Verificación de la Exclusión del Cliente 802.1X en un WLC de AireOS

Contenido

Introducción

Este documento describe la exclusión del cliente 802.1X en un controlador de LAN inalámbrica (WLC) de AireOS.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- WLC de Cisco AireOS
- Protocolo 802.1X
- Servicio de usuario de acceso telefónico de autenticación remota (RADIUS)
- Identity Service Engine (ISE)

Componentes Utilizados

La información de este documento se basa en AireOS.

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

La exclusión de clientes 802.1X es una opción importante que se debe tener en un autenticador 802.1X como un WLC. Esto se realiza para evitar una sobrecarga de la infraestructura del servidor de autenticación por parte de los clientes del protocolo de autenticación extensible (EAP, Extensible Authentication Protocol) que son hiperactivos o funcionan incorrectamente.

Casos de usuario

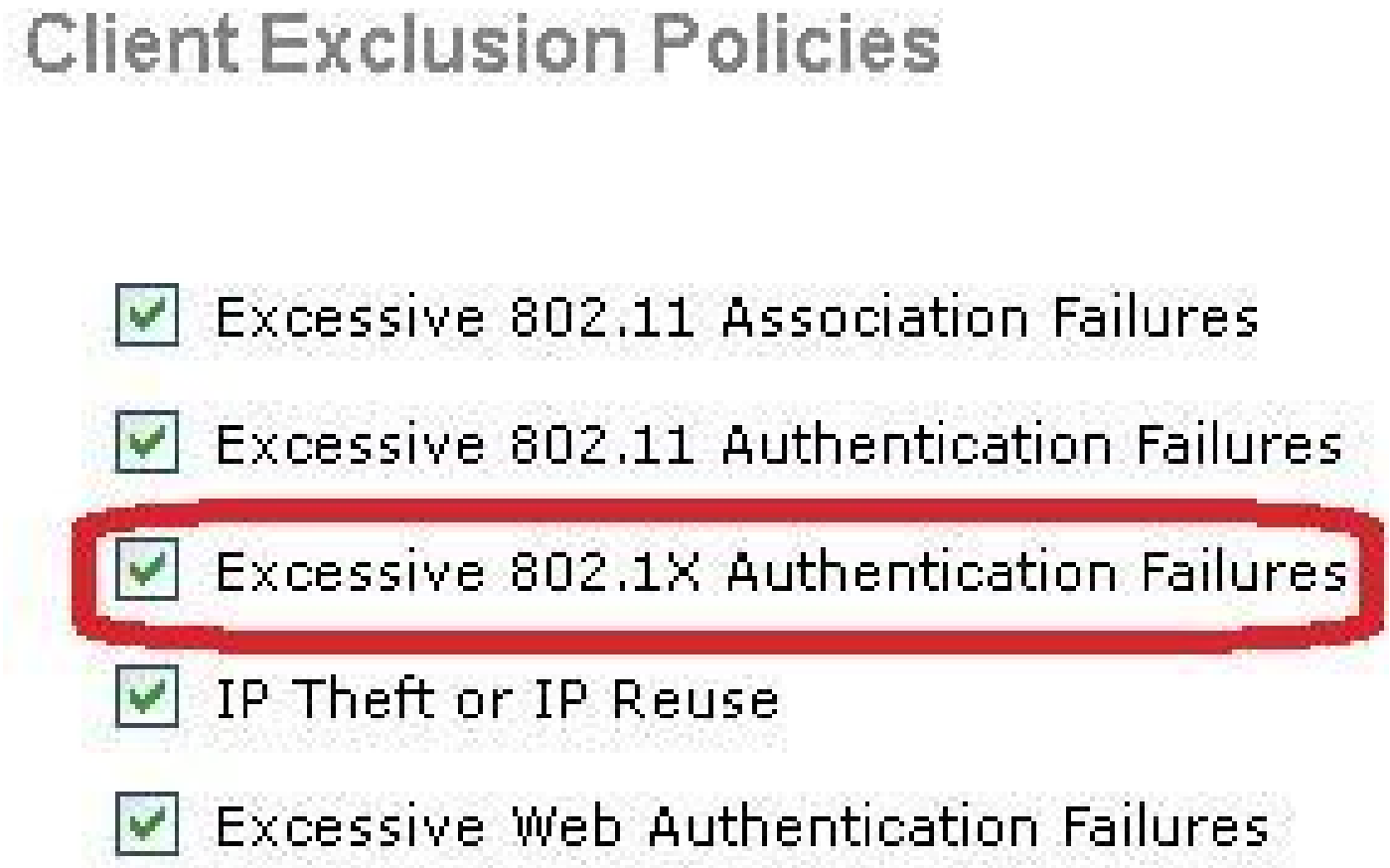
Algunos ejemplos de casos prácticos son:

