde la sesión se autentica en entornos donde no se admite la redirección. Durante la etapa dos, todas las sondas son secuenciales.

- Sondeo 1: durante el primer sondeo, el módulo de estado de AC ISE intenta establecer con IP/FQDN

de la lista de inicio de llamada. Se debe configurar una lista de los objetivos para la sonda en el perfil de estado de CA en el lado de ISE. Puede definir IP/FQDN separados por comas; con dos puntos puede definir el número de puerto para cada destino de Call Home. Este puerto debe ser igual al puerto en el que se ejecuta el portal de aprovisionamiento de clientes. En el lado del cliente, la información sobre los servidores de inicio de llamadas se encuentra en ISEPostureCFG.xml, este archivo se puede encontrar en la carpeta - C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture\.

En caso de que el destino de la casa de llamada no sea el propietario de la sesión, se necesita una búsqueda para el propietario en esta etapa. El módulo de estado de AC ISE ordena a ISE que inicie la búsqueda del propietario con el uso de una URL de destino especial: /auth/ng-discovery petición. También contiene la lista de direcciones IP y MAC del cliente. Después de que la sesión PSN reciba este mensaje, primero se realiza una búsqueda local (esta búsqueda utiliza IP y MAC a partir de la solicitud enviada por el módulo de estado de AC ISE). Si no se encuentra la sesión, PSN inicia una consulta de nodo MNT. Esta solicitud contiene solo la lista de MAC, por lo tanto, el FQDN del propietario debe obtenerse del MNT. Después de esto, PSN devuelve el FQDN de los propietarios al cliente. La siguiente solicitud del cliente se envía al FQDN del propietario de la sesión con autenticación/estado en la URL y la lista de IP y MAC.

- Sondeo 2: en esta etapa, el módulo de estado de AC ISE prueba FQDN de PSN que se encuentran en ConnectionData.xml. Puede encontrar este archivo en C:\Users\

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

. El módulo de postura de AC ISE crea este archivo después del primer intento de postura. El archivo contiene una lista de FQDN de ISE PSN. El contenido de la lista se puede actualizar dinámicamente durante los siguientes intentos de conexión. El objetivo final de este sondeo es obtener el FQDN del propietario de la sesión actual. La implementación es idéntica a la de la sonda 1, con la única diferencia en la selección del destino de la sonda.

El archivo en sí se encuentra en la carpeta del usuario actual en caso de que el dispositivo sea utilizado por varios usuarios. Otro usuario no puede utilizar la información de este archivo. Esto puede llevar a los usuarios al problema del huevo y la gallina en entornos sin redirección cuando no se especifican los objetivos de Call home.

Paso 15. Una vez obtenida la información sobre el propietario de la sesión, todos los pasos siguientes son idénticos al flujo anterior a ISE 2.2.

Configurar

Para este documento, ASAv se utiliza como un dispositivo de acceso a la red. Todas las pruebas se realizan con postura sobre VPN. La configuración de ASA para el soporte de postura sobre VPN está fuera del alcance del documento. Para obtener más detalles, refiérase al [Ejemplo de Configuración de la Postura VPN de ASA Versión 9.2.1 con ISE](#).

Nota: para la implementación con usuarios de VPN, la configuración recomendada es el estado basado en la redirección. No se recomienda la configuración de callhomelist. Para todos los usuarios no basados en vpn, asegúrese de que la DACL se aplica de modo que no se comuniquen con PSN donde se ha configurado el estado.

Diagrama de la red

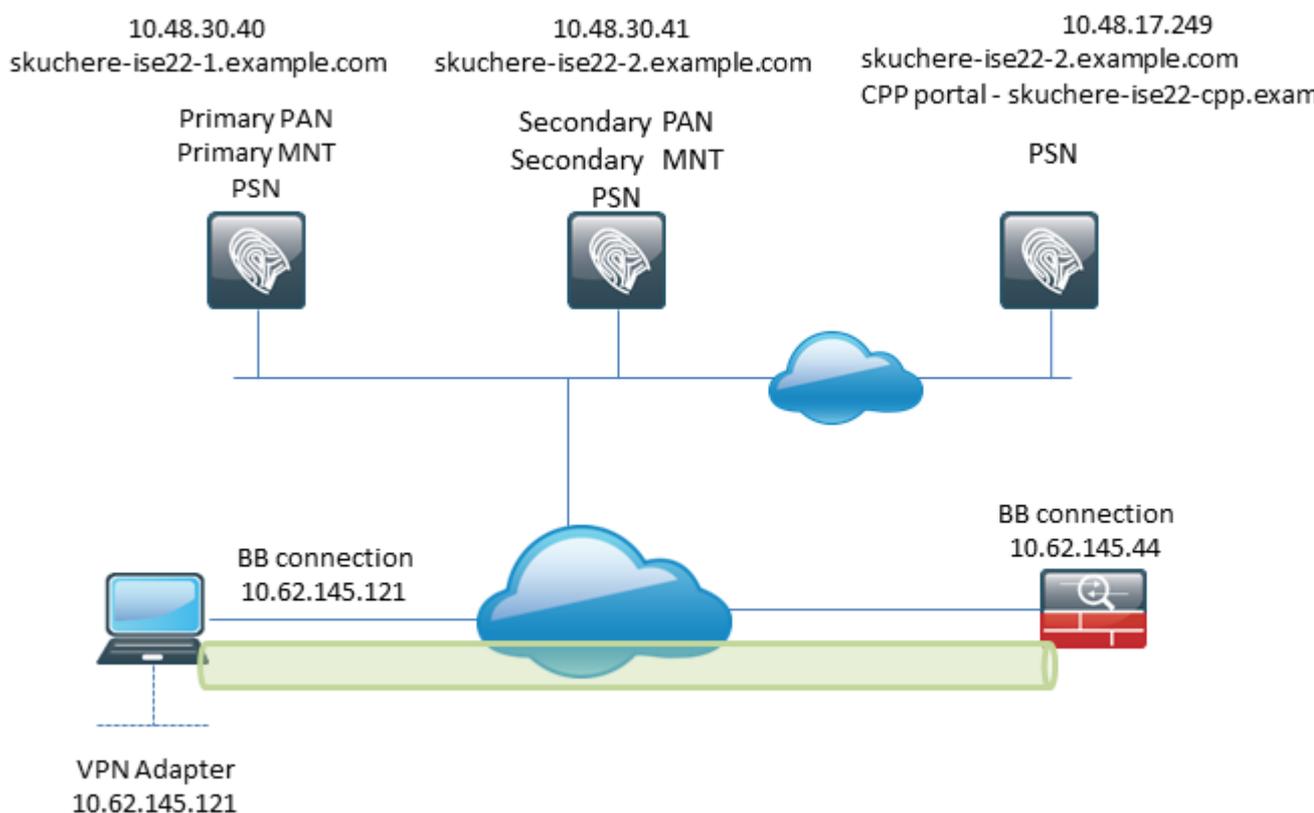


Figura 3-1

Esta topología se utiliza en pruebas. Con ASA, es posible simular fácilmente el escenario cuando el mecanismo SSO para el portal de aprovisionamiento de clientes falla en el lado PSN, debido a la función NAT. En el caso de un flujo de estado regular a través de VPN, SSO debe funcionar correctamente, ya que NAT no se aplica normalmente para las IP de VPN cuando los usuarios entran en la red corporativa.

Configuraciones

Configuración de aprovisionamiento de clientes

Estos son los pasos para preparar la configuración de Anyconnect.

Paso 1. Descarga del paquete Anyconnect. El paquete Anyconnect en sí no está disponible para su descarga directa desde ISE, por lo que antes de comenzar, asegúrese de que AC esté disponible en su PC. Este enlace se puede utilizar para la descarga de CA: <https://www.cisco.com/site/us/en/products/security/secure-client/index.html>. En este documento, anyconnect-win-4.4.00243-webdeploy-k9.pkg se utiliza el paquete.

Paso 2. Para cargar el paquete de CA en ISE, vaya a Policy > Policy Elements > Results > Client Provisioning > Resources y haga clic en Add. Seleccione Recursos de agente en el disco local. En la nueva ventana, seleccione Cisco Provided Packages, haga clic en browse y elija el paquete AC en su PC.

Agent Resources From Local Disk

Category ⓘ

anyconnect-win-4.4.00243-webdeploy-k9.pkg

▼ **AnyConnect Uploaded Resources**

Name	Type	Version	Description
AnyConnectDesktopWindows 4.4.24...	AnyConnectDesktopWindows	4.4.243.0	AnyConn...

Figura 3-2

Haga clic en **Submit** para finalizar la importación.

Paso 3. El módulo de conformidad debe cargarse en ISE. En la misma página, haga clic en **Add** y seleccione la **Agent resources from Cisco site**. En la lista de recursos, debe comprobar un módulo de conformidad. Para este documento, el **AnyConnectComplianceModuleWindows 4.2.508.0** se utiliza el módulo de conformidad.

Paso 4. Ahora se debe crear un perfil de postura AC. Haga clic en **Add** y seleccione la **NAC agent or Anyconnect posture profile**.

Posture Agent Profile Settings

a.

* Name: **b.**

Description:

Agent Behavior

Figura 3-3

- Elija el tipo de perfil. Se debe utilizar AnyConnect para este escenario.
- Especifique el nombre del perfil. Desplácese hasta el Posture Protocol del perfil.

Posture Protocol

Parameter	Value	Notes
PRA retransmission time	<input type="text" value="120"/> secs	
Discovery host	<input type="text"/>	
* Server name rules	<input type="text" value="*"/> a.	need to be blank by default to force agent to enter a value. "*" means agent will connect to all
Call Home List	<input type="text" value="skuchere-ise22-2.examp"/> b.	List of IP addresses, FQDNs with or without port must be comma-separated and without 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	<input type="text" value="30"/> secs	Enter value of back-off timer in seconds. supported range is between 10s - 600s

Figura 3-4

- Especifique el Server Name Rules, este campo no puede estar vacío. El campo puede contener FQDN con comodín que restringe la conexión del módulo de estado de AC ISE a PSN desde el espacio de nombres adecuado. Coloque una estrella si se debe permitir cualquier FQDN.
- Los nombres y direcciones IP especificados aquí están en uso durante la etapa 2 del descubrimiento de estado. Puede separar los nombres por coma, así como los números de puerto que se pueden agregar después de FQDN/IP con el uso de dos puntos. En caso de que el AC implementado fuera de banda (no desde el portal de aprovisionamiento de clientes de ISE) con el uso del GPO o cualquier otro sistema de aprovisionamiento de software, la presencia de direcciones de Call Home se convierte en esencial, ya que este es solo un sondeo que puede alcanzar ISE PSN correctamente. Esto significa que, en el caso del aprovisionamiento de CA fuera de banda, el administrador debe crear un perfil de estado de AC ISE con el uso del editor de perfiles de AC y aprovisionar este archivo junto con la instalación de AC.

