Technical Guide

How to setup 802.1x Transparent Login with a CAPWAP-tunneled AP

Released: 2020-05-27
Table of Contents

1. Introduction ........................................................................................................................................... 3
2. Configuring CAPWAP and WAPM ........................................................................................................ 4
3. Pre-deployment or On-site Configuration ............................................................................................... 6
4. Configuring the desired Service Zone and RADIUS 802.1x authentication ................................. 8
5. Apply Template to the complete-tunneled AP with 802.1x SSID .............................................. 10
6. Client Side Verification ......................................................................................................................... 12
7. Conclusion ............................................................................................................................................. 14
8. Remarks ............................................................................................................................................... 14
Pre-requisite
Refer to the technical guide “CAPWAP Tunnel Configuration.” Complete Tunnel uses the CAPWAP protocol to communicate with an Access Point so that all management traffic, authentication traffic, and data traffic from the service area Access Point provided area transmitted back to the Controller before forwarding data traffic to the internet.

1. Introduction
This technical guide provides the administrator with instructions on how to set up the scenarios above.
The Controller can implement role-based policies over Layer 3 networks, with user access control available in the remote sites. This feature allows the Controller to support centralized
Access Point management and user management, including authenticated with a RADIUS server in 802.1x Authentication (transparent login). User can deploy this scenario if there RADIUS server is in a intranet, but they could have a Controller deployed with a public IP, so that their network could extend across the Internet, penetrating NATs, and deploy the local network to a remote site, such as penetrating the Great Fire Wall.

2. Configuring CAPWAP and WAPM

2.1. Configure CAPWAP Settings on the Controller with complete-tunnel

Step 1. Enable CAPWAP Status under CAPWAP Tab in WAPM

**CAPWAP Configuration**

- **CAPWAP Status**: Enable/Disable
- **Apply Certificate to APs**: DEFAULT
- **Trusted Certificate Authority (CA)**: DEFAULT
- **IP Address For Control Channel**: 100.144.144.254
- **IP Netmask For Control Channel**: 255.255.255.0 (253)
- **Control Channel IP Range**: 100.144.144.1 - 100.144.144.253

Main › Device Management › Wide Area AP Management › CAPWAP

Note: Certificate field can be modified with an uploaded certificate if required.
Note: Not recommended to modify IP Address and Netmask for Control Channel.

2.2. Configure Template for Remote AP Configuration

**Template AP Setting**

- **Select Template**: Template1
- **Country Code**: USA
- **General Settings**: Configure
- **VAP Configuration**: Configure
- **Security Settings**: Configure
- **Advanced Wireless Settings**: Configure
- **Hotspot 2.0 Settings**: Configure

Step 1. Confirm the specifications of the AP before configuring the Template.
Step 2. Configure Template.
Step 3. Configure General Settings.
Step 5. Step 5. Click Apply and return to the Template page.
Step 6. Configure VAP Configuration.
Step 7. Enable VAP.
Step 8. Fill in a Profile Name and ESSID.
Step 9. Configure VAPs with Complete Tunnel.
   Select Complete Tunnel under CAPWAP Tunnel Interface.
   Select Service Zone for AP to be managed and Apply.
3. Pre-deployment or On-site Configuration

Step 1. Enable CAPWAP on AP’s WMI.
Step 2. Enable only Static Discovery.
Step 3. Enter and Apply AC’s WAN IP Address into field.
Step 4. Reboot as required.

Note: Static discovery is the most recommended discovery method since it is intuitive to implement without any pre-settings to complete in advance. Enable the function and type in the IP address of the Controller that will manage this AP.

Successful CAPWAP joining will lead to the Access Point being listed in the managed AP list, as illustrated below:
CAPWAP column will display a ‘RUN’ status, and the tunnel status will show a clickable ‘Edit’ button in black if configure a VAP tunneled back to the Controller.

Note: Remember the Public IP shown on the Controller, for example, 10.70.7.27. We will need it when editing the 802.1x settings. This will be mentioned in the later chapter.

The Access Point’s WMI will show the VAP enabled, the VAP’s tunnel status with a green checkmark and the CAPWAP status on the System Overview page:
On the Access Point side, a successful CAPWAP will display the Status as Run and followed by the AC’s IP Address. The Data Channel as Active indicates both Control and Data Channels are successfully established.

Go to USERS→Authentication Servers, select “Server 2.”

And edit the User Postfix="" Then Apply.
4. Configuring the desired Service Zone and RADIUS 802.1x authentication

Step 1. Go to SYSTEM→Service Zones→Authentication Options
Enable RADIUS.

Step 2. Go to USERS→External Authentication
Enable 802.1x Authentication, then select “802.1X Settings.”
Step 3. 802.1X Settings

- In the 802.1X Auth Setting, select Default Auth Server as “Server 2 (Postfix:.).

- In the 802.1x Auth Setting, write the public IP of the AP to the list.
  Note: Secret Key is RVHS. It is the secret key between the Controller and the complete-tunneled AP, regardless of the authentication RADIUS server.

- →Apply

Step 4. Back to the USERS→External Authentication→RADIUS
Edit your own Primary RADIUS Server information.
5. **Apply Template to the complete-tunneled AP with 802.1x SSID**

Now we have a complete-tunneled AP and the RADIUS 802.1x settings, we need to apply the 802.1x SSID to the AP.

**Step 0. Go to Device → Wide Area AP Management → CAPWAP, and check your IP Address for Control Channel**

**Step 1. Go to Device → Wide Area AP Management → Template**
Select a template and configure an SSID, for example, 802.1x, and be sure to set the CAPWAP Tunnel Interface=Complete Tunnel, with the corresponding Service Zone. Then Apply.
Step 2. Back to the Template, continue to edit the Security Settings of that SSID.

- Security Type=WPA-Enterprise
- Cipher Suite=WPA2
- Protected Management Frames=Disable
- Group Key Update Period=86400
- Primary RADIUS Server
  - Host= IP Address for Control Channel
  - Authentication Port=1812
  - Secret Key=RVHS
1. Then Apply

Step 3. Go to DEVICES→Wide Area AP Management→Select the AP and apply the Template.

6. Client Side Verification

Step 1. Connect to the 802.1x SSID, with the following settings.
- EAP method=PEAP
- CA certificate=Do not validate
- Enter Identify and Password
Step 2. Connected.

※Note: Verified with Android 9 & 10.
Step 3. Go to the Controller, and you could see the 802.1x user on the Monitor Users.

![Online Users List]

Step 4. You could also get detailed information on the User Event Log.

![User Events]

7. Conclusion
Now the configuration is ready, and you can test the SSID with 802.1x Transparent Authentication from a remote AP, via the Controller, to the RADIUS of the main office. The Complete Tunnel makes the remote network and the central office network as the same segment and allows the RADIUS account to authenticate from the remote location. You can implement the deployment when there is NATs between main office and remote site.

8. Remarks