National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Cisco IronPort S-Series Web Security Appliance (WSA) (S160, S360, S660) running AsyncOS 5.6.1

Report Number: CCEVS-VR-VID10244-2009
Dated: 22 October 2009
Version: 2.5

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell, Senior Validator
Jean Hung, Lead Validator

Common Criteria Testing Laboratory

Terrie Diaz, Lead Evaluator
Science Applications International Corporation (SAIC)
Columbia, Maryland

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco IronPort S-Series Web Security Appliance (WSA) (S160, S360, S660) running AsyncOS 5.6.1.

The Validation Report presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of Cisco IronPort S-Series Web Security Appliance (WSA) (S160, S360, S660) running AsyncOS 5.6.1 was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory in the United States and was completed on 8 October 2009.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by SAIC. The ETR and test report used in developing this validation report were written by SAIC. The evaluation team determined the product to be Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL 2. The product is conformant with the U.S. Government Intrusion Detection System (IDS) System Protection Profile (IDSSPP), Version 1.6, April 4, 2006. All security functional requirements are derived from Part 2 of the Common Criteria or expressed in the form of Common Criteria Part 2 requirements.

The TOE is Cisco IronPort S-Series Web Security Appliance (WSA) (S160, S360, S660) running AsyncOS 5.6.1 provided by Cisco IronPort Systems, Inc. The TOE is an Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) that protects the enterprise against web-based malware and spyware programs, as well as providing protection for standard communication protocols.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced.

During this validation, the Validators determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the Validator concludes that the SAIC findings are accurate, the conclusions justified, and the conformance claims correct.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products, desiring a security evaluation, contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant; and
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Cisco IronPort S-Series Web Security Appliance (WSA) (S160, S360, S660) running AsyncOS 5.6.1
Protection Profile	U.S. Government Intrusion Detection System (IDS) System Protection Profile (IDSSPP), Version 1.6, April 4, 2006
ST:	Cisco IronPort S-Series Web Security Appliance Security Target, Version 1.0, 12 October 2009
Evaluation Technical Report	Evaluation Technical Report for Cisco IronPort S-Series Web Security Appliance (WSA) (S160, S360, S660) running AsyncOS 5.6.1, Part 1 (Non-Proprietary), Version 3.5, 22 October 2009, Part 2 (Proprietary),

Item	Identifier
	Version 2.0, 8 October 2009
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
Conformance Result	CC Part 2 extended and Part 3 conformant, EAL 2
Sponsor	Cisco IronPort Systems, Inc.
Developer	Cisco IronPort Systems, Inc.
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation (SAIC), Columbia, MD
CCEVS Validator	Paul Bicknell (Senior Validator), pab@mitre.org, (781) 271-3917 Jean Hung (Lead Validator), jhung@mitre.org, (781) 271-8824

3 TOE Security Functions

This section summarizes the security functions provided by the TOE:

- Security Audit :The TOE generates audit events for the basic level of audit. Note that the IDS_SDC and IDS_ANL requirements address the recording of results from IDS scanning, sensing and analyzing tasks (e.g., System data).

- Identification and Authentication: The TOE maintains user identities, authentication data, authorizations and groups. The administrative console provides the single TOE logon mechanisms for authorized Administrator to manage security functions. No user is allowed access to the security functions without being authenticated and identified by the system.

- Security Management: The TOE restricts the ability to administer functions related to auditing, use of the authentication mechanism, user security attributes, information flow control policy, scanning, sensing and analyzing tasks data (e.g., System data) to authorized Administrator.

- Protection of the TSF: The TOE provides a reliable timestamp for logging purposes and provides a security domain for its own use. The TOE also provides the ability to detect modification and to verify the integrity of all signature updates received from a remote update server in the IT environment of the TOE.

- Intrusion Detection System: The TOE monitors network traffic on containing malware and/or reputation policy data, acting as an IDS scanner. The TOE performs signature and integrity analysis on network traffic, security configuration changes, data introduction, detected known vulnerabilities and detected malware on monitored web traffic and records corresponding event data.

4 Assumptions, Policies, and Threats

The statement of TOE security environment describes the security aspects of the environment in which it is intended that the TOE will be used and the manner in which it is expected to be employed. The statement of TOE security environment therefore identifies the assumptions made on the operational environment and the intended method for the product, defines the threats that the product is designed to counter and the organizational security policies which the product is designed to comply.

Following are the assumptions identified in the Security Target:

- It is assumed the TOE is appropriately scalable to the IT System the TOE monitors and has access to all the IT System data it needs to perform its functions.
- It is assumed the TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
- It is assumed the processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access and modifications.
- It is assumed those responsible to manage the TOE are competent individuals, that only authorized users can gain access to the TOE, and that they are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

Following are the organizational security policies levied against the TOE and its environment as identified in the Security Target.

- All data collected and produced by the TOE shall only be used for authorized purposes and must be protected.
- The TOE must be protected from unauthorized accesses and disruptions of TOE data and functions.
- Users of the TOE must be accountable for their actions within the system.
- The TOE must collect data that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity.

- The TOE must perform analytical processes and information to derive conclusions about inappropriate activity (past, present, or future) on collected system data and appropriate response actions taken.

Following are the threats levied against the TOE and its environment as identified in the Security Target. The threats that are identified are mitigated by the TOE and its environment. All of the threats identified in the ST are addressed.

- An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
- An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
- An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
- An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
- An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
- An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
- An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
- Unauthorized attempts to access TOE data or security functions may go undetected.

The TOE is an Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) that protects the enterprise against web-based malware and spyware. The TOE also provides protection for the following standard communication protocols: Hyper-Text Transfer Protocol (HTTP), Secure HTTP (HTTPS) and File Transfer Protocol (FTP). Additionally, the TOE can be characterized as a network application security and gateway device.

5 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 2 extended in this case).
2. As with all EAL 2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one

that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

3. Cryptographic protection of signature updates is provided by the TOE; however, the cryptography used in this product was not analyzed or tested to conform to cryptographic standards during this evaluation.

6 Architectural Information

This section provides a high level description of the TOE and its components as described in the Security Target.

The TOE is an Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) that protects the enterprise against web-based malware and spyware programs, as well as providing protection for standard communication protocols.

The TOE analyzes the characteristics of web requests and responses and makes determinations regarding whether the request or response will be blocked, monitored, or allowed. The TOE provides two independent sets of security services to fulfill its objectives, Web Proxy Services and the Layer 4 (L4) Traffic Monitor.

Web Proxy Services examine outbound client requests and consist of four features, which work in concert to prevent users from accessing known or suspected malware distribution vectors. The four features of Web Proxy Services are:

Policy Groups – administrator defined groups of users, which specify exceptions to global policy settings based on client IP address, authentication group, or username.

Uniform Resource Locator (URL) Filters – control user access to URLs based on the category of a particular HTTP request.

Web Reputation Filters – analyze web server behavior and characteristics to identify suspicious activity.

Anti-Malware Scanning – when a URL has a questionable reputation, the HTTP traffic receives an in-depth inspection using the IronPort Dynamic Vectoring and Streaming (DVS) engine in concert with the Webroot Signature database.

The L4 Traffic Monitor detects rogue traffic by monitoring all network traffic received on all Transmission Control Protocol (TCP) ports on the appliance and matching that traffic to an internal database based on domain names and Internet Protocol (IP) addresses

The TOE is installed as self-contained network appliance. The physical boundary of the TOE extends to the RJ45 network interface connections that serve as the connection point between the TOE and the IT environment. The TOE requires either a L4 switch or a WCCP router in the IT environment to direct client traffic to the appliance.

Table 1 – TOE Physical Interfaces

Label	Purpose
T1	L4 Traffic Monitor (passive): In simplex mode – monitors all outgoing network traffic In duplex mode – monitors all incoming and outgoing network traffic
T2	L4 Traffic Monitor (passive): Simplex mode only – monitors all incoming network traffic
P1	Proxy port (active) – connects the TOE to an L4 switch or Web Cache Coordination Protocol (WCCP) router in the environment
P2	Unused – disabled
M1	Management port (active) – connects the appliance Personal Computer (PC) or management network for configuration and administration of the TOE
M2	Unused – disabled

The TOE is intended to monitor a computer network that is considered part of its Information Technology (IT) environment. There are expectations that the environment provides hardware to which the TOE can attach so that monitoring can take place and so that HTTP traffic is routed through the TOE. The intended hardware environment and suggested configuration are detailed in the following diagram. Note, the connection for passive monitoring in the diagram below is to illustrate the connection to the TOE itself, not a separate device.

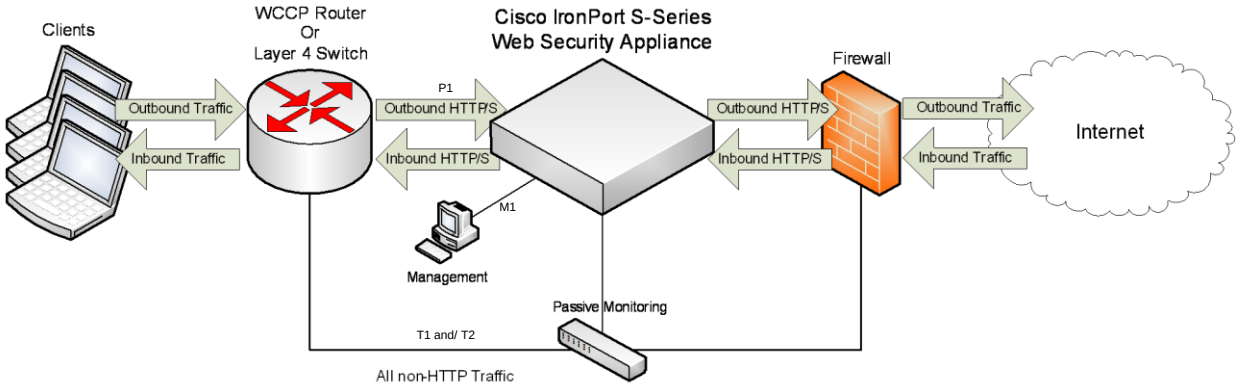

Figure 1 – TOE Environment and Traffic Flow

The Graphical User Interface (GUI) used for TOE administration requires a web browser that is installed on a dedicated PC physically connected via an isolated (private) Ethernet

management network. There are no limitations on the selection of the web browser. The CLI is available via a terminal physically connected to the serial port.

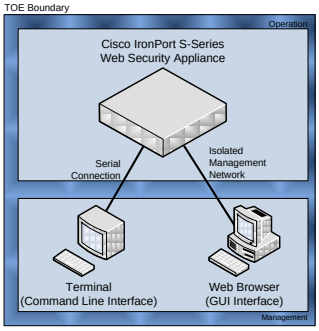

Figure 2 - TOE Boundary

7 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor).

7.1 Design documentation

Document	Version	Date
Cisco IronPort S-Series Web Security Appliance Design Document (HLD, FSP, and RCR)	6	29 July 2009

7.2 Guidance documentation

Document	Version	Date
ASYNCOS™ 5.6.1 USER GUIDE for Web Security Appliances	Part Number 421-0524	8 September 2008
Cisco IronPort S-Series Web Security Appliance running AsyncOS™ 5.6.1 COMMON CRITERIA GUIDE for IronPort Appliances	Part Number 421-0073	29 July 2009
IronPort AsyncOS™ 5.6.1 RELEASE NOTES for Web Security Appliances	Part Number 423-0070(B)	11 May 2009
Networking Worksheet IronPort S-Series Web Security Appliance (Quick Start Guide)	Part Number 421-0502(B)	

7.3 Configuration Management documentation

Document	Version	Date
IronPort Configuration Management Plan	Version 0.7	2008/12/17

7.4 Delivery and Operation documentation

Document	Version	Date
IronPort Delivery Procedures	Version 2	7 May 2009

7.5 Test documentation

Document	Version	Date
Cisco IronPort S Series Web Security Appliance Test Document (FUN and COV) EDCS-767742	Version 1.2	11 August 2009
Test Case mapping Table	Version 1.1	28 May 2009

The actual test results have been submitted to the evaluation team in various log files. The Test document also includes snippets of the logs and screenshots within the test case.

7.6 Vulnerability Assessment documentation

Document	Version	Date
IronPort Vulnerability Analysis	Version 0.4	4 August 2009
IronPort Strength of Function Analysis	Version 0.1	9 March 2009

7.7 Security Target

Document	Version	Date
Cisco IronPort S-Series Web Security Appliance Security Target	1.0	12 October 2009

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

8.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function tested. The scope of the developer tests included all the TOE Security Function Interface (TSFI). The testing covered the security functional requirements in the ST including: Security audit, Identification and authentication, Security management, Protection of the TSF, and Intrusion Detection (EXP). All security functions were tested and the TOE behaved as expected. The evaluation team determined that the developer's actual test results matched the vendor's expected results.

8.2 Evaluation Team Independent Testing

The evaluation team exercised a subset of the vendor's test cases manual test suite between three appliance models; S160, S360, and S660. In addition to rerunning the vendor's tests, the evaluation team developed a set of independent team tests to address areas of the ST that did not seem completely addressed by the vendor's test suite, or areas where the ST did not seem completely clear. All were run as manual tests.

The vendor provided the IronPort appliances, management console, and the necessary computers for the test environment.

The following hardware is necessary to create the test configuration:

- TOE Hardware
  - IronPort hardware appliance versions S160, S360, and S660
- IT Environment Hardware
  - One commodity Windows-based PC acting as a client,
  - One commodity Windows-based PC acting as a FreeBSD based Web Server
  - One commodity Windows-based PC acting as a e-mail server
  - One WCCP Capable Cisco ASA 5505 device, a terminal application and a web browser application

The following software is required to be installed on the machines used for the test:

- TOE Software
  - Above TOE Hardware running AsyncOS version 5.6.1
- IT Environment Software
  - Windows operating system (XP)
  - FreeBSD based Web Server
  - MS Exchange/other e-mail application
  - Putty

In addition to developer testing, the evaluation team conducted its own suite of tests, which were developed independently of the sponsor. These also completed successfully.

8.3 Penetration Testing

The evaluators developed penetration tests to address the Protection of the TSF security function, as well as expanding upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no vulnerabilities in the specific functions provided by the TOE.

9 Evaluated Configuration

The evaluated configuration requires one IronPort hardware appliance versions S160, S360, or S660 running IronPort AsyncOS software v5.6.1. The TOE's physical interfaces consist of six (6) RJ45 Interfaces operating at gigabit speeds. The interfaces are detailed below:

Label	Purpose
T1	L4 Traffic Monitor (passive): In simplex mode – monitors all outgoing network traffic In duplex mode – monitors all incoming and outgoing network traffic
T2	L4 Traffic Monitor (passive): Simplex mode only – monitors all incoming network traffic
P1	Proxy port (active) – connects the TOE to an L4 switch or Web Cache Coordination Protocol (WCCP) router in the environment
P2	Unused – disabled
M1	Management port (active) – connects the appliance Personal Computer (PC) or management network for configuration and administration of the TOE
M2	Unused – disabled

The TOE is intended to monitor a computer network that is considered part of its Information Technology (IT) environment. There are expectations that the environment provides hardware to which the TOE can attach so that monitoring can take place and so that HTTP traffic is routed through the TOE.

For specific configuration settings required in the evaluated configuration see ASYNCOS™ 5.6.1 USER GUIDE for Web Security Appliances and IronPort Web Security Appliance running AsyncOS™ 5.6.1 COMMON CRITERIA GUIDE for IronPort Appliances.

10 Results of the Evaluation

The evaluation was conducted based upon the Common Criteria (CC), Version 2.3, dated August 2005; the Common Evaluation Methodology (CEM), Version 2.3, dated August 2005; and all applicable International Interpretations in effect on December 2005. The evaluation confirmed that the Cisco IronPort S-Series Web Security Appliance (WSA) (S160, S360, S660) running AsyncOS 5.6.1 product is compliant with the Common Criteria Version 2.3, functional requirements (Part 2), Part 2 extended, and assurance requirements (Part 3) for EAL 2. The product is conformant with the U.S. Government Intrusion Detection System (IDS) System Protection Profile (IDSSPP), Version 1.6, April 4, 2006. The details of the evaluation are recorded in the CCTL's evaluation technical report; Final Evaluation Technical Report for the Cisco IronPort S-Series Web Security Appliance (WSA) (S160, S360, S660) running AsyncOS 5.6.1, Part 1 (Non-Proprietary) and Part 2 (Proprietary). The product was evaluated and tested against the claims presented in the Cisco IronPort S-Series Web Security Appliance Security Target, Version 1.0, 12 October 2009.

The Validators followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The Validators observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The Validators therefore conclude that the evaluation team's results are correct and complete.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL.

10.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of threats, policies, and assumptions, a statement of security requirements claimed to be met by the Cisco IronPort S-Series Web Security Appliance (WSA) (S160, S360, S660) running AsyncOS 5.6.1 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

10.2 Evaluation of the CM capabilities (ACM)

The evaluation team applied each EAL 2 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. In addition the evaluation team ensured changes to the implementation representation are controlled and that TOE associated configuration item modifications is properly controlled.

10.3 Evaluation of the Delivery and Operation documents (ADO)

The evaluation team applied each EAL 2 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed identification of the TOE and allows for detection of unauthorized modifications of the TOE. The evaluation team followed the ASYNCOS™ 5.6.1 USER GUIDE for Web Security Appliances and IronPort Web Security Appliance running AsyncOS™ 5.6.1 COMMON CRITERIA GUIDE for IronPort Appliances to test the installation procedures to ensure the procedures result in the evaluated configuration.

10.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and high-level design documents. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

10.5 Evaluation of the guidance documents (AGD)

The evaluation team applied each EAL 2 AGD CEM work unit. The evaluation team ensured the adequacy of the guidance documents in describing how to securely administer the TOE. The ASYNCOS™ 5.6.1 USER GUIDE for Web Security Appliances and IronPort Web Security Appliance running AsyncOS™ 5.6.1 COMMON CRITERIA GUIDE for IronPort Appliances were assessed during the design and testing phases of the evaluation to ensure it was complete.

10.6 Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation Team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team exercised a subset of the complete Vendor test suite and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

10.7 Vulnerability Assessment Activity (AVA)

The Evaluation Team applied each EAL 2 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer vulnerability analysis and the evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

10.8 Summary of Evaluation Results

The Evaluation Team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation Team's performance of the entire set of the vendor's test suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

11 Validator Comments/Recommendations

All Validator concerns with respect to the evaluation have been addressed. No issues are outstanding.

12 Security Target

The Security Target is identified Cisco IronPort S-Series Web Security Appliance Security Target, Version 1.0, 12 October 2009. The document identifies the security functional requirements (SFRs) that are levied on the TOE, which are necessary to implement the TOE security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 2.

13 Glossary

The following definitions are used throughout this document:

BSD	Berkely Software Distribution
CC	Common Criteria
CIDR	Classless Inter-Domain Routing
CLI	Command Line Interface
DVS	Dynamic Vectoring and Streaming
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hyper-text Transfer Protocol
HTTPS	Secure HTTP
ID	Identity / Identification
IDS	Intrusion Detection System
IDSSPP	IDS System PP
IE	Internet Explorer
IP	Internet Protocol
IPS	Intrusion Prevention System
IRC	Internet Relay Chat
IT	Information Technology
L4	Layer 4
LDAP	Lightweight Directory Access Protocol
LAN	Local Area Network
MIB	Management Information Base
NTLM	NT LAN Manager
OS	Operating System

P2P	Peer-to-Peer
PC	Personal Computer
PD	Precedent Decision
PP	Protection Profile
WBNP	SenderBase Network Participation
SFR	Security Functional Requirement
SHD	System Health Daemon
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
WBNP	SenderBase Network Participation
WBRS	Web Reputation Score
WCCP	Web Cache Coordination Protocol
WSA	Web Security Appliance
XML	eXtensible Markup Language

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 2.3, August 2005.

Common Criteria for Information Technology Security Evaluation - Part 2: Security Functional Requirements, Version 2.3, August 2005.

Common Criteria for Information Technology Security Evaluation - Part 3: Security Assurance Requirements, Version 2.3, August 2005.

Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005.

Evaluation Technical Report For Cisco IronPort S-Series Web Security Appliance (WSA) (S160, S360, S660) running AsyncOS 5.6.1 Part 2 (SAIC and Cisco IronPort Proprietary) Version 3.5, 22 October 2009 and Supplemental Team Test Report, Version 2.0, 8 October 2009.

Cisco IronPort S-Series Web Security Appliance Security Target, Version 1.0 12 October July 2009.

NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.