Autenticación del acceso basado con un ejemplo de configuración del REVESTIMIENTO y ACS 5.2

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Antecedentes
Configurar
Diagrama de la red
Suposición
Pasos de configuración
REVESTIMIENTO de la configuración
Switch de la configuración
Servidor de RADIUS de la configuración
Recursos de red de la configuración
Usuarios de la configuración
Defina los elementos de la directiva
Aplique las políticas de acceso
Verificación
Troubleshooting
Información Relacionada

Introducción

Este documento describe cómo configurar un Lightweight Access Point (LAP) como supplicant 802.1x para autenticarse en un servidor RADIUS como un Access Control Server (ACS) 5.2.

prerrequisitos

Requisitos

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

- Tenga conocimiento básico del regulador del Wireless LAN (WLC) y de los revestimientos.
- Tenga conocimiento funcional del servidor de AAA.

- Tenga conocimiento completo de las redes inalámbricas y de los problemas de seguridad de red inalámbrica.

Componentes Utilizados

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

- WLC de Cisco 5508 que funciona con la versión de firmware 7.0.220.0
- REVESTIMIENTO de las Cisco 3502 Series
- Cisco Secure ACS que funciona con la versión 5.2
- Cisco 3560 Series Switch

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

Antecedentes

Los revestimientos factory installed los Certificados X.509 - firmados por una clave privada - que se queman en el dispositivo a la hora de la fabricación. Los revestimientos utilizan este certificado para autenticar con el WLC en el proceso del unido. Este método describe otra manera de autenticar los revestimientos. Con el software WLC, usted puede configurar la autenticación del 802.1x entre un punto de acceso del Cisco Aironet y un switch Cisco. El en este caso, el AP actúa como el supplicant del 802.1x y es autenticado por el Switch contra un servidor de RADIUS (ACS) ese EAP-FAST de las aplicaciones con el aprovisionamiento anónimo PAC. Una vez que se configura para la autenticación del 802.1x, el Switch no permite que ningún tráfico con excepción del tráfico del 802.1x pase a través del puerto hasta que el dispositivo conectado con el puerto autentique con éxito. Un AP se puede autenticar o antes de que se una a un WLC o después de que se ha unido a un WLC, en este caso usted configura el 802.1x en el Switch después de que el REVESTIMIENTO se una al WLC.

Configurar

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

Diagrama de la red

En este documento, se utiliza esta configuración de red:

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

- La dirección IP del servidor ACS (RADIUS) es 192.168.150.24.
- La Administración y el direccionamiento de la interfaz del AP manager del WLC es 192.168.75.44.
- Los servidores DHCP dirigen 192.168.150.25.
- El REVESTIMIENTO se pone en el VLA N 253.
- VLA N 253: 192.168.153.x/24. Gateway: 192.168.153.10
- VLA N 75: 192.168.75.x/24. Gateway: 192.168.75.1

Suposición

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

Pasos de configuración

Esta configuración se separa en tres categorías:

1. REVESTIMIENTO de la configuración.
2. Configure el Switch.
3. Configure al servidor de RADIUS.

Configure el REVESTIMIENTO

Suposiciones

El REVESTIMIENTO se registra ya al WLC usando la opción 43, DNS, o IP estáticamente configurado de la interfaz de administración del WLC.

Complete estos pasos:

1. Van a la **Tecnología inalámbrica** > a los **Puntos de acceso** > **todos los AP** para verificar el registro del REVESTIMIENTO en el WLC.
2. Usted puede configurar las credenciales del 802.1x (es decir, nombre de usuario/contraseña) para todos los revestimientos de dos maneras:**Global**Para un REVESTIMIENTO ya unido, usted puede fijar las credenciales global así que cada REVESTIMIENTO que se une al WLC heredará esas credenciales.**Individualmente**Perfiles del 802.1x de la configuración por el AP. En nuestro ejemplo, configuraremos las credenciales por el AP.Van a la **Tecnología inalámbrica** > **todos los AP**, y seleccionan el AP en cuestión.Agregue el nombre de usuario y contraseña en los campos de las **credenciales del supplicant del 802.1x**.**Note**: Las credenciales del login se utilizan a Telnet, a SSH, o a la consola adentro al AP.
3. Configure la sección de gran disponibilidad, y el tecleo **se aplica**.**Note**: Una vez que están guardadas, estas credenciales se conservan a través del WLC y de las reinicializaciones AP. Las credenciales cambian solamente cuando el REVESTIMIENTO se une a un nuevo WLC.

El REVESTIMIENTO asume el nombre de usuario y contraseña que fue configurado en el nuevo WLC.Si el AP no se ha unido a un WLC todavía, usted debe consolar adentro al REVESTIMIENTO para fijar las credenciales. Publique este comando CLI en el enable mode:*<password> de la* ***contraseña del*** *<username> del* ***nombre de usuario del dot1x de LAP#lwapp ap*** o*<password> de la* ***contraseña del*** *<username> del* ***nombre de usuario del dot1x de LAP#capwap ap*** **Note**: Este comando está disponible solamente para los AP que funcionan con la imagen de recuperación.El nombre de usuario predeterminado y la contraseña para el REVESTIMIENTO es `Cisco` y `Cisco` respectivamente.

Switch de la configuración

El Switch actúa como authenticator para el REVESTIMIENTO y autentica el REVESTIMIENTO contra un servidor de RADIUS. Si el Switch no tiene el software obediente, actualice el Switch. En el Switch CLI, publique estos comandos para habilitar la autenticación del 802.1x en un puerto del switch:

```
switch#configure terminal
switch(config)#dot1x system-auth-control
switch(config)#aaa new-model
!--- Enables 802.1x on the Switch. switch(config)#aaa authentication dot1x default group radius
switch(config)#radius server host 192.168.150.24 key cisco
!--- Configures the RADIUS server with shared secret and enables switch to send !--- 802.1x
information to the RADIUS server for authentication. switch(config)#ip radius source-interface
vlan 253
!--- We are sourcing RADIUS packets from VLAN 253 with NAS IP: 192.168.153.10.
switch(config)interface gigabitEthernet 0/11 switch(config-if)switchport mode access
switch(config-if)switchport access vlan 253 switch(config-if)mls qos trust dscp switch(config-
if)spanning-tree portfast !--- gig0/11 is the port number on which the AP is connected.
switch(config-if)dot1x pae authenticator !--- Configures dot1x authentication. switch(config-
if)dot1x port-control auto !--- With this command, the switch initiates the 802.1x
authentication.
```

Note: Si usted tiene otros AP en el mismo Switch y usted no quisiera que utilizaran el 802.1x, usted puede salir del puerto O.N.U-configurado para el 802.1x o publicar este comando:

```
switch(config-if)authentication port-control force-authorized
```

Servidor de RADIUS de la configuración

El REVESTIMIENTO se autentica con el EAP-FAST. Aseegurese que el servidor de RADIUS usted utiliza los soportes este método EAP si usted no está utilizando Cisco ACS 5.2.

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

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

El ACS 5.x es un policy basado ACS. Es decir el ACS 5.x utiliza un modelo basado en las reglas

de la directiva en vez del modelo basado en el grupo usado en las versiones 4.x.

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

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

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

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

Si entonces resulta la condición

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

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

Como consecuencia, esto nos da la flexibilidad para limitar las condiciones bajo las cuales se permite al usuario acceder la red y también se permite qué nivel de la autorización cuando se cumplen las condiciones específicas.

Recursos de red de la configuración

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

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

Complete estos pasos:

1. Del ACS GUI, haga clic a los **recursos de red**.
2. Haga clic a los **grupos de dispositivos de red**.
3. Vaya a la **ubicación > crean** (en la parte inferior).
4. Agregue los campos obligatorios y el tecleo **somete**.
5. La ventana restaura:
6. **El tipo de dispositivo del** tecleo **> crea**.
7. Haga clic en Submit (Enviar). Una vez que está completada, la ventana restaura:
8. Vaya a los **recursos de red >** a los **dispositivos de red y a los clientes AAA**.
9. El tecleo **crea**, y completa los detalles según lo representado aquí:
10. Haga clic en Submit (Enviar). La ventana restaura:

Usuarios de la configuración

En esta sección, usted verá cómo crear a un usuario en el ACS configurado previamente. Usted asignará al usuario a un grupo llamado los “usuarios del REVESTIMIENTO”.

Complete estos pasos:

1. Vaya a los **usuarios y la identidad salva** > los **grupos de la identidad** > **crea**.
2. Haga clic en Submit (Enviar).
3. Cree **3502e** y asígnelo para agrupar a los “usuarios del REVESTIMIENTO”.
4. Vaya a los **usuarios y la identidad salva** > los **grupos de la identidad** > Users > **crea**.
5. Usted verá la información actualizada:

Defina los elementos de la directiva

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

Aplique las políticas de acceso

En esta sección, usted seleccionará el EAP-FAST pues el método de autentificación usado para los revestimientos para autenticar. Usted entonces creará las reglas basadas en los pasos anteriores.

Complete estos pasos:

1. Va a las **políticas de acceso** > al **acceso mantiene** > el **acceso de red predeterminada** > **edita: “Acceso de red predeterminada”**.
2. Aseegurese le haber habilitado el **EAP-FAST** y el **aprovisionamiento anónimo de la En-banda PAC**.
3. Haga clic en Submit (Enviar).
4. Verifique al grupo de la identidad que usted ha seleccionado. En este ejemplo, los **usuarios internos del** uso (que fue creado en el ACS) y salvan los cambios.
5. Van a las **políticas de acceso** > al **acceso mantiene** > el **acceso** > la **autorización de red predeterminada** para verificar el perfil de la autorización.Usted puede personalizar bajo qué condiciones usted no prohibirá a acceso del usuario a la red y qué perfil de la autorización (atributos) usted pasará autenticado una vez. Este granularity está solamente disponible en ACS 5.x. En este ejemplo, seleccionan la **ubicación**, al **tipo de dispositivo**, el **protocolo**, al **grupo de la identidad**, y el **método de autenticación EAP**.
6. Haga Click en OK, y **cambios de la salvaguardia**.
7. El siguiente paso es crear una regla. Si no se define ningunas reglas, el REVESTIMIENTO no se prohibe el acceso sin ningunas condiciones.
8. El tecleo **crea** > **Rule-1**. Esta regla está para los usuarios en el grupo “usuarios del REVESTIMIENTO”.
9. **Cambios de la salvaguardia del** tecleo. Si usted quiere a los usuarios que no corresponden con las condiciones que se negarán, edite la regla predeterminada para decir “niegan el acceso”.
10. El paso más reciente es definir las reglas de selección del servicio. Utilice esta página para configurar una directiva simple o basada en las reglas para determinar que mantengan para aplicarse a los pedidos entrantes. Por ejemplo:

Verificación

Una vez que el 802.1x se habilita en el puerto del switch, todo el tráfico a menos que el tráfico del

802.1x se bloquee a través del puerto. El REVESTIMIENTO, que se registra ya al WLC, consigue desasociado. Solamente después que una autenticación acertada del 802.1x es el otro tráfico permitido pasar a través. El registro exitoso del REVESTIMIENTO al WLC después de que el 802.1x se habilite en el Switch indica que la autenticación del REVESTIMIENTO es acertada.

Consola AP:

```
*Jan 29 09:10:24.048: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5246
*Jan 29 09:10:27.049: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5247
!--- AP disconnects upon adding dot1x information in the gig0/11. *Jan 29 09:10:30.104: %WIDS-5-
DISABLED: IDS Signature is removed and disabled. *Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP
changed state to DISCOVERY *Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to
DISCOVERY *Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down *Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio1, changed
state to administratively down *Jan 29 09:10:30.186: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to reset *Jan 29 09:10:30.201: %LINK-3-UPDOWN: Interface Dot11Radio1, changed
state to up *Jan 29 09:10:30.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:10:30.220: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to reset Translating
"CISCO-CAPWAP-CONTROLLER"...domain server (192.168.150.25) *Jan 29 09:10:36.203: status of
voice_diag_test from WLC is false
*Jan 29 09:11:05.927: %DOT1X_SHIM-6-AUTH_OK: Interface GigabitEthernet0 authenticated [EAP-FAST]
*Jan 29 09:11:08.947: %DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0 assigned DHCP address
192.168.153.106, mask 255.255.255.0, hostname 3502e
!--- Authentication is successful and the AP gets an IP. Translating "CISCO-CAPWAP-
CONTROLLER.Wlab"...domain server (192.168.150.25) *Jan 29 09:11:37.000: %CAPWAP-5-DTLSREQSEND:
DTLS connection request sent peer_ip: 192.168.75.44 peer_port: 5246 *Jan 29 09:11:37.000:
%CAPWAP-5-CHANGED: CAPWAP changed state to *Jan 29 09:11:37.575: %CAPWAP-5-DTLSREQSUCC: DTLS
connection created successfully peer_ip: 192.168.75.44 peer_port: 5246 *Jan 29 09:11:37.578:
%CAPWAP-5-SENDJOIN: sending Join Request to 192.168.75.44 *Jan 29 09:11:37.578: %CAPWAP-5-
CHANGED: CAPWAP changed state to JOIN

*Jan 29 09:11:37.748: %CAPWAP-5-CHANGED: CAPWAP chan
wmmAC status is FALSEged state to CFG
*Jan 29 09:11:38.890: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
   down
*Jan 29 09:11:38.900: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   reset
*Jan 29 09:11:38.900: %CAPWAP-5-CHANGED: CAPWAP changed state to UP
*Jan 29 09:11:38.956: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller
   5508-3
*Jan 29 09:11:39.013: %CAPWAP-5-DATA_DTLS_START: Starting Data DTLS handshake.
   Wireless client traffic will be blocked until DTLS tunnel is established.
*Jan 29 09:11:39.013: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.016: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[0]
*Jan 29 09:11:39.028: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to
   down
*Jan 29 09:11:39.038: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
   reset
*Jan 29 09:11:39.054: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Jan 29 09:11:39.060: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
   down
*Jan 29 09:11:39.069: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   reset
*Jan 29 09:11:39.085: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.135: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[1]DTLS
   keys are plumbed successfully.
*Jan 29 09:11:39.151: %CAPWAP-5-DATA_DTLS_ESTABLISHED: Data DTLS tunnel
   established.
*Jan 29 09:11:39.161: %WIDS-5-ENABLED: IDS Signature is loaded and enabled
```

```
!--- AP joins the 5508-3 WLC.
```

Registros ACS:

1. Vea las cuentas del golpe:Si usted está marcando los registros en el plazo de 15 minutos de autenticación, aseegurese le restaurar la cuenta del golpe. En la misma página, en la parte inferior usted tiene una lengueta de la **cuenta del golpe**.
2. **La supervisión del** tecleo **y los informes** y una nueva ventana emergente aparece. **Autenticaciones del** tecleo **– RADIUS – Hoy**. Usted puede también hacer clic los **detalles** para verificar que mantienen la regla de selección eran aplicados.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Cisco Secure Access Control System
- Soporte Técnico y Documentación - Cisco Systems