December 1, 2014

To Whom It May Concern,

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

1. AnyConnect Desktop, version 4.0

The AnyConnect Desktop application is known to operate on the following Operating Systems:

- Microsoft Windows Vista,
- Microsoft Windows 7,
- Microsoft Windows 8/8.1,
- Mac OS X 10.6,
- Mac OS X 10.7,
- Mac OS X 10.8,
- Mac OS X 10.9,
- Red Hat 6 (64 bit),
- Ubuntu 10 (64 bit),
- Ubuntu 11 (64 bit),
- Ubuntu 12 (64 bit).

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

- Microsoft Windows 7,
- Mac OS X 10.9,
- Ubuntu 10.

During the course of the review, Acumen Security confirmed that the following FIPS 140-2 validated cryptographic module is incorporated into the product,

1. Cisco FIPS Object Module, version 4.1, FIPS 140-2 certificate # 2100

Acumen Security confirmed that the following features leverage the embedded cryptographic module to provide cryptographic services for *TLS* and *IKE/IPsec*:

1. Session establishment supporting each service,

2. All underlying cryptographic algorithms supporting each services' key derivation functions,

3. Bulk encryption for each service.

Each of the above referenced services can be configured in a manner that restricts algorithm selection to only FIPS 140-2 approved algorithms.

Additionally, Acumen Security confirmed that the above referenced embedded cryptographic module is initialized in a manner consistent with the instructions provided in its non-proprietary FIPS 140-2 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,

Ashit Vora

Laboratory Director