Nota: tenga en cuenta que la presencia de direcciones de inicio de llamadas es fundamental para los PC multiusuario. Revise el paso 14. en Flujo de estado posterior a ISE 2.2.

Paso 5. Crear configuración de CA. Desplácese hasta Policy > Policy Elements > Results > Client Provisioning > Resources, clic Add, luego elija AnyConnect Configuration.

* Select AnyConnect Package: AnyConnectDesktopWindows 4.4.243.0 **a.**

* Configuration Name: AC-44-CCO **b.**

Description:

DescriptionValue **Notes**

* Compliance Module: AnyConnectComplianceModuleWindows 4.2.508.0 **c.**

AnyConnect Module Selection

- ISE Posture
- VPN
- Network Access Manager
- Web Security
- AMP Enabler
- ASA Posture
- Network Visibility
- Umbrella Roaming Security
- Start Before Logon
- Diagnostic and Reporting Tool

Profile Selection

* ISE Posture: AC-44-Posture **d.**

Figura 3-5

- Elija el paquete AC.
- Proporcione el nombre de la configuración de CA.
- Elija la versión del módulo de conformidad.
- Elija el perfil de configuración de postura de CA en la lista desplegable.

Paso 6. Configure la política de aprovisionamiento de clientes. Desplácese hasta Policy > Client Provisioning. En el caso de la configuración inicial, puede rellenar los valores vacíos en la política presentada con los valores predeterminados. Si necesita agregar una política a la configuración de estado que existe, navegue hasta la política que se puede reutilizar y elija Duplicate Above Or Duplicate Below . También se puede crear una política completamente nueva.

Este es un ejemplo de la política utilizada en el documento.

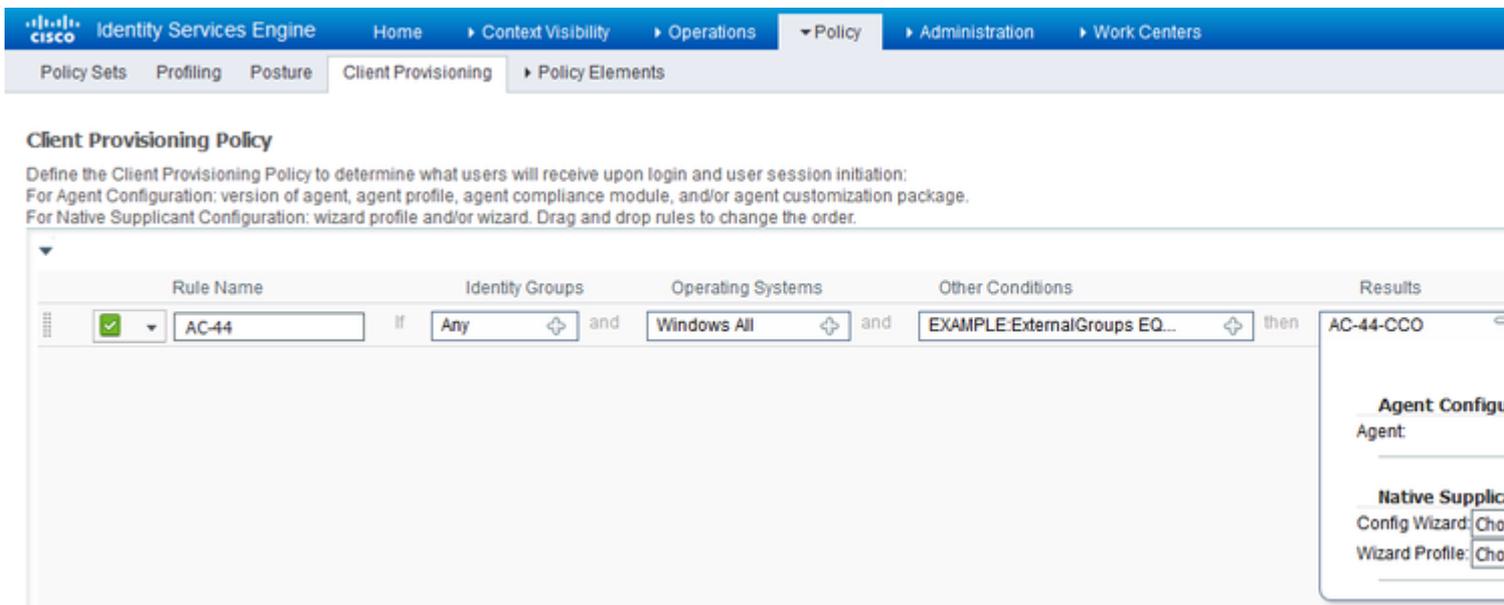


Figura 3-6

Elija su configuración de CA en la sección de resultados. Tenga en cuenta que, en caso de fallo de SSO, ISE solo puede tener atributos desde el inicio de sesión al portal. Estos atributos se limitan a la información que se puede recuperar acerca de los usuarios de almacenes de identidades internos y externos. En este documento, el grupo de AD se utiliza como condición en la política de aprovisionamiento de clientes.

Políticas y condiciones de estado

Se utiliza una simple comprobación de postura. ISE se configura para comprobar el estado del servicio de Windows Defender en el lado del dispositivo final. Los escenarios de la vida real pueden ser mucho más complicados, pero los pasos generales de configuración son los mismos.

Paso 1. Crear condición de postura. Las condiciones de postura se encuentran en Policy > Policy Elements > Conditions > Posture. Elija el tipo de condición de postura. Este es un ejemplo de una condición de servicio que debe comprobar si el servicio de Windows Defender se está ejecutando.

[Service Conditions List > WinDefend](#)

Service Condition

* Name

Description

* Operating Systems +

Compliance Module

* Service Name

Service Operator

Figura 3-7

Paso 2. Configuración de los requisitos de estado. Desplácese hasta **Policy > Policy Elements > Results > Posture > Requirements**. Este es un ejemplo de una verificación de Windows Defender:

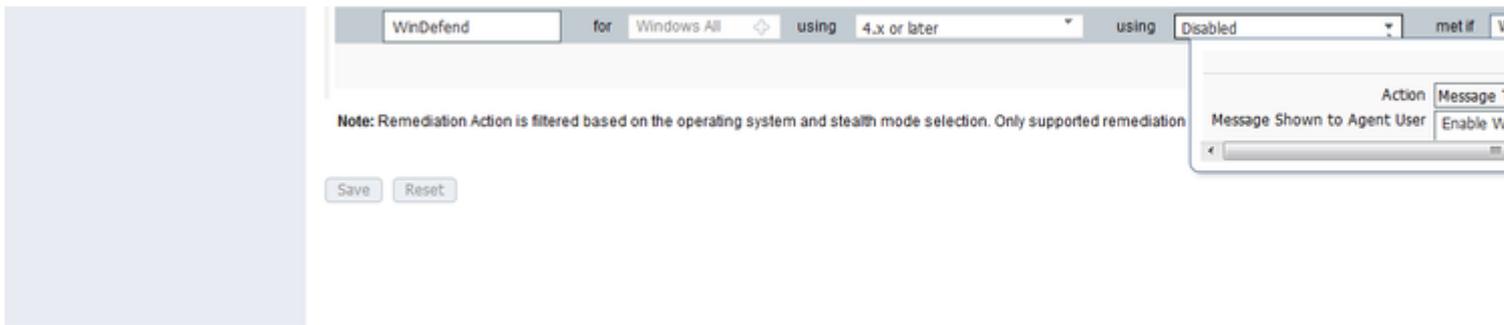


Figura 3-8

Elija su condición de estado en el nuevo requisito y especifique la acción de remediación.

Paso 3. Configuración de la política de estado. Desplácese hasta **Policy > Posture**. Aquí puede encontrar un ejemplo de la política utilizada para este documento. La directiva tiene el requisito de Windows Defender asignado como obligatorio y solo contiene el nombre de grupo de AD externo como condición.

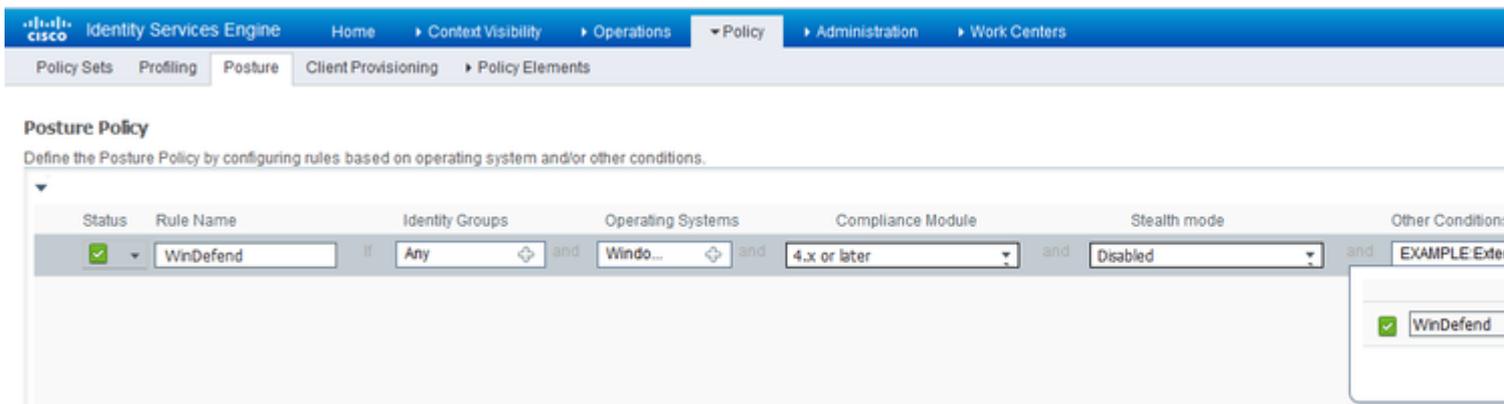


Figura 3-9

Configuración de Client Provisioning Portal

Para el estado sin redirección, se debe editar la configuración del portal de aprovisionamiento de clientes. Desplácese hasta **Administration > Device Portal Management > Client Provisioning**. Puede utilizar el portal predeterminado o crear el suyo propio. El mismo portal se puede utilizar para ambas posturas con y sin redirección.

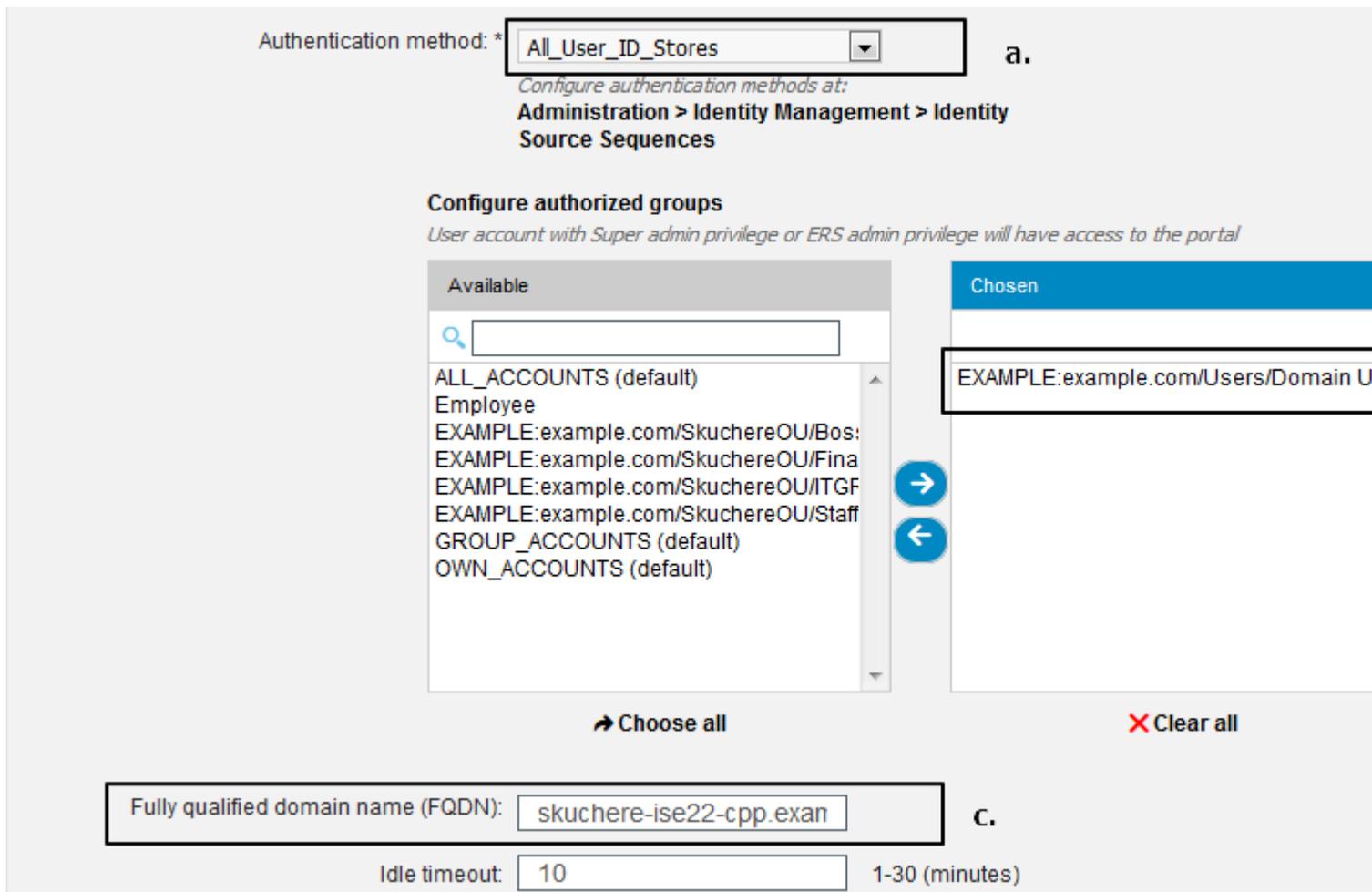


Figura 3-10

Estas configuraciones se deben editar en la configuración del portal para el escenario de no redirección:

- En Autenticación, especifique la secuencia de origen de identidad que se debe utilizar si SSO no puede localizar una sesión para el usuario.
- Según la secuencia de origen de identidad seleccionada, se rellena la lista de grupos disponibles. En este momento, debe seleccionar los grupos que están autorizados para el inicio de sesión en el portal.
- Se debe especificar el FQDN del portal de aprovisionamiento de clientes para los escenarios en los que debe implementarse AC desde el portal de aprovisionamiento de clientes. Este FQDN debe poder resolverse en direcciones IP de PSN de ISE. Se debe indicar a los usuarios que especifiquen el FQDN en el explorador web durante el primer intento de conexión.

Configurar perfiles y directivas de autorización

Se debe restringir el acceso inicial para los clientes cuando el estado de postura no está disponible. Esto se puede lograr de varias maneras:

- Asignación de DACL: durante la fase de acceso restringido, se puede asignar DACL al usuario para limitar el acceso. Este enfoque se puede utilizar para los dispositivos de acceso a la red de Cisco.
- Asignación de VLAN: antes de que los usuarios con un estado satisfactorio puedan entrar en una VLAN restringida, este enfoque debe funcionar correctamente para casi cualquier proveedor de NAD.
- Radius Filter-Id: con este atributo, la ACL definida localmente en NAD se puede asignar al usuario con un estado desconocido. Dado que se trata de un atributo RFC estándar, este enfoque debe funcionar bien para todos los proveedores de NAD.

Paso 1. Configuración de DACL. Dado que este ejemplo se basa en ASA, se puede utilizar una DACL NAD. Para escenarios de la vida real, debe considerar VLAN o ID de filtro como posibles opciones.

Para crear una DACL, navegue hasta `Policy > Policy Elements > Results > Authorization > Downloadable ACLs` haga clic en `Add`.

Durante el estado desconocido, se deben proporcionar al menos estos permisos:

- Tráfico DNS
- tráfico DHCP
- Tráfico a ISE PSN (puertos 80 y 443) para una posibilidad de abrir FQDN descriptivos del portal. El puerto en el que se ejecuta el portal CP es 8443 de forma predeterminada y el puerto 8905 para compatibilidad con versiones anteriores)
- Tráfico a servidores de corrección si es necesario

Este es un ejemplo de DACL sin servidores de corrección:

[Downloadable ACL List](#) > [New Downloadable ACL](#)

Downloadable ACL

* Name

Description

* DACL Content

1	permit udp any any eq 53
2	permit udp any any eq bootps
3	permit tcp any host 10.48.30.40 eq 80
4	permit tcp any host 10.48.30.40 eq 443
5	permit tcp any host 10.48.30.40 eq 8443
6	permit tcp any host 10.48.30.40 eq 8905
7	permit tcp any host 10.48.30.41 eq 80
8	permit tcp any host 10.48.30.41 eq 443
9	permit tcp any host 10.48.30.41 eq 8443
10	permit tcp any host 10.48.30.41 eq 8905

▶ [Check DACL Syntax](#)

Figura 3-11

Paso 2. Configure el perfil de autorización.

Como es habitual para el estado, se requieren dos perfiles de autorización. El primero debe contener cualquier tipo de restricciones de acceso a la red (perfil con DACL utilizado en este ejemplo). Este perfil se puede aplicar a las autenticaciones para las que el estado de estado no es igual a compatible. El segundo perfil de autorización solo puede contener permiso de acceso y se puede aplicar a sesiones con un estado igual a cumplimiento.

Para crear un perfil de autorización, vaya a `Policy > Policy Elements > Results > Authorization > Authorization Profiles`.

Ejemplo del perfil de acceso restringido:

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

▼ **Common Tasks**

DACL Name

Figura 3-12

En este ejemplo, el perfil predeterminado de ISE PermitAccess se utiliza para la sesión después de una comprobación de estado correcta.

Paso 3. Configure la directiva de autorización. Durante este paso, se deben crear dos directivas de autorización. Una es hacer coincidir la solicitud de autenticación inicial con el estado desconocido y la segunda es asignar acceso completo después de un proceso de estado exitoso.

Este es un ejemplo de políticas de autorización simples para este caso:

▼ **Authorization Policy**

► **Exceptions (0)**

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Posture-Compliant	if (Session:PostureStatus EQUALS Compliant AND EXAMPLE:ExternalGroups EQUALS example.com/Users/Domain Users)	then PermitAccess
<input checked="" type="checkbox"/>	Posture-Unknown-No-Redirect	if (Session:PostureStatus NOT_EQUALS Compliant AND EXAMPLE:ExternalGroups EQUALS example.com/Users/Domain Users)	then VPN-No-Redirect-Unknown
<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAccess

Figura 3-13

La configuración de la política de autenticación no forma parte de este documento, pero debe tener en

cuenta que antes de que la política de autorización procese correctamente la autenticación debe suceder.

Verificación

La verificación básica del flujo puede consistir en tres pasos principales:

Paso 1. Verificación del flujo de autenticación.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...
Feb 23, 2017 06:00:07.028 PM	✓				10.62.145.95			
Feb 23, 2017 06:00:07.028 PM	✓		e.		10.62.145.95			
Feb 23, 2017 06:00:04.368 PM	ⓘ		0	d. user1	00:0B:7F:D0:F8:F4	Windows7-...	VPN-LAB >>...	VPN-LAB >>...
Feb 23, 2017 05:59:04.750 PM	✓		c.	user1				
Feb 23, 2017 05:44:57.921 PM	✓		b.	#ACSACL#IP-VPN-No-Redi...				
Feb 23, 2017 05:44:57.680 PM	✓		a.	user1	00:0B:7F:D0:F8:F4	Windows7-...	VPN-LAB >>...	VPN-LAB >>...

Figura 4-1

1. Autenticación inicial. En este paso, puede estar interesado en la validación a la que se ha aplicado el perfil de autorización. Si se ha aplicado un perfil de autorización inesperado, investigue un informe de autenticación detallado. Puede abrir este informe haciendo clic en la lupa de la columna Detalles. Puede comparar los atributos de los informes de autenticación detallados con las condiciones de la directiva de autorización que espera que coincidan.
2. Evento de descarga de DACL. Esta cadena sólo se presenta en el caso de que el perfil de autorización seleccionado para la autenticación inicial contenga un nombre DACL.
3. Autenticación del portal: este paso del flujo indica que el mecanismo SSO no ha podido localizar la sesión de usuario. Esto puede suceder debido a varias razones:
 - NAD no está configurado para enviar mensajes de cuentas o la dirección IP entramada no está presente en ellos
 - El FQDN del portal CPP se ha resuelto en la dirección IP del nodo ISE diferente del nodo en el que se ha procesado la autenticación inicial
 - El cliente se encuentra detrás de la NAT
4. Cambio de datos de sesión. En este ejemplo concreto, el estado de la sesión ha cambiado de Desconocido a Conforme.
5. COA al dispositivo de acceso a la red. Este COA debe ejecutarse correctamente para que la nueva autenticación provenga del lado NAD y las nuevas asignaciones de políticas de autorización del lado ISE. Si COA ha fallado, puede abrir un informe detallado para investigar el motivo. Los problemas más comunes con el COA pueden ser:
 - Tiempo de espera de COA: en tal caso, el PSN que ha enviado la solicitud no está configurado como cliente COA en el lado NAD o la solicitud COA se ha descartado en algún lugar del camino.
 - COA negativo ACK - Indica que el COA ha sido recibido por NAD pero debido a alguna razón la operación del COA no puede ser confirmada. Para este escenario, un informe detallado debe

contener una explicación más detallada.

Dado que ASA se utiliza como NAD para este ejemplo, no puede ver ninguna solicitud de autenticación posterior para el usuario. Esto se debe al hecho de que ISE utiliza la inserción de COA para ASA, lo que evita la interrupción del servicio VPN. En este escenario, el propio COA contiene nuevos parámetros de autorización, por lo que no es necesaria la reautenticación.

Paso 2.Verificación de la selección de políticas de aprovisionamiento de clientes: para ello, puede ejecutar un informe sobre ISE que le ayudará a comprender qué políticas de aprovisionamiento de clientes se aplicaron al usuario.

Desplácese hasta **Operations > Reports Endpoint and Users > Client Provisioning** y ejecute el informe para la fecha que necesite.

Client Provisioning ⓘ

From 2017-02-04 00:00:00.0 to 2017-03-06 21:06:33.980

Logged At	Server ⓘ	Event	Identity ⓘ	Client
× Last 30 Days ×			Identity	
2017-02-24 18:33:46....	skuchere-ise22-3	Client provisioning succeeded	user1	AC-44
2017-02-23 18:46:42....	skuchere-ise22-3	Client provisioning succeeded	user1	AC-44
2017-02-23 17:59:07....	skuchere-ise22-3	Client provisioning succeeded	user1	AC-44

Figura 4-2

Con este informe, puede verificar qué política de aprovisionamiento de clientes se ha seleccionado. Asimismo, en caso de fallo, deberán presentarse los motivos en el **Failure Reason** columna.

Paso 3.Verificación del informe de estado: acceda a **Operations > Reports Endpoint and Users > Posture Assessment by Endpoint**.

Posture Assessment by Endpoint ⓘ

From 2017-02-04 00:00:00.0 to 2017-03-06 21:24:17.603

Logged At	Status	Details	Identity ⓘ	Endpoint ID ⓘ	IP Address
× Last 30 Days ×			Identity	Endpoint ID	
2017-02-24 18:34:31....	✓		user1	00:0B:7F:D0:F8:F4	10.62.145.44
2017-02-23 19:33:35....	✓		user1	00:0B:7F:D0:F8:F4	10.62.145.44

Figura 4-3

Desde aquí puede abrir un informe detallado de cada evento concreto para comprobar, por ejemplo, a qué ID de sesión pertenece este informe, qué requisitos de estado exactos ha seleccionado ISE para el terminal y el estado de cada requisito.

Troubleshoot

Información general

Para la resolución de problemas del proceso de estado, estos componentes de ISE deben habilitarse para depurar en los nodos de ISE donde puede ocurrir el proceso de estado:

- `client-webapp` - El componente responsable del aprovisionamiento de agentes. Archivos de registro de destino `guest.log` y `ise-psc.log`.
- `guestaccess` - El componente responsable de la búsqueda del componente del portal de aprovisionamiento de clientes y del propietario de sesión (cuando la solicitud llega a la PSN incorrecta). Archivo de registro de destino: `guest.log`.
- `provisioning` - El componente responsable del procesamiento de políticas de aprovisionamiento de clientes. Archivo de registro de destino: `guest.log`.
- `posture` - Todos los acontecimientos relacionados con la postura. Archivo de registro de destino: `ise-psc.log`.

Para la resolución de problemas en el lado del cliente, puede utilizar lo siguiente:

- `acisensa.log` -En caso de fallo de aprovisionamiento del cliente en el lado del cliente, este archivo se crea en la misma carpeta en la que se ha descargado la NSA (directorio de descargas para Windows normalmente).
- `AnyConnect_ISEPosture.txt` - Este archivo se encuentra en el paquete DART del directorio `Cisco AnyConnect ISE Posture Module`. Toda la información sobre la detección de PSN de ISE y los pasos generales del flujo de estado se registra en este archivo.

Solución de problemas comunes

Problemas relacionados con SSO

En caso de un SSO correcto, puede ver estos mensajes en el `ise-psc.log`, este conjunto de mensajes indica que la búsqueda de sesión ha finalizado correctamente y que se puede omitir la autenticación en el portal.

```
<#root>
```

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

Found session c0a801010002600058232bb8 using ipAddr 10.62.145.121
```

Ventana de texto 5-1

Puede utilizar la dirección IP del terminal como clave de búsqueda para encontrar esta información.

Un poco más adelante en el registro de invitados, debe ver que se ha omitido la autenticación:

```
<#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.F
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] com.cisco.ise.portalSessionManager.F
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.processo
```

Ventana de texto 5-2

En caso de que el SSO no funcione, el `ise-psc log` contiene información sobre la falla de búsqueda de sesión:

```
<#root>
```

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

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

```
No Radius session found
```

Ventana de texto 5-3

En el `guest.log` en tal caso, debe ver la autenticación de usuario completa en el portal:

```
<#root>
```

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

```
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
```

Ventana de texto 5-4

En caso de que se produzcan errores de autenticación en el portal, debe centrarse en la verificación de la configuración del portal. ¿Qué almacén de identidades está en uso? ¿Qué grupos están autorizados para iniciar sesión?

Solucionar problemas de selección de directiva de aprovisionamiento de clientes

En caso de que se produzcan fallos en las políticas de aprovisionamiento del cliente o un procesamiento de políticas incorrecto, puede comprobar el `guest.log` para obtener más información:

```
<#root>
```

```
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][ ] guestaccess.flowmanager.step.guest.C
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][ ] cpm.guestaccess.common.utils.OSMappe
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][ ] cpm.guestaccess.common.utils.OSMappe
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][ ] guestaccess.flowmanager.step.guest.C
2017-02-23 17:59:07,505 DEBUG [http-bio-10.48.17.249-8443-exec-2][ ] guestaccess.flowmanager.step.guest.C
:userInfo:- CP Policy Status =SUCCESS, needToDoVlan=false, CoaAction=NO_COA
```

Ventana de texto 5-5

En la primera cadena, puede ver cómo se inyecta la información sobre la sesión en el motor de selección de políticas; en caso de que no haya coincidencia de políticas o ésta sea incorrecta, puede comparar los atributos desde aquí con la configuración de la política de aprovisionamiento del cliente. La última cadena indica el estado de la selección de directivas.

Troubleshooting del Proceso de Postura

En el lado del cliente, debe estar interesado en la investigación de las sondas y sus resultados. Este es un ejemplo de una sonda de etapa 1 exitosa:

```
*****
```

```
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..
```

```
*****
```

Ventana de texto 5-6

En esta etapa, PSN vuelve a la información de AC sobre el propietario de la sesión. Puede ver estos dos mensajes más adelante:

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..

Ventana de texto 5-7

Los propietarios de sesiones devuelven al agente toda la información necesaria:

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>
```

Ventana de texto 5-8

Desde el lado de PSN, puede centrarse en estos mensajes en la `guest.log` cuando se espera que la solicitud inicial que llega al nodo no sea propietaria de la sesión:

```
<#root>
```

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

```
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.NextGenDis
```

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

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

```
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.NextGenDis
```

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

Ventana de texto 5-9

Aquí puede ver que PSN primero intenta encontrar una sesión localmente, y después de la falla inicia una solicitud a MNT con el uso de la lista de IPs y MACs para localizar al propietario de la sesión.

Un poco más tarde debe ver una solicitud del cliente en el PSN correcto:

```
<#root>
```

```
2017-02-23 17:59:56,790 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRuntime
Looking for session using session ID: null, IP addrs: [172.16.31.12, 10.62.145.95], mac Addr [00:0B:7F:D0:F8:F4]

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

Found session c0a801010009e00058af0f7b using ipAddr 172.16.31.12
```

Ventana de texto 5-10

Como siguiente paso, PSN realiza la búsqueda de políticas de aprovisionamiento de clientes para esta sesión:

```
<#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.PostureRuntime
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRuntime
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRuntime
2017-02-23 17:59:56,795 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePolicy
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
```

Ventana de texto 5-11

En el siguiente paso, puede ver el proceso de selección de requisitos de postura. Al final del paso, se prepara una lista de requisitos que se devuelve al agente:

```
<#root>
```

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

```
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 18:00:00,432 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 18:00:00,433 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 18:00:00,433 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePoli
2017-02-23 18:00:03,884 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cpm.posture.runtime.agent.AgentXmlGen
2017-02-23 18:00:03,904 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cpm.posture.runtime.agent.AgentXmlGen
2017-02-23 18:00:03,904 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cpm.posture.runtime.agent.AgentXmlGen
2017-02-23 18:00:04,069 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureHand
<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>
```

Ventana de texto 5-12

Posteriormente, puede ver que PSN recibió el informe de estado:

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

Ventana de texto 5-13

Al final del flujo, ISE marca el terminal como conforme e inicia el COA:

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

Ventana de texto 5-14

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).