Solucionar problemas da PSK de identidade em controladores de LAN sem fio

Contents

Introduction

Este documento descreve como solucionar problemas de conexão de chave pré-compartilhada de identidade (PSK) no Cisco Wireless LAN Controller (WLC).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco WLC com código 8.5 e posterior e Identity Services Engine (ISE)
- WLAN com comutação central (atualmente não há suporte para o FlexConnect Local Switching com PSK de identidade)
- Configuração de PSK de identidade na WLC e no ISE. Isso pode ser encontrado neste link: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-5/b_Identity_PSK_Feature_Deployment_Guide.html

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 5508 Series WLC que executa o software versão 8.5.103.0
- Cisco ISE que executa a versão 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.

Entender o fluxo da PSK de identidade

Etapa 1. O cliente envia uma solicitação de associação ao SSID (Service Set Identifier) habilitado com autenticação PSK+MAC.

Etapa 2. Como a autenticação MAC ativou os contatos da WLC, o servidor radius é verificar o endereço MAC do cliente.

Etapa 3. O servidor Radius verifica os detalhes do cliente e envia os pares av da Cisco para os quais ele especifica PSK como o tipo de autenticação a ser usado, bem como o valor chave a ser usado para o cliente.

Etapa 4. Uma vez recebido, a WLC envia a resposta de associação ao cliente. É importante estar ciente dessa etapa, como se houvesse um atraso na comunicação entre o WLC e o servidor radius, os clientes podem ficar presos em um loop de associação, onde enviam uma segunda solicitação de associação antes que a resposta seja recebida do servidor radius.

Etapa 5. A WLC usa o valor-chave enviado pelo servidor radius como a chave PMK. O ponto de acesso (AP) continua com o handshake de quatro vias, que verifica se a senha configurada no cliente corresponde ao valor enviado pelo servidor radius.

Etapa 6. Em seguida, o cliente conclui o processo DHCP e se move para o estado RUN também.

Solucionar problemas de cenários

Essas depurações são necessárias para solucionar problemas de PSK de identidade:

Depurações na WLC:

- **debug client_mac,** onde **client_mac** é o endereço MAC do teste do cliente.
- **debug aaa detail enable**

Cenário 1. Passar um cenário em que o cliente se conecta com êxito

O cliente envia a solicitação de associação ao 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
```

A WLC entra em contato com o servidor radius para verificar o endereço MAC do 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
```

O servidor radius responde com a mensagem Access-Accept, que também contém o tipo de método PSK e a chave usados para autenticação:

```
*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)
```

Depois que isso é recebido, você pode ver que a WLC envia a resposta da associação e um handshake de quatro vias acontece:

```
*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
```

O handshake de quatro vias:

```
*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
```

Depois disso, o cliente conclui o processo DHCP e entra no estado RUN (a saída é recortada para mostrar as seções 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
```

Cenário 2. O cliente tenta se conectar com uma senha incorreta

A sequência inicial de passos permanece a mesma que a de uma autenticação passada.

- O cliente envia uma solicitação de associação.
- Quando a WLC recebe isso, ela inicia a comunicação com o servidor radius para verificar o endereço MAC do cliente.
- Se o servidor radius tiver os detalhes do cliente, ele enviará uma aceitação de acesso com o valor da chave e o tipo de autenticação que é PSK.
- A seção útil onde a falha pode ser notada está no handshake de quatro vias.

O AP envia a mensagem 1, à qual o cliente responde com a mensagem 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
```

No entanto, devido a valores de chave PMK diferentes (senha), o AP e o cliente derivam chaves diferentes que resultam em um recebimento MIC inválido na mensagem 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>
```

Outra saída útil a ser verificada é o 'show client detail'. Aqui você pode ver que o cliente está preso no 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)
```

Cenário 3. Servidor Radius inalcançável

A WLC tenta entrar em contato com o servidor radius depois de receber a solicitação de associação. Caso o servidor radius não possa ser alcançado, a WLC tenta repetidamente entrar em contato com o servidor radius (até que a contagem de novas tentativas seja atingida). Quando o servidor radius é detectado como inalcançável após o número configurado de novas tentativas (o valor padrão é 5), a WLC envia uma resposta de associação com o código de status 1, como mostrado aqui:

```
*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
```

Você também pode ver o número de solicitações de nova tentativa e solicitações de timeout que crescem nas estatísticas do servidor radius, para as quais você pode navegar até **Monitor > Statistics > RADIUS Servers** como mostrado na imagem:

Cenário 4. Parâmetro de substituição incorreto enviado pelo servidor Radius

Há vários parâmetros que podem ser enviados junto com a PSK e a chave, como VLAN, ACL e Função de usuário. No entanto, se a entrada da ACL enviada pelo servidor radius não estiver configurada, a WLC rejeitará o cliente, mesmo que o servidor radius aprove a solicitação de autenticação. Isso pode ser visto claramente nas depurações de clientes:

```
*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)
```

Depurações de clientes:

```
*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
```

Cenário 5. Política de Cliente Não Configurada no Servidor Radius

Quando o servidor radius estiver acessível, mas não houver nenhuma política configurada no servidor radius para o cliente, ele poderá ser conectado somente se usar a PSK, configurada globalmente na WLAN. Qualquer outra entrada falharia. Não há nada específico para diferenciar entre uma autenticação PSK global em funcionamento e uma autenticação PSK de identidade funcional, exceto na saída de debug Authentication, Authorization, and Accounting (AAA) que não terá nenhum parâmetro de substituição enviado:

```
*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)
```