



PROJECTS

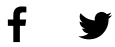
CRYPTOGRAPHIC MODULE VALIDATION PROGRAM

VALIDATED MODULES

SEARCH

# Cryptographic Module Validation

## Program CMVP



### PROJECT LINKS

---

[Overview](#)

[News & Updates](#)

[Publications](#)

## Certificate #3232

### Details

Module Name

Cisco ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X SSP-10, ASA 5585-X SSP-20, ASA 5585-X SSP-40 and ASA 5585-X SSP-60

Adaptive Security Appliances

Standard

FIPS 140-2

Status

Active

Sunset Date

7/12/2023

**Validation Dates**

07/13/2018

**Overall Level**

2

**Caveat**

When operated in FIPS mode and with the tamper evident seals and security devices installed as indicated in the Security Policy

**Security Level Exceptions**

- Roles, Services, and Authentication: Level 3
- Mitigation of Other Attacks: N/A

**Module Type**

Hardware

**Embodiment**

Multi-Chip Stand Alone

**Description**

The market-leading Cisco ASA Security Appliance Series deliver robust user and application policy enforcement, multi-vector attack protection, and secure connectivity services in cost-effective, easy-to-deploy solutions. The ASA 5500 Series Adaptive Security Appliances provide comprehensive security, performance, and reliability for network environments of all sizes.

**Tested Configuration(s)**

- N/A

**FIPS Algorithms**

AES	Certs. # <a href="#">2050</a> , # <a href="#">2444</a> , # <a href="#">2472</a> , # <a href="#">3301</a> and # <a href="#">4905</a>
CKG	vendor affirmed
CVL	Cert. # <a href="#">1521</a>
DRBG	Certs. # <a href="#">332</a> , # <a href="#">336</a> , # <a href="#">819</a> and # <a href="#">1735</a>
ECDSA	Cert. # <a href="#">1254</a>
HMAC	Certs. # <a href="#">1247</a> , # <a href="#">1514</a> , # <a href="#">2095</a> and # <a href="#">3272</a>
RSA	Cert. # <a href="#">2678</a>
SHS	Certs. # <a href="#">1794</a> , # <a href="#">2091</a> , # <a href="#">2737</a> and # <a href="#">4012</a>
Triple-DES	Certs. # <a href="#">1321</a> , # <a href="#">1513</a> , # <a href="#">1881</a> and # <a href="#">2559</a>

### Allowed Algorithms

Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength); NDRNG; RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)

### Hardware Versions

ASA 5506-X[1][2], ASA 5506H-X[1][2], ASA 5506W-X[1][2], ASA 5508-X[1][3], ASA 5516-X[1][4], ASA 5525-X[1], ASA 5545-X[1], ASA 5555-X[1] and [ASA 5585-X SSP-10, ASA 5585-X SSP-20, ASA 5585-X SSP-40 and ASA 5585-X SSP-60][1][5] with [AIR-AP-FIPSKIT=][1], [ASA5506-FIPS-KIT=][2], [ASA5508-FIPS-KIT=][3], [ASA5516-FIPS-KIT=][4] and [ASA5585-X-FIPS-KIT][5]

### Firmware Versions

9.8

## Vendor

### Cisco Systems, Inc.

170 West Tasman Drive  
San Jose, CA 95134  
USA

Global Certification Team  
certteam@cisco.com

## Related Files

[Security Policy](#)  
[Consolidated Certificate](#)

## Lab

GOSSAMER SECURITY SOLUTIONS INC  
NVLAP Code: 200997-0

**HEADQUARTERS**

100 Bureau Drive  
Gaithersburg, MD 20899



Want updates about CSRC and our  
publications?

[Webmaster](#) | [Contact Us](#) | [Our Other Offices](#)

---

**PROJECTS****PUBLICATIONS**

Drafts for Public Comment

All Public Drafts

Final Pubs

FIPS

Special Publications (SPs)

NISTIRs

ITL Bulletins

White Papers

Journal Articles

Conference Papers

Books

**TOPICS**

Security & Privacy

Applications

Technologies

Sectors

Laws & Regulations

Activities & Products

**NEWS & UPDATES****EVENTS****GLOSSARY****ABOUT CSRC**

Computer Security Division

Applied Cybersecurity Division

## Contact Us

### **Information Technology Laboratory**

#### **Computer Security Division**

TEL: 301.975.8443

#### **Applied Cybersecurity Division**

Contact CSRC Webmaster: [webmaster-csrc@nist.gov](mailto:webmaster-csrc@nist.gov)

---

[Privacy Statement](#) | [Privacy Policy](#) | [Security Notice](#) | [Accessibility Statement](#) | [NIST Privacy Program](#) | [No Fear Act Policy](#)

[Disclaimer](#) | [FOIA](#) | [Environmental Policy Statement](#) | [Cookie Disclaimer](#) | [Scientific Integrity Summary](#) | [NIST Information Quality Standards](#)

[Business USA](#) | [Commerce.gov](#) | [Healthcare.gov](#) | [Science.gov](#) | [USA.gov](#)