



December 9, 2021

To Whom It May Concern

A conformance review of Cisco Secure Network Analytics (SNA), version 7.4 deployed in the following:

- Secure Network Analytics Manager
- Secure Network Analytics Flow Collector (including Flow Collector for Netflow)
- Secure Network Analytics Flow Sensor
- Secure Network Analytics UDP Director

was completed and found to properly incorporate the following FIPS 140-2 validated cryptographic module:

- Cisco FIPS Object Module version 7.2a (Certificate #4036)

Cisco confirms that the embedded cryptographic module listed above provides all of the cryptographic services for the following:

- TLS v1.2 (HTTPS) (Management interface for all appliances and TLS between appliance for secure communications).
- SSHv2

Users can communicate to appliances using HTTPS and/or SSH. HTTPS is the primary protocol used, but SSH is available for those who desire/need it.

The review/testing confirmed that:

1. The cryptographic module (mentioned above) is initialized in a manner that is compliant with its security policy.
2. All cryptographic algorithms used in SSHv2 and TLS v1.2 for sessions establishment, are handled within the Cisco FIPS Object Module, Certificate #4036

Cisco Secure Network Analytics enters FIPS mode after the User selects Enable FIPS and reboots the appliance.

Details of Cisco's review, which consisted of build process, source code review and operational testing (both positive and negative), can be provided upon request.

The intention of this letter is to provide an assessment and assurance that the Product correctly integrates and uses the validated cryptographic modules listed above within the scope of the claims indicated above. The Cryptographic Module Validation Program (CMVP) has not independently reviewed this analysis, testing or the results.

Any questions regarding these statements may be directed to the Cisco Global Certification Team (certteam@cisco.com).

Thank you,

A handwritten signature in black ink that reads "Edward D Paradise".

Ed Paradise
VP Engineering
Cisco S&TO