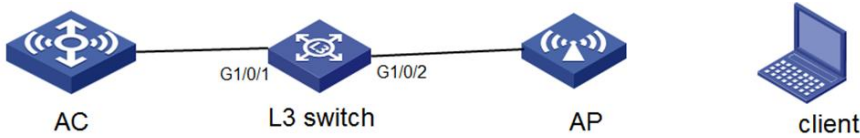


目前V7版本中的FIT AP与AC之间通过capwap隧道来通信，但此时的数据并未经过加密通过wireshark等抓包软件可以直接抓取、解读数据。而随着大家对数据安全越来越重视，对AC与AP间隧道数据的加密也就显得非常有必要了，目前V7版本中可以通过简单的配置就实现AP与AC间capwap隧道的加密。



组网说明：AC与AP交换机相连，AP通过二层或三层注册方式均可，此案例中已二层注册方式为例。AP管理vlan为VLAN 100，dhcp server位于AC上。

配置步骤：

1、AC侧配置

```

#
wlan ap ap1 model WA4320-ACN-SI
serial-id 219801A0T78166E00061
tunnel encryption enable //在AC与AP侧导入相应文件后，开启AP与AC间的隧道加密功能

radio 1
radio 2
#
interface Vlan-interface100
ip address 192.168.100.254 255.255.255.0
#
dhcp server ip-pool vlan100
gateway-list 192.168.100.254
network 192.168.100.0 mask 255.255.255.0
#
    
```

2、SW侧配置

```

#
interface GigabitEthernet1/0/1
port link-mode bridge
port access vlan 100
#
interface GigabitEthernet1/0/2
port link-mode bridge
port access vlan 100
poe enable
#
    
```

结果验证：

从抓包来看加密后AC与AP间交互报文已被加密。

1、加密前AC与AP间报文交互

Time	Source	Destination	Protocol	Length	Info
5212	192.168.20.3	192.168.20.254	CAPWAP	78	CAPWAP-Control - Echo Request
5213	192.168.20.254	192.168.20.3	CAPWAP	60	CAPWAP-Control - Echo Response
5542	Broadcast	Minervak_23:00:10	0x3891	72	Ethernet II
5543	Broadcast	Minervak_23:00:10	0x3891	72	Ethernet II
6196	192.168.20.3	255.255.255.255	CAPWAP	204	CAPWAP-Control - Discovery Request
6197	192.168.20.3	224.0.1.140	CAPWAP	204	CAPWAP-Control - Discovery Request
6198	192.168.20.254	192.168.20.3	CAPWAP	170	CAPWAP-Control - Discovery Response
6199	192.168.20.254	192.168.20.3	CAPWAP	170	CAPWAP-Control - Discovery Response
6267	192.168.20.254	192.168.20.254	CAPWAP	260	CAPWAP-Control - Join Request
6386	192.168.20.254	192.168.20.254	CAPWAP	260	CAPWAP-Control - Join Request
6387	192.168.20.254	192.168.20.3	CAPWAP	187	CAPWAP-Control - Join Response
6388	192.168.20.254	192.168.20.254	CAPWAP	456	CAPWAP-Control - Configuration Status Request
6389	192.168.20.254	192.168.20.3	CAPWAP	1490	CAPWAP-Control (Fragment ID: 0, Fragment Off
6390	192.168.20.254	192.168.20.3	CAPWAP	1490	CAPWAP-Control (Fragment ID: 0, Fragment Off
6391	192.168.20.254	192.168.20.3	CAPWAP	787	CAPWAP-Control - Configuration Status Respor
6401	192.168.20.3	192.168.20.254	CAPWAP	80	CAPWAP-Control - Change State Request
6402	192.168.20.254	192.168.20.3	CAPWAP	60	CAPWAP-Control - Change State Response
6403	Broadcast	Minervak_23:00:10	0x3891	72	Ethernet II
6404	Broadcast	Minervak_23:00:10	0x3891	72	Ethernet II

2、加密后AC与AP间报文交互

2177	2017-02-08	19:45:44.899276	192.168.20.16	192.168.20.254	DTLSv1.	123	Application Data
2178	2017-02-08	19:45:44.900230	192.168.20.254	192.168.20.16	DTLSv1.	1403	Application Data
2179	2017-02-08	19:45:44.904782	192.168.20.16	192.168.20.254	DTLSv1.	123	Application Data
2180	2017-02-08	19:45:44.916364	192.168.20.254	192.168.20.16	DTLSv1.	1387	Application Data
2181	2017-02-08	19:45:44.920562	192.168.20.16	192.168.20.254	DTLSv1.	123	Application Data
2182	2017-02-08	19:45:44.932511	192.168.20.254	192.168.20.16	DTLSv1.	1451	Application Data
2183	2017-02-08	19:45:44.981671	192.168.20.16	192.168.20.254	DTLSv1.	123	Application Data
2184	2017-02-08	19:45:44.982687	192.168.20.254	192.168.20.16	DTLSv1.	1451	Application Data
2185	2017-02-08	19:45:45.015955	192.168.20.16	192.168.20.254	DTLSv1.	123	Application Data
2186	2017-02-08	19:45:45.017207	192.168.20.254	192.168.20.16	DTLSv1.	1451	Application Data
2187	2017-02-08	19:45:45.021730	192.168.20.16	192.168.20.254	DTLSv1.	123	Application Data
2188	2017-02-08	19:45:45.022491	192.168.20.254	192.168.20.16	DTLSv1.	155	Application Data
2189	2017-02-08	19:45:45.023215	192.168.20.16	192.168.20.254	DTLSv1.	123	Application Data
2190	2017-02-08	19:45:45.024689	192.168.20.254	192.168.20.16	DTLSv1.	155	Application Data
2191	2017-02-08	19:45:45.106200	192.168.20.16	192.168.20.254	DTLSv1.	123	Application Data
2192	2017-02-08	19:45:45.106948	192.168.20.254	192.168.20.16	DTLSv1.	155	Application Data
2193	2017-02-08	19:45:45.109510	192.168.20.16	192.168.20.254	DTLSv1.	123	Application Data
2194	2017-02-08	19:45:45.110243	192.168.20.254	192.168.20.16	DTLSv1.	155	Application Data
2195	2017-02-08	19:45:45.110723	192.168.20.16	192.168.20.254	DTLSv1.	123	Application Data

Frame 2183: 123 bytes on wire (984 bits), 123 bytes captured (984 bits)
Ethernet II, Src: 38:91:d5:9a:7a:e0 (38:91:d5:9a:7a:e0), Dst: 38:97:d6:c8:77:08 (38:97:d6:c8:77:08)
Internet Protocol Version 4, Src: 192.168.20.16 (192.168.20.16), Dst: 192.168.20.254 (192.168.20.254)
User Datagram Protocol, Src Port: 22784 (22784), Dst Port: capwap-control (5246)
Control And Provisioning of Wireless Access Points
Datagram Transport Layer Security
DTLSv1.0 Record Layer: Application Data Protocol: Application Data
Content Type: Application Data (23)
Version: DTLS 1.0 (0xfeff)
Epoch: 1
Sequence Number: 11
Length: 64
Encrypted Application Data: 9889a084be15f8c568c1b7e2bd8f2dea6e7d07bde1be4d45...

```

000 38 97 d6 c8 77 08 38 91 d5 9a 7a e0 08 00 45 e0 8...w.8. ...E.
010 00 6d 00 34 00 00 ff 11 10 0d c0 a8 14 10 c0 a8 .m.4....

```

- 1、一定要将相应的*.pem文件分别导入到AC与AP的根目录下。在AC的根目录下导入root.pem、server.pem文件；在AP根目录下导入root.pem、client.pem文件 //*.pem文件不区分AC与AP具体型号。
- 2、AP需在AC上线后再执行隧道加密配置，证书文件导入操作及加密配置完成后需让AP重新执行一次上线流程。