Dépannez l'identité PSK sur les contrôleurs LAN Sans fil

Contenu

Introduction

Ce document décrit comment dépanner les questions principales pré-partagées de connexion d'identité (PSK) sur le contrôleur LAN Sans fil de Cisco (WLC).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco WLC qui exécute le code 8.5 et plus élevé et le Cisco Identity Services Engine (ISE).
- Configuration de l'identité PSK sur le WLC et l'ISE. Ceci peut être trouvé dans ce lien :

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

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- La gamme Cisco 5508 WLC qui exécute la version logicielle 8.5.103.0.
- Cisco ISE qui exécute la version 2.2.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Comprenez l'écoulement de l'identité PSK

Étape 1. Le client envoie une demande d'association à l'Identifiant SSID (Service Set Identifier) activé avec l'authentification PSK+MAC.

Étape 2. Puisque l'authentification MAC a activé les contacts WLC, le serveur de rayon doit vérifier l'adresse MAC du client.

Étape 3. Le serveur de rayon vérifie les petits groupes de client et envoie les poids du commerce-paires de Cisco pour lesquelles elle spécifie PSK pendant que le type d'authentification à utiliser aussi bien que la valeur principale à utiliser pour le client.

Étape 4. Une fois que ceci est reçu le WLC envoie la réponse d'association au client. Il est important de se rendre compte de cette étape, comme si il y a un retard dans la transmission entre le WLC et le serveur de rayon, des clients peut être bloqué dans une boucle d'association, où ils envoient une deuxième demande d'association avant que la réponse soit reçue du serveur de rayon.

Étape 5. Le WLC utilise la valeur principale envoyée par le serveur de rayon comme clé principale. Le Point d'accès (AP) se poursuit alors par la prise de contact à quatre voies qui vérifie que le mot de passe configuré sur le client apparie la valeur envoyée par le serveur de rayon.

Étape 6. Le client alors complète le processus DHCP et entre dans l'état de PASSAGE aussi bien.

Dépannez les scénarios

Ceux-ci met au point sont exigés pour dépanner des questions de l'identité PSK :

Debugs sur le WLC :

- **mettez au point le client_mac de client,** où le _mac de client est l'adresse MAC du test du client.
- **enable de détail de debug aaa**

Scénario de passage du scénario 1. où le client se connecte avec succès

Le client envoie la demande d'association à 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
```

Le WLC contacte alors le serveur de rayon pour vérifier l'adresse MAC de client :

```
*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
```

Le serveur de rayon répond avec le message d'Access-recevoir qui contient également le type et la clé de méthode PSK qui est utilisée pour l'authentification :

```
*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)
```

Une fois que ceci est reçu vous pouvez voir que le WLC envoie la réponse d'association et une prise de contact à quatre voies se produit :

```
*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
```

La prise de contact à quatre voies :

```
*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
```

Une fois que ceci est fait, le client complète le processus DHCP et entre dans l'état de PASSAGE (la sortie est coupée pour afficher les importantes sections) :

```
(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
```

Essais de client du scénario 2. à connecter au mot de passe incorrect

La séquence initiale d'étapes reste les mêmes que celui d'une authentification passée.

- Le client envoie une demande d'association.
- Une fois que le WLC reçoit ceci, il initie la transmission avec le serveur de rayon pour vérifier l'adresse MAC de client.
- Si le serveur de rayon a le client le détaille envoie un Access-recevoir avec la valeur principale et le type d'authentification qui est PSK.
- La section utile où la panne peut être notée est dans la prise de contact à quatre voies.

AP envoie message 1, auquel le client répond avec le message 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
```

Cependant, en raison de différentes valeurs de clé principale (mot de passe) AP et le client dérivent différentes clés qui a comme conséquence une réception non valide MIC dans le message 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)
```

Une autre sortie utile à vérifier est le « show client detail ». Voici que vous pouvez voir que le client est coincé dans l'état de DÉBUT :

```
*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)
```

Scénario serveur de 3. rayons inaccessible

Les essais WLC pour contacter le serveur de rayon une fois qu'il reçoit la demande d'association. Au cas où le serveur de rayon serait inaccessible, WLC les essais à plusieurs reprises pour contacter le serveur de rayon (jusqu'à ce que le nombre de tentatives est atteint). Une fois que le serveur de rayon est détecté pour être inaccessible après que le nombre configuré de relances (la

valeur par défaut est 5) le WLC envoie une réponse d'association avec code d'état 1 comme affiché ici :

```
*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
```

Vous pouvez également voir que le nombre de demandes et de délai d'attente de relance demande ce qui se développe en statistiques de serveur de rayon, pour lesquelles vous pouvez naviguer **pour surveiller des serveurs du >Statistics >RADIUS** suivant les indications de l'image :

Paramètre incorrect de priorité du scénario 4. envoyé par le serveur de rayon

Il y a plusieurs paramètres qui peuvent être poussés avec PSK et la clé, telle que le VLAN, l'ACL et le rôle de l'utilisateur. Cependant, si le rubrique de liste ACL envoyé par le serveur de rayon n'est pas configuré alors le WLC rejette le client, même si le serveur de rayon approuve la demande d'authentification. Ceci peut être clairement vu dans le client met au point :

```
*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)
```

Le client met au point :

```
*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
```

Stratégie de client du scénario 5. non configurée sur le serveur de rayon

Quand le serveur de rayon est accessible mais il n'y a aucune stratégie configurée sur le serveur de rayon pour le client, elle peut obtenir connecté seulement si elle utilise le PSK, configuré globalement sous le WLAN. Toutes les autres entrées échoueraient. Il n'y a rien spécifique pour différencier entre une authentification globale fonctionnante PSK et une authentification fonctionnante de l'identité PSK excepté dans le debug authentication, l'autorisation, et la comptabilité (AAA) sortie qui n'aura aucun paramètre de priorité qui est poussé :

```
*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)
```