Solución de problemas de PSK de identidad en controladores de LAN inalámbricos

Contenido

Introducción

Este documento describe cómo resolver problemas de conexión de clave precompartida de identidad (PSK) en el controlador de LAN inalámbrica de Cisco (WLC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco WLC que ejecuta el código 8.5 y posterior y Identity Services Engine (ISE)
- WLAN conmutada centralmente (actualmente no se admite el switching local FlexConnect con identidad PSK)
- Configuración PSK de identidad en el WLC y el ISE. Esto se puede encontrar en este enlace: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-5/b_Identity_PSK_Feature_Deployment_Guide.html

Componentes Utilizados

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

- WLC de la serie 5508 de Cisco que ejecuta la versión de software 8.5.103.0
- Cisco ISE que ejecuta la versión 2.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is

live, make sure that you understand the potential impact of any command.

Comprender el flujo de identidad PSK

Paso 1. El cliente envía una solicitud de asociación al identificador de conjunto de servicios (SSID) habilitado con autenticación PSK+MAC.

Paso 2. Dado que la autenticación MAC ha habilitado los contactos del WLC, el servidor radius debe verificar la dirección MAC del cliente.

Paso 3. El servidor Radius verifica los detalles del cliente y envía los pares AV de Cisco para los que especifica PSK como el tipo de autenticación que se utilizará, así como el valor clave que se utilizará para el cliente.

Paso 4. Una vez que se recibe esto, el WLC envía la respuesta de asociación al cliente. Es importante ser consciente de este paso, como si hubiera un retraso en la comunicación entre el WLC y el servidor RADIUS, los clientes pueden atascarse en un loop de asociación, donde envían una segunda solicitud de asociación antes de que se reciba la respuesta del servidor RADIUS.

Paso 5. El WLC utiliza el valor de clave enviado por el servidor radius como la clave PMK. A continuación, el punto de acceso (AP) continúa con el intercambio de señales de cuatro vías que verifica que la contraseña configurada en el cliente coincida con el valor enviado por el servidor radius.

Paso 6. Luego, el cliente completa el proceso DHCP y también pasa al estado RUN.

Solución de problemas de escenarios

Estos debugs son necesarios para resolver problemas de PSK de identidad:

Depuraciones en el WLC:

- **debug client client_mac,** donde **client _mac** es la dirección MAC de la prueba del cliente.
- **debug aaa detail enable**

Escenario 1. Pasar escenario donde el cliente se conecta correctamente

El cliente envía la solicitud de asociación al AP:

```
*apfMsConnTask_6: Sep 21 15:01:43.496: e8:50:8b:64:4f:45 Association received from mobile on
BSSID 28:6f:7f:e2:24:cf AP AP_2802-1
```

El WLC luego se pone en contacto con el servidor RADIUS para verificar la dirección MAC del cliente:

```
*aaaQueueReader: Sep 21 15:01:43.498: AuthenticationRequest: 0x2b8c8a9c
*apfMsConnTask_6: Sep 21 15:01:43.498: e8:50:8b:64:4f:45 apfProcessAssocReq (apf_80211.c:11440)
Changing state for mobile e8:50:8b:64:4f:45 on AP 28:6f:7f:e2:24:c0 from Associated to AAA
```

```
Pending

*aaaQueueReader: Sep 21 15:01:43.498:
Callback.....................................0x10762018

*aaaQueueReader: Sep 21 15:01:43.498:
protocolType.................................0x40000001
```

El servidor radius responde con el mensaje Access-Accept que también contiene el tipo de método PSK y la clave que se utiliza para la autenticación:

```
*radiusTransportThread: Sep 21 15:01:43.794: AuthorizationResponse: 0x171b5c00

*radiusTransportThread: Sep 21 15:01:43.794:
structureSize................................313

*radiusTransportThread: Sep 21 15:01:43.794:
resultCode...................................0


*radiusTransportThread: Sep 21 15:01:43.794:         Packet contains 5 AVPs:

*radiusTransportThread: Sep 21 15:01:43.794:             AVP[01] User-
Name.............................E8-50-8B-64-4F-45 (17 bytes)

*radiusTransportThread: Sep 21 15:01:43.794:             AVP[02]
State................................ReauthSession:0a6a20770000000059c346ed (38 bytes)

*radiusTransportThread: Sep 21 15:01:43.794:             AVP[03]
Class................................CACS:0a6a20770000000059c346ed:ISE/291984633/6 (45
bytes)

*radiusTransportThread: Sep 21 15:01:43.794:             AVP[04] Cisco / PSK-
Mode.....................ascii (5 bytes)

*radiusTransportThread: Sep 21 15:01:43.794:             AVP[05] Cisco /
PSK..........................cisco123 (8 bytes)
```

Una vez que se recibe esto, puede ver que el WLC envía la respuesta de la asociación y se produce un intercambio de señales de cuatro vías:

```
*apfReceiveTask: Sep 21 15:01:43.924: e8:50:8b:64:4f:45 Sending assoc-resp with status 0
station:e8:50:8b:64:4f:45 AP:28:6f:7f:e2:24:c0-01 on apVapId 1
```

El apretón de manos de cuatro vías:

```
*Dot1x_NW_MsgTask_5: Sep 21 15:01:43.994: e8:50:8b:64:4f:45 Sending EAPOL-Key Message to mobile
e8:50:8b:64:4f:45
   state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
*Dot1x_NW_MsgTask_5: Sep 21 15:01:43.998: e8:50:8b:64:4f:45 Received EAPOL-key in PTK_START
state (message 2) from mobile e8:50:8b:64:4f:45
*Dot1x_NW_MsgTask_5: Sep 21 15:01:43.998: e8:50:8b:64:4f:45 Received valid MIC in EAPOL Key
Message M2!!!!!
*Dot1x_NW_MsgTask_5: Sep 21 15:01:43.999: e8:50:8b:64:4f:45 Sending EAPOL-Key Message to mobile
e8:50:8b:64:4f:45
```

```
   state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01
*Dot1x_NW_MsgTask_5: Sep 21 15:01:44.003: e8:50:8b:64:4f:45 Received EAPOL-key in
PTKINITNEGOTIATING state (message 4) from mobile e8:50:8b:64:4f:45
```

Una vez hecho esto, el cliente completa el proceso DHCP y pasa al estado RUN (la salida se recorta para mostrar las secciones importantes):

```
(WLC_1) >show client detail e8:50:8b:64:4f:45
Client MAC Address.............................. e8:50:8b:64:4f:45
Client Username ................................ E8-50-8B-64-4F-45
Hostname: ...................................... S6-edge
Device Type: ................................... Android-Samsung-Galaxy-Phone
AP MAC Address.................................. 28:6f:7f:e2:24:c0
AP Name......................................... AP_2802-1
Wireless LAN Network Name (SSID)................ Identity PSK
Wireless LAN Profile Name....................... Identity PSK
Security Policy Completed....................... Yes
Policy Manager State............................ RUN
```

Situación hipotética 2. El cliente intenta conectarse con una contraseña incorrecta

La secuencia inicial de pasos permanece igual a la de una autenticación pasada.

- El cliente envía una solicitud de asociación.
- Una vez que el WLC recibe esto, inicia la comunicación con el servidor radius para verificar la dirección MAC del cliente.
- Si el servidor RADIUS tiene los detalles del cliente, envía un access-accept con el valor de clave y el tipo de autenticación que es PSK.
- La sección útil en la que se puede observar la falla se encuentra en la entrada en contacto en cuatro direcciones.

El AP envía el mensaje 1, al cual el cliente responde con el mensaje 2:

```
*Dot1x_NW_MsgTask_7: Sep 21 15:12:47.661: 50:8f:4c:9d:ef:87 Received EAPOL-key in PTK_START
state (message 2) from mobile 50:8f:4c:9d:ef:87
```

Sin embargo, debido a los diferentes valores de clave PMK (contraseña), el AP y el cliente derivan diferentes claves que resultan en una confirmación de MIC no válida en el mensaje 2:

```
*Dot1x_NW_MsgTask_7: Sep 21 15:12:47.662: 50:8f:4c:9d:ef:87 Received EAPOL-key M2 with invalid
MIC from mobile 50:8f:4c:9d:ef:87 version 2
*osapiBsnTimer: Sep 21 15:12:48.824: 50:8f:4c:9d:ef:87 802.1x 'timeoutEvt' Timer expired for
station 50:8f:4c:9d:ef:87 and for message = M2
*Dot1x_NW_MsgTask_7: Sep 21 15:12:48.824: 50:8f:4c:9d:ef:87 Retransmit 1 of EAPOL-Key M1 (length
121) for mobile 50:8f:4c:9d:ef:87

The client then is then de-authenticated by the WLC:
*Dot1x_NW_MsgTask_7: Sep 21 15:12:50.825: 50:8f:4c:9d:ef:87 Sent Deauthenticate to mobile on
BSSID 28:6f:7f:e2:24:c0 slot 0(caller 1x_ptsm.c:655)

<noscript>
```

Otro resultado útil que se debe comprobar es el comando 'show client detail'. Aquí puede ver que el cliente está atascado en el estado START:

```
*Dot1x_NW_MsgTask_7: Sep 21 15:12:47.662: 50:8f:4c:9d:ef:87 Received EAPOL-key M2 with invalid
MIC from mobile 50:8f:4c:9d:ef:87 version 2
*osapiBsnTimer: Sep 21 15:12:48.824: 50:8f:4c:9d:ef:87 802.1x 'timeoutEvt' Timer expired for
```

```
station 50:8f:4c:9d:ef:87 and for message = M2
*Dot1x_NW_MsgTask_7: Sep 21 15:12:48.824: 50:8f:4c:9d:ef:87 Retransmit 1 of EAPOL-Key M1 (length
121) for mobile 50:8f:4c:9d:ef:87

The client will then be de-authenticated by the WLC:
*Dot1x_NW_MsgTask_7: Sep 21 15:12:50.825: 50:8f:4c:9d:ef:87 Sent Deauthenticate to mobile on
BSSID 28:6f:7f:e2:24:c0 slot 0(caller 1x_ptsm.c:655)
```

Situación hipotética 3. Servidor Radius Inalcanzable

El WLC intenta comunicarse con el servidor radius una vez que recibe la solicitud de asociación. En caso de que el servidor RADIUS no sea accesible, el WLC intenta comunicarse repetidamente con el servidor RADIUS (hasta que se alcance el recuento de reintentos). Una vez que se detecta que el servidor RADIUS es inalcanzable después del número configurado de reintentos (el valor predeterminado es 5), el WLC envía una respuesta de asociación con el código de estado 1 como se muestra aquí:

```
*apfReceiveTask: Sep 21 15:28:55.777: 50:8f:4c:9d:ef:87 Sending assoc-resp with status 1
station:50:8f:4c:9d:ef:87 AP:a0:e0:af:62:f3:c0-00 on apVapId 1
*apfReceiveTask: Sep 21 15:28:55.777: 50:8f:4c:9d:ef:87 Sending Assoc Response (status:
'unspecified failure') to station on AP AP_2802-2 on BSSID a0:e0:af:62:f3:c0 ApVapId 1 Slot 0,
mobility role 0
```

También puede ver el número de solicitudes de reintento y solicitudes de tiempo de espera que crecen en las estadísticas del servidor RADIUS, para las cuales puede navegar a **Monitor > Statistics > RADIUS Servers** como se muestra en la imagen:

Situación hipotética 4. Parámetro de anulación incorrecto enviado por servidor RADIUS

Hay varios parámetros que se pueden enviar junto con PSK y la clave, como VLAN, ACL y rol de usuario. Sin embargo, si la entrada ACL enviada por el servidor radius no se configura entonces el WLC rechaza al cliente, incluso si el servidor radius aprueba la solicitud de autenticación. Esto se puede ver claramente en las depuraciones del cliente:

```
*radiusTransportThread: Sep 22 14:39:05.499: AuthorizationResponse: 0x171b5c00

*radiusTransportThread: Sep 22 14:39:05.499:
structureSize.............................376

*radiusTransportThread: Sep 22 14:39:05.499:
resultCode.................................0

*radiusTransportThread: Sep 22 14:39:05.499:
protocolUsed.............................0x00000001

*radiusTransportThread: Sep 22 14:39:05.499:         Packet contains 7 AVPs:

*radiusTransportThread: Sep 22 14:39:05.499:             AVP[01] User-
Name.............................E8-50-8B-64-4F-45 (17 bytes)

*radiusTransportThread: Sep 22 14:39:05.499:             AVP[02]
State.................................ReauthSession:0a6a20770000002659c493e9 (38 bytes)
```

```
*radiusTransportThread: Sep 22 14:39:05.499:            AVP[03]
Class.................................CACS:0a6a20770000002659c493e9:ISE/291984633/78 (46
bytes)

*radiusTransportThread: Sep 22 14:39:05.499:            AVP[04] Cisco / PSK-
Mode.....................ascii (5 bytes)

*radiusTransportThread: Sep 22 14:39:05.499:            AVP[05] Cisco /
PSK............................cisco123 (8 bytes)

*radiusTransportThread: Sep 22 14:39:05.499:            AVP[06] Unknown Cisco / Attribute
19.............teacher (7 bytes)

*radiusTransportThread: Sep 22 14:39:05.499:            AVP[07] Airespace / ACL-
Name.....................testing (7 bytes)
```

Depuración del cliente:

```
*apfReceiveTask: Sep 22 14:39:05.564: e8:50:8b:64:4f:45  ACL received from RADIUS does not exist
in WLC de-authenticating the client
*apfReceiveTask: Sep 22 14:39:05.628: e8:50:8b:64:4f:45 Sending assoc-resp with status 12
station:e8:50:8b:64:4f:45 AP:28:6f:7f:e2:24:c0-01 on apVapId 1
```

Situación hipotética 5. Política de cliente no configurada en el servidor Radius

Cuando el servidor RADIUS es accesible pero no hay ninguna política configurada en el servidor RADIUS para el cliente, sólo puede conectarse si utiliza el PSK, configurado globalmente bajo la WLAN. Cualquier otra entrada fallaría. No hay nada específico para diferenciar entre una autenticación PSK global en funcionamiento y una autenticación PSK de identidad en funcionamiento excepto en la salida de depuración Autenticación, Autorización y Contabilización (AAA) que no tendrá parámetros de reemplazo que se presionen:

```
*radiusTransportThread: Sep 22 14:32:13.734: AuthorizationResponse: 0x171b5c00

*radiusTransportThread: Sep 22 14:32:13.734:
structureSize.............................269

*radiusTransportThread: Sep 22 14:32:13.734:
resultCode................................0

*radiusTransportThread: Sep 22 14:32:13.734:
protocolUsed..............................0x00000001

*radiusTransportThread: Sep 22 14:32:13.734:
proxyState................................50:8F:4C:9D:EF:87-00:00

*radiusTransportThread: Sep 22 14:32:13.734:         Packet contains 3 AVPs:

*radiusTransportThread: Sep 22 14:32:13.734:            AVP[01] User-
Name.............................50-8F-4C-9D-EF-87 (17 bytes)

*radiusTransportThread: Sep 22 14:32:13.734:            AVP[02]
State................................ReauthSession:0a6a20770000002359c49240 (38 bytes)

*radiusTransportThread: Sep 22 14:32:13.734:            AVP[03]
Class.................................CACS:0a6a20770000002359c49240:ISE/291984633/74 (46
bytes)
```