- Un suplicante EAP configurado con credenciales incorrectas. La mayoría de los suplicantes, como los suplicantes EAP, detienen los intentos de autenticación después de algunos errores sucesivos. Sin embargo, algunos suplicantes EAP continúan intentando reautenticarse en caso de error, posiblemente muchas veces por segundo. Algunos clientes sobrecargan servidores RADIUS y provocan una denegación de servicio (DoS) en toda la red.
- Después de una falla de red principal, cientos o miles de clientes EAP pueden intentar autenticarse simultáneamente. Como resultado, los servidores de autenticación se pueden sobrecargar y proporcionar una respuesta lenta. Si los clientes o el autenticador agotan el tiempo de espera antes de que se procese la respuesta lenta, puede producirse un círculo vicioso en el que los intentos de autenticación continúan agotando el tiempo de espera e intentan procesar la respuesta de nuevo.

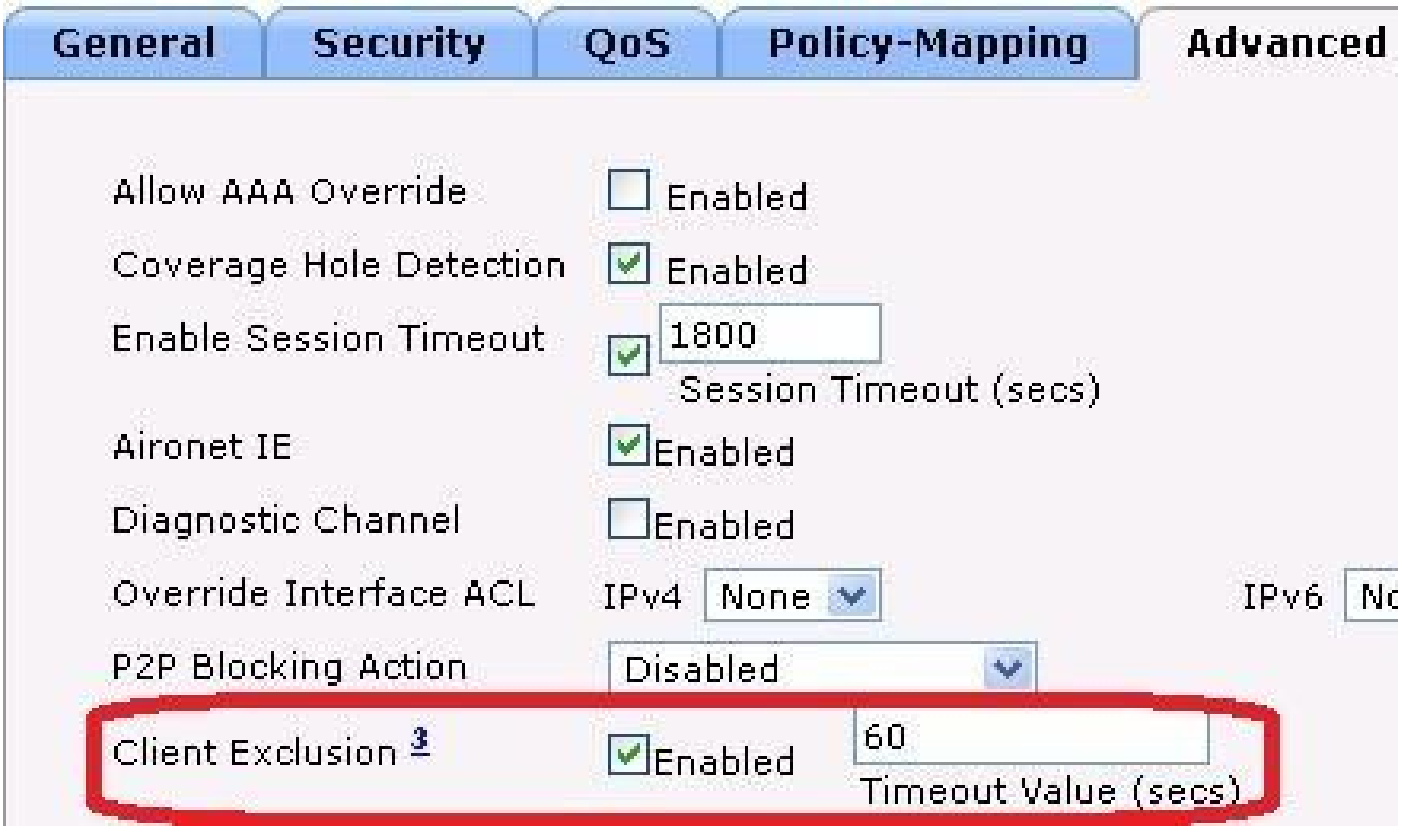
Nota: se requiere un mecanismo de control de admisión para permitir que los intentos de autenticación tengan éxito.

¿Cómo funciona la exclusión de clientes de 802.1X?

La exclusión de clientes de 802.1X impide que los clientes envíen intentos de autenticación durante un período de tiempo después de que se produzcan errores de autenticación de 802.1X excesivos. En un WLC 802.1X de AireOS, la exclusión del cliente se habilita globalmente navegando hasta Seguridad > Políticas de protección inalámbrica > Políticas de exclusión del cliente de forma predeterminada y se puede ver en esta imagen.



La exclusión de clientes se puede habilitar o deshabilitar para cada WLAN. De forma predeterminada, se habilita con un tiempo de espera de 60 segundos antes de AireOS 8.5 y 180 segundos a partir de AireOS 8.5.



Configuración de exclusión para proteger los servidores RADIUS de la sobrecarga

Para validar que el servidor RADIUS está protegido contra sobrecarga debido a clientes inalámbricos que funcionan incorrectamente, verifique que estas configuraciones estén vigentes:

- Se seleccionan fallas de autenticación 802.1X excesivas en las políticas globales de exclusión de clientes del WLC.
- Client Exclusion se establece en Enabled en la configuración avanzada de WLAN.
- El valor de límite de tiempo de exclusión del cliente se establece en 60 a 300 segundos.

> Nota: los valores superiores a 300 segundos proporcionan una mejor protección, pero pueden generar quejas de los usuarios.

- Configurar los temporizadores EAP de AireOS y los parámetros del protocolo de autenticación extensible protegido (PEAP) de ISE

Problemas que impiden que funcione la exclusión de 802.1X

Varios ajustes de configuración, en el WLC y en el servidor RADIUS pueden impedir que la exclusión de clientes 802.1X funcione.

Clientes no excluidos debido a la configuración del temporizador WLC EAP

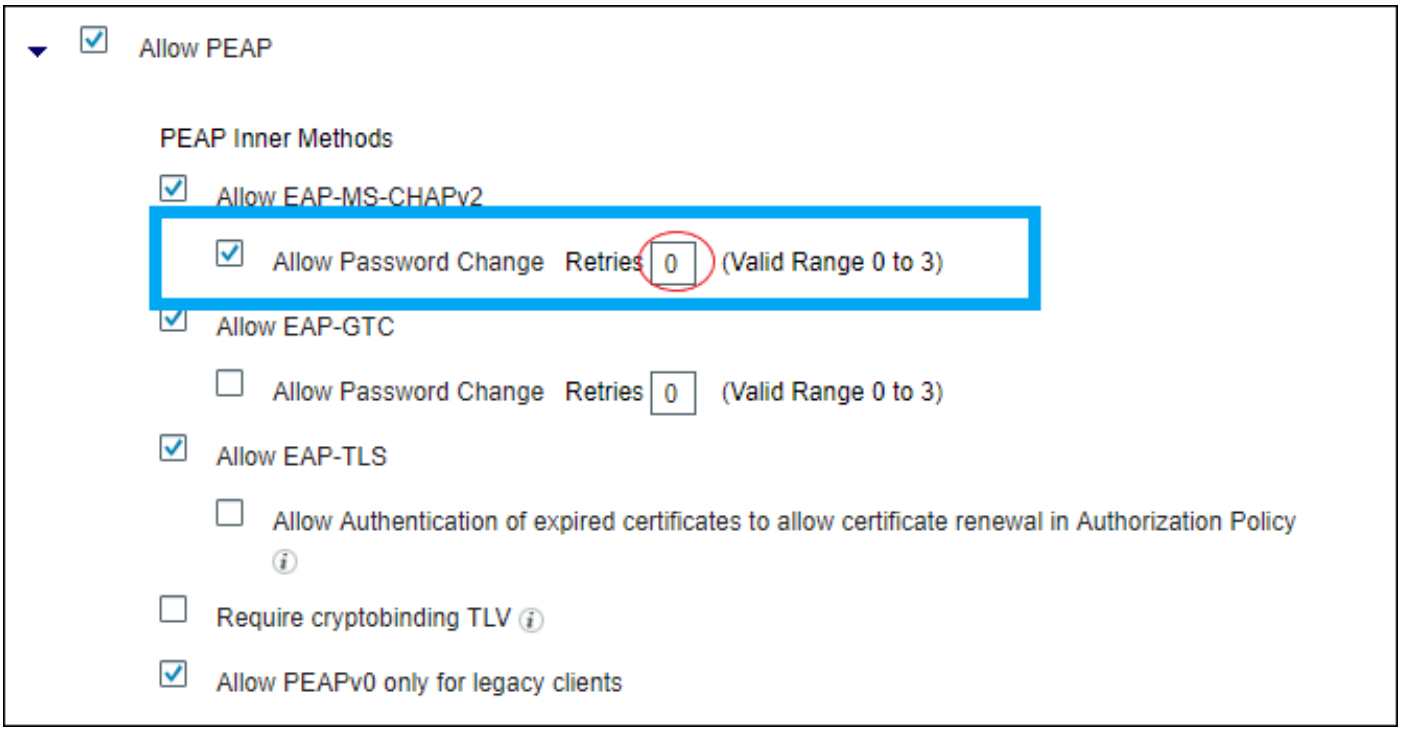
De forma predeterminada, los clientes inalámbricos no se excluyen cuando Exclusión de clientes se establece en Activado en la WLAN. Esto se debe a los largos tiempos de espera EAP predeterminados de 30 segundos que hacen que un cliente que se comporta mal nunca llegue a suficientes fallas sucesivas para activar una exclusión. Configure tiempos de espera EAP más cortos con un mayor número de retransmisiones para permitir que la exclusión de clientes 802.1X surta efecto. Consulte el ejemplo de tiempo de espera.

```
config advanced eap identity-request-timeout 3
config advanced eap identity-request-retries 10
config advanced eap request-timeout 3
config advanced eap request-retries 10
```

Clientes no excluidos debido a la configuración de ISE PEAP

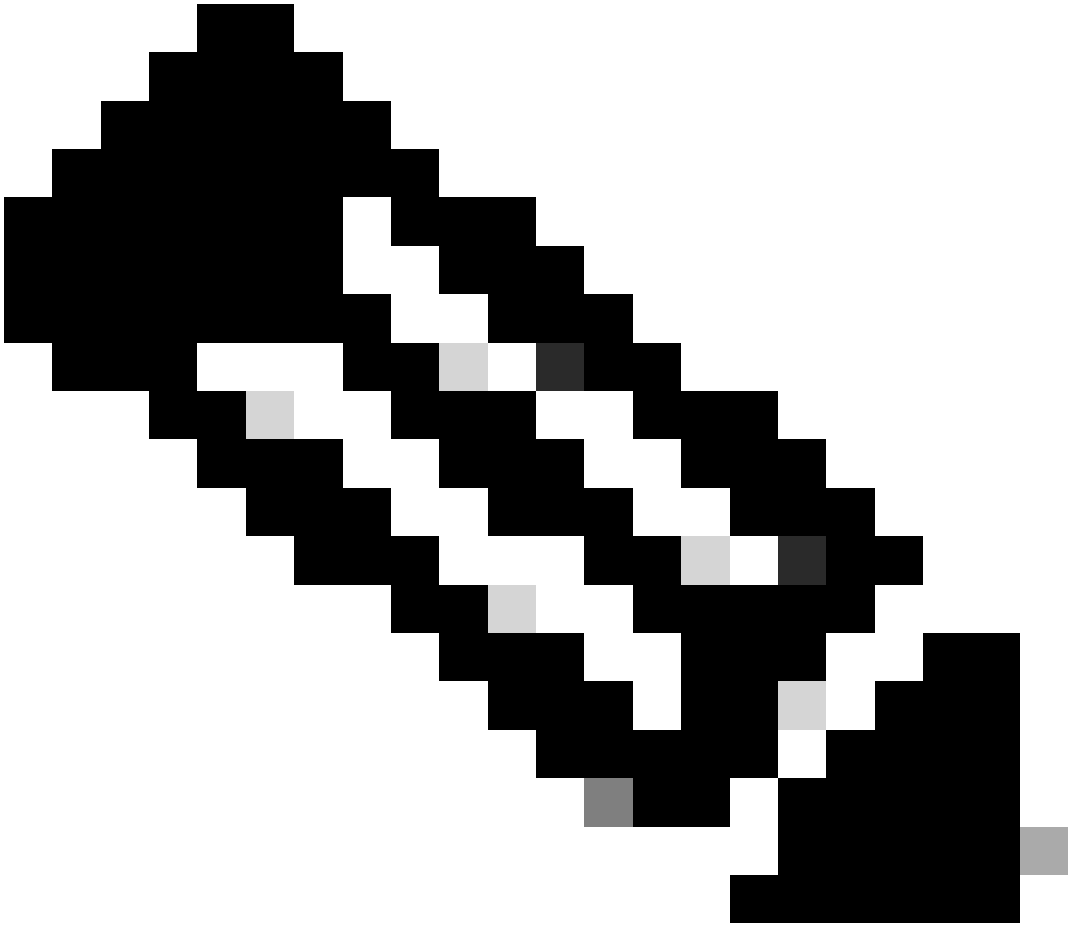
Para que la exclusión de clientes 802.1X funcione, el servidor RADIUS debe enviar un rechazo de acceso cuando la autenticación falle. Si el servidor RADIUS es ISE y PEAP está en uso, la exclusión no puede producirse y depende de la configuración de ISE PEAP. Dentro de ISE,

navegue hasta Policy > Results > Authentication > Allowed Protocols > Default Network Access como se muestra en la imagen.



Si configura Retries (marcado en rojo a la derecha) en 0, ISE debe enviar Access-Reject inmediatamente al WLC, que debe habilitar el WLC para excluir al cliente (si intenta autenticarse tres veces).

Nota: la configuración de Retries es algo independiente de la casilla de verificación Allow Password Change, es decir, el valor de Retries puede ser respetado, incluso si Allow Password Change no está marcado. Sin embargo, si Reintentos se establece en 0, entonces Permitir Cambio de Contraseña no funciona.



Nota: para obtener más información, consulte el ID de bug de Cisco CSCsq16858. Solo los usuarios registrados de Cisco pueden acceder a la información y las herramientas de errores de Cisco.

Información Relacionada

- Evite que se colapse la red RADIUS inalámbrica a gran escala
- Soporte técnico y descargas de Cisco

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).