4ipnet

RE:FCC ID	VZ9150001
Applicant:	4IPNET, INC.

Software Security Description	
General description	
FCC question/requested information	Company Response
1. Describe how any software/firmware update will be obtained, downloaded, and installed.	1. Updates can only be obtained from www.4ipnet.com 2. After firmware image is downloaded, administrator can login to the appliance management UI to perform firmware upgrading over HTTPS.
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?	4ipnet EAP706/705 uses Public Key Infrastructure (PKI) to authenticate source of firmware reliably. It secure signing server uses PKI private key to sign the firmware. And appliance has PKI public key to authenticate the firmware image. Digital Signature Algorithm (DSA) and secure hashing algorithm (SHA) to validate only signed legitimate firmware can be allowed for upgrading. DSA can ensure firmware is authentic.
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.	EAP706/705 appliance built in ROM Pack verifies firmware platform target to ensure firmware matches the appliance hardware product code. Only firmware dedicated for specific hardware platform is allowed for upgrading.
4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.	EAP706/705 appliance built in ROM Pack verifies firmware platform target to ensure firmware matches the appliance hardware product code. Only firmware dedicated for specific hardware platform is allowed for upgrading.
5. Describe, if any, encryption methods used.	Digital Signature Algorithm (DSA) ensures firmware is authentic.

Third-Party Access Control	
1. How are unauthorized software/firmware changes prevented?	Through the PKI, DSA and SHA authentication and verification. Only matching firmware can be accepted.
2. 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
3. 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.	Not possible. 4ipnet device sold in US can only be operated in FCC regulatory domain and US allowed frequencies. The product regulatory domain identification cannot be modified by all means
4. What prevents third parties from loading non-US versions of the software/firmware on the device?	4ipnet device is registered, device unique Serial number and regulatory domain are tied in to backend database to prevent third party from downloading non-US versions of firmware. And device authenticates and verifies firmware signature to only allow US-versions of firmware for upgrading.
5. For modular devices, describe how authentication is achieved when used with different hosts.	NA

SOFTWARE CONFIGURATION DESCRIPTION	
User configuration guide	
1. To whom is the UI accessible? (Professional installer, end user, other.)	UI can only be accessed through user name and password authentication. The purchaser of the appliance defines roles and how they want to manage this access and what is restricted. Nothing in the UI can set appliance outside the parameter per grant of authorization
a) What parameters are viewable to the professional installer/enduser?	Depends on purchaser policy.
b) What parameters are accessible or modifiable to the professional installer?	Nothing in the UI can set appliance outside the parameter per grant of authorization. No special modes for installers or professionals or user.
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Nothing in the UI can set appliance outside the parameter per grant of authorization. No special modes for installers or professionals or user.

ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Nothing in the UI can set appliance outside the parameter per grant of authorization. No special modes for installers or professionals or user.
c) What configuration options are available to the end-user?	Nothing in the UI can set appliance outside the parameter per grant of authorization. No special modes for installers or professionals or user.
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Nothing in the UI can set appliance outside the parameter per grant of authorization. No special modes for installers or professionals or user.
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Nothing in the UI can set appliance outside the parameter per grant of authorization. No special modes for installers or professionals or user.
d) Is the country code factory set? Can it be changed in the UI?	Appliances sold in US are set at factory. Country code can't change in the UI.
i) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	Appliances sold in US are set at factory. Country code can't change in the UI.
e) What are the default parameters when the device is restarted?	When device is restarted it will return to last saved setting. Only when administrator explicitly chooses to reset device configuration to factory default, device can return to default parameters.
2. 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.	EAP706/705 appliance radio is configured in normal BSS access point mode.
3. 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, within the UI, to ensure compliance for each mode. If the device acts as a master in some bands and client in others, how is this configured to ensure compliance?	NA

Date: Jun 3th 2015

Name and signature of applicant:: Lilian Lu

Title: Manager

Company name: 4IPNET, INC.

E-mail: cert@4ipnet.com

Tel: +886-2-27187000