Matriz de Compatibilidad de Seguridad de Capa 2 y Capa 3 del WLC

Contenido

Introducción

Este documento proporciona la matriz de compatibilidad para los mecanismos de seguridad de Capa 2 y Capa 3 soportados en el Wireless LAN Controller (WLC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Información básica sobre la configuración de puntos de acceso ligeros y WLC de Cisco
- Información básica sobre el protocolo de punto de acceso ligero (LWAPP)
- Conocimientos básicos de las soluciones de seguridad inalámbrica

Componentes Utilizados

La información de este documento se basa en un WLC de Cisco serie 4400/2100 que ejecuta la versión de firmware 7.0.116.0

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). If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las

convenciones del documento.

Soluciones Cisco Unified Wireless Network Security

Cisco Unified Wireless Network admite métodos de seguridad de capa 2 y capa 3.

- Seguridad de capa 2
- Seguridad de capa 3 (para WLAN) o seguridad de capa 3 (para LAN de invitado)

La seguridad de capa 2 no se admite en las LAN de invitado.

Esta tabla enumera los diversos métodos de seguridad de Capa 2 y Capa 3 soportados en el Wireless LAN Controller. Estos métodos de seguridad se pueden habilitar desde la ficha **Security** en la página **WLANs > Edit** de la WLAN.

Mecanismo de seguridad de capa 2		
Parámetro		**Descripción**
Seguridad de capa 2	Ninguno	No se ha seleccionado ninguna seguridad de capa 2.
	WPA+WPA2	Utilice esta configuración para habilitar el acceso Wi-Fi protegido.
	802.1x	Utilice esta configuración para habilitar la autenticación 802.1x.
	WEP estática	Utilice este parámetro para activar la encriptación WEP estática.
	WEP estática + 802.1x	Utilice esta configuración para activar los parámetros WEP estáticos y 802.1x.
	CKIP	Utilice esta configuración para habilitar el protocolo de integridad de clave de Cisco (CKIP). Funcional en los AP modelos 1100, 1130 y 1200, pero no en AP 1000. Es necesario activar Aironet IE para que esta función funcione. CKIP expande las claves de cifrado a 16 bytes.
Filtrado de MAC	Seleccione esta opción para filtrar los clientes por dirección MAC. Configure localmente los clientes por dirección MAC en la página Filtros MAC > Nuevo. De lo contrario, configure los clientes en un servidor RADIUS.	
Mecanismo de seguridad de capa 3 (para WLAN)		
Parámetro		**Descripción**
Seguridad	Ninguno	No se ha seleccionado ninguna seguridad de capa 3.

<table>
<tr><td rowspan="2">de capa 3</td><td>IPSec</td><td>Utilice esta configuración para habilitar IPSec. Debe comprobar la disponibilidad del software y la compatibilidad del hardware del cliente antes de implementar IPSec.
Nota: Debe tener instalado el módulo de seguridad mejorada/VPN (tarjeta de procesador criptográfico) opcional para activar IPSec. Verifique que esté instalado en su controlador en la página Inventory .</td></tr>
<tr><td>Paso a través de VPN</td><td>Utilice esta configuración para habilitar el paso a través de VPN.
Nota: Esta opción no está disponible en los controladores de la serie Cisco 5500 y Cisco 2100. Sin embargo, puede replicar esta funcionalidad en un Cisco 5500 Series Controller o Cisco 2100 Series Controller creando una WLAN abierta usando una ACL.</td></tr>
<tr><td>Política web</td><td colspan="2">Active esta casilla de verificación para habilitar la directiva Web. El controlador reenvía el tráfico DNS hacia y desde los clientes inalámbricos antes de la autenticación.
Nota: La política web no se puede utilizar en combinación con las opciones de paso a través de IPsec o VPN.
Se muestran estos parámetros:
Autenticación: Si selecciona esta opción, se solicitará al usuario un nombre de usuario y una contraseña mientras conecta el cliente a la red inalámbrica.
Passthrough (Paso a través): Si selecciona esta opción, el usuario puede acceder a la red directamente sin la autenticación de nombre de usuario y contraseña.
Redirección web condicional: si selecciona esta opción, el usuario puede ser redirigido condicionalmente a una página web determinada después de que la autenticación 802.1X se haya completado correctamente. Usted puede especificar la paginación de la reorientación y las</td></tr>
</table>

	condiciones bajo las cuales la reorientación ocurre en tu servidor de RADIUS. • Redirección web de página de bienvenida: si selecciona esta opción, el usuario se redirige a una página web concreta después de que la autenticación 802.1X se haya completado correctamente. Después de la redirección, el usuario tiene acceso completo a la red. Puede especificar la página Web de bienvenida en el servidor RADIUS. • En fallo de filtro MAC: habilita los fallos de filtro MAC de autenticación Web.
ACL de autenticación previa	Seleccione la ACL que se utilizará para el tráfico entre el cliente y el controlador.
Sustituir configuración global	Se muestra si selecciona Autenticación. Marque esta casilla para invalidar la configuración de autenticación global establecida en la Página de Login Web.
Tipo de autenticación Web	Se muestra si selecciona Política web y Sustituir configuración global. Seleccione un tipo de autenticación Web: • Interno • Personalizado (descargado) Página de inicio de sesión: seleccione una página de inicio de sesión de la lista desplegable.Página Login Failure: Seleccione una página de inicio de sesión que se muestre al cliente si falla la autenticación Web.Página de cierre de sesión: seleccione una página de inicio de sesión que se muestre al cliente cuando el usuario cierre la sesión del sistema. • Externo (redirigir a servidor externo) URL: introduzca la URL del servidor externo.
Correo electrónico	Se muestra si selecciona Paso a través. Si selecciona esta opción, se le solicitará su dirección de correo electrónico mientras se conecta a la red.

Mecanismo de seguridad de capa 3 (para LAN de invitado)		
Parámetro		**Descripción**
Seguridad	Ninguno	No se ha seleccionado ninguna seguridad de capa 3.

de capa 3	Autenticación Web	Si selecciona esta opción, se le solicitarán el nombre de usuario y la contraseña mientras conecta el cliente a la red.
	Paso a través de Web	Si selecciona esta opción, puede acceder a la red directamente sin la autenticación de nombre de usuario y contraseña.
ACL de autenticación previa		Seleccione la ACL que se utilizará para el tráfico entre el cliente y el controlador.
Sustituir configuración global		Marque esta casilla para invalidar la configuración de autenticación global establecida en la Página de Login Web.
Tipo de autenticación Web		Se muestra si selecciona Sustituir configuración global. Seleccione un tipo de autenticación Web: • Interno • Personalizado (descargado) Página de inicio de sesión: seleccione una página de inicio de sesión de la lista desplegable.Página Login Failure: Seleccione una página de inicio de sesión que se muestre al cliente si falla la autenticación Web.Página de cierre de sesión: seleccione una página de inicio de sesión que se muestre al cliente cuando el usuario cierre la sesión del sistema. • Externo (redirigir a servidor externo) URL: introduzca la URL del servidor externo.
Correo electrónico		Se muestra si selecciona Paso a través de Web. Si selecciona esta opción, se le solicitará su dirección de correo electrónico mientras se conecta a la red.

Nota: En la versión de software del controlador 4.1.185.0 o posterior, CKIP se admite para su uso únicamente con WEP estática. No se admite para su uso con WEP dinámica. Por lo tanto, un cliente inalámbrico configurado para utilizar CKIP con WEP dinámica no puede asociarse a una LAN inalámbrica configurada para CKIP. Cisco recomienda utilizar WEP dinámico sin CKIP (que es menos seguro) o WPA/WPA2 con TKIP o AES (que son más seguros).

Matriz de compatibilidad de seguridad de capa 2 y capa 3 del controlador de LAN inalámbrica

Al configurar la seguridad en una LAN inalámbrica, se pueden utilizar conjuntamente los métodos de seguridad de capa 2 y capa 3. Sin embargo, no todos los métodos de seguridad de capa 2 se pueden utilizar con todos los métodos de seguridad de capa 3. En esta tabla se muestra la matriz de compatibilidad para los métodos de seguridad de capa 2 y capa 3 admitidos en el controlador de LAN inalámbrica.

Mecanismo de seguridad de capa 2	Mecanismo de seguridad de capa 3	Compatibilidad
Ninguno	Ninguno	Válido
WPA+WPA2	Ninguno	Válido
WPA+WPA2	Autenticación Web	No válido
WPA-PSK/WPA2-PSK	Autenticación Web	Válido
WPA+WPA2	Paso a través de Web	No válido
WPA-PSK/WPA2-PSK	Paso a través de Web	Válido
WPA+WPA2	Redireccionamiento web condicional	Válido
WPA+WPA2	Redirección web de página de bienvenida	Válido
WPA+WPA2	Paso a través de VPN	Válido
802.1x	Ninguno	Válido
802.1x	Autenticación Web	No válido
802.1x	Paso a través de Web	No válido
802.1x	Redireccionamiento web condicional	Válido
802.1x	Redirección web de página de bienvenida	Válido
802.1x	Paso a través de VPN	Válido
WEP estática	Ninguno	Válido
WEP estática	Autenticación Web	Válido

WEP estática	Paso a través de Web	Válido
WEP estática	Redireccionamiento web condicional	No válido
WEP estática	Redirección web de página de bienvenida	No válido
WEP estática	Paso a través de VPN	Válido
Static-WEP+ 802.1x	Ninguno	Válido
Static-WEP+ 802.1x	Autenticación Web	No válido
Static-WEP+ 802.1x	Paso a través de Web	No válido
Static-WEP+ 802.1x	Redireccionamiento web condicional	No válido
Static-WEP+ 802.1x	Redirección web de página de bienvenida	No válido
Static-WEP+ 802.1x	Paso a través de VPN	No válido
CKIP	Ninguno	Válido
CKIP	Autenticación Web	Válido
CKIP	Paso a través de Web	Válido
CKIP	Redireccionamiento web condicional	No válido
CKIP	Redirección web de página de bienvenida	No válido
CKIP	Paso a través de VPN	Válido

Información Relacionada

- Ejemplo de la configuración básica del controlador y del Lightweight Access Point del Wireless LAN
- Registro de AP Ligero (LAP) a un Controlador de LAN Inalámbrica (WLC)
- Guía de Configuración de Cisco Wireless LAN Controller, Versión 7.0.116.0
- Preguntas frecuentes sobre el controlador LAN inalámbrico (WLC)
- Soporte Técnico y Documentación - Cisco Systems

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).