Matriz de Compatibilidad de Seguridad de Capa 2 y Capa 3 del Controlador de LAN Inalámbrico

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Soluciones de la seguridad de la red del Cisco Unified Wireless](#)
[Capa 2 del regulador del Wireless LAN – Matriz de compatibilidad de la Seguridad de la capa 3](#)
[Información Relacionada](#)

Introducción

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

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de la configuración de los AP ligeros y del WLCs de Cisco
- Conocimiento básico del protocolo ligero AP (LWAPP)
- Conocimiento básico de las soluciones de la seguridad de red inalámbrica

Componentes Utilizados

La información en este documento se basa en un WLC de las 4400/2100 Series de Cisco que funciona con 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). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las

convenciones del documento.

Soluciones de la seguridad de la red del Cisco Unified Wireless

La red del Cisco Unified Wireless soporta los métodos de seguridad de la capa 2 y de la capa 3.

- Seguridad de la capa 2
- Seguridad de la capa 3 (para la red inalámbrica (WLAN)) o Seguridad de la capa 3 (para el invitado LAN)

La Seguridad de la capa 2 no se soporta en el invitado LAN.

Esta tabla enumera los diversos métodos de seguridad de la capa 2 y de la capa 3 soportados en el regulador del Wireless LAN. Estos métodos de seguridad se pueden habilitar de la **ficha de seguridad** en los **WLAN > editan la** página de la red inalámbrica (WLAN).

Mecanismo de seguridad de la capa 2		
Parámetro		**Descripción**
Seguridad de la capa 2	Ninguno	Ninguna Seguridad de la capa 2 seleccionada.
	WPA+WPA2	Utilice esta determinación para habilitar el acceso protegido Wi-Fi.
	802.1x	Utilice esta determinación para habilitar la autenticación del 802.1x.
	WEP estático	Utilice esta determinación para habilitar el cifrado del WEP estático.
	WEP estático + 802.1x	Utilice esta determinación para habilitar los parámetros del WEP estático y del 802.1x.
	CKIP	Utilice esta determinación para habilitar el Protocolo de integridad de clave Cisco (CKIP). Funcional en el AP modela 1100, 1130, y 1200, pero no AP 1000. El Aironet IE necesita ser habilitado para que esta característica trabaje. CKIP amplía las claves de encripción a 16 bytes.
Filtración MAC	Seleccione para filtrar a los clientes por la dirección MAC. Localmente configure a los clientes por la dirección MAC en el MAC filtra > nueva página. Si no, configure a los clientes en un servidor de RADIUS.	
Mecanismo de seguridad de la capa 3 (para la red		

inalámbrica (WLAN))		
Parámetro		**Descripción**
Seguridad de la capa 3	Ninguno	Ninguna Seguridad de la capa 3 seleccionada.
	IPSec	Utilice esta determinación para habilitar el IPSec. Usted necesita marcar la disponibilidad del software y la compatibilidad del hardware del cliente antes de que usted implemente el IPSec. **Nota:** Usted debe hacer el módulo opcional de la Seguridad VPN/Enhanced (placa del procesador crypto) instalar para habilitar el IPSec. Verifiquela está instalado en su regulador en la página del inventario.
	Paso VPN	Utilice esta determinación para habilitar el paso VPN. **Nota:** Esta opción no está disponible en los reguladores de las Cisco 5500 Series y los reguladores de las Cisco 2100 Series. Sin embargo, usted puede replicar estas funciones en las Cisco 5500 Series regulador o el regulador de las Cisco 2100 Series creando una red inalámbrica (WLAN) abierta usando un ACL.
Directiva de la red	Seleccione esta casilla de verificación para habilitar la directiva de la red. Del regulador el tráfico adelante DNS a y desde los clientes de red inalámbrica antes de la autenticación. **Nota:** La directiva de la red no se puede utilizar conjuntamente con las opciones del IPSec o del paso VPN. Se visualizan estos parámetros: • Autenticación — Si usted selecciona esta opción, indican al usuario para el nombre de usuario y contraseña mientras que conecta al cliente con la red inalámbrica. • Passthrough — Si usted selecciona esta opción, el usuario puede acceder la red directamente sin la autenticación del nombre de usuario y contraseña. • La red condicional reorienta — Si usted	

	selecciona esta opción, el usuario puede ser reorientado condicional a una página web determinada después de que la autenticación del 802.1x complete con éxito. Usted puede especificar la paginación de la reorientación y las condiciones bajo las cuales la reorientación ocurre en tu servidor de RADIUS. • La red de la página del chapoteo reorienta — Si usted selecciona esta opción, reorientan al usuario a una página web determinada después de que la autenticación del 802.1x complete con éxito. Después de que la reorientación, el usuario tenga acceso total a la red. Usted puede especificar la página web del chapoteo en su servidor de RADIUS. • En el error del filtro MAC — Habilita los errores del filtro de la autenticación Web MAC.
Autenticación previa ACL	Seleccione el ACL para ser utilizado para el tráfico entre el cliente y el regulador.
Reemplace la configuración global	Visualizaciones si usted selecciona la autenticación. Marque este cuadro para reemplazar la configuración de la autenticación global fijada en la página de registro de la red.
Tipo del auth de la red	Visualizaciones si usted selecciona la directiva de la red y reemplaza la configuración global. Seleccione un tipo de autenticación Web: • Interno • Personalizado (descargado) Página de registro — Seleccione una página de registro de la lista desplegable.Página de la falla de registro — Seleccione una página de registro que visualice al cliente si la autenticación Web falla.Página del logout — Seleccione una página de registro que visualice al cliente cuando el sistema de los de los registros de usuario. • Externo (reoriente al servidor externo) URL — Ingrese el URL del servidor externo.
Envíe	Visualizaciones si usted selecciona el

