PEAP y EAP-FAST con ACS 5.2 y el ejemplo de la configuración de controlador del Wireless LAN

Contenido

Introducción

Este documento explica cómo configurar el controlador de LAN inalámbrico (WLC) para la autenticación EAP (Extensible Authentication Protocol) con el uso de un servidor RADIUS externo como Access Control Server (ACS) 5.2.

prerrequisitos

Requisitos

Aseegurese que usted cumple estos requisitos antes de que usted intente esta configuración:

- Tenga un conocimiento básico del WLC y de los Puntos de acceso ligeros (los revestimientos)
- Tenga un conocimiento funcional del servidor de AAA
- Tenga un conocimiento completo de las redes inalámbricas y de los problemas de seguridad de red inalámbrica

Componentes Utilizados

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

- WLC de Cisco 5508 que funciona con la versión de firmware 7.0.220.0
- REVESTIMIENTO de las Cisco 3502 Series
- Supplicant del natural de Microsoft Windows 7 con la versión del driver 14.3 de Intel 6300-N
- Cisco Secure ACS que funciona con la versión 5.2
- Cisco 3560 Series Switch

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 Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Éstos son los detalles de la configuración de los componentes usados en este diagrama:

- La dirección IP del servidor ACS (RADIUS) es 192.168.150.24.
- La Administración y el direccionamiento de la interfaz del AP manager del WLC es 192.168.75.44.
- Los servidores DHCP dirigen 192.168.150.25.

- El VLA N 253 se utiliza en esta configuración. Ambos usuarios conectan con el mismo SSID “goa”. Sin embargo, el user1 se configura para autenticar usando PEAP-MSCHAPv2 y user2 usando el EAP-FAST.
- Asignarán los usuarios en el VLA N 253:VLA N 253: 192.168.153.x/24. Gateway: 192.168.153.1VLA N 75: 192.168.75.x/24. Gateway: 192.168.75.1

Suposición

- El Switches se configura para todos los VLA N de la capa 3.
- Asignan el servidor DHCP un alcance de DHCP.
- La Conectividad de la capa 3 existe entre todos los dispositivos en la red.
- El REVESTIMIENTO se une a ya al WLC.
- Cada VLA N tiene máscara de /24.
- El ACS 5.2 tiene un certificado autofirmado instalado.

Pasos de configuración

Esta configuración se separa en tres pasos de alto nivel:

1. Configure al servidor de RADIUS.
2. Configure el WLC.
3. Configure la utilidad del cliente de red inalámbrica.

Configure al servidor de RADIUS

La configuración de servidor de RADIUS se divide en cuatro pasos:

1. Recursos de red de la configuración.
2. Usuarios de la configuración.
3. Defina los elementos de la directiva.
4. Aplique las políticas de acceso.

El ACS 5.x es un Sistema de control de acceso del policy basado. Es decir, el ACS 5.x utiliza un modelo basado en las reglas de la directiva en vez del modelo basado en el grupo usado en las versiones 4.x.

El modelo basado en las reglas de la directiva ACS 5.x proporciona un control de acceso más potente y más flexible comparado al más viejo acercamiento basado en el grupo.

En el más viejo modelo basado en el grupo, un grupo define la directiva porque contiene y ata juntos tres tipos de información:

- Información de identidad - Esta información se puede basar en la calidad de miembro en los grupos AD o LDAP o una asignación estática para los usuarios de ACS internos.
- Otras restricciones o condiciones - Restricciones de tiempo, restricciones del dispositivo, y así sucesivamente.
- Permisos - Niveles de privilegio del ® de los VLA N o del Cisco IOS.

El modelo de la directiva ACS 5.x se basa en las reglas de la forma:

- Si entonces resulta la condición

Por ejemplo, utilizamos la información descrita para el modelo basado en el grupo:

- Si identidad-condición, autorización-perfil de la restricción-condición entonces.

Como consecuencia, esto nos da la flexibilidad para limitar bajo qué condiciones permiten el usuario que accedan la red así como se permite qué nivel de la autorización cuando se cumplen las condiciones específicas.

