NP, reguladores del Wireless LAN, y ejemplo de configuración de las redes inalámbricas

Contenido

Introducción

Este documento proporciona una configuración de muestra para el protocolo extensible authentication protegido (PEAP) con la autenticación de la versión 2 del protocolo microsoft challenge handshake authentication (MS-CHAP) en una red del Cisco Unified Wireless con el servidor de políticas de la red de Microsoft (NP) como el servidor de RADIUS.

Prerrequisitos

Requisitos

Asegúrese de que usted sea familiar con estos procedimientos antes de que usted intente esta configuración:

- Instalación de Windows 2008 del conocimietno básico
- Conocimiento de la instalación del controlador de Cisco

Asegúrese de que se hayan cumplido estos requisitos antes de que usted intente esta configuración:

- Instale el sistema operativo 2008 del Microsoft Windows server en cada uno de los servidores en el laboratorio de prueba.
- Ponga al día todos los paquetes de servicios.
- Instale los reguladores y los Puntos de acceso ligeros (revestimientos).
- Configure las actualizaciones de último software.

Para la instalación inicial y la información de la configuración para los reguladores inalámbricos de las Cisco 5508 Series, refiera a la guía de instalación del controlador inalámbrica de las Cisco 5500 Series.

Nota: Este documento se piensa para dar a los lectores un ejemplo en la configuración requerida en un servidor de Microsoft para la autenticación PEAP-MS-CHAP. La configuración del Microsoft Windows server presentada en este documento se ha probado en el laboratorio y se ha encontrado para trabajar como se esperaba. Si usted tiene problema con la configuración, entre en contacto Microsoft para la ayuda. El Centro de Asistencia Técnica de Cisco (TAC) no soporta la configuración del Microsoft Windows server.

Microsoft Windows 2008 guías de instalación y configuración se puede encontrar en la red de la tecnología de Microsoft.

Componentes Utilizados

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

- Regulador de la Tecnología inalámbrica de Cisco 5508 que funciona con la versión de firmware 7.4
- Cisco Aironet 3602 puntos de acceso con el protocolo del Lightweight Access Point (LWAPP)
- Servidor de Enterprise de Windows 2008 con los NP, el Certificate Authority (CA), el (DHCP) del Dynamic Host Control Protocol, y los servicios del Domain Name System (DNS) instalados
- Microsoft Windows 7 PC del cliente
- Cisco Catalyst 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.

Descripción PEAP

Seguridad del nivel del transporte de las aplicaciones PEAP (TLS) para crear un canal cifrado entre un cliente PEAP de autenticidad, tal como una laptop inalámbrica, y un authenticator PEAP, tal como Microsoft NP o cualquier servidor de RADIUS. El PEAP no especifica un método de autentificación, sino proporciona la seguridad complementaria para otros protocolos extensible authentication (EAP), por ejemplo el v2 EAP-MS-CHAP, que puede actuar a través del canal TLS-cifrado proporcionado por el PEAP. El proceso de autenticación PEAP consiste en dos fases principales.

Fase uno PEAP: Canal TLS-cifrado

Los socios del cliente de red inalámbrica con el AP. Una asociación de IEEE 802.11-based proporciona un sistema operativo o una clave de autenticación compartida antes de que una asociación segura se cree entre el cliente y el Punto de acceso. Después de que la asociación de IEEE 802.11-based se establezca con éxito entre el cliente y el Punto de acceso, la sesión de TLS se negocia con el AP. Después de que la autenticación se complete con éxito entre el cliente de red inalámbrica y los NP, la sesión de TLS se negocia entre el cliente y los NP. La clave que se deriva dentro de esta negociación se utiliza para cifrar toda la comunicación subsiguiente.

Fase dos PEAP: Comunicación EAP-autenticada

La comunicación EAP, que incluye la negociación EAP, ocurre dentro del canal de TLS creado por el PEAP dentro de la primera fase del proceso de autenticación PEAP. Los NP autentican al cliente de red inalámbrica con el v2 EAP-MS-CHAP. El REVESTIMIENTO y los mensajes delanteros del regulador solamente entre el cliente de red inalámbrica y el servidor de RADIUS. El regulador del Wireless LAN (WLC) y el REVESTIMIENTO no pueden desencriptar estos mensajes porque no es el punto extremo de TLS.

La secuencia del mensaje de RADIUS para una tentativa de la autenticación satisfactoria (donde el usuario ha suministrado las credenciales basadas en la contraseña válidas el v2 PEAP-MS-CHAP) es:

1. Los NP envían un mensaje request de la identidad al cliente: `EAP-petición/identidad`.
2. El cliente responde con un mensaje de respuesta de la identidad: `EAP-respuesta/identidad`.
3. Los NP envían un mensaje de impugnación del v2 MS-CHAP: `EAP-Request/EAP-Type=EAP MS-CHAP-V2 (desafío)`.
4. El cliente responde con un desafío y una respuesta del v2 MS-CHAP: `EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (respuesta)`.
5. Los NP devuelven un paquete del éxito del v2 MS-CHAP cuando el servidor ha autenticado con éxito al cliente: `EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (éxito)`.
6. El cliente responde con un paquete del éxito del v2 MS-CHAP cuando el cliente ha autenticado con éxito el servidor: `EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (éxito)`.
7. Los NP envían un EAP-tipo-longitud-valor (TLV) que indique la autenticación satisfactoria.
8. El cliente responde con un Mensaje de éxito del estatus EAP-TLV.
9. El servidor completa la autenticación y envía un mensaje del EAP-éxito en el sólo texto. Si los VLA N se despliegan para el aislamiento del cliente, los atributos del VLA N se incluyen en este mensaje.

Configurar

En esta sección, le presentan con la información para configurar el v2 PEAP-MS-CHAP.

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

Esta configuración utiliza esta configuración de red:

En esta configuración, un servidor de Microsoft Windows 2008 realiza estos papeles:

- Controlador de dominio para el dominio wireless.com
- Servidor DHCP/DNS
- Servidor de CA
- ¿NP? para autenticar a los usuarios de red inalámbrica
- ¿Active Directory? para mantener la base de datos de usuarios

El servidor conecta con la red alámbrica a través de un 2 Switch de la capa como se muestra. El WLC y el REVESTIMIENTO registrado también conectan con la red a través del 2 Switch de la capa.

El Wi-Fi del uso de los clientes de red inalámbrica protegió el acceso 2 (WPA2) - autenticación del v2 PEAP-MS-CHAP para conectar con la red inalámbrica.

Configuraciones

El objetivo de este ejemplo es configurar el servidor de Microsoft 2008, el regulador del Wireless LAN, y el AP ligero para autenticar a los clientes de red inalámbrica con la autenticación del v2 PEAP-MS-CHAP. Hay tres pasos principales en este proceso:

1. Configure el servidor de Microsoft Windows 2008.
2. Configure el WLC y los AP ligeros.
3. Configure a los clientes de red inalámbrica.

Configure el servidor de Microsoft Windows 2008

En este ejemplo, una configuración completa del servidor de Microsoft Windows 2008 incluye estos pasos:

1. Configure el servidor como controlador de dominio.
2. Instale y configure los servicios del DHCP.
3. instale y configure el servidor como servidor de CA.
4. Conecte a los clientes con el dominio.
5. Instale los NP.
6. Instale un certificado.
7. Configure los NP para la autenticación PEAP.

8. Agregue a los usuarios al Active Directory.

Configure el servidor de Microsoft Windows 2008 como controlador de dominio

Complete estos pasos para configurar el servidor de Microsoft Windows 2008 como controlador de dominio:

1. Haga clic el **comienzo** > al **administrador de servidor**.

2. Haga clic los **papeles de los papeles** > Add.

3. Haga clic en Next (Siguiente).

4. Seleccione los **servicios del dominio de Active Directory del** servicio, y haga clic **después**.

5. Revise la introducción a los servicios del dominio de Active Directory, y haga clic **después**.

6. El tecleo **instala** para comenzar el proceso de instalación.

   La instalación procede y completa.

7. Haga clic **cerca a este Asisitente y inicie al asistente de instalación de los servicios del dominio de Active Directory (dcpromo.exe)** para continuar la instalación y la configuración del Active Directory.

8. Haga clic **al lado de** funcionan con al asistente de instalación de los servicios del dominio de Active Directory.

9. Revise la información sobre el sistema operativo Compatbilty, y haga clic **después**.

10. El tecleo **crea un nuevo dominio en un nuevo bosque > después** para crear un nuevo dominio.

11. Ingrese el nombre DNS completo para el nuevo dominio (wireless.com **en** este ejemplo), y haga clic después**.**

12. Seleccione el nivel funcional del bosque para su dominio, y haga clic **después**.

13. Seleccione el nivel funcional del dominio para su dominio, y haga clic **después**.

14. Asegúrese que seleccionen al servidor DNS, y haga clic **después**.

15. Haga clic **sí** para que el asistente de instalación cree una nueva zona en el DNS para el dominio.

16. Seleccione las carpetas que el Active Directory debe utilizar para sus archivos, y haga clic **después**.

17. Ingrese la contraseña del administrador, y haga clic **después**.

18. Revise sus selecciones, y haga clic **después**.

    Los ingresos de la instalación.

19. Clic en Finalizar **para cerrar al Asisitente.**

20. Recomience el servidor para que los cambios tomen el efecto.

Instale y configure los servicios del DHCP en el servidor de Microsoft Windows 2008

El servicio del DHCP en el servidor de Microsoft 2008 se utiliza para proporcionar los IP Addresses a los clientes de red inalámbrica. Complete estos pasos para instalar y configurar los servicios del DHCP:

1. Haga clic el **comienzo** > al **administrador de servidor**.

2. Haga clic los **papeles de los papeles** > Add.

3. Haga clic en Next (Siguiente).

4. Seleccione al **servidor DHCP del** servicio, y haga clic **después**.

5. Revise la introducción al servidor DHCP, y haga clic **después**.

6. Seleccione la interfaz que el servidor DHCP debe monitorear para las solicitudes, y haga clic **después**.

7. Configure las configuraciones del valor por defecto DNS que el servidor DHCP debe proporcionar a los clientes, y haga clic **después**.

8. Configure los TRIUNFOS si la red soporta los TRIUNFOS.

9. El tecleo **agrega** para utilizar al Asisitente para crear un alcance de DHCP o el tecleo **al lado de** crea un alcance de DHCP más adelante. Para continuar, haga clic en Next (Siguiente).

10. Del permiso o de la neutralización DHCPv6 en el servidor, y tecleo soporte **después**.

11. Configuraciones del IPv6 DNS de la configuración si DHCPv6 fue habilitado en el paso anterior. Para continuar, haga clic en Next (Siguiente).

12. Proporcione las credenciales del administrador de dominio para autorizar al servidor DHCP en el Active Directory, y haga clic **después**.

13. Revise la configuración en la página de la confirmación, y el tecleo **instala** para completar el instalar.

    Los ingresos de la instalación.

14. El tecleo **cerca de** cierra al Asisitente.

    El servidor DHCP ahora está instalado.

15. Haga clic el **Start (Inicio) > Administrative Tools (Herramientas administrativas) >** el **DHCP** para configurar el servicio del DHCP.

16. Amplíe al servidor DHCP (win-mvz9z2umms.wireless.com en este ejemplo), haga clic con el botón derecho del ratón el IPv4, y elija el **nuevo alcance**. para crear un alcance de DHCP.

17. Tecleo **al lado de la** configuración el nuevo alcance vía el nuevo asistente de alcance.

18. Proporcione un nombre para el nuevo alcance (clientes de red inalámbrica en este ejemplo), y haga clic **después**.

19. Ingrese el rango de los IP Addresses disponibles que se puede utilizar para los arriendos del DHCP. Para continuar, haga clic en Next (Siguiente).

20. Cree una lista opcional de direccionamientos excluidos. Para continuar, haga clic en Next (Siguiente).

21. Configure el Tiempo de validez, y haga clic **después**.

22. Haga clic **sí, quiero ahora configurar estas opciones**, y hago clic **después**.

23. Ingrese el IP Address del default gateway para este alcance, tecleo **agregan > después**.

24. Configure el Domain Name y al servidor DNS DNS que se utilizarán por los clientes. Para continuar, haga clic en Next (Siguiente).

25. Ingrese la información de los TRIUNFOS para este alcance si la red soporta los TRIUNFOS. Para continuar, haga clic en Next (Siguiente).

26. Para activar este alcance, haga clic **sí, yo quieren activar este alcance ahora > después**.

27. Clic en Finalizar para completar y para cerrar al Asisitente.

Instale y configure el servidor de Microsoft Windows 2008 como servidor de CA

El PEAP con el v2 EAP-MS-CHAP valida al servidor de RADIUS basado en el certificado presente en el servidor. Además, el certificado de servidor se debe publicar por un público CA que sea confiado en por la computadora cliente (es decir, el certificado de CA público existe ya en la carpeta del Trusted Root Certification Authority en el almacén de certificados de la computadora cliente).

Complete estos pasos para configurar el servidor de Microsoft Windows 2008 como servidor de CA que publique el certificado a los NP:

1. Haga clic el **comienzo >** al **administrador de servidor**.

2. Haga clic los **papeles de los papeles** > Add.

3. Haga clic en Next (Siguiente).

4. Seleccione los **servicios de certificados de Active Directory del** servicio, y haga clic **después**.

5. Revise la introducción a los servicios de certificados del Active Directory, y haga clic **después**.

6. Seleccione el **Certificate Authority**, y haga clic **después**.

7. Seleccione la **empresa**, y haga clic **después**.

8. Seleccione **raíz CA**, y haga clic **después**.

9. Selecto **cree una nueva clave privada**, y haga clic **después**.

10. Haga clic **después** en configurar la criptografía para CA.

11. El tecleo **al lado de** valida el Common Name predeterminado para este CA.

12. Seleccione la longitud del tiempo que este certificado de CA es válido, y haga clic **después**.

13. El tecleo **al lado de** valida la ubicación de la base de datos predeterminada del certificado.

14. Revise la configuración, y el tecleo **instala** para comenzar los servicios de certificados del Active Directory.

15. Después de que se complete el instalar, **cierre del** tecleo.

Conecte a los clientes con el dominio

Complete estos pasos para conectar a los clientes con la red alámbrica y descargar la información específica del dominio del nuevo dominio:

1. Conecte a los clientes con la red alámbrica con un cable Ethernet directo recto.
2. Inicie encima del cliente, y inicie sesión con el nombre de usuario del cliente y la contraseña.
3. Haga clic el **Start (Inicio) > Run (Ejecutar)**, ingrese el **cmd**, y haga clic la **AUTORIZACIÓN**.
4. En el comando prompt, ingrese el **ipconfig**, y el tecleo **ingresa** para verificar que el DHCP trabaja correctamente y que el cliente recibió un IP Address del servidor DHCP.
5. Para unirse a al cliente al dominio, al **comienzo del** tecleo, **Computadora del** click derecho, elegir las **propiedades**, y elegir las **configuraciones del cambio** en la inferior derecha.
6. **Cambio del** tecleo.
7. Haga clic el **dominio**, ingrese **wireless.com**, y haga clic la **AUTORIZACIÓN**.

8. Ingrese el **administrador del** nombre de usuario y el específico de la contraseña al dominio al cual el cliente se une a. Ésta es la cuenta del administrador en el Active Directory en el servidor.

9. Haga Click en OK, y **AUTORIZACIÓN del** tecleo otra vez.

10. Tecleo **cercano > reinicio ahora** para recomenzar el ordenador.
11. Una vez que el ordenador recomienza, inicie sesión con esta información: Nombre de usuario = administrador; Password> de la contraseña = del <domain; Dominio = Tecnología inalámbrica.
12. Haga clic el **comienzo**, haga clic con el botón derecho del ratón la **Computadora**, elija las **propiedades**, y elija las **configuraciones del cambio** en la inferior derecha de verificar que usted está en el dominio de wireless.com.
13. El siguiente paso es verificar que el cliente recibió el certificado de CA (confianza) del servidor.

14. Haga clic el **comienzo**, ingrese el **mmc**, y el Presione ENTER.
15. El clic en Archivo, y el tecleo **agregan/quitan broche-**en.
16. Elija los **Certificados**, y el haga click en Add

17. Haga clic la **cuenta de la Computadora**, y haga clic **después**.

18. Haga clic la **computadora local**, y haga clic **después**.

19. Haga clic en OK.
20. Amplíe las carpetas de los **Certificados (computadora local)** y de los **Trusted Root Certification Authority**, y haga clic los **Certificados**. Encuentre el **CERT de CA del dominio de red inalámbrica** en la lista. En este ejemplo, el CERT de CA se llama wireless-WIN-MVZ9Z2UMNMS-CA.

21. Relance este procedimiento para agregar a más clientes al dominio.

Instale el servidor de la política de red en el servidor de Microsoft Windows 2008

En esta configuración, los NP se utilizan como servidor de RADIUS para autenticar a los clientes de red inalámbrica con la autenticación PEAP. Complete estos pasos para instalar y configurar los NP en el servidor de Microsoft Windows 2008:

1. Haga clic el **comienzo >** al **administrador de servidor**.

2. Haga clic los **papeles de los papeles >** Add.

3. Haga clic en Next (Siguiente).

4. Seleccione los **servicios de la política de red y del acceso del** servicio, y haga clic **después**.

5. Revise la introducción a los servicios de la política de red y del acceso, y haga clic **después**.

6. Seleccione el **servidor de la política de red**, y haga clic **después**.

7. Revise la confirmación, y el tecleo **instala**.

   Después de que se complete el instalar, una pantalla similar ésta se visualiza.

8. Haga clic en Close (Cerrar).

Instale un certificado

Complete estos pasos para instalar el certificado del ordenador para los NP:

1. Haga clic el **comienzo**, ingrese el **mmc**, y el Presione ENTER.
2. El clic en Archivo > Add**/quita Broche-en**.
3. Elija los **Certificados**, y el haga click en Add

4. Elija la **cuenta de la Computadora**, y haga clic **después**.

5. Seleccione la **computadora local**, y el clic en Finalizar.

6. Haga Click en OK a volver al Microsoft Management Console (MMC).

7. Amplíe los **Certificados (computadora local)** y las **carpetas personales**, y haga clic los **Certificados**.

8. Haga clic con el botón derecho del ratón en el whitespace debajo del certificado de CA, y elija **todas las tareas > certificado de la petición nuevo**.

9. Haga clic en Next (Siguiente).

10. Seleccione el **controlador de dominio**, y el tecleo **alista**.

11. Clic en Finalizar una vez que el certificado está instalado.

    El certificado NP ahora está instalado.

12. Asegúrese de que el propósito previsto del certificado lee la **autenticación de cliente, autenticación de servidor**.

Configure el servicio de servidor de la política de red para la autenticación del v2 PEAP-MS-CHAP

Complete estos pasos para configurar los NP para la autenticación:

1. Haga clic el **Start (Inicio) > Administrative Tools (Herramientas administrativas)** > el **servidor de la política de red**.
2. Haga clic con el botón derecho del ratón los **NP (locales)**, y elija el **servidor del registro en el Active Directory**.

3. Haga clic en OK.

4. Haga clic en OK.

5. Agregue el regulador del Wireless LAN como cliente del Authentication, Authorization, and Accounting (AAA) en los NP.
6. Amplíe los **clientes RADIUS y los servidores**. Haga clic con el botón derecho del ratón a los **clientes RADIUS**, y elija al **nuevo cliente RADIUS**.

7. Ingrese un nombre cómodo (WLC en este ejemplo), el IP Address de administración del

WLC (192.168.162.248 en este ejemplo) y un secreto compartido. El mismo secreto compartido se utiliza para configurar el WLC.

8. Haga Click en OK a volver a la pantalla anterior.

9. Cree una nueva política de red para los usuarios de red inalámbrica. Amplíe las **directivas**, haga clic con el botón derecho del ratón las **políticas de red**, y elija **nuevo**.

10. Ingrese un nombre de la directiva para esta regla (Tecnología inalámbrica PEAP en este ejemplo), y haga clic **después**.

11. Para hacer que esta directiva permita solamente a los usuarios del dominio de red inalámbrica, agregue estas tres condiciones, y haga clic **después**:

    - Grupos de Windows - Domain User
    - Tipo de puerto NAS - Tecnología inalámbrica - IEEE 802.11
    - Tipo de autenticación - EAP

12. **El acceso del** tecleo **concedido** para conceder los intentos de conexión que hacen juego esta directiva, y hace clic **después**.

13. Inhabilite todos los métodos de autentificación bajo métodos de autentificación menos seguros.

14. El tecleo **agrega**, PEAP selecto, y **AUTORIZACIÓN del** tecleo para habilitar el PEAP.

15. Seleccione **Microsoft: El EAP protegido (PEAP)**, y el tecleo **editan**. Asegure que el certificado previamente creado del controlador de dominio está seleccionado en la lista desplegable publicada certificado, y haga clic la **autorización**.

16. Haga clic en Next (Siguiente).

17. Haga clic en Next (Siguiente).

18. Haga clic en Next (Siguiente).

19. Haga clic en Finish (Finalizar).

Agregue a los usuarios al Active Directory

En este ejemplo, la base de datos de usuarios se mantiene en el Active Directory. Complete estos pasos para agregar a los usuarios a la base de datos del Active Directory:

1. Abra a los usuarios de directorio activo y computadora. Haga clic el **Start (Inicio) > Administrative Tools (Herramientas administrativas) >** a los **usuarios de directorio activo y computadora**.
2. En el árbol de la consola de los usuarios de directorio activo y computadora, amplíe el dominio, haga clic con el botón derecho del ratón a los **usuarios > nuevo**, y elija al **usuario**.
3. ¿En el nuevo objeto? El cuadro de diálogo del usuario, ingresa el nombre del usuario de red inalámbrica. Este ejemplo utiliza el client1 del nombre en el campo de primer nombre y el client1 en el campo de nombre de inicio de usuario. Haga clic en Next (Siguiente).

4. ¿En el nuevo objeto? El cuadro de diálogo del usuario, ingresa una contraseña de su opción en la contraseña y confirma los campos de contraseña. Desmarque al **usuario debe cambiar la contraseña en la** casilla de verificación **siguiente del inicio**, y hace clic **después**.

5. ¿En el nuevo objeto? Cuadro de diálogo del usuario, clic en Finalizar.

6. Relance los pasos 2 a 4 para crear las cuentas de usuario adicionales.

Configure el regulador y los revestimientos del Wireless LAN

Configure los dispositivos de red inalámbrica (los reguladores y los revestimientos del Wireless LAN) para esta configuración.

Configure el WLC para la autenticación de RADIUS

Configure el WLC para utilizar los NP como el servidor de autenticación. El WLC se debe configurar para remitir los credenciales de usuario a un servidor RADIUS externo. El servidor RADIUS externo después valida los credenciales de usuario y proporciona el acceso a los clientes de red inalámbrica.

Complete estos pasos para agregar los NP como servidor de RADIUS en la página de la **Seguridad** > de la **autenticación de RADIUS**:

1. Elija la **Seguridad** > el **RADIUS** > la **autenticación de la** interfaz del regulador para visualizar la página de los servidores de autenticación de RADIUS. Haga clic **nuevo** para definir a un servidor de RADIUS.

2. Defina 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. Las casillas de verificación del usuario de la red y de la Administración determinan si la autenticación basada en RADIUS se aplica a los usuarios de la Administración y de la red (Tecnología inalámbrica). Este ejemplo utiliza los NP como el servidor de RADIUS con una dirección IP de 192.168.162.12. Haga clic en Apply (Aplicar).

Configure una red inalámbrica (WLAN) para los clientes

Configure al conjunto de servicio más identfier (SSID) (red inalámbrica (WLAN)) a quien los clientes de red inalámbrica conecta. En este ejemplo, cree el SSID, y nómbrelo PEAP.

Defina la autenticación de la capa 2 como WPA2 de modo que los clientes realicen la autenticación EAP-basada (v2 PEAP-MS-CHAP en este ejemplo) y utilicen el Advanced Encryption Standard (AES) como el mecanismo de encripción. Deje el resto de los valores en sus valores por defecto.

Nota: Este documento ata la red inalámbrica (WLAN) con las interfaces de administración. Cuando usted tiene VLAN múltiples en su red, usted puede crear un VLAN distinto y atarlo al SSID. Para la información sobre cómo configurar los VLA N en el WLCs, refiera a los VLA N en el ejemplo de configuración de los reguladores del Wireless LAN.

Complete estos pasos para configurar una red inalámbrica (WLAN) en el WLC:

1. Haga clic los **WLAN de la** interfaz del regulador para visualizar la página WLAN. Esta página enumera los WLAN que existen en el regulador.
2. Elija **nuevo** para crear una nueva red inalámbrica (WLAN). Ingrese el ID DE WLAN y el WLAN SSID para el WLAN, y el tecleo **se aplica**.

3. Para configurar el SSID para el 802.1x, complete estos pasos: Haga clic la **ficha general** y habilite la red inalámbrica (WLAN).

Haga clic las lenguetas de la **Seguridad** > de la **capa 2**, fije la Seguridad de la capa 2 a **WPA + WPA2**, marque los boxesas del control de los parámetros WPA+WPA2 (por ejemplo, WPA2 AES) necesarios, y haga clic el **802.1x** como la Administración de clave de autenticación.

Haga clic las lenguetas de los **servidores de la Seguridad** >AAA, elija la dirección IP de los NP de la lista desplegable del **server1**, y el tecleo **se aplica**.

Configure a los clientes de red inalámbrica para la autenticación del v2 PEAP-MS-CHAP

Complete estos pasos para configurar al cliente de red inalámbrica con Windows cero herramienta de los Config para conectar con la red inalámbrica (WLAN) PEAP.

1. Haga clic el **icono de red** en la barra de tareas. Haga clic el **PEAP** SSID, y el tecleo **conecta**.

2. El cliente debe ahora ser conectado con la red.

3. Si la conexión falla, intente volver a conectar a la red inalámbrica (WLAN). Si persiste el problema, refiera a la sección del Troubleshooting.

Verificación

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

Troubleshooting

Si su cliente no conectó con la red inalámbrica (WLAN), esta sección proporciona la información que usted puede utilizar para resolver problemas la configuración.

Hay dos herramientas que se pueden utilizar para diagnosticar las fallas de autenticación del 802.1x: **el comando client del debug** y el **visor de eventos** en Windows.

La ejecución de un debug del cliente del WLC no es uso intensivo de recurso y no hace servicio del imnpact. Para comenzar una sesión del debug, abrir el comando line interface(cli) del WLC, y ingresar el **MAC Address del cliente del debug**, donde está el MAC address el MAC address sin hilos del cliente de red inalámbrica que no puede conectar. Mientras que este debug se ejecuta, intente conectar al cliente; allí se debe hacer salir en el CLI del WLC que parece similar a este

ejemplo:

Éste es un ejemplo de un problema que podría ocurrir con un misconfiguration. Aquí, el debug del WLC muestra el WLC se ha trasladado al estado de autenticidad, que significa que el WLC está esperando una respuesta de los NP. Esto es generalmente debido a un secreto compartido incorrecto en el WLC o los NP. Usted puede confirmar esto vía el visor de eventos del Servidor Windows. Si usted no encuentra un registro, la petición nunca lo hizo a los NP.

Otro ejemplo que se encuentra del debug del WLC es un rechazo de acceso. Un rechazo de acceso muestra que los NP recibieron y rechazaron las credenciales del cliente. Éste es un ejemplo de un cliente que recibe un rechazo de acceso:

Cuando usted ve un rechazo de acceso, marque abre una sesión los registros de acontecimientos del Servidor Windows para determinar porqué los NP respondieron al cliente con un rechazo de acceso.

Una autenticación satisfactoria tiene un access-accept en el debug del cliente, como se ve en este ejemplo:

Resolver problemas los rechazos de acceso y los tiempos de espera de respuesta agotados requiere el acceso al servidor de RADIUS. El WLC actúa como authenticator que pasa los mensajes EAP entre el cliente y el servidor de RADIUS. Un servidor de RADIUS que responde con un rechazo de acceso o un tiempo de espera de respuesta agotado debe ser examinado y ser diagnosticado por el fabricante del servicio RADIUS.

Nota: TAC no proporciona el Soporte técnico para los servidores de RADIUS de tercera persona; sin embargo, abre una sesión al servidor de RADIUS explican generalmente porqué un pedido de cliente fue rechazado o ignorado.

Para resolver problemas los rechazos de acceso y los tiempos de espera de respuesta agotados de los NP, examine los NP abre una sesión el visor de eventos de Windows en el servidor.

1. Haga clic el **Tools (Herramientas) > Event Viewer (Visor de eventos) del comienzo >** del **administrador** para encender el visor de eventos y para revisar los registros NP.
2. Amplíe las **visiones >** las **Funciones del servidor >** la **política de red y el acceso de encargo**.

En esta sección de la opinión del evento, hay registros de pasado y las autenticaciones fallidas. Examine estos registros para resolver problemas porqué un cliente no está pasando la autenticación. Pasado y las autenticaciones fallidas aparecen como informativo. Navegue a través de los registros para encontrar que el nombre de usuario que tiene autenticación fallida y recibido un rechazo de acceso según el WLC hace el debug de.

Éste es un ejemplo de los NP que niegan un acceso del usuario:

Al revisar un enunciado de negación en el visor de eventos, examine la sección de los detalles de la autenticación. En este ejemplo, usted puede ver que los NP negaron el acceso del usuario debido a un nombre de usuario incorrecto:

La opinión del evento sobre los NP también ayuda con el troubleshooting si el WLC no recibe una respuesta detrás de los NP. Esto es causada generalmente por un secreto compartido incorrecto entre los NP y el WLC.

En este ejemplo, los NP desechan la petición del WLC debido a un secreto compartido incorrecto:

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems