Ejemplo de Configuración de Servidor EAP Local de Red Inalámbrica Unificada

Contenido

Introducción

Este documento describe la configuración de un servidor local de Extensible Authentication Protocol (EAP) en un Controlador de LAN de Red Inalámbrica Cisco (WLC) para la autenticación de los usuarios de red inalámbrica.

EAP local es un método de autenticación que permite que los usuarios y los clientes inalámbricos se autentiquen localmente. Está diseñado para oficinas remotas que deseen mantener la conectividad con clientes inalámbricos cuando el sistema back-end se interrumpa o el servidor de autenticación externo deje de funcionar. Cuando habilita el EAP local, el controlador sirve como el servidor de autenticación y la base de datos de usuario local, eliminando así la dependencia de un servidor de autenticación externo. EAP local recupera las credenciales de usuario de la base de datos de usuarios local o de la base de datos back-end del protocolo ligero de acceso a directorios (LDAP) para autenticar a los usuarios. EAP local admite autenticación EAP ligero (LEAP), EAP-autenticación flexible a través de tunelación segura (EAP-FAST) y EAP-seguridad de la capa de transporte (EAP-TLS) entre el controlador y los clientes inalámbricos.

Tenga en cuenta que el servidor EAP local no está disponible si hay una configuración de servidor RADIUS externa global en el WLC. Todas las solicitudes de autenticación se reenvían al RADIUS externo global hasta que el servidor EAP local esté disponible. Si el WLC pierde la conectividad con el servidor RADIUS externo, entonces el servidor EAP local se vuelve activo. Si no hay ninguna configuración de servidor RADIUS global, el servidor EAP local se activa inmediatamente. El servidor EAP local no se puede utilizar para autenticar a los clientes, que están conectados a otros WLC. En otras palabras, un WLC no puede reenviar su solicitud EAP a otro WLC para la autenticación. Cada WLC debe tener su propio servidor EAP local y base de datos individual.

Nota: Utilice estos comandos para detener el envío de solicitudes de WLC a un servidor RADIUS externo .

```
config wlan disable
        config wlan radius_server auth disable
        config wlan enable
```

El servidor EAP local soporta estos protocolos en la versión de software 4.1.171.0 y posteriores:

- SALTO
- EAP-FAST (nombre de usuario/contraseña y certificados)
- EAP-TLS

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de cómo configurar los WLC y los Lightweight Access Point (LAP) para el funcionamiento básico
- Conocimiento de los métodos de seguridad inalámbrica y del protocolo ligero de punto de acceso (LWAPP)
- Conocimiento básico de la autenticación EAP local.

Componentes Utilizados

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

- Windows XP con tarjeta adaptadora CB21AG y Cisco Secure Services Client versión 4.05

- Cisco 4400 Wireless LAN Controller 4.1.171.0
- Entidad emisora de certificados de Microsoft en Windows 2000 Server

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Configuración de EAP local en el controlador de LAN inalámbrica de Cisco

Este documento asume que la configuración básica del WLC ya está completada.

Configuración de EAP local

Complete estos pasos para configurar el EAP local:

1. Agregue un usuario de red local:

   Desde la GUI. elija Security > Local Net Users > New, ingrese el nombre de usuario, contraseña, usuario invitado, ID de WLAN y descripción y haga clic en Apply.

   Desde la CLI, puede utilizar el comando config netuser add <username> <password> <WLAN id> <description> :

   Nota: Este comando se ha bajado a una segunda línea debido a razones espaciales.

   <#root>

   ```
   (Cisco Controller) >
   config netuser add eapuser2 cisco123 1 Employee user local database
   ```

2. Especifique el orden de recuperación de credenciales de usuario.

   En la GUI, elija Security > Local EAP > Authentication Priority. A continuación, seleccione LDAP, haga clic en el botón "<" y haga clic en Apply. Esto coloca primero las credenciales de usuario en la base de datos local.

   Desde la CLI:

   <#root>

   ```
   (Cisco Controller) >
   config local-auth user-credentials local
   ```

3. Agregar un perfil EAP:

   Para hacerlo desde la GUI, elija Security > Local EAP > Profiles y haga clic en New. Cuando aparezca la nueva ventana, escriba el nombre del perfil y haga clic en Apply.

   También puede hacer esto usando el comando CLI config local-auth eap-profile add <profile-name>. En nuestro ejemplo, el nombre del perfil es EAP-test.

   <#root>

   ```
   (Cisco Controller) >

   config local-auth eap-profile add EAP-test
   ```

4. Agregue un método al perfil EAP.

   En la GUI, elija Security > Local EAP > Profiles y haga clic en el nombre del perfil para el que desea agregar los métodos de autenticación. Este ejemplo utiliza LEAP, EAP-FAST y EAP-TLS. Haga clic en Aplicar para establecer los métodos.

   También puede utilizar el comando CLI config local-auth eap-profile method add <nombre de método> <nombre de perfil> . En nuestro ejemplo de configuración, agregamos tres métodos al perfil EAP-test. Los métodos son LEAP, EAP-FAST y EAP-TLS cuyos nombres de método son leap, fast y tls respectivamente. Este resultado muestra los comandos de configuración de CLI:

   <#root>

   ```
   (Cisco Controller) >

   config local-auth eap-profile method add leap EAP-test

   (Cisco Controller) >

   config local-auth eap-profile method add fast EAP-test

   (Cisco Controller) >

   config local-auth eap-profile method add tls EAP-test
   ```

5. Configure los parámetros del método EAP. Sólo se utiliza para EAP-FAST. Los parámetros que se configurarán son:

   - Clave de servidor (server-key): clave de servidor para cifrar/descifrar las credenciales de acceso protegido (PAC) (en hexadecimal).
   - Tiempo de vida para PAC (pac-ttl): establece el tiempo de vida de la PAC.

- ID de autoridad (authority-id) : establece el identificador de autoridad.
- Provisión anónima (no probada): configura si se permite la provisión anónima. Esto se activa como opción predeterminada.

Para la configuración a través de la GUI, elija Security > Local EAP > EAP-FAST Parameters e ingrese la clave del servidor, el tiempo de vida para la PAC, el ID de autoridad (en hexadecimal) y los valores de información de ID de autoridad.

Estos son los comandos de configuración de CLI que se deben utilizar para establecer estos parámetros para EAP-FAST:

```
<#root>

(Cisco Controller) >

config local-auth method fast server-key 12345678

(Cisco Controller) >

config local-auth method fast authority-id 43697369f1 CiscoA-ID

(Cisco Controller) >

config local-auth method fast pac-ttl 10
```

6. Habilite la autenticación local por WLAN:

   En la GUI, elija WLANs en el menú superior y seleccione la WLAN para la que desea configurar la autenticación local. Aparecerá una nueva ventana. Haga clic en las pestañas Security > AAA. Verifique la autenticación EAP local y seleccione el nombre de perfil EAP correcto del menú desplegable, como se muestra en este ejemplo:

   También puede ejecutar el comando de configuración CLI config wlan local-auth enable <profile-name> <wlan-id> , como se muestra aquí:

```
<#root>

(Cisco Controller) >

config wlan local-auth enable EAP-test 1
```

7. Establezca los parámetros de seguridad de la capa 2.

   Desde la interfaz GUI, en la ventana WLAN Edit vaya a las pestañas Security > Layer 2 y elija WPA+WPA2 en el menú desplegable Layer 2 Security. En la sección Parámetros WPA+WPA2, establezca la encriptación WPA en TKIP y la encriptación WPA2 en AES. A continuación, haga clic en Aplicar.

Desde la CLI, utilice estos comandos:

<#root>

```
(Cisco Controller) >
config wlan security wpa enable 1

(Cisco Controller) >
config wlan security wpa wpa1 ciphers tkip enable 1
(Cisco Controller) >
config wlan security wpa wpa2 ciphers aes enable 1
```

8. Verifique la Configuración:

<#root>

```
(Cisco Controller) >
show local-auth config

User credentials database search order:
    Primary .....................................
Local DB

Timer:
    Active timeout ............................. Undefined

Configured EAP profiles:

 Name ..................................... EAP-test

      Certificate issuer ........................ cisco
      Peer verification options:
        Check against CA certificates ........... Enabled
        Verify certificate CN identity .......... Disabled
        Check certificate date validity ......... Enabled
      EAP-FAST configuration:
        Local certificate required .............. No
        Client certificate required ............. No

Enabled methods ........................... leap fast tls

Configured on WLANs ....................... 1

EAP Method configuration:
```

```
    EAP-FAST:
--More-- or (q)uit
      Server key ................................. <hidden>
      TTL for the PAC ............................ 10
      Anonymous provision allowed ................ Yes
      Authority ID ............................... 43697369f10000000000000000000000
      Authority Information ...................... CiscoA-ID
```

Puede ver parámetros específicos de wlan 1 con el comando show wlan <wlan id>:

<#root>

```
(Cisco Controller) >

show wlan 1


WLAN Identifier.................................. 1
Profile Name..................................... austinlab
Network Name (SSID).............................. austinlab
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 0
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. 1800 seconds
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Disabled
CCX - AironetIe Support.......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
Dot11-Phone Mode (7920).......................... Disabled
Wired Protocol................................... None
--More-- or (q)uit
IPv6 Support..................................... Disabled
Radio Policy..................................... All

Local EAP Authentication........................ Enabled (Profile 'EAP-test')

Security


   802.11 Authentication:........................ Open System
   Static WEP Keys.............................. Disabled
   802.1X....................................... Disabled


Wi-Fi Protected Access (WPA/WPA2)............. Enabled
      WPA (SSN IE)............................... Enabled
         TKIP Cipher............................. Enabled

         AES Cipher.............................. Disabled


   WPA2 (RSN IE)............................... Enabled
```

```
        TKIP Cipher..............................  Disabled

  AES Cipher..............................  Enabled

                                                                  Auth Key Management
        802.1x...................................  Enabled
        PSK......................................  Disabled
        CCKM.....................................  Disabled
   CKIP .........................................  Disabled
   IP Security...................................  Disabled
   IP Security Passthru..........................  Disabled
   Web Based Authentication......................  Disabled
--More-- or (q)uit
   Web-Passthrough...............................  Disabled
   Conditional Web Redirect......................  Disabled
   Auto Anchor...................................  Disabled
   Cranite Passthru..............................  Disabled
   Fortress Passthru.............................  Disabled
   H-REAP Local Switching........................  Disabled
   Infrastructure MFP protection.................  Enabled
                                          (Global Infrastructure MFP Disabled)
   Client MFP....................................  Optional
   Tkip MIC Countermeasure Hold-down Timer.......  60

 Mobility Anchor List
 WLAN ID     IP Address       Status
```

Hay otros parámetros de autenticación local que se pueden configurar, en particular el temporizador de tiempo de espera activo. Este temporizador configura el período durante el cual se utiliza el EAP local después de que todos los servidores RADIUS hayan fallado.

En la GUI, elija Security > Local EAP > General y establezca el valor de tiempo. A continuación, haga clic en Aplicar.

Desde la CLI, ejecute estos comandos:

```
<#root>

(Cisco Controller) >

config local-auth active-timeout ?

<1 to 3600> Enter the timeout period for the Local EAP to remain active,
in seconds.
(Cisco Controller) >

config local-auth active-timeout 60
```

Puede verificar el valor para el cual se configura este temporizador cuando ejecuta el comando show local-auth config.

```
<#root>
```

```
(Cisco Controller) >

show local-auth config

User credentials database search order:
    Primary ..................................... Local DB


Timer:
    Active timeout ............................. 60


Configured EAP profiles:
    Name ........................................ EAP-test
... Skip
```

9. Si necesita generar y cargar la PAC manual, puede utilizar la GUI o la CLI.

   En la GUI, seleccione COMMANDS en el menú superior y elija Upload File en la lista del lado derecho. Seleccione PAC (Protected Access Credential, credencial de acceso protegido) en el menú desplegable Tipo de archivo. Introduzca todos los parámetros y haga clic en Cargar.

   Desde la CLI, ingrese estos comandos:

   <#root>

```
(Cisco Controller) >

transfer upload datatype pac


(Cisco Controller) >

transfer upload pac ?


username     Enter the user (identity) of the PAC

 (Cisco Controller) >

transfer upload pac test1 ?


<validity>     Enter the PAC validity period (days)

(Cisco Controller) >

transfer upload pac test1 60 ?


<password>     Enter a password to protect the PAC

 (Cisco Controller) >

transfer upload pac test1 60 cisco123


(Cisco Controller) >
```

```
transfer upload serverip 10.1.1.1


(Cisco Controller) >
transfer upload filename manual.pac


(Cisco Controller) >
transfer upload start


Mode..................................... TFTP
TFTP Server IP........................... 10.1.1.1
TFTP Path................................ /
TFTP Filename............................ manual.pac
Data Type................................ PAC
PAC User................................. test1
PAC Validity............................. 60 days
PAC Password............................. cisco123

Are you sure you want to start? (y/N) y
PAC transfer starting.
File transfer operation completed successfully.
```

Autoridad de certificación de Microsoft

Para utilizar la versión 2 de EAP-FAST y la autenticación EAP-TLS, el WLC y todos los dispositivos cliente deben tener un certificado válido y también deben conocer el certificado público de la autoridad de certificación.

Instalación

Si Windows 2000 Server aún no tiene instalados los servicios de Entidad emisora de certificados, deberá instalarlo.

Complete estos pasos para activar la Autoridad de certificación de Microsoft en un servidor Windows 2000:

1. En el Panel de control, elija Agregar o quitar programas. :
2. Seleccione Add/Remove Windows Components en el lado izquierdo.
3. Verifique Servicios de Certificate Server.

   Revise esta advertencia antes de continuar:
4. Seleccione el tipo de entidad emisora de certificados que desea instalar. Para crear una autoridad independiente simple, seleccione la CA raíz independiente.
5. Introduzca la información necesaria sobre la entidad emisora de certificados. Esta información crea un certificado autofirmado para la entidad emisora de certificados.

Recuerde el nombre de la CA que utiliza.

La entidad emisora de certificados almacena los certificados en una base de datos. Este ejemplo utiliza la configuración predeterminada propuesta por Microsoft:

6. Los servicios de Microsoft Certification Authority utilizan Microsoft Web Server de IIS para crear y administrar certificados de cliente y de servidor. Necesita reiniciar el servicio IIS para esto:

   Microsoft Windows 2000 Server instala ahora el nuevo servicio. Debe disponer del CD de instalación de Windows 2000 Server para instalar los nuevos componentes de Windows.

   La entidad emisora de certificados ya está instalada.

Instale el certificado en el controlador de LAN inalámbrica de Cisco

Para utilizar EAP-FAST versión 2 y EAP-TLS en el servidor EAP local de un Cisco Wireless LAN Controller, siga estos tres pasos:

1. Instale el certificado del dispositivo en el controlador de LAN inalámbrica.
2. Descargue un certificado de CA del proveedor al controlador de LAN inalámbrica.
3. Configure el controlador de LAN inalámbrica para utilizar EAP-TLS.

Observe que en el ejemplo que se muestra en este documento, Access Control Server (ACS) está instalado en el mismo host que Microsoft Active Directory y Microsoft Certification Authority, pero la configuración debe ser la misma si el servidor ACS está en un servidor diferente.

Instale el certificado del dispositivo en el controlador de LAN inalámbrica

Complete estos pasos:

1. . Complete estos pasos para generar el certificado para importar al WLC:

   a. Vaya a http://<serverIpAddr>/certsrv.

   b. Elija Request a Certificate y haga clic en Next.

   c. Elija Advanced Request y haga clic en Next.

   d. Elija Enviar una solicitud de certificado a esta CA mediante un formulario y haga clic en Siguiente.

   e. Elija Web server para Certificate Template e ingrese la información pertinente. A continuación, marque las claves como exportables.

   f. Ahora recibirá un certificado que necesita instalar en su equipo.

2. Complete estos pasos para recuperar el certificado de la PC:

   a. Abra un navegador Internet Explorer y elija Herramientas > Opciones de Internet > Contenido.

   b. Haga clic en Certificados.

   c. Seleccione el certificado recién instalado en el menú desplegable.

   d. Haga clic en Exportar.

   e. Haga clic en Next dos veces y elija Yes export the private key. Este formato es PKCS#12 (formato .PFX).

   f. Elija Enable strong protection.

   g. Escriba una contraseña.

   h. Guárdelo en un archivo <time2.pfx>.

3. Copie el certificado en formato PKCS#12 en cualquier equipo en el que tenga instalado Openssl para convertirlo al formato PEM.

```
openssl pkcs12 -in tme2.pfx -out tme2.pem

!--- The command to be given, -in


          .


Enter Import Password:

!--- Enter the password given previously, from step 2g.

MAC verified OK
Enter PEM pass phrase:

!--- Enter a phrase.

Verifying - Enter PEM pass phrase:
```

4. Descargue el certificado de dispositivo de formato PEM convertido en el WLC.

```
(Cisco Controller) >
transfer download datatype eapdevcert

(Cisco Controller) >
transfer download certpassword password

!--- From step 3.

Setting password to <cisco123>

(Cisco Controller) >
transfer download filename tme2.pem

(Cisco Controller) >
transfer download start

Mode............................................. TFTP
Data Type........................................ Vendor Dev Cert
TFTP Server IP................................... 10.1.1.12
TFTP Packet Timeout.............................. 6
TFTP Max Retries................................. 10
TFTP Path........................................ /
TFTP Filename.................................... tme2.pem

This may take some time.
Are you sure you want to start? (y/N) y

TFTP EAP Dev cert transfer starting.

Certificate installed.
  Reboot the switch to use new certificate.
```

5. Una vez reiniciado, verifique el certificado.

<#root>

```
(Cisco Controller) >
show local-auth certificates

Certificates available for Local EAP authentication:

Certificate issuer .............................. vendor
  CA certificate:
    Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
     Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
      Valid: 2007 Feb 28th, 19:35:21 GMT to 2012 Feb 28th, 19:44:44 GMT
  Device certificate:
    Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme2
     Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
```

```
        Valid: 2007 Mar 28th, 23:08:39 GMT to 2009 Mar 27th, 23:08:39 GMT
```

Descargar un certificado de CA del proveedor al controlador de LAN inalámbrica

Complete estos pasos:

1. Complete estos pasos para recuperar el certificado de CA del proveedor:
   a. Vaya a http://<serverIpAddr>/certsrv.
   b. Elija Recuperar el certificado de CA y haga clic en Siguiente.
   c. Elija el certificado de la CA.
   d. Haga clic en DER codificado.
   e. Haga clic en Download CA certificate y guarde el certificado como rootca.cer.
2. Convierta la CA del proveedor del formato DER al formato PEM con el comando openssl x509 -in rootca.cer -inform DER -out rootca.pem -outform PEM.

   El archivo de salida es rootca.pem en formato PEM.
3. Descargue el certificado de CA del proveedor:

```
<#root>
(Cisco Controller) >
transfer download datatype eapcacert

(Cisco Controller) >
transfer download filename ?

<filename>     Enter filename up to 16 alphanumeric characters.
(Cisco Controller) >
transfer download filename rootca.pem

(Cisco Controller) >
transfer download start ?

(Cisco Controller) >
transfer download start

Mode..................................... TFTP
Data Type................................ Vendor CA Cert
```

```
TFTP Server IP................................... 10.1.1.12
TFTP Packet Timeout.............................. 6
TFTP Max Retries................................. 10
TFTP Path........................................ /
TFTP Filename.................................... rootca.pem

This may take some time.
Are you sure you want to start? (y/N) y

TFTP EAP CA cert transfer starting.

Certificate installed.
  Reboot the switch to use new certificate.
```

Configuración del controlador de LAN inalámbrica para utilizar EAP-TLS

Complete estos pasos:

En la GUI, elija Security > Local EAP > Profiles, elija el perfil y verifique estas configuraciones:

- El certificado local obligatorio está activado.
- El certificado de cliente requerido está habilitado.
- El emisor del certificado es el proveedor.
- La comprobación de certificados de CA está habilitada.

Instalar el certificado de autoridad certificadora en el dispositivo cliente

Descargue e instale un certificado de CA raíz para el cliente

El cliente debe obtener un certificado de CA raíz de un servidor de entidad emisora de certificados. Hay varios métodos que puede utilizar para obtener un certificado de cliente e instalarlo en el equipo con Windows XP. Para adquirir un certificado válido, el usuario de Windows XP debe haber iniciado sesión con su ID de usuario y debe tener una conexión de red.

Se utilizó un explorador web en el cliente Windows XP y una conexión con cables a la red para obtener un certificado de cliente del servidor de la entidad emisora de certificados raíz privada. Este procedimiento se utiliza para obtener el certificado de cliente de un servidor de Microsoft Certification Authority:

1. Utilice un explorador web en el cliente y dirija el explorador al servidor de la entidad emisora de certificados. Para hacer esto, ingrese http://IP-address-of-Root-CA/certsrv.
2. Inicie sesión con Domain_Name\user_name. Debe iniciar sesión con el nombre de usuario de la persona que va a utilizar el cliente XP.

3. En la ventana Welcome, elija Retrieve a CA certificate y haga clic en Next.
4. Seleccione Codificación Base64 y Descargar certificado de CA.
5. En la ventana Certificado emitido, haga clic en Instalar este certificado y haga clic en Siguiente.
6. Elija Automatically select the certificate store y haga clic en Next, para un mensaje de importación exitoso.
7. Conectar con la entidad de certificación para recuperar el certificado de la entidad de certificación:
8. Haga clic en Descargar certificado de CA.
9. Para verificar que el certificado de la Autoridad de certificación esté correctamente instalado, abra Internet Explorer y elija Herramientas > Opciones de Internet > Contenido > Certificados.

   En Entidad emisora de certificados raíz de confianza, debe ver la entidad emisora de certificados recién instalada:

Generar un certificado de cliente para un dispositivo de cliente

El cliente debe obtener un certificado de un servidor de la autoridad de certificación para que el WLC autentique un cliente EAP-TLS de WLAN. Hay varios métodos que puede utilizar para obtener un certificado de cliente e instalarlo en el equipo con Windows XP. Para adquirir un certificado válido, el usuario de Windows XP debe haber iniciado sesión con su ID de usuario y debe tener una conexión de red (una conexión con cables o una conexión WLAN con la seguridad 802.1x deshabilitada).

Un explorador web en el cliente Windows XP y una conexión con cables a la red se utilizan para obtener un certificado de cliente del servidor de la entidad emisora de certificados raíz privada. Este procedimiento se utiliza para obtener el certificado de cliente de un servidor de Microsoft Certification Authority:

1. Utilice un explorador web en el cliente y dirija el explorador al servidor de la entidad emisora de certificados. Para hacer esto, ingrese http://IP-address-of-Root-CA/certsrv.
2. Inicie sesión con Domain_Name\user_name. Debe iniciar sesión con el nombre de usuario de la persona que utiliza el cliente XP. (El nombre de usuario se incrusta en el certificado de cliente.)
3. En la ventana de bienvenida, elija Solicitar un certificado y haga clic en Siguiente.
4. Elija Advanced request y haga clic en Next.
5. Elija Enviar una solicitud de certificado a esta CA mediante un formulario y haga clic en Siguiente.

6. En el formulario Advanced Certificate Request (Solicitud de certificado avanzada), elija la plantilla Certificate Template as User, especifique el tamaño de clave como 1024 y haga clic en Submit.

7. En la ventana Certificado emitido, haga clic en Instalar este certificado. Esto da como resultado la instalación correcta de un certificado de cliente en el cliente de Windows XP.

8. Seleccione Certificado de autenticación de cliente.

   Ahora se crea el certificado de cliente.

9. Para verificar que el certificado está instalado, vaya a Internet Explorer y elija Herramientas > Opciones de Internet > Contenido > Certificados. En la ficha Personal, debe ver el certificado.

EAP-TLS con Cisco Secure Services Client en el dispositivo cliente

Complete estos pasos:

1. El WLC, de forma predeterminada, difunde el SSID, por lo que se muestra en la lista Create Networks de SSIDs escaneados. Para crear un perfil de red, puede hacer clic en el SSID en la lista (Enterprise) y hacer clic en Create Network.

   Si la infraestructura WLAN está configurada con el SSID de difusión desactivado, debe agregar manualmente el SSID. Para hacer esto, haga clic en Agregar bajo Dispositivos de acceso e ingrese manualmente el SSID apropiado (por ejemplo, Empresa). Configure el comportamiento de la sonda activa para el cliente. Es decir, donde el cliente sondea activamente su SSID configurado. Especifique Actively search for this access device después de introducir el SSID en la ventana Add Access Device .

   Nota: La configuración del puerto no permite los modos de empresa (802.1X) si la configuración de autenticación EAP no se ha configurado primero para el perfil.

2. Haga clic en Create Network para iniciar la ventana Network Profile , que le permite asociar el SSID elegido (o configurado) con un mecanismo de autenticación. Asigne un nombre descriptivo al perfil.

   Nota: Bajo este perfil de autenticación se pueden asociar varios tipos de seguridad WLAN y/o SSID.

3. Active la autenticación y verifique el método EAP-TLS. Luego haga clic en Configure para configurar las propiedades EAP-TLS.

4. Bajo Resumen de Configuración de Red, haga clic en Modify para configurar los valores de EAP / credenciales.

5. Especifique Activar autenticación, elija EAP-TLS en Protocolo y elija Nombre de usuario

como identidad.

6. Especifique Use Single Sign on Credentials para utilizar las credenciales de inicio de sesión para la autenticación de red. Haga clic en Configure para configurar los parámetros EAP-TLS.

7. Para tener una configuración EAP-TLS segura, debe verificar el certificado del servidor RADIUS. Para hacer esto, marque Validar certificado de servidor.

8. Para validar el certificado de servidor RADIUS, debe proporcionar información de Cisco Secure Services Client para aceptar sólo el certificado correcto. Elija Client > Trusted Servers > Manage Current User Trusted Servers.

9. Especifique un nombre para la regla y compruebe el nombre del certificado de servidor.

   La configuración EAP-TLS ha finalizado.

10. Conéctese al perfil de red inalámbrica. Cisco Secure Services Client solicita el inicio de sesión del usuario:

    Cisco Secure Services Client recibe el certificado del servidor y lo comprueba (con la regla configurada y la entidad emisora de certificados instalada). A continuación, solicita el certificado que se va a utilizar para el usuario.

11. Después de que el cliente se autentique, elija SSID en Perfil en la pestaña Administrar redes y haga clic en Estado para consultar los detalles de conexión.

    La ventana Detalles de la conexión proporciona información sobre el dispositivo cliente, el estado y las estadísticas de la conexión, y el método de autenticación. La ficha WiFi Details (Detalles WiFi) proporciona detalles sobre el estado de la conexión 802.11, que incluye el RSSI, el canal 802.11 y la autenticación/cifrado.

Comandos de Debug

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 Debug antes de utilizar los comandos debug.

Estos comandos de depuración se pueden emplear en el WLC para monitorear el progreso del intercambio de autenticación:

- debug aaa events enable
- debug aaa detail enable
- debug dot1x events enable

- debug dot1x states enable
- debug aaa local-auth eap events enable

  O

- debug aaa all enable

Información Relacionada

- Guía de Configuración del Controlador de LAN Inalámbrica de Cisco, versión 4.1
- Soporte de la Tecnología de la WLAN
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).