Recursos de red de la configuración

En esta sección, configuramos al cliente AAA para el WLC en el servidor de RADIUS.

Este procedimiento explica cómo agregar el WLC como cliente AAA en el servidor de RADIUS de modo que el WLC pueda pasar los credenciales de usuario al servidor de RADIUS.

Complete estos pasos:

1. Del ACS GUI, vaya a los **recursos de red >** a los **grupos de dispositivos de red >** a la **ubicación**, y el tecleo **crea** (en la parte inferior).
2. Agregue los campos obligatorios, y el tecleo **somete**.Usted ahora verá esta pantalla:
3. **El tipo de dispositivo del** tecleo **> crea**.
4. Haga clic en Submit (Enviar). Usted ahora verá esta pantalla:
5. Vaya a los **recursos de red >** a los **dispositivos de red y a los clientes AAA**.
6. El tecleo **crea**, y completa los detalles como se muestra aquí:
7. Haga clic en Submit (Enviar). Usted ahora verá esta pantalla:

Usuarios de la configuración

En esta sección, crearemos a los usuarios locales en el ACS. Asignan ambos usuarios (user1 y user2) en los “usuarios de red inalámbrica llamados grupo”.

1. Vaya a los **usuarios y la identidad salva >** los **grupos de la identidad > crea**.
2. Una vez que usted tecleo **somete**, la página parecerá esto:
3. Cree el **user1 de los** usuarios y **user2**, y asígnelos al grupo de los “usuarios de red inalámbrica”.Haga clic a los **usuarios y la identidad salva >** los **grupos de la identidad >** Users **> crea**.Semejantemente, cree user2.La pantalla parecerá esto:

Defina los elementos de la directiva

Verifique que el **acceso del permiso** esté fijado.

Aplique las políticas de acceso

En esta sección, seleccionaremos qué métodos de autentificación deben ser utilizados y cómo las reglas deben ser configuradas. Crearemos basado en las reglas los pasos anteriores.

Complete estos pasos:

1. Va a las **políticas de acceso >** al **acceso mantiene >** el **acceso de red predeterminada >**

edita: "Acceso de red predeterminada".
2. Seleccione que el método EAP usted como los clientes de red inalámbrica autenticaría. En este ejemplo, utilizamos el **MSCHAPv2** y el **EAP-FAST PEAP-**.
3. Haga clic en Submit (Enviar).
4. Verifique al grupo de la identidad que usted ha seleccionado. En este ejemplo, utilizamos a los **usuarios internos**, que creamos en el ACS. Guarde los cambios.
5. Para verificar el perfil de la autorización, vaya a las **políticas de acceso** > al **acceso mantiene** > **acceso** > **autorización de red predeterminada**.Usted puede personalizar bajo qué condiciones usted no prohibirá a acceso del usuario a la red y qué perfil de la autorización (atributos) usted pasará autenticado una vez. Este granularity está solamente disponible en ACS 5.x. En este ejemplo, seleccionamos la **ubicación**, el **tipo de dispositivo**, el **protocolo**, el **grupo de la identidad**, y el **método de autenticación EAP**.
6. Haga Click en OK, y **cambios de la salvaguardia**.
7. El siguiente paso es crear una regla. Si no se define ningunas reglas, no prohiben el cliente el acceso sin ningunas condiciones.El tecleo **crea** > **Rule-1**. Esta regla está para los usuarios en el grupo "usuarios de red inalámbrica".
8. Guarde los cambios. La pantalla parecerá esto:Si usted quiere a los usuarios que no corresponden con las condiciones entonces que se negarán editan la regla predeterminada para decir "niegan el acceso".
9. Ahora definiremos las **reglas de selección del servicio**. Utilice esta página para configurar una directiva simple o basada en las reglas determinar que mantengan para aplicarse a los pedidos entrantes. En este ejemplo, se utiliza una directiva basada en las reglas.

Configure el WLC

La configuración requiere estos pasos:

1. Configure el WLC con los detalles del servidor de autenticación.
2. Configure las interfaces dinámicas (VLA N).
3. Configure los WLAN (SSID).

Configure el WLC con los detalles del servidor de autenticación

Es necesario configurar el WLC así que puede comunicar con el servidor de RADIUS para autenticar a los clientes, y también para cualquier otra transacción.

Complete estos pasos:

1. Del regulador GUI, haga clic la **Seguridad**.
2. Ingrese el IP Address del servidor de RADIUS y de la clave secreta compartida usados entre el servidor de RADIUS y el WLC.Esta clave secreta compartida debe ser lo mismo que la que está configurada en el servidor de RADIUS.

Configure las interfaces dinámicas (los VLA N)

Este procedimiento describe cómo configurar las interfaces dinámicas en el WLC.

Complete estos pasos:

1. La interfaz dinámica se configura del regulador GUI, en la ventana del **regulador > de las interfaces**.
2. Haga clic en Apply (Aplicar).Esto le lleva a la ventana del editar de esta interfaz dinámica (VLA N 253 aquí).
3. Ingrese el IP Address y el default gateway de esta interfaz dinámica.
4. Haga clic en Apply (Aplicar).
5. Las interfaces configuradas parecerán esto:

Configure los WLAN (el SSID)

Este procedimiento explica cómo configurar los WLAN en el WLC.

Complete estos pasos:

1. Del regulador GUI, van a los **WLAN > crean nuevo** para crear una nueva red inalámbrica (WLAN). Se visualiza la nueva ventana del WLAN.
2. Ingrese la información del ID DE WLAN y WLAN SSID.Usted puede ingresar cualquier nombre como el WLAN SSID. Este ejemplo utiliza el **goa** como la red inalámbrica (WLAN) SSID.
3. El tecleo **se aplica** para ir a la ventana del editar del goa de la red inalámbrica (WLAN).

Configure la utilidad del cliente de red inalámbrica

PEAP-MSCHAPv2 (user1)

En nuestro probar cliente, estamos utilizando el supplicant nativo de Windows 7 con un indicador luminoso LED amarillo de la placa muestra gravedad menor de Intel 6300-N que funciona con la versión del driver 14.3. Se recomienda para probar usando los últimos drivers de los vendedores.

Complete estos pasos para crear un perfil en Windows cero Config (WZC):

1. Vaya al **panel de control** > a la **red y Internet > maneja las redes inalámbricas**.
2. Haga clic la lengueta del **agregar**.
3. El tecleo **crea manualmente un perfil de la red**.
4. Agregue los detalles según lo configurado en el WLC.**Nota:** El SSID es con diferenciación entre mayúsculas y minúsculas.
5. Haga clic en Next (Siguiente).
6. **Configuraciones de la conexión del cambio del** tecleo para comprobar las configuraciones con minuciosidad.
7. Aseegurese le hacer el **PEAP** habilitar.
8. En este ejemplo, no estamos validando el certificado de servidor. Si usted marca este cuadro y no puede conectar, intente inhabilitar la característica y la prueba otra vez.
9. Alternativamente, usted puede utilizar sus credenciales de Windows para iniciar sesión. Sin embargo, en este ejemplo no vamos a utilizar eso. Haga clic en OK.
10. **Configuraciones avanzadas del** tecleo para configurar el nombre de usuario y contraseña.

Su utilidad de cliente está lista ahora para conectar.

EAP-FAST (user2)

En nuestro probar cliente, estamos utilizando el supplicant nativo de Windows 7 con un indicador luminoso LED amarillo de la placa muestra gravedad menor de Intel 6300-N que funciona con la versión del driver 14.3. Se recomienda para probar usando los últimos drivers de los vendedores.

Complete estos pasos para crear un perfil en WZC:

1. Vaya al **panel de control** > a la **red y Internet** > **maneja las redes inalámbricas**.
2. Haga clic la lengueta del **agregar**.
3. El tecleo **crea manualmente un perfil de la red**.
4. Agregue los detalles según lo configurado en el WLC.**Nota:** El SSID es con diferenciación entre mayúsculas y minúsculas.
5. Haga clic en Next (Siguiente).
6. **Configuraciones de la conexión del cambio del** tecleo para comprobar las configuraciones con minuciosidad.
7. Aseegurese le hacer el EAP-FAST habilitar.**Nota:** Por abandono, WZC no tiene EAP-FAST como método de autentificación. Usted tiene que descargar la utilidad de un proveedor externo. En este ejemplo, puesto que es un indicador luminoso LED amarillo de la placa muestra gravedad menor de Intel, tenemos Intel PROSet instalado en el sistema.
8. Habilite **permiten el aprovisionamiento automático PAC** y se aseeguran **validar el certificado de servidor** se desmarca.
9. Haga clic la lengueta de los **credenciales de usuario**, y ingrese las credenciales de user2. Alternativamente, usted puede utilizar sus credenciales de Windows para iniciar sesión. Sin embargo, en este ejemplo no vamos a utilizar eso.
10. Haga clic en OK.

Su utilidad de cliente está lista ahora para conectar para user2.

Nota: Cuando user2 está intentando autenticar, el servidor de RADIUS va a enviar un PAC. Valide el PAC para completar la autenticación.

Verificación

Utilize esta sección para confirmar que su configuración funcione 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.

Verifique el user1 (PEAP-MSCHAPv2)

Del WLC GUI, vaya al **monitor** > a los **clientes**, y seleccione la dirección MAC.

Stats del WLC RADIUS:

```
(Cisco Controller) >show radius auth statistics Authentication Servers: Server
Index..................................... 1 Server Address.................................
192.168.150.24 Msg Round Trip Time.......................... 1 (msec) First
Requests................................... 8 Retry Requests.................................
0 Accept Responses.............................. 1 Reject
Responses.............................. 0 Challenge Responses............................ 7
Malformed Msgs................................. 0 Bad Authenticator
Msgs.......................... 0 Pending Requests.............................. 0 Timeout
Requests.............................. 0 Unknowntype Msgs.............................. 0
```

```
Other Drops.................................... 0
```

Registros ACS:

1. Complete estos pasos para ver las cuentas del golpe:Si usted marca los registros en el plazo de 15 minutos de autenticación, aseegurese le restaurar la cuenta del golpe.Usted tiene una lengueta para la **cuenta del golpe** en la parte inferior de la misma página.
2. **La supervisión del** tecleo **y los informes** y una nueva ventana emergente aparece. Vaya a las **autenticaciones – Radio – Hoy**. Usted puede también hacer clic los **detalles** para verificar que mantienen la regla de selección eran aplicados.

Verifique user2 (el EAP-FAST)

Del WLC GUI, vaya al **monitor >** a los **clientes**, y seleccione la dirección MAC.

El ACS registra:

1. Complete estos pasos para ver las cuentas del golpe:Si usted marca los registros en el plazo de 15 minutos de autenticación, aseegurese le restaurar la cuenta del GOLPE.Usted tiene una lengueta para la **cuenta del golpe** en la parte inferior de la misma página.
2. **La supervisión del** tecleo **y los informes** y una nueva ventana emergente aparece. Vaya a las **autenticaciones – Radio – Hoy**. Usted puede también hacer clic los **detalles** para verificar que mantienen la regla de selección eran aplicados.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

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.

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

1. Si usted experimenta cualesquiera problemas, publique estos comandos en el WLC:*el <mac del* **cliente del debug** *agrega del client>***debug aaa all enablemuestre el** *addr> del <mac del* **detalle del cliente** - Verifique el estado del administrador de la directiva.**muestre las estadísticas del auth del radio** - Verifique la razón del error.**haga el debug de neutralización-todo** - Apague los debugs.**borre las** estadísticas del radio del **cese de alarma del auth del radio stats** sobre el WLC.
2. Verifique abre una sesión el ACS y observa la razón del error.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems