Probleemoplossing voor identiteit PSK op draadloze LAN-controllers

Inhoud

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen met de vooraf gedeelde sleutel (PSK) verbinding via de Cisco draadloze LAN-controller (WLC).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco WLC-applicatie met code 8.5 en hoger en Identity Services Engine (ISE)
- Centraal switched WLAN (FlexConnect Local Switching met Identity PSK wordt momenteel niet ondersteund)
- Identity PSK configuratie op de WLC en ISE. Dit is te vinden op deze link :

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-5/b_Identity_PSK_Feature_Deployment_Guide.html

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 5508 Series WLC-software met release 8.5.103.0
- Cisco ISE die versie 2.2 uitvoert

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van

elke opdracht begrijpen.

Verken stroom van identiteit PSK

Stap 1. De client stuurt een verzoek om een associatie naar de Service Set Identifier (SSID) die is ingeschakeld met verificatie van PSK+MAC.

Stap 2. Aangezien MAC-verificatie de WLC-contacten heeft ingeschakeld, moet de Straalserver het MAC-adres van de client controleren.

Stap 3. Radius-server verifieert de clientgegevens en verstuurt de Cisco v-paren waarvoor PSK is gespecificeerd als het op verificatie gerichte type en de voor de client te gebruiken hoofdwaarde.

Stap 4. Zodra dit is ontvangen, stuurt de WLC de reactie van de vereniging naar de cliënt. Het is belangrijk om van deze stap op de hoogte te zijn, alsof er een vertraging is in de communicatie tussen de WLC en de Straalserver, kunnen klanten vastzitten in een associatieronde, waar ze een tweede associatieverzoek verzenden voordat de reactie van de Straalserver wordt ontvangen.

Stap 5. De WLC gebruikt de sleutelwaarde die door de boogserver als PMK-toets wordt verstuurd. Het access point (AP) gaat dan verder met de handdruk op vier manieren die verifieert dat het wachtwoord dat op de client is ingesteld overeenkomt met de waarde die door de Straalserver wordt verstuurd.

Stap 6. De client voltooit vervolgens het DHCP-proces en gaat ook naar de RUN-status.

Probleemoplossing

Deze deposito's zijn vereist om problemen met Identity PSK problemen op te lossen:

Debugs op de WLC:

- **debug client_mac,** waarbij **client _mac** het MAC adres van de client test is.
- **u kunt gegevens debug a**

Scenario 1. Pass Scenario waar Client met succes verbindingen maakt

De cliënt stuurt het verzoek om vereniging naar de 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
```

De WLC contacteert vervolgens de Straalserver om het adres van client-MAC te verifiëren:

```
*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
```

De Straalserver reageert met het bericht Access-Accept dat ook het type PSK-methode en de sleutel bevat die voor verificatie worden gebruikt:

```
*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)
```

Zodra deze ontvangen is, kan je zien dat de WLC de associatie respons verstuurt en er een handdruk op vier manieren plaatsvindt:

```
*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
```

Handdruk op vier manieren:

```
*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
```

Zodra dit wordt gedaan, voltooit de client het DHCP-proces en gaat deze naar de status RUN

(uitvoer wordt geklikt om de belangrijke secties te tonen):

```
(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
```

Scenario 2. Clientprobeert verbinding te maken met onjuist wachtwoord

De eerste reeks stappen blijft hetzelfde als die van een goedgekeurde authenticatie.

- De cliënt stuurt een verzoek om vereniging.
- Zodra WLC dit ontvangt, initieert het communicatie met de Straalserver om het client-MAC-adres te controleren.
- Als de Straalserver de clientgegevens heeft, verstuurt het een toegangscontrole-acceptatie met de hoofdwaarde en het verificatietype PSK.
- De nuttige sectie waar de mislukking kan worden opgemerkt is in de viervoudige handdruk.

AP stuurt bericht 1, waarop de cliënt reageert met bericht 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
```

Vanwege verschillende PMK-waarden (wachtwoord) leiden de AP en de client echter verschillende toetsen af die in bericht 2 een ongeldig MIC-ontvangstbewijs opleveren:

```
*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>
```

Een andere nuttige uitvoer om te controleren is de "show client detail". Hier zie je dat de client is vastgezet in de START-status:

```
*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)
```

Scenario 3. Radius Server onbereikbaar

De WLC probeert de straal server te contacteren zodra het de associatie verzoek ontvangt. Heeft de Straalserver onbereikbaar, dan probeert de WLC herhaaldelijk contact op te nemen met de Straalserver (totdat de teller opnieuw is bereikt). Zodra de Straalserver wordt gedetecteerd om onbereikbaar te zijn na het geconfigureerde aantal herhalingen (de standaardwaarde is 5), verstuurt de WLC een associatie-respons met statuscode 1 zoals hier wordt getoond:

```
*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
```

U kunt ook het aantal verzoeken om opnieuw te proberen en timeout verzoeken zien die in de statistieken van de Straalserver groeit, waarvoor u kunt navigeren om **> Statistieken > RADIUS servers** zoals in het beeld te tonen:

Scenario 4. Onjuiste, door Radius Server verzonden parameter voor negeren

Er zijn verschillende parameters die samen met de PSK en de toets kunnen worden geduwd,

zoals VLAN, ACL en Gebruiker Rol. Als de ACL-ingang die door de Straalserver wordt verstuurd echter niet is ingesteld, verwerpt de WLC de client, zelfs als de Straalserver de verificatieaanvraag goedkeurt. Dit is duidelijk te zien in de uitvindingen van cliënten:

```
*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)
```

Clientdebugs:

```
*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
```

Scenario 5. Clientbeleid niet ingesteld op Radius Server

Wanneer de Straalserver bereikbaar is maar er geen beleid is ingesteld op de Straalserver voor de client, kan de server alleen worden aangesloten als de PSK, die globaal is geconfigureerd onder de WLAN. Alle andere inzendingen zouden mislukken. Er is niets specifieks om te differentiëren tussen een werkende mondiale PSK-verificatie en een werkende identiteit PSK-verificatie behalve in de debug-verificatie, -autorisatie en -accounting (AAA) uitvoer die geen parameters zal hebben die worden geduwd:

```
*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)
```