Date: 2014-08-17

Model: FAP-320C
Contains FCC ID: **U2M-PCE4551AH**
Contains FCC ID: **U2M-PCE3300AN**

Software Operational Description

We, **Fortinet, Inc.** hereby declare that requirements of KDB594280 have been met and shown on the following question.

1. Describe how any software/firmware update will be obtained, downloaded, and installed.

The update is controlled by the FortiGate that are assigned to manage this device and it can only be obtained from Fortinet update website.

2. Describe all the radio frequency parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited, such that, it will not exceed the authorized parameters?

The only radio frequency parameters which could be modified through software are the frequency bands and channels which are limited to US regulatory domain.

3. Are there any authentication protocols in place to ensure that the source of the software/firmware is legitimate? If so, describe in details; if not, explain how the software is secured from modification.

The update can only come from a locally authenticated user's PC (via "upload") or from the trusted FortiGate. The FortiGate only gets update from local authenticated adminstrator, or from our trusted fortiGuard cloud.

4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.

The update is packed in internal format, and being sent from FortiGate to FAP in capwap tunnel, this prevents unauthorized software/firmware change.

5. Describe, if any, encryption methods used.

Refer to 4.

6. For a device that can be configured as a master and client (with active or passive scanning), explain how the device ensures compliance for each mode? In particular if the device acts as master in some band of operation and client in another; how is compliance ensured in each band of operation?

This device is a master only.

7. How are unauthorized software/firmware changes prevented?

Our code will make many checks and verifications to prevent incorrect update.

8. Is it possible for third parties to load device drivers that could modify the RF parameters, country of operation or other parameters which impact device compliance? If so, describe procedures to ensure that only approved drivers are loaded.

No

9. Explain if any third parties have the capability to operate a US sold device on any other regulatory domain, frequencies, or in any manner that is in violation of the certification.

No

10. What prevents third parties from loading non-US versions of the software/firmware on the device?

The device is fixed to be operating in US regulatory domain only

11. For modular devices, describe how authentication is achieved when used with different hosts.

N/A

12. To whom is the UI accessible? (Professional installer, end user, other…)

Professional Installer.

a) What parameters are viewable to the professional installer/end-user?5

SSID, Operation mode (None, AP or monitor), Background scan Disable/Enable, Frequency band (802.11bgn, 802.11an), channels available and TX power level (%) for US regulatory domain, Auto TX Power Control Disable/Enable

b) What parameters are accessible or modifiable to the professional installer?

All those in a).

i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?

Yes and all parameters are limited to US Regulatory Domain.

ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?

The device Regulatory domain is set at factory. User will not be able to change it.

c) What configuration options are available to the end-user?
None

i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
N/A

ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
N/A

d) Is the country code factory set? Can it be changed in the UI?
Yes and cannot be changed in the UI.

i) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
Factory set only

e) What are the default parameters when the device is restarted?
The last saved configuration of the parameters listed in a).

13. Can the radio be configured in bridge or mesh mode? If yes, an attestation may be required. Further information is available in KDB Publication 905462 D02.
Yes

14. For a device that can be configured as a master and client (with active or passive scanning) If this is user configurable, describe what controls exist to ensure compliance.
N/A, Master mode only

If you should have any question(s) regarding this declaration, please don't hesitate to contact us. Thank you!

Andrew Ji / Director
TEL: 408 235 7700
FAX: 408 235 7737
E-mail: aji@fortinet.com