ACS versión 5.2 y WLC por por el ejemplo de la configuración de autenticación de la red inalámbrica (WLAN)

ID del Documento: 118661

Actualizado: De enero el 14 de 2015

Contribuido por Brahadesh Srinivasaraghavan, ingeniero de Cisco TAC.

Productos Relacionados

- Wireless, LAN (WLAN)

Contenido

Introducción

Este documento proporciona un ejemplo de configuración para restringir por usuario el acceso a un Wireless LAN (red inalámbrica (WLAN)) basado en el Service Set Identifier (SSID).

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cómo configurar el regulador del Wireless LAN (WLC) y el Lightweight Access Point (REVESTIMIENTO) para la operación básica
- Cómo configurar el Cisco Secure Access Control Server (ACS)
- Métodos del protocolo (LWAPP) y de la seguridad de red inalámbrica del Lightweight Access Point

Componentes Utilizados

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

- WLC de las Cisco 5500 Series que funciona con la versión de firmware 7.4.110
- REVESTIMIENTO de las Cisco 1142 Series
- Versión del servidor 5.2.0.26.11 del Cisco Secure ACS

Configurar

Para configurar los dispositivos para esta configuración, usted necesita:

1. Configure el WLC para los dos WLAN y servidores de RADIUS.
2. Configure el Cisco Secure ACS.
3. Configure a los clientes de red inalámbrica y verifique la configuración.

Configure el WLC

Complete estos pasos para configurar el WLC para esta configuración:

1. Configure el WLC para remitir los credenciales de usuario a un servidor RADIUS externo. El servidor RADIUS externo (Cisco Secure ACS en este caso) después valida los credenciales de usuario y proporciona el acceso a los clientes de red inalámbrica. Complete estos pasos: Seleccione la **Seguridad > la autenticación de RADIUS del** regulador GUI para visualizar la página de los servidores de autenticación de RADIUS.Haga clic **nuevo** para definir los parámetros del servidor de RADIUS.Estos parámetros incluyen la dirección IP, el secreto compartido, el número del puerto, y el estado del servidor del servidor de RADIUS. El checkboxes del usuario de la red y de la Administración determina si la autenticación basada en RADIUS solicita la Administración y los usuarios de la red. Este ejemplo utiliza el Cisco Secure ACS como el servidor de RADIUS con la dirección IP 10.104.208.56.Haga clic en Apply (Aplicar).
2. Complete estos pasos para configurar la una red inalámbrica (WLAN) para el empleado con el **empleado** SSID y la otra red inalámbrica (WLAN) para los contratistas con el **contratista** SSID. Haga clic los **WLAN del** regulador GUI para crear una red inalámbrica (WLAN). La ventana del WLAN aparece. Esta ventana enumera los WLAN configurados en el regulador.Tecleo **nuevo** para configurar una nueva red inalámbrica (WLAN).Este ejemplo

crea una red inalámbrica (WLAN) nombrada Employee y el ID DE WLAN es 1. tecleos **se aplica**.Seleccione la **red inalámbrica (WLAN) > editan la** ventana y definen los parámetros específicos a la red inalámbrica (WLAN): De la ficha de seguridad de la capa 2, seleccione el **802.1x**. Por abandono, la opción de seguridad de la capa 2 es 802.1x. Esto habilita 802.1 autenticaciones del protocolo de autenticación x/Extensible (EAP) para la red inalámbrica (WLAN).De los servidores de AAA tabule, seleccione al servidor de RADIUS apropiado de la lista desplegable bajo los servidores de RADIUS. Los otros parámetros se pueden modificar basaron en el requisito de la red WLAN. Haga clic en Apply (Aplicar).Semejantemente, para crear una red inalámbrica (WLAN) para los contratistas, relance los pasos b a D.

Configure el Cisco Secure ACS

En el servidor del Cisco Secure ACS usted necesita:

1. Configure el WLC como cliente AAA.
2. Cree la base de datos de usuarios (credenciales) para la autenticación SSID-basada.
3. Habilite la autenticación EAP.

Complete estos pasos en el Cisco Secure ACS:

1. Para definir el regulador como cliente AAA en el servidor ACS, seleccione los **recursos de red > los dispositivos de red y a los clientes AAA del** ACS GUI. Bajo los dispositivos de red y los clientes AAA**, el** tecleo **crea.**
2. Cuando aparece la página de la configuración de red, defina el nombre del WLC, la dirección IP, y el secreto compartido y el método de autentificación (RADIUS).
3. Seleccione a los **usuarios y la identidad salva > los grupos de la identidad del** ACS GUI. Cree a los grupos correspondientes para el empleado y el contratista y el tecleo **crean**. En este ejemplo nombran al grupo creado Employees.
4. **Los usuarios** selectos **y la identidad salva > los almacenes internos de la identidad**. Haga clic **crean** y ingresan el nombre de usuario. Coloqúelos en el grupo correcto, defina su contraseña, y el tecleo **somete**. En este ejemplo crean a un usuario nombrado employee1 en el empleado del grupo. Semejantemente, cree a un usuario nombrado contractor1 bajo los contratistas del grupo.
5. Seleccione los **elementos de la directiva > los estados de la red > los filtros de la estación terminal**. Haga clic en **Crear**.Ingrese un nombre significativo y bajo lengueta del **IP Address** ingrese el IP Address del WLC. En este ejemplo los nombres son empleado y contratista.Bajo lengueta CLI/DNIS, deje el CLI como - y ingrese el DNIS como *<SSID>. En este ejemplo, el campo DNIS se ingresa como *Employee como para este fin el filtro de la estación se utiliza para restringir el acceso solamente al empleado WLAN. El atributo DNIS define el SSID que se permite al usuario acceder. El WLC envía el SSID en el atributo DNIS al servidor de RADIUS.Relance los mismos pasos para el filtro de la estación terminal del contratista.
6. Seleccione los **elementos de la directiva > la autorización y los permisos > los perfiles del acceso a la red > de la autorización**. Debe haber un perfil predeterminado para el acceso del permiso.
7. **Las políticas de acceso > el acceso** selectos **mantiene > las reglas de selección del servicio**. El tecleo **personaliza**. Agregue cualquier condición conveniente. Este ejemplo utiliza el protocolo como radio como la condición que corresponde con.Haga clic en **Crear**. Nombre la regla. Seleccione el **protocolo** y seleccione el **radio.**Bajo **resultados**, elija el servicio

apropiado del acceso. En este ejemplo, se deja como **acceso de red predeterminada.**

8. **Las políticas de acceso > el acceso** selectos **mantiene > acceso > identidad de red predeterminada**. Elija la solas selección del resultado y **fuente de la identidad** como usuarios internos.Seleccione las **políticas de acceso > el acceso mantiene > acceso > autorización de red predeterminada.** El tecleo **personaliza** y agrega las condiciones personalizadas. Este ejemplo utiliza al grupo de la identidad, NDG: Tipo de dispositivo, y filtro de la estación terminal en esa orden.Haga clic en **Crear**. Nombre la regla y elija al grupo apropiado de la identidad bajo todos los grupos. En este ejemplo es empleado.Haga clic el botón de radio del **filtro de Stn del final del empleado** o ingrese el nombre que usted entra en Step1b en sección “configuración del WLC”.Marque el cuadro de **verificación de acceso del permiso**.Relance los mismos pasos arriba para las reglas del contratista también. Asegúrese que la acción predeterminada sea **negar el acceso**.Una vez que usted ha completado el paso e, sus reglas deben parecer este ejemplo:

Esto concluye la configuración. Después de esta sección, el cliente necesita ser configurado por consiguiente con el SSID y los parámetros de seguridad para conectar.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Discusiones relacionadas de la comunidad del soporte de Cisco

La comunidad del soporte de Cisco es un foro para que usted haga y conteste a las preguntas, las sugerencias de la parte, y colabora con sus pares.

Actualizado: De enero el 14 de 2015
ID del Documento: 118661