Filtros MAC con el ejemplo de configuración de los reguladores del Wireless LAN (WLCs)

Contenido

Introducción

Este documento explica cómo configurar los filtros MAC con controladores de LAN inalámbricos (WLC) con un ejemplo de configuración. Este documento también explica cómo autorizar Lightweight Access Points (LAP) en un servidor AAA.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimientos básicos de la configuración de LAPs y WLCs de Cisco
- Conocimiento básico de las soluciones acerca de la seguridad del Cisco Unified Wireless

Componentes Utilizados

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

hardware.

- WLC de Cisco 4400 que funciona con la versión de software 5.2.178.0
- Revestimientos de las Cisco 1230AG Series
- adaptador de red inalámbrica de cliente del a/b/g del 802.11 con el firmware 4.4
- Utilidad Aironet Desktop versión 4.4 (ADU)

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.

Filtro de la dirección MAC (autenticación de MAC) en el WLCs

Cuando usted crea un filtro de la dirección MAC en el WLCs, conceden los usuarios o el acceso negado a la red WLAN se basa en la dirección MAC del cliente que utilizan.

Hay dos tipos de autenticación de MAC que se soportan en el WLCs:

- Autenticación del MAC local
- Autenticación de MAC usando un servidor de RADIUS

Con la autenticación del MAC local, las direcciones MAC del usuario se salvan en una base de datos en el WLC. Cuando un usuario intenta acceder la red inalámbrica (WLAN) que se configura para el MAC que filtra, el MAC Address del cliente se valida contra la base de datos local en el WLC, y conceden el cliente el acceso a la red inalámbrica (WLAN) si la autenticación es acertada.

Por abandono, los soportes de base de datos local del WLC hasta 512 entradas de usuario.

La base de datos de usuarios locales se limita a un máximo de 2048 entradas. La base de datos local salva las entradas para estos elementos:

- Usuarios de la administración local, que incluye a los embajadores del pasillo
- Usuarios de la red local, que incluye a los Usuarios invitados
- Entradas del filtro MAC
- Entradas de la lista de la exclusión
- Entradas de la lista de la autorización del Punto de acceso

Junto, todos estos tipos de usuarios no pueden exceder el tamaño de la base de datos configurado.

Para aumentar la base de datos local, utilice este comando del CLI:

```
<Cisco Controller>config database size ?
<count>        Enter the maximum number of entries (512-2048)
```

Alternativamente, la autenticación de la dirección MAC se puede también realizar usando un servidor de RADIUS. La única diferencia es que la base de datos de la dirección MAC de los

usuarios está salvada en el servidor de RADIUS en vez del WLC. Cuando una base de datos de usuarios se salva en un servidor de RADIUS el WLC adelante la dirección MAC del cliente al servidor de RADIUS para la validación del cliente. Entonces, el servidor de RADIUS valida la dirección MAC basada en la base de datos que tiene. Si la autenticación de cliente es acertada, conceden el cliente el acceso a la red inalámbrica (WLAN). Cualquier servidor de RADIUS que soporte la autenticación de la dirección MAC puede ser utilizado.

Autenticación del MAC local de la configuración en el WLCs

Complete estos pasos para configurar la autenticación del MAC local en el WLCs:

1. Configure una red inalámbrica (WLAN) y habilite la filtración MAC
2. Configure la base de datos local en el WLC con los MAC Address del clienteNote: Antes de que usted configure la autenticación de MAC, usted debe configurar el WLC para la operación básica y registrar los revestimientos al WLC. Este documento asume que el WLC está configurado ya para la operación básica y que los revestimientos están registrados al WLC. Si usted es usuario nuevo que intenta configurar el WLC para la operación básica con los revestimientos, refiera al registro ligero AP (REVESTIMIENTO) a un regulador del Wireless LAN (WLC).Note: No hay configuración especial necesaria en el cliente de red inalámbrica para soportar la autenticación de MAC.

Configure una red inalámbrica (WLAN) y habilite la filtración MAC

Complete estos pasos para configurar una red inalámbrica (WLAN) con la filtración MAC:

1. 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.
2. Tecleo **nuevo** para configurar una nueva red inalámbrica (WLAN).En este ejemplo, la red inalámbrica (WLAN) se nombra *MAC-WLAN* y el ID DE WLAN es *1.*
3. Haga clic en Apply (Aplicar).
4. En la red inalámbrica (WLAN) > edite la ventana, definen los parámetros específicos a la red inalámbrica (WLAN).Bajo las políticas de seguridad > Seguridad de la capa 2, marque la casilla de verificación de **filtración MAC**.Esto habilita la autenticación de MAC para la red inalámbrica (WLAN).Bajo las políticas generales > nombre de la interfaz, seleccione la interfaz a la cual se asocia la red inalámbrica (WLAN).En este ejemplo, la red inalámbrica (WLAN) se asocia a la interfaz de administración.Seleccione los otros parámetros, que dependen de los requisitos de diseño de la red inalámbrica (WLAN).Haga clic en Apply (Aplicar).

El siguiente paso es configurar la base de datos local en el WLC con los MAC Address del cliente.

Refiera a los VLA N en el ejemplo de configuración de los reguladores del Wireless LAN para la información sobre cómo configurar las interfaces dinámicas (VLA N) en el WLCs.

Configure la base de datos local en el WLC con los MAC Address del cliente

Complete estos pasos para configurar la base de datos local con un MAC Address del cliente en el WLC:

1. Haga clic la **Seguridad del** regulador GUI, y después haga clic el **MAC que filtra del** menú del lado izquierdo.La ventana de filtración MAC aparece.
2. Haga clic **nuevo** para crear una entrada de MAC Address de la base de datos local en el WLC.
3. En el MAC filtra > nueva ventana, ingresa el MAC address, el nombre del perfil, la descripción y el nombre de la interfaz para el cliente.Aquí tiene un ejemplo:
4. Haga clic en Apply (Aplicar).
5. Relance los pasos 2-4 para agregar a más clientes a la base de datos local.Ahora, cuando los clientes conectan con esta red inalámbrica (WLAN), el WLC valida la dirección MAC de los clientes contra la base de datos local y si la validación es acertada, conceden el cliente el acceso a la red.**Note**: En este ejemplo, solamente un filtro de la dirección MAC sin cualquier otro mecanismo de seguridad de la capa 2 fue utilizado. Cisco recomienda que la autenticación de la dirección MAC se debe utilizar junto con otros métodos de seguridad de la capa 2 o de la capa 3. No es recomendable utilizar solamente la autenticación de la dirección MAC para asegurar su red WLAN porque no proporciona un mecanismo de fuerte seguridad.

Autenticación de MAC de la configuración usando un servidor de RADIUS

Complete estos pasos para configurar la autenticación de MAC usando un servidor de RADIUS. En este ejemplo, el servidor del Cisco Secure ACS se utiliza como el servidor de RADIUS.

1. Configure una red inalámbrica (WLAN) y habilite la filtración MAC
2. Configure al servidor de RADIUS con los MAC Address del cliente

Configure una red inalámbrica (WLAN) y habilite la filtración MAC

Complete estos pasos para configurar una red inalámbrica (WLAN) con la filtración MAC:

1. 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.
2. Tecleo **nuevo** para configurar una nueva red inalámbrica (WLAN).En este ejemplo, la red inalámbrica (WLAN) se nombra *MAC-ACS-WLAN* y el ID DE WLAN es *2.*
3. Haga clic en Apply (Aplicar).
4. En la red inalámbrica (WLAN) > edite la ventana, definen los parámetros específicos a la red inalámbrica (WLAN).Bajo las políticas de seguridad > Seguridad de la capa 2, marque la casilla de verificación de **filtración MAC**.Esto habilita la autenticación de MAC para la red inalámbrica (WLAN).Bajo las políticas generales > nombre de la interfaz, seleccione la interfaz a la cual se asocia la red inalámbrica (WLAN).Bajo los servidores de RADIUS, seleccione al servidor de RADIUS que será utilizado para la autenticación de MAC.**Note**: Antes de que usted pueda seleccionar al servidor de RADIUS de la red inalámbrica (WLAN) > edite la ventana, usted debe definir al servidor de RADIUS en la ventana de la Seguridad > de la autenticación de RADIUS y habilitar al servidor de RADIUS.Seleccione los otros parámetros, que dependen de los requisitos de diseño de la red inalámbrica (WLAN).Haga clic en Apply (Aplicar).
5. **Seguridad del** tecleo **> filtración MAC**.

6. En la ventana de filtración MAC, elija el tipo de servidor de RADIUS bajo modo de compatibilidad RADIUS.Este ejemplo utiliza Cisco ACS.
7. Del delimitador MAC tire hacia abajo el menú, eligen el delimitador MAC.Este ejemplo utiliza los dos puntos.
8. Haga clic en Apply (Aplicar).

El siguiente paso es configurar al servidor ACS con los MAC Address del cliente.

Configure al servidor de RADIUS con los MAC Address del cliente

Complete estos pasos para agregar una dirección MAC al ACS:

1. Defina el WLC como cliente AAA en el servidor ACS. Haga clic la **configuración de red del** ACS GUI.
2. Cuando aparece la ventana de la configuración de red, defina el nombre del WLC, de la dirección IP, del secreto compartido y del método de autentificación (Cisco Aironet RADIUS o Airespace RADIUS).Refiera a la documentación del fabricante para otros servidores de autenticación NON-ACS.**Note**: La clave secreta compartida que usted configura en el WLC y el servidor ACS debe hacer juego. El secreto compartido es con diferenciación entre mayúsculas y minúsculas.
3. Del menú principal ACS, **configuración de usuario del** tecleo.
4. En el cuadro de texto del usuario, ingrese el MAC address para agregar a la base de datos de usuarios.**Note**: La dirección MAC debe estar exactamente mientras que es enviada por el WLC para el nombre de usuario y la contraseña. Si la autenticación falla, marque el registro de los intentos fallidos para ver cómo el MAC es señalado por el WLC. No corte y pegar la dirección MAC, como esto puede introducir los caracter fantasmas.
5. En la ventana de la configuración de usuario, ingrese el MAC address en el cuadro de texto de la contraseña Seguro-PAP.**Note**: La dirección MAC debe estar exactamente mientras que es enviada por el WLC para el nombre de usuario y la contraseña. Si la autenticación falla, marque el registro de los intentos fallidos para ver cómo el MAC es señalado por el AP. No corte y pegar la dirección MAC, como esto puede introducir los caracter fantasmas.
6. Haga clic en Submit (Enviar).
7. Relance los pasos 2-5 para agregar a más usuarios a la base de datos ACS.Ahora, cuando los clientes conectan con esta red inalámbrica (WLAN), el WLC pasa las credenciales al servidor ACS. El servidor ACS valida las credenciales contra la base de datos ACS. Si el MAC Address del cliente está presente en la base de datos, el servidor de RADIUS ACS vuelve un éxito de la autenticación al WLC y concederán el cliente el acceso a la red inalámbrica (WLAN).

Utilice el CLI para configurar el filtro MAC en el WLC

Este documento discutido previamente cómo utilizar el WLC GUI para configurar los filtros MAC. Usted puede también utilizar el CLI para configurar los filtros MAC en el WLC. Usted puede utilizar estos comandos para configurar el filtro MAC en el WLC:

- Publique el comando de mac-**filtración wlan del wlan_id del permiso de los config** para habilitar la filtración MAC. el bEnter el comando **wlan de la demostración** para verificar que usted tenga filtración MAC habilitó para la red inalámbrica (WLAN).
- **comando add del macfilter de los config**:**El comando add del macfilter de los config** le deja

agregar un macfilter, interfaz, descripción, y así sucesivamente.Utilice el **comando add del macfilter de los config** para crear una entrada del filtro MAC en el controlador LAN de la tecnología inalámbrica de Cisco. Utilice este comando para agregar a un cliente localmente a un Wireless LAN en el controlador LAN de la tecnología inalámbrica de Cisco. Este filtro desvía el proceso de autenticación de RADIUS.

```
config macfilter add MAC_address wlan_id [interface_name]
[description] [IP address]
```

Ejemplo: Ingrese una correspondencia de direcciones estática MAC-a-IP. Esto se puede hacer para apoyar a un *cliente pasivo*, es decir, uno que no utilice el DHCP y no transmita los paquetes del IP no solicitados.

```
>config macfilter add 00:E0:77:31:A3:55 1 lab02 "labconnect" 10.92.125.51
```

- **comando ip-address del macfilter de los configEl comando ip-address del macfilter de los config** le deja asociar un MAC-filtro existente a una dirección IP. Utilice este comando para configurar una dirección IP en la base de datos del filtro del MAC local:

```
config macfilter ip-address
 MAC_address IP address
```

Ejemplo:

```
>config macfilter add 00:E0:77:31:A3:55 1 lab02 "labconnect" 10.92.125.51
```

Configure un descanso para los clientes discapacitados

Usted puede configurar un descanso para los clientes discapacitados. Inhabilitan a los clientes que no pueden autenticar tres veces durante las tentativas de asociarse automáticamente de tentativas más futuras de la asociación. Después del período de agotamiento del tiempo de espera expira, se permite revisar la autenticación hasta que asocie o falle la autenticación y se excluye al cliente otra vez.

Ingrese el **comando timeout wlan del wlan_id del exclusionlist de los config** para configurar el descanso para los clientes discapacitados. El valor de agotamiento del tiempo puede ser a partir 1 a 65535 segundos, o usted puede ingresar 0 para inhabilitar permanentemente al cliente.

Verificación

Utilice estos comandos para verificar si el filtro MAC se configura correctamente:

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **muestre el resumen del macfilter** — Visualiza un resumen de todas las entradas del filtro MAC.
- **muestre a detalle del macfilter la *dirección MAC* <client >** — Visualización detallada de una entrada del filtro MAC.

Aquí está un ejemplo del **comando summary del macfilter de la demostración**:

```
(Cisco Controller) >show macfilter summary

MAC Filter RADIUS Compatibility mode..... Cisco ACS
MAC Filter Delimiter..................... None
```

```
Local Mac Filter Table

MAC Address               WLAN Id          Description
-----------------------   --------------   --------------------------------
00:40:96:ac:e6:57           1              Guest


(Cisco Controller) >show macfilter detail 00:40:96:ac:e6:57
```

Aquí está un ejemplo del **comando detail del macfilter de la demostración**:

```
(Cisco Controller) >show macfilter detail 00:40:96:ac:e6:57

MAC Address..................................... 00:40:96:ac:e6:57
WLAN Identifier................................. 1
Interface Name.................................. mac-client
Description..................................... Guest
```

Troubleshooting

Usted puede utilizar estos comandos de resolver problemas su configuración:

Note: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- **haga el debug del aaa todo el permiso** — Proporciona el debugging de todos los mensajes AAA.
- **<Client-MAC-direccionamiento *xx de las* direcciones MAC del debug*: xx: xx: xx: xx: xx* >** — Para configurar el debugging MAC, utilice el **comando mac del debug**.

Aquí está un ejemplo del **comando debug aaa all enable**:

```
Wed May 23 11:13:55 2007: Looking up local blacklist 004096ace657
Wed May 23 11:13:55 2007: Looking up local blacklist 004096ace657
Wed May 23 11:13:55 2007: User 004096ace657 authenticated
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 Returning AAA Error 'Success' (0)
                          for mobile 00:40:96:ac:e6:57
Wed May 23 11:13:55 2007: AuthorizationResponse: 0xbadff97c
Wed May 23 11:13:55 2007: structureSize.............................76
Wed May 23 11:13:55 2007: resultCode...............................0
Wed May 23 11:13:55 2007: protocolUsed.............................0x00000008
Wed May 23 11:13:55 2007: proxyState................................
                                00:40:96:AC:E6:57-00:00
Wed May 23 11:13:55 2007: Packet contains 2 AVPs:
Wed May 23 11:13:55 2007:     AVP[01] Service-Type..........................
                                    0x0000000a (10) (4 bytes)
Wed May 23 11:13:55 2007:     AVP[02] Airespace / Interface-Name.............
                                    staff-vlan (10 bytes)
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 processing avps[0]: attribute 6
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 processing avps[1]: attribute 5
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 Applying new AAA override for
                          station 00:40:96:ac:e6:57
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 Override values for station 00:40:96:ac:e6:57
source: 2, valid bits: 0x200 qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff,
sessionTimeout: -1dataAvgC: -1, rTAvgC: -1, dataBurstC:

-1, rTimeBurstC: -1vlanIfName: 'mac-client'
```

Cuando un cliente de red inalámbrica no está presente en la base de datos de la dirección MAC en el WLC (base de datos local) o en el servidor de RADIUS intenta asociarse a la red

inalámbrica (WLAN), excluirán a ese cliente. Aquí está un ejemplo del **comando debug aaa all enable** para una autenticación de MAC fracasada:

```
Wed May 23 11:05:06 2007: Unable to find requested user entry for 004096ace657
Wed May 23 11:05:06 2007: AuthenticationRequest: 0xa620e50
Wed May 23 11:05:06 2007: Callback.....................................0x807e724
Wed May 23 11:05:06 2007: protocolType.................................0x00000001
Wed May 23 11:05:06 2007: proxyState...................................
                                00:40:96:AC:E6:57-00:00
Wed May 23 11:05:06 2007: Packet contains 14 AVPs (not shown)
Wed May 23 11:05:06 2007: 00:40:96:ac:e6:57 Returning AAA Error 'No Server' (-7)
                          for mobile 00:40:96:ac:e6:57
Wed May 23 11:05:06 2007: AuthorizationResponse: 0xbadff7e4
Wed May 23 11:05:06 2007: structureSize................................28
Wed May 23 11:05:06 2007: resultCode...................................-7
Wed May 23 11:05:06 2007: protocolUsed.................................0xffffffff
Wed May 23 11:05:06 2007: proxyState...................................
                                00:40:96:AC:E6:57-00:00
Wed May 23 11:05:06 2007: Packet contains 0 AVPs:
```

Rechazan a los clientes de red inalámbrica que intentan autenticar por la dirección MAC; El informe de la autenticación fallida muestra los errores internos

Cuando usted utiliza el ACS 4.1 que se ejecuta en un Servidor de Enterprise de Microsoft Windows 2003, rechazan a los clientes que intentan autenticar por la dirección MAC. Esto ocurre cuando un cliente AAA envía el valor de atributo Service-Type=10 al servidor de AAA. Esto está debido al Id. de bug Cisco CSCsh62641 (clientes registrados solamente). Los clientes AAA afectados por este bug incluyen el WLCs y el Switches que utilizan puente de la autenticación de MAC.

Las soluciones son:

- Retroceda a ACS 4.0.o
- Agregue las direcciones MAC que se autenticarán a una protección del acceso a la red (SIESTA) bajo la tabla interna de la dirección MAC ACS DB.

No capaz de agregar un filtro MAC usando el WLC GUI

Esto puede suceder becaue del Id. de bug Cisco CSCsj98722 (clientes registrados solamente). El bug se repara en la versión 4.2 del código. Si usted es versiones corrientes anterior de 4.2, usted puede actualizar el firmware a 4.2 o utilizar estas dos soluciones alternativas para este problema.

- Utilice el CLI para configurar el filtro MAC con este comando:

  config macfilter add <MAC address> <WLAN ID#> <Interface>
- De la red GUI del regulador, elija **cualquier WLAN** conforme a la ficha de seguridad y ingrese el MAC address que se filtrará.

Cliente silencioso no colocado en el estado de funcionamiento

Si el DHCP requerido no se configura en el regulador, los AP aprenden la dirección IP de los clientes de red inalámbrica cuando los clientes de red inalámbrica envían el primer paquete del IP o ARP. Si los clientes de red inalámbrica son dispositivos pasivos, por ejemplo, los dispositivos que no inician una comunicación, después los AP no pueden aprender la dirección IP de los dispositivos de red inalámbrica. Como consecuencia, el regulador espera diez segundos el cliente para enviar un paquete del IP. Si no hay respuesta del paquete del cliente, entonces el regulador cae cualquier paquete a los clientes de red inalámbrica pasivos. Este problema se documenta en

el Id. de bug Cisco CSCsq46427 (el clientes registrados solamente)

Mientras que una solución alternativa recomendada para los dispositivos pasivos como las impresoras, PLC inalámbrico bombea y así sucesivamente, usted necesita fijar la red inalámbrica (WLAN) para el MAC que filtra y hacer la invalidación AAA marcar para permitir que estos dispositivos sean conectados.

Un filtro de la dirección MAC se puede crear en el regulador que asocia la dirección MAC del dispositivo de red inalámbrica a una dirección IP.

Note: Esto requiere la dirección MAC que filtra para ser habilitado en la configuración de la red inalámbrica (WLAN) para la Seguridad de la capa 2. También requiere `permite que el AAA Overide` sea habilitado en las configuraciones anticipadas de la configuración de la red inalámbrica (WLAN).

Del CLI, ingrese este comando para crear el filtro del MAC address:

```
config macfilter add <MAC address>  <WLAN ID#> <Interface>
```

Aquí tiene un ejemplo:

```
config macfilter add <MAC address>  <WLAN ID#> <Interface>
```

Información Relacionada

- ACL en el ejemplo de la configuración de controlador del Wireless LAN
- Autenticación en los ejemplos de configuración de los reguladores del Wireless LAN
- Ejemplo de Configuración de VLANs en Controladores de LAN Inalámbrica
- Guía de Configuración del Controlador de LAN Inalámbrica de Cisco, versión 4.1
- Página de soporte de tecnología de red inalámbrica
- Soporte Técnico y Documentación - Cisco Systems