por correo electrónico la entrada	passthrough. Si usted selecciona esta opción, le indican para su dirección de correo electrónico mientras que conecta con la red.

Mecanismo de seguridad de la capa 3 (para el invitado LAN)		
Parámetro		**Descripción**
Seguridad de la capa 3	Ninguno	Ninguna Seguridad de la capa 3 seleccionada.
	Autenticación Web	Si usted selecciona esta opción, le indican para el nombre de usuario y contraseña mientras que conecta al cliente con la red.
	Passthrough de la red	Si usted selecciona esta opción, usted puede acceder la red directamente sin la autenticación del nombre de usuario y contraseña.
Autenticación previa ACL		Seleccione el ACL para ser utilizado para el tráfico entre el cliente y el regulador.
Reemplace la configuración global		Marque este cuadro para reemplazar la configuración de la autenticación global fijada en la página de registro de la red.
Tipo del auth de la red		Visualizaciones si usted selecciona la configuración global de la invalidación. Seleccione un tipo de autenticación Web: • Interno • Personalizado (descargado) Página de registro — Seleccione una página de registro de la lista desplegable.Página de la falla de registro — Seleccione una página de registro que visualice al cliente si la autenticación Web falla.Página del logout — Seleccione una página de registro que visualice al cliente

	cuando el sistema de los de los registros de usuario. • Externo (reoriente al servidor externo) URL — Ingrese el URL del servidor externo.
Envíe por correo electrónico la entrada	Visualizaciones si usted selecciona el passthrough de la red. Si usted selecciona esta opción, le indican para su dirección de correo electrónico mientras que conecta con la red.

Nota: En la versión de software 4.1.185.0 del regulador o más adelante, CKIP se soporta para el uso solamente con el WEP estático. No se soporta para el uso con el WEP dinámico. Por lo tanto, un cliente de red inalámbrica que se configura para utilizar CKIP con el WEP dinámico no puede asociarse a un Wireless LAN que se configura para CKIP. Cisco recomienda que usted utiliza o el WEP dinámico sin CKIP (que es menos seguro) o WPA/WPA2 con TKIP o el AES (que sean más seguros).

Capa 2 del regulador del Wireless LAN – Matriz de compatibilidad de la Seguridad de la capa 3

Cuando usted configura la Seguridad en un Wireless LAN, acode 2 y acode 3 métodos de seguridad puede ser utilizado en la conjunción. Sin embargo, no todos los métodos de seguridad de la capa 2 se pueden utilizar con todos los métodos de seguridad de la capa 3. Esta tabla muestra la matriz de compatibilidad para los métodos de seguridad de la capa 2 y de la capa 3 soportados en el regulador del Wireless LAN.

Mecanismo de seguridad de la capa 2	Mecanismo de seguridad de la 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	Passthrough de la red	No válido
WPA-PSK/WPA2-PSK	Passthrough de la red	Válido
WPA+WPA2	La red condicional reorienta	Válido
WPA+WPA2	La red de la	Válido

	página del chapoteo reorienta	
WPA+WPA2	VPN-passthrough	Válido
802.1x	Ninguno	Válido
802.1x	Autenticación Web	No válido
802.1x	Passthrough de la red	No válido
802.1x	La red condicional reorienta	Válido
802.1x	La red de la página del chapoteo reorienta	Válido
802.1x	VPN-passthrough	Válido
WEP estático	Ninguno	Válido
WEP estático	Autenticación Web	Válido
WEP estático	Passthrough de la red	Válido
WEP estático	La red condicional reorienta	No válido
WEP estático	La red de la página del chapoteo reorienta	No válido
WEP estático	VPN-passthrough	Válido
802.1x Static-WEP+	Ninguno	Válido
802.1x Static-WEP+	Autenticación Web	No válido
802.1x Static-WEP+	Passthrough de la red	No válido
802.1x Static-WEP+	La red condicional reorienta	No válido
802.1x Static-WEP+	La red de la página del chapoteo reorienta	No válido
802.1x Static-WEP+	VPN-passthrough	No válido
CKIP	Ninguno	Válido

CKIP	Autenticación Web	Válido
CKIP	Passthrough de la red	Válido
CKIP	La red condicional reorienta	No válido
CKIP	La red de la página del chapoteo reorienta	No válido
CKIP	VPN-passthrough	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 del controlador LAN de la tecnología inalámbrica de Cisco, versión 7.0.116.0
- Regulador del Wireless LAN (WLC) FAQ
- Soporte Técnico y Documentación - Cisco Systems