Идентификационный PSK устранения неполадок на контроллерах беспроводной локальной сети

Содержание

Введение

Этот документ описывает, как устранить неполадки Идентификационных проблем с подключением Предварительного общего ключа (PSK) на контроллере беспроводной локальной сети Cisco (WLC).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- WLC Cisco, который выполняет код 8.5 и выше и платформа Identity Services Engine (ISE).
- Идентификационная конфигурация PSK на WLC и ISE. Это может быть найдено в этой ссылке:

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

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- WLC Cisco серии 5508, который выполняет выпуск ПО 8.5.103.0.
- Cisco ISE, который выполняет версию 2.2.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Поймите поток идентификационного PSK

Шаг 1. Клиент отправляет запрос ассоциации к идентификаторам наборов сервисов (SSID), включенным с аутентификацией PSK+MAC.

Шаг 2. Так как проверка подлинности MAC включила контакты WLC, сервер RADIUS должен проверить MAC-адрес клиента.

Шаг 3. Сервер RADIUS проверяет, что клиент детализирует и передает av-пар Cisco, для которых он задает PSK как тип проверки подлинности, который будет использоваться, а также значение параметра, которое будет использоваться для клиента.

Шаг 4. . Как только это получено, WLC передает ответ ассоциации клиенту. Важно знать об этом шаге, как будто существует задержка связи между WLC и сервером RADIUS, клиенты могут застрять в петле ассоциации, где они отправляют второй запрос ассоциации, прежде чем ответ будет получен от сервера RADIUS.

Шаг 5. . WLC использует значение параметра, передаваемое сервером RADIUS как главный ключ. Точка доступа (AP) тогда продолжает четыре этапных установления связи, которые проверяют, что пароль, настроенный на клиенте, совпадает со значением, передаваемым сервером RADIUS.

Шаг 6. Клиент тогда завершает процесс DHCP и перемещается в ВЫПОЛНЕННОЕ состояние также.

Сценарии устранения неполадок

Эти отладки требуются, чтобы решать Идентификационные проблемы PSK:

Отладки на WLC:

- **отладьте клиентский client_mac,** где клиентский _mac является MAC-адресом теста клиента.
- **подробность debug aaa включает**

Сценарий 1. Сценарий прохода, где Клиентские Подключения Успешно

Клиент отправляет запрос ассоциации к 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
```

WLC тогда связывается с сервером RADIUS для проверки MAC - адреса клиента:

```
*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
```

Сервер RADIUS отвечает сообщением Access-Accept, которое также содержит тип метода PSK и ключ, который используется для аутентификации:

```
*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)
```

Как только это получено, вы видите, что WLC передает ответ ассоциации, и происходят четыре этапных установления связи:

```
*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
```

Четыре этапных установления связи:

```
*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
```

Как только это сделано, клиент завершает процесс DHCP и входит в ВЫПОЛНЕННОЕ состояние (выходные данные отсечены для показа важных разделов):

```
(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
```

Сценарий 2. Клиент пытается соединиться с неверным паролем

Первоначальная нумерация шагов остается то же как та из переданной аутентификации.

- Клиент отправляет запрос ассоциации.
- Как только WLC получает это, он инициирует связь с сервером RADIUS для проверки MAC - адреса клиента.
- Если сервер RADIUS имеет клиентские подробные данные, он передает access-accept со значением параметра и типом проверки подлинности, который является PSK.
- Полезный раздел, где сбой может быть замечен, находится в четырех этапных установлениях связи.

AP передает сообщение 1, к которому клиент отвечает сообщением 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
```

Однако из-за другого главного ключа оценивает (пароль), AP и клиент получают другие ключи, который приводит к недопустимому получению MIC в сообщении 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)
```

Другие полезные выходные данные для проверки являются 'show client detail'. Здесь вы видите, что клиент застревает в Начальном состоянии:

```
*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)
```

Ситуация 3. Недостижимый сервер RADIUS

WLC пытается связаться с сервером RADIUS, как только это получает запрос ассоциации. В случае, если сервер RADIUS недостижим, WLC неоднократно пытается связаться с сервером RADIUS (пока число повторов не достигнуто). Как только сервер RADIUS обнаружен, чтобы быть недостижимым после настроенного номера повторных попыток (значение по умолчанию равняется 5), WLC передает ответ ассоциации с кодом статуса 1 как показано сюда:

```
*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
```

Можно также видеть количество запросов повторной попытки и запросов таймаута, который растет в статистике сервера RADIUS, для которой можно перейти для **Мониторинга> Статистика> серверы RADIUS** как показано в образе:

Сценарий 4. Неправильный параметр замены, передаваемый сервером RADIUS

Существует несколько параметров, которые могут уйтись с PSK и ключом, таким как VLAN,

ACL и Роль пользователя. Однако, если запись ACL, передаваемая сервером RADIUS, не настроена тогда, WLC отклоняет клиента, даже если сервер RADIUS утверждает запрос аутентификации. Это может быть ясно замечено в клиентских отладках:

```
*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)
```

Отладочные данные клиента:

```
*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
```

Сценарий 5. Клиентская политика, не настроенная на сервере RADIUS

Когда сервер RADIUS достижим, но нет никакой политики, настроенной на сервере RADIUS для клиента, это может быть связано, только если это использует PSK, настроенный глобально под WLAN. Любые другие записи отказали бы. Нет ничего определенного для дифференциации между рабочей глобальной аутентификацией PSK и рабочей идентификационной аутентификацией PSK кроме debug Authentication, Авторизации и выходных данных Accounting (AAA), которые не будут иметь никаких параметров замены, который выдвинут:

```
*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)
```