



2400 Research Blvd, Suite 395
Rockville, MD 20850
tel: +1 (703) 375-9820
info@acumensecurity.net
www.acumensecurity.net

May 1, 2018

Whom It May Concern:

Acumen Security verified that the following product faithfully embeds a FIPS 140-2 validated cryptographic module,

- AnyConnect version 4.6

The software version is known to operate on the following platform(s):

- Apple iOS 10.0 (or higher)
- Android 4.0 (or higher)

During the course of the review, Acumen Security confirmed that the following cryptographic module is properly incorporated into the product:

- CiscoSSL FIPS Object Module, version 6.0, FIPS 140-2 Certificate #2505

As part of the review, the software was tested on the following platforms:

- Apple iOS 10.0
- Android 4.0

Acumen Security confirmed that the following features leverage at least one of the embedded cryptographic modules to provide cryptographic services for **IKE/IPsec and TLS**.

- Session establishment supporting each service,
- All underlying cryptographic algorithms supporting each services' key derivation functions,
- Hashing for each service.
- Symmetric encryption for each service.

Additionally, Acumen Security confirmed that the above referenced cryptographic module is initialized in a manner consistent with the instructions provided in the non-proprietary Security Policy.

Details of the verification may be obtained from Cisco Systems, Inc. at the request of interested parties. This letter represents the independent opinions of Acumen Security and does not imply endorsement of the product by the CMVP or any other parties.

Sincerely,

A handwritten signature in black ink, appearing to read 'Ashit Vora', with a horizontal line underneath.

Ashit Vora
Laboratory Director