Tecnología inalámbrica BYOD con el Identity Services Engine

Contenido

Introducción

El Cisco Identity Services Engine (ISE) es el servidor de políticas de la última generación de Cisco que proporciona la infraestructura de la autenticación y autorización a la solución de Cisco TrustSec. También proporciona dos otros servicios críticos:

- El primer servicio es proporcionar una manera de perfilar el tipo de dispositivo de punto final basado automáticamente en los atributos que Cisco ISE recibe de las diversas fuentes de información. Este servicio (llamado Profiler) proporciona las funciones equivalentes a lo que ha ofrecido Cisco previamente con el dispositivo del Cisco NAC Profiler.
- Otro servicio importante que Cisco ISE proporciona es analizar la conformidad del punto final; por ejemplo, instalación del software AV/AS y su validez del archivo de definición (conocidas como postura). Cisco ha estado proveyendo previamente de esta función exacta de la postura solamente el dispositivo NAC de Cisco.

Cisco ISE proporciona un nivel equivalente de funciones, y se integra con los mecanismos de autenticación del 802.1x.

Cisco ISE integrado con los reguladores del Wireless LAN (WLCs) puede proporcionar el perfilado de los mecanismos de los dispositivos móviles tales como iDevices de Apple (iPhone, iPad, e iPod), Android-basó los smartphones, y otros. Para los usuarios del 802.1x, Cisco ISE puede proporcionar el mismo nivel de servicios tales como perfilado y exploración de la postura. Los servicios del invitado en Cisco ISE pueden también ser integrados con el WLC de Cisco reorientando las peticiones de la autenticación Web a Cisco ISE para la autenticación.

Este documento introduce la solución de red inalámbrica para Bring Your Own Device (BYOD), por ejemplo proporcionar al acceso distinguido basado en los puntos finales conocidos y la política de usuario. Este documento no proporciona la solución completa de BYOD, sino sirve demostrar un caso simple del uso del acceso dinámico. Otros ejemplos de configuración incluyen usando el portal del patrocinador ISE, en donde un usuario con privilegios puede patrocinar a un invitado para disposición el acceso de invitado inalámbrico.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Controlador LAN 2504 o 2106 de la tecnología inalámbrica de Cisco con la versión de software 7.2.103
- Puertos del Catalyst 3560 – 8
- WLC 2504
- Identity Services Engine 1.0MR (versión de imagen del servidor de VMware)
- Servidor de Windows 2008 (imagen de VMware) — los 512M, disco 20GBActive DirectoryDNSDHCPServicios de certificados

Topología

Convenciones

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

NAC del regulador RADIUS del Wireless LAN y descripción CoA

Esta configuración permite al WLC para buscar los Pares AV del cambio de dirección URL que vienen del servidor de RADIUS ISE. Esto está solamente en una red inalámbrica (WLAN) que se ate a una interfaz con la configuración de NAC RADIUS habilitada. Cuando el cisco av-pair para el cambio de dirección URL se recibe, ponen al cliente en el estado POSTURE_REQD. Éste es básicamente lo mismo que el estado WEBAUTH_REQD internamente en el regulador.

Cuando el servidor de RADIUS ISE juzga el cliente es Posture_Compliant, él publica un CoA ReAuth. El Session_ID se utiliza para unirlo. Con este nuevo AuthC (re-auth) no envía los Pares AV URL-Redirec. Porque no hay URL reoriente los Pares AV, el WLC sabe que el cliente no requiere la postura más de largo.

Si la configuración de NAC RADIUS no se habilita, el WLC ignora el URL reorienta los VSA.

CoA-ReAuth: Esto se habilita con la determinación del RFC 3576. La capacidad de ReAuth fue agregada a los comandos existentes CoA que fueron soportados previamente.

La configuración de NAC RADIUS es mutuamente - exclusiva de esta capacidad, aunque se requiera para que el CoA trabaje.

PRE-postura ACL: Cuando un cliente está en el estado POSTURE_REQ, el comportamiento predeterminado del WLC es bloquear todo el tráfico excepto DHCP/DNS. La PRE-postura ACL (que se llama en el Par AV URL-reorientar-ACL) se aplica al cliente, y qué se permite en ese ACL es lo que puede alcanzar el cliente.

PRE-auth ACL contra la invalidación del VLA N: Un VLA N de la cuarentena o de AuthC que es diferente del Acceso-VLA N no se soporta en 7.0MR1. Si usted fija un VLA N del servidor de políticas, será el VLA N para la sesión entera. No hay cambios de VLAN necesarios después de primer AuthZ.

NAC del regulador RADIUS del Wireless LAN y flujo de la

característica CoA

La figura abajo proporciona los detalles del intercambio del mensaje cuando autentican al cliente a la validación del servidor de extremo posterior y de la postura del NAC.

1. El cliente autentica usando la autenticación del dot1x.
2. El acceso a RADIUS valida lleva el URL reorientado para el puerto 80 y el PRE-auth ACL que incluye permitir los IP Addresses y los puertos, o VLA N de la cuarentena.
3. Reorientarán al cliente al URL proporcionado en el acceso valida, y puso en un nuevo estado hasta que se haga la validación de la postura. El cliente en este estado habla con el servidor ISE y se valida contra las directivas configuradas en el servidor del NAC ISE.
4. El agente del NAC en el cliente inicia la validación de la postura (tráfico al puerto 80): El agente envía la petición de la detección HTTP al puerto 80 que el regulador reorienta al URL proporcionado en el acceso valida. El ISE sabe que cliente que intenta alcanzar y responde directamente al cliente. Esta manera que el cliente aprende sobre el ISE IP del servidor y de ahora en adelante, el cliente habla directamente con el servidor ISE.
5. El WLC permite este tráfico porque el ACL se configura para permitir este tráfico. En caso de la invalidación del VLA N, se interliga el tráfico de modo que alcance el servidor ISE.
6. Una vez que el ISE-cliente completa la evaluación, un CoA-req RADIUS con el servicio del reauth se envía al WLC. Esto inicia la reautentificación del cliente (enviando el EAP START). Una vez que la reautentificación tiene éxito, el ISE envía el acceso valida con un nuevo ACL (eventualmente) y ningún URL reorienta, o accede el VLA N.
7. El WLC tiene el soporte para el CoA-req y Desconexión-req según el RFC 3576. Las necesidades del WLC de soportar el CoA-req para el servicio del re-auth, según el RFC 5176.
8. En vez de los ACL transferibles, los ACL preconfigurados se utilizan en el WLC. El servidor ISE apenas envía el nombre ACL, que se configura ya en el regulador.
9. Este diseño debe trabajar para los casos del VLA N y ACL. En caso de la invalidación del VLA N, apenas reorientamos el puerto 80 nos reorientamos y permitimos el resto (del Bridge) del tráfico en el VLA N de la cuarentena. Para el ACL, el PRE-auth ACL recibido en el acceso valida es aplicado.

Esta figura proporciona una representación visual de este flujo de la característica:

ISE que perfila la descripción

El servicio del profiler de Cisco ISE proporciona las funciones en el descubrimiento, la localización, y determinar de las capacidades de todos los puntos finales asociados en su red, sin importar sus tipos de dispositivo, para asegurar y mantener el acceso apropiado a su red para empresas. Recoge sobre todo un atributo o un conjunto de los atributos de todos los puntos finales en su red y los clasifica según sus perfiles.

El profiler se comprende de estos componentes:

- El sensor contiene varias sondas. Las sondas capturan los paquetes de red preguntando los dispositivos de acceso a la red, y remiten los atributos y sus valores de atributo que se recogen de los puntos finales al analizador.
- Un analizador evalúa los puntos finales usando las directivas configuradas y los grupos de la identidad para hacer juego los atributos y sus valores de atributo recogidos, que clasifica los

puntos finales al grupo especificado y salva los puntos finales con el perfil correspondido con en la base de datos de Cisco ISE.

Para la detección del dispositivo móvil, es recomienda utilizar una combinación de estas sondas para la identificación de dispositivo apropiada:

- RADIUS (Llamar-Estación-ID): Proporciona la dirección MAC (el OUI)
- DHCP (hostname): Nombre de host – el nombre de host predeterminado puede incluir el tipo de dispositivo; por ejemplo: jsmith-ipad
- DNS (operaciones de búsqueda reversas IP): FQDN - el nombre de host predeterminado puede incluir el tipo de dispositivo
- HTTP (agente de usuario): Detalles en el tipo de dispositivo móvil específico

En este ejemplo de un iPad, el profiler captura la información del buscador Web del atributo del agente de usuario, así como otros atributos HTTP de los mensajes request, y los agrega a la lista de atributos del punto final.

Cree a los usuarios internos de la identidad

El Active Directory MS (AD) no se requiere para un proof-of-concept simple. El ISE se puede utilizar como el único almacén de la identidad, que incluye el distinción del acceso de usuarios para el acceso y el control de políticas granular.

En la versión de ISE 1.0, usando la integración AD, el ISE puede utilizar a los grupos AD en las directivas de la autorización. Si se utiliza el almacén del usuario interno ISE (ninguna integración AD), los grupos no pueden ser utilizados en las directivas conjuntamente con los grupos de la identidad del dispositivo (bug identificado que se resolverá en ISE 1.1). Por lo tanto, solamente los usuarios individuales pueden ser distinguidos, por ejemplo los empleados o los contratistas cuando están utilizados además de los grupos de la identidad del dispositivo.

Complete estos pasos:

1. Abra una ventana del buscador en el direccionamiento de https://ISEip.
2. Navegue a la **administración > a la Administración de la identidad > a las identidades**.
3. Seleccione a los **usuarios**, después haga clic **agregan** (usuario del acceso a la red). Ingrese estos valores de usuario y asígnelos al grupo del empleado:Nombre: empleadoContraseña XXXX
4. Haga clic en Submit (Enviar).Nombre: contratistaContraseña XXXX
5. Confirme ambas cuentas se crean.

Agregue el regulador del Wireless LAN al ISE

Cualquier dispositivo que inicie los pedidos de RADIUS al ISE debe tener una definición en el ISE. Estos dispositivos de red se definen sobre la base de su dirección IP. Las definiciones del dispositivo de red ISE pueden especificar los alcances del IP Address que permiten así que la definición represente los dispositivos reales múltiples.

Más allá de qué se requiere para la comunicación RADIUS, las definiciones del dispositivo de red ISE contienen las configuraciones para la otra comunicación ISE/device, tal como SNMP y SSH.

Otro aspecto importante de la definición del dispositivo de red está agrupando apropiadamente

los dispositivos para poder leveraged éste que agrupa en la directiva de acceso a la red.

En este ejercicio, las Definiciones del dispositivo requeridas para su laboratorio se configuran.

Complete estos pasos:

1. Del ISE vaya a la **administración > a los recursos de red > a los dispositivos de red**.
2. De los dispositivos de red, haga click en Add Ingrese el IP Address, enmascare la configuración de la autenticación del control, después ingrese “Cisco” para el secreto compartido.
3. Salve la entrada del WLC, y confirme el regulador en la lista.

Configure el ISE para la autenticación inalámbrica

El ISE necesita ser configurado para los clientes de red inalámbrica de autenticidad del 802.1x y utilizar el Active Directory como el almacén de la identidad.

Complete estos pasos:

1. Del ISE navegue a la **directiva > a la autenticación**.
2. Haga clic para ampliar el dot1x > el Wired_802.1X (-).
3. Haga clic en el icono del engranaje **para agregar la condición de la biblioteca**.
4. Del descenso-abajo de la selección de la condición, elija la **condición compuesta > Wireless_802.1X**.
5. Fije la condición expresa a **O**.
6. Amplíe después de permiten la opción de los protocolos, y validan a los usuarios internos predeterminados (valor por defecto).
7. Deje todo lo demás en el valor por defecto. Haga clic la **salvaguardia** para completar los pasos.

Ate el regulador del Wireless LAN con correa

Conexión del WLC con una red

Un Guía de despliegue del regulador del Wireless LAN del Cisco2500 está también disponible en el Guía de despliegue inalámbrico del regulador de las Cisco 2500 Series.

Configure el regulador que usa al Asisitente de lanzamiento

```
(Cisco Controller)
 Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup
 Would you like to terminate autoinstall? [yes]: yes AUTO-INSTALL: process terminated
-- no configuration loaded System Name [Cisco_d9:24:44] (31 characters max):
   ISE-Podx Enter Administrative User Name (24 characters max): admin
   Enter Administrative Password
   (3 to 24 characters): Cisco123
   Re-enter Administrative Password: Cisco123
Management Interface IP Address: 10.10.10.5
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Management Interface VLAN Identifier (0 = untagged): 0
```

```
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.10.10.10
 Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: ISE
 Network Name (SSID): PODx
Configure DHCP Bridging Mode [yes][NO]: no
Allow Static IP Addresses [YES][no]: no
 Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
 Enter Country Code list (enter 'help' for a list of countries) [US]: US

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes
 Configure a NTP server now? [YES][no]: no
Configure the ntp system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: mm/dd/yy
Enter the time in HH:MM:SS format: hh:mm:ss
Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
 Configuration saved!
 Resetting system with new configuration...
Restarting system.
```

Configuración del switch de vecino

El regulador está conectado con el acceso de Ethernet en el switch de vecindad (fast ethernet 1). El puerto del switch de vecino se configura como tronco 802.1q y permite todos los VLA N en el trunk. El VLAN nativo 10 permite que la interfaz de administración del WLC sea conectada.

La configuración del puerto del 802.1Q Switch es como sigue:

```
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN 10
switchport mode trunk
end
```

Agregue a los servidores de autenticación (ISE) al WLC

El ISE necesita ser agregado al WLC para habilitar el 802.1x y la característica CoA para los puntos finales de red inalámbrica.

Complete estos pasos:

1. Abra a un navegador, después conecte con el WLC de la vaina (usando el HTTP seguro) > https://wlc.
2. Navegue a **Security > Authentication > nuevo**.
3. Ingrese estos valores:Dirección IP del servidor: 10.10.10.70 (asignación del control)Secreto compartido: CiscoSoporte para el RFC 3576 (CoA): Habilitado (valor por defecto)Todo lo demás: Predeterminado
4. El tecleo **se aplica** para continuar.
5. Seleccione el **RADIUS considerando > Add NUEVO**.
6. Ingrese estos valores:Dirección IP del servidor: 10.10.10.70Secreto compartido: CiscoTodo lo demás: Predeterminado
7. El tecleo **aplica**, después salva la configuración para el WLC.

Cree la interfaz dinámica del empleado del WLC

Complete estos pasos para agregar una nueva interfaz dinámica para el WLC y asociarla al VLA N del empleado:

1. Del WLC, navegue al **regulador > a las interfaces**. Entonces, haga clic **nuevo**.
2. Del WLC, navegue al **regulador > a las interfaces**. Ingrese el siguiente:Nombre de la interfaz: EmpleadoIdentificación de VLAN: 11
3. Ingrese el siguiente para la interfaz del empleado:Número del puerto: 1Identificador de VLAN: 11Dirección IP: 10.10.11.5Netmask: 255.255.255.0Gateway: 10.10.11.1DHCP: 10.10.10.10
4. Confirme que la nueva interfaz dinámica del empleado está creada.

Cree la interfaz dinámica del invitado del WLC

Complete estos pasos para agregar una nueva interfaz dinámica para el WLC y asociarla al VLA N del invitado:

1. Del WLC, navegue al **regulador > a las interfaces**. Entonces, haga clic **nuevo**.
2. Del WLC, navegue al **regulador > a las interfaces**. Ingrese el siguiente:Nombre de la interfaz: GuestIdentificación de VLAN: 12
3. Ingrese éstos para la interfaz del invitado:Número del puerto: 1Identificador de VLAN: 12Dirección IP: 10.10.12.5Netmask: 255.255.255.0Gateway: 10.10.12.1DHCP: 10.10.10.10
4. Confirme que se ha agregado la interfaz del invitado.

Agregue la red inalámbrica (WLAN) del 802.1x

De la carga inicial inicial del WLC, pudo haber habido una red inalámbrica (WLAN) predeterminada creada. Si es así modifiqúela o cree una nueva red inalámbrica (WLAN) para soportar la autenticación inalámbrica del 802.1x como se indica en la guía.

Complete estos pasos:

1. Del WLC, navegue a la **red inalámbrica (WLAN) > crean nuevo**.
2. Para el WLAN, ingrese el siguiente:Nombre del perfil: pod1xSSID: Lo mismo
3. Para las configuraciones > la ficha general de la red inalámbrica (WLAN), utilice el siguiente:Radie la directiva: TodosInterfaz/grupo: AdministraciónTodo lo demás: predeterminado
4. Para la lengueta > la capa 2 del > Security (Seguridad) de la red inalámbrica (WLAN), fije el siguiente:Acode 2 Security:WPA+WPA2Directiva WPA2/cifrado: Habilitado/AESMgmt dominante del auth: 802.1x
5. Para los servidores de la lengueta del > Security (Seguridad) de la red inalámbrica (WLAN) >AAA, fije el siguiente:El servidor de radio sobregraba la interfaz: InhabilitadoAutenticación/servidores de contabilidad: HabilitadoServer1: 10.10.10.70
6. Para la red inalámbrica (WLAN) > la ficha Avanzadas, fije el siguiente:Permita la invalidación AAA: HabilitadoEstado del NAC: NAC del radio (seleccionado)
7. De nuevo a la red inalámbrica (WLAN) > a la red inalámbrica (WLAN) de la ficha general >

del permiso (casilla de verificación).

Pruebe las interfaces dinámicas del WLC

Usted necesita hacer una verificación rápida para las interfaces válidas del empleado y del invitado. Utilice cualquier dispositivo para asociarse a la red inalámbrica (WLAN), después cambie la asignación de la interfaz de la red inalámbrica (WLAN).

1. Del WLC, navegue a la **red inalámbrica (WLAN) > a los WLAN**. Haga clic para editar su SSID seguro creado en el ejercicio anterior.
2. Cambie la interfaz/el grupo de interfaces al **empleado**, después haga clic **se aplican**.
3. Si está configurado correctamente, un dispositivo recibe una dirección IP del VLA N del empleado (10.10.11.0/24). Este ejemplo muestra un dispositivo IOS que consiga una nueva dirección IP.
4. La interfaz anterior se ha confirmado, cambia la asignación de la interfaz de la red inalámbrica (WLAN) al **invitado**, después hace clic una vez **se aplica**.
5. Si está configurado correctamente, un dispositivo recibe una dirección IP del VLA N del invitado (10.10.12.0/24). Este ejemplo muestra un dispositivo IOS que consiga una nueva dirección IP.
6. **IMPORTANTE:** Cambie la asignación de la interfaz de nuevo a la Administración original.
7. El tecleo **aplica** y salva la configuración para el WLC.

Autenticación inalámbrica para IOS (iPhone/iPad)

Asocie al WLC vía un SSID autenticado un usuario interno (o al usuario integrada, AD) usando un dispositivo IOS tal como un iPhone, un iPad, o un iPod. Salte estos pasos si no aplicables.

1. En el dispositivo IOS, vaya a las configuraciones de la red inalámbrica (WLAN). Habilite WIFI, después seleccione el SSID habilitado 802.1x creado en la sección anterior.
2. Proporcione esta información para conectar:Nombre de usuario: empleado (interno – Empleado) o contratista (interno – contratista)Contraseña XXXX
3. Haga clic para validar el certificado ISE.
4. Confirme que el dispositivo IOS está consiguiendo una dirección IP de la interfaz de la Administración (VLAN10).
5. En el WLC > el monitor > los clientes, verifique la información del punto final incluyendo el uso, estado, y tipo EAP.
6. Semejantemente, la información del cliente se puede proporcionar por ISE > página del monitor > de la autenticación.
7. Haga clic el icono de los **detalles** para perforar abajo a la sesión para la información minuciosa de la sesión.

Agregue la postura reorientan el ACL al WLC

La postura reorienta el ACL se configura en el WLC, donde el ISE utilizará para restringir al cliente para la postura. Con eficacia y en un mínimo el ACL permite el tráfico entre el ISE. Las reglas opcionales se pueden agregar en este ACL si es necesario.

1. Navegue al **> Security (Seguridad) > a las listas de control de acceso > a las listas de control de acceso del WLC**. Haga clic en **New**.
2. Proporcione un nombre (ACL-POSTURE-REDIRECT) para el ACL.
3. El tecleo **agrega la nueva regla** para el nuevo ACL. Fije los valores siguientes a la secuencia #1 ACL. El tecleo **se aplica** cuando está acabado.Fuente: NingunosDestino: Dirección IP 10.10.10.70, 255.255.255.255Protocolo: NingunosAcción: Permiso
4. Confirme la secuencia se ha agregado.
5. El tecleo **agrega la nueva regla**. Fije los valores siguientes a la secuencia #2 ACL. El tecleo **se aplica** cuando está acabado.Fuente: Dirección IP 10.10.10.70, 255.255.255.255Destino: NingunosProtocolo: NingunosAcción: Permiso
6. Confirme la secuencia se ha agregado.
7. Fije los valores siguientes a la secuencia #3 ACL. El tecleo **se aplica** cuando está acabado.Fuente: NingunosDestino: NingunosProtocolo: UDPPuerto de origen: DNSPuerto destino: NingunosAcción: Permiso
8. Confirme la secuencia se ha agregado.
9. El tecleo **agrega la nueva regla**. Fije los valores siguientes a la secuencia #4 ACL. El tecleo **se aplica** cuando está acabado.Fuente: NingunosDestino: NingunosProtocolo: UDPPuerto de origen: NingunosPuerto destino: DNSAcción: Permiso
10. Confirme la secuencia se ha agregado.
11. Salve la configuración actual del WLC.

Habilite el perfilado de las sondas en el ISE

El ISE necesita ser configurado como sondas para perfilar con eficacia los puntos finales. Por abandono, se inhabilitan estas opciones. Esta sección muestra cómo configurar el ISE para ser sondas.

1. De la Administración ISE, navegue a la **administración > al sistema > al despliegue**.
2. Elija el **ISE**. El tecleo **edita el host ISE**.
3. De la página del nodo del editar, seleccione la configuración de perfilado y configure el siguiente:DHCP: Habilitado, todos (o valor por defecto)DHCPSPAN: Habilitado, todos (o valor por defecto)HTTP: Habilitado, todos (o valor por defecto)RADIUS: Habilitado, N/ADNS: Habilitado, N/A
4. Reasocie los dispositivos (iPhone/iPads/Droids/Mac, etc.).
5. Confirme las identidades del punto final ISE. Navegue a la **administración > a la Administración de la identidad > a las identidades**. Haga clic en los puntos finales para enumerar se ha perfilado qué.**Nota:** El perfilado de la inicial es de las sondas RADIUS.

Directivas del perfil del permiso ISE para los dispositivos

El cuadro de los, ISE proporciona una biblioteca de los diversos perfiles del punto final. Complete estos pasos para habilitar los perfiles para los dispositivos:

1. Del ISE, navegue a la **directiva > perfilando**.
2. Del panel izquierdo, amplíe el **perfilado de las directivas**.
3. Haga clic el **iPad del dispositivo de Apple > de Apple**, y fije el siguiente:Directiva habilitada: HabilitadoCree al grupo de la identidad que corresponde con: Seleccionado

4. **El iPhone del dispositivo de Apple del** tecleo **> de Apple**, fijó el siguiente:Directiva habilitada: HabilitadoCree al grupo de la identidad que corresponde con: Seleccionado
5. El tecleo **Android**, fijó el siguiente:Directiva habilitada: HabilitadoCree al grupo de la identidad que corresponde con: Seleccionado

El perfil de la autorización ISE para la detección de la postura reorienta

Complete estos pasos para configurar una postura de la directiva de la autorización reorientan permite que los nuevos dispositivos sean reorientados al ISE para la detección adecuada y perfilar:

1. Del ISE, navegue a la **directiva > a los elementos > a los resultados de la directiva**.
2. Amplíe la **autorización**. Haga clic los **perfiles de la autorización** (panel izquierdo) y el haga click en Add
3. Cree el perfil de la autorización con el siguiente:Nombre: Posture_RemediationTipo de acceso: Access_AcceptHerramientas comunes:Detección de la postura, habilitadaDetección de la postura, ACL ACL-POSTURE-REDIRECT
4. El tecleo **somete** para completar esta tarea.
5. Confirme que el nuevo perfil de la autorización está agregado.

Cree el perfil de la autorización ISE para el empleado

Agregar un perfil de la autorización para un empleado permite que el ISE autorice y que permita el acceso con los atributos asignados. El VLAN 11 del empleado se asigna en este caso.

Complete estos pasos:

1. Del ISE, navegue a la **directiva > a los resultados**. Amplíe la **autorización**, después haga clic los **perfiles de la autorización** y el haga click en Add
2. Ingrese el siguiente para el perfil de la autorización del empleado:Nombre: Employee_WirelessTareas del campo común:VLA N, habilitadoVLA N, valor sub 11
3. El tecleo **somete** para completar esta tarea.
4. Confirme que el nuevo perfil de la autorización del empleado fue creado.

Cree el perfil de la autorización ISE para el contratista

Agregar un perfil de la autorización para un contratista permite que el ISE autorice y que permita el acceso con los atributos asignados. El VLAN 12 del contratista se asigna en este caso.

Complete estos pasos:

1. Del ISE, navegue a la **directiva > a los resultados**. Amplíe la **autorización**, después haga clic los **perfiles de la autorización** y el haga click en Add
2. Ingrese el siguiente para el perfil de la autorización del empleado:Nombre: Employee_WirelessTareas del campo común:VLA N, habilitadoVLA N, valor sub 12
3. El tecleo **somete** para completar esta tarea.

4. Confirme que el perfil de la autorización del contratista fue creado.

Directiva de la autorización para la postura/el perfilado del dispositivo

Poca información se sabe sobre un nuevo dispositivo cuando primero viene sobre la red, un administrador creará la directiva apropiada para permitir que los puntos finales desconocidos sean identificados antes de permitir el acceso. En este ejercicio, la directiva de la autorización será creada de modo que un nuevo dispositivo sea reorientado al ISE para la evaluación de la postura (para los dispositivos móviles sea agentless, por lo tanto solamente el perfilado es relevante); los puntos finales serán reorientados al porta prisionero ISE e identificados.

Complete estos pasos:

1. Del ISE, navegue a la **directiva > a la autorización**.
2. Hay una directiva para los Teléfonos IP Profiled Cisco. Éste es cuadro de los. Edite esto como directiva de la postura.
3. Ingrese los valores siguientes para esta directiva:‘Nombre de la regla Posture_RemediationGrupos de la identidad: NingunosOtras condiciones > crean nuevo: Sesión (avanzada) > PostureStatusPostureStatus > iguales: Desconocido
4. Fije el siguiente para los permisos:Permisos > estándar: Posture_Remediation
5. Haga clic en Save (Guardar).**Nota:** Los elementos de la directiva alternativamente de encargo se pueden crear para agregar la facilidad de empleo.

Directiva de prueba de la corrección de la postura

A la demostración simple puede ser realizado para mostrar que el ISE está perfilando correctamente un nuevo dispositivo basado en la directiva de la postura.

1. Del ISE, navegue a la **administración > a la Administración de la identidad > a las identidades**.
2. Haga clic los **puntos finales**. Asocie y conecte un dispositivo (un iPhone en este ejemplo).
3. Restaure la lista de los puntos finales. Observe se da qué información.
4. Del dispositivo de punto final, hojee a:URL: http://www (o 10.10.10.10)Se reorienta el dispositivo. Valide cualquier prompt para los Certificados.
5. Después de que el dispositivo móvil haya reorientado totalmente, del ISE restaure la lista de los puntos finales otra vez. Observe qué ha cambiado. El punto final anterior (por ejemplo, Apple-dispositivo) debe haber cambiado a “Apple-iPhone” etc. La razón es que el sondeo HTTP obtiene con eficacia la información del agente de usuario, como parte del proceso de la reorientación al portal del cautivo.

Directiva de la autorización para el acceso distinguido

Después con éxito de probar la autorización de la postura, continúe construyendo las directivas para soportar el acceso distinguido para el empleado y el contratista con los dispositivos sabidos y diverso específico de la asignación VLAN al rol del usuario (en este escenario, empleado y contratista).

Complete estos pasos:

1. Navegue a **ISE > directiva > autorización**.
2. Agregue/separador de millares una nueva regla sobre la directiva/la línea de la corrección de la postura.
3. Ingrese los valores siguientes para esta directiva:‘Nombre de la regla EmpleadoGrupos de la identidad (amplíese): Grupos de la identidad del punto finalGrupos de la identidad del punto final: PerfiladoPerfilado: Android, Apple-iPad o Apple-iPhone
4. Para especificar los tipos de dispositivo adicionales, haga clic **+** y agregue más dispositivos (si es necesario):Grupos de la identidad del punto final: PerfiladoPerfilado: Android, Apple-iPad o Apple-iPhone
5. Especifique los valores de los permisos siguientes para esta directiva:Otras condiciones (amplíese): Cree la nueva condición (la opción avanzada)Condición > expresión (de la lista): InternalUser > nombreInternalUser > nombre: empleado
6. Agregue una condición para la sesión de la postura obediente:Los permisos > perfilan > estándar: Employee_Wireless
7. Haga clic en Save (Guardar). Confirme que la directiva se ha agregado correctamente.
8. Continúe agregando la directiva del contratista. En este documento, la directiva anterior se duplica para acelerar el proceso (o, usted puede configurar manualmente para la práctica adecuada).De la directiva > de las acciones del empleado, **duplicado del** tecleo **abajo**.
9. Edite los campos siguientes para esta directiva (copia duplicado):‘Nombre de la regla ContratistaLas otras condiciones > InternalUser > nombre: contratistaPermisos: Contractor_Wireless
10. Haga clic en Save (Guardar). Confirme que la copia duplicada anterior (o la nueva directiva) está configurada correctamente.
11. Para ver las directivas de antemano, haga clic el Directiva-en-uno-**vistazo**.La directiva de un vistazo ve proporciona consolidado resumido y fácil considerar las directivas.

CoA de prueba para el acceso distinguido

Con los perfiles y las directivas de la autorización preparados para distinguir el acceso, es hora de probar. Teniendo una sola red inalámbrica (WLAN) asegurada, asignarán un empleado el VLA N del empleado y un contratista estará para el VLA N del contratista. Apple iPhone/iPad se utiliza en los próximos ejemplos.

Complete estos pasos:

1. Conecte con la red inalámbrica (WLAN) asegurada (POD1x) con el dispositivo móvil y utilice estas credenciales:Nombre de usuario: empleadoContraseña
2. El tecleo **se une a**. Confirme que el empleado es el VLAN asignado 11 (VLA N del empleado).
3. El tecleo **olvida esta red**. Confirme haciendo clic **olvidan**.
4. Vaya al WLC y quite las conexiones cliente existentes (si lo mismo fue utilizada en los pasos anteriores). Navegue **para monitorear > los clientes > dirección MAC**, después haga clic **quitan**.
5. Otra manera segura de borrar a las sesiones de cliente anteriores es inhabilitar/permiso la red inalámbrica (WLAN).Vaya al **WLC > a los WLAN > a la red inalámbrica (WLAN)**, después haga clic la red inalámbrica (WLAN) para editar.el O.N.U-control **habilitado > se aplica**

(inhabilitar).Marque el cuadro para **habilitado > se aplican** (volver a permitir).
6. Vuelva al dispositivo móvil. Conecte otra vez con la misma red inalámbrica (WLAN) con estas credenciales:Nombre de usuario: contratistaContraseña XXXX
7. El tecleo **se une a**. Confirme que el usuario del contratista es el VLAN asignado 12 (VLA N del contratista/del invitado).
8. Usted puede mirar la opinión en tiempo real del registro ISE en **ISE > monitor > las autorizaciones**. Usted debe ver que los usuarios individuales (empleado, contratista) consiguen los perfiles distinguidos de la autorización (Employee_WirelessvsContractor_Wireless) en diversos VLA N.

red inalámbrica (WLAN) del invitado del WLC

Complete estos pasos para agregar una red inalámbrica (WLAN) del invitado para permitir que los invitados accedan el portal del invitado del patrocinador ISE:

1. Del WLC, navegue a los **WLAN > los WLAN > Add nuevos**.
2. Ingrese el siguiente para el nuevo invitado WLAN:Nombre del perfil: pod1guestSSID: pod1guest
3. Haga clic en Apply (Aplicar).
4. Ingrese el siguiente bajo el invitado WLAN > ficha general:Estado: InhabilitadoInterfaz/grupo de interfaces: Guest
5. Navegue al **> Security (Seguridad) del** invitado **WLAN > a Layer2** y ingrese el siguiente:Seguridad de la capa 2: Ninguno
6. Navegue al **> Security (Seguridad) del** invitado **WLAN > a la** lengueta **Layer3** y ingrese el siguiente:Seguridad de la capa 3: NingunoDirectiva de la red: HabilitadoValor del submarino de la directiva de la red: AutenticaciónAutenticación previa ACL: ACL-POSTURE-REDIRECTTipo del auth de la red: Externo (reoriente al servidor externo)URL: https://10.10.10.70:8443/guestportal/Login.action
7. Haga clic en Apply (Aplicar).
8. Aseegurese **salvar la configuración del WLC**.

Prueba de la red inalámbrica (WLAN) del invitado y del portal del invitado

Ahora, usted puede probar la configuración de la red inalámbrica (WLAN) del invitado. Debe reorientar a los invitados al portal del invitado ISE.

Complete estos pasos:

1. De un dispositivo IOS tal como un iPhone, navegue a las **redes > al permiso del Wi-Fi**. Entonces, seleccione la red del invitado de la VAINA.
2. Su dispositivo IOS debe mostrar un IP Address válido del VLA N del invitado (10.10.12.0/24).
3. Abra al navegador del safari y conecte con:URL: http://10.10.10.10Una autenticación Web reorienta aparece.
4. El tecleo **continúa** hasta que usted haya llegado la página porta del invitado ISE.El tiro de pantalla siguiente de la muestra muestra el dispositivo IOS en un login porta del invitado. Esto confirma que la configuración correcta para portal del invitado de la red inalámbrica

(WLAN) y ISE es activa.

La Tecnología inalámbrica ISE patrocinó el acceso de invitado

El ISE se puede configurar para permitir que patrocinen a los invitados. En este caso usted configurará las directivas del invitado ISE para permitir a los usuarios internos o AD del dominio (si es integrado) para patrocinar el acceso de invitado. Usted también configurará el ISE para permitir que los patrocinadores vean la contraseña del invitado (opcional), que es útil a este laboratorio.

Complete estos pasos:

1. Agregue al usuario del empleado al grupo de SponsorAllAccount. Hay maneras diferentes de hacer esto: vaya directamente al grupo, o edite al usuario y asigne al grupo. Por este ejemplo, navegue a la **administración > a la Administración de la identidad > Groups > los grupos de la Identificación del usuario**. Entonces, el tecleo **SponsorAllAccount** y agrega al usuario del empleado.
2. Navegue a los **grupos de la administración > de la Administración > del patrocinador del invitado**.
3. El tecleo **edita**, después elige **SponsorAllAccounts**.
4. Seleccione los niveles de la autorización y fije el siguiente:Vea la contraseña del invitado: Sí
5. **Salvaguardia del** tecleo para completar esta tarea.

Invitado que patrocina

Previamente, usted ha configurado la directiva y a los grupos apropiados del invitado para permitir que el Domain User AD patrocine a los invitados temporales. Después, usted accederá al patrocinador porta y creará un acceso de invitado temporal.

Complete estos pasos:

1. De un navegador, navegue a cualquiera de estos URL: <ise ip>:8080/sponsorportal/ de http:// **o** <ise ip>:8443/sponsorportal/ de https://. Entonces, login con el siguiente:Nombre de usuario: aduser (Active Directory), empleado (usuario interno)Contraseña XXXX
2. De la página del patrocinador, el tecleo **crea la sola cuenta de Usuario invitado**.
3. Para un invitado temporal, agregue el siguiente:Primer nombre: Requerido (por ejemplo, Sam)Último nombre: Requerido (por ejemplo, Jones)Papel del grupo: GuestPerfil del tiempo: DefaultOneHourHuso horario: Ningunos/valor por defecto
4. Haga clic en Submit (Enviar).
5. Una cuenta de invitado se crea sobre la base de su entrada anterior. Observe que la contraseña es visible (del ejercicio anterior) en comparación con el *** del hash.
6. Deje a esta ventana la demostración abierta el nombre de usuario y contraseña para el invitado. Usted los utilizará para probar el login porta del invitado (después).

Acceso porta de prueba del invitado

Con la nueva cuenta de invitado creada por un usuario/el patrocinador AD, es hora de probar el

portal y el acceso del invitado.

Complete estos pasos:

1. En un dispositivo preferido (en este caso un IOS de Apple/un iPad), conecte con el invitado SSID de la vaina y marque la dirección IP /connectivity.
2. Utilice al navegador e intente navegar a http://www.Le reorientan a la página de registro del portal del invitado.
3. Inicie sesión usando la cuenta de invitado creada en el ejercicio anterior.Si es acertada, la página del Acceptable Use Policy aparece.
4. El control **valida los términos y condición**, después hace clic **valida**.Se completa El URL original, y el punto final es acceso permitido como invitado.

Configuración del certificado

Para las comunicaciones seguras con el ISE, determinan si la comunicación es autenticación relacionada o para la Administración ISE. Por ejemplo, para la configuración usando la red UI ISE, los Certificados X.509 y los encadenamientos de la confianza del certificado necesitan ser configurados para habilitar la encriptación asimétrica.

Complete estos pasos:

1. De su PC conectado atado con alambre, abra una ventana del buscador en https://AD/certsrv.**Nota:** Utilice el HTTP seguro.**Nota:** Utilice el Mozilla Firefox o MS Internet Explorer para acceder el ISE.
2. Inicie sesión como administrator/Cisco123.
3. Haga clic la **descarga un certificado de CA, una Cadena de certificados, o un CRL**.
4. Haga clic el **certificado de CA de la descarga** y sálvelo (observe la ubicación de la salvaguardia).
5. Abra una ventana del buscador en el <Pod-ISE> de https://.
6. Vaya a los **Certificados de la administración > del sistema > de los Certificados > de la autoridad de los Certificados**.
7. Seleccione la operación de los **Certificados del Certificate Authority** y hojee al CERT previamente descargado de CA.
8. **La confianza** selecta **para el cliente con el EAP-TLS**, entonces somete.
9. Confirme que CA ha sido de confianza agregado como raíz CA.
10. De un navegador, vaya a los **Certificados de la administración > del sistema > de los Certificados > de la autoridad de los Certificados**.
11. El tecleo **agrega**, después **genera el pedido de firma de certificado**.
12. Someta estos valores:Tema del certificado: CN=ise.corp.rf-demo.comLongitud de clave: 2048
13. Prompts ISE que el CSR está disponible en la página CSR. Haga clic en OK.
14. Seleccione el CSR de la página ISE CSR y haga clic la **exportación**.
15. Salve el archivo a cualquier ubicación (por ejemplo, las descargas, los etc.)
16. El archivo será guardado como *.pem.
17. Localice el archivo CSR y editelo con cualquier libreta/Wordpad/edición de textos.
18. Copie el contenido (seleccione todos > copia).
19. Abra una ventana del buscador en https:// <Pod-AD>/certsrv.

20. Haga clic la **petición un certificado**.
21. Haga clic para presentar un **pedido de certificado avanzado**.
22. Pegue el contenido CSR en el campo del Saved Request.
23. Seleccione al **servidor Web** como el Certificate Template plantilla de certificado, después haga clic **someten**.
24. Seleccione el **DER codificado**, después haga clic el **certificado de la descarga**.
25. Salve el archivo a una ubicación conocida (por ejemplo, las descargas)
26. Vaya a los **Certificados de la administración > del sistema > de los Certificados > de la autoridad de los Certificados**.
27. El tecleo **agrega > certificado de CA del lazo**.
28. Hojee al certificado de CA previamente descargado.
29. Seleccione el **protocolo EAP** y la **interfaz de administración**, después haga clic **someten**.
30. Confirme que CA ha sido de confianza agregado como raíz CA.

Integración de Active Directory de Windows 2008

El ISE puede comunicar directamente con el Active Directory (AD) para la autenticación del usuario/de la máquina o para extraer los atributos de usuario de la información de autorización. Para comunicar con el AD, el ISE se debe “unir a” a un dominio AD. En este ejercicio usted se unirá al ISE a un dominio AD, y confirma la comunicación AD está trabajando correctamente.

Complete estos pasos:

1. Para unirse al ISE al dominio AD, del ISE va a la **administración > a la Administración de la identidad > las fuentes externas de la identidad**.
2. Del panel izquierdo (fuentes externas de la identidad), seleccione el **Active Directory**.
3. En el Lado derecho, seleccione la lengueta de la **conexión** y ingrese el siguiente:Domain Name: corp.rf-demo.comNombre del almacén de la identidad: AD1
4. Haga clic en Probar conexión. Ingrese el nombre de usuario AD (aduser/Cisco123), después haga clic la **AUTORIZACIÓN**.
5. Confirme que el estado de la prueba muestra la **prueba tenida éxito**.
6. Seleccione el registro detallado demostración y observe los detalles útiles para resolver problemas. Para continuar, haga clic en OK (Aceptar).
7. **Configuración de la salvaguardia del** tecleo.
8. El tecleo **se une a**. Ingrese al usuario AD (administrator/Cisco123), después haga clic la **AUTORIZACIÓN**.
9. Confirme que se unen a las demostraciones del estado de la operación **tenidas éxito**, después hacen clic la **AUTORIZACIÓN** para continuar.Las demostraciones del estatus de la conexión del servidor **CONECTADAS**. Si este los cambios de estado en cualquier momento, una conexión de prueba ayudan a resolver problemas los problemas con las operaciones AD.

Agregue los grupos del Active Directory

Cuando agregan a los grupos AD, un control más granular se permite sobre las directivas ISE. Por ejemplo, los grupos AD pueden ser distinguidos por los papeles funcionales, tales como grupos del empleado o de contratista, sin el bug relacionado que es experimentado en los

ejercicios anteriores ISE 1.0 donde las directivas fueron limitadas solamente a los usuarios.

En este laboratorio, solamente utilizan a los Domain User y/o al grupo del empleado.

Complete estos pasos:

1. Del ISE, van a la **administración > a la Administración de la identidad > las fuentes externas de la identidad**.
2. Lengueta selecta del **Active Directory > Groups**.
3. Haga clic **+Add**, después **seleccione a los grupos del directorio**.
4. En la ventana de la continuación (grupos selectos del directorio), valide los valores por defecto para el dominio (corp-rf-demo.com) y filtre (*). Entonces, tecleo RetrieveGroups**.**
5. Seleccione los cuadros para los grupos de los **Domain User** y del **empleado**. Haga Click en OK cuando está acabado.
6. Confirme que han agregado a los grupos a la lista.

Agregue la secuencia de la fuente de la identidad

Por abandono, el ISE se fija para utilizar a los usuarios internos para el almacén de la autenticación. Si se agrega el AD, una orden de la prioridad de la secuencia se puede crear para incluir el AD que el ISE utilizará para marcar para saber si hay autenticación.

Complete estos pasos:

1. Del ISE, navegue a las **secuencias de la fuente de la administración > de la Administración de la identidad > de la identidad**.
2. Haga clic **+Add** para agregar una nueva secuencia.
3. Ingrese el nuevo nombre: **AD_Internal**. Agregue todas las fuentes disponibles al campo seleccionado. Entonces, reordene según las necesidades para AD1 moverse al top de la lista. Haga clic en Submit (Enviar).
4. Confirme que la secuencia se ha agregado a la lista.

La Tecnología inalámbrica ISE patrocinó el acceso de invitado con el AD integrado

El ISE se puede configurar para permitir patrocinen a los invitados con las directivas para permitir que los Domain User AD patrocinen el acceso de invitado.

Complete estos pasos:

1. Del ISE, navegue a la **administración > a la Administración > a las configuraciones del invitado**.
2. Amplíe al **patrocinador**, y haga clic la **fuente de la autenticación**. Entonces, **AD_Internal** selecto como secuencia del almacén de la identidad.
3. Confirme AD_Internal como la secuencia del almacén de la identidad. Haga clic en Save (Guardar).
4. Navegue a la **Administración de la administración > del invitado > a la directiva del grupo del patrocinador**.

5. Inserte la nueva directiva sobre la primera regla (haga clic el icono de las **acciones de la** derecha).
6. Para la nueva directiva del grupo del patrocinador, cree el siguiente:‘Nombre de la regla Domain UserGrupos de la identidad: NingunosOtras condiciones: (Cree nuevo/avanzó) > AD1AD1: Grupos externosAD1 los grupos externos > igualan > los usuarios de corp.rf-demo.com/Users/Domain
7. En los grupos del patrocinador, fije el siguiente:Grupos del patrocinador: SponsorAllAccounts
8. Navegue a los **grupos de la administración > de la Administración > del patrocinador del invitado**.
9. Seleccione para editar > **SponsorAllAccounts**.
10. Seleccione los niveles de la autorización y fije el siguiente:Vea la contraseña del invitado: Sí

SPAN de la configuración en el Switch

SPAN de la configuración - El mgt ISE/la interfaz de la sonda es L2 adyacente a la interfaz de administración del WLC. El Switch se puede configurar PARA ATRAVESAR y otras interfaces, tales como VLA N de la interfaz del empleado y del invitado.

```
Podswitch(config)#monitor session 1 source vlan10 , 11 , 12
Podswitch(config)#monitor session 1 destination interface Fa0/8
ISE virtual probe interface.
```

Referencia: Autenticación inalámbrica para Apple MAC OS X

Socio al WLC vía un SSID autenticado como un usuario interno (o usuario integrada, AD) usando una laptop de la Tecnología inalámbrica de Apple Mac OS X. Salto si no aplicable.

1. En un mac, vaya a las configuraciones de la red inalámbrica (WLAN). Habilite WIFI, después selecciónelo y conecte con la VAINA habilitada 802.1x SSID creada en el ejercicio anterior.
2. Proporcione la siguiente información para conectar:Nombre de usuario: aduser (si usa el AD), empleado (– empleado), contratista (interno – contratista interno)Contraseña XXXX802.1x: AutomáticoCertificado de TLS: NingunoAhora, la laptop no pudo conectar. Además, el ISE puede lanzar un evento fallado como sigue:`Authentication failed :12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client certificates chain`
3. Vaya a la **preferencia > a la red > al aeropuerto > al 802.1x del sistema** que fija y fije la nueva autenticación del perfil de la VAINA SSID/WPA como:TLS: InhabilitadoPEAP: HabilitadoTTL: InhabilitadoEAP-FAST: Inhabilitado
4. Haga Click en OK para continuar y para permitir que la configuración sea guardada.
5. En la pantalla de la red, seleccione el apropiado perfil SSID + del 802.1x WPA y el tecleo **conecta**.
6. El sistema pudo indicar para un nombre de usuario y contraseña. Ingrese el usuario y la contraseña () AD, después haga clic la **AUTORIZACIÓN**.El cliente debe mostrar **conectado** vía el PEAP con un IP Address válido.

Referencia: Autenticación inalámbrica para el Microsoft Windows XP

Socio al WLC vía un SSID autenticado como un usuario interno (o usuario integrada, AD) usando una laptop de la Tecnología inalámbrica de Windows XP. Salto si no aplicable.

Complete estos pasos:

1. En la laptop, vaya a las configuraciones de la red inalámbrica (WLAN). Habilite WIFI y conecte con la VAINA habilitada 802.1x SSID creada en el ejercicio anterior.
2. Acceda las propiedades Propiedades de la red para la interfaz de WIFI.
3. Navegue a las **redes inalámbricas que** cuadro selecciona las propiedades Propiedades de la red de la vaina SSID > la lengueta de la autenticación > el tipo EAP = EAP protegido (PEAP).
4. Haga clic las propiedades EAP.
5. Fije el siguiente:Valide el certificado de servidor: InhabilitadoMétodo de autentificación: Contraseña asegurada (v2 EAP-MSCHAP)
6. Haga Click en OK en todas las ventanas para completar esta tarea de configuración.
7. Prompts del cliente de Windows XP para el nombre de usuario y contraseña. En este ejemplo, es.
8. Confirme la conectividad de red, el IP Addressing (v4).

Referencia: Autenticación inalámbrica para Microsoft Windows 7

Socio al WLC vía un SSID autenticado como un usuario interno (o usuario integrada, AD) usando una laptop de la Tecnología inalámbrica de Windows 7.

1. En la laptop, vaya a las configuraciones de la red inalámbrica (WLAN). Habilite WIFI y conecte con la VAINA habilitada 802.1x SSID creada en el ejercicio anterior.
2. Acceda al administrador inalámbrico y edite el nuevo perfil de la Tecnología inalámbrica de la VAINA.
3. Fije el siguiente:Método de autentificación: PEAPRecuerde mis credenciales…: InhabilitadoValide el certificado de servidor (configuración avanzada): InhabilitadoMétodo de autentificación (adv. Determinación): V2 EAP-MSCHAPUtilice automáticamente mi inicio de Windows…: Inhabilitado

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems