Implementar el estado de ISE

Contenido

Introducción

Este documento describe algunas configuraciones de línea base que abordan varios casos prácticos con una postura basada en la redirección.

Restricciones

Las configuraciones de este documento funcionan para los NAD de Cisco, pero no necesariamente para los NAD de terceros.

Comportamiento del cliente de postura

El cliente de estado puede activar sondas en estos momentos:

- Inicio de sesión
- Cambio en la capa 3 (L3)/cambio en la tarjeta de interfaz de red (NIC) (nueva dirección IP, cambio de estado de NIC)

Casos de uso

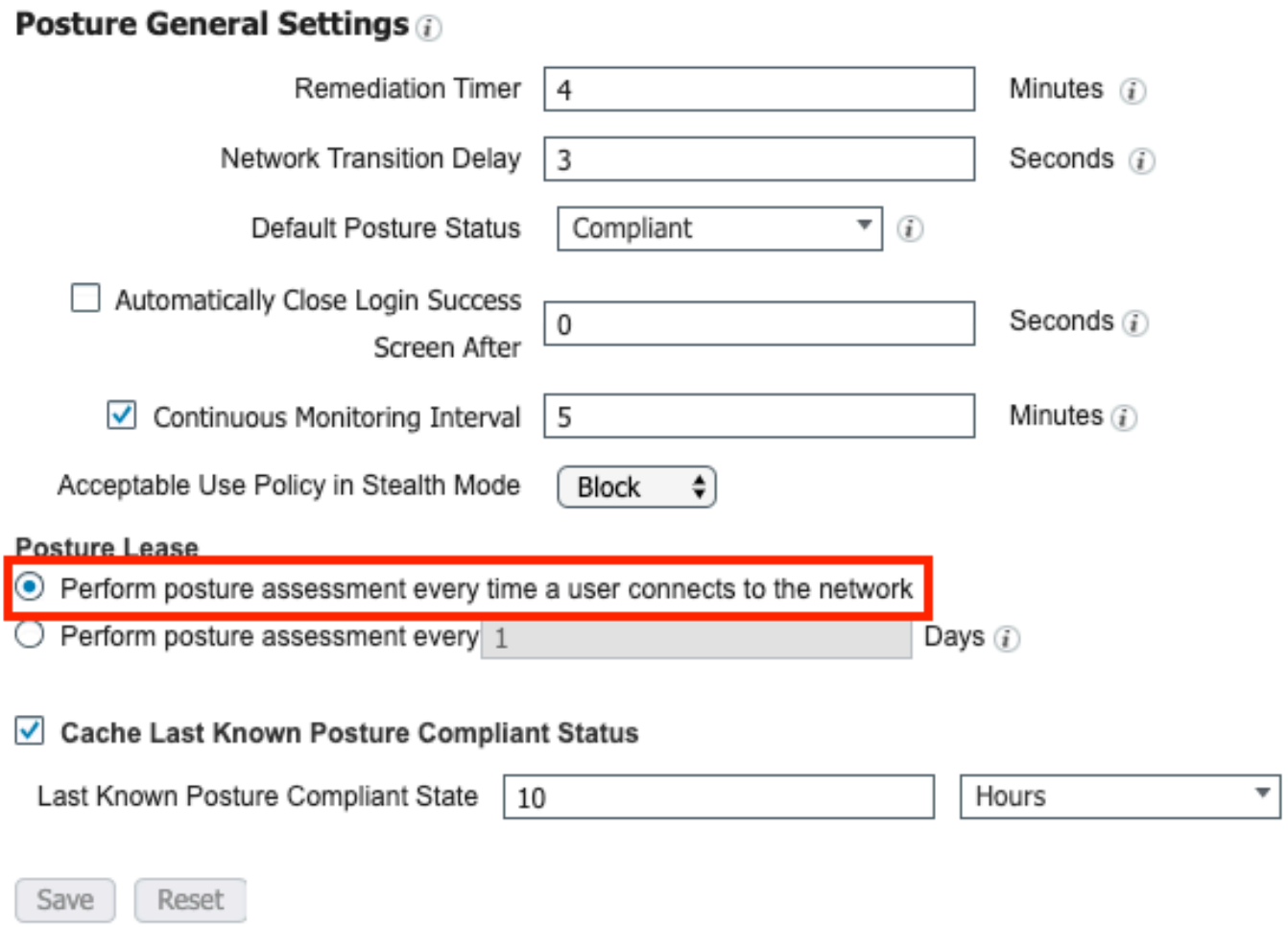
Caso práctico 1: la reautenticación del cliente obliga al NAD a generar un nuevo ID de sesión.

En este caso práctico, el cliente sigue cumpliendo con las normativas, pero debido a la

reautenticación, el NAD se encuentra en estado de redirección (URL de redirección y lista de acceso).

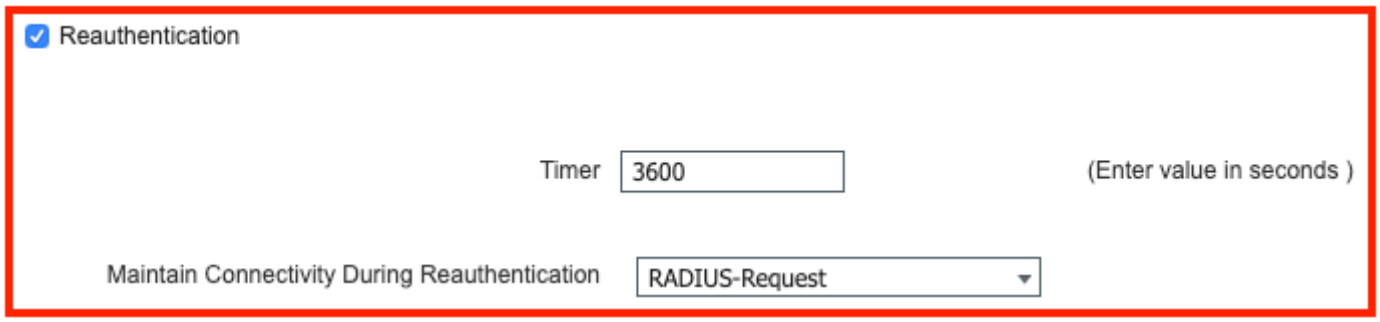
De forma predeterminada, Identity Services Engine (ISE) se configura para realizar una evaluación de estado cada vez que se conecta a la red, más concretamente para cada nueva sesión.

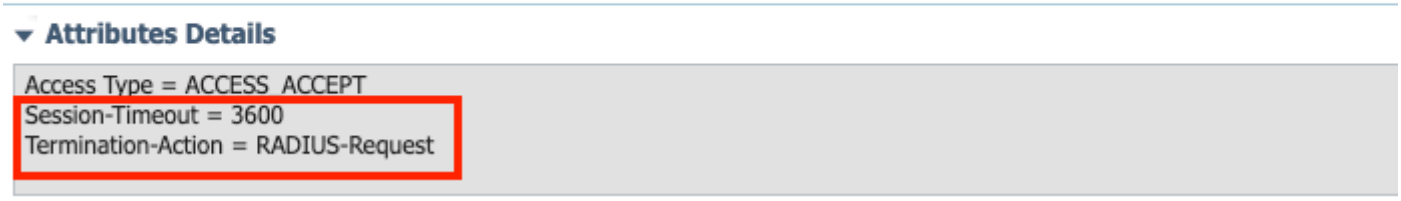
Este ajuste se configura en Centros de trabajo > Estado > Configuración > Configuración general de estado.



Para evitar que el NAD genere un nuevo ID de sesión en la reautenticación, configure estos valores de reautenticación en el perfil de autorización. El temporizador de reautenticación mostrado no es una recomendación estándar y considere temporizadores de reautenticación por implementación en función del tipo de conexión (inalámbrica/con cables), el diseño (cuáles son las reglas de persistencia en el equilibrador de carga), etc.

Política > Elementos de Política > Resultados > Autorización > Perfiles de Autorización





En los switches, debe configurar cada interfaz, o plantilla, para obtener su temporizador de reautenticación de ISE.

```
authentication timer reauthenticate server
```

Nota: Si hay un equilibrador de carga, debe asegurarse de que la persistencia se configura de forma que las reautenticaciones se puedan devolver al Servicio de políticas (PSN) original.

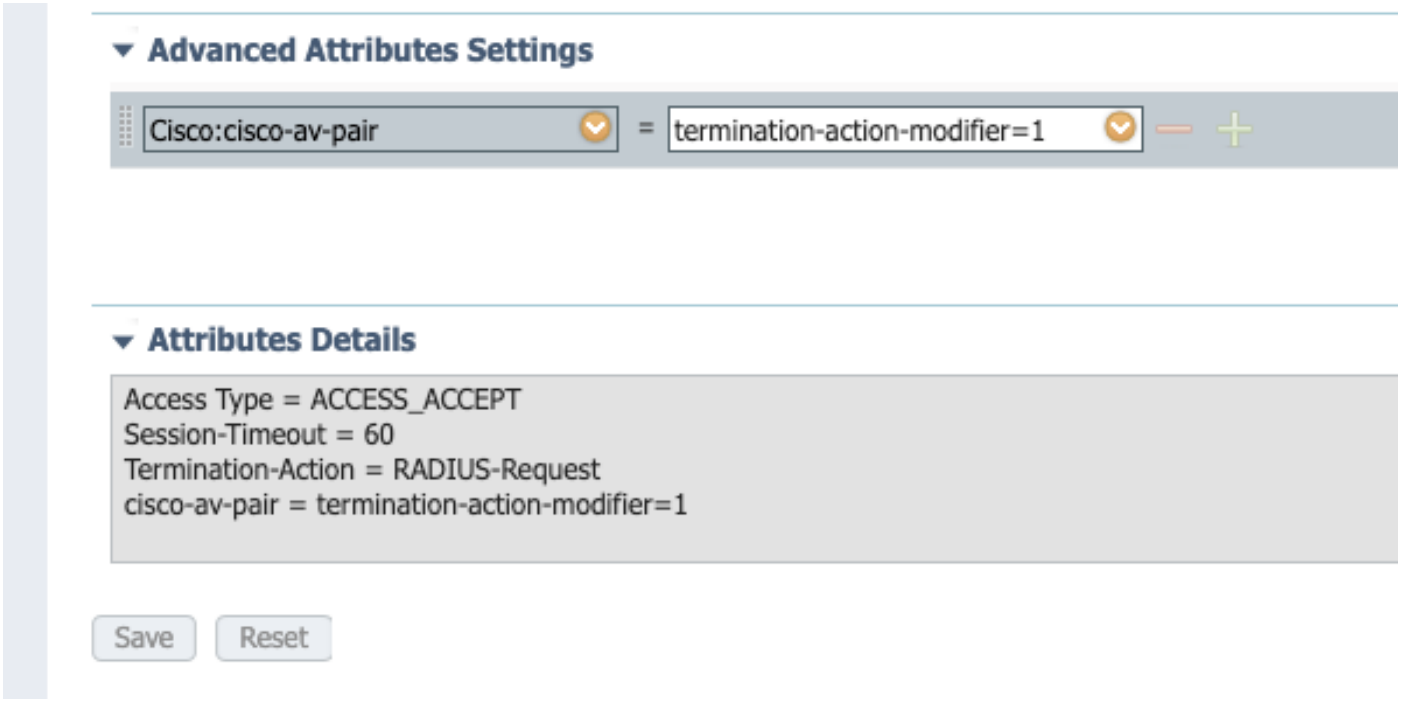
Caso práctico 2: el switch se configura con el orden MAB DOT1X y la prioridad DOT1X MAB (con cables).

En este caso, las reautenticaciones se pueden terminar, porque se puede enviar una detención de contabilización para la sesión 802.1x cuando se intenta la omisión de autenticación MAC (MAB) durante la reautenticación.

- La detención de contabilización que se envía para el proceso MAB cuando falla la autenticación es correcta, ya que el nombre de usuario para el cliente cambia del nombre de usuario 802.1X al nombre de usuario MAB.
- Dot1x como id de método en la parada de contabilidad también es correcto ya que el método de autorización era dot1x.

- Cuando el método Dot1x tiene éxito, envía un inicio de contabilidad con method-id como dot1x. Aquí también, este comportamiento es como se esperaba.

Para resolver este problema, configure el cisco-av-pair:termination-action-modifier=1 en el perfil authZ utilizado cuando un punto final cumple con la normativa. Este par atributo-valor (AV) especifica que NAD reutiliza el método elegido en la autenticación original independientemente del orden configurado.



Caso práctico 3: Los clientes inalámbricos se desplazan y las autenticaciones de diferentes puntos de acceso se dirigen a diferentes controladores.

Para esta situación, la red inalámbrica debe diseñarse de modo que los puntos de acceso (AP) que se encuentren al alcance de otros AP para itinerancia utilicen el mismo controlador activo. Un ejemplo es la conmutación stateful por error (SSO) del controlador de LAN inalámbrica (WLC). Para obtener más información sobre High Availability (HA) SSO para WLC, consulte la Guía de implementación de High Availability (SSO).

Caso práctico 4: implementaciones con equilibradores de carga (revisión 2.6 anterior 6, revisión 2.7, revisión P2 y 3.0).

En implementaciones con equilibradores de carga involucrados, es importante asegurarse de que después de realizar los cambios en los casos prácticos anteriores, las sesiones continúen yendo al mismo PSN. Antes de las versiones/revisiones enumeradas para este paso, el estado de estado no se replica entre los nodos mediante Light Data Distribution (anteriormente, Light Session Directory). Debido a esto, es posible que diferentes PSN devuelvan resultados de estado de postura diferentes.

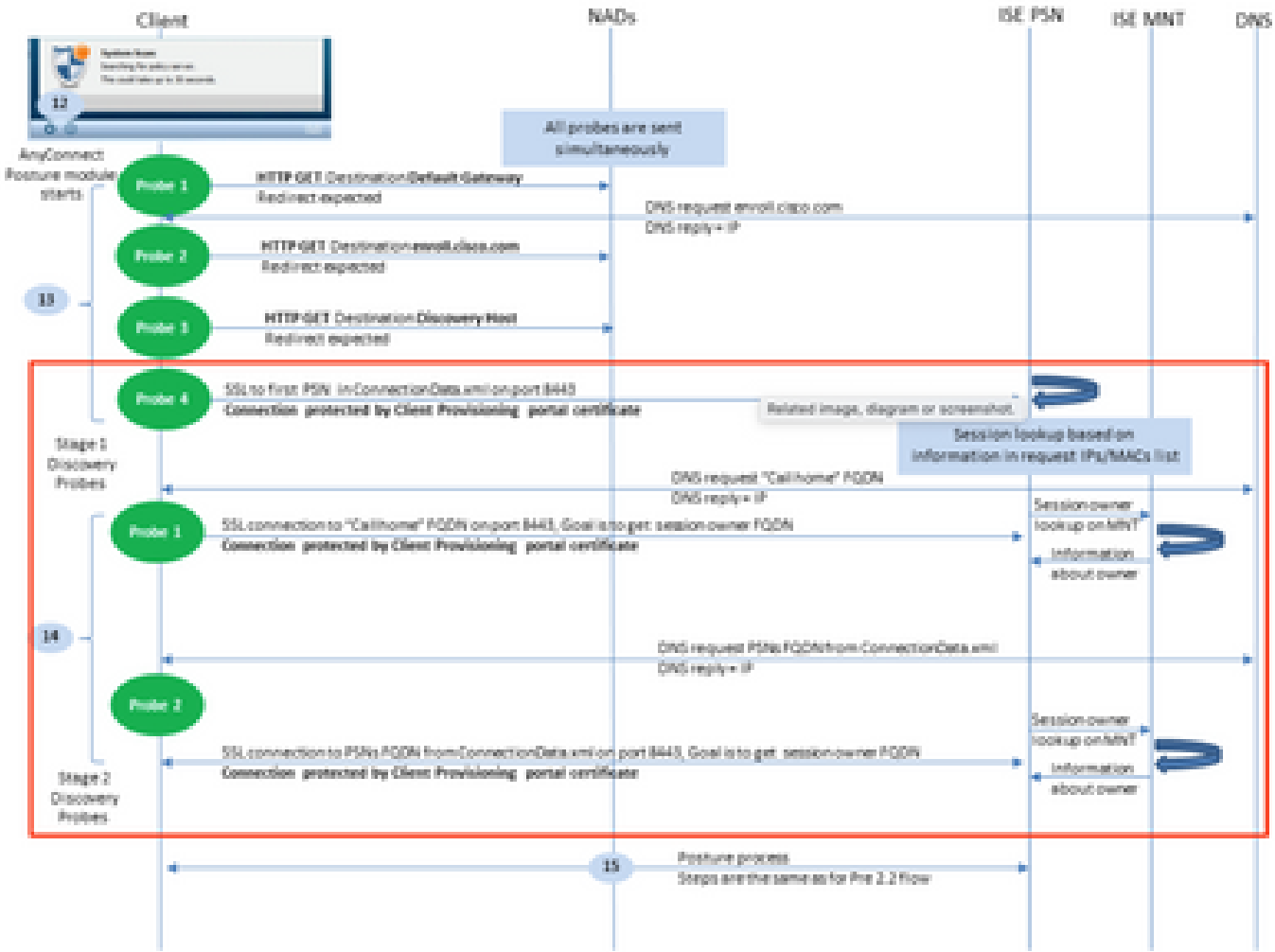
Si la persistencia no se configura correctamente, las sesiones que se vuelven a autenticar podrían ir a un PSN diferente al que se utilizó originalmente. Si esto sucede, el nuevo PSN podría marcar

el estado de cumplimiento de las sesiones como desconocido y pasar el resultado de authZ con la lista de control de acceso (ACL)/URL de redirección y limitar el acceso de los terminales. Una vez más, este cambio en el NAD no sería reconocido por el módulo de postura y no se activarían las sondas.

Para obtener más información sobre cómo configurar equilibradores de carga, consulte la Guía de implementación de Cisco y F5: Equilibrio de carga de ISE con BIG-IP. Proporciona una descripción general de alto nivel y una configuración específica de F5 de un diseño de prácticas recomendadas para implementaciones de ISE en un entorno de carga equilibrada.

Caso de uso 5: los sondeos de detección de la fase 2 son respondidos por un servidor diferente al que autentica el cliente (Parche 6 anterior a la versión 2.6, Parche 2.7 y 3.0).

Eche un vistazo a las sondas del cuadro rojo de este diagrama.



Los PSN almacenan los datos de sesión durante cinco días, por lo que, en ocasiones, los datos de sesión de una sesión "compatible" aún permanecen en el PSN original aunque el cliente ya no se autentique con ese nodo. Si los sondeos incluidos en el cuadro rojo son respondidos por un PSN que no sea el que autentica actualmente la sesión Y que PSN ha poseído y marcado anteriormente este terminal conforme, es posible que haya una discordancia entre el estado de

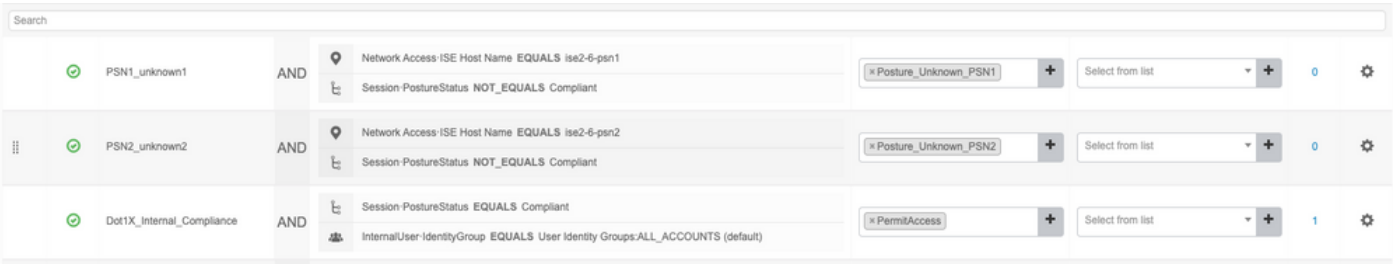
estado del módulo de estado en el terminal y el PSN de autenticación actual.

A continuación se indican algunos escenarios comunes en los que puede producirse esta discordancia:

- No se recibe una detención de cuentas para un terminal cuando se desconecta de la red.
- El NAD falló de un PSN a otro.
- Un equilibrador de carga reenvía las autenticaciones a diferentes PSN para el mismo terminal.

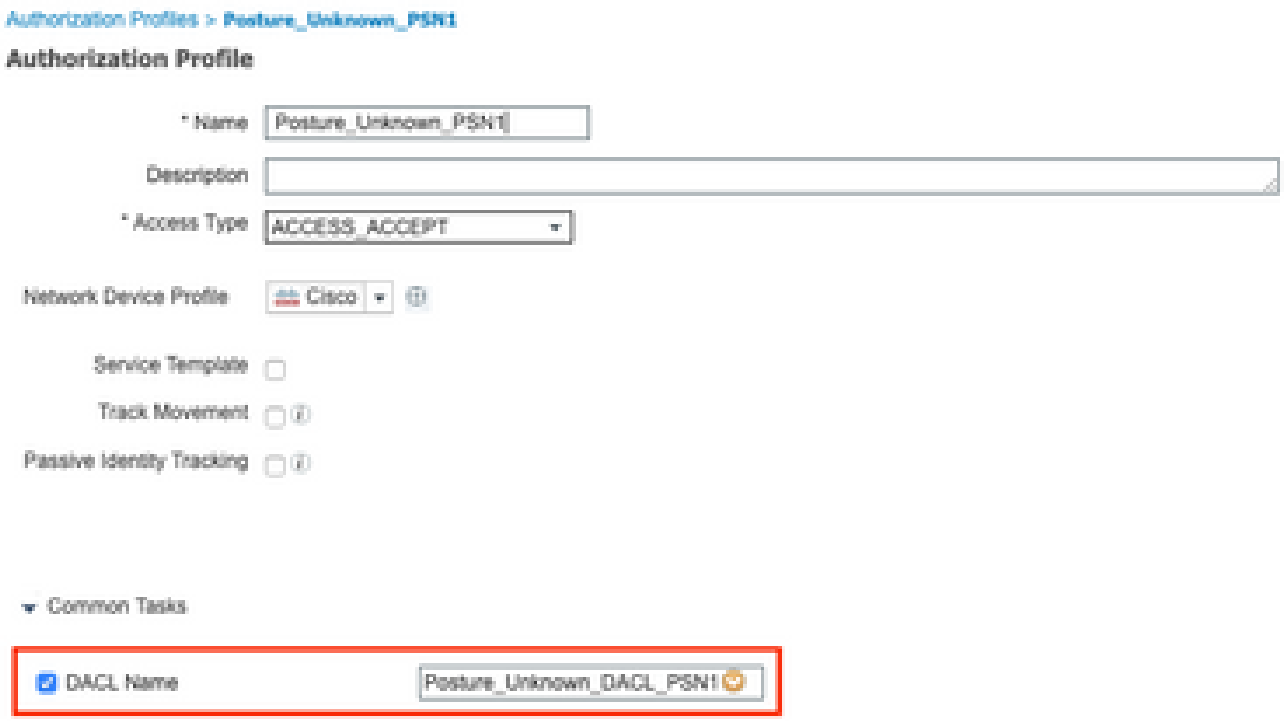
Para protegerse de este comportamiento, ISE se puede configurar para permitir que solo las sondas de detección de un terminal determinado lleguen a PSN en el que se autentica actualmente. Para lograr esto, configure una política de autorización diferente para cada PSN en su implementación. En estas políticas, haga referencia a un perfil authZ diferente que contenga una lista de control de acceso descargable (DACL) que permita sondeos SOLAMENTE al PSN especificado en la condición authZ. Vea este ejemplo:

Cada PSN tiene una regla para el estado de postura desconocido:

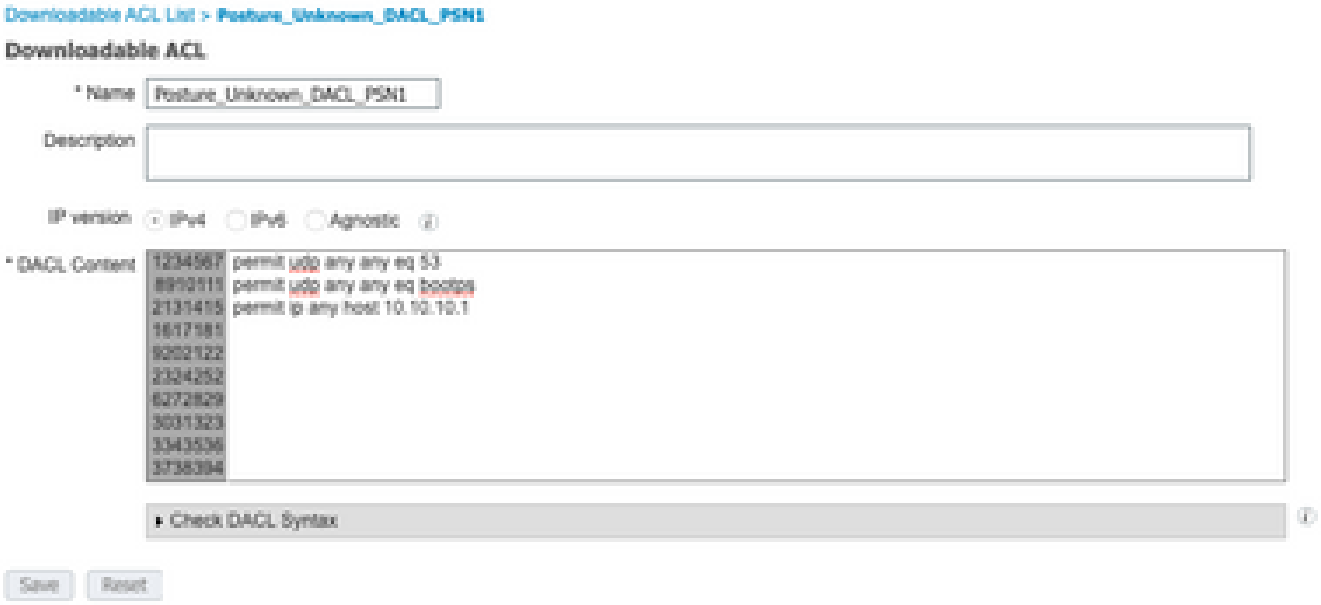


Cada perfil individual hace referencia a una DACL diferente.

Nota: Para conexiones inalámbricas, utilice las ACL de Airespace.



Cada DACL solo permite el acceso de sondeo al PSN que gestiona la autenticación.



En el ejemplo anterior, 10.10.10.1 es la dirección IP de PSN 1. La DACL a la que se hace referencia se puede modificar para cualquier servicio/IP adicional según sea necesario, pero limita el acceso solo a PSN que gestiona la autenticación.

Parche 6, Parche 2.7 y 3.0 de Cambio de Comportamiento Post 2.6

El estado de postura se ha agregado al directorio de sesión de RADIUS a través del marco de

distribución de datos ligeros. Cada vez que se recibe una actualización del estado en cualquier PSN, se replica en TODOS los PSN de la implementación. Una vez que este cambio está en vigor, se eliminan las implicaciones de las autenticaciones y/o sondeos que llegan a diferentes PSN en diferentes autenticaciones y cualquier PSN puede responder a todos los terminales independientemente de dónde estén autenticados actualmente.

En los cinco casos prácticos de este documento, tenga en cuenta estos comportamientos:

Caso práctico 1: la reautenticación del cliente obliga al NAD a generar un nuevo ID de sesión. El cliente sigue cumpliendo con las normativas, pero debido a la reautenticación, el NAD se encuentra en estado de redirección (URL de redirección y lista de acceso).

- Este comportamiento no cambia y esta configuración todavía se puede implementar en ISE y los NAD.

Caso práctico 2: el switch se configura con el orden MAB DOT1X y la prioridad DOT1X MAB (con cables).

- Este comportamiento no cambia y esta configuración todavía se puede implementar en ISE y los NAD.

Caso práctico 3: Los clientes inalámbricos se desplazan y las autenticaciones de diferentes puntos de acceso se dirigen a diferentes controladores.

- Este comportamiento no cambia y esta configuración todavía se puede implementar en ISE y los NAD.

Caso práctico 4: implementaciones con equilibradores de carga.

- Se pueden seguir las prácticas recomendadas definidas en la guía de equilibrio de carga, pero en el caso de que el equilibrador de carga reenvíe las autenticaciones a diferentes PSN, se puede devolver al cliente el estado correcto.

Caso práctico 5: la respuesta a los sondeos de detección de la fase 2 la realiza un servidor diferente al que autentica el cliente

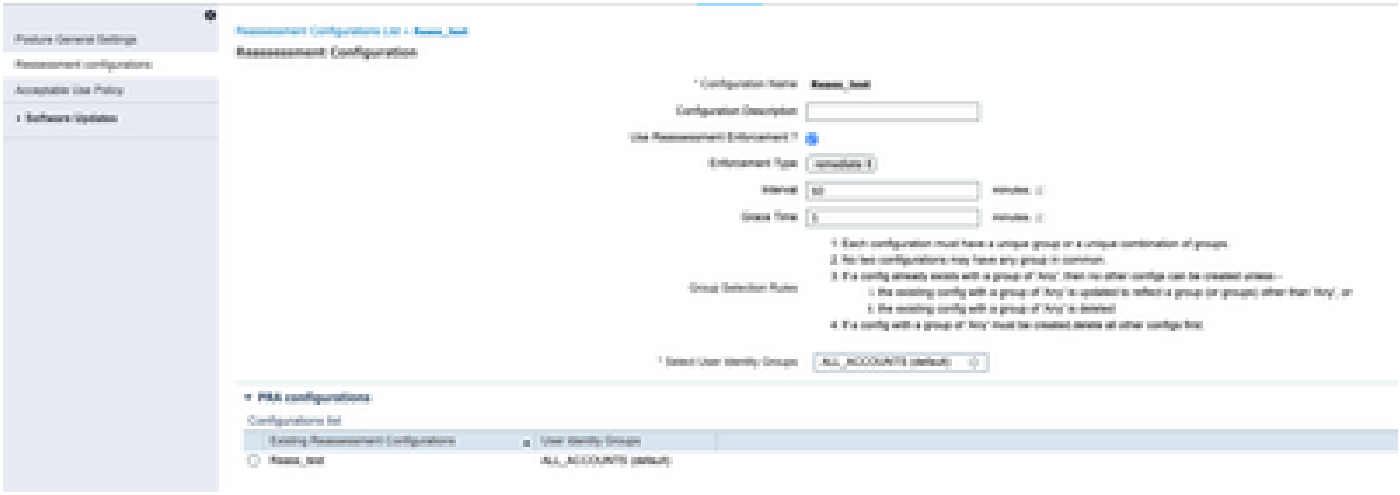
- Esto no puede ser un problema con el nuevo comportamiento y el perfil de autorización por PSN es innecesario.

Consideraciones al mantener el mismo Id. de sesión

Cuando se utilizan los métodos enumerados en este documento, un usuario que permanece conectado a la red podría seguir siendo compatible durante largos períodos de tiempo. Aunque se vuelvan a autenticar, el sessionID no cambia y, por lo tanto, ISE continúa pasando el resultado de AuthZ para que su regla coincida con el estado de cumplimiento.

En este caso, debe configurarse la reevaluación periódica para que se requiera Posture para asegurarse de que el terminal sigue cumpliendo las políticas corporativas en intervalos definidos.

Esto se puede configurar en Centros de trabajo > Estado > Configuración > Configuraciones de reevaluación